**Information Technology Security Report**
**Lead Agency Publication R2-002**

# Future Trends in Malicious Code - 2006 Report

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: August 2006

# Disclaimer of Responsibility

This publication was prepared by the RCMP for the use of the federal government. The publication is informal and limited in scope. It is not an assessment or evaluation, and does not represent an endorsement of any sort by the RCMP. The material in it reflects the RCMP's best judgment, in light of the information available to it at the time of preparation. Any use which a third party makes of this publication, or any reliance on or decisions made based on it, are the responsibility of such third parties. The RCMP accepts no responsibility for damages, if any, by any third party as a result of decisions or actions based on this publication.

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Malicious code (malware) is a major threat to information systems around the world. As malware evolves at a tremendous pace, remaining current in this field can be very difficult. The purpose of this document is to outline the future trends of malicious code that researchers and experts believe will affect the global information infrastructure in the coming year. The document also addresses some of the current features of malicious programs found circulating around the world. Today, malware is changing more rapidly, it has become modular in design and propagates using new and novel methods. As well, the primary goal of malware has shifted in recent years. More and more the trend is for malicious code to be written to turn a profit for its creators.

Malware development is expected to continuously evolve and demonstrate new ways to exploit, infect and victimize computer systems. Many of the trends covered in this document address new ways malware can be utilized for monetary gain. This includes everything from selling malicious codes to criminals on the black market to renting the use of victimized systems. Some malware authors are making use of new technologies such as rootkits to hide their viruses, while others are making malware easier to create by releasing their source code under the GNU Public Licence (GPL) as open source software. Worms and viruses are also becoming more prevalent on other platforms such as, but not limited to: cell phones, PDAs, USB memory sticks and even Radio Frequency Identifier (RFID) chips.

With malware development becoming progressively more organized and well-funded by criminal organizations it is becoming more difficult to track and predict. Ongoing research and diligence will be required to better understand these threats and this document will serve as a good starting point. In the meantime, malicious code continues to prey on those systems with the weakest defences. Anti-virus and firewall programs should be installed and kept up to date; users should exercise constant diligence when online. Finally, advisories from vendors and government centers such as the Canadian Cyber Incident Response Center (CCIRC) need to be heeded.

# 1 Introduction

Malicious code has been generally accepted as one of the top security threats to computer systems around the globe for several years now.[1]

Due to direct, or indirect, connections to the public Internet, Government computer systems can be vulnerable to a variety of different threats known as malicious code or otherwise referred to as 'malware'. The consequences of an IT security incident caused by malware can vary by degree of impact from 'low' to 'high'. It is in the best interest of all federal government departments to practice 'due diligence' to prevent malware from affecting the confidentiality, integrity and availability of services they provide and/or the data they protect.

Until recently, the vast majority of attacks systems faced from the Internet were highly automated and non-directed. Although government systems may have been the target of directed attacks, they were still more likely to face indiscriminate probing from other infected systems. However, the malicious code landscape is changing. Attacks are becoming more specialized by combining social engineering with other methods to get past defences. Attacks are also becoming more directed; systems storing sensitive data are highly prized.

One of the primary reasons malicious code remains such a threat is the speed at which it moves and changes. As well, we are now seeing new innovation as malicious code moves away from being a way to disrupt systems and communications. Today, it is a 'crime-enabler' for spammers, hackers and organized criminals. These 'tools' enhance the capabilities of such individuals to generate millions of dollars in illicit profit.

# 2 Purpose

This report will provide an overview of the numerous malicious code trends experts are observing and those they predict will be seen in the foreseeable future.[2] This is not a document that will chart the future of malicious code as that would be impossible. Malware writers move very quickly. They are adaptable and very often they are exploiting vulnerabilities before the rest of the security industry is fully aware of them.[3] Their flexibility and reaction speed is essential if they wish to continue to make a profit and stay ahead of the anti-virus companies who are constantly devising new ways to detect and remove hostile code.[4] As a result, some of the trends covered in this document may never fully evolve and others that have not been mentioned will, no doubt, appear.

This document will give readers a better sense of what is coming "down the pipe" and perhaps, a better idea of what to look for when dealing with tomorrow's malicious code.

