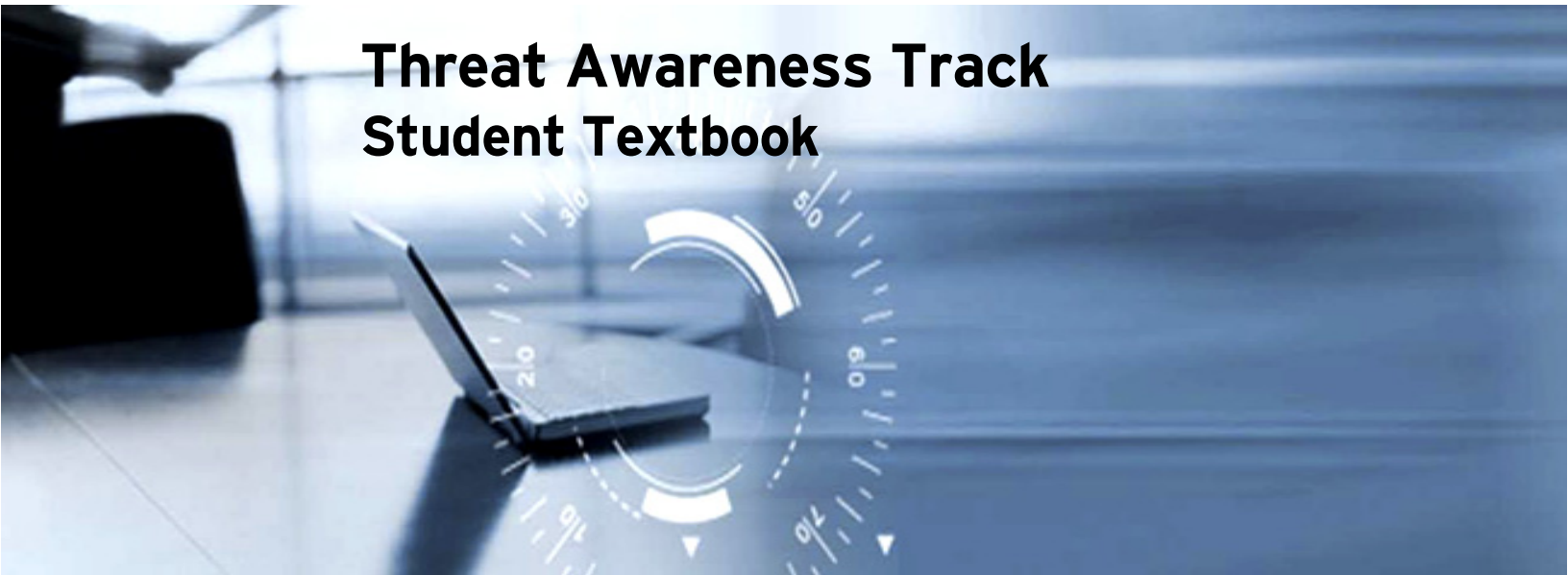




Trend Micro™ Fundamental Malware Awareness

Threat Awareness Track Student Textbook



Anti-Spyware



Anti-Spam



Antivirus



Anti-Phishing



Content & URL
Filtering



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Portions of this manual have been reprinted from the Trend Micro Understanding Unpredictable Threats 2 Training Course, copyright 2008 Trend Micro, Inc.

Copyright © 2008 Trend Micro Incorporated. All rights reserved.

No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Program Manager: Remo Mattei
Editorial: Sieloff

Released: June, 2008 v2.00



Table of Contents

Chapter 1: Trend Micro Fundamental Malware Awareness	5
1.1 > Course Objectives.....	6
1.2 > Target Audience and Prerequisites	6
1.3 > How to Use This Material	6
Chapter 2: The Threat Landscape.....	9
2.1 > Introduction to the Threat Landscape	10
2.1.1 What Is Threat Landscape?	10
2.1.2 Threat Landscape in Recent Years.....	10
2.1.3 Once Threat Landscapes featured the Global Outbreak	13
2.1.4 The 2005 Marks a Pivot Point in Threats	14
2.2 > Cyber Crime Grows	16
2.2.1 Money: Still the Main Driver for Malware Authors	17
2.2.2 Web Threats Emerged from the Shadows of Email Threats	22
2.2.3 Regional and Targeted Attacks Replace Global Outbreaks	22
2.2.4 Blended Threats are Better than One.....	23
2.2.5 Spam.....	23
2.2.6 Phishing.....	24
2.2.7 Spyware	24
2.3 > The Present: Threat Landscape	25
2.3.1 Infrastructure Vulnerabilities.....	26
2.3.2 High-Impact Threats.....	27
2.3.3 Content-Based Threats.....	29
2.3.4 Process-Based Threats.....	30
2.3.5 Distributed Threats.....	31
2.4 > Forecast on Future Threat Landscape	31
2.5 > Chapter 2 Summary and Review Questions	33
Chapter 3: Malware	35
3.1 > Introduction to Malware.....	36
3.1.1 What Is Malware?	36
3.1.2 Software Bugs vs. Malicious Activities.....	36
3.2 > Types of Malware.....	36
3.2.1 Virus	36
3.2.2 Worm	42
3.2.3 Trojan Horse.....	49
3.2.4 Understanding Malware Behavior.....	53
3.2.5 Rootkits	58
3.2.6 Blended Threats	58
3.3 > Understanding Malware Forms.....	58
3.3.1 Binary Malware	58
3.3.2 Encryption and Polymorphism.....	59
3.3.3 Packed Malwares.....	59
3.3.4 Macro Malwares.....	59

3.3.5 Script Malwares	60
3.4 > Defending Against Malware	61
3.5 > Chapter 3 Summary and Review Questions	62
Chapter 4: Grayware.....	65
4.1 > Introduction to Grayware	66
4.1.1 What Is A Grayware?.....	66
4.1.2 Classification of Grayware.....	66
4.2 > Understanding Grayware Behavior	78
4.2.1 Grayware Behavior during Installation.....	78
4.2.2 Grayware Behavior while Running.....	79
4.2.3 Grayware Behavior during Uninstallation.....	80
4.3 > Defending Against Grayware	81
4.4 > Chapter 4 Summary and Review Questions.....	82
Chapter 5: Web Threats.....	85
5.1 > Introduction to Web Threats	86
5.1.1 What is a Web Threat?	86
5.1.2 Web 1.0-Web 2.0 Security Implications.....	86
5.1.3 Impacts and Extent of Web Threats	87
5.2 > Social Engineering.....	87
5.2.1 What is Social Engineering?	88
5.2.2 Types of Message Content.....	88
5.3 > Forms of Web Threats	96
5.3.1 Spam.....	96
5.3.2 Hoax.....	99
5.3.3 Phishing	100
5.3.4 Pharming.....	104
5.3.5 Man-In-The-Middle Attack.....	105
5.3.6 Compromised Websites and Diseased Vectors	106
5.3.7 Botnets.....	107
5.4 > Defending Against Web Threats.....	108
5.5 > Chapter 5 Summary and Review Questions	109
Chapter 6: Using Trend Micro Solutions	111
6.1 > Trend Micro Smart Protection Network (SPN)	112
6.1.1 What is Trend Micro SPN?	112
6.1.2 A Multilayered Framework for Enterprise-Wide Protection.....	118
6.1.3 Multilayered Security	123
6.2 > Trend Micro Web Threat Protection Strategy	123
6.2.1 Integrated Multilayered Protection	123
6.3 > Trend Micro Free Tools and Services.....	125
6.3.1 Free AntiVirus Solutions	125
6.3.2 System Diagnostic Tools	126
6.3.3 Virus Encyclopedia	129
6.4 > Chapter 6 Summary and Review Questions.....	132
Appendix A: Answers to Review Questions	135



Chapter 1: Trend Micro Fundamental Malware Awareness

This course is designed for resellers and IT professionals responsible for protecting networks from virus attacks and other security threats. Those who will typically benefit the most include:

- System administrators
- Network engineers

Before you take this course, Trend Micro recommends that you have a working knowledge of Trend Micro products and services as well as of basic networking concepts and principles.



1.1 > Course Objectives

Taking this course should enable you to complete these knowledge- and skills-based tasks:

Knowledge

- Define and understand malware threats
- Define and understand grayware threats
- Define and understand Web-based threats
- Understand the Trend Micro Smart Protection Network (SPN)
- Understand the multi-layered approach to security used by Trend Micro
- Understand Trend Micro solutions and tools that support the Trend Micro SPN

Skills

- Define the security problems created by malware, grayware, and Web-based threats
- Differentiate between software bugs and malicious code that cause security threats
- Describe the techniques used by malicious code on your IT resources
- Identify social engineering threats
- Identify Trend Micro solutions that provide multi-level security against malware, grayware, and Web-based threats
- Describe the threat landscape, attack types that IT professionals currently face and are likely to face in the near future, based on developing trends in threat content

1.2 > Target Audience and Prerequisites

This course is designed for resellers and IT professionals responsible for protecting networks from virus attacks and other security threats. Those who will typically benefit the most include:

- System administrators
- Network engineers

Before you take this course, Trend Micro recommends that you have a working knowledge of Trend Micro products and services as well as of basic networking concepts and principles. You should also have a working knowledge of the following products:

- Windows 2000/2003 servers and clients
- Microsoft Internet Information Server (IIS)

1.3 > How to Use This Material

This training course combines instructor-led presentation with hands-on lab activities. It includes two manuals: this student manual, which provides the framework for the course, and a lab



manual, which identifies tasks that you can perform to develop key skills. Prompts to complete various lab activities appear in relevant locations throughout the textbook.

To help ensure that you learn the skills you need to install, configure, and manage Control Manager, this course has been created using a learning model that is based on:

Chapters - The student manual is divided into chapters. In addition to defining important concepts and terms, each chapter outlines the various administration tasks you need to perform.

Chapter Objectives - Each chapter starts with a list of objectives so that you can see how the chapter fits into your overall course goal. After reading the chapter, you should be able to fulfill the chapter objectives.

Summary and Review Questions - Each chapter ends with a summary that outlines the important information explained in the chapter and includes review questions that test your understanding of the material. After reading a chapter, if you cannot answer a question easily, please consider reviewing the chapter for any additional key points that you may have overlooked.

↪ Answers to review questions appear in Appendix A: *Answers to Review Questions* on pg. 135.



Chapter 2: The Threat Landscape

Chapter Objectives

After completing this chapter, you should be able to:

- Recognize past, present, and future threat landscape
- Determine how malware threats has evolved since 2005 up to the present



2.1 > Introduction to the Threat Landscape

The threat landscape could be a concern to almost everyone who owns or uses a computer. Knowing which threats exist and how professionals combat the threats is important to personal and asset-related security. Today's threat landscape has evolved from global attacks to targeted attacks with data harvesting and cyber crime at the foundation of most new threats.

2.1.1 What Is Threat Landscape?

The term threat landscape describes the trends of malware and threat evolution as the years go by. Of particular growth in the threat landscape are Web Threats. The nature of threats is changing from widespread to "targeted" and regional, and the web, in addition to email, is emerging as a powerful infection vector. Malware creators have an ever increasing and technologically sophisticated tool set at their disposal, comprised of bots and botnets, rootkits, social engineering, spyware and adware, and are motivated more than ever by financial gain. The threats they craft are becoming increasingly surreptitious and have many variants-all with the goal of evading detection.

The information that you are about to review shows how dangerous the Web is for computer users. As a security professional, your work fighting the threat landscape appears to be ongoing.

2.1.2 Threat Landscape in Recent Years

Consider how many changes have occurred in recent years. For example, 2005 could be referred to as the "Year of Grayware", with 65% of the top 15 threats noted, below – responsible for nearly 11 million unique reports – having included some sort of spyware, adware, backdoor, rootkit, or bot functionality. Some other statistics to note, regarding the total threat landscape of recent years:

- 10% were BOTs
- 11% were Spyware trojans
- 18% were Adware
- 0.60% were Rootkits
- 0.60% were Office macros
- 3% were Scripts
- 25% were viruses or worms
- 27% were Trojan horses (including rootkits)



Trend Micro has created the term Web Threat, back in 2005, because we saw an increase in new generation malware, where the malware relies on the Internet to download additional components. Web Threats is described in Figure 2-1.

Google Technical Report provos-2008a
All Your iFRAMES Point to Us
 Niels Provos Panayiotis Mavrommatis
 MoheebAbu Rajab Fabian Monroe

1.3% of the incoming search queries to Google's search engine returned at least one URL labeled as malicious in the results page

Abstract

As the web continues to play an ever increasing role in information exchange, so too is it becoming the prevailing platform for infecting vulnerable hosts. In this paper, we provide a detailed study of the pervasiveness of so-called drive-by downloads on the Internet. Drive-by downloads are caused by URLs that attempt to exploit their visitors and cause malware to be installed and run automatically. Our analysis of billions of URLs over a 10 month period shows that a non-trivial amount, of over 3 million malicious URLs, initiate drive-by downloads. An even more troubling finding is that approximately 1.3% of the incoming search queries to Google's search engine returned at least one URL labeled as malicious in the results page. We also explore several aspects of the drive-by downloads problem. We study the relationship between the user browsing habits and exposure to malware, the different techniques used to lure the user into the malware distribution networks, and the different properties of these networks.

Figure 2-1: Web Threats abstract (Source: Google Technical Report, Niels Provos, 2008).

Since early 2005, Trend Micro put malware as defined into the category Web Threats. As you can see, in Figure 2-2, Web Threats increase dramatically. It could be noted, that traditional malware only increased by 22% over the same time period.

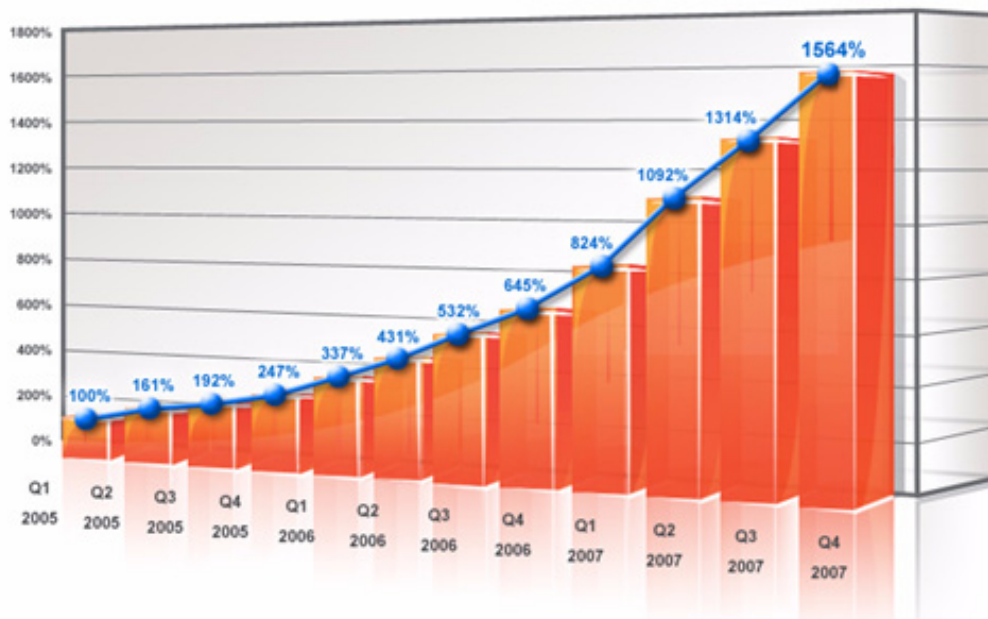


Figure 2-2: Increase in Web Threats from 100% in 2005 to 1600% at the end of 2007.

Shown on the next page are the Top 15 threats of 2005 taken at face value. WORM_NETSKY.P was on the charts for almost two years since the first variant was discovered in March of 2004 and remained the top threat affecting computers ever since – with

the exception of September 2005, where variants of TROJ_AGENT and TROJ_DLOADER took both of the top spots. The latter two are basic downloader Trojans and have been linked to adware and spyware attacks. Their prevalence is noted among the top grayware threats, with a combined number of installations nearly equal to the number of NETSKY infections.

PE_PARITE.A was first discovered in January 2001 and has proven to be surprisingly tenacious, despite many contemporary antivirus solutions. It injects its code as part of the Windows Explorer.exe file, thereby making itself part of every normal operation. This is a prime example of a pseudo-user-mode rootkit. By affecting how Explorer.exe works PARITE is able to gain pre-control over processes and quickly infect other executables (*.EXE) as well as screen-savers (*.SCR).

First detected in November of 1999, PE_FUNLOVE.4099 is the oldest file infector to appear in the chart. This threat also acted as a network worm and thus had the capability to more easily propagate, since network shares have historically proven to be the most effective threat vector. This infector also dropped viral code and patched the files NTLDR and NTOSKrn.exe, thereby enabling it to bypass the file-integrity checking by Windows for the NT Boot Loader Kernel, as well as the integrity checking of infected Windows files. Thus, via a pseudo-kernel-mode rootkit function, this malware was able to defeat the security implementation available to protect Windows users from viruses at the time, and continue to be active for more than 5 years. Due to its complex infection routine, FUNLOVE has been used as a payload by both WORM_BRAID and WORM_WINEVAR, and in a recent discovery of double-infections by riding piggy-back on the WORM_BAGLE.H variant which resulted in a new family called WORM_FUNBAG, initially found in March of 2004.

Top 15 Infections for 2005*		
Name	Count	Type
WORM_NETSKY.P	1,602,069	Worm
JAVA_BYTEVER.A	667,448	Java applet
PE_PARITE.A	320,924	File infector
TSPY_SMALL.SN	268,171	Grayware
WORM_NETSKY.D	242,243	Worm
SPYW_GATOR.B	163,495	Grayware
PE_FUNLOVE.4099	147,416	File infector
VBS_REDLOFA	145,701	VBScript
HKTL_RADMIN.A	63,557	Grayware
PE_ZAFI.B	62,708	File infector
ADW_SOLU180.A	61,929	Grayware
PE_TENGA.A	44,036	File infector
PE_JEEFO.A	27,831	File infector
PE_LOVGATE.AC	25,598	File infector
PE_NIMDA.A	16,824	Worm

Figure 2-3: Top 15 Infections for 2005. *These threats were at the forefront not too long ago.



PE_ZAFI.B, first seen in June of 2004, may not have been the first file-infector and worm, nor was it the first bi-lingual virus delivering both English and German mass-mailed messages. However, its combination of dropping infected copies in P2P shares and preventing users from checking their tasklist or Windows registry has enabled it to propagate enough to become one of 2005's most widespread infections.

VBS_REDLOF.A is a special case that underlines the danger of using HTML-formatted email or browsing non-work related websites. It exploits an old MS Virtual Machine ActiveX vulnerability and has a patch dating back to October 2000, so it seems surprising that this threat (released in August of 2004) still manages to show up on our radar. Its most dangerous payload is that it infects all web extensions (*.html, *.htm, *.asp, *.php, *.jsp, and *.vbs), as well as the default Outlook Stationary, thereby causing all outgoing messages to be infected – and spreading virally to recipients.

2.1.3 Once Threat Landscapes featured the Global Outbreak

At one point in the recent past, the threat landscape saw an increasing number of outbreaks related to malicious code—worms with global implications. With this rise came increasing danger of damage, theft, and destruction to computer assets and data on a global scale. The chart in Figure 2-4 illustrates the point.

Outbreaks of 2005*			
Name	Date declared	Quarterly	Count
WORM_BEAGLE.AZ	Wednesday, January 26, 2005	Q1 (6)	1
WORM_BROPIA.F	Wednesday, February 2, 2005	Q1 (6)	2
WORM_MYDOOM.BB	Wednesday, February 16 2005	Q1 (6)	3
WORM.BEAGLE.BE	Tuesday, March 01, 2005	Q1 (6)	4
WORM.FATSO.A	Monday, March 07, 2005	Q1 (6)	5
WORM.KELVIR.B	Monday, March 07, 2005	Q1 (6)	6
WORM_SOBER.S	Monday, May 02, 2005	Q2 (7)	7
WORM_MYTOB.ED	Sunday, May 08, 2005	Q2 (7)	8
WORM.MYTOB.EG	Monday, May 09, 2005	Q2 (7)	9
WORM.WURMARK.J	Wednesday, May 11, 2005	Q2 (7)	10
WORM.MYTOB.AR	Sunday, May 29, 2005	Q2 (7)	11
WORM.MYTOB.BI	Tuesday, May 31, 2005	Q2 (7)	12
WORM_BOBAX.P	Friday, June 03, 2005	Q2 (7)	13
WORM_ZOTOB.D	Tuesday, August 16, 2005	Q3 (2)	14
WORM_RBOT.CBQ	Tuesday, August 16, 2005	Q3 (2)	15
WORM_SOBER.AC	Wednesday, October 05, 2005	Q4 (3)	16
WORM_SOBER.AG	Monday, November 21, 2005	Q4 (3)	17
WORM_MYTOB.MX	Thursday, November 24, 2005	Q4 (3)	18

Figure 2-4: Outbreaks of 2005 with global implications.

For all the alerts declared during 2005, 26% were due to variants of WORM_MYTOB, a combined threat resulting from grafting parts of WORM_MYDOOM, which caused widespread infections in 2004, with BOT components. Its success stems from a host of previously known effective infiltration techniques such as trumping users seeking help by modifying the HOSTS file, as well as fake mail delivery failure messages leading on users to closely examine errors in transmission. WORM_SOBER variants comprised 16% of outbreaks in 2005, due to its bilingual approach in its spammed messages. Similar to WORM_MYTOB, this threat included retaliation techniques against major antivirus products by attempting to disable them from memory and thus safely drop its malicious components undetected. The use of major world events like the “FIFA World Cup” match in Germany, a technique borrowed from spammers, also lent to this threat’s successful propagation. Through the use of unsecured network shared folders and the wide use of P2P applications, WORM_BAGLE variants accounted for 11% of world wide threats to enterprises. Similar to the top outbreak families of 2005, WORM_BAGLE also used retaliation techniques as well as faked mail delivery errors to bait users.

2.1.4 The 2005 Marks a Pivot Point in Threats

In 2005, the vast majority of threats were inspired by financial gain, rather than the apparent desire for notoriety or bragging rights that influenced malicious behavior in prior years. These attackers preyed on users with the intention of information theft. As such, they invented whatever tricks they could, as modern-day con artists with a worldwide field of millions serving as potential victims. *The switch in motivation changed the very fabric of the threat landscape.* New malware is mostly inspired by *financial gain*. We are observing more and more targeted attacks focusing on a certain company and their users, or on a particular group with a common connection. Specially crafted Trojans are spammed to these targets with the hopes that unsuspecting users will fall into the trap. Favoring this kind of slow spreading as opposed to the big worm infection dramatically increases the odds of the malware going undetected for a longer period of time. This strategy allows for gathering more confidential information before the Trojan is detected and removed.

2005 also bore witness to a new kind of attack, which Trend Micro calls “spy-phishing”, which borrows techniques from both phishing scams and pharming attacks – along with some new tricks – to target on-line banks, financial institutions, and other password-driven sites. In spy-phishing the author seeds email messages with either a Trojan, or a link to download the Trojan. When downloaded and executed, either manually or via an exploited vulnerability, this malware monitors web traffic until it detects web access to the target page. When this happens, it sends any login or confidential data back to the attacker. There have been different variants targeting specific entities or related web companies, all with the same objective. The text in the spammed email can be related to the target company, or it can employ other forms of social engineering, similar to those utilized for traditional viruses. In either case, the effect is more dangerous than traditional Phishing, since it does not have to rely on tricking the user into visiting a spoofed site. And since it is such easier from a technical perspective than launching a Pharming attack, even so-called “script-kiddies” can potentially launch a successful attack. Spy-phishing effectively starts with the authentic bank page when the user willingly logs in. And once the user enters his information, he proceeds to the intended site without interruption, so there is no unusual behavior that may alert him to a potential problem. The only difference is that the user’s information has also been diverted to a third party, who is now empowered to use the same to conduct illicit activities.

A prominent trend in the pivotal change in cyber crime in 2005 was the de facto usage of blended threats. Motivated by financial gain, attackers did not limit their activities to the theft of bank and e-commerce credentials. Many also infected victims’ systems with spyware, adware and other grayware. By including spyware and adware from third parties in their attacks, some



malware authors were able to participate in marketing campaigns that offered a commission per unit installed. So the more users the attacker infected, the more money he would make. Multi-trojan attacks started with a downloader/dropper program that only existed to bring more files to the system and install a variety of other trojans, adware, or spyware. This was not rare to see in 2005, and the trend was directly linked to the switch in motivation discussed above.

Each of the aforementioned techniques share one common element – the longer they stay undetected, the higher their prospects for success for the cyber criminal. Stealing information is an activity that has limited usefulness if its capabilities are active for only one day. The longer they are listening, the higher the probability of obtaining valuable information. This need to avoid detection had two immediate effects in the threat landscape of 2005:

- Malware authors learned, as far back as 2003, to use different packers in order to mask the internal structure of binary programs. Packer programs compress executable files to make them smaller, but they also make them different from the detection point of view of traditional scanners not using code emulation and behavioral analysis. Using this ability as a stealth factor can potentially prolong the life of the program, as antivirus vendors need to obtain the multiple samples to properly detect the malware variant. In 2005, attackers frequently spammed many different waves of the same malicious Trojan, each compressed with a different packer – and sometimes even using a combination of different packers – in an attempt to elude detection.
- Attackers have looked for other stealth methods and have found the most effective of them all: rootkits. Towards the end of 2005, rootkits were being used as the ultimate weapon to assist in cloaking malware and grayware activity. Rootkits modify the operating system behavior to hide certain processes, files, folders, and registry entries. This grants unparalleled power to the malicious application while making it vastly more complicated to detect and remove them. Since rootkits are publicly available – many use open source standards – even writers who do not possess the technical skills required to produce a rootkit can potentially utilize them because the work has already been done for them. As rootkits become increasingly popular among the malware writers, content security vendors must hone their tools to detect these devices. Trend Micro has observed rootkits as part of bot and Trojan tandems with increasing regularity, particularly in the third-quarter where more than 150,000 computers were found to have been affected.

Another important trend in malware in 2005 was the increased modularity of malware employed for attacks. Bot worms grew to be the fastest spreading malware, due primarily to the fact that many of them were readily available from open-source developments, built in a modular fashion. Any miscreant need only download the source code of these bots, select the modules to use and create a new variant.

By adding new modules to bot worms, malicious writers moved bots, a traditionally slow-spreading attack, to a new category: the most flexible malware ever. They can function as email worms, network worms, P2P worms, or all of these things simultaneously. With this increased flexibility, malware writers proved something else in 2005: they could add any new vulnerability exploit as soon as it was announced. In October of 2000, the NIMDA Worm took nearly a year to exploit the published vulnerability; by 2004, the release of SASSER had cut that number to 17 days; but in 2005, ZOTOB painted an alarming picture where it took only five days from the announcement of the vulnerability to the time when a successful exploit was added to a worm's code.

Now that bot worms have become the Swiss Army Knife of all malware with their email-spreading capabilities, network vulnerability exploitation, companion rootkits, and so on – detection numbers are on the rise. The main bot families have thousands of different variants

documented and as such pegged detections are in the millions. The usage of bot functionality in worms has not changed from the past.

Bot-net owners use them to upload spyware/adware, steal information, create spamming platforms, and launch distributed denial-of-service attacks against third parties. All of these offer financial gain to the bot-master in proportion to the number of victims in the bot-net. Once the bot-net has reached a considerable size, it can be sold or portions rented out for other malicious uses: as proxies for sending spammed emails, stealing private data, or uploading spyware or adware to the infected machines.

Since 2002, bot worms have been growing exponentially, and 2005 was no exception. They are becoming increasingly complex and dangerous and have demonstrated their ability to use network vulnerabilities as soon as they are found. In 2005, police and investigation units uncovered bot-nets consisting of more than 200,000 victims worldwide. Bots have easily become one of the most formidable threats to be reckoned with and quite possibly possess the highest potential for damage.

2.2 > Cyber Crime Grows

The year 2006 continued on the pivotal changes in financially-motivated cyber crime growth and showed a dramatic inclination toward malware-related threats. Additionally, crimeware-related Trojans gained notable prominence. Of the top 20 threats in 2006, 80% specifically involved viruses and worms.

Top 20 Threats	Reports
Name	Count
WORM_NYXEM.E	571,291
TROJ_Generic	569,845
HTML_NETSKY.P	386,943
WORM_NETSKY.DAM	242,609
PE_PARITE.A	235,476
SPYW_DASHBAR.300	234,565
SPYW_GATOR.F	216,291
WORM_MOFEL.B	191,205
WORM_NETSKY.P	175,084
JAVA_BYTEVER.A	167,738
EXPL_WMF.GEN	143,848
ADW_WEBSEARCH.K	142,994
WORM_ANIG.A	137,490
PE_FUNLOVE.4099	122,096
WORM_NETSKY.D	118,168
WORM_RONTKBR.GEN	115,849
WORM_RONTOKBRO.B	111,016
TROJ_ROOTKIT.E	107,915
BKDR_Generic	95,668
ADW_SLAGENT.A	95,067

Figure 2-5: Top 20 Threats in 2006 dominated by viruses and worms.

2.2.1 Money: Still the Main Driver for Malware Authors

In 2006, the overwhelming majority of malware attacks was driven by financial theft, and employed such tactics as password stealing, keylogging, and other related activities. Trend Micro and other industry analysts refer to this type of threat as crimeware—the fastest-growing threat in the malware category. It all started with malware vendors collaborating with the underground to create a cyber crime industry of large proportions, as shown in Figure 2-6.

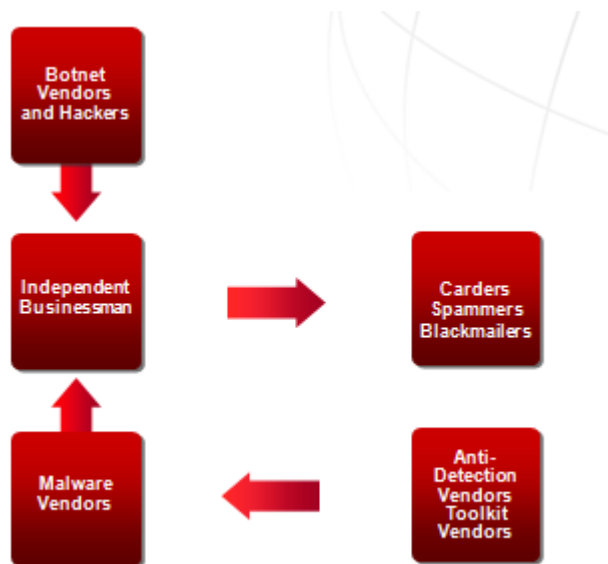


Figure 2-6: Collaboration in the underground.

Malware authors in the cyber crime industry include the likes of many malicious applications and strategies. Criminals in the underground world of cyber crime are often bold about their work:

David L. Smith/ Melissa	Smith wrote Melissa on his computer with a registered Winword version. Every computer has a unique Windows ID, called Global Unique Identifier (GUID). It seems like Microsoft worked with law enforcement and opened their database, because the GUID was send over to Microsoft "accidentally" during online product registration of Microsoft P\products.
Onel de Guzman/ ILOVEYOU	Guzman wrote a thesis proposal about a Trojan horse, which could be used to steal passwords to get free Internet access. The AMA Computer College rejected the thesis proposal, but based on his description, ILOVEYOU could be traced back to him.
Jeffrey Lee Parson/MS Blaster Variant	Parson embedded his nickname "teekid" within his Blaster-B code. Furthermore, one worm component was connected to a Webpage owned by him.
Sven Jaschan/Sasser	Sven Jaschan wrote the Netsky worms, as well as Sasser-A and several variants. He showed off at school, told fellow students what he did, and was betrayed by one of his friends, who wanted bounty money from Microsoft - which he reportedly received.

Crimeware

Few crimeware authors—or those cyber criminals writing malware application—write for malicious fun. The malware writers of today want to avoid attention; they want silent killers to be installed, unrecognized. They want the infection code to be stable and stealth-like. For this they get help from anti-detection vendors. These vendors test the malware against antivirus products to ensure that the infection is not recognized by the security product installed on the victims computer. Toolkit vendors provide malware construction kits or add on tools, which alter malware or which contains routines to install a rootkit, or/and disable Firewall and Antivirus components.

