Malware History

bitdefender

Table of Contents

Table of Figures

Revision History

7/16/2008

- Initial release of the document, covering the malware landscape between 1970 and 2008

4/30/2010

- Second revision of the document, adding data for the 2008-2010 timeline.
- Some minor corrections to the previous material have also been performed.
- Added information on Rogue AV software

Disclaimer

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post -release information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide.

Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Introduction

Although malicious software is often regarded as an entirely new concept, its history dates way back in time. While completely mechanical computing tools, such as the abacus or Charles Babbage's Differential Machine are sure to have been spared by pestering malware, electronic devices have often had to face the challenge of security threats. In the following pages, you will find a history of malware, as well as some safety & security guidelines to let you, the users, enjoy a pleasant experience on the Internet.

What Malware Really Is

The term "malware" stands for malicious software, and usually defines a broad range of intrusive, hostile software applications. Although there are multiple pieces of software that can harm your computer because they are poorly written or allow easy access to the users' systems, the term only covers software that has been deliberately designed to disrupt the normal computing activity[1]. Therefore, buggy applications are not malware, since their security faults have not been implemented on purpose.

Malware is an umbrella-term that covers a broad range of harmful (or potentially harmful) software applications, such as viruses, worms, backdoors, Trojans, keyloggers, password stealers, script viruses, rootkits, macro viruses, spyware or even adware. While in the IT industry's early days threats were labelled as either viruses or Trojan horses, the rapid escalation of technology called for a general term to cover all the above-mentioned threats.

Spreading Malware – A Business that Brings Billions

Malware applications have initially been conceived as practical jokes, pranks or even as experiments to demonstrate artificial intelligence. For instance, the first Internet Worm and a great deal of MS-DOS "viruses" were harmless to both the user and the computer. They were designed to be annoying and let the world know about their creator. Such pseudo-malicious applications were easy to remove and

[1] It might look confusing, but some computer worms are allegedly designed to help the user. This was the case of the Nachi family of worms, a research project carried at Xerox PARC. The worm attempted to download and install available patches form the Microsoft website, in order to patch some known security vulnerabilities. However, it would not notify the user of its actions, and sometimes would disrupt users' activity by generating high amounts of network traffic, as well as rebooting the machine as part of the update process.

did not pose a security threat at all. More than that, their authors did not pay any attention to methods of concealing the virus; on the contrary, they used it to boast their achievements.

Things have dramatically shifted lately, as malware writers don't want glory anymore, but rather financial gains. They have started to pay extra attention to hiding the malware from both the user and antivirus software, in order to be able to exploit it for as much as possible. Malware authors invented new methods to conceal and protect their malicious creations, and make them undetectable for specialized antivirus software.

Writing and spreading malware is a business that's worth billions of dollars per year. According to a report issued by research company Computer Economics, the direct damage attributed to malware totaled $20 billion[2] globally in 2007.

Modern malware writers exploit their creations to quietly use infected machines, and then send spam messages, steal banking credentials, or leverage their revenue by advertisement click fraud. More than that, corporate espionage also brings constant revenue, as malware opens backdoors into the organization's network.

Types of Malware

As previously stated, malware is an umbrella term that covers multiple security threats. Infectious malware is comprised of viruses and worms, while Trojans, backdoors and rootkits are concealed pieces of malicious code. Last, but not least, malware for profit gathers spyware, botnets, keystroke loggers, as well as telephony dialers.

1. Viruses

Computer viruses are pieces of software that can replicate themselves and stealthily infect the host computer. Due to the fact that viruses are associated with destructive behaviors, they are wrongfully used to define multiple types of malware. Depending on its complexity, the initial virus may modify its next copies, in order to escape the simple string detection algorithms in antivirus software. Viruses can spread using either the network / Internet, or by infecting files on removable media (floppy disk, CD or USB drives).

2. Worms and Mass-Mailers

Worms are also self-replicating programs that stealthily spread across computer networks. Unlike viruses, the replication process is automated, as worms do not have to infect an existing software

[2] The full report can be read here: http://www.gss.co.uk/news/article/4029/go

program. Their destructive potential lies in the fact that they eat up large amounts of bandwidth, while viruses usually modify, delete or corrupt the files on the infected system.

Mass-mailers are regarded as part of the worm. Given the fact that worms can't rely on file-to-file transfers, they are designed in such a manner to send themselves to other computers via e-mail. Worms spam themselves to every address found in the address book. However, worms need a person's action to infest a computer: their malicious potential is unleashed when the computer user opens the attachment that comes with the infected e-mail[3].