# 3 Current Malware Features

## 3.1 Malware - A New Purpose

In the last few years malicious code has undergone a key transformation. For the most part, gone are the days when viruses and worms were designed with payloads that only destroyed data, crashed the system or cut off communications. Although malware that is destructive continues to be very common, there has been a noticeable rise in the number of malicious codes not carrying a destructive payload. There is clearly an increasing interest in keeping the victim's system online and operational.[5] More and more the trend is for malicious code to be written to turn a profit.[6]

Today, malicious code goes about making a profit in several different ways. One of the most common methods is by stealing sensitive information which is then sold on the black market to criminal organizations. Information such as credit card and social insurance numbers, usernames and passwords and other sensitive files stored on hard drives are stolen and readily monetized.[7] The financial industry is one of the most heavily targeted. Not surprisingly Trojan horse programs that specifically target usernames and passwords for banking Web sites have experienced increased growth in the last couple of years.[8] Another common approach, using bot programs, is to force the victim's system to join a botnet. Botnets being monitored by anti-virus companies and law enforcement are said to often comprise upwards of 30,000 to 40,000 systems. (One of the largest botnets ever discovered was said to have been controlling 100,000 zombie systems.)[9] These networks of systems can be used to launch Distributed Denial of Service (DDoS) attacks, host illegal material and send spam.

Over the last few years, malicious code has shown it is very well suited to making money for the criminal entrepreneur.[10] The money-making aspect of malware is a feature that is here to stay.

## 3.2 Decline of the Epidemic

Worm epidemics have been the scourge of the Internet for years. It started with the Morris worm in 1988 and continued later with Melissa, I LOVE YOU and many others. However, in the last year or two there has been a marked decline in these outbreaks. This can likely be explained by increased security in operating systems and advances in anti-virus technology.[11] At the same time, malware has also changed due to a shift in social dynamics. Many pieces of malicious code released onto the Internet today are directed at only a few targets. This means the attacker can craft the malware to use more sophisticated social engineering tricks to dupe users. This has become necessary as users learn to ignore unsolicited E-mails and messages.[12] Targeting fewer victims also means anti-virus companies will not see the code as soon as they would if the program was disseminated across the Internet.[13] This increases the window of opportunity for the malware author before anti-virus companies update their detection signatures.

## 3.3 Malware Development Time

As the Internet world has sped up in the past few years, so it would seem, has the malicious code. When vulnerabilities are publicly announced it becomes a race between malicious code writers and software vendors. Malware authors are getting very good at producing exploit code before the company produces a patch.

When the Nimda worm was discovered in September 2001, the vulnerability it exploited had been publicly known for 366 days. Microsoft had made a patch available in October 2000. Administrators had close to a year to patch the security hole. Four years later the Zotob worm was discovered in the wild. The vulnerability Zotob exploited had been public knowledge for only four days.[14]

With the development time required to produce exploit code for publicly disclosed vulnerabilities plummeting over the years, the window of opportunity to exploit vulnerable systems has expanded. Although the time to exploit has risen recently (6.4 days on average) it is still very low in comparison to the average 49 days it takes vendors to release patches for publicly disclosed vulnerabilities.[15]

## 3.4 Malware Types & Propagation Vectors

Several other changes have taken place in the world of malicious code. In recent years, the 'classic' virus category of malicious code has seen a marked decline.[16] This is due to the fact that many viruses, to date, have typically spread slowly and/or carried a destructive payload. Today's exploit-based worms, Trojans and bots move much faster and provide the functionality required to turn a profit.

Propagation vectors have changed recently as well. Worms propagating through the Peer-To-Peer (P2P) file sharing networks have dropped substantially in the last couple of years. The primary reason for this drop has been attributed to the efforts of organizations, such as those responsible for protecting copyright materials, in the movie and music industries. In their place have come worms and malicious code propagating over instant messaging (IM) networks. In 2004 Kaspersky Labs witnessed an average of one new IM worm per month. In 2005, the average jumped to twenty-eight per month.[17] This activity is expected to increase as instant messages are expected to overtake E-mail traffic sometime in 2006. Some IM worms can send messages to every person on a user's contact list. Other worms are capable of "chatting" with victims, enticing them to click on a malicious link. The fact most individuals inherently trust those on their contact list only makes attacks over IM more effective.[18]

### 3.5 Modularity of Malware

Malware was once solely the domain of skilled coders. They were capable of building a program from scratch, understanding the programming languages as well as the networking and system concepts needed to create a working malicious code. As time progressed, instructions and tutorials became more common and those who needed some help could acquire it.[19]