CRIMEWARE IS ON THE RISE

Crimeware is growing by leaps and bounds. As shown in Figure 2-8, malware binaries have grown 10 times over in the past 10 years.



Figure 2-8: Increases in malware binaries (2008 data based on projections from early 2008 Trend Micro data and AV-Test.org information).

Interestingly enough, Google also shows the steady increase of Web Threats. The data illustrates that the Web Threats from trusted search engines return millions of suspicious and malicious Web sites that prey on unsuspecting users.

Data Collection Period	Jan - Oct 2007
Total URLs Checked In-Depth	66,534,330
Total Suspicious Landing URLs	3,385,889
Total Malicious Landing URLs	3,417,590
Total Malicious Landing Sites	181,699
Total Distribution Sites	9,340

Table 2.1: It's all about Web Threats (Source: Google Technical Report, Niels Provos, 2008)



There has been an explosion in unique malware samples. AV-Test.org has seen roughly a 550% increase in samples between 2006 and 2007. It is worth noting that these numbers are also increasing because of variants, i.e., the same Trojan is changed sometimes hourly or daily, just to try and deceive the scanners. In this case, it is not the case that there are over 5 million unique pieces of malware. There are many that are variants of the same piece of malware. Nevertheless, this is a good representation of the staggering load of malware that anti-malware vendors help you fight.

PATHS TO THE PAYLOAD

All crimeware—from TSPY_BANCOS, which steals passwords, to TROJ_YABE, which attacks eBay users—follows three typical paths to their payloads: identity theft, extortion, and/or espionage. Once these efforts are successful, crimeware employs a variety of methods for actually stealing money—such as hijacking banking passwords, holding files captive under threat, or raiding proprietary corporate information.

COMMUNITY-FORMING MALWARE

Additionally, two other malware effects not directly related to crimeware—but popular among malicious attackers as a means of financial theft—include community-forming and the download of more malicious components. Community-forming malware is usually called a bot worm or, simply, a bot. A bot's primary objective is to achieve as broad a threat distribution as possible, while enabling its creator to maintain centralized control. Combining individual bots into a network—or botnet—increases the bots' power and enables creators to exploit this power over hundreds and thousands of PCs for financial gain. During 2006, botnets experienced significant growth—the most notable being the WORM_SDBOT family.

JOINT VENTURE ATTACKS

The financial motivation inherent in today's malware demonstrates that malicious attackers are no longer mere individuals, as in the past. Now, attacks are commonly executed as joint ventures among professional malware programmers with access to greater pooled resources—and such consortiums are dedicated to the creation and distribution of malicious software intended to steal money from individual and corporate victims.

CRIMEWARE COMBINES THREATS

Crimeware includes spyware and other keylogging Trojans, hacking tools, and phishing-related email spam. New hybrid combinations also have emerged, including spy-phishing—a targeted spyware attack in which a downloaded Trojan, programmed to steal specific information from a specific legitimate URL, activates and sends information to a malicious third party; and vishing—a targeted phishing attack using voice over IP (VoIP). Since the stakes for information theft are rising, applying the term crimeware to the above activities provides an appropriate level of understanding for computer users regarding the threats they face.

HACKING TOOLS

Hacking tools account for most crimeware-related threats. However, users should not feel reassured by the success of such old-fashioned infiltration techniques; the majority of systems remain ineffectively patched and firewalled against current threats, mostly due to new machines coming online, as well as users being unfamiliar with security concerns. Phishing, spyware, and spy-phishing are very real threats. Spy-phishing, especially, is a particular concern, as its two-pronged approach (see above) means that users are vulnerable the moment they visit an implicated URL. Even if users suspect a site and navigate away from it, the malware remaining on their machines completes the theft.

2.2.2 Web Threats Emerged from the Shadows of Email Threats

In the year 2006, most malware threats propagated via email. In 2006, attackers combined phishing emails with malicious attachments to create a strong attack vector, identified by Trend Micro as spy-phishing. Spy-phishing initially uses email spamming techniques to distribute messages which, in turn, rely on social engineering ploys to trick users into running malicious file attachments. Identity theft remains the highest objective for spy-phishing.

In addition to email, the second most prevalent means of malware distribution in 2006 was via the Web. Most often, attackers prey upon users' beliefs that a malicious program is needed or expected—and therefore legitimate. For example, in developed countries, increased Internet bandwidth has spawned explosive growth in video sharing and downloading. In order to view the variety of file formats available, users need codecs—small programs that encode and decode digital data streams—which are often available as downloads from video-sharing sites. Malware authors exploit this by regularly setting up bogus codecs in public networks; sometimes, they go so far as to create entire malware websites around the fake codec. The TROJ_ZLOB family consistently uses this strategy, masking files as “mandatory downloads” necessary to watch online videos.

Malware authors effectively use another Web-based distribution method: publishing malicious links in search engines, discussion forums, and other public places. These links point to download pages with heavily obfuscated script code in order to prevent detection. For example, the FEEBS worm attacked when a user visited a page containing one of these scripts—which enabled the worm to download and infect the user's computer.

New vulnerabilities surface every month, and malware creators respond by adding fresh network-spreading capabilities to their arsenal. This helps them acquire new, unprotected victims each time an exploitable vulnerability is made public. Ever since the Blaster worm first occurred in 2003, malware authors have very successfully exploited network vulnerabilities—immediately updating their libraries when a new vulnerability is released. Bot worms have traditionally been the fastest to incorporate support for newly published exploits.

New in 2006, Trend Micro observed malware that exploits client-side vulnerabilities. Such threats operate via exploit files which, when run, drop a piece of malware in the user's system. The WMF exploit marked this new trend in early January. Consisting of specially-created WMF image files, this attack exploited a vulnerability in the Widows image rendering engine, which allowed rogue code to execute once a user viewed the bogus image. Eventually, this code enabled crimeware. Similar waves of exploits followed, many of which took advantage of client-side vulnerabilities within the popular Microsoft Office suite, as well as applications such as the music player Winamp. Because users typically don't recognize these exploit files as threats—and therefore open them without consideration—the social engineering component in these cases is significant.

2.2.3 Regional and Targeted Attacks Replace Global Outbreaks

In 2006, Trend Micro observed that—with the exception of bot worms—most modern malware lacks the means to easily propagate. This fact implies that unlike older generations of malware, creators of modern threats intend their malware to remain localized. This greatly impacts the types of infections experienced by businesses and consumers alike.

For example, in 2004, a malware outbreak would have wreaked havoc on all seven continents—causing security companies to pursue an immediate solution for cleaning and preventing



infections. In 2006, malware outbreaks instead targeted email address lists, or visitors to a malicious Web page—and may only infect those specific computers. Once an attack is successful, today’s malware only remains active until it can steal a user’s personal information and, eventually, money.

“Targeted attacks” follow the same principle. Deployed in order to steal confidential information from specific companies, such threats mimic internal emails and target certain individuals within a given organization. As soon as even one user is tricked to run the attached malware file, the company becomes vulnerable to widespread theft of often vital data. Similar to a regional attack, a targeted attack is even narrower in scope with a more specialized objective.

Both regional and targeted attacks affect fewer users than in the past, and often involve blended threats. This presents a new challenge for security companies, for cleaning narrowly focused, self-updating malware is much more difficult than cleaning a widespread, static worm. Therefore, the threat landscape has become more dangerous than ever.

2.2.4 Blended Threats are Better than One

Although the term blended threats was coined a while ago, it has become increasingly relevant to today’s Internet landscape. In fact, most malware attacks in 2006 involved multiple pieces of malware.

Typically, a malware infection launches when a user—either wittingly or unwittingly—downloads an executable file that, in turn, downloads other malicious components and/or spyware. The unfortunate result is infection of the targeted computer by as many as four different types of malware, spyware, and adware—and sometimes, more. For example, in the Gromozon case of Q406, Italian users were tricked into visiting a malicious Web page. This page redirected users, via a script, to a chain of other pages that eventually caused users to download a file. This file then unleashed a malware download process that dropped adware and other components onto affected systems, installing and protecting it with a rootkit.

Similarly, also in Q406, the NUWAR worm attacked several different regions. NUWAR mass-emailed messages with “nuclear war” subject lines and an attached executable file. This file, when run, dropped a downloader component onto the affected machine and planted copies of the mass-mailer module; then, it downloaded four other components, including a new downloader (which enabled the import of new modules without detection) and a rootkit that hid the entire malware army. The unfortunate result was a collection of computers transformed into spam- and infectious-worm email generators. The main component of the NUWAR threat was a module that sent spam emails advertising stock sales.

Sadly, these are not isolated cases. Blended threats are a growing concern for all Internet users, and a challenge for antivirus companies. Trend Micro anticipates this type of attack to continue at least into the near future.

2.2.5 Spam

Spam is nothing new. Unsolicited advertising, bandwidth hogging, and productivity drops have been irritating users for at least several years—and in 2006, spam continued to rise.

One factor behind this spike involves the ways in which bot owners leverage their botnets to propagate spam. In this scenario, the email origination point constantly shifts among members of the botnet—which makes blacklisting as a defensive tactic nearly impossible. Similar

instances of using malware as a spamming platform have also been observed. The best example involves the STRAT worm distribution, which occurred in the third and fourth quarters of 2006. This worm behaved very much like a typical, fast-spreading massmailing worm, with a special twist: it spammed advertisements for an online pharmacy from each infected host. The NUWAR worm, mentioned previously, also used infected machines as spam-sending platforms. Trend Micro predicts this is not the last time such a plot will exhibit itself, which bodes poorly for all email users and their inboxes.

Incidentally, these spammer worms leverage the latest mass-mailing technique: image spam. In 2006, in order to bypass spam filters, spammers revived an old trick that has now become quite common: placing email advertising text within an image, and scattering random elements such as dots or lines throughout the text. The resulting complexity of such emails makes it difficult for heuristic engines and other antispam vehicles to detect image spam.

On average, Trend Micro identified more than two million different pieces of spam flooding the Internet each month. English is the predominant language used, likely due to its global application in the business world; English-language spam constituted 61% of all samples processed, representing a whopping 20% increase over 2005. Regionally targeted spam for the Japanese market was also on the rise. Chinese spam is the third largest, at more than a half-million pieces recorded in 2006.

Commercial spam (spam involving trading or Web-offers) represented 13% of all spam. This is an almost 5% drop from the 2005 value, likely due to spammers testing the effectiveness of new topics. Financial spam, such as offers for debt consolidation or mortgage programs, was a close second at 8% of the pie. Health-related spam came in third at 6%. The most successful spam leverages topics that are likely to be of concern to a majority of people—thus ensuring propagation via social engineering. Users who fall victim to such scams, however, are left with nothing—while scam artists make off with their money.

2.2.6 Phishing

By February of 2006, Trend Micro analyzed a growing average of 4,000 new phishing attacks each month.

Although samples are processed continuously on a daily basis, almost 60% of phishing sites have either been discovered and taken down, or have morphed to avoid detection, during the time in which an actual sample is received for processing. This underlines the need for products that either have permanent online connections or are equipped with heuristic technologies to effectively detect and block phishing sites.

Traditionally, phishers have used at least ten different techniques to lure users into their schemes. However, due to various browser improvements—as well as government- and private sector-sponsored awareness campaigns—only one of these techniques remains effective: address-bar spoofing. Address-bar spoofing abuses Java or ActiveX scripting to overlay a legitimate address bar with a fake image. Otherwise, more than 96% of all phishing attempts occur via explicit display of a spoofed URL, using a combination of character encoding to impart a false sense of security to users.

2.2.7 Spyware

The past several years have witnessed the rise of spyware and other non-malicious threats. These threats have been a concern for home and corporate users for two main reasons: the annoyance



their unsolicited advertising displays cause; and the data leakage their presence introduces. In 2006, spyware and adware have continued to increase, thanks to their creators' discovering innovative new ways of distributing them. As previously mentioned, many malware attacks are, in reality, blended threats that install spyware and/or adware on the infected computer—which vastly increases their dissemination. The fight against spyware is at its peak, and the market for anti-spyware software is growing.

On their own, aggressive marketing tactics may not appear to be much of a threat—but, especially recently, the results of such activities have included technological abuse. For example, spyware—which profiles users' activities and browsing preferences—feeds into a database that loads these preferences into adware campaigns designed to either promote more visits to a particular site, or to leverage the data to compete with a different brand.

TrendLabs has noticed—via almost four million spyware and adware reports—that several pieces of malware were used to generate click-through revenues. This means that the prevalence of spyware filtering solutions, unregulated markets may utilize malware in order to force marketing content onto users. Commercial spam already employs this approach, as with WORM_STRAT distributing pharmaceutical spam as part of its payload.

2.3 > The Present: Threat Landscape

The era of the global outbreak is over. Cyber crime is at an all-time high. Today's threats are:

Stealthy	Try to remain undetected
Regional & Targeted	Go after users in a specific region or country or users of a specific type of Website
Blended & Sequential	Use combinations of malware that each play a role in the delivery of the payload
Web-based	Use the Web for delivery, update, and entrenchment and to report back stolen information
Profit-driven	Goal is to make money

There are economies built around the creation, sale and utilization of malware. The year 2007 presented several examples of just how the threat landscape has evolved, including “Storm” at the beginning of the year and the “Italian Job,” which came later.

Trend Micro continues to see explosive growth in Web threats and little abatement in messaging threats. Web threats, threats that use the Internet to perform malicious activities unbeknownst to the PC user, persist in their utilization of automated techniques and exploitation of vulnerabilities to achieve identity and information theft. They target specific groups of users and employ blended techniques to accomplish their goals.

The technologies and techniques used for malicious purposes continue to grow more sophisticated. In the past 18 months, Trend Micro saw file infectors taking on new roles, social engineering techniques becoming very adept at leveraging current affairs, phishing scams targeting smaller regional establishments, and authentic looking email messages carrying malware. The use of Web 2.0 technologies, such as Javascript, was frequently used for drive-by-downloads, where users need only visit a malicious URL to become infected.

Within the year, there is a renewed vigilante-style interest in undiscovered application and OS vulnerabilities, as various Month of Bugs projects emerged to challenge software developers. As a result, malware exploiting these vulnerabilities was written and introduced into the wild. Web applications experienced the brunt of the attacks, as latent vulnerabilities were used in XSS and XSRF attacks targeting social networking sites.

Perhaps the most disturbing development is the persistent rise in the use of bots and botnets to distribute spam and malware and perpetrate cyber crimes. Many people who would not rob a bank, have few issues stealing credit card information and redirecting money, online. Botnets remain the most powerful tool at malware authors' disposal in the bid for computer-automated crime. Several malware activities during this period continue to betray a possible underground economy that harnesses the computing power of compromised computers to perform certain tasks.

In an effort to provide the best analysis, Trend Micro looks for new ways to analyze and understand the threat landscape as it evolves. This report examines threats in the following categories:

Infrastructure vulnerabilities	Threats that originate from the existence of security weaknesses in applications, network architecture or operating systems
High-impact threats	Threats that have the capacity to cause very high localized damage. Examples include global outbreaks and targeted attacks
Content-based threats	Threats which are delivered to the target victim as part of content, such as phishing or spam
Process-based threats	Threats that are in the form of an executable application resident on the host PC. Examples include malware, spyware and adware
Distributed threats	Threats, like bots, where the infection is used to mount an attack on a third party victim

2.3.1 Infrastructure Vulnerabilities

Malware authors rely on security holes in software applications to be able to introduce malicious code to a user's computer. Some proactively look for vulnerabilities and sell their information in digital black markets. Some wait for public disclosure of the vulnerability, then craft an exploit hoping to reach users before vendor updates are created. Inadvertently helping the cause were initiatives such as the "Month-of" projects—like January's Month of Apple Bugs and March's Month of PHP Bugs—where developers and programmers were encouraged to find and flag software holes.

XSS: A Bane to the Web 2.0 Boon

Vulnerabilities exist not only in software products but also in Internet applications, such as cross-site scripting. JS_QSPACE.A, a malicious JavaScript discovered December 2006, took advantage of a QuickTime HREF Track feature and MySpace XSS vulnerability. Later in March, a new malicious script exploiting another flaw in QuickTime in conjunction with MySpace was detected as JS_SPACESTALK.A. It is imperative that developers of Web 2.0 applications balance providing innovative applications and elegant usability with secure applications. Often, security is the second priority.



Vector Markup Language Exploits

A week after the January 9, 2007 release of Microsoft patches, which addressed the way Windows handles Vector Markup Language, an exploit for the patch appeared in the wild. It was soon followed by several other variants at a rate of almost two a month. This illustrates the importance of keeping a computer updated with the latest patches, considering the speed with which exploits are created soon after vulnerabilities are discovered.

Exploit Toolkits

Another trend is the proliferation of exploit toolkits. These toolkits automate the generation of code that is used to exploit known vulnerabilities.

Exploit kits for MS07-017 were also discovered. In the same vein, other commercial-grade software, such as MPack which was used in the Italian Job IFrame attack, are being sold and distributed in underground channels. These exploit kits are continuously updated as new vulnerabilities are discovered and purchasers are able to pay to upgrade. This further makes the creation of code targeting unpatched systems easier for script kiddies.

Other Notable Exploits

Several Trojans were discovered to exploit Windows applications, specifically Microsoft® Office Word. These proof-of-concept Trojans remained in the wild as December's Patch Tuesday (Microsoft's regular release of security bulletins addressing identified software vulnerabilities) came and went. The popularity of this exploit is attributable to the universality of Word. Other variants exploiting Microsoft Office Excel and PowerPoint soon followed.

In December 2006, Microsoft confirmed the existence of the first Windows® Vista flaw, a Proof-of-Concept code that targeted the Client Server Run-Time Subsystem. Other operating platforms were not immune, including the Sun Solaris 10 Telnet service which became exposed in February (ELF_WANUK.A).

Over past several months there has been an active bounty hunt for software vulnerabilities, translating into an increase in malware exploits. The most notable, the Windows ANI vulnerability relating to the way Windows handles animated cursors, caused Microsoft to release an out-of-cycle patch as reports of infections quickly rose.

2.3.2 High-Impact Threats

The high-impact threats from the first half of this year illustrate how malware authors can deploy codes that specifically target victims with the help of social engineering.

The Stormy Saga of TROJ_SMALL.EDW Mutations

The NUWAR family emerged in 2006, but it made headlines in January 2007, when specific Trojan variants arrived via spammed email messages. Leveraging a 200-kph storm ravaging Eastern Europe, a slew of email messages containing the subject "230 dead as storm batters Europe" were spammed to unsuspecting recipients. Concerned and curious, recipients who were lured into opening the attachments named full Clip.exe, full Story.exe, full Video.exe, and read More.exe, inadvertently introduced a Trojan downloader onto their computers.

In April, a WORM_NUWAR variant was detected to be carrying TROJ_SMALL.EDW, the same Trojan that made its rounds in Europe earlier in the year, only this time the subject headers were the following ominous but unreal pronouncements:

- Iran Just Have Started World War III (sic)
- Israel Just Have Started World War III (sic)
- Missle Strike: The USA kills more then 1000 Iranian citizens
- Missle Strike: The USA kills more then 10000 Iranian citizens
- Missle Strike: The USA kills more then 20000 Iranian citizens
- USA Declares War on Iran
- USA Just Have Started World War III (sic)
- USA Missle Strike: Iran War just have started (sic)

Email worms from the same family sent other messages with catchy headlines such as: 'Spyware Activity Detected!', 'Virus Alert!', 'Worm Detected!', 'A Token of My Love', 'Come Dance with Me,' and 'Our Love Will Last'.

The persistence of these infections relies on the authors' ability to craft engaging and timely subject headers in order to hook more victims in a short amount of time. As the infection counts show, although more than half of the infections remain in North America, numbers from Asia and Europe are still increasing.

TROJ_SMALL.GHI Spreads False News of Australian PM's Death

SMALL continued to find victims. February found unsuspecting Australians clicking on mass-mailed email messages purporting to contain details about the supposed heart attack of Australian PM John Howard. Among the subject lines the email messages used are the following:

- Current Australia's Prime Minister survived a hear (sic) attack
- The life of the Prime Minister is in grave danger
- Prime Minister survived a heard (sic) attack

The email message even contained a link to a bogus news site specially crafted to mirror the popular legitimate Web site The Australian. The fake site had a second invisible IFrame that covertly accessed a second URL with obfuscated scripts which, in turn, took advantage of old Internet Explorer vulnerabilities. This set in motion a download routine that was as complex as it was coordinated.

First, a Trojan downloader checked to eliminate systems located in Estonia, Latvia, and Lithuania—possibly because the malware creators were from these countries and wanted to avoid rousing the suspicion of local authorities.

Second, a backdoor component dropped another component that served as its watchdog as it sent and received messages to specific servers via random ports. The servers behaved like bot masters, raising the suspicion that the backdoor could have been a creator of an impromptu zombie network.



TROJ_ANICMOO.AX Tricks Asian Animated Cursor Fans

In March 2007, a Trojan exploiting an unknown vulnerability in the way Windows handles animated cursors prompted Microsoft to release an out-of-cycle patch. This .ANI file downloaded other malware from malicious URLs. 83% of the infections occurred in Asian countries. While the motive remains unknown, the attack may provide insight as to where the malware author resides or who his intended victims were.

JS_DLOADER.KQZ Spoils Super Bowl Weekend for Football Junkies

During the first week of February 2007, malware authors attempted to capitalize on Super Bowl XLI in the United States. They created a malicious script, hacked into the official site of the Miami Dolphins Stadium, and delivered a keylogger to anyone who happened to visit the site as part of a “drive-by-download.” The malware associated with this attack included TROJ_ZLOB.BZE, which downloaded a spyware once the user visited the hacked site, and SPY_WOWCRAFT.BL, which gathered sensitive account information from the affected systems. TSPY_WOWCRAFT.BL is from a family of spyware that specifically stole information related to the popular online game World of Warcraft. Although the attack against the Dolphin Stadium Web site received the most attention, it was the several other Web pages, mostly from gaming sites, which reflect the real intention of the author(s) that planted the codes.

Fortunately, damage to victims of JS_DLOADER.KQZ from the Dolphin Stadium Web site was limited as security companies working in tandem with law enforcement alerted the site administrators, who were able to remove the malware after a couple of hours.

2.3.3 Content-Based Threats

There are threats that use content for malicious purposes. These are called content-based threats and can include spam and phishing.

SPAM

Unsolicited email messages that contain links which download malware continued to rise during the first months of 2007. Botnets have been implicated for a significant volume of spammed email messages sent out during the previous months. The payloads of worm families NUWAR and STRATION provide evidence of an orchestrated effort to pool computing power for a very specific end: which is to send out unsolicited mail to the most number of users. Data from TrendLabs shows that spammed email messages are still largely written in English. However, Asian languages such as Japanese and Chinese now claim the top spot in terms of the most popular non-English spam languages and Korean has emerged in the top 10. Spanish and Russian language spam have fallen on the list and now follow Asian language spam. Commercial subject matter remains the popular spam content.

TREND: A SPIKE IN GERMAN SPAM

The volume of German spam increased three-fold in the second quarter of 2007 compared to the first quarter. This surge is due to the thousands of German users who exposed their systems to downloaders (TROJ_AGENT.IQN) in March by clicking on links or opening .PDF attachments in messages purporting to be invoices or billing statements.

TREND: TIMELY SUBJECT HEADINGS TRUMP GENERIC MESSAGES

Subject headings of spam this period were extremely timely and relevant. WORM_NUWAR variants were quite adept at exploiting real world events, and human interest in doomsday pronouncements of war.

TREND: ATTACHMENT ENHANCEMENTS

Malware authors have also been trying to confuse signature-based antivirus engines by using different archiving applications like .RAR and .ZIP (WORM_NUWAR.RAR and WORM_NUWAR.ZIP, respectively), which require passwords before they are launched.

TREND: DECREASE IN IMAGE SPAM VOLUME SHARE

In December 2006, image spam constituted 32% of the total spam volume collected. By the first quarter of 2007, the percentage fell to 12.83% in time with the general decline in holiday zeal. And from the available data for the second quarter, the number had fallen further to 11%. The decline is attributable to the positive effects of the increased awareness and efforts (albeit in reaction to image spam already circulating in the latter part of 2006) of security companies in developing smarter OCR technologies.

PHISHING

Phishing remained prevalent from December to May, with phishers using the same techniques, the most widely-used being the explicit display of the phishing URL, which still manages to lure users into divulging account information. The percentage of reported phishing links which are already found dead at subsequent visits suggest there is a relative ease by which phishers are able to register and evacuate from online domains.

2.3.4 Process-Based Threats

The latest infection counts show that the growth in the number of infections from heuristically-detected malware have nearly doubled from December 2006 through May 2007. This means that compared to six months ago, users were twice as prone to have been infected with malware.

Trend: File Infectors with New Roles

2007 saw an increase in file infector families which employ complex infection routines and serve as propagation vectors for other threats. PE_LOOKED variants downloaded several malware onto the affected system. PE_FUJACKS is known for its three-pronged propagation routine (including propagation via instant messaging) and involvement in the download of a keylogger. PE_DARKSNOW possesses an intricate infection scheme as it infects system files and steals system information. Finally, PE_VIRUT arrived as a spammed email attachment, and had backdoor capabilities.

Trend: Online Gaming Information Theft

Trojan spyware are still targeting the same type of user information. Online gaming information accounts for 37%, due mostly to the massive popularity of online gaming in Asia. Spyware stealing bank- or account-related information accounts for 17% while 5% exclusively sought out instant messaging account information, primarily from the Asian IM application QQ Messenger.



Trend: Rise in Rogue Anti-Spyware Infections

Capitalizing on people's inherent paranoia about getting infected are several rogue anti-spyware vendors that first convince users that they have been infected then sell them a product they really do not need. The software purchased online is virtually useless, and the fraudulent company may consequently steal a customer's credit card accounts. Examples of the phony software packages include Winfixer, SpywareQuake, ErrorSafte, ErrorGuard, SpyShield, SpyAxe, SpywareNuker, and most recently, Spyhealer, DriverCleaner, and SystemDoctor.

2.3.5 Distributed Threats

Although intelligence gathering processes are underway, the depth and extent of botnet infiltration—how many exist and which computers have been compromised—are still hard to pinpoint. Malware infection may provide clues, inconclusively though, that a said computer may have been involved in a botnet. What is dangerous is that the user is often never made aware that such a compromise exists.

The reason for the proliferation of these attacks is that there are many talented programmers in the world who are faced with slow job markets or are lured by lucrative paychecks. Many of these programmers reside in Latin America, Eastern Europe, and Asia, all of which have a history of organized crime.

Malware activities give clues to the existence and persistence of botnets. Late last year, a malicious Hypertext Preprocessor (PHP) script was detected as being hosted on Web servers, where unsuspecting users may accidentally run it. Upon execution, it opens random ports on the affected system, and may then submit to the commands of a remote user.

In March 2007, Rinbot launched an attack against U.S. media outlets by exploiting newly-published vulnerabilities, causing it to spread across connected systems running on Windows. Also, as the past few months have demonstrated, there is a distinct effort by botnet masters, particularly those that send out spam (NUWAR and STRAT) to increase their batting average in infection rates by closely monitoring real-world events and crafting timely email messages to increase the likelihood that each spammed message ends up in a hit. As discussed in content-based threats, the changing subject readings are proving to be effective. Unbeknownst to users, launching a worm into the system allows a remote malicious user a foot in the door, as it surreptitiously installs other files, steals information and takes advantage of its computer resources to participate in spamming activities or even Distributed Denial of Service (DDoS) attacks.

And just very recently, WORM_SOBER.AX was found to corrupt a legitimate system file, causing network connection for the affected computer to slow down. It also performs a variety of routines, including process termination, lowering security settings, and disabling Windows auto-update. What puts suspicion that this is involved in a bigger scheme is its mass-mailing routine and the steps it takes to avoid encountering the authorities by filtering email addresses like .gov and .edu. Its vast capabilities put users in critical danger.

2.4 > Forecast on Future Threat Landscape

Attacks similar to those seen during the past six months are expected to continue in the ensuing months, taking advantage of back-to-school and the holidays as online commerce peaks in December. Malware authors will try to evade signature-based detections, saturating other means

apart from compression tools to avoid exposure by security vendors. Trend Micro expects to see the number of Web threats expand due to a variety of reasons. First, the availability of exploit kits and accessibility of bots and botnets makes it extremely easy to implement Web threats. Second, as increasing numbers of Web 2.0 websites emerge, creating interactive Web applications, malware authors will be on the look-out for technical flaws which they may then use to execute their own codes.

Phishing attempts will likely increase as a result of the introduction of phishing kits into the underground markets and the ease of obtaining an online presence (due to cheaper domain registration rates). Attempts need only look more convincing to lure more victims, in the same way image spam may pick up in terms of sophistication, as retaliation against security companies' efforts to weed them out of email traffic.

Botnets remain a threat, and will require a deep, integrated view before authorities begin an attempt at taking them down. Meanwhile, malicious codes will continue to use each and every avenue available to malware authors online, to net the most number of victims. Web threats will continue to permeate the online computing experience for users all over the world, as long as the deployment of malicious code remains a profitable enterprise for malware authors.



2.5 > Chapter 2 Summary and Review Questions

Summary

Threats to computer resources, data and personal security are at an all-time high in the global world of computing, especially where the use of networks and the Web are involved. Money is a primary factor in the use of Malware, Spam, Phishing, Pharming, and other infiltrations. Attacks that are regional or targeted to a more specific population overshadow the threats caused by global, mass-distributed viruses.

Trends include an increase in German-based threats, threats with more timely headings rather than more generic headings, attachments are better disguised, and a slight decrease in image Spam. Malware downloads are on the rise, as are viruses related to online gaming. There is also an increase in rogue anti-spyware software vendors. They convince users that their computers are infected, only to sell them spyware software that doesn't work, and in the meantime take their credit card information.

Review Questions

1. What aspect of the threat landscape is most related to infrastructure vulnerabilities?
 - a.) Rogue anti-spyware
 - b.) Security holes in software
 - c.) Online gaming
 - d.) Phishing
2. What do malware authors use when they deploy codes that specifically target victims and lure them to malicious websites? (Choose all that apply)
 - a.) Viruses.
 - b.) Rogue anti-spyware
 - c.) Social engineering
 - d.) Phishing
3. Which are forms of content-based threats?
 - a.) Spam
 - b.) File infector families
 - c.) Phishing
 - d.) Worms



4. Which threats are on the increase? (Choose all that apply)
 - a.) Image Spam
 - b.) Timely subject headings
 - c.) Enhanced attachments
 - d.) Rogue anti-spyware

5. What are one of the difficulties in defining the extent of botnet threats in the threat landscape?
 - a.) Botnet applications are untraceable
 - b.) Botnets are inherently difficult to identify
 - c.) Talented IT professionals in countries with organized crime develop botnets
 - d.) Many users are unaware that their system has been compromised



Chapter 3: Malware

Chapter Objectives

After completing this chapter, you will be able to:

- Define and understand malware threats
- Identify the different types of malware and their characteristics
- Describe malware phases such as arrival, installation, and malicious activities
- Recognize payloads or symptoms of malware infection



3.1 > Introduction to Malware

3.1.1 What Is Malware?

The term malware refers to any malicious software or computer program that performs malicious activities. Malwares are primarily unwanted and potentially dangerous set of programs. They can cause harm to your computers or even stop you from using it. Malwares are complex and are a constantly evolving area in computer technology. Of all the problems that are encountered in IT, few are as prevalent and costly as malware attacks and the associated costs of dealing with them. Understanding how they work and how they evolve over time can help you deal with the issue proactively. This in turn can provide you with a more efficient and effective reactive process when they do affect you or your organization.

3.1.2 Software Bugs vs. Malicious Activities

Typically, when users encounter errors in a program, the first assumption is a “bug” in the software. On occasion, “bugs” do occur which affect program performance. These “bugs” are not intentional. However, malware can have similar affects; and these effects are always intentional. Malware always intends to do harm and this is what we call malicious activity. The following are considered examples of malicious activities:

Propagating	Spread copies of themselves
Destructive	Destroy files and computers
Unexpected/Unauthorized	Do something without the user's consent
Backdoor	Compromise the system to unknown remote accesses
Information Theft	Steal information
Exploiting	Take advantage of system vulnerabilities to break system security
Deceiving	Trick users
Hidden	Hide behaviors from the user

3.2 > Types of Malware

There are three (3) general types of malware and these are: Virus, Worm, and the Trojan horse (or simply Trojans). The following sections will discuss each of these malware types.