Now, it seems, the era of modular malware and virus 'kits' has arrived. 'Modular' malware is often defined in two different ways. First, some malware is modular when written. Today, the components and payloads for a malicious program are available in modules which are easily swapped in or out. Thus, many variations of functions and payloads are readily available. As was pointed out in one paper, "(If you) want it to have P2P propagation capability, add it, want it to disseminate (the malware) over IM, done."[20] Now malware creation has reached the stage where someone can point and click their way to a new worm. Malware kits even provide the user with a Windows interface and check boxes to include or exclude different payloads or propagation methods.[21] The second type of modular malware makes use of 'modularity' to enhance functionality once a system is compromised. For example, the malware can be coded to remain small (< 50kb), stealthy and highly mobile. The goal is simply to establish a foothold on the system.[22] From there the worm or Trojan will contact servers on the Internet to download modules of code in order to acquire increased functionality. Many bots are hard-coded with the instructions to log into Internet Relay Chat (IRC) channels and await instructions. This is a very efficient method for adding functionality since the 'owner' of the botnet can centrally issue commands instructing all listening bots to download specific modules. The downloaded code can include updates to the malware itself, keystroke loggers, proxy servers, adware, spyware and any other 'crimeware' capable of helping turn an illegal profit.[23]

## 4 Future Trends

### 4.1 Cell Phones & Mobile Devices

Malware authors are constantly looking for new and vulnerable targets to exploit - especially now that malicious code has been monetized. Mobile device malware has been an increasing threat in the last few years. It is believed that there are upwards of one hundred variants of malicious code that exploit mobile devices such as cell phones and PDA's already in circulation.[24] These variants have been responsible for damaging mobile devices, deleting data, compromising sensitive information and now there are variants that are capable of jumping from mobile devices to Windows desktop systems.[25]

As cell phone providers add Internet gateways and other services for improved performance and functionality,[26] interest in the devices increases. However, the major upswing is expected to come as mobile device users gain access to online banking and payment services from their cell phones. This will, without a doubt, cause an increase in interest from the criminal element. This new threat will only be compounded by the general lack of security awareness and the penchant users have for accepting unsolicited incoming messages.[27]

## 4.2 Portable Media

Although this is not explicitly a malicious code issue, it is certainly a security issue; one which malicious code may exploit in the future. Portable media devices, such as USB jump drives and memory sticks / chips, have been around for several years. They have evolved to the point where they can hold substantial amounts of data and are extremely easy to conceal and install. The threat here is modeled on what is known as "Pod-Slurping".[28] This is the idea of using an iPod music device to copy files off a computer and then leave the area with a device most people think only carries music. Malware could exploit this vulnerability in two ways.

First, it could learn to piggyback into an organization. Infecting a portable drive at a user's home,[29] the malware would hide and let the user unwittingly carry it past the external access controls of a company. From there the worm would be free to attack the computing infrastructure from the inside where there is often less protection. Of note here is that this would be a way that malicious code would be able to penetrate a network that was considered highly secure. Using the idea of "180-degree hacking"[30], a concept presented at the Black Hat USA 2002 conference, the code would probe for ways back out of the network so as to phone home and begin stealing sensitive data.

Perhaps more insidious would be the second possibility. The same scenario would play itself out except the user would knowingly bring the malicious code into the office on their portable media. Having created the malicious code personally, (something that is incredibly easy to do today) the malicious user could then release it onto the internal network. The user could spread the "infection" themselves by physically accessing multiple systems or they could program the malware to spread quietly across the network, ensuring that it did not go beyond the borders of the corporate LAN. Once installed on multiple systems, the disgruntled employee would simply wait for the code to send the sensitive files back to the portable media device. When the theft was complete, the worm could then delete itself and the employee could leave the company with a device on their key chain which people could mistake for a pocket-sized highlighter instead of a storage container holding an untold number of sensitive files.

## 4.3 Rootkit Technologies

It makes sense that the longer a piece of malware can remain undetected on a victim system the more effective it will be (or in today's case the more money it will make).[31] It should come as no surprise the number of rootkits detected on compromised systems has been increasing of late. This is a disturbing trend as rootkits can be very difficult to detect, and can be used to hide other types of malware. Anti-virus companies have already begun to point out that they see rootkits as a credible future threat.[32]

Perhaps more disturbing have been the recent findings by researchers in the field. Experts and university students alike have found and developed new rootkit technologies that will further increase the difficulty of detecting malware. Microsoft and students at the University of Michigan succeeded in creating a proof of concept virtual machine rootkit that is capable of operating outside the boundaries of the operating system. The rootkit creates a separate layer, a virtual machine monitor (VMM), between the hardware and the operating system. When the system boots, the BIOS hands control of the computer to the VMM, thereby subverting the normal boot process. Once the boot process is complete all interaction between the user and the computer is done via the VMM.[33]