3.2.1 Virus

A virus is a type of malware that infects files to spread or propagate. When we say “infects files”, it is the capability of the virus to insert a copy of itself or any malicious code on another executable code (called host). Some viruses search for executable files to infect in its desired directories and sub-directories. These are often called “direct infectors” or “direct infecting viruses”. Some viruses need to get loaded to memory first and then they will infect files once they got triggered by certain events such as executing a file, opening, or even closing a file. Most



likely, the executable file that triggered the event would be the one that will get infected. These viruses are called “memory resident viruses”.

What Do Viruses Infect?

By definition, viruses infect files since most of the executable codes are stored in terms of files on the disk and in memory. However, generally speaking, viruses are executable codes/programs that are being inserted into another executable code/program. Executable codes are often compiled into a file but they can also be compiled to be placed in memory chips, or even in the given sectors of the disk even though they may not be listed as files. Meaning to say, as long as an executable code can be contained and there is still enough space, a virus can possibly insert or injects its code there. The following are examples of common virus types:

- Boot Virus** Viruses that infect a boot sector of a disk (or a master boot record, if it speaks of hard disk). A boot sector contains a code that is being executed at system startup to load the operating system. Once a boot sector is infected, the virus will execute in every system boot-up.
- Binary File Infectors** Viruses that infect binary executable files (i.e. EXE and DLL files). Once an executable file is infected, the virus executes every time the said executable file is executed.
- Multipartite Viruses** Viruses that are capable of infecting both boot sectors and binary executable files.
- Macro Viruses** Viruses (which are in a form of a VBA code) that infect Microsoft Office files. MSOffice uses macro codes to automate the way an application behaves to a particular file (such as like what MSWord would do after opening a document or perhaps MExcel to a spreadsheet). These viruses are able to place a malicious macro inside a document (or a sheet) that every time these files are being opened (or even closed) the viruses will execute.
- Script Viruses** Viruses (which are also in the form of script) that infect scripts. A script is an executable code that is being interpreted instead of being compiled. It is just in a form of a text file by which it needs an interpreter to get executed (such as Visual Basic Script (VBS), Java script (JS), Batch files, PERL, IRC, etc.). Scripts viruses are direct file infectors. They just search the whole disk for their kind to infect.

Types of File Infection

Viruses infect files in different ways. Some of them insert their codes at the beginning, some at the end, and some at the middle. The following subsections describe the various ways in which viruses infect files.

Prepending Infection Insertion of the virus code at the beginning of the host file.

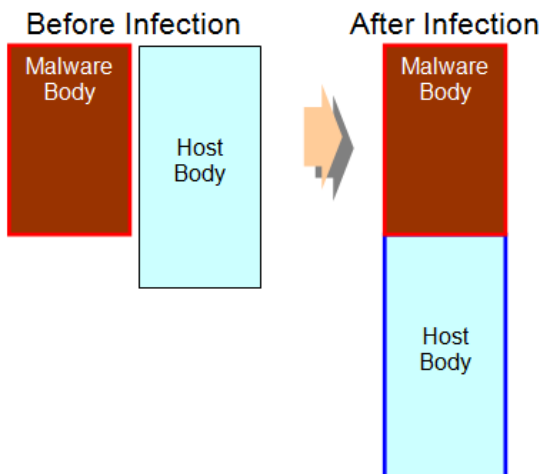


Figure 3-1: Prepending Infection.

Cavity Infection The virus code will search for unused spaces in the host body by which if the total space is enough for the virus code then it will insert its code there on the unused spaces.

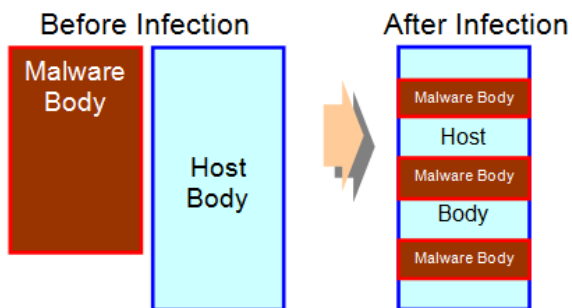


Figure 3-2: Cavity Infection.



Appending Infection Insertion of the virus code at the end of the host file.

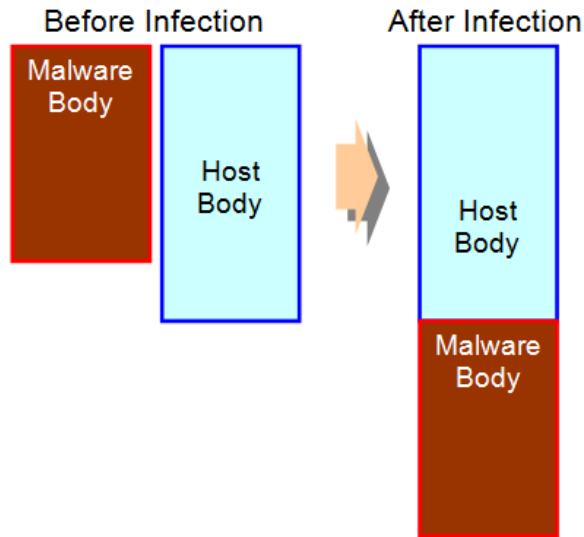


Figure 3-3: Appending Infection.

Overwriting Infection The virus literally overwrites the host file.

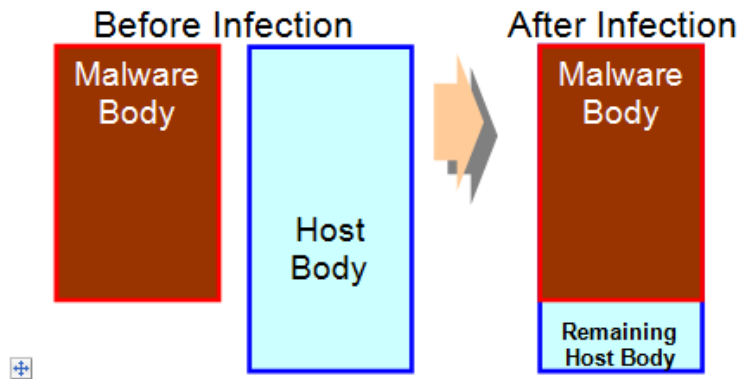


Figure 3-4: Overwriting Infection.

Sandwich Infection (or Amoeba) The virus engulfs the host body with its code upon infection. It is also called “Amoeba” type of infection because the virus behaves like amoeba that also engulfs its food with its body upon capturing it.

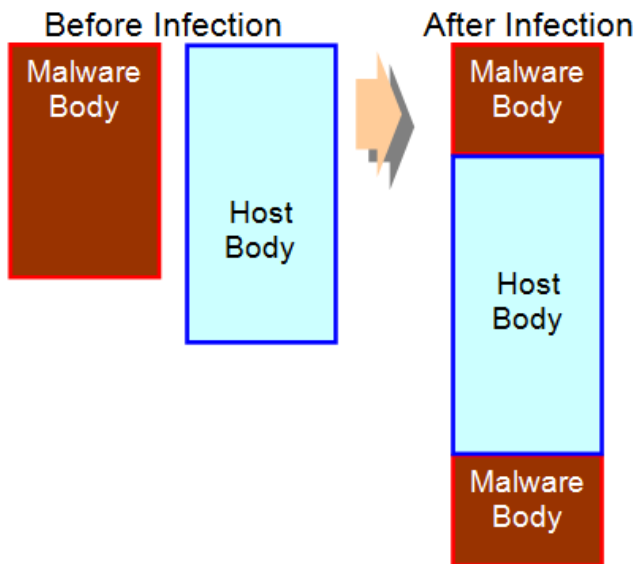


Figure 3-5: Sandwich Infection.

Complex Infection A combination of several types of infection technique as discussed above plus some manipulations on the host file like compression and encryption. Complex types of infection is done in order for the host file not to be easily recognize and not easily be restored back to normal by antivirus applications. Viruses of this type are capable of hiding the host inside their body in compressed and/or encrypted form.

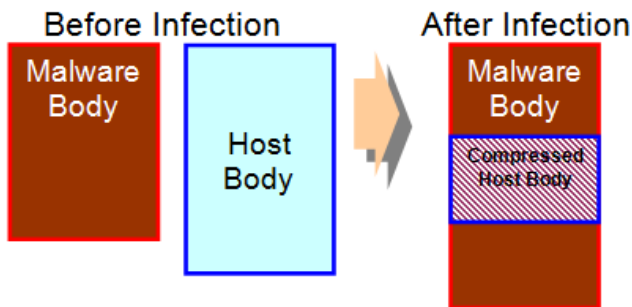


Figure 3-6: Complex Infection.



Operating Algorithm of Viruses

The following are common virus routines.

Direct File Infectors

Get a target file to infect

- Search directories and sub-directories to look for target files to infect

Verify target file if suited for infection

- Validate target file
- Check target file if already infected or not

Infect target file

Generate a payload (if any)

Pass control to host (or execute the host)

Memory Resident Viruses

Install Itself

- Check if a copy of itself is already residing in the memory (or memory residency check)
- Allocate memory for itself
- Load itself to allocated memory and become resident
- Hook DOS functions or Windows APIs and point it to self

Get a target file to infect

- An executable file that will use any of the hooked functions/API would be become the target of infection

Verify target file if suited for infection

- Validate target file
- Check target file if already infected or not

Infect target file

Generate a payload (if any)

Pass control to host (or execute the host)

What is a Virus (or Malware) Payload?

Malware behavior can be placed into one of three classifications:

Installation	How the malware is able setup itself on the system to be able to run properly
Propagation	An act of malware to replicate for the purpose of spreading across different computers
Payload	Any malicious activity being done by the malware aside from installation and propagation

Viruses were the first malware to implement payloads as part of their malicious routines. However, not all malwares have payloads. Payloads are also known as symptoms of infection because most of them are obvious to users. Below are examples of malware payloads:

- Display Graphics
- Display Messages
- Generate Sounds
- Execute other application without the user intervention
- Automatic Reboot
- System shutdown
- System slowdown
- Any changes in the desktop and taskbar settings
- Abnormal execution of other application

3.2.2 Worm

Worms are another form of threat to computers and data that resides inside or is produced by them. The behavior of a worm is represented by its name: it quietly finds its way in to your machines to do their work.


What is a Worm?

A worm is another type of malware that creates a copy of itself and then sends it over the network to infect other systems. The advent of the internet has made it easy for computer users to share information one with another. People use their email or even instant messaging applications to send files to their colleagues. They can also share their files over the network by providing other people access to their system.

However, the technological advances used to facilitate easy file sharing between computer users also benefits worms. Worms utilize these same technologies to propagate. Worms can send their own copies using email, instant messaging applications, and Internet Relay Chat (IRC) without user intervention. Some worms also are capable of dropping their copies on every shared resource on the network. Worms propagate faster compared to viruses. Viruses can only make their way to other systems if the unaware user copies the infected files and executes them on other machines. Most worms don't need unaware users; they simply propagate without user intervention.

Methods of How Worms Propagate

Worms are well known for spreading through email. However, worms are capable of propagating in many other ways, such as through network shares and other file sharing methods.

NOTE  Mass mailing worms look in several places for email addresses on the infected computer, including email addresses from the user's inbox, Windows address book (WAB) file, and Files that might contain email addresses (such as HTML files).

PROPAGATION VIA EMAIL

Worms that can propagate via email are called “mass mailing worms”. Mass mailing worms can use SMTP commands, MAPI functions, or Outlook objects to send email. They also have predefined messages incorporated in their body. These messages have enough words to make target recipients believe that the email is legitimate. Once the user activates the mass mailing worm (by either opening an attachment or clicking on a URL in the message), the worm will be downloaded to the user’s computer.

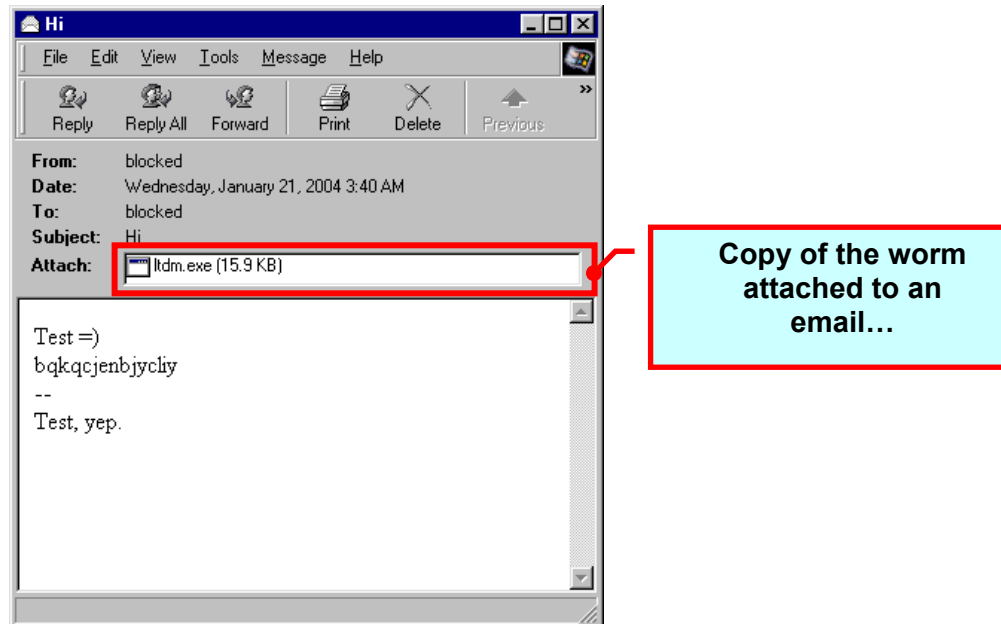


Figure 3-7: Copy of a worm attached to an email.

NOTE 📖 The most popular client IRC application is the mIRC which was created by Khaled Mardam Bey in 1995.

PROPAGATION VIA IRC

Internet Relay Chat (IRC) was created by Jarkko Oikarinen in 1988 with the purpose of allowing a group of people to send messages (or chat) among them simultaneously over a given communication channel. IRC is comprised of both a server and a client application. The server is used to host the communication channels while the client refers to the application being used to communicate with other people via IRC protocol. IRC client applications use scripts (called “IRC scripts”) to automate user responses. Due to these scripts, sending responses can be done automatically just like what an answering machine does whenever it receives a telephone call. These scripts are used by malware to perform malicious activities over an IRC channel.

File sharing is also available through IRC. IRC users can send files to their chat mates using an IRC command: DCC SEND. Since scripts are utilized in IRC communication, worms can use a

script to automatically use the DCC SEND command to send their copy to all users in a given IRC channel. IRC scripts are read from either of these files:

- mIRC.ini
- script.ini

Below is an example of IRC script that enables a sending of the worm to IRC users.

```
n0=on 1:join:#: { if ( $nick == $me ) halt
n1=else /dcc send $nick C:\MIRC\WORM.EXE }
n2=on 1:TEXT:leave!!!:#{ /msg $chan Your will is my
      command
n3= /part $chan }
```

Figure 3-8: IRC Script example.

The given IRC script above means:

- Once a certain user joins the channel, the worm will verify the nick of the user. The nick refers to the user's IRC account name.
- If the nick doesn't belong to the worm then a copy of the worm, WORM.EXE, would be sent to that nick.
- The worm also recognizes the message, "leave!!!"
- Once the said message is sent on the channel, the worm will leave the channel.

PROPAGATION VIA INSTANT MESSAGING (IM) APPLICATIONS

Instant messaging applications (or simply IM) are modern applications that implement another type of communication on the internet. Though they are designed to do internet chat similar to what IRC does, their initial aim is different. While IRC aims to provide a channel of communication (called a chat room) in order for two or more people to chat, instant messengers aim to establish one-on-one chat, whereby only two people communicate directly. Today, instant messaging applications have added capabilities to hold group chats or conference just like IRC. The remaining difference of IM applications from IRC is that they don't use scripts. There are many instant messaging applications but there are only a handful which are popular. The following are common instant messaging applications:

- Yahoo Messenger (powered by Yahoo.com)
- AIM (powered by AOL)
- MSN Messenger (now called Windows Live Messenger which is powered by Microsoft)
- ICQ (powered by AOL Time Warner)
- QQ (powered by Tencent – the most popular IM in China)

Instant messaging applications also allow file sharing. They give users an option to send files to their friends while chatting with them. This sharing mechanism is also being utilized by worms to propagate. There are two ways how worms spread through this medium.

1. Internally manipulate window messages making the IM application automatically send a copy of the worm without user intervention.
2. Pop a link to an online user and lure him/her to click the link. Upon clicking the link, the worm will get downloaded on the user's computer.

Below is an example of a worm propagating via MSN Messenger.

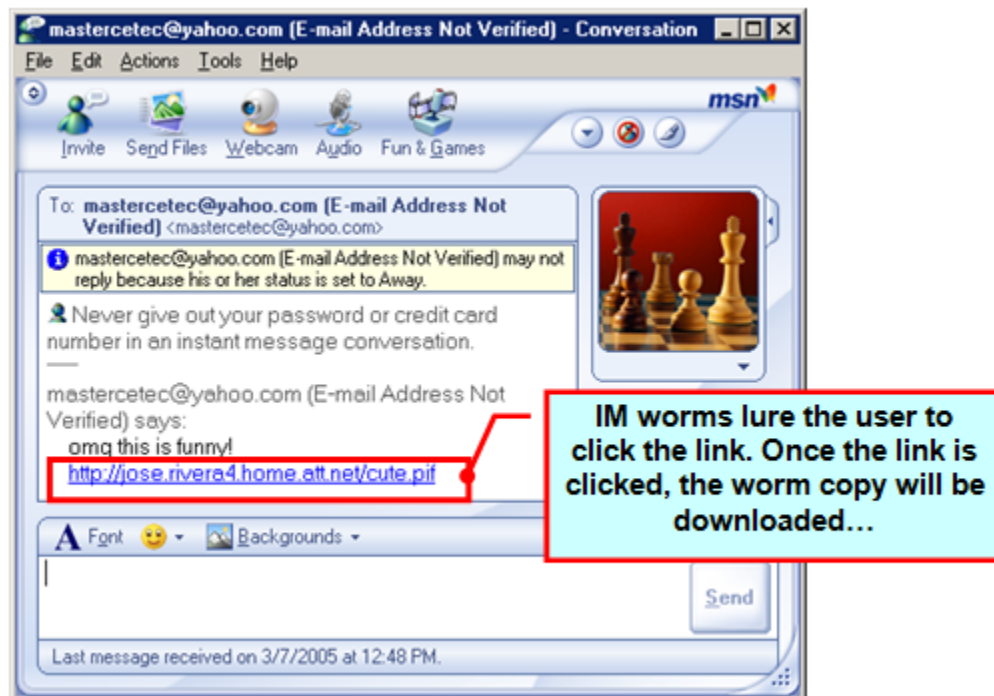


Figure 3-9: Worm propagation example.

PROPAGATION VIA PEER-TO-PEER FILE SHARING APPLICATIONS

There are two types of network implementation:

1. Client-Server
2. Peer-to-Peer (P2P)

In a Client-Server environment, there are machines that only act as Servers and the rest are Clients. However in Peer-to-Peer environment, all machines act as both Server and a Client.

NOTE In a Client-Server network, the client software sends data requests to the server. The server accepts the requests, process them, and returns the requested information to the client.

The internet primarily implements Client-Server network environment whereby the web sites act as Web Servers and internet users are the Clients. But on the other hand, Peer-to-Peer networks are also being implemented over the internet. Peer-to-peer (or simply P2P) connection via the internet doesn't use web browsers. Instead, they use so-called common Peer-to-Peer applications to share files with other peers worldwide. Below is the list of known P2P applications:

- Kazaa
- iMesh
- Grokster
- Napster
- eDonkey
- eMule
- BitTorrent
- LimeWire
- BearShare
- Morpheus

The purpose of P2P applications is to allow internet users to easily and directly share files to many people simultaneously. With this, users don't need to upload files via HTTP or FTP servers. They simply specify the shared folder and all users of a common P2P application have access to the files and folders.

As with other legitimate communication and sharing mechanisms mentioned previously, P2P applications can also be used to distribute worms. Worms that propagate via P2P applications drop their copies on the shared folders. They use interesting filenames so that they can lure other P2P users to download them.

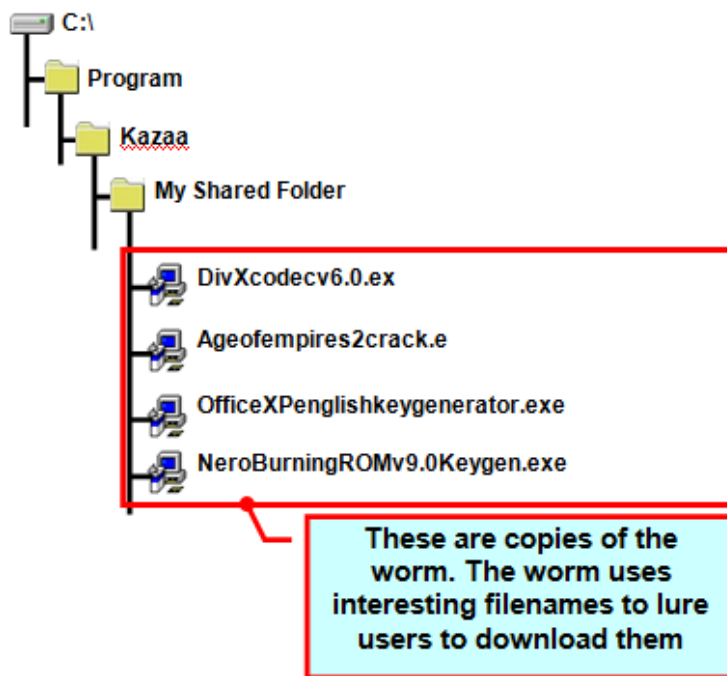


Figure 3-10: Worm file name examples.

NOTE In a Client Server network, the client software sends data requests to the server. The server accepts the requests, processes them, and returns the requested information to the client.

PROPAGATION VIA NETWORK SHARES

On a local network, it is very normal to share files with other users. Some users create a shared folder to share files while others create a mapped drive on their system to easily access the shared files. Some network resources are available but are hidden by default, whereby only network administrators are capable of accessing them. As demonstrated previously, wherever files are shared, worms will thrive.

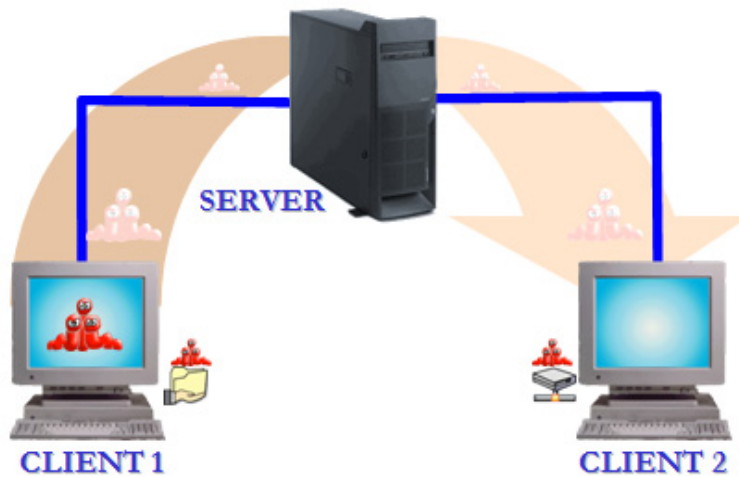


Figure 3-11: Worms thrive in a network where files are shared.

PROPAGATION VIA VULNERABILITY EXPLOITS

In the world of Information Technology, there is no such thing as perfect computer software or program. This would mean that all software has imperfections. Imperfections in a computer program might be in the form of feature insufficiency, anti-user friendliness, program bug/error, or vulnerability.

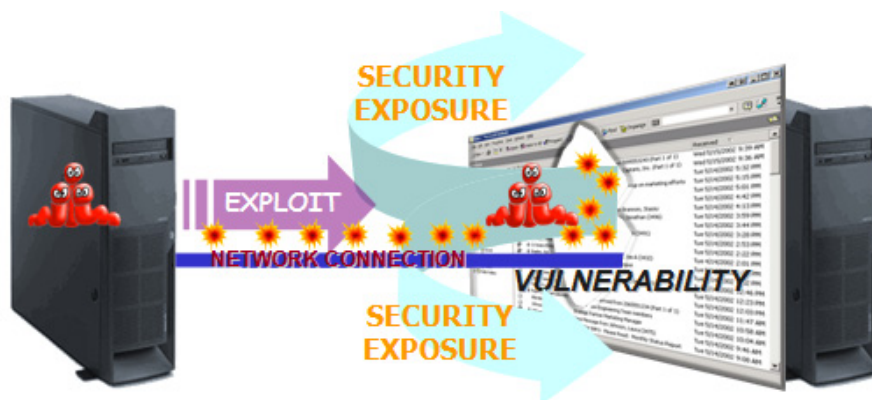



Figure 3-12: Worms exploit computer vulnerabilities.

NOTE 📖 A zero-day exploit is an exploit that comes out on the same day that its target vulnerability becomes publicly known.

Vulnerabilities may result from bugs or design flaws in the program. Once a vulnerability is discovered in a particular piece of software, it that vulnerability can be manipulated or exploited for malicious purposes.

NOTE  The idea of buffer overflow is very simple: placing two or more KB of data in a memory location that is designed to hold only one KB of data.

Exploit is a term used to describe a technique of taking advantage of software vulnerabilities to execute malicious codes. Malicious codes can be embedded or injected depending on how the target vulnerability works. Vulnerabilities inside a program are difficult to find. However, there are several people (like malware writers and hackers) who spend time discovering new vulnerabilities. Once the vulnerability is discovered, the malicious code will be able to find out how to exploit it.

An exploit can be done differently depending on the vulnerability. There are so-called browser exploits which take advantage of vulnerabilities found in the process of how browsers interpret scripts in web pages. There are also application exploits which take advantage of the vulnerabilities found in file formats of known user files such as JPEG, GIF, WMF, and MSOffice OLE files (i.e. DOC, XLS, PPT, etc.) However, the most popular type of exploit is the buffer overflow exploit. This exploit is mostly done on binary executable files whereby it takes advantage of vulnerabilities caused by unchecked buffers in the executable program. This exploit is being used by worms to propagate.

Buffer overflow may cause overwriting of significant codes in the running program which, once overwritten, program flow might be altered to the point that injected malicious code would be executed instead.

Below is a summarized procedure on how worms able to propagate via vulnerability exploit:

- The worm initiates the search for vulnerable machines across the network. This is done through the process of IP scanning.
- Once a vulnerable machine is found, the worm will send crafted packets that contain an exploit code (or payload).
- Due to the vulnerability, the exploit code is executed on the exploited machine.
- The exploit code:
 - Opens a command shell.
 - Initiates FTP (or TFTP) sessions between the infected machine (this is where the worm resides) and the exploited machines. FTP commands are being executed in the open command shell.
 - These execution FTP commands will cause the malware copy to be downloaded on the exploited machine.
 - After being downloaded, the malware copy will eventually be executed on the exploited machine.

3.2.3 Trojan Horse

As story goes, the famous vehicle referred to as the Trojan horse, was wheeled into the city of Troy to disguise its contents of warriors. Once inside the city walls, the warriors opened the doors and wreaked destruction over the city. So malware that disguises its way into a computer got its name.

What is a Trojan Horse (or simply Trojans)?

Unlike viruses and worms, Trojans are malware that do not have the capability to spread or propagate. They cannot propagate by themselves because they do not have the mechanism to send their own copy to another computer. So the question is, how these Trojans able to get onto a user's machine? Trojans are able to reach machines to infect by riding on some third party applications that are coming from the internet in the form of freeware and shareware. These third-party applications are being trusted by users who are unaware that they are already infected. Some freeware (or shareware) creators and providers intentionally bundle malware (these malware could be mostly Trojans, but there could also be worms and viruses) in their applications for malicious purposes. Some hackers and malware writers are also able to use some browser exploits on certain web pages which, once accessed by users, Trojans will automatically be downloaded on their machines. Below is a simple illustration on how Trojans reaches their victims.



Figure 3-13: Trojan horses are malware that are hidden in other applications.

Kinds of Trojans

There are many different kinds of Trojans, and their actions are as diversified as their sources of origination. To better classify Trojans, we will evaluate them based upon their intentions and payloads.

DESTRUCTIVE TROJANS

Destructive Trojans have payloads that can be triggered by time or event depending on how they are designed to execute their payloads.

Intention:	To destroy
Payload:	Format disk drives Overwrite MBR or boot sectors Delete files Delete important registry entries Corrupt files Corrupt data/information Corrupt CMOS Disable hardware settings Hang Windows Make OS unusable Make OS unbootable

TROJAN DROPPERS

Trojan Droppers act as carriers for other malware. They can be in the form of an installation or setup files. They can also be in the form of SFX files which are being created by file compression utilities such as WinZip or WinRAR. Most likely, they are by-products of those applications that are used to join two or more executable files. These applications are called PE joiners, binders or bundlers which are sometimes part of a tool called “Trojan construction kit” or “Trojan generators”.

Intention:	To drop and execute other malware
Payload:	Drop one or more malicious files in the system Execute the files they dropped

TROJAN DOWNLOADERS

Trojan Downloaders act as agents for other malware. Most of the time, Trojan downloaders only work if there is an internet connection available. They often use WININET APIs to download malicious files. The downloaded files are usually other Trojans but sometimes it can include worms and viruses.

Intention:	To download malware and execute
Payload:	Connect to a malicious website Download malware from malicious website Execute the downloaded files

TROJAN CLICKERS

Trojan Clickers help users to access malicious websites or any sites users do not intend to access. Clickers might also cause the downloading of other malware. If Trojan downloaders directly download malwares, Trojan clickers do it indirectly by which it needs to redirect the user to the malicious website. Upon accessing it, malware is downloaded to the computer.

Intention:	To cause users to access malicious websites
Payload:	Continuously attempting to connect to the internet Modify Windows HOSTS file to redirect users to the infected website Modify browser settings (such as default Home Page, Search Page, etc.) Hijack any attempt of the user to access websites by auto-completing the typed URL in the address bar

FLOODERS, NUKERS, AND DoS/DDoS ATTACKS

Denial-of-Service (or DoS) attack is a general term used to describe what malware is doing to deny users of their computing privileges. There are several forms of DoS.

- If an infected machine is being denied access to the network, this type of DoS is called a Land Attack. This is done by simply redirecting all the packets, which the infected machine has been sending, to itself.
- If everybody is being denied to access network resources by flooding the network with garbage packets, then the Trojans behind it are called flooders.
- Nuking is a term used for sending too many garbage packets directing them to a single target machine. If the target machine can't respond anymore due to lots of data packets it receives then the effect could be every user that has to access the said machine would be denied.
- If simultaneous nuking attacks are being done on a single target machine then these attacks are collectively called distributed denial-of-service attack or simply DDoS.

The following diagram is an illustration of how denial-of-service or nuking works.

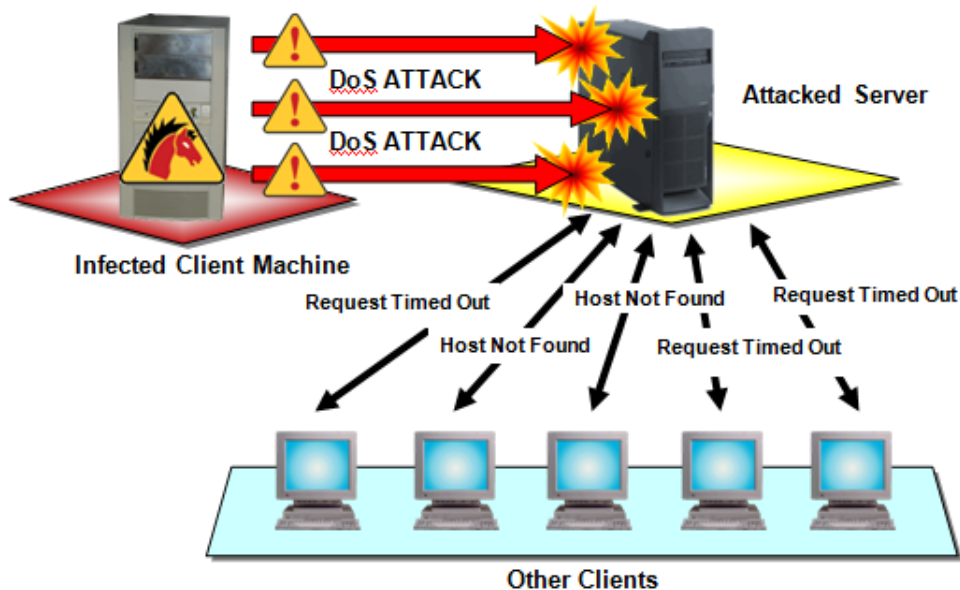


Figure 3-14: DDoS attack example.