Shortly before this research came to light, a presentation at the Black Hat Conference introduced the concept of hiding rootkits in the Basic Input Output System (BIOS) of a computer. Although there have been relatively few malicious codes that attempt to modify the BIOS, the threat is considered credible because access to the programming language (ACPI), compilers and instructions is trivial. Other researchers at the conference disagreed on how likely it was that an automated piece of malware could spread such a rootkit due to computer hardware security mechanisms. Nevertheless it would certainly be a plausible threat were an insider to install the rootkit themselves. If the rootkit were installed on a laptop, for example, it could be used as a backdoor into the organization long after the user was no longer using the system. Such a rootkit would be capable of surviving hard drive reformats and replacements, making this a very hardy piece of malware.[34]

## 4.4 DDoS on Demand

For years criminals have made use of extortion as a way to intimidate others and make money. In the last couple of years computer criminals have honed their abilities to extort large sums of money from online companies in return for the "protection" of their Web sites. Generally an E-mail will arrive informing the company that they must pay protection money or face a distributed denial of service attack that will knock their Web site offline. With the size of botnets today many of these threats are very credible.
Although denial of service attacks have existed for years, it has only been in the last year or two that there has been a major spike in DDoS extortion activity.[35]

Organized crime groups have begun controlling or renting botnets for use in their attacks and it is a clearly profitable, if illegal, venture. The UK's National Hi-Tech Crime Unit (NHTCU) reported having arrested a Russian organized crime group who had extorted £1.3 million in 90 days.[36]
It is believed likely that the rise in attacks can be blamed on the fact that many organizations feel it is easier to pay the protection money instead of investing more to defend their bandwidth or lose access to their Web site entirely. Experts believe that as extortionists continue to see growing returns on their efforts and as their botnets increase in complexity and power, this trend will become progressively more widespread.[37]

## 4.5 Cryptoviral Extortion / Ransomware

Encryption has, for a long time, been thought of as a defensive technology. Files are protected from prying eyes and only those authorized to see the information have the necessary key. However, it was eventually realized that cryptography could be used as an offensive technology as well.[38] If the wrong people had the only key to the encrypted data then it would be possible to make demands before the data was returned. The AIDS Trojan, discovered in 1989, was the first malicious code to infect a system and then encrypt the hard drive in an attempt to ransom the data for money.[39] Cryptoviral programs never became a major threat during the eighties and nineties. However, in the last year, several ransomware-type programs have been discovered by anti-virus companies. It appears that these programs may be gaining in popularity.

These recent examples of ransomware have shown that the encryption algorithms used are still weak and, in some cases, the decryption key is left hidden on the victim's system.[40] Although there have been relatively few examples of this sort of threat to date, it is clear that the malware community is experimenting and beginning to learn. As the dissemination techniques and encryption improve, and if the extortion attempts begin to succeed, this will quickly become a more common occurrence.

## 4.6 New Technologies & Targeting Tactics

As crime has moved to the online world, vendors and merchants have begun to fight back. Increasingly, companies are employing IP-based geolocation technology to determine where a prospective buyer is geographically located in an effort to reduce fraudulent purchases. There are several companies that have compiled huge databases and are capable of reverse-mapping an IP address to at least the country of origin.[41] Unfortunately, online businesses are not the only ones capable of using this IP geolocation technology. With social engineering becoming a major vector for malware attacks information becomes a very important asset. The more information attackers can acquire about a target the more effective the attack. Today IP geolocation services have become incredibly accurate, capable of revealing the country, region, city, postal code, latitude / longitude, ISP name and company name associated with a specific IP address. All of this is available for a relatively low price and a limited number of lookups can even be done for free.[42]

Other technologies will also begin to have an increased effect on the potency of worms, viruses and bots arriving at our computer. For years one of the most telling signs of an E-mail worm were the many spelling and grammatical errors in the message body. Now malware authors are making use of grammar and language checks[43] as well as creating worms that can arrive at a system in multiple languages depending on the language the worm determines is in use on the victim’s system.

Another tactic that has been used for many years has been the act of capitalizing on world events or celebrity news in an effort to dupe users. Until now this has been a non-targeted phenomenon where infected E-mails would be sent world-wide.[44] With new technologies for locating IP addresses these attacks can now become far more effective. Riding on the momentum of a localized event, malicious code writers will be able to create and spread malware that is targeted at a very specific segment of the world’s population. This would make the E-mails appear all the more legitimate. Already E-mails separated not only by country and city, but also by industry have been found for sale online.[45] This may be the beginning of an increase in underground trade and sale of targeting information.

## 4.7 Open Source Malware

Malicious code has finally gotten to the point where it is accessible by just about anyone. Malware is now being released under the GNU Public Licence (GPL) as open source software. Not only is anyone allowed to modify and re-release the code onto the Internet, but they are essentially being encouraged to do so. This may explain the sudden drop in the number of families of malicious code released in the second half of 2005, while the numbers of variants from those families continued to climb throughout 2005.[46] All sorts of malware have been opened up by way of the GPL. This includes worms, viruses, Trojans, Remote Access Trojans (RATs)[47] and rootkits.[48]

As Dancho Danchev, managing director for Astalavista.com, points out, this is an interesting move by the experienced malware writers. It creates a situation where there are hundreds of inexperienced writers out there now who are far more likely to be caught than the veterans. All of the variants that are being released generate so much noise that the more experienced writers can remain hidden in the background. Theoretically it would even allow the real authors to hijack the best mutations of their original programs.[49]

## 4.8 New Methods for P2P Hosting

There has been a noticeable decline in the number of P2P clients available and the number of networks hosting media files and other data. Organizations responsible for fighting copyright infringement have been working steadily to close down as many of the networks and major players in the P2P arena as possible. So it is not surprising to see that the popularity of P2P worms has also dropped.[50]

Not discouraged by these crackdowns, it appears that botnet herders have begun finding a way around this issue. The solution involves the sizeable botnets that already exist on the Internet. These large numbers of computers provide huge amounts of disk space and bandwidth - the perfect place for new covert P2P networks. Consider a huge dynamic storage facility for all manner of illegal material.[51] This would be a system where hosts were constantly being added and losing a host or two would not affect the overall network. BitTorrent technology would allow for the transfer of very large files and encryption and password authentication could be used to further keep the network closed to prying eyes. A network just like this has already been discovered. A botnet under surveillance was observed uploading movie files to victim systems. The botnet owners were using a customized version of BitTorrent software to upload sizeable files without arousing the victim's suspicion. Another troubling aspect of this situation is the possibility that with BitTorrent software installed, attackers will now be able to easily seed victim systems with bigger bundles of malware.[52]

## 4.9 Malware for Sale

In a sense computer security is very much about speed. The speed with which a hacker develops code to exploit a vulnerability, the speed with which a company releases a patch or the speed with which an organization can get information out to the public. One way that some companies have addressed this issue of zero-day (0day) exploits has been to begin offering monetary rewards for information about unpublished vulnerabilities in software programs. This allows them to provide the information in advance to their own clients before providing it to the rest of the world. The average time to publish an exploit went up slightly in recent months and this may be because the more experienced hackers / researchers have been submitting their exploits to private companies for remuneration.[53] The question arises, however, if researchers are willing to sell their knowledge to private companies what is to stop them from selling their knowledge on the black market? Organized criminal enterprises will always be able to offer more money and other incentives to individuals for such valuable information. Clearly the market is already being cultivated. The Windows Metafile Vulnerability (MS06-001) discovered in late December 2005 had already been in use for weeks. Hackers in Russia found the exploit at the beginning of December and then proceeded to offer it to organized crime groups for $4000. The vulnerability information was never passed on to private security firms. It was several weeks before anti-virus companies became aware of the vulnerability and associated exploit code. Web sites such as Shadowcrew.com and Carderplanet.com were the first to capitalize on this illegal market and had been providing on-demand hacking, malware, credit card fraud tools and code on their sites until they were shut down by the US Secret Service.[54]

The underground market is developing quickly for these sorts of buyer / seller arrangements[55] and this will likely fuel the development of more private exploit code that security companies will have to find out about the hard way.

## 4.10 Web Application Malware

In the Current Malware Features section of this paper it was highlighted that worm and virus epidemics have seen a noticeable drop recently and that there appeared to be a shift in malware tactics that would see attacks becoming more targeted and localized. However, there is a caveat that goes with this. There is still the belief, in the IT security community, that we have not seen the last of the major worm epidemics.

Network administrators have blocked common ports to cut off malicious code communication routes and attackers have had to change their tactics to compensate. The new vulnerabilities experts expect to be exploited are those found in Web applications.[56] These security holes have the potential to enable malicious code to reach an incredible number of victims in a very short amount of time and such a threat can be difficult to protect against. By exploiting a vulnerability in a Web application on a heavily trafficked site, attackers would be able to reach a huge number of users. Experts anticipate this could be accomplished via content spoofing[57] or cross site scripting[58] vulnerabilities. Such a vulnerability was found in one of Yahoo!'s servers. Had it been exploited, millions of users could have been redirected to all sorts of malicious code.[59]

A factor that compounds the problem is that Web applications are usually Internet-facing and also interact with internal back-end servers. Online companies cannot simply block the common ports (e.g. port 80, HTTP) clients use to access their servers. Because of this and the fact that Web traffic can be very complex, detecting and protecting against Web exploits can be very difficult.[60]

Already anti-virus companies have classified several malicious codes that exploit Web application vulnerabilities. It should come as no surprise that malware authors have already picked up on this new attack vector. The next serious vulnerability in a common Web application will, very likely, generate much interest and exploit code from the malware community.