Almost all types of network packets could be used for DoS attack.

- Ping Flood (or Ping Of Death) – In this type of DoS attack, ICMP (or ping) packets are used to attack a target computer.
- SYN Flood – In this type of DoS attack, the TCP SYN packets are used to attack the target machine. In standard TCP communication, for every SYN message that is sent, the target machine must respond with an ACK message. If there is a large amount of SYN messages simultaneously, the target machine will not be able to respond with ACK message anymore. Thus, communication would be denied.

Intention:	To make computer resources unavailable
Payload:	Network traffic slow down Modify Windows HOSTS file to deny connection to some websites 100% CPU utilization Make it difficult to access the network or the internet

TROJAN BACKDOORS (OR SIMPLY BACKDOORS)

Backdoor malware has two components: a server and a client part. The client component is in the possession of the hacker and it is being used as the remote control program. The server component, on the other hand, is the one that is being spread across the internet which can be controlled by the hacker using the client component.

Intention:	To allow a (malicious) remote user to connect to the affected machine and to have access/control over it.
Payload:	Open/close CD tray Pop-up messages Execute available applications on the system Shut down Windows Browse file system Capture clipboard data and screenshots

TROJAN SPIES

The main focus of Trojan Spies is information theft. These malware are capable of monitoring and logging information that is related to users' computing and web browsing habits. These logs will be sent to an unknown user via email, IRC or instant messaging applications, or even FTP uploads at a later time. These malware may also be capable of hijacking web browsing activities of users. They may intercept accesses to online banking websites and internet shopping websites to steal information about users' banking and payment transactions.

Intention:	To monitor and log user computing activities which will be sent to an unknown host. It also intends to trick users to divulge their personal information.
Payload:	Steal information from the system such as the following: <ul style="list-style-type: none">• User accounts and passwords• User keystrokes (key logging)• System informationInternet browsing-related information• Serial keys of installed applications• Email messages• Clipboard data and screenshots

TROJAN PROXIES

Trojan Proxies have only two purposes. First is to sniff internet traffic whereby it can monitor internet activities in and out of the network. Second is to be used by hackers as a cover for the hacker's true location (so that if the hacker's activities are uncovered and traced, it will only lead back to the infected computer).

Intention:	To install themselves as web proxy on the affected machine
Payload:	Accept all internet traffic



RANSOMWARE

The aim of Ransomware is money. Hackers using Ransomware seize users' important files, encrypt them and request a ransom for their restoration and/or decryption.

Intention:	To encrypt user data files so that it cannot be used/opened by the user. Afterwards, the hacker will extort some money from the user in payment for the restoration of the data files
Payload:	Encrypt user data files

3.2.4 Understanding Malware Behavior

Malware uses technology that depends on two things: the infection channel and the installation technique.

Malware Infection Channel

Malware may arrive through different mediums. But definitely, where there is copying, moving, sharing, sending, downloading, uploading, and transferring of files, there you will also find malware. An Infection Channel is any medium that malware is using to gain access to a computer in order to infect. The following are known malware infection channel:

Removable Media	Floppy diskettes were the original medium used by malware to spread from one system to another. CDs and DVDs might also intentionally contain malwares (most likely those which contain pirated applications and other multimedia files). Also, USB removable storage devices are widely used and they are prevailingly replacing floppy diskettes due to their large capacity. Some malwares are used to ride on these devices so that they can be copied and infect other systems.
Email	Malware (including worms, viruses and Trojans) are commonly transmitted via email.
Network Shares	Peer-to-Peer and Client/Server network infrastructures have made it extremely easy for users to share files with each other. However, it also facilitates the spread of malware. Malware can simply drop their copies on shared resources so that unknowing users might get them.
Internet Chat	Communication using the internet is now very popular in the form of chat. Users can chat with remote users using IRC and instant messaging applications. These applications also have feature where users can also share or send their own files. Due to this, malware might also arrive through file sharing feature of the said applications.
Web	In today's world, the web is used for everything including communication, research and entertainment. Due to this, malware is being injected into web pages, ready to get downloaded onto new systems to infect. Malwares can be downloaded using HTTP, HTTPS and FTP services.
Peer-to-Peer Applications	Bulk file sharing is being done using peer-to-peer implementation over the internet. There are many peer-to-peer (or P2P) applications which facilitate file sharing. This ease of file sharing also contributes to the simple distribution of infected files.
Vulnerabilities & Exploits	Applications which receive and transmit data over the network or internet are prone to exploit attacks. Malware may arrive through a security hole caused by an exploited vulnerability.

Malware Installation Techniques

Once malware has arrived on a system, the next thing to do is to install itself. There are three basic procedures that the malware has to do to install:

- Memory residency
- Dropped copies
- Autostart mechanisms

MEMORY RESIDENCY TECHNIQUES

Memory residency is the first step in malware execution. It is the process of installing itself in the memory and remaining there (taking residence) without the user noticing it.

The following are ways to achieve memory residency:

Normal background process	Most malware has no user interface at all (though some have made their window hidden). When such malware is executed, they remain in the background to hide from normal user interaction.
Service process	Some malware install themselves as Windows services. Windows services are processes that have administrative rights. Windows services are managed through Service Control Manager (or SCM).
Injected DLL	DLL files contain library of functions that are being exported to an executing application and they are executed together with the application. Some malware are in the form of DLL executables and are being injected by their malicious accomplices in a legitimate process, such as EXPLORER.EXE. In this case, the malware remains resident as long as EXPLORER.EXE remains in memory.
Injected Thread	A process consists of one or more threads. A thread is a basic sequence of codes to which the operating system allocates processor time. Some malware, once executed, may inject a malicious thread in a legitimate process, such as EXPLORER.EXE. This thread will remain resident as long as EXPLORER.EXE is running.
Watchdog	Some malware create several instances of malicious processes in memory. While one of the malware processes is responsible for the malicious activities, the other malware processes will protect it from being terminated.

DROPPED COPIES

As part of installation, malware needs to drop several files on the system to complete system infection. Below are the types of files that the malware drops.

Copies of itself	Upon first execution, some malware need to erase the traces of their arrival on the system. They need to create copies of themselves, place them in not so obvious locations (like Windows directory and Windows system directory), and execute it. The original copy of the malware will then be deleted. Malware copies are also used for propagation.
Components	Malware may also drop other component files to help them execute properly. Not all malware components are malicious. Some components could also be non-malicious. For example, if the malware is written in Visual Basic (VB) then it would need this non-malicious component, MSVBVM60.DLL, file to get executed on the system. Without this file, the malware will not be able to execute. To ensure execution, some Visual Basic malware drop the VB DLL file.
Other malware	Some malware act as carriers for other malware which are not related to them, causing multiple infections on the system. Dropped malware



sometimes work as accomplices to complete one big malicious task together with the dropper.

AUTOSTART MECHANISMS

Most malware are designed not to execute once but to always execute. Anything that triggers the malware to execute at any time can be considered as its autostart mechanism. Most malware are being executed every time the system starts. This would only mean that the said malware have autostart mechanism at system startup.

The following is a list of known autostart mechanisms:

1. Autostart folder

C:\Windows\Start Menu\Programs\Startup
 C:\Windows\All Users\Start Menu\Programs\Startup
 C:\Documents and Settings\\Start Menu\Programs\Startup
 C:\Documents and Settings\All Users\Start Menu\Programs\Startup

The autostart folder directory is saved in the following registry entries:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders]
Startup="C:\Windows\Start Menu\Programs\Startup"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\User Shell Folders]
Startup="C:\Windows\Start Menu\Programs\Startup"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Explorer\User Shell Folders]
"Common Startup"="C:\Windows\Start Menu\ Programs\Startup"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders]
"Common Startup"="C:\Windows\Start Menu\ Programs\Startup"
```

By setting it to anything other than C:\Windows\Start Menu\Programs\Startup will lead to execution of ALL and EVERY executable inside set directory.

2. Win.ini (Win9x)

```
[windows]
load=malware.exe
run=malware.exe
```

In Windows NT/XP:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\
CurrentVersion\Windows]
"run"=""
"load"=""
```

3. System.ini (Win9x)

```
[boot]
Shell=Explorer.exe malware.exe
```

In Windows XP/NT/2000:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Winlogon
Shell=Explorer.exe malware.exe
```

4. C:\Windows\Winstart.bat

This file behaves like a usual batch (.bat) file. It is used for copying and deleting specific files. It executes every time Windows starts.

5. Registry Run/RunOnce/RunServices keys

These registry keys below execute the files that are configured in them at system startup.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServices]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServicesOnce]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\RunOnce]
"Whatever"="c:\runfolder\malware.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\RunOnceEx]
"Whatever"="c:\runfolder\malware.exe"
```

6. Autoexec.bat

Stands for automatically executed batch file, the file that DOS automatically executes when a computer boots up.

7. Registry Shell Spawning

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
```




```
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]
[HKEY_CLASSES_ROOT\piffile\shell\open\command]
[HKEY_CLASSES_ROOT\vbsfile\shell\open\command]
[HKEY_CLASSES_ROOT\vbefile\shell\open\command]
[HKEY_CLASSES_ROOT\jsfile\shell\open\command]
[HKEY_CLASSES_ROOT\jsefile\shell\open\command]
[HKEY_CLASSES_ROOT\wshfile\shell\open\command]
[HKEY_CLASSES_ROOT\wsffile\shell\open\command]
[HKEY_CLASSES_ROOT\scrfile\shell\open\command]
[HKEY_CLASSES_ROOT\txtfile\shell\open\command]
```

The default value data for that key should be "%1" %*; if this is changed to malware.exe "%1 %*", the file malware.exe is executed EVERYTIME an exe/pif/com/bat/hta/txt is executed.

8. Active-X Component

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\
Installed Components\KeyName]
StubPath=C:\PathToFile\Malware.exe
```

9. UserInit reg value (NT/2000/XP)

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
CurrentVersion\Winlogon]
"Userinit"="C:\WINDOWS\system32\userinit.exe,
```

A path to a malware can be added after the comma and then be executed after the user logged on.

10. AppInit_DLLs

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Windows]
"AppInit_DLLs"="malware.dll"
```

The DLLs specified in this value are loaded into the process memory of processes that executed after the registry change has been made.

There are lots of possible autostart mechanisms that can be used inside the Windows registry. In fact, every executable file reference that can be found inside the registry could be used to autostart malware execution.

3.2.5 Rootkits

The term rootkit is used to describe the mechanisms and techniques whereby malware attempts to hide their presence from users and system utilities. It is a way of gaining root system privileges for the purpose of getting undetected by system utilities that has lesser privileges. Rootkit technology is used by malware for stealth mechanisms.

NOTE 📖 The term stealth means “making something hidden or undetected”.

Malware that undergo rootkit are being installed as drivers. Sometimes, they use a driver component (.SYS files) to achieve it. Through the use of the installed drivers, these malware are able to hook several functions that virus scanners and system utilities use to hide themselves and remain undetected.

Rootkit Types

Application-Level Rootkits – Tools that add a separate application to a system. The user must be tricked into running and installing the application.

Kernel-Level Rootkits – Give an attacker complete control of the underlying system. Can be a simple modification of the kernel or can completely replace the kernel.

Traditional Rootkits – Work by replacing system components.

User-Level Rootkits – Inject code into different processes. Typically run in system processes (i.e. winlogon.exe, services.exe) to ensure users cannot kill the process without the system becoming unstable.

3.2.6 Blended Threats

Blended Threats is the term used to describe malware that have complex malicious behaviors. These types of malware may have combined capabilities of viruses, worms and Trojans. Most of the time, they exhibit multiple payloads. They could also be hard to detect or even hard to remove.

3.3 > Understanding Malware Forms

Malware is designed to take many forms, including binary files, encrypted files, polymorphisms, packed files, macros, and scripts.

3.3.1 Binary Malware

These are malware that are in the form of binary executable files like Win32 (or portable executable – PE) EXE and DLL files. They are compiled executable programs. Malware files that were compiled under assembly language compiler are smaller in sizes while those that were compiled using high level languages like Borland Delphi and Visual Basic have larger sizes. There are also those that were compiled under Borland C/C++ and Visual C/C++ and even Microsoft .NET and Java.

of automating highly repetitive tasks. Malware writers have also utilized macro codes to create malwares inside Microsoft Office documents.

NOTE 📖 The notorious LOVELETTER worm (aka “I Love You” virus) was written in Visual Basic Script.

3.3.5 Script Malwares

Scripts are also set of executable codes that are being interpreted rather than compiled. Examples of scripts are the following:

- Visual Basic Script (VBS)
- Jscript (Microsoft)
- JavaScript (Sun)
- HTML (HyperText Markup Language)
- XML (Extensible Markup Language)
- PHP (Hypertext Preprocessor)
- PERL (Practical Extraction and Report Language)
- Python
- Ruby
- IRC (Internet Relay Chat) Script
- Batch files (DOS/Windows)
- BASH Script (Unix)

Script Encoding

The problem with scripts is that they can easily be read, modified and manipulated. Microsoft has created a means to hide the script code (can only be done in VBS and Jscript) and that is through script encoding. Script malware utilizes script encoding and other sophisticated techniques, such as script encryption to avoid easy detection and analysis.

The following diagrams illustrate a simple comparison of a normal VBS script and an encoded one.

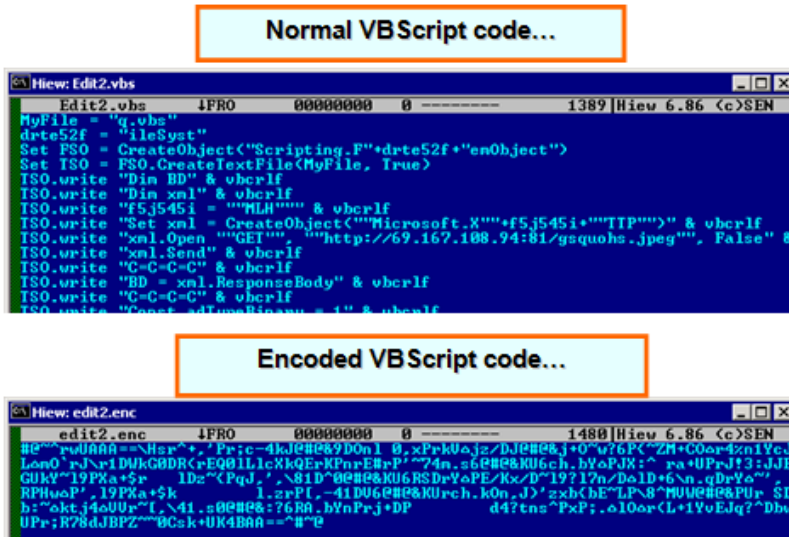


Figure 3-15: Encoded versus non-encoded script.

3.4 > Defending Against Malware

There are some basics precautions that can be taken to protect you against malware:

- Keep antivirus software up-to-date** – use security software which includes both antivirus and spyware protection for best results.
- Run full system scans frequently** – Scan all areas of your computer at least weekly.
- Keep operating system and applications up-to-date** – Many web threats utilize wholes or vulnerabilities in operating systems and applications. Ensure that all security patches and updates have been installed to close these gaps.
- Use a firewall** – Ensure all unused ports and connections are closed to your computer.
- Be wary of all messages with links or attachments** – Even if you receive a message from a friend or relative, never blindly click on links or open attachments.
- Use strong passwords** – Always use passwords with a minimum of eight (8) characters. Passwords should contain a mix of letters numbers and symbols.

3.5 > Chapter 3 Summary and Review Questions

Summary

Malware is also known as virus, worm, Trojan horse and logic bomb. Malware robs productivity and jeopardizes every organization's information security and infrastructure. These computer programs, written with spiteful intent, perform unauthorized routines to damage and destroy data, or degrade system performance.

Malware can be classified based on how they get executed, how they spread, and/or what they do. The classification is not perfect, however, in the sense that the groups often overlap and the difference is often not obvious.

The various characteristics that each category of malware can exhibit are often very similar. For example, a virus and a worm may both use the network as a transport mechanism. However, the virus will look for files to infect, while the worm will simply attempt to copy itself.

Review Questions

1. Which traits do all malware—viruses, worms, and Trojan—share in common? (Choose all that apply.)
 - a.) They originate from outside the network.
 - b.) They use or damage computer resources.
 - c.) They enter computer systems, usually without the user's knowledge or intent.
 - d.) They release hidden payloads designed to damage hard drives and corrupt data files.
2. What is the defining characteristic of Trojan horse programs?
 - a.) They appear to be harmless but hide malicious intent.
 - b.) They are not intended to cause harm and only make fun of the user.
 - c.) They replicate and attach themselves to host files.
 - d.) They do not require user intervention to spread or function.
3. Why are worms described as “self contained?”
 - a.) Worms do not replicate.
 - b.) Worms do not spread to other computer systems.
 - c.) Worms do not require a host file to spread.
 - d.) Worms do not carry payloads.



4. How does a mass mailing worm spread? (Choose all that apply.)
 - a.) Create a copy of itself in a directory
 - b.) Create a registry entry
 - c.) Get email addresses
 - d.) Executes a program

5. How are damages arising from computer threats categorized?
 - a.) Lost productivity, recovery and cleanup costs, lost data and damaged reputations
 - b.) Lost productivity, increased vulnerability to future virus attacks, loss of confidential data, loss of other data
 - c.) Network downtime, decreased availability of computer resources, disk damage, and problems in virus isolation
 - d.) Network disconnection, increased errors in the network, and damaged reputation due to loss of customer data



Chapter 4: Grayware

After completing this chapter, you should be able to:

- Define and understand grayware threats
- Identify the types of grayware and their characteristics
- Describe grayware behaviors and malicious activities
- Recognize payloads or symptoms of grayware infection



4.1 > Introduction to Grayware

There are species of codes and techniques that are designed to acquire information or cause users to behave in ways that they otherwise wouldn't, that are really on the border between malware and disputable as to the value of the application or message. However seemingly harmless, threats exist and can cause problems from lost productivity, illegal behavior, to data theft and more.

4.1.1 What Is A Grayware?

The term grayware refers to seemingly normal applications that have somewhat malicious behaviors. Just like malware, they are unwanted and potentially dangerous set of programs. They usually have annoying, undesired, and undisclosed malicious behaviors on the system. Below is a table that compares grayware with malware.

	Malware	Grayware
Origin	Virus Writers, Hackers	Legitimate software vendors
Considered Malicious	Always	User-dependent
Legal Issues	None	Yes
User Interface	None	Yes
EULA	None	Usually

Table X.Y: A high-level comparison between malware and grayware.

In some ways, Grayware are similar to legitimate applications because they are usually owned and released by real software vendors. However, due to some undisclosed behavior, they are detected by anti-virus and/or anti-spyware software. Some grayware programs are also potentially dangerous due to the fact that they can be used for malicious purposes; though, in and of themselves, they may not be malicious. What makes grayware similar to normal applications is due to the following:

- Grayware may have file properties
- Grayware may have installation guidelines and also may provide an uninstallation program to remove
- Grayware may also have end-user license agreement (or EULA) upon installation
- And most of the time, they have user interface which can either be GUI or a command line interface.

4.1.2 Classification of Grayware

Grayware can be classified according to what actions they take after being installed on a system. Although many people use the general term Spyware to describe Grayware, it is solely one classification within the Grayware category. The following sections describe the Grayware categories based upon the actions taken once installed.



Adware

Adware are applications that display advertising banners in Web browsers. They generate advertisements in the form of pop-up windows or hotlinks on Web pages. Usually, they encourage users to download items from the internet that may lead to malicious web sites or the so-called Disease Vectors.

Below are forms of Adware that can be encountered while browsing the internet and downloading untrusted applications.

NOTE If you choose to remove adware, some shareware programs which you installed may not function properly.



Figure 4-1: Adware example with "free" lure.

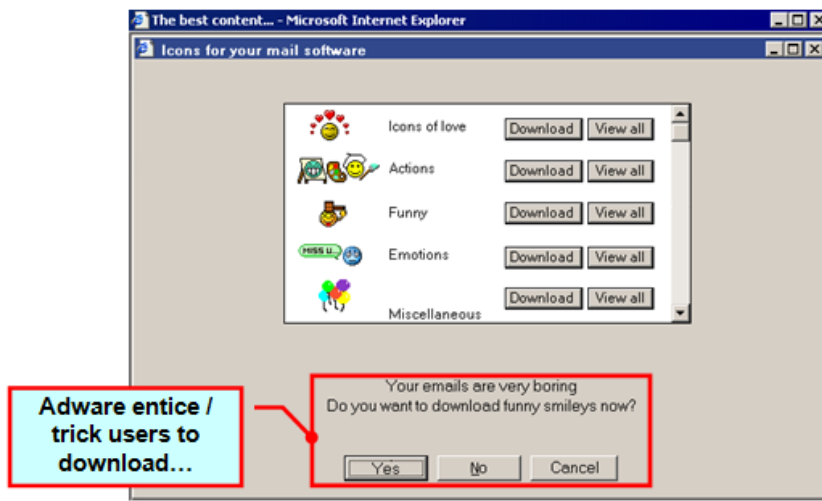


Figure 4-2: Adware example with built-in trick.



Figure 4-3: Adware example with scare tactic.

Browser Hijackers

Browser Hijackers are programs which can either be malware (Trojan clickers and Trojan spies) or grayware (might be an adware or spyware component) that alters a computer's browser settings to redirect users to web sites that they had no intention of visiting.

Browser hijacking can be done through the following methods:

- Modification of default home page and search page configuration
- Modification of URL bookmarks/favorites
- Pharming
- Real-time monitoring of user internet activities waiting for the “key word” on the address bar as a trigger for hijacking.

NOTE 📄 Pharming is the process of redirecting a website's traffic to fraudulent imitation websites.

An example of a Browser Hijacker is shown on the next page. Note that the URL is fake, which is a definite indication of a hijacking.



Figure 4-4: Example of Browser Hijacker.

Browser Helper Objects (BHO)

Browser Helper Objects are DLL modules designed as plug-ins for web browser applications to provide added functionality. The intent of many BHO's is not malicious. However, malicious behavior comes in if the BHO is intended to monitor user's browsing habits or to cause annoyances to users.

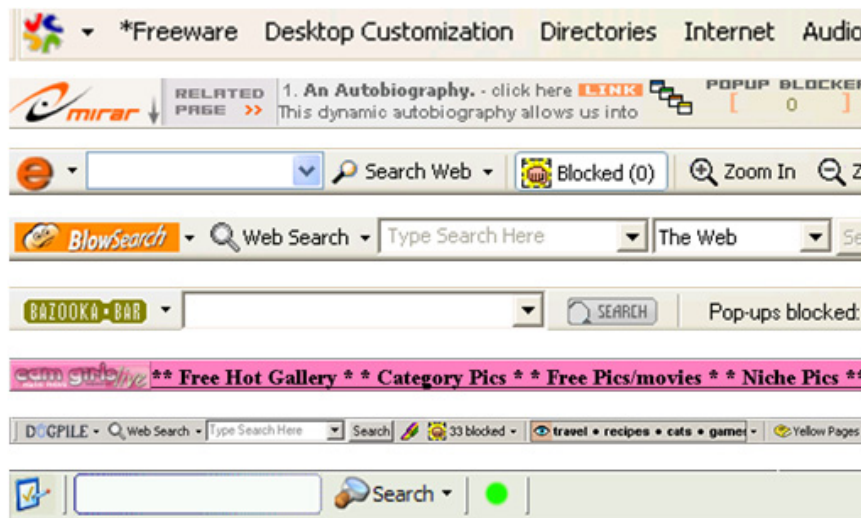


Figure 4-5: Browser Helper Object example plug-ins.

CoolWebSearch (or CWS)

CoolWebSearch is a general term for an adware or spyware that implements complex browser hijacking and complex installation on Windows, making them more difficult to remove. It is a robust infection that exhibits robust intelligence, technical prowess and a determination to survive removal attempts.

CoolWebSearch has evolved as a series of variants, each somewhat different than its predecessors, with the later variants significantly more complex to detect and remove. It is believed that the reason why new variants of CWS are regularly released is to avoid or defeat attempts to remove it from a computer which it has infected.

The difficulty of removing CoolWebSearch from a user's system is significant. In the early variants, CWS was slightly tricky to remove, but it could be done, carefully, by a knowledgeable Windows user. However, CWS has stepped up the battle and recent variants are virtually impossible to remove manually. Some CWS variants even use methods of hiding and running themselves that had never been used before in any other spyware strains.

Spyware

Spyware is a program that monitors and gathers user information for different purposes depending on what it is intended to do. It intercepts and logs user computing activities and transmits that information to an unknown third party without notifying the user.

Below are examples of spyware:

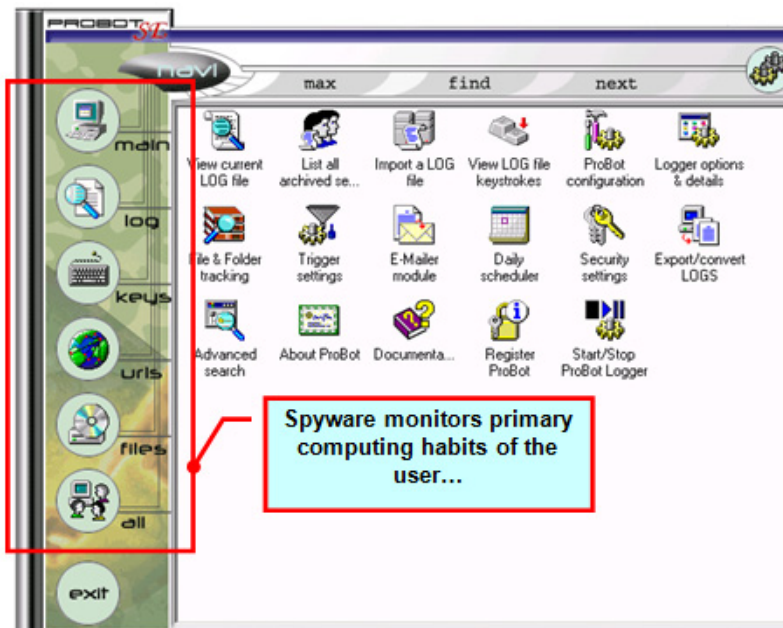


Figure 4-6: Spyware example that monitors user behavior.



Figure 4-7: Spyware example that logs computing habits.

Keylogger

Keylogger is a type of spyware that logs user keystrokes. Some Keyloggers are also capable of not just logging keystrokes but also capable of logging other information such as clipboard data, and screenshots. The logs might be transmitted to other unknown third party users.

Below are examples of keyloggers:



Figure 4-8: Keylogger example with user keystroke information.

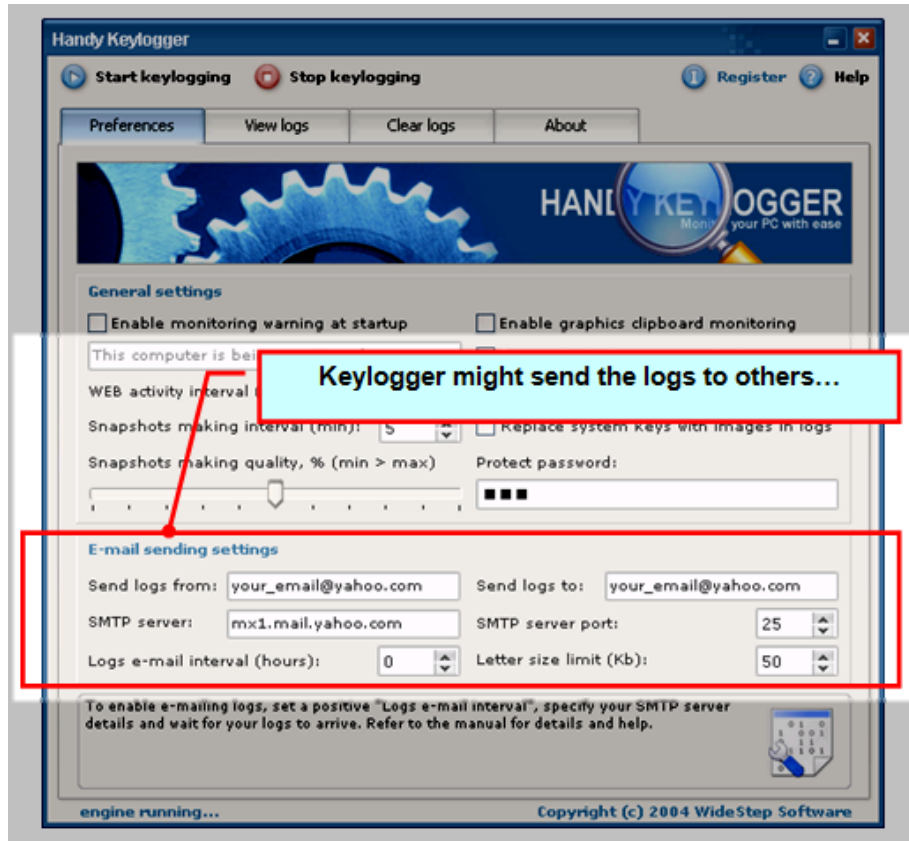


Figure 4-9: Example keylogger with log information.

Trackware

Trackware is a spyware program that collects demographic and usage information and sends it to some remote server via the internet where it can be used by other people in a variety of different ways, including marketing.

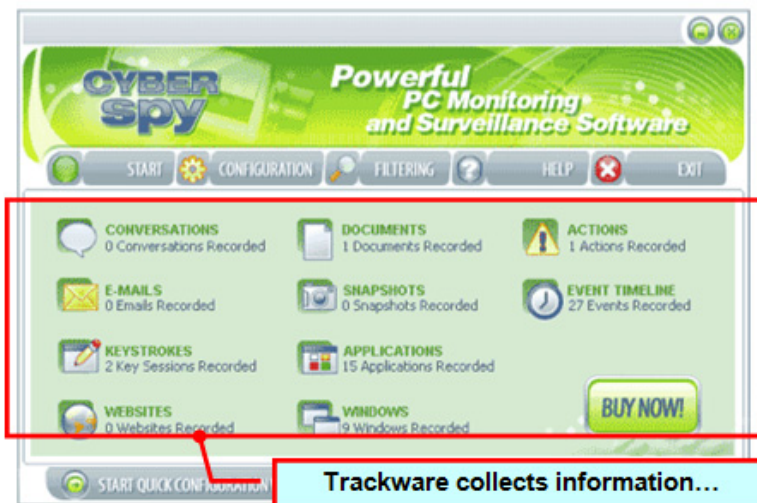


Figure 4-10: Example trackware that collects information.

Crackers and Keygens

A Cracker is a program that is used for illegally breaking (cracking) various copyright-protection and registration techniques used in commercial software.

Below is an example of a Cracker:

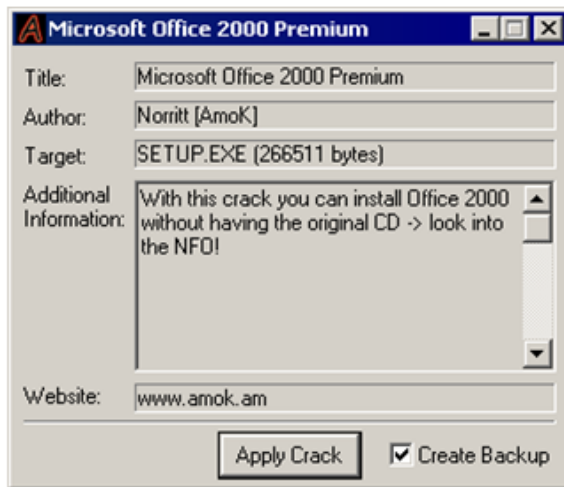


Figure 4-11: Cracker example with Crack button.

A Keygen (short term for Key Generator) is a program used to generate serial or license keys of a specific commercial software.

Below is an example of a Keygen:



Figure 4-12: Keygen example used to generate a key.

Dialers

A Dialer is a program which creates a connection to the Internet or another computer network over an analog telephone or ISDN network. Dialers are necessary to connect to the internet (at least for non-broadband connections), but some dialers are designed to connect to premium-rate numbers. The providers of such dialers often search for security holes (usually in Microsoft Windows) on the user's computer and use them to change the computer to dial up through their number, pocketing the additional money for themselves. Alternatively, some dialers inform the user what it is that they are doing, with the promise of special content, accessible only via the special number. Examples of this content include software for download, (usually illegal) MP3s, pornography, and in the case of at least one website, underground hacking materials (such as viruses).

Below are examples of Dialers:



Figure 4-13: Dialer example.



Figure 4-14: Dialer example.

Freeloaders

Freeloaders are programs that piggyback onto the installation of other software often without the user’s knowledge or consent. This means malicious programs are being bundled together with legit or normal applications without the use knowing it. Rogue anti-spyware programs are the most common example of this type of grayware.

Below is an example of rogue anti-spyware:

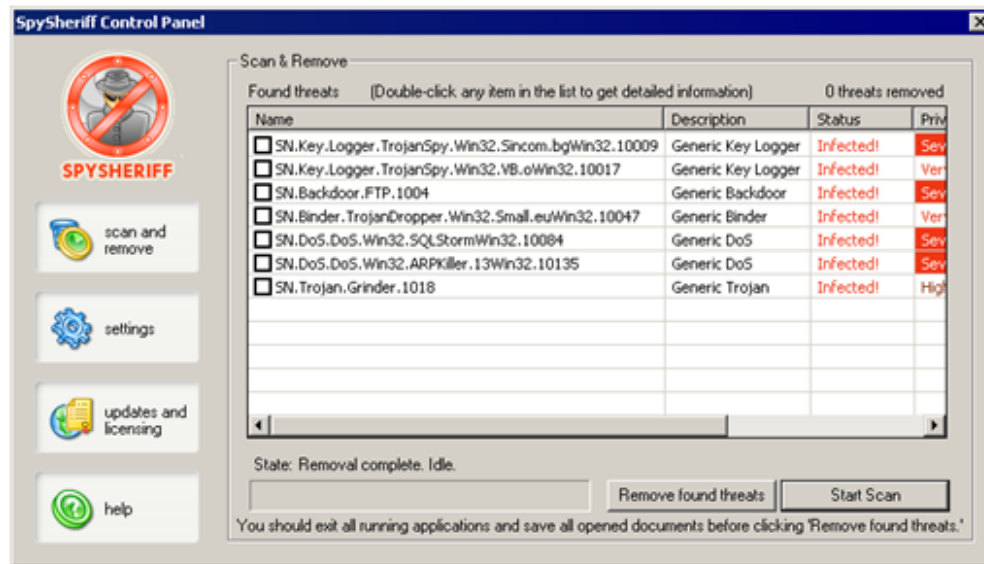


Figure 4-15: Example of freeloader type of anti-spyware.

The above example is a form of Freeloader because the program has seemingly detected several malicious files on the system. However, in reality, the same program is also the one who installed those malicious files.

Hacking Tool

Hacking Tools (or simply Hacktools) are programs that crack/break computer and network security measures. System administrators sometimes use these programs to test security and identify possible avenues for intrusion. These tools can be tagged as malicious if used or handled by wrong hands.

There are several main purposes of Hacking Tools:

Footprinting	The gathering of information about the target (i.e. computer and network domain security)
Scanning	Determining network security holes or vulnerabilities
Enumeration	Data extraction and queries

Below are examples of Hacktools:

```
[C:\>]rrpc.exe
RPC DCOM exploit coded by .:[oc192.us]:. Security
modified by bkb11 <bkb11@cnhonker.net> 2003/08/07
Usage:

rrpc.exe -d <host> [options]
Options:
-d:      Hostname to attack [Required]
-t:      Type [Default: 0]
-r:      Return address [Default: Selected from target]
-p:      Attack port [Default: 135]
-l:      Bindshell port [Default: 666]
-h:      the IP connect back to.
-P:      the port connect back to.
        Connect back using eyas's shellcode

Types:
0 [0x0018759f]: [Win2k-Universal]
1 [0x0100139d]: [WinXP-Universal]
```

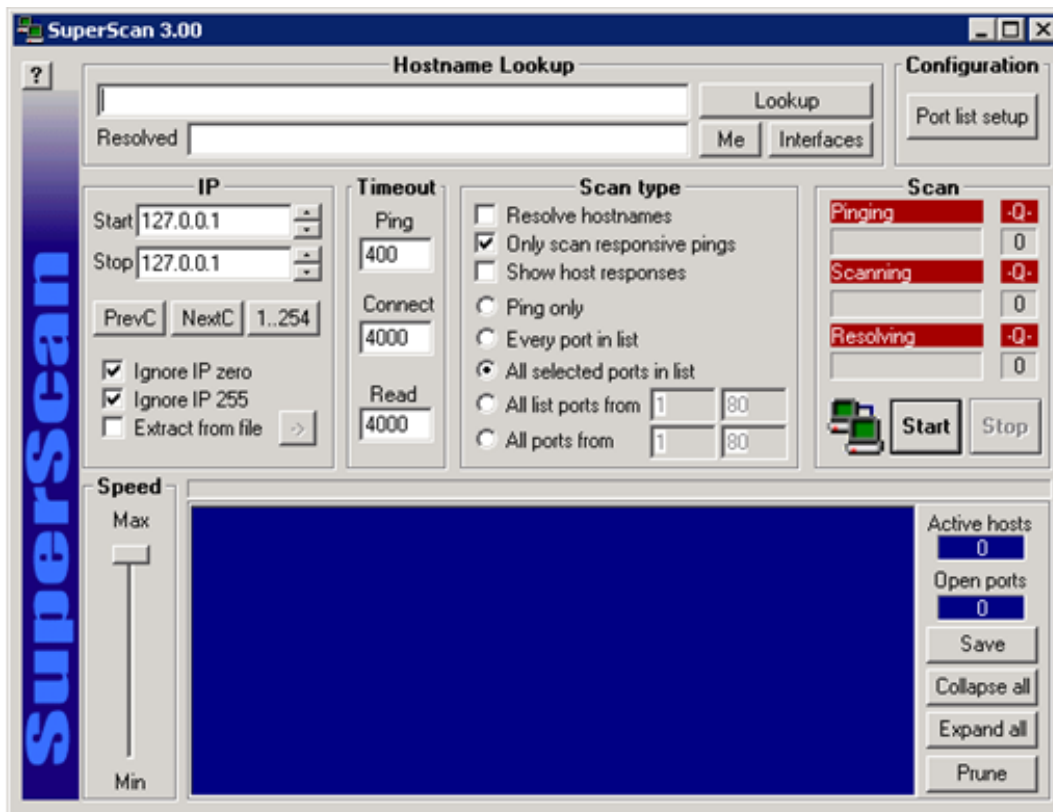


Figure 4-16: Example of two types of hacktools.

Remote Access Programs (RAP)

Remote Access Programs (or RAP) are programs that allow users to access and manipulate remote systems. They are legitimate tools used by network administrators to access files and data on remote computers. Like hacktools, these programs become malicious if used by wrong hands.

Below are examples of Remote Access Programs:

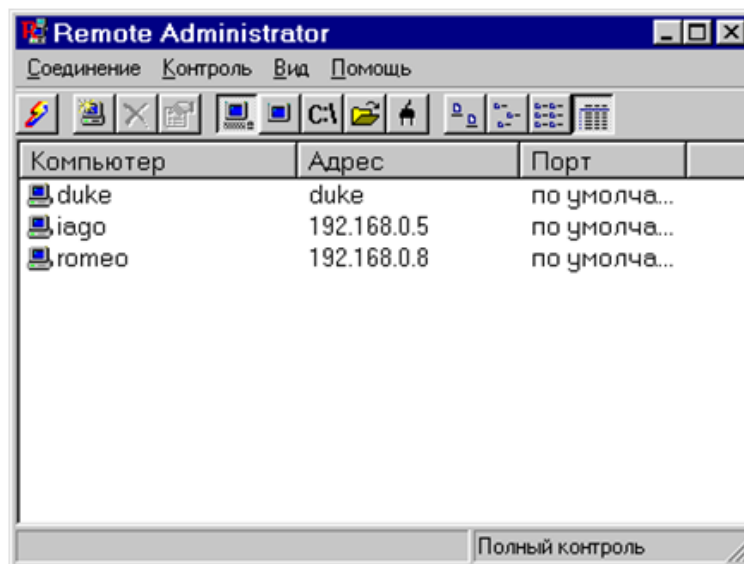
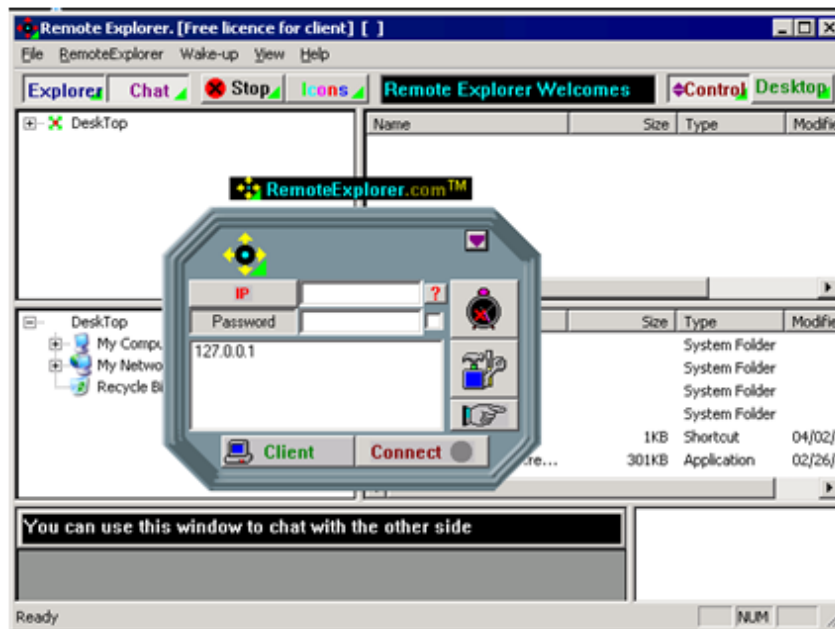


Figure 4-17: Examples of Remote Access Programs (RAP).

Joke Programs

Joke Programs are considered relatively harmless and are often designed to annoy or make fun of users. Many joke programs cause unnecessary panic - especially those that cause computers to behave as if something has been damaged.

Below is an example of a joke program:

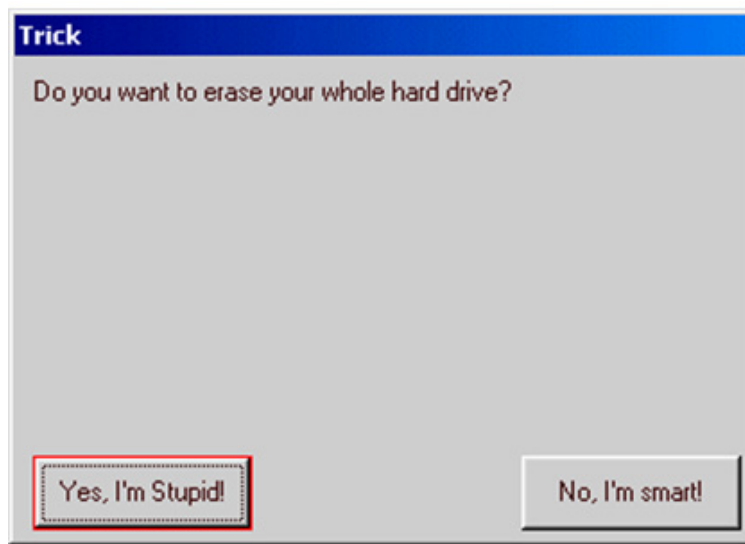


Figure 4-18: Joke program example.

4.2 > Understanding Grayware Behavior

Grayware can be identified easily by identifying their behavior. There three ways we can observe grayware malicious behavior.

- During installation
- During execution/running
- During uninstallation

The following three sections detail the behaviors of Grayware in each of these situations.

4.2.1 Grayware Behavior during Installation

Grayware has specific behavior during its installation. These behaviors include:

- End-User License Agreement (or simply EULA)
 - Is not displayed (or not adhered to)
 - Only partial EULA displayed
 - EULA is shown, but in tricky wording
- Privacy Policy is not displayed or not adhered to
- Installer fails to provide clear purpose, functionality and/or intention
- Installs additional applications or programs with or without notification
- Exploits on certain vulnerabilities are used to install
- Rses ActiveX, Java and/or other web-based installers



- Installed by malware, such as viruses and Trojans
- Installs new or custom run-time packed files
- Installs Browser Helper Object (BHO)
- Lowers browser Security Settings
- Lowers OS Security Settings
- Makes critical registry changes (i.e. AutoStart)
- Injects itself to other running applications/programs
- Registers itself on Windows by having its own CLSID or PROGID
- Modifies existing browser favorites (or bookmarks)
- Modifies Layered Service Provider (LSP) Stack
- Modifies Host File (Pharming)
- Uninstalls competitive applications without user's consent during installation

4.2.2 Grayware Behavior while Running

Grayware behaves in a variety of ways while running, depending on the design and intent of the approach. The behaviors include:

- Monitors or collects personal data (including documents)
- Monitors or collects bank account information
- Monitors or collects passwords
- Monitors or collects keystrokes
- Monitors or collects screenshots
- Monitors or collects existing application list
- Monitors or collects document history
- Monitors or captures email
- Monitors or captures instant messaging communication
- Monitors or captures personal information (Name, Address, SS#, TIN, etc)
- Monitors or captures data or information about running applications
- Monitors or captures network traffic packets
- System vulnerabilities are collected or revealed
- Auto-updating without notification
- Displays advertising banners
- Replaces or alters web contents
- Replaces search results
- Abuses network, CPU, and memory resources
- Allows remote process execution and/or termination

- Used to perform DoS/DDoS
- Disables/terminates other applications
- Fails to clearly label advertising pop-ups
- Fails to clearly label advertising windows coming from the application
- Impacts system stability
- Installed items' file properties are bogus or incomplete
- No visible taskbar or system tray icon
- Process (or Processes) re-spawn upon manual termination
- Uses stealth/rootkit techniques to conceal files, windows, processes, and registry keys
- Hijacks default search and home pages of browser
- Alters default internet connection (telephony/broadband)
- Dials an unprompted or unauthorized internet connection
- Opens web sites not initiated by users
- Misleading taskbar or system tray icon
- Uninstalls competitive applications without user's consent while its running
- Displays fake or annoying messages that trick users into believing something is wrong
- Modifies/patches applications, programs, or files to bypass copyright protections

4.2.3 Grayware Behavior during Uninstallation

Grayware behaves differently than most desired applications that you intentionally install on a computer. The uninstallation process that includes these behaviors generally indicates the presence of grayware:

- Does not provide uninstallation program
- Uninstallation program does not work (or fails to complete full uninstall)
- Uninstaller causes substantial damage during uninstall
- Does not allow removal/uninstall through third party application
- Reboot is necessary for manual removal to work
- Installs other applications and/or files during uninstall
- Uninstallation requires internet connection
- Uninstaller fails to remove bundled applications
- Uninstaller is not easily accessible
- Uninstalls competitive applications without user's consent during removal
- Complete removal but removal has tricky uninstaller (wording and features of uninstaller)
- Uninstallation requires a survey to be completed before uninstallation can be completed



4.3 > Defending Against Grayware

There are some basic precautions that can be taken to protect you against grayware:

Keep antivirus software up-to-date – use security software which includes both antivirus and spyware protection for best results.

Use a firewall – Ensure all unused ports and connections are closed to your computer.

Adjust browser security settings – Ensure your browser does not allow content to run automatically or in the background when visiting web pages.

Use safe browsing habits – Only download from trusted sources. Read license agreements and security warnings. Be wary of popup ads notifying you of infections.

4.4 > Chapter 4 Summary and Review Questions

Summary

Grayware is a subcategory of malware. Like malware, grayware contains unwanted and sometimes malicious code. Grayware is associated with annoying, undesired, and undisclosed malicious behavior, such as harvesting user data, computer use data, and Web activities.

Grayware is classified by the type of action it performs. Adware displays advertising banners. Browser Hijackers alter the computer's browser setting so that the user is redirected to another site. Browser Helper Objects (BHOs) are browser plug-ins that can be used to monitor the user's browsing habits. CoolWebSearch (CWS) is a more complex form of browser hijacking. Spyware monitors, gathers, and sends user information for different purposes. Keyloggers are a form of spyware that logs and sends user keystroke information. Trackware collects and sends user-related demographic and usage information. Crackers and keygens illegally break copyright protected software keys. Dialers create analog connections to the internet to typically lure users to spend money on dialup numbers of websites. Freeloaders are programs that piggyback onto the installation of other software that users install, without the user's knowledge or consent. Hacking tools crack computer and network security measures. Remote Access Programs (RAP) allow users or hackers to manipulate remote systems. Joke programs annoy or make fun of users.

Grayware is also known for specific behaviors during installation, while the computer is running, and during uninstallation attempts. Clues that grayware is attempting to install include the lack of a privacy policy, that there is no clear purpose, functionality, or intention, and it installs BHOs. Grayware may be on a computer, for example, when web content is altered, applications are terminated, advertising pop-ups are not labeled, or auto-updating is performed without notification. Grayware may be on a computer if, for example during an uninstall, the uninstallation program does not work or other files are installed during an uninstall attempt.

Review Questions

1. Which form of grayware has infected your computer if your keystroke data is logged?
 - a.) Adware
 - b.) Browser Helper Object
 - c.) Keylogger
 - d.) Trackware
2. Which form of grayware is used to crack software copyright protection keys?
 - a.) Browser Helper Object
 - b.) Keylogger
 - c.) Keygen
 - d.) Spyware



3. Which form of grayware tries to tempt users to use create a connection to the Internet using a telephone line and connection fee?
 - a.) Spyware
 - b.) Dialer
 - c.) Hacking Tool
 - d.) Joke Program
4. Which computer behavior would make you suspect that you might be installing grayware? (Choose all that apply.)
 - a.) Additional programs are also being installed at the time of installation
 - b.) ActiveX is being used as an installer
 - c.) A Browser Helper Object (BHO) plug-in gets installed on the browser
 - d.) The browser security settings remain the same
5. Which computer behavior would make you suspect that you are running grayware on a machine without your consent? (Choose all that apply)
 - a.) Advertising banners are displayed
 - b.) The computer performs an auto-restart
 - c.) The system becomes unstable
 - d.) The computer disconnects from the Internet



Chapter 5: Web Threats

After completing this chapter, you should be able to:

- Discuss web threats and the concepts behind it
- Discuss forms of web threats and how they affect web users



5.1 > Introduction to Web Threats

Web threats infect computers through the World Wide Web. The internet is home to hundreds of thousands of people, places, and things that have intent to misuse your computer and your data.

5.1.1 What is a Web Threat?

Web Threats are any threat that uses the internet to perform malicious activities. They arrive, spread, deliver additional exploits and entrench themselves via the internet and may include Trojan Horse programs, spyware, adware, Pharming and other malware. They also may be triggered by a hyperlink or an executable file attachment in a spam email.

Web Threats are characterized by blended techniques, an explosion of variants, and targeted regional attacks. They pose a broad range of potential costs, including identify theft, loss of business confidential information, damaged brand reputation, and erosion of consumer confidence in Web commerce.

5.1.2 Web 1.0-Web 2.0 Security Implications

Topic	Web 1.0	Web 2.0	Security Notes
Code	HTML	AJAX	Asynchronous Javascript and XML (AJAX) is a cluster of programming languages designed to make Web pages behave more like applications. HTML-architected Web pages require users to reload Web pages to view new data sets, but AJAX continually exchanges data with the server so that users can enjoy faster responses with their requests. In Google Maps, for example, AJAX enables rapid loading times and heightened user activity with the application (e.g., zooming in and out to check current locations). Since AJAX is an amalgam of constantly evolving languages, it creates a larger exploitable attack surface for cyber criminals. AJAX so far has been implicated in XSS and XSRF attacks (see below).
Platform	Browser and Operating System	Web	With Web sites themselves acting as applications, protecting the browser and operating system (OS) does not guarantee security against Web 2.0 threats. Consider mashups, or Websites that integrate input from disparate sources to create a unified experience. HousingMaps.com, for example, is a mashup of Google Maps and Craigslist. Google Maps handles the visual mapping, while Craigslist provides associated real estate information. Although mashups enable a rich user experience, their aggregation of multiple applications creates more potential points of vulnerability for malware to exploit.
Client Role	Limited	Heavy	Cyber criminals can inject malware directly into Web 2.0 sites and applications. For Web 2.0 hackers, there's "More fun to be had on the front end."



Topic	Web 1.0	Web 2.0	Security Notes
Syndication Model	None	RSS, Atom	Syndication built atop Atom standard, and employing the Really Simple Syndication (RSS) file format allows publishers of Web logs, or blogs, to automatically distribute posts to a body of subscribers. If a Web 2.0 worm such as the Storm Trojan infiltrates a given blog, syndication is a simple way of distributing the threat to many unsuspecting potential victims.
Peer-to-Peer Model	None	BitTorrent, Napster, etc.	Peer-to-Peer (P2P) is a computing model in which clients connect directly to each other. P2P became popular when Napster first afforded individuals the power to store and share music files from their desktops. P2P remains a central part of the Web 2.0 model. Technologies such as BitTorrent allow users to upload and download large files without build-in security. This increases the risk of inadvertently acquiring ride-along malware.
Content Creation/ Editing	Single User	Community	Allowing a user to add content to an online community enables users to target that community with malware. A manifest case is cross-Site Scripting (XSS)—a means of injecting malicious code from one Web site into another. Cross-site reference forgery (XSRF) combines XSS and social engineering techniques.
Completeness	Iterative	Perpetual Beta	Web 2.0 evolves in response to user inputs. Perpetual immaturity means Web 2.0 Web sites will almost always present new weak links for malware to attack.

Table 5.1: Security Implications of Web Threats.

5.1.3 Impacts and Extent of Web Threats

Web Threats help cyber criminals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is primarily confidential information leakage in the form of identity loss or use of the infected user as a vector to deliver phishing or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in Web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities, such as sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

5.2 > Social Engineering

In order for Web Threats to be successful on fulfilling their goals, there is always a need to entice or lure people into becoming victims of such threats. This overall process of attracting people, luring them to do things for the fulfillment of malicious goals, is known as Social Engineering.

5.2.1 What is Social Engineering?

Social Engineering is a term popularized as the means by which people are manipulated into performing certain actions. Most Social Engineering techniques are based on flaws in human logic, known as Cognitive Biases. Without delving too much into the psychology, it is enough to say that when played right, Social Engineering can and will, time and again, force people into actions that would, on hindsight, be against their common sense. In the case of malware authors, there are three aspects that may be of use to this end:

- The purported sender
- The malware reference
- The message content

The sender, or the apparent origin of the message, bolsters the impression that the message is legitimate. The malware may do this by spoofing known email addresses or addresses from the affected user's contacts list, or by stating that the sender is a certain authority such as, the network administrator or perhaps a bank. The attachment or link referring to the actual malware may be renamed for additional leverage, either by changing the file name into something consistent with the message content, or by adding a file name extension before the real file type (such as renaming an .EXE file as CHRISTMAS.TXT.EXE).

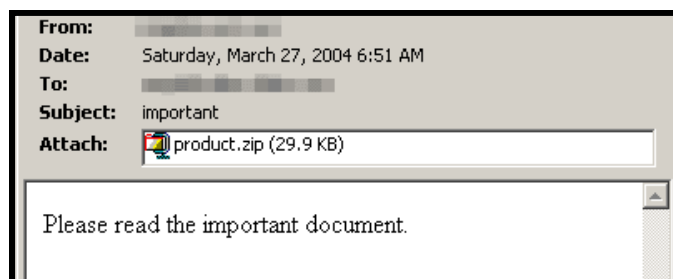
Of the three, the message content carries the brunt of the impact, as it may evoke a certain reaction or action from the receiving party. We will begin our understanding of Social Engineering by identifying the different types of message content being used.

5.2.2 Types of Message Content

There are several approaches that social engineering takes to accomplish its objective. Typically, the content affects the user behavior, or at least tries to lure the user to fall for the trap.

Generic Conversation

Messages of this type are often conversational and friendly in nature. It is the most basic type of message, consisting of short and simple sentences that are easy to compose on the part of the malware author. It appears harmless to most users, which increases the chances of them clicking on the link or attachment. Also, such messages attempt to take advantage of the feeling of familiarity with the user, especially if the message sender has been spoofed. Some messages are also crafted to make it appear as if the sender was replying to something that the recipient has previously sent. WORM_NETSKY, in particular, was seen to have used this type of message content as shown by the following samples:



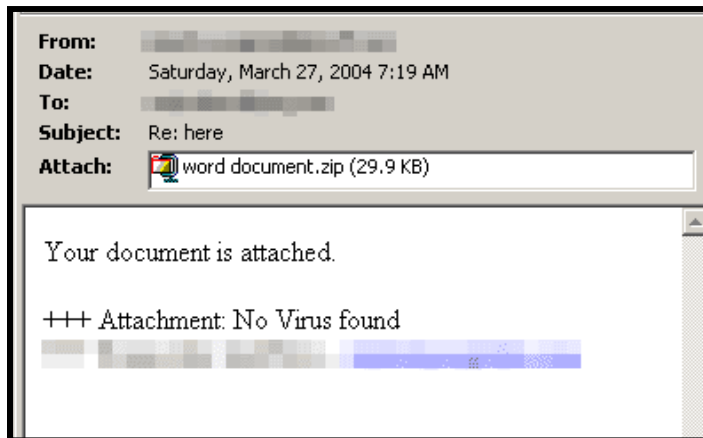


Figure 5-1: Examples of generic conversation.

Non-English Language Used

Most worms that are in the wild compose their email messages or instant messages in English presumably for universality. Some worms, however, send messages in a foreign language. A particular variant of WORM_SOHANAD sent instant messages via Yahoo! Messenger (YM) in Vietnamese.

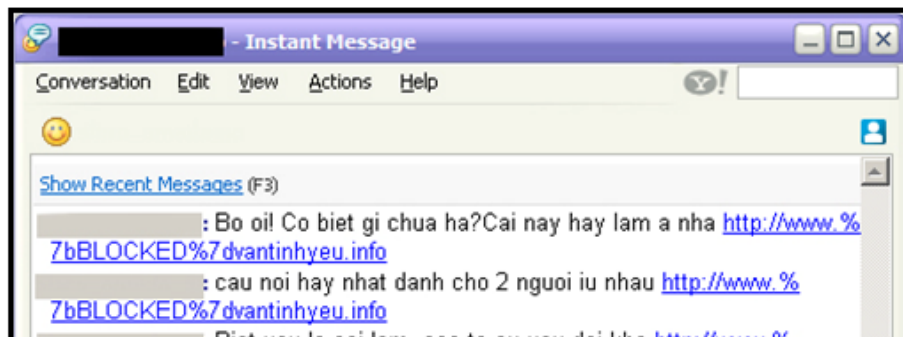


Figure 5-2: Example of Non-English Language Used.

There are two possible reasons for this. First, if the recipient of the message knows only English, a message written in a foreign language might pique interest. Second, the malware behind the message may be targeting a particular geographical area or group of people.

Virus Alert/Software Patch Required

This type of message is crafted to take advantage of the common user's fear of malware. Recipients of this message are alerted for a new and dangerous virus that is currently spreading and also that the only way to get rid of the virus would be to install the software patch that is attached to the email. In some cases, the message is composed to appear legitimate. For instance, footers can be inserted at the end of the email saying that the message has been scanned by an antivirus product when in fact it is not. Below are examples of this type of message from WORM_SOHANAD and WORM_NUWAR malwares.

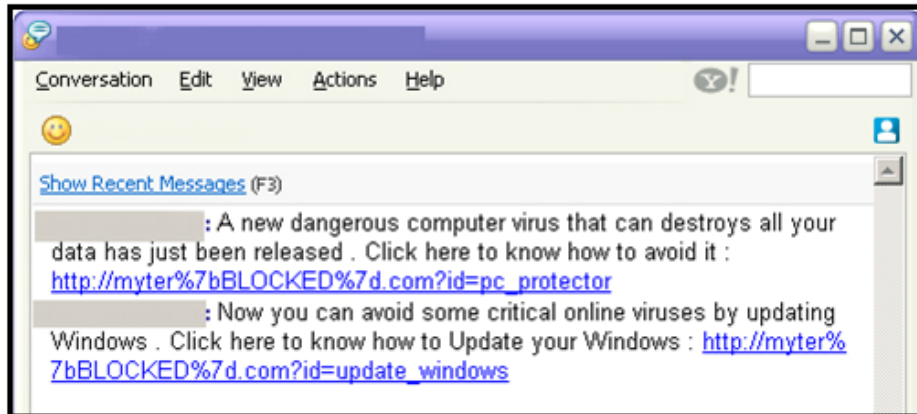


Figure 5-3: Example of virus alert message.

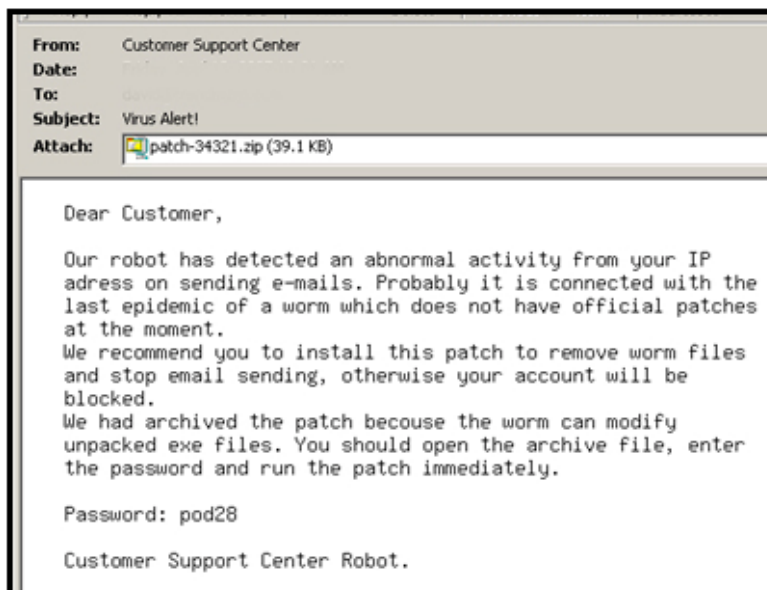


Figure 5-4: Example of software patch required message.

Malware Found

Messages of this type often appear as an email announcement from the network administrator informing the user that a malware has infected the workstation. It then instructs the affected user to click on the attachment to mitigate the threat. The attachment or link that is referred to in this message is a copy of the malware itself. Similar to the previous message type, some messages in this category may also be crafted to appear legitimate and credible. Below are the examples of these messages.

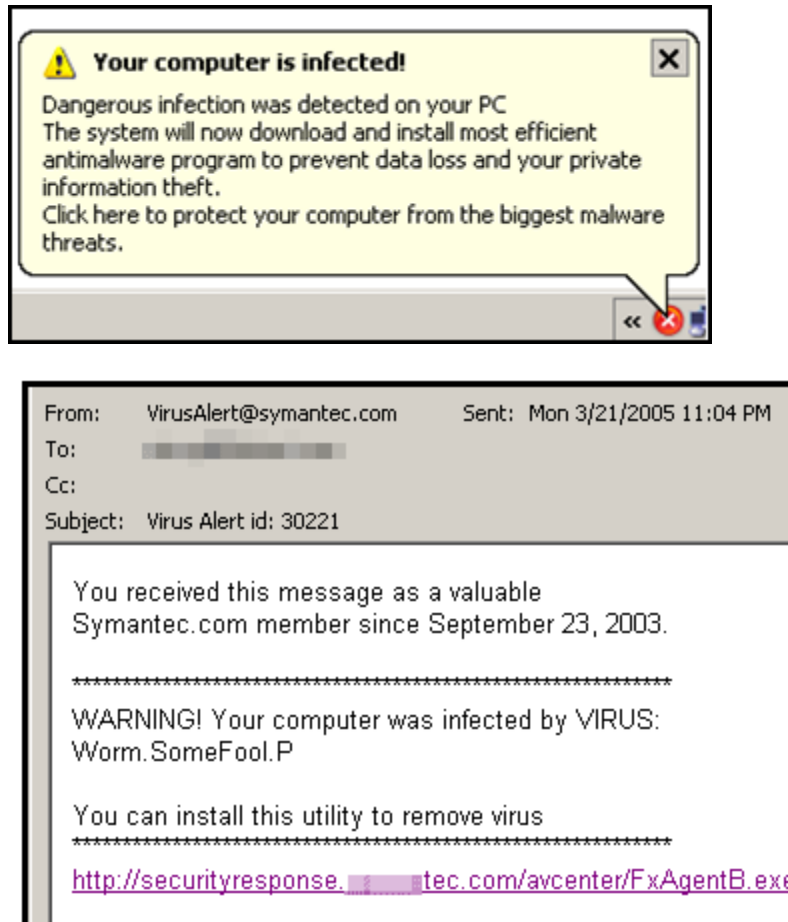


Figure 5-5: Examples of malware found message.