### 4.11 RFID as a Propagation Vector

Radio Frequency ID (RFID) technology is expected to take over from bar codes in the coming years. RFIDs allow for the quick and easy auditing of products on stockroom floors as well as allowing for simplified checkouts at retail stores. However, recent research has found that RFID is not a completely benign technology. RFID tags interface with the same sorts of back-end database servers that other technologies, such as Web servers, use. RFID tags are also capable of being re-written and can hold small amounts of data.[61] Not surprisingly, researchers have found that RFID can be exploited in ways similar to other technologies. Buffer overflows, SQL injection attacks and even malicious code capable of replication can be written to RFID. Researchers in the Netherlands were successful in creating the world's first virus-infected RFID tag. This accomplishment may signal a new and dangerous vector for malware infections.

If RFID tags succeeded at infecting back-end servers, and, in turn, these servers then replicated their data on the internal network, the malware could spread very quickly. Backdoors could also be opened allowing access to servers thought not to be at risk. Even without back-end communications or the mirroring of servers, the movement of infected RFID tags around the globe could do similar damage.[62] Some airports are already considering augmenting their baggage handling infrastructure with RFID technology. Infections at several major airports could cause serious problems. These sorts of attacks would not be limited to airports or warehouses either. The local grocery store using RFID or the veterinarian who is scanning a pet's infected RFID chip could also experience problems after exposure to the malware.[63]

The research on this subject is only in the proof of concept stage and RFID technology is nowhere near as ubiquitous as experts claim it may become. It may take a while, but RFID malware may well surface in the near future as a serious threat.

## 5 Conclusion

The malicious code landscape is forever changing. In the past couple of years there has been a shift in malware tactics and the future trends will see a continuation of this. Attacks continue to demonstrate increased levels of complexity and organization. Organized criminal elements are becoming more involved; money and threats of violence are now being introduced into the malware community.[64] Malicious code writers are acquiring a better understanding of how to profit from the Internet in an illicit manner. It will require a lot of effort to keep up with these new and emerging threats.

Since some of the threats mentioned here can be strategically combined with other methods of attack, such as social engineering, the importance of user awareness is obvious. Ongoing research and diligence will be required to better understand these threats and this document will serve as a good starting point. In the meantime, malicious code continues to prey on those systems with the weakest defences. Anti-virus and firewall programs should be installed and kept up to date. Users should exercise constant care when online and malicious incidents, of a criminal nature, should be reported to local law enforcement. Finally, advisories from vendors and government centers such as the Canadian Cyber Incident Response Center

(CCIRC) need to be heeded. Having as much knowledge and information as possible about what is being exploited will be one of the best ways to counter these new threats.

# 6 Glossary of Terms[65]

**Botnet** – Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised machines running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure.

**Botnet Herder** – ‘Botnet herder’ is a commonly accepted term for individuals who control the vast networks of compromised systems that form botnets.

**Bot** – A bot is common parlance on the Internet for a software program that is a software agent. The most common bots are those that are installed without the knowledge of a computer's owner for malicious purposes.

**Content Spoofing** – Another kind of spoofing is "Web page spoofing". In this attack, a legitimate Web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. The intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest user names and passwords.

**Cross-Site Scripting (XSS)** – A type of computer security vulnerability typically found in Web applications which can be used by an attacker to compromise the same origin policy of client-side scripting languages.

**Hacker** – In computer security, a hacker is a person able to exploit a system or gain unauthorized access through skill and tactics. This usually refers to a black hat (or malicious) hacker.

**P2P** – A peer-to-peer (or P2P) computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. P2P networks are typically used for connecting nodes via largely ad hoc connections.

**Propagation Vector** – A vector in computing, specifically when talking about malicious code such as viruses or worms, is the method that this code uses to propagate itself or infect the computer and this sense is similar to, and derived from, its meaning in biology. Examples of common vectors include:

- buffer overflows
- HTML E-mail with JavaScript or other scripting enhancements
- networking protocol flaws – this is how the Blaster worm was able to propagate

**Rootkit** – A rootkit is a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge.

**Spammer** – Spammers are those individuals who send spam. Spamming is commonly defined as the sending of unsolicited bulk e-mail - that is, E-mail that was not asked for (unsolicited) and received by multiple recipients (bulk).

**Trojan** – In the context of computer software, a Trojan horse is a malicious program that is disguised as legitimate software. The term is derived from the classical myth of the Trojan Horse.