Account Information

This kind of message takes advantage of the user's sense of responsibility. In this case, the message informs the user of a particular issue regarding an account, such as a bank account, credit card account, etc. It requires the user to perform a specific action, usually initiated by clicking on the attachment or link. This method is also used by most phishing Web sites. Below is an example of this message type.

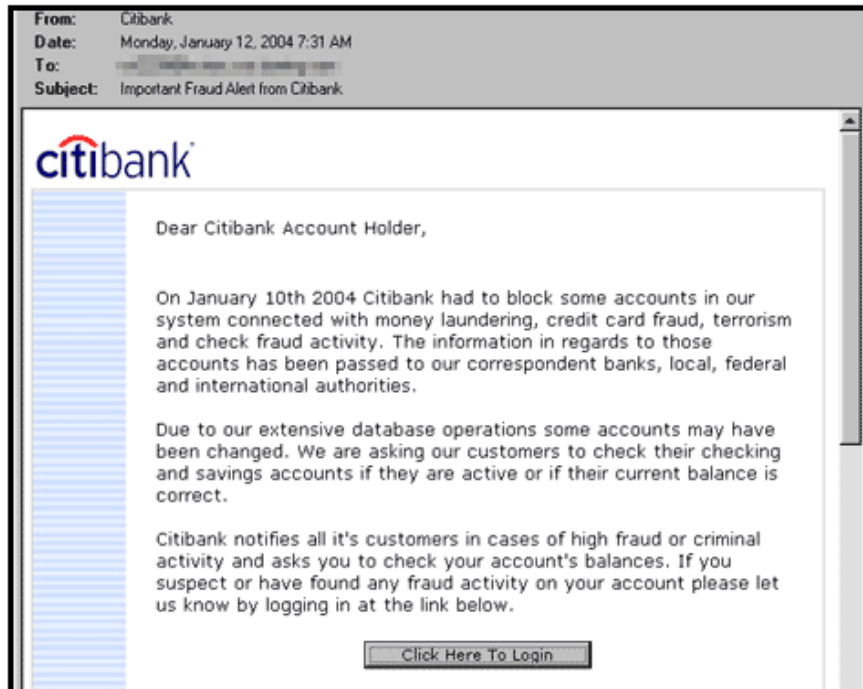


Figure 5-6: Example of solicitation for account information.

Mail Delivery Error

This message type is another popular tactic of email-borne malware. Worms that send this message take advantage of the ordinary user's unfamiliarity with how email feedback systems work. What the user receives is a message mimicking a Non-deliverable Receipt (NDR), informing him that the email that he previously sent failed to reach the intended recipient and that the details of the original message are included in the attachment or link, which is a copy of the malware itself. WORM_MYDOOM has employed this method as shown below.

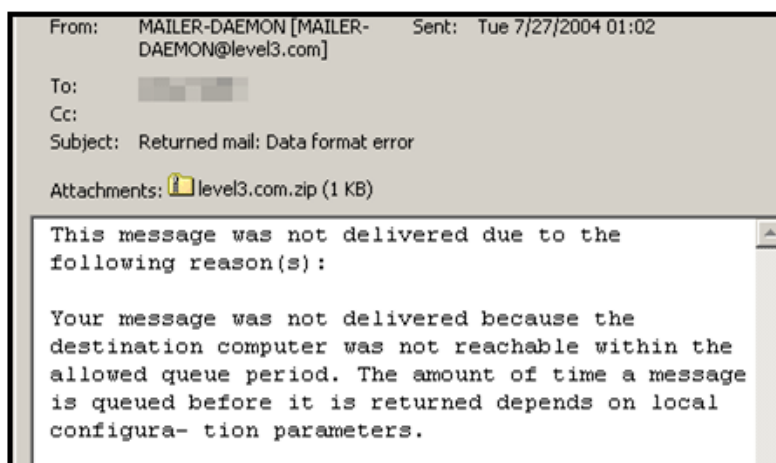


Figure 5-7: Example of mail delivery error message and attachment.

Physical Attraction

This is one of the most common types of messages that are sent by malware, not only in the recent years but in the past as well. The message is often short and straightforward, offering pictures of naked women, especially popular female celebrities. Sometimes, the picture is actually the malware attachment with a modified icon to resemble that of .JPG files. An example below is an email generated by a certain variant of WORM_BAGLE.

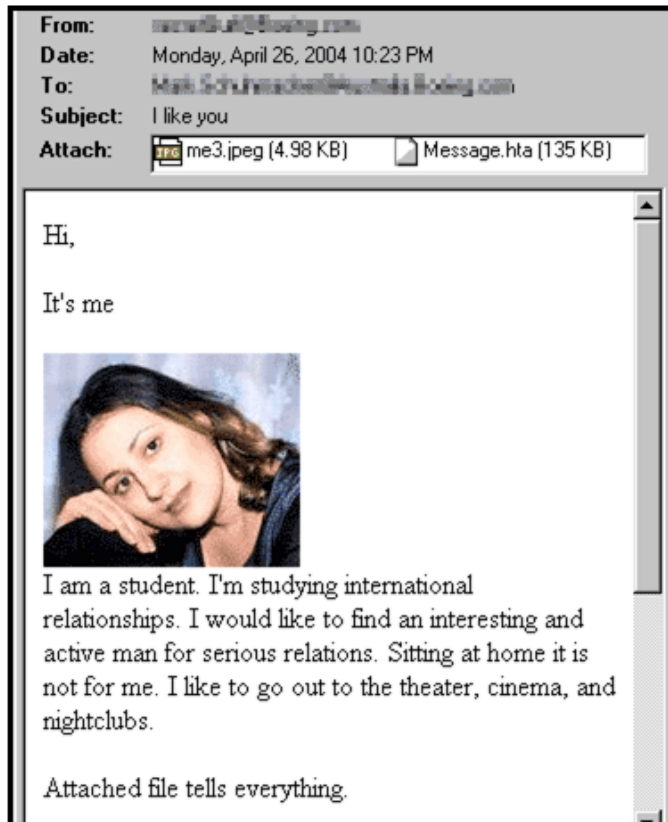


Figure 5-8: Example of physical attraction message and attachment.

Accusatory

Malware that send messages that fit into this category rely on the user's guilt to entice them into clicking on the attachment or link. Messages of this kind accuse the user that he has done something wrong or even illegal. To correct the situation, it instructs the user to open the attachment or to visit the indicated link, which would eventually download and install the malware on the user's system. To provide credibility and authenticity, some messages are crafted so that they appear to come from a legitimate entity such as a law enforcement agency or a government organization. Malware rarely compose messages such as this perhaps because it alarms users and makes them more suspicious and wary. Below is an example of this type of message.

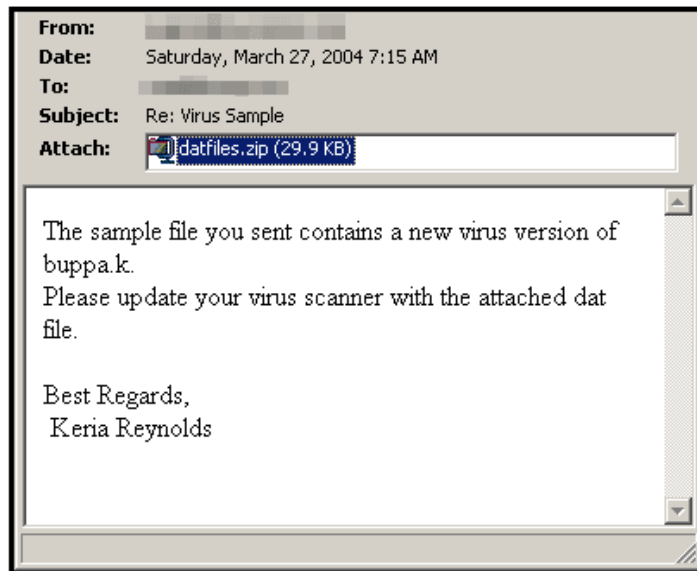


Figure 5-9: Example of accusatory message.

Current Events

Some malware capitalize on the interest of users in news and current events. Popular events in sports, entertainment and global politics are often the content of such messages. The email is crafted like a teaser for a news article; the subject contains the headline, which is written in a sensational manner. The message contains a one-liner summary of the news article and offers a full news story that the user can access by clicking on the attachment or link. A certain variant of WORM_NUWAR is notorious for using actual CNN headlines as the subject of the email that it sends out.



Figure 5-10: Example of current events message.

Free Stuff/Free Download

Messages of this kind work in the same way as messages that offer pornographic or sexually explicit material, but this one banks on greed. The actual content is brief and straightforward, usually offering easy money, cracked software, free MP3s and the like. Below is an example of this type of message that is being generated by WORM_NOOMY malware.

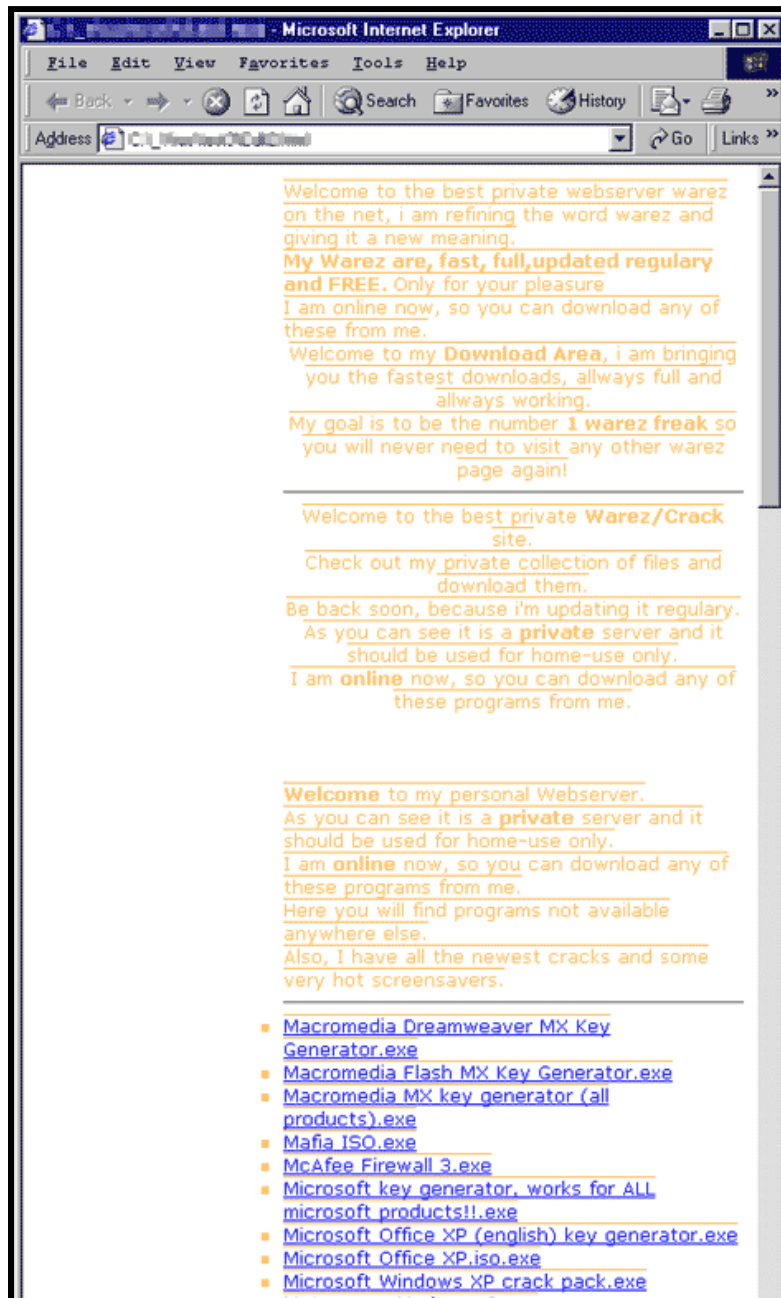


Figure 5-11: Example of free stuff/free download message.

5.3 > Forms of Web Threats

The common forms of Web Threats include Spam, Phishing, and Pharming. While they all use the Web to perform malicious deeds, each has its characteristics that are unique.

5.3.1 Spam

Spam represents a high volume of the threats that exist on the Web. *Spam* messages can promote social engineering and put your machines and personnel at risk.

What is Spam?

Most people define *Spam* generally as any unsolicited e-mail. However, if a long-lost brother finds your e-mail address and sends you a message, this could hardly be called *Spam*, even though it's unsolicited. Real *Spam* is e-mail advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, *Spam* also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight *Spam* with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some private online service, such as America Online, have instituted policies to prevent spammers from spamming their subscribers.

There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song: "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam..." Like the song, spam is an endless repetition of worthless text.



Figure 5-12: Example of Spam.

Spam is generally a collective term for “unwanted messages or information” that are being sent across the internet. Its purpose is to commercially promote some information related to advertising which can either be true (real advertisement) or false (hoax). These are “unwanted” because people who receive it, typically do not need it. Most *Spam* messages are accompanied by certain URL link/s for the purpose of phishing.



Forms of Spam

Spam take several forms, the most well known is email Spam. However, *Spam* can be targeted toward other places, such as newsgroups and chat.

EMAIL SPAM

Emails are considered *Spam*, if it is unsolicited and unwanted. The purpose of spammed email messages is for mass advertisement promotions that do not require a huge amount of money. Most of the time, unsolicited commercial email only intends to inform users about new products and services available on the market. However, this communication mechanism has been transformed to the point where spammed mails became bulk and spammers have become abusive. Users are now avoiding any unsolicited emails, considering them unwanted and annoying.

Spammers need to gather huge lists of potential e-mail addresses. Since Spam is, by definition, unsolicited, this address harvesting is done without the consent of the address owners. Spammers may harvest e-mail addresses from a number of sources. The first is newsgroups and chat rooms, especially on big sites like AOL. People often use their screen names, or leave their actual e-mail addresses, in newsgroups. Spammers use pieces of software to extract the screen names and e-mail addresses automatically.

The second source for e-mail addresses is the Web itself. There are tens of millions of Web sites, and spammers can create search engines that spider the Web specifically looking for the telltale "@" sign that indicates an e-mail address. The programs that do the spidering are often called *spambots*.

The third source is sites created specifically to attract e-mail addresses. For example, a spammer creates a site that says, "Win \$1 million!!! Just type your e-mail address here!" In the past, lots of large sites also sold the e-mail addresses of their members. Or the sites created "opt-in" e-mail lists by asking, "Would you like to receive e-mail newsletters from our partners?" If you answered *yes*, your address was then sold to a spammer.

The fourth source of e-mail addresses could be a "dictionary" search of the e-mail servers of large e-mail hosting companies like MSN, AOL or Hotmail. This is the use of the so-called "dictionary attack" being implemented to open a connection to the target mail server and then rapidly submits millions of random e-mail addresses. Many of these addresses have slight variations, such as "empoy1@yahoo.com" and "empoy2@yahoo.com." The software then records which addresses are "live," and it adds those addresses to the spammer's list. These lists are typically resold to many other spammers.

The last but not the least common practice of spammers is to create accounts on free webmail services, such as Hotmail and Yahoo Mail, to send spam or to receive e-mailed responses from potential customers. Because of the amount of mail sent by spammers, they require several e-mail accounts, and use web bots to automate the creation of these accounts.

In an effort to cut down on this abuse, many of these services have adopted a system called the *captcha*: users attempting to create a new account are presented with a graphic of a word, which uses a strange font, on a difficult to read background. Humans are able to read these graphics, and are required to enter the word to complete the application for a new account, while computers are unable to get accurate readings of the words using standard optical character recognition (OCR) techniques. Blind users of *captchas* typically get an audio sample.



annoy or get the attention of the victim. A *SpIM* typically contains a link to a Web site that the SpIM'ers is trying to market.

In many cases, SpIM'ers send messages to vulnerable machines consisting of text like "Annoyed by these messages? Visit this site." The link leads to a Web site where, for a fee, users are told how to disable the Windows messenger service. Though the messenger service is easily disabled for free, the scam works because it creates a perceived need and offers a solution. Often the only "annoying messages" the user receives through Messenger are ads to disable Messenger itself. It is often using a false ID to get money or credit card numbers.

Chat Spam can occur in any live chat environment like IRC and in-game multiplayer chat of online games. It consists of repeating the same word or sentence many times to get attention or to interfere with normal operations. It is generally considered very rude and may lead to swift exclusion of the user from the used chat service by the owners or moderators.

MOBILE PHONE SPAM OR SMS SPAM

Mobile Phone Spam is a form of spamming directed at the text messaging service of a mobile phone. It is described as mobile spamming, *SMS Spam* or *SpaSMS* but is most frequently referred to as m-spam.

As the popularity of mobile phones surged in the early 2000's, frequent users of text messaging began to see an increase in the number of unsolicited (and generally unwanted) commercial advertisements being sent to their telephones through text messaging.

Spam as a Threat

Aside from being unwanted and annoying for most web users, Spam is also considered as a potential threat to IT security. One purpose of Spam is phishing, by which it is used as a method of attracting and tricking users upon divulging personal information on the web. Most Spams that are related to phishing always carry a hyperlink in the message body whereby users are encouraged to click the said link and, upon doing so, will lead them to become victims of information theft on the web.

Spams may also be used to do denial of service. Since they are unwanted, they can be used as garbage data to slow down network traffic by eating a lot of network bandwidth and for the result, everybody will going to have hard times accessing the network. They can also be used to fill in the target user's mailbox until it can not anymore accommodate any other incoming mails resulting to "exceeded mailbox quota" on the part of the user thus no more mails shall be received. This malicious act is what is called "mail bombing".

5.3.2 Hoax

A *hoax* is a form of social engineering that, while seemingly low on the threat scale, affects the security of a computer and the user's productivity.

What is Hoax?

A *hoax* is an attempt to trick people into believing that something false is real. There is often some material object involved which is actually a forgery; however, it is possible to perpetrate a hoax by making only true statements using unfamiliar wording or context. Unlike a fraud or con (which is usually aimed at a single victim and are made for illicit financial or material gain), a

hoax is often perpetrated as a practical joke, to cause embarrassment, or to provoke social change by making people aware of something. Many hoaxes are motivated by a desire to satirize or educate by exposing the credulity of the public and the media or the absurdity of the target.

The Threat behind Hoax

Since hoax messages contain false facts, it may be unwanted after all. However, the question is why do some people keep on sending false information and try to let others believe? There is only one answer and that is to measure the working of Social Engineering while harvesting information from users who are forwarding these hoax messages.

A hoax is an attempt to determine how gullible web users are. The more who believe, the more will be sent, and the more will be victimized. Hoax messages can be easily recognized since they often contain this line: "...forward this message to 10 or more people..." or "...spread this message around immediately..." If one user has received it and believed it after reading it, then he/she will spam the same message to 10 or more other people. The problem with this scenario is that every time hoax messages, mostly in the form of email, are being forwarded to more people, email addresses will also reflect on the message thus as time goes by, these addresses are getting collected on the same email thread. Afterwards, spammers will also receive these messages and eventually harvest the collected email addresses.

5.3.3 Phishing

Another form of Web Threat is *Phishing*. Its effect as a social engineering tool rates high among malicious intent.

What is Phishing?

Phishing is a malicious activity involving Social Engineering techniques that would lead users to divulge their personal information such as personal account details, usernames and passwords, credit card details and banking transaction details. Phishing mostly is in a form of a spammed mail but it can also be in the forms of spammed IM messages and fraudulent pop-up messages and web pages.

Phishing involves three components and those are:

- Authentic-looking sender
- Socially-engineered message
- Link to a fraudulent web page

The sender of the crafted message should look authentic in the eyes of the user. The content of the socially-engineered message is usually designed to confuse, upset or even excite the recipient. Typical topics involve to phishing include account problems, account verifications, security updates/upgrades, and new product/service offerings. Recipients of the message are prompted to react immediately. They then click on the link provided in the message body, which actually directs them to the phishing Web page. Below is an example of a phishing attempt.

Like the phishing e-mail, the phishing Web page almost always possesses the look and feel of the original—often containing the same company logos, graphics, writing style, fonts, layout, etc. This spoofed Web page may also include a graphical user interface (GUI) intended to lure the user into entering his/her bank account information, credit card number, Social Security number,

passwords or other sensitive information. All types of stolen information may then be used either by the phisher or sent to anonymous, remote users.

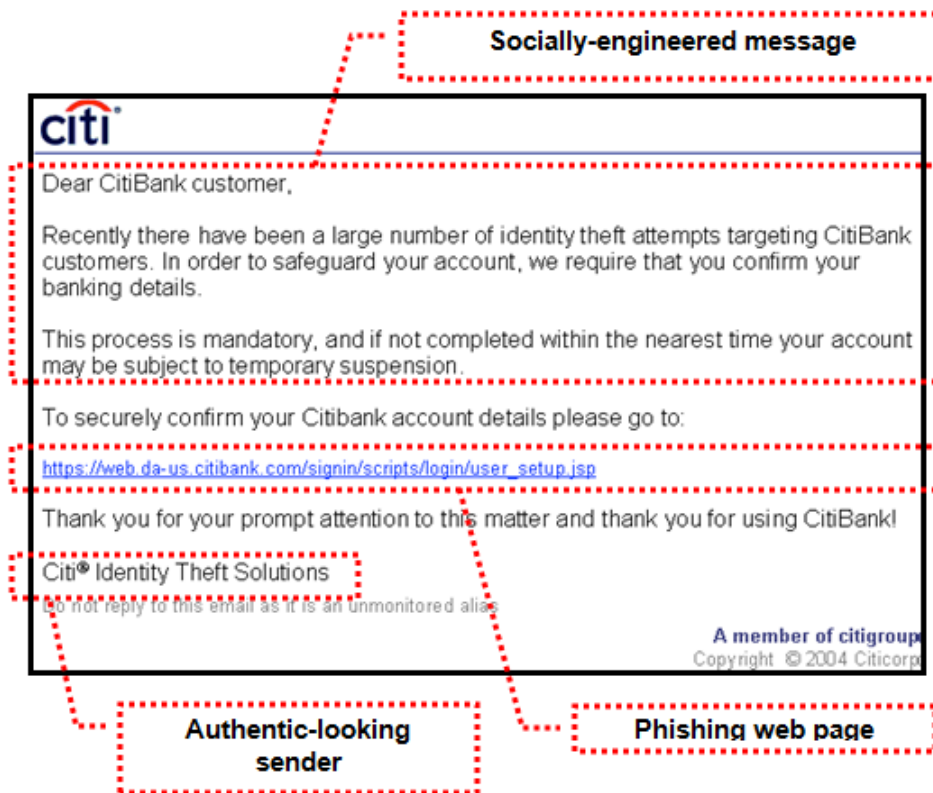


Figure 5-14: Examples of Phishing.

Recognizing Phishing Attack

To recognize a phishing attack, any one should be able to identify first if a message received is legit or not. Below is a suggested guideline to follow.

THE GREETING

Messages coming from a legitimate source will have information on who the directed recipient is and can address them directly (first and last name). Phishers do not have this information and must generalize their salutations to address the widest possible audience or using small pieces of information that are available (such as email domain or email address).

MESSAGE FORMATTING

A legitimate message should be free from simple grammatical and typographical errors, especially if the message originated from a professional institution (such as banks or credit card companies). Messages with such simple errors should be considered suspicious.

ALARMIST TONE

As discussed earlier, a phishing attack should contain a message that would prompt the recipient to react immediately, as if there is a situation that needs urgent attention.

“...This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it...”

Such immediate calls to action should always be considered suspicious. The alarmist tone is intended to scare the recipient into immediate action, without thinking.

FALSE LINK

Last but not the least is the presence of a hyperlink. The wording of the hyperlink may appear to be a valid link. However, the actual URL associated with the text will lead to the phishing web page. Getting the user to click on the disguised link is the entire purpose of the Phishing attack.

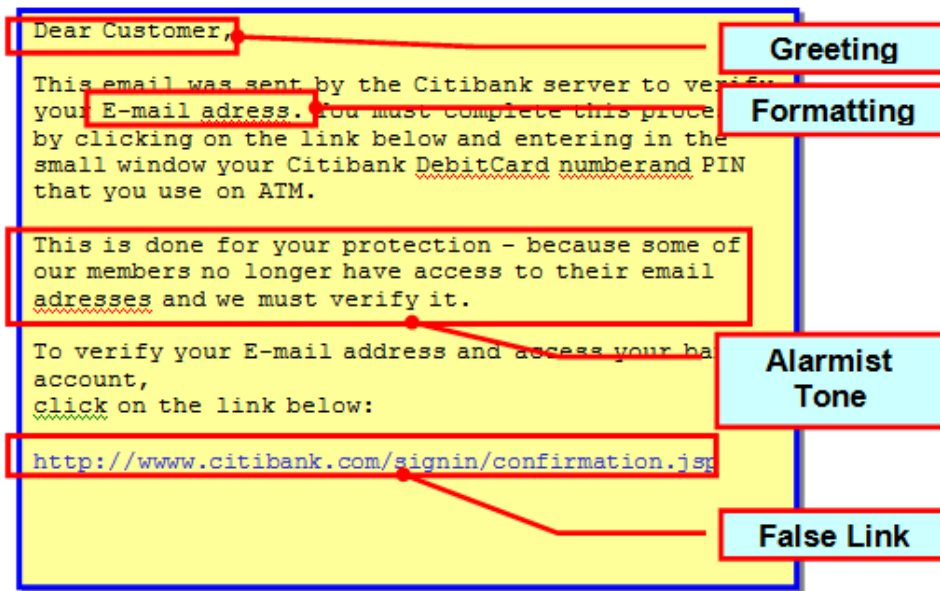


Figure 5-15: Phishing characteristics.

Phishing Techniques

EXPLICIT DISPLAY OF PHISHING URL

This is arguably the easiest technique to identify. In this case, phishers make no effort in hiding the actual phishing URL, and so the phishing URL is explicitly displayed on the address bar. In some cases, it involves the use of domain names that resemble legitimate domains.

ADDRESS BAR SPOOFING

This involves the alteration of the browser's address bar to display a legitimate address. The overall effect is that a text object with a white background hovers over the phishing URL to display a legitimate bank address. However, checking the properties window of the Web page reveals the real address of the spoofed site.

USING POP-UP WINDOWS

This technique uses a script that opens a legitimate Web site in the background. The spoofed pop-up window is usually identical to the legitimate Web site and is opened in the foreground. It misleads the user into thinking that the pop-up window is directly related to the official page. In some cases, the pop-up window only covers a portion of the legitimate Web site.

Using Forms within the Phishing E-mail



In this case, the Phishing e-mail arrives in HTML format. It already contains the embedded form that is used to gather personal/account information from users. Stolen details are usually sent to a specified e-mail address or are being posted to a particular Web site.

WEB SITE SPOOFING

This involves the laborious creation of exact replicas of legitimate, trusted sites. The spoofed Web site looks entirely like the real one, down to the last detail. All links visible in the spoofed site are under one phishing domain.

Phishing scams usually exploit certain browser vulnerabilities concerning URL redirections on unpatched machines.

Spy-Phishing

Spy-phishing is a targeted spyware attack that uses phishing techniques that, instead of leading the recipient to a phishing website, leads the user to unknowingly download a spyware (or even a Trojan spy) to the system. Once these malicious programs are executed they might hijack all the online banking activities of the recipient and steal any information they can get.

In *spy-phishing* the author seeds email messages with a Trojan file attachment, or a link to download a Trojan. When downloaded and executed, either manually or via an exploited vulnerability, this malware monitors web traffic until it detects web access to the target page. When this happens, it sends any login or confidential data back to the attacker. There have been different variants targeting specific entities or related web companies, all with the same objective. The text in the spammed email can be related to the target company, or it can employ other forms of social engineering, similar to those utilized for traditional viruses. In either case, the effect is more dangerous than traditional Phishing, since it does not have to rely on tricking the user into visiting a spoofed website.

Spy-phishing effectively starts with the authentic bank page when the user willingly logs in. And once the user enters his information, he proceeds to the intended site without interruption, so there is no unusual behavior that may alert him to a potential problem. The only difference is that the user's information has also been diverted to a third party.

Spear-Phishing

Spear-phishing is a targeted phishing attack. Unlike the regular phishing attacks that are being spammed around, this type of phishing attack doesn't use spamming method to attack its targeted victims. *Spear-phishing* attack is directed specifically and selectively to a small group of people who have somehow commonality among them like those people who are members of a high-profiled financial institution. This type of attack will attempt to seek unauthorized access to confidential data.

Like e-mail messages used in regular phishing attacks, *spear-phishing* messages appear to come from a trusted source. Regular phishing messages usually appear to come from a large and well-known institution or Web site like Paypal, eBay, CitiBank, etc. In the case of spear-phishing attack, the apparent source of the message would likely to be an individual within the recipient's own company who has a higher position or authority.

Here is a scenario of a spear-phishing attack: The attacker will look first for any necessary information regarding the targeted organization. Using available information to make the message seem authentic, the attacker creates an e-mail appearing to come from an individual who might reasonably request for confidential information, such as an IT department manager. The

attacker will then request user names and passwords or asks recipients to click on a link that will result in the user downloading malicious programs. Of course, the message uses social engineering techniques to convince the recipient. If a single employee falls for the attacker's ploy, the attacker can masquerade as that individual and gain access to sensitive data.

The Impact of Phishing Attacks

Stolen bank account information can be exploited in a variety of ways. After illegally accessing the victim's account, phishers can change account passwords, effectively locking the legitimate user out of his or her own account. They can then transfer available funds electronically to a temporary account and withdraw them before the victim becomes aware of it. Phishers may also write bogus checks on the account of the victim.

Harvested credit card credentials are used to make unauthorized online subscriptions or purchases. Victims would only know about it when they see their outrageous monthly bills or if they discover that their credit cards have been maxed out.

Stolen ATM account information, such as card numbers, PINs, and expiration dates may be used by phishers to create duplicate ATM cards. Phishers may then proceed to empty the corresponding ATM accounts.

Generally, all stolen information may be kept for future use and may also be traded or sold in online underground communities.

However, the overall impact of phishing attacks does not necessarily end with individual victims having their accounts emptied. One has to consider the fact that successful phishing attacks also result in a violation of privacy of the individual consumer, and an unauthorized use of the network identity of an enterprise.

Phishing may invariably taint the reputation and diminish the credibility of the companies that were used in phishing attacks. In business, the trade name is an important asset of each company, and it takes years of hard work to build a name that customers actually trust. Victims of phishing attacks may find it hard to transact business with companies that seemingly could not protect their assets and privacy. Customer trust is an asset that is difficult to measure, but losing it could certainly spell bad news for any business.

In the long run, the success of phishing attacks could influence more and more people to lose trust in the Internet as a means of doing business. This could impede the further growth and development of the Internet as a technological innovation that actually contributes to the improvement of life in general.

5.3.4 Pharming

Threats on the Web can take advantage of servers as users surf the 'net. *Pharming*, in particular, is designed by malicious hackers that take advantage of the vulnerabilities of technology while preying on user's behavior patterns.

What is Pharming?

Pharming is a way of redirecting users to malicious websites (or to phishing websites) through a technique called DNS cache poisoning. DNS cache poisoning is a new strategy in which malicious hackers use a DNS server they control to feed erroneous information to other DNS

servers. A *pharming* attack takes advantage of a vulnerable feature of DNS that allows any DNS server, which receives a request about the IP address of a Web domain, to return information about the address of other Web domains. For example, if a certain host sends a request about the IP address of Yahoo.com, a poisoned DNS server will return information about the IP address of Malware.com instead. This makes the user to be redirected to Malware.com website instead of going to Yahoo.com.

Internet users who rely on a poisoned DNS server to manage their Web surfing requests might find that entering the URL of a well-known Web site directs them to an unexpected or malicious Web page.

The Cousins: Pharming and Phishing

Like phishing, pharming aims to gather personal information from unsuspecting victim. The only difference is that pharming methodologies don't require a "lure" such as a Web link that victims should click on to be taken to the malicious Web site. Pharming doesn't rely on e-mail solicitation to ensnare its victims. Instead, its attack method essentially tinkers with the road maps that computers use to navigate the Web, such that large numbers of users can wind up giving personal data to a bogus site even if they've typed in a legitimate URL.

Pharming is technically harder to accomplish than phishing, but also sneakier because it can be done without any active mistake on the part of the victim. Documented pharming attacks are rare, but security experts say computer security organizations should be preparing defenses and educating users, by which many of whom are under the mistaken impression that as long as they avoid clicking on phishing e-mails, they're completely safe.

5.3.5 Man-In-The-Middle Attack

Hackers can grab data during transmission over the Web. What they do with that data can be highly destructive or malicious.

What is Man-In-The-Middle Attack?

A *Man-In-The-Middle* (or MITM) attack is a real-time attack on the network where the person or even the malware attacking attempts to intercept, read or alter information moving between two or more communicating computers. This kind of attack is a form of espionage that is taken place while the network is busy transmitting data whereby any information that are sent across the network shall be copied or intercepted first by the attacker which could either be a cyber criminal or a malware and then retransmit it again to the original destination.

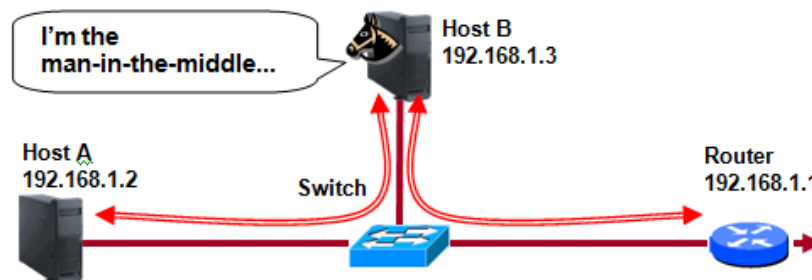


Figure 5-15: Man-In-The-Middle attacks intercept data.

Man-in-the-middle attacks can be achieved using the following methods:

1. The attacking machine would act as a DHCP server to redirect all network traffic through itself
2. The attacking machine would be intercepting all the traffic by poisoning the switch's ARP cache, which maps IP addresses to MAC addresses
3. The attacking machine would spoof target host IP address

5.3.6 Compromised Websites and Diseased Vectors

A website can be a source of threat to users, especially if not secured from the malice of hackers.

Definition of Compromised Website

A *compromised website* can be defined as a legit website which contains a threat on its web pages. The owners of these websites are not aware of these threats inside their web pages because a cyber criminal have placed the threat in there. The only problem with these websites is that they are not secured. Hackers are always capable of intruding into their systems and are able to edit the web pages inside. Once cyber criminals has hacked the website, they are now capable of adding some malicious code on the web pages. If internet users attempt to visit the site, most likely they would be redirected to a phishing site or even to a malicious website that would lead them to download malwares.

For example, www.citibank.com is a legit website but this link can be considered compromised: www.citibank.com/fun_stuff/payhere.html

Diseased Vectors (or Malicious Websites)

Diseased vectors are websites that host malicious programs. Once internet users accessed this type of websites, most likely, malwares will be downloaded to their system without them knowing it. Below are several ways how internet users may download malware files from diseased vectors.

- **Agent Download** – this type of malware downloading is being done by Trojan downloaders. Trojan downloaders are advance party Trojans that causes the multiple downloading of malware files from several diseased vectors.
- **Drive-By Download** – this type of malware downloading is the use of browser exploits to cause automatic downloading of malware files without the user noticing it. Compromised websites and diseased vectors often use exploits so that file download will be kept silent.
- **Drive-By Installation** – this type of malware downloading is often cause by untrusted applications that implements online installation by which one of the files included in the installation is malicious.
- **Freeware/Shareware Download** – this type of malware downloading uses social engineering techniques to encourage internet users to download malware files. Malware files being downloaded this way are in a form of legit applications such as tools, codecs, plugins, games, etc.

Browser Exploits


Browser exploits are exploits that attack browser vulnerabilities on handling and interpreting script codes. Exploit codes aim to redirect users to a compromised website, phishing site, or diseased vectors. Most exploits attack vulnerabilities that were found mostly on Internet Explorer. One of the most attacked vulnerability is the ability of the browser to handle HTML IFRAME tag.

5.3.7 Botnets

A robot performs automated tasks in accordance with its program. There are programs that act like robots, called *bots*, that can be used as a form of Web Threat to your security.

Bot Malwares

Bot is a term used to describe a script, a program or an application designed to perform predefined automated tasks. *Bots* are being used widely on the Internet for various purposes. *Bot* functionality may vary from search engines to game bots and IRC channel bots. Google *bot* is one such famous search *bot*, which crawls through the web pages on the net to collect information and build database to enable variety of searches. Computer controlled opponents and enemies in multiple player video games are also a kind of *bot*, where the computer process tries to emulate the human behavior. Nowadays, *bot* programs are also being used for malicious purposes. Malicious bots are called *bot malwares*.

NOTE  The term “bot” is derived from the term “robot.”

Bot malwares belong to blended threats type of malwares. Most of them are so-called IRC bots because they utilize IRC protocol to do malicious activities. They also belong to worm malware category since almost all bots can propagate. They are widely used to perform malicious activities such as information theft, denial-of-service attacks, backdooring, etc.

Bot malwares are designed to obey a set of commands being sent remotely to the affected machine to do its malicious acts. Once computers are infected by a bot malware then it would obey any commands that a cyber criminal may send thus remotely controlling the affected machines. Affected machines such as these are called *zombie* machines or simply *zombies*.

What is a Botnet?

Botnet is a network of zombie machines (being infected by bot malwares) that is under the control of cyber criminals. These zombies can be used by cyber criminals to launch attacks or to engage in various kinds of malicious activities. Zombies open backdoor ports and listen for commands issued by attackers. The most used medium for controlling botnets are IRC channels.

A botnet can contain thousands of zombie machines. Botnets can be used to launch major attacks to bring down target corporate networks. Internet users may be affected by bots on either by means of making their machines to become zombies or by experiencing the attack made by remote zombie machines. The following are popular malicious activities of botnets:

- **Distributed Denial of Service (DDoS Attack)** – DDoS attacks are the most common attacks performed by Botnets. The attack may be done by sending large ICMP packets or SYN packets to the targeted network, or just sending thousands of legitimate http, ftp requests to the site.

- **Phishing** – Bots are also effectively used for hosting phishing sites, making it extremely difficult for financial organizations to track such fraudulent sites. They can also be used to hack certain legit websites and compromised them to host phishing sites.
- **Spam** – Spam bots come along with an SMTP engine and they can send spammed mails on attacker's will.
- **Spreading of New Malware** – Botnets can also assist to make new malwares spread across the internet.
- **Hacking** – Botnets can also be used to find security holes on several websites. If a security hole is found then most likely it will be exploited by cyber criminals who control the involved botnets and attempt to have it compromised.
- **Adware Behavior** – Botnets can also issue pop-up messages to help promote certain advertisements.
- **Man-In-The-Middle Attacks** – Botnets can also initiate man-in-the-middle attacks to steal confidential information on larger networks.

5.4 > Defending Against Web Threats

There are some basics precautions that can be taken to protect you against web threats:

Keep antivirus software up-to-date – use security software which includes both antivirus and spyware protection for best results.

Keep operating system and applications up-to-date – Many web threats utilize wholes or vulnerabilities in operating systems and applications. Ensure that all security patches and updates have been installed to close these gaps.

Use Real-Time antivirus scanning – Real-Time AV scanning will catch the majority of threats as they attack your system.

Web Reputation Technology – Utilize software that uses real-time Web Reputation Technology to verify the legitimacy of websites.

Use a firewall – Ensure all unused ports and connections are closed to your computer.

Adjust browser security settings – Ensure your browser does not allow content to run automatically or in the background when visiting web pages.

Use safe browsing habits – Only download from trusted sources. Read license agreements and security warnings. Be wary of popup ads notifying you of infections.

Use anti-spam software – Anti-spam software can identify the majority of spam and phishing schemes.

Be wary of all messages with links or attachments – Even if you receive a message from a friend or relative, never blindly click on links or open attachments.



5.5 > Chapter 5 Summary and Review Questions

Summary

Web Threats are any threats that use the Internet to perform malicious activity, including data harvesting, redirecting users to malicious Websites, and installing malware or grayware.

Behind many Web Threats are the social engineering practices that hackers and people who run legal and illegal commercial operations from the data that they gather or steal from users. Social engineering is the overall process of attracting and luring people to do things for the fulfillment of malicious goals. Involved in Social engineering and the malware author are the following used to trick the user: a purported sender, the malware reference and the message content.

Social engineering techniques are plentiful. Generic conversations are conversational and friendly in nature, luring users to trust the author. Non-English Language Used, Mail Delivery Error, Physical Attraction, and Current Event content preys on the user's curiosity. Virus Alerts, Software Patch Required notices, Malware Found notices, Account Information, Accusatory take advantage of the user's fear or sense of responsibility. Free Stuff or Free Downloads address a user's sense of greed.

Spam is a Web Threat delivered through email and contains advertising for some product. It is delivered to large groups of users. Spam messages are typically sent with URL links to lure the user to a Website where Phishing may be conducted and personal data may be stolen from the user by many different criminal schemes. In today's threat landscape, Spam exists as email, usenet/newsgroup, Spam over Instant Messaging (SpIM), and mobile phone Spam.

Phishing and Pharming are two other forms of unpredictable Web threats. Phishing is a form of social engineering that leads users to provide personal information, such as credit card or account details, banking information, usernames and passwords. Pharming is a technique that redirects users to malicious Websites, through vulnerabilities in DNS cache poisoning, without the user's direct involvement. Pharming also aims to gather personal information.

Additional unpredictable Web threats include Man-in-the-Middle attacks, where data may be intercepted and copied or modified before being sent forward from the user to the destination. Another threat are compromised Websites, which involve insecure Websites that have been modified, often without the site owner's knowledge, and injecting malicious code to attack site users. Diseased vectors are Websites that host malicious programs. Browser exploits are an attack on a user's browser vulnerabilities. Bot malwares are a form of blended malware that are used to perform malicious activities.

Review Questions

1. How can a mail delivery error be a threat to a user?
 - a.) The message could contain malware attachments that cause problems if the user clicks on it.
 - b.) The message may be delayed.
 - c.) The error may actually be a Man-in-the-Middle attack.
 - d.) The email message automatically poses a threat.
2. What is the defining characteristic of an Account Information social engineering ploy?
 - a.) The user is asked to click on an attachment to view false account information.
 - b.) The user will not be able to identify the threat.
 - c.) The user is asked to click on a link that takes them to a site intended to get account information.
 - d.) The user downloads account software and infects the computer with malware.
3. What type of social engineering and malware design take advantage of a user's guilt?
 - a.) Accusatory
 - b.) Free Stuff
 - c.) Generic Conversations
 - d.) Virus Alert
4. What graphical technique is used to prevent spammers from attacking a Website and allow legitimate users access to information?
 - a.) Graphical User Interface (GUI)
 - b.) A captcha
 - c.) A browser plug-in
 - d.) Adware pop-up
5. What message characteristics indicate that you are the recipient of a Phishing attack? (Choose all that apply)
 - a.) Email address
 - b.) Greeting does not have a first and last name
 - c.) Typing errors in the messages from businesses
 - d.) Alarmist tone in the message



Chapter 6: Using Trend Micro Solutions

Chapter Objectives

After completing this chapter, you should be able to:

- Discuss the present Trend Micro solutions against current and emerging threats.
- Discuss free tools and services offered by Trend Micro that would provide immediate solutions against malware.



6.1 > Trend Micro Smart Protection Network (SPN)

Because conventional security solutions no longer adequately protect against the evolving set of Web threats, users need a new approach. Trend Micro delivers that approach with the *Trend Micro Smart Protection Network (SPN)*.

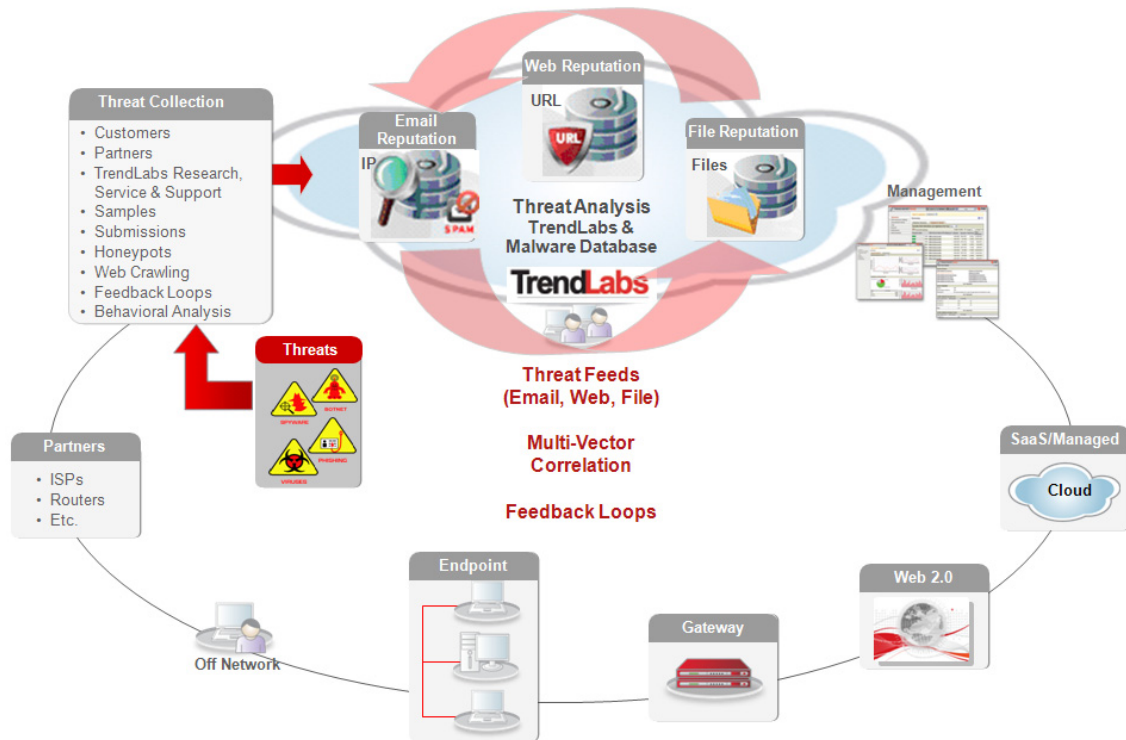


Figure 6-1: The Trend Micro Smart Protection Network (SPN).

6.1.1 What is Trend Micro SPN?

The *Trend Micro Smart Protection Network (SPN)* is composed of a global network of threat intelligence technologies and sensors that provide comprehensive protection against all types of threats—from malicious files, spam, phishing, and Web threats, to denial of service attacks, Web vulnerabilities, and even data loss. By incorporating in-the-cloud reputation, scanning, and correlation technologies, the *Trend Micro Smart Protection Network (SPN)* reduces reliance on conventional pattern file downloads and eliminates the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings.

The process in Figure 6-2, on the next page, is very straightforward. However, with the amount of malware being seen in the security industry, keeping up with the volume is a challenge. The question raised on the customer’s end, then, is “How many updates per day will be acceptable?” This is critical in light of the fact that not all computers will receive the update in time to protect them well, for many reasons. With this in mind, protecting individual devices and systems is important, but it is only a first step.

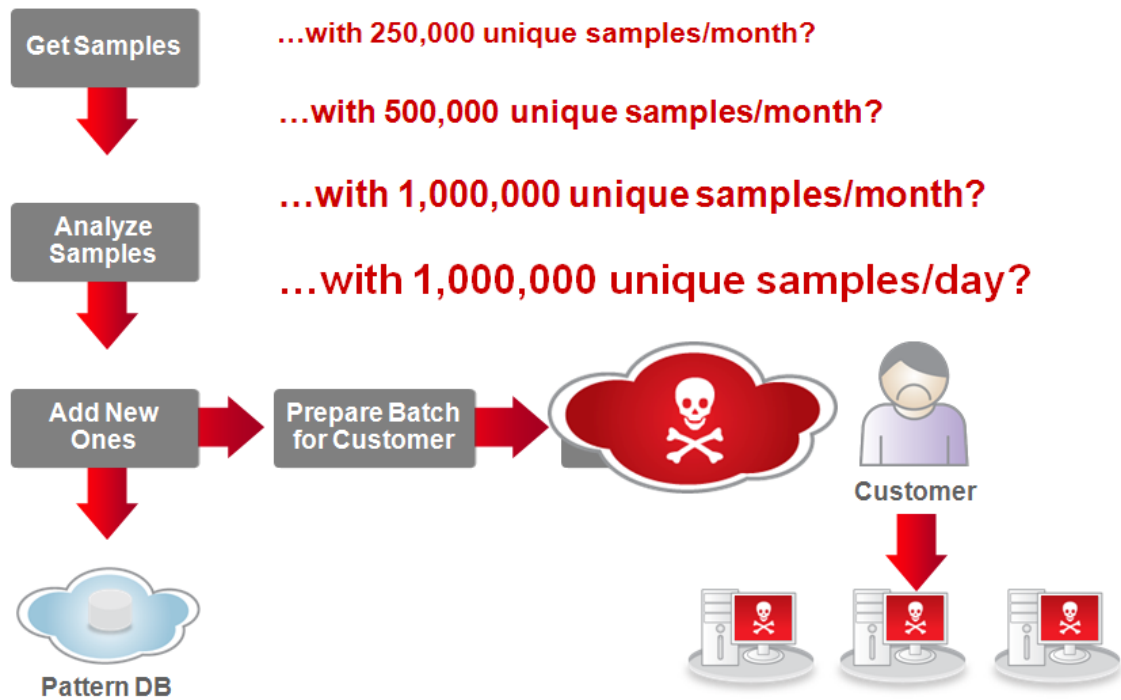


Figure 6-2: The pattern update challenge in security management.

The *Trend Micro Smart Protection Network (SPN)* is a next-generation cloud-client content security infrastructure that delivers security that is smarter than conventional approaches by blocking the latest threats before they reach a user's PC or a company's network. Leveraged across Trend Micro's solutions and services, the Trend Micro Smart Protection Network combines unique Internet-based—or "in-the-cloud"—technologies with lighter-weight clients. By checking URLs, emails, and files against continuously updated and correlated threat databases in the cloud, customers always have immediate access to the latest Trend Micro protection wherever they connect to the Internet.

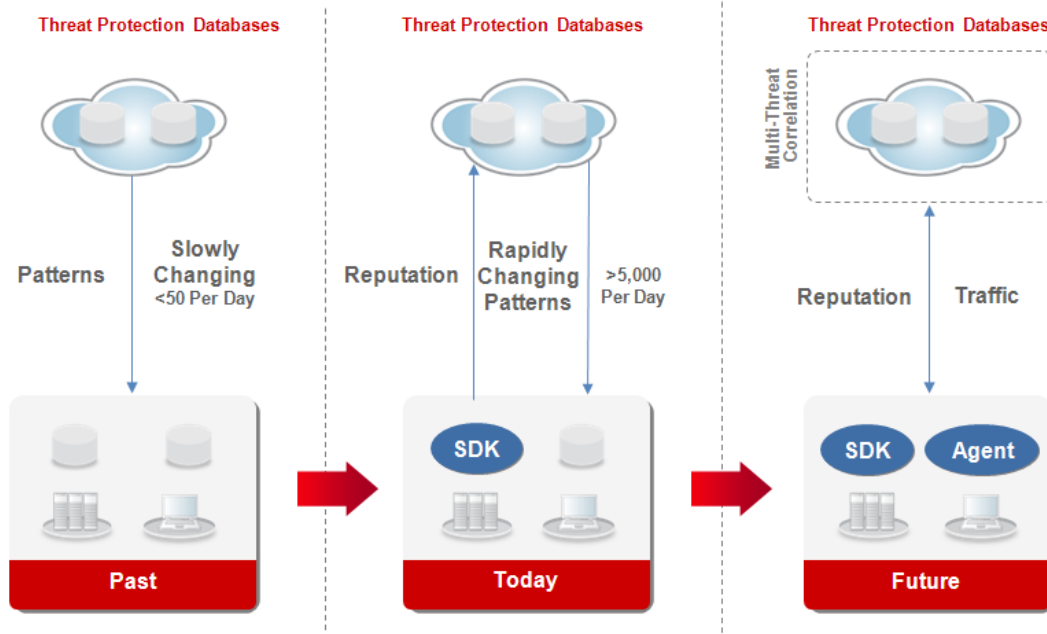


Figure 6-3: Content security moves into the Cloud to process quickly enough to keep up with the threat population.

By moving the largest portion of patterns or signatures into the cloud, it is possible to:

- Significantly reduce endpoint memory consumption
- Protect our customers in real time
- Reduce the need for pattern updates to our customers
- Reduce bandwidth consumption on corporate networks
- Increase awareness of threats affecting our customers
- Solve the pattern file download volume problem

The Trend Micro Smart Protection Network (SPN) is security made smarter for many reasons. Key characteristics of this innovative security solution model include:

<p>New Threats, New Defense</p>	<p>Extensive cloud-based threat protection network, correlated processing, immediate and automatic protection</p>
<p>Stronger, Faster Protection—Lighter on Your System Resources</p>	<p>Light-weight clients communicate with cloud-based threat protection network, reducing resource requirements on the endpoint</p>
<p>Anywhere, Anytime Security</p>	<p>Communication with cloud network upon each connection, always providing access to the latest protection, on network or off</p>
<p>Multi-Layered Protection</p>	<p>Threat protection across Web, messaging and endpoints in on-site or hosted solutions</p>
<p>Comprehensive Security</p>	<p>Protection against all types of threats—</p>



malicious files, spam, phishing, Web threats, DoS, Web vulnerabilities, data leakage

Better Together Security

“Neighborhood Watch” approach to security

Backed by Proven Content Security Leadership and Expertise

20 years of Internet content security leadership, 1,000 security experts worldwide, 24/7

The Trend Micro Secure Protection Network (SPN) incorporates a complete end-to-end security solution, based on the high level of threats and growing malware numbers, increased cyber crime, and expanding threat landscape. This model includes Protection, Enforcement, Review and Education, as shown in Figure 6-4 on the next page.

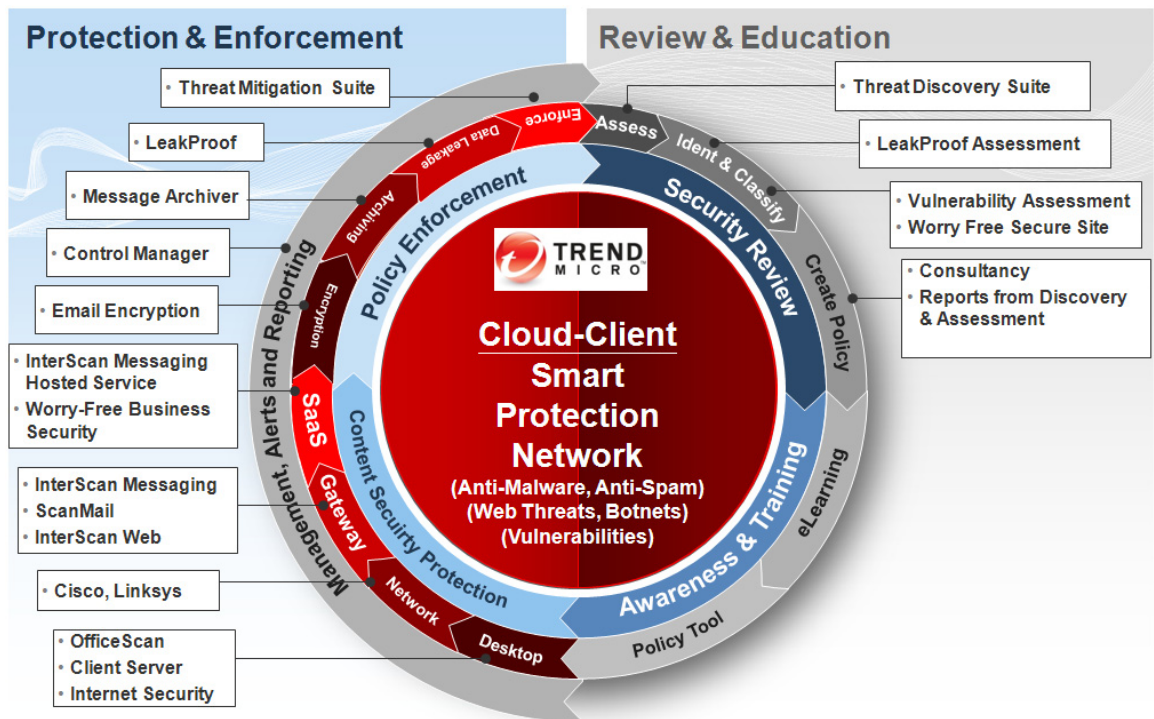


Figure 6-4: Trend Micro Smart Protection Network (SPN) with complete end-to-end security solutions.

The *Trend Micro Smart Protection Network (SPN)* is composed of the following components:

- Web reputation technology
- Email reputation technology
- File reputation technology
- Correlation technology with behavior analysis
- Feedback loops
- Threat intelligence (threat collection, threat analysis)

Web Reputation Technology

As a critical element of the Trend Micro Smart Protection Network (SPN), Web reputation technology guards against Web-based threats before they endanger a network or a user's PC. By assigning a relative reputation score to domains and individual pages within these domains, Web reputation technology weighs several factors, including:

- Web site's age
- Historical location changes
- Other factors that might indicate suspicious behavior

The technology then advances this assessment through malware behavior analysis, monitoring network traffic to identify any malware activity originating from a domain. Trend Micro Web reputation technology also performs Web site content crawling and scanning to complement this analysis with a block list of known bad or infected sites. Access to malicious Web pages is then blocked based on domain reputation ratings. To reduce false positives and increase accuracy, Trend Micro's Web reputation technology assigns reputations to specific pages or links, rather than an entire site, as sometimes only portions of a legitimate site are hacked.

Email Reputation Technology

As an additional layer of protection, email reputation technology can stop up to 80 percent of email-based threats, including emails with links to dangerous Web sites, before these threats reach the network or the user's PC. Email reputation technology validates IP addresses—or computer addresses—against both a reputation database of known spam sources and a dynamic service that can assess email sender reputation in real time. Reputation ratings are further refined through continuous analysis of the IP addresses' behavior, scope of activity, and prior history. Malicious emails are blocked in the cloud based on the reputation of the sender's IP address, preventing threats such as botnets from reaching the network or the user's PC. The reputation status is continually updated to ensure that a good reputation is restored when infected bots are cleaned, resuming delivery of legitimate email.

File Reputation Technology

The Trend Micro Smart Protection Network leverages file reputation technology, in addition to Web and email reputation technologies. Cyber criminals frequently move individual files with malicious content from one Web site to another to avoid detection, making file reputation checking a critical element to security in a Web 2.0 world. File reputation capabilities also address the fact that a reputation may not yet be assessed for a Web site that contains a malicious file. In addition, any file attached to an email is checked for malware. Malware in email attachments, if installed, can access the Web as an implementation mechanism. Files should also be checked on the Web itself. File reputation technology essentially checks the reputation of a file against an extensive database before permitting the user to download it. To accomplish this, a data crawl of each file hosted on a Web page or attached to an email, as well as an assessment of each file's reputation, is performed to continuously update a database of file reputation in real time.

Correlation Technology with Behavior Analysis

The Trend Micro Smart Protection Network uses "correlation technology" with behavioral analysis to correlate combinations of threat activities to determine if they are malicious. Although a single email or other component of a Web threat may appear innocuous, several activities used in conjunction can create a malicious result. So a holistic view—gained by examining the



relationship between and across the different components of a potential threat—is required to determine if a threat is actually present.

For example, a user may receive an email from a sender whose IP address has not yet been identified as that of a spam sender. The email includes a URL to a legitimate Web site that is not yet listed as malicious in a Web reputation database. By clicking on the URL, the user is unknowingly redirected to a malicious Web site hosting “information stealers” that are downloaded and installed on the user’s computer, gathering private information for criminal purposes.

Behavior analysis also correlates activities of a single session on the same protocol (e.g. an SMTP attachment with a suspicious double extension), as well as activities during multiple network connection sessions on the same protocol (e.g. a downloader blended threat in which individual files that each appear to be innocent are downloaded, but together form a malicious program). In addition, activities of multiple sessions and different protocols (e.g. SMTP and HTTP) are correlated to identify suspicious combinations of activities (e.g. an email with a URL link to several recipients and an HTTP executable file download from the linked Web page).

Information learned in the behavior analysis function at the gateway is looped back to provide the Web reputation technology and database with site-threat correlation data and to update the email reputation database of known bad IPs and domains. Similarly, information acquired at the endpoint is looped back to the file scanning capability at the gateway, network servers, and the Web reputation capability in the cloud. Both feed-through and loop-back techniques are needed to ensure real-time, Web threat protection across the entire network.

By correlating different threat components and continuously updating its threat databases, Trend Micro has the distinct advantage of responding in real time, providing immediate and automatic protection from email and Web threats.

Feedback Loops

Additionally, because Trend Micro solutions act as a single, cohesive security platform, built-in feedback loops provide continuous communication between Trend Micro products and Trend Micro’s threat research centers and technologies in a two-way update stream to ensure rapid and optimal protection against the latest threats.

Functioning like the “neighborhood watch” approach occurring in many communities, Trend Micro’s extensive global feedback loop system contributes to a comprehensive, up-to-date threat index that enables real-time detection and immediate, “smarter together” protection. Each new threat identified via a single customer’s routine reputation check, for example, automatically updates all Trend Micro’s threat databases around the world, blocking any subsequent customer encounters of a given threat. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, latency is not an issue, and the privacy of a customer’s personal or business information is always protected.

Threat Intelligence

Trend Micro supplements user feedback and submissions with internal research culled from researchers in the United States, the Philippines, Japan, France, Germany, and China. Multilingual staff members at TrendLabs—Trend Micro’s global network of research, service and support centers—respond in real time, providing 24/7 threat surveillance and attack prevention to detect, pre-empt, and eliminate attacks.

Using a combination of technologies and data collection methods—including Honey Pots, Web crawlers, customer and partner submissions, feedback loops, and TrendLabs threat research—Trend Micro proactively gains intelligence about the latest threats. This threat data is analyzed and correlated in real time via queries of Trend Micro’s malware knowledge databases in the Internet cloud and by TrendLabs research, service, and support centers.

6.1.2 A Multilayered Framework for Enterprise-Wide Protection

Keeping IT resources, data, and users secure is a complex proposition in today’s threat landscape, when an infection can quickly occur. While the antivirus vendor gets samples from sources, such as infected customers, HoneyPots, industry submissions, and crawling activities, it takes time to analyze the samples, add the samples to a master pattern database, and deploy the pattern in a batch update to the customer database. All this happens before your systems can be updated. That is why a multilayered framework with protection at many levels is important.

Trend Micro uses a multilayered framework, such as that in Figure 6-5. It contains solutions that span messaging, Web, endpoint, and network security.