**Virus Kit** – A software program designed to allow a user with few or no programming skills to create a virus or worm and release it onto the Internet.

**Worm** – A computer worm is a self-replicating computer program. It is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.

**Zero-Day (0day) Attack** – A zero-day attack is one that attacks a vulnerability for which there is no available patch. It also generally means an attack against a vulnerability that is not yet public knowledge or even known of by the vendor of the affected technology.

**Zombie** – A zombie computer, abbreviated zombie, is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse.

[1] Robert Richardson *et al.*, *CSI/FBI Computer Crime and Security Survey* (San Francisco: Computer Security Institute, 2005) at 13, online: Computer Security Institute <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf>.

[2] The original idea for this report was born out of the paper *Malware – future trends*, written by Dancho Danchev. His complete paper can be found here: http://www.packetstormsecurity.org/papers/general/malware-trends.pdf.

[3] Ryan Naraine, "Researcher: WMF Exploit Sold Underground for $4,000," (2 February 2006) online: eWeek.com <http://www.eweek.com/article2/0,1895,1918198,00.asp>. [*WMF*]

[4] Yury Mashevsky, "Watershed in malicious code evolution," (29 July 2005) online: Viruslist.com <http://www.viruslist.com/en/analysis?pubid=167798878>. [*Watershed*]

[5] Dr. Steven Furnell & Dr. Jeremy Ward, "The True Computer Parasite," (1 June 2005) online: SecurityFocus <http://www.securityfocus.com/infocus/1838>.

[6] National Infrastructure Security Coordination Center, "The Quarterly – The growing online marketplace," (February 2005) at 4, online: NISCC <http://www.niscc.gov.uk/niscc/docs/re-20050728-00635.pdf?lang=en>.

[7] National Infrastructure Security Coordination Center, "Targeted Trojan E-mail Attacks," (16 June 2005) at 4, online: NISCC <http://www.niscc.gov.uk/niscc/docs/ttea.pdf>.

[8] *Watershed*, *supra* note 4.

[9] Tom Sanders, "Cops smash 100,000 node botnet," (10 October 2005) online: Vnunet.com <http://www.vnunet.com/vnunet/news/2143475/dutch-police-foil-100-node>.

[10] Adel Melek *et al.*, *2006 Global Security Survey* (London: Deloitte, 2006) at 13, online: Deloitte Touche Tohmatsu <http://www.deloitte.com/dtt/research/0,1015,sid%253D1000%2526cid%253D121102,00.html>.

[11] Alexander Gostev, "Malware Evolution: January - March 2005," (18 April 2005) online: Viruslist.com <http://www.viruslist.com/en/analysis?pubid=162454316>.

[12] David Emm, "Rise of the 'business worm'?," (19 August 2005) online: Viruslist.com <http://www.viruslist.com/en/analysis?pubid=168953110>.

[13] U.S. Department of Energy – Computer Incident Advisory Capability, "P-256 Targeted Attacks," (18 July 2005) online: US DoE – CIAC <http://www.ciac.org/ciac/bulletins/p-256.shtml>.

[14] David Sancho, "The Future of Bot Worms," (18 August 2005) at 1, online: Trend Micro <http://www.trendmicro.com/en/offers/global/outbreak-aug18-wp.htm>.

[15] Dean Turner *et al.*, *Symantec Internet Security Threat Report – Trends for July 05-December 05* (Cupertino, California: Symantec, 2006) at 55-57. [*Symantec*]

[16] *Watershed*, *supra* note 4.

[17] *Watershed*, *supra* note 4.

[18] *Symantec*, *supra* note 14 at 14.