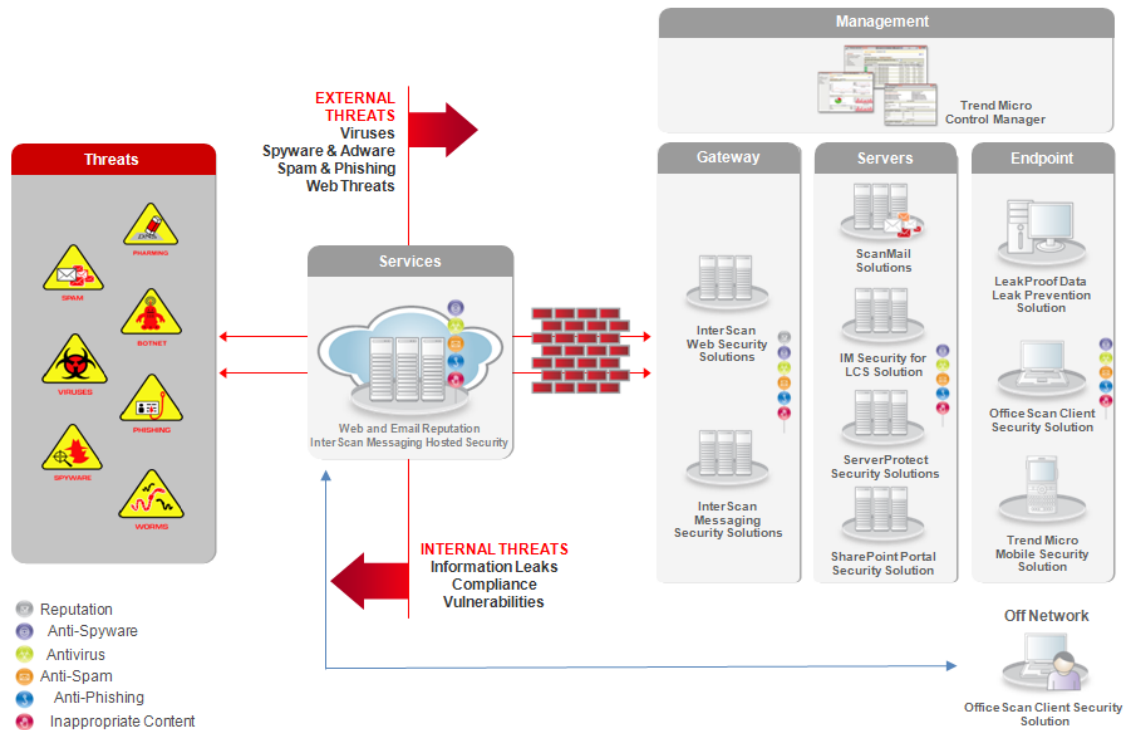


Figure 6-5: Trend Micro Multilayered Framework.

Messaging Security

Email is the backbone of a strong business. It is the main communications mechanism both within and outside of an organization. The high utilization and reliance upon email made it the perfect source for spreading malware. Traditionally, the majority of malware has been propagated via email.

Securing the content coming into and going out of an organization is a must. For this reason, Trend Micro provides a wealth of products focusing on securing messaging communications.



Comprehensive Messaging Security					ENTERPRISE	
	Anti-Spyware	Anti-Spam	Antivirus	Anti-Phishing	Content & URL Filtering	Security Compliance
InterScan™ Messaging Security Suite	✓	✓	✓	✓	✓	✓
InterScan Messaging Security Appliance	✓	✓	✓	✓	✓	✓
InterScan Messaging Hosted Security	✓	✓	✓	✓	✓	✓
Spam Prevention Solution		✓		✓		
Email Reputation Services		✓		✓		
ScanMail™ Suite for Exchange		✓	✓	✓	✓	✓
ScanMail™ Suite for Lotus™ Domino™		✓	✓	✓	✓	✓
IM Security			✓		✓	✓
PortalProtect™			✓			✓

Trend Micro Security

Figure 6-6: Trend Micro Comprehensive Messaging Security.

LAYERED SECURITY FOR MESSAGING AND COLLABORATION SYSTEMS

Secure your enterprise's messaging and collaboration tools with Trend Micro messaging security solutions. These proven products reduce the risks to business continuity, employee productivity and data security while minimizing impact on messaging systems and staff. Unlike vendors with point solutions, Trend Micro provides integrated layered protection across the full range of threats, communication methods, and network components.

ADVANTAGES OF TREND MICRO MESSAGING SECURITY

The advantages of Trend Micro Messaging Security are numerous, with the main advantages including the following:

- Delivers integrated and layered solutions for maximum coverage and security
- Based on proven Trend Micro threat engines
- Backed by TrendLabs global network
- Provides centralized management across entire network using Trend Micro Control Manager

Web Security

The Internet is a source of threats for many IT professionals, since a significant amount of malware tries to access your resources from various Web-related delivery vehicles. Trend Micro's Web Security solutions offer thorough protection from attacks at the gateway. The solutions from Trend Micro that integrate well into a multilayered framework include IWSS / IWSA, URL Filtering, and WebProtect, as described in Figure 6-7.

Comprehensive Web Security		ENTERPRISE				
	Anti-Spyware	Anti-Spam	Antivirus	Anti-Phishing	Content & URL Filtering	Security Compliance
InterScan™ Web Security Suite	✓	✓	✓	✓	✓	✓
InterScan Web Security Appliance	✓	✓	✓	✓	✓	✓
InterScan WebProtect for ISA	✓		✓			

Trend Micro Security

Figure 6-7: Trend Micro Comprehensive Web Security.

INDUSTRY-LEADING PROTECTION FOR THE INTERNET GATEWAY

Secure your enterprise's network by blocking attacks beginning at the Internet gateway with Trend Micro Web security solutions. Available as software or appliances, these solutions provide a first line of defense, blocking malware and inappropriate content at the point of entry. Centralized management simplifies deployment and maintenance. Lower your total cost of ownership with an integrated approach to threat-management.

ADVANTAGES OF TREND MICRO WEB SECURITY

There are many organizational and security advantages in using solutions from the Trend Micro Web Security lineup, including the following:

- Provides comprehensive protection against spyware and other Web-borne threats
- Offers automatic remediation for infected end-user PCs with Damage Cleanup Services
- Delivers latest anti-spyware and antivirus patterns from TrendLabs global network for optimal protection
- Provides centralized management across entire network using Trend Micro Control Manager
- Affords broadest choice of software and hardware solutions to match customer sizes and environments



Network Security

Networks are expensive to design and maintain, so you want to protect the network resources as much as possible from security threats. Trend Micro has Network Security solutions such as NVW and Network Content Inspection Technology (NCIT) to help you fight the threats of malicious behavior and destruction caused by malware.

PLUG-AND-PROTECT SECURITY POLICY ENFORCEMENT

Secure your enterprise network by screening and remediating infected users before they access your network with Trend Micro Network Security solutions. Trend Micro's flagship network access control (NAC) appliance provides agentless protection that is easy and cost-effective to deploy and manage. Seamless NAC flow integration lowers IT administration and costs.

ADVANTAGES OF TREND MICRO NETWORK SECURITY

Trend Micro addresses the security needs of the entire network through its solutions. The main Network Security advantages are:

- Provides granular and consistent security policy enforcement
- Scans managed and unmanaged devices—with or without an agent installed
- Deploys cleanup templates to noncompliant users automatically
- Uses highly effective vulnerability signatures to block worms and Bots
- Offer optional centralized management across entire network using Trend Micro Control Manager

Endpoint Security

The Trend Micro Multilayered Framework includes the Endpoint Security solutions that are aligned with the Messaging, Web and Network Security to complete the intra-product collaboration. The Endpoint Security, shown in Figure 6-8, illustrates the depth of endpoint protection.

Comprehensive Endpoint Security		ENTERPRISE				
	Anti-Spyware	Anti-Spam	Antivirus	Anti-Phishing	Content & URL Filtering	Security Compliance
OfficeScan	✓	✓	✓	✓	✓	✓
Anti-Spyware Enterprise Edition	✓		✓			
ServerProtect for Microsoft Windows / Novell NetWare	✓		✓			
ServerProtect for Network Appliance Filers	✓		✓		✓	✓
ServerProtect for EMC Celerra	✓		✓			
ServerProtect for Linux	✓		✓			
HouseCall Server Edition	✓		✓			
Mobile Security	✓	✓	✓			
Network VirusWall Enforcer	Provides network access control and protects against network worms					

Trend Micro Security

Figure 6-8: Trend Micro Comprehensive Endpoint Security.

COMPREHENSIVE THREAT PROTECTION FOR ALL ENDPOINTS

Secure your endpoints from external threats and network-bound threats with Trend Micro endpoint security solutions. Tailored to meet every type of endpoint security need, these solutions promote user and system productivity, and minimize the costs of interruptions to your end users and business. Trend Micro products are based on leading technologies and are tightly integrated with leading industry initiatives, ensuring mature, reliable solutions.

ADVANTAGES OF TREND MICRO ENDPOINT SECURITY

Trend Micro’s Comprehensive Endpoint Security simplifies security management through a highly-integrated approach, brings advantages that allow you to:

- Protect multiple server platforms and storage subsystems, client machines and mobile users from multiple threats
- Protect multiple server platforms and storage subsystems, client machines and mobile users from multiple threats
- Integrate with leading industry initiatives including Cisco’s Network Admission Control Program
- Reduce administration and security costs with simple deployment and consolidated solutions from a single vendor
- Provide centralized management across entire network using Trend Micro Control Manager



6.1.3 Multilayered Security

Secure your enterprise network with a fully integrated, centrally managed security suite. NetSuite Advanced protects your Internet gateway, mail and network servers, storage systems, desktops and laptops by blocking Web-based attacks, spyware, spam, blended threats, and other malware. It scales to meet the needs of your enterprise, offering extensive configuration options, maximum administrative efficiency, support for the broadest range of operating systems, and tight integration with Microsoft and Cisco technologies.

6.2 > Trend Micro Web Threat Protection Strategy

Web threats exist today and are growing in numbers and impact. Their complexity, large number of variants, and use of multiple vectors, combined with their exploitation of the most commonly used medium today, make Web threats the most challenging threat that enterprises, services providers, and consumers have faced in a long time. The cost of these threats assumes the form of confidential information leakage, with the consequent impact on brand reputation, regulatory and legal implications, and cost of loss of confidentiality to competitors. Because traditional approaches fail to protect against Web threats, the information security industry is at a crossroads. Businesses of all sizes, as well as service providers, need to deploy solutions via an integrated, multi-layered approach to provide adequate protection against these threats.

A multilayered approach is needed to protect against malware. This includes pattern matching as a baseline. This has advantages, such as low false positives, fast scanning, and the ability to provide proper cleanup. However, Trend Micro has stronger methods for protecting customers because a greater percentage of malware is being designed to avoid detection by pattern matching. This is why a more sophisticated approach to Web Threat protection is a must.

6.2.1 Integrated Multilayered Protection

The key to effectively addressing Web threats is a multi-layered approach. This can be accomplished by implementing measures at three different layers:

- “In-the-Cloud” (i.e., before the traffic reaches the Internet gateway)
- Internet gateway
- Endpoint (i.e., the client)

Web threats often use email as a medium to deliver an initial Web link. Hence, intercepting Web threats in-the-cloud reduces email traffic to the gateway, frees up bandwidth, consumes less processing power, requires less storage and archiving of emails and other information to comply with regulatory requirements, and hence, is more cost effective.

In-The-Cloud

At this level, the primary function is to check the “reputation” of each Web site before allowing user access. This is analogous to performing a “credit check” before consummating a financial transaction. A Web reputation check involves a URL filtering database; however, the addition of

approximately 5000 new domains per day means that additional measures are needed to complement this important element. These measures should include checking a database of “security ratings” that are developed based on a periodic data crawl of Web sites to check for malware, and a database of known phishing and pharming URLs. Cyber criminals often change the physical locations of IP addresses to evade detection; hence, an additional measure in-the-cloud should perform an IP location check in which IP locations are correlated with URLs. For maximum effectiveness, an analysis of all top level domains (i.e., the letters in a URL to the right of the last dot, including country codes) is also recommended.

Internet Gateway

Important functions are also needed at the second of the three levels, the Internet gateway. Performed via either software or a hardware appliance, gateway capabilities should include file checking. The file checking function essentially checks the reputation of each file before permitting the user to download it. To do this, a data crawl of each file at the Web site and an assessment of each file’s “reputation” are periodically performed to establish and maintain a database of file reputation. This file checking is needed; in addition to the function of Web reputation in-the-cloud, because cyber criminals can easily move individual files with malicious content from one Web site to another.

The second form of protection from Web threats needed at the gateway is some form of behavior analysis that can correlate combinations of activities to determine if they are malicious. This analysis can develop a score for each combination of activities and block the combination if the score exceeds a threshold level. This approach can also identify triggers, which are evidence or clues in session data or a protocol property that can be used to help identify suspicious activity. Further, this approach can implement rules, which are a correlation of triggers that match defined conditions of malicious activity, at the gateway.

This approach should correlate, for example, activities of a single session on the same protocol (e.g., an SMTP attachment with a suspicious double extension). The approach should also correlate activities during multiple network connection sessions on the same protocol (e.g., a downloader blended threats in which individual files that each appear to be innocent are downloaded, but together they form a malicious program). Activities of multiple sessions and different protocols (e.g., SMTP and HTTP) should even be correlated to identify suspicious combinations of activities (e.g., an email with a URL link to several recipients, and an HTTP executable file download from the link).

Endpoint

Despite implementation of these measures in-the-cloud and at the gateway, a third level of protection at the endpoint (i.e., the client) remains critical. Approximately two-thirds of recent U.S. computer retail sales are notebook computers. These machines require protection because they connect to multiple networks and visitors and contractors physically carry them past the company gateway; corporate Web security policy must be enforced whether the user is on or off the network. Therefore, a solution is needed that provides client-level prevention (e.g., access control and scanning), and in case of infection, cleaning, and recovery. So, for example, if a notebook computer has been compromised elsewhere and is part of a botnet, the notebook could attempt to connect back to the bot herder (the botnet originator). Another example is phone-home spyware, which periodically attempts to transfer information captured on the infected host back to the spyware owner. In either case, this activity can be detected and blocked, and a clean-up operation can be directed if needed.



Endpoint-based prevention should consist of URL filtering, Web site reputation capabilities, and use of a “restore point” for the machine that is saved prior to Web surfing. Using the latter, if the user detects any abnormal activity after downloading a file or browsing the Web, the machine could be returned to the restore point. Other prevention options should include establishing a “virtual environment” for the user to surf the Web; in this arrangement, Web threats reach only the virtual environment and do not penetrate the user’s actual environment.

Clean up capabilities should assume two forms: agent-based cleaning, and non-agent-based cleaning. Using agent-based cleaning, an agent that is centrally managed resides on the laptop computer, coordinating activities. Non-agent-based cleaning applies to the situation in which an agent is not installed on the notebook computer of a visitor or contractor; in this case, cleaning is accomplished on-demand with network access control (i.e., that allows limited access to the network to complete cleaning). Total recovery is also needed in cases when cleanup is not feasible due to a rootkit infection, for example.

6.3 > Trend Micro Free Tools and Services

Trend Micro offers commercial enterprise, small and medium business, and personal computer security products and services. Trend Micro also offers free tools and services, as described in this section.

6.3.1 Free AntiVirus Solutions

There are three antivirus solutions that you can download from Trend Micro. There is no charge to use them.

Emergency Repair Disk

Emergency Repair Disk (ERD) is a Trend Micro solution for boot infectors and viruses that infect on old systems such as DOS, Windows 9x, etc. This free tool is designed to run only on Windows 98 and older. Trend Micro is committed to combat all threats even those that run on old systems. For more information on ERD, you can visit this link:

<http://us.trendmicro.com/us/threats/home-user/preventing-intrusions/using-and-creating-a-rescue-disk/>

HouseCall

Trend Micro HouseCall is a free online virus scanner offered by Trend Micro, which checks whether your computer has been infected by viruses, spyware, or other malware. HouseCall performs additional security checks to identify and fix vulnerabilities to prevent reinfection. To access HouseCall, you can visit either of this links below:

http://housecall.trendmicro.com/?WT.TM_clusty_flg=7

http://www.trendsecure.com/security_solutions/housecall_free_scan.php#

Features include:

- Detects and removes malware
- Detects and removes grayware
- Restores damage caused by malware to affected system
- Notifies about vulnerabilities in installed programs and connected network services
- Multi-platform support for: Windows, Linux, Solaris
- Easy-to-use with the following browsers: Microsoft Internet Explorer, Mozilla Firefox

SysClean

Trend Micro SysClean is a free downloadable antivirus program that is used to scan for malwares and executes Trend Micro Damage Cleanup Templates (DCT) to restore the system. SysClean incorporates the Damage Cleanup Engine and Template. It replaces the traditional fix tool by addressing a wide variety of system infections rather than a specific malware infection.

This tool supports the following features:

- Terminate all malware instances in memory
- Remove malware registry entries
- Remove malware entries from system files
- Scan for and delete all malware copies in all local hard drives

To download SysClean, you can visit this link below:

<http://www.trendmicro.com/download/sysclean.asp>

6.3.2 System Diagnostic Tools

There are free system diagnostic tools available for download from Trend Micro. The tools and links are described herein.

Case Diagnostic Tool

The Trend Micro Case Diagnostic Tool (CDT) is a facilitating tool that helps the Trend Micro Service Engineering Group, Core Team, Technical Support Team, and customers in diagnosing problems in Trend Micro products. It aims to shorten the diagnostic communication process between Trend Micro and its customers.

CDT collects all necessary debugging information from a customer's product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories.

What does CDT do?

- CDT lets users provide detailed problem description
- CDT supports multiple product diagnostics
- CDT collects relevant system information from the customer's environment



- CDT turns product and specific module debug status on and off according to problem category without requiring user interaction
- CDT monitors specific process status information, such as CPU load and memory usage
- CDT automatically retrieves problem-related files and compresses them into a password-protected ZIP file (password is “trend”)
- CDT supports the following Windows platforms:
 - Windows 98 Second Edition
 - Windows 2000 Professional/Server Edition
 - Windows XP Professional Edition
 - Windows 2003 Server Edition

To download CDT, you can visit this link below:

<http://www.trendmicro.com/download/product.asp?productid=25>

System Information Collector Tool

The System Information Collector or SIC Tool is a program that collects critical information in a system which helps aid our TrendLabs Threat Researchers in isolating and identifying malicious objects in a suspected malicious system.

SIC Tool was developed to automate the collection of information that can pinpoint possible infections of unknown malware in the system. Currently, the AV Support Engineers correspond with customers via email, instructing the user where to look for the telltale signs of malware infections.

Since our customers do not wish to perform complex task and procedures, our engineers usually request for the system information and other details in small pieces through email instructions. They usually start with the operating system and the products installed, followed by the auto start entries in the registry, then the list of the running processes and services and so on and so forth.

Often times, the snapshot of the system via the list of executable files, product and system information, and registry entries are insufficient to identify the system infection. In these events, engineers usually request for the actual file samples from their systems and send the files to TrendLabs for analysis.

The whole diagnostic process is burdensome to engineers and the customers. Thus, a tool that can automate the gathering of this pertinent information was envisioned.

To download SIC tool, you can visit this link below:

<http://www.trendmicro.com/download/sic.asp>

HiJackThis

HijackThis is a free utility which quickly scans your Windows computer to find settings that may have been changed by spyware, malware or other unwanted programs. The program is notable for taking a heuristic approach on detecting malware. Rather than relying on a database of known spyware, it quickly scans a user's computer, creates a list of differences from a known spyware-free environment and allows the user to decide what are needed to remove.

HijackThis can generate a plain text log file detailing all entries it finds, and most entries can be removed or disabled by HijackThis. Caution should be exercised when using the latter option, as HijackThis does not discriminate between legitimate and unwanted items with the exception of a small whitelist of legitimate entries — thus allowing a user to unintentionally disable important programs from running, which may possibly cause their system or peripherals to stop working. HijackThis will, however, attempt to create backups of the files and registry entries it removes, which can be used to restore the system in the event of a mistake.

To download HijackThis, you can visit this link below:

http://www.trendsecure.com/portal/en-US/threat_analytics/hijackthis.php

Rootkit Buster

Trend Micro RootkitBuster is a rootkit scanner that offers ability to scan for hidden files, registry entries, processes, drivers and hooked system service. It also includes the cleaning capability for hidden files and registry entries.

To download Rootkit Buster, you can visit this link below:

<http://www.trendmicro.com/download/rbuster.asp>

CWShredder

Trend Micro CWShredder is the premier tool to find and remove traces of CoolWebSearch – the name for a wide range of insidious browser hijackers– from your PC.

CWShredder removes these browser hijackers. CoolWebSearch installs dozens of bookmarks– mostly to porn Web sites–on your desktop, changes your home page without asking, and continually changes it back if you attempt to correct it. Furthermore, it significantly slows down the performance of your PC, and introduces modifications which cause Microsoft Windows™ to freeze, crash or randomly reboot.

To download CWShredder, you can visit these links below:

<http://us.trendmicro.com/us/products/personal/CWShredder/>
http://www.intermute.com/spysubtract/cwshredder_download.html



TrendProtect

TrendProtect is a FREE browser plug-in that helps you avoid Web pages with unwanted content and hidden threats. TrendProtect rates the current page and pages listed in Google, MSN, and Yahoo search results. You can use the rating to decide if you want to visit or avoid a given Web page. To rate Web pages, TrendProtect refers to an extensive database that covers the following information for billions of Web pages:

- Content category
- Phishing scam detection
- Site reputation
- Page reputation

TrendProtect allows you to avoid sources of infection. If you inadvertently open a Web site rated unsafe by TrendProtect, scan your computer immediately.

To download Trend Protect, you can visit this link below:

http://www.trendsecure.com/portal/en-US/free_security_tools/trendprotect.php

Transaction Guard

Transaction Guard is free software that protects you against spyware while performing sensitive online tasks on a public computer, like Internet banking or other financial transactions.

Transaction Guard has two components:

Spyware Monitor	Monitors for spyware and notifies you of any intrusions
Password ClipBoard	An on-screen keyboard for securely entering user names and passwords

To download try Transaction Guard, you can visit this link below:

http://www.trendsecure.com/portal/en-US/free_security_tools/transaction_guard.php

6.3.3 Virus Encyclopedia

Trend Micro Virus Encyclopedia is a repository of information regarding malware threats. It contains relevant information for a particular malware threat that is found so useful by most people that does research on malwares. To access virus encyclopedia, you can visit this link below:

<http://www.trendmicro.com/vinfo/virusencyclo/default.asp>

There is only one entry per malware in the virus encyclopedia. And, each entry contains the following information about the malware.

Overview	Monitors for spyware and notifies you of any intrusions
Solution	An on-screen keyboard for securely entering user names and passwords
Technical Details	Contains detailed information about the malware behavior
Statistics	Contains a graph that shows the actual occurrence of malware infection globally

Below is an example of an entry in the virus encyclopedia:

WORM_NOOMY.A

Overview
Solution
Technical Details
Statistics

QUICK LINKS [Understanding New Pattern Format](#) | [Printer Friendly Page](#)

<p><u>Malware type</u>: Worm</p> <p><u>Aliases</u>: Email-Worm.Win32.VB.p (Kaspersky), W32/Generic.d (McAfee), W32.Noomy.A@mm (Symantec), Worm/VB.P.1 (Avira), Infection: W32/VB.KN (F-Prot), Mal/VBMail-B (Sophos),</p> <p><u>In the wild</u>: Yes</p> <p><u>Destructive</u>: No</p> <p><u>Language</u>: English</p> <p><u>Platform</u>: Windows 98, ME, NT, 2000, XP</p> <p><u>Encrypted</u>: No</p>	<p><u>Overall risk rating</u>: Low</p> <hr style="border: 0; border-top: 1px solid #ccc; margin: 5px 0;"/> <p><u>Reported infections</u>: Low</p> <p><u>Damage potential</u>: High</p> <p><u>Distribution potential</u>: High</p>
--	---

Description:

This mass-mailing worm propagates via email and Internet Relay Chat (IRC). It drops copies of itself using attractive file names in order to trick users into opening the email attachment or link.

Figure 6-10: Sample Virus Encyclopedia.



Aside from the virus encyclopedia, there is also a repository of information about other threats aside from malware threats. You can visit the following links for more information:

Spyware & Grayware	http://www.trendmicro.com/vinfo/grayware/default.asp
Joke Programs	http://www.trendmicro.com/vinfo/jokes/default.asp
Scams & Hoax	http://www.trendmicro.com/vinfo/hoaxes/default.asp
Security Advisories	http://www.trendmicro.com/vinfo/default.asp?sect=SA

6.4 > Chapter 6 Summary and Review Questions

Summary

The Trend Micro Smart Protection Network (SPN) uses in-the-cloud reputation, scanning, and correlation technologies as a global network of threat intelligence technologies and sensors to provide comprehensive protection against all types of Web threats—including malicious files, spam, phishing, and Web threats, to denial of service attacks, Web vulnerabilities, and even data loss.

Trend Micro solutions include Messaging Security, Web Security, End Point Security, and Network Security. Within the Trend Micro Smart Protection Network (SPN) model are several Trend Micro products, services, and management capabilities that enable you to maintain high levels of security against today's threats. These are all built on the TrendLabs foundation and years of proven security solutions and technologies that can fight threats in the current Threat Landscape.

Review Questions

1. Why does the Trend Micro Smart Protection Network (SPN) use in-the-cloud technologies for monitoring threats?
 - a.) That is where the threats are located
 - b.) Threats can be scanned more quickly there
 - c.) The technologies are developed for in-the-cloud locations
 - d.) It is faster to use Trend Micro's updated solutions in the cloud, than to perform the daily updates on a machine to protect against the new Web threats of the day
2. Which Trend Micro Smart Protection Network (SPN) technology performs a data crawl of each file hosted on a Web page to confirm the reputation of that page?
 - a.) File reputation technology
 - b.) Web reputation technology
 - c.) Email reputation technology
 - d.) Correlation technology
3. Which Trend Micro solution provides security with the following: anti-spyware, anti-Spam, antivirus, and anti-Phishing?
 - a.) HouseCall Server Edition
 - b.) Mobile Security
 - c.) OfficeScan
 - d.) Network VirusWall Enforcer



4. What characteristic of a web site is being checked when your security software checks the “In the Cloud” layer?
 - a.) Firewall settings
 - b.) Internet connection
 - c.) Website reputation
 - d.) URL validity

5. What does Trend Protect help you avoid? (Choose all that apply)
 - a.) Web pages with unwanted content*
 - b.) Web pages that require too much bandwidth
 - c.) Web pages with downloads
 - d.) Web pages with hidden threats



Appendix A: Answers to Review Questions

Chapter 1

No questions.

Chapter 2

1. What aspect of the threat landscape is most related to infrastructure vulnerabilities?
 - a.) Rogue anti-spyware
 - b.) Security holes in software
 - c.) Online gaming
 - d.) Phishing

2. What do malware authors use when they deploy codes that specifically target victims and lure them to malicious websites? (Choose all that apply)
 - a.) Viruses.
 - b.) Rogue anti-spyware
 - c.) Social engineering
 - d.) Phishing

3. Which are forms of content-based threats?
 - a.) Spam
 - b.) File infector families
 - c.) Phishing
 - d.) Worms

4. Which threats are on the increase? (Choose all that apply)
 - a.) Image Spam
 - b.) Timely subject headings
 - c.) Enhanced attachments



- d.) Rogue anti-spyware
5. What is one difficulty in defining the extent of botnet threats in the threat landscape?
- a.) Botnet applications are untraceable
 - b.) Botnets are inherently difficult to identify
 - c.) Talented IT professionals in countries with organized crime develop botnets
 - d.) Many users are unaware that their system has been compromised

Chapter 3

1. Which traits do all malware – viruses, worms and tojans share in common? (Choose all that apply.)
- a.) They originate from outside the network.
 - b.) They use or damage computer resources.
 - c.) They enter computer systems, usually without the user's knowledge or intent.
 - d.) They release hidden payloads designed to damage hard drives and corrupt data files
2. What is the defining characteristic of Trojan horse programs?
- a.) They appear to be harmless but hide malicious intent.
 - b.) They are not intended to cause harm and only make fun of the user.
 - c.) They replicate and attach themselves to host files.
 - d.) They do not require user intervention to spread or function.
3. Why are worms described as “self-contained?”
- a.) Worms do not replicate.
 - b.) Worms do not spread to other computer systems.
 - c.) Worms do not require a host file to spread.
 - d.) Worms do not carry payloads.
4. How does a mass mailing worm spread? (Choose all that apply.)
- a.) Create a copy of itself in a directory
 - b.) Create a registry entry
 - c.) Get email addresses
 - d.) Executes a program



5. How are damages arising from computer threats categorized?
 - a.) Lost productivity, recovery and cleanup costs, lost data, and damaged reputations
 - b.) Lost productivity, increased vulnerability to future virus attacks, loss of confidential data, loss of other data
 - c.) Network downtime, decreased availability of computer resources, disk damage, and problems in virus isolation
 - d.) Network disconnection, increased errors in the network, and damaged reputation due to loss of customer data

Chapter 4

1. Which form of grayware has infected your computer if your keystroke data is logged?
 - a.) Adware
 - b.) Browser Helper Object
 - c.) Keylogger
 - d.) Trackware
2. Which form of grayware is used to crack software copyright protection keys?
 - a.) Browser Helper Object
 - b.) Keylogger
 - c.) Keygen
 - d.) Spyware
3. Which form of grayware tries to tempt users to use create a connection to the Internet using a telephone line and connection fee?
 - a.) Spyware
 - b.) Dialer
 - c.) Hacking Tool
 - d.) Joke Program
4. Which computer behavior would make you suspect that you might be installing grayware? (Choose all that apply.)
 - a.) Additional programs are also being installed at the time of installation
 - b.) ActiveX is being used as an installer
 - c.) A Browser Helper Object (BHO) plug-in gets installed on the browser
 - d.) The browser security settings remain the same

5. Which computer behavior would make you suspect that you are running grayware on a machine without your consent? (Choose all that apply)
- a.) Advertising banners are displayed
 - b.) The computer performs an auto-restart
 - c.) The system becomes unstable
 - d.) The computer disconnects from the Internet

Chapter 5

1. How can a mail delivery error be a threat to a user?
- a.) The message could contain malware attachments that cause problems if the user clicks on it.
 - b.) The message may be delayed.
 - c.) The error may actually be a Man-in-the-Middle attack.
 - d.) The email message automatically poses a threat.
2. What is the defining characteristic of an Account Information social engineering ploy?
- a.) The user is asked to click on an attachment to view false account information.
 - b.) The user will not be able to identify the threat.
 - c.) The user is asked to click on a link that takes them to a site intended to get account information.
 - d.) The user downloads account software and infects the computer with malware.
3. What type of social engineering and malware design take advantage of a user's guilt?
- a.) Accusatory
 - b.) Free Stuff
 - c.) Generic Conversations
 - d.) Virus Alert
4. What graphical technique is used to prevent spammers from attacking a Website and allow legitimate users access to information?
- a.) Graphical User Interface (GUI)
 - b.) A captcha
 - c.) A browser plug-in
 - d.) Adware pop-up



5. What message characteristics indicate that you are the recipient of a Phishing attack? (Choose all that apply)
- a.) Email address
 - b.) Greeting does not have a first and last name
 - c.) Typing errors in the messages from businesses
 - d.) Alarmist tone in the message

Chapter 6

1. Why does the Trend Micro Smart Protection Network (SPN) use in-the-cloud technologies for monitoring threats?
- a.) That is where the threats are located
 - b.) Threats can be scanned more quickly there
 - c.) The technologies are developed for in-the-cloud locations
 - d.) It is faster to use Trend Micro's updated solutions in the cloud, than to perform the daily updates on a machine to protect against the new Web threats of the day
2. Which Trend Micro Smart Protection Network (SPN) technology performs a data crawl of each file hosted on a Web page to confirm the reputation of that page?
- a.) File reputation technology
 - b.) Web reputation technology
 - c.) Email reputation technology
 - d.) Correlation technology
3. Which Trend Micro solution provides security with the following: anti-spyware, anti-Spam, antivirus, and anti-Phishing?
- a.) HouseCall Server Edition
 - b.) Mobile Security
 - c.) OfficeScan
 - d.) Network VirusWall Enforcer
4. What characteristic of a web site is being checked when your security software checks the "In the Cloud" layer?
- a.) Firewall settings
 - b.) Internet connection
 - c.) Website reputation
 - d.) URL validity



5. What does Trend Protect help you avoid? (Choose all that apply)
- a.) Web pages with unwanted content
 - b.) Web pages that require too much bandwidth
 - c.) Web pages with downloads
 - d.) Web pages with hidden threats