[19] Dancho Danchev, “Malware – future trends,” (9 January 2006) at 3, online: PacketStorm Security <http://www.packetstormsecurity.org/papers/general/malware-trends.pdf>. [*Malware*]
[20] *Ibid*. at 3.
[21] Infectionvectors, “Agobot and the ‘Kit’chen Sink,” (July 2004) at 4-5, online: Infectionvectors.com <http://www.infectionvectors.com/vectors/Agobot_&_the_Kit-chen_Sink.pdf>.
[22] *Symantec*, *supra* note 14 at 16.
[23] *Symantec*, *supra* note 14 at 75.
[24] *Malware*, *supra* note 19 at 17.
[25] *Symantec*, *supra* note 14 at 72.
[26] *Malware*, *supra* note 19 at 18.
[27] *Watershed*, *supra* note 4.
[28] Sharp Ideas LLC, “Pod Slurping,” (2005) online: Sharp Ideas LLC <http://www.sharp-ideas.net/pod_slurping.php>.
[29] Trend Micro, “SYMBOS_CARDTRP.D,” online: Trend Micro <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName= SYMBOS%5FCARDTRP%2ED&VSect=T>.
[30] Chris Davis & Aaron Higbee, “DC Phone Home,” (31 July 2002) online: Black Hat <http://www.blackhat.com/presentations/bh-usa-02/higbee-davis/higbeedavis-bh-us-02-phone.ppt>.
[31] iDefense, “Rootkits and Other Concealment Techniques in Malcode,” (17 February 2006) at 19, online: iDefense <http://www.idefense.com/intelligence/researchpapers.php>.
[32] *Symantec*, *supra* note 14 at 20.
[33] Alisa, “Subversive SubVirt,” (16 March 2006) online: Viruslist.com <http://www.viruslist.com/en/weblog?weblogid=182153387 >.
[34] Robert Lemos, “Researchers: Rootkits headed for BIOS,” (26 January 2006) online: SecurityFocus <http://www.securityfocus.com/news/11372>.
[35] *Symantec*, *supra* note 14 at 12.
[36] Paul Stamp *et al.*, “Increasing Organized Crime Involvement Means More Targeted Attacks,” (2 August 2005) at 2, online: SEC Consult <http://www.sec-consult.com/fileadmin/Newsletters/newsletter092005.pdf>.
[37] *Symantec*, *supra* note 14 at 12.
[38] Adam Young & Moti Young, “Cryptovirology: Extortion-Based Security Threats and Countermeasures,” (6 May 1996) online: VX Heavens <http://vx.netlux.org/lib/ayo00.html>.
[39] “AIDS (trojan horse),” online: Wikipedia <http://en.wikipedia.org/wiki/AIDS_%28trojan_horse%29>.
[40] LURHQ Threat Intelligence Group, “Cryzip Ransomware Trojan Analysis,” (11 March 2006) online: LURHQ <http://www.lurhq.com/cryzip.html>.
[41] Daniele Micci-Barreca, “Unawed by Fraud,” (September 2003) online: Security Management Online <http://www.securitymanagement.com/library/001490.html >.
[42] MaxMind, “MaxMind GeoIP® City Database,” online: MaxMind <http://www.maxmind.com/app/city>.
[43] *Malware, supra* note 19 at 18.
[44] John Leyden, “Slobodan Trojan poses as murder pics,” (15 March 2006) online: The Register <http://www.theregister.co.uk/2006/03/15/slobodan_trojan>.
[45] *Malware*, *supra* note 19 at 18.
[46] *Symantec*, *supra* note 14 at 17.
[47] Massimiliano Romano *et al.*, “Robot Wars – How Botnets Work,” (20 October 2005) online: WindowsSecurity.com <http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html>. [*Robot*]
[48] David Sancho, “Rootkits: The new wave of invisible malware is here,” (2005) at 2, online: Trend Micro <http://www.trendmicro.com/NR/rdonlyres/388874B6-C27C-4354-9078-42771EABEBB1/18503/rootkitwp.pdf>.
[49] *Malware*, *supra* note 19 at 18-19.
[50] *Watershed*, *supra* note 4.
[51] *Robot*, *supra* note 47.
[52] Paul F. Roberts, “Botnet Uses BitTorrent to Push Movie Files,” (21 December 2005) online: eWeek.com <http://www.eweek.com/article2/0,1759,1904429,00.asp>.
[53] *Symantec*, *supra* note 14 at 56.
[54] *WMF*, *supra* note 3.
[55] *Malware*, *supra* note 19 at 21.

[56] *Symantec*, *supra* note 14 at 22.
[57] Web Application Security Consortium, “Content Spoofing,” online: WASC <http://www.webappsec.org/projects/threat/classes/content_spoofing.shtml>.
[58] “Cross site scripting,” online: Wikipedia <http://en.wikipedia.org/wiki/Cross_site_scripting>.
[59] *Malware*, *supra* note 19 at 24.
[60] *Symantec*, *supra* note 14 at 22.
[61] Melanie R. Rieback *et al.*, “Is Your Cat Infected with a Computer Virus?,” (March 2006) at 3, online: Vrije Universiteit Amsterdam <http://www.rfidvirus.org/papers/percom.06.pdf>.
[62] *Ibid*. at 4.
[63] “RFID Viruses and Worms,” online: Vrije Universiteit Amsterdam <http://www.rfidvirus.org>.
[64] Phil Williams, “Organized Crime and Cyber-Crime: Implications for Business,” (2002) at 2, online: CERT.org <http://www.cert.org/archive/pdf/cybercrime-business.pdf>.
[65] The definitions for the terms found in the glossary are originally found in the Wikipedia. <http://www.wikipedia.org>.