3. Trojan Horses

Trojan horses are probably the widest-spread security threats nowadays. The term "Trojan" defines a piece of software that lets the user think that it performs a specific task, while in fact it performs a totally different action and most of the time it would harm either the users or their computers. Usually, a Trojan horse would download and install a computer virus. Some other times, the Trojan comes with no hidden payload, which means that it is harmless. However, the most important aspect as far as terminology is concerned is the fact that Trojan horses are completely different from viruses. They lack self-replication capabilities, and they heavily rely on computer users to cause damage. Trojan horses are usually spreading using social-engineering techniques[4]; the most recent social engineering technique tricks the user trying to watch video content[5] (usually downloaded via P2P networks) to install a special codec, that ultimately proves to be a backdoor or an exploit.

As Trojans are extremely specialized software applications, they can be broken down into several categories by the way they affect the host computer. Although there is no nailed classification as far as Trojan horses are concerned, they can be accurately labeled according to their behavior and destination.

- **Remote Access Trojans** are by far the most aggressive manifestation of this type of malware. Once installed, they grant third-party human users complete control over the system. Another interesting aspect is the fact that Remote Access Trojans (also known as RATs) allows the person at the other end of the Internet connection to monitor users' desktop, download and install other software, record keystrokes or even export critical files to other locations (either using FTP or HTTP

[3] The Internet worm LoveLetter and its variants used to replicate themselves by tricking the user into opening an infected attachment with the .VBS file extension.

[4] The term covers a wide range of techniques that trick the end-user into divulging confidential information. The social engineer usually appears to come from a legitimate business (banking, credit company or a corporate IT staff member) requesting "verification" of information.

[5] For instance, Trojan-Downloader.Zlob.Media-Codec often claims that it is an important upgrade to Windows Media Player, that allows users enjoy adult video directly from the web. Instead, it downloads and installs rogue security programs such as SpywareQuake, SpyFalcon and WinAntivirusPro. Other variants even feature backdoor functionalities, that allow an attacker to seize control over the entire machine.

protocols). The author of such Trojan application[6] gains complete control over the system and can control it in any way to suit their malicious purposes. Many times, RAT authors use the "captured" machine to store games and other cracking tools, taking up nearly all the user's available hard disk space and resources.

- **Data Destruction Trojans**[7] have the ability to completely erase or corrupt the data stored on the computer, be it operating system files or user data. Although such malware does not endanger users' banking credentials or other confidential information, it takes the computer out of service and causes significant data loss. For instance, imagine that you have a presentation due the next day and it gets wiped out by a data destruction Trojan. This would be a critical blow to your career, not to mention the fact that your system will be out of order until the IT specialists clean it and then re-install the necessary applications. A newer approach at tampering with the users' files involves a Trojan that launches a crylptoviral attack[8] on users' personal data. If they want their data back, they have to pay the attacker a specified amount of money, part of the extortion scheme.

- **Downloader Trojans** are software applications that can not hurt a computer by themselves, should the system be not connected to the Internet. Their payload code connects to the Internet, and then it facilitates the installation of other applications on the host computer. Downloaders may install adware and spyware (along other types of malware) or from multiple servers or sources on the Internet.
- **Security Software Disablers** are Trojans that, once installed onto the host computer, try to stop or kill security software such as antivirus applications or firewalls without the user's consent. More than that, such Trojans often come bundled with another Trojan or virus that acts like a payload. Once antivirus or firewall applications are disabled, the compromised system is completely unprotected to subsequent attacks coming from the Internet.
- **Denial-of-Service (DoS) Trojans** are especially-crafted pieces of software that do not affect the host PC. Instead, they are designed to hinder or stop the normal functioning of a web site, server or

[6] The most "popular" Remote Access Trojans are known as Back Orifice or SubSeven. They are all-in-one hacking libraries, that let their authors take screenshots, capture sound and video or intercept keystrokes and sensitive passwords. Such tools come with their own FTP and HTTP server to increase their efficiency. However, their complexity reflects in the large installation file, which varies between 100 and 300 KB.

[7] Data destruction and corruption are usually the result of viruses. However, there are various types of malware that spread like Trojans, while their payload is strikingly similar to the viruses'.

[8] Malware users have been using cryptography to hide the payload for quite a while now, but cryptoviral attacks encrypt files with many different extensions, and then advise their owner to send money into a specific account. The first piece of malware to request a ransom in exchange for the affected files was the "Win32.Gpcode.ag" virus.

other network resource by flooding it with more network traffic than it is able to handle. Distributed Denial-of-Service (DDoS) attacks are somewhat similar to the DoS ones, except for the fact that they are carried using multiple compromised machines at the same time. Attackers often use a compromised machine as the "master" – a computer that co-ordinates the attack across other infected machines (also known as zombies).

- **Dialers** are Trojans that got their glory in the heydays of dial-up connections. This type of Trojans would use the modem / phone line in order to place calls to premium-rate phone numbers. Dialers usually promise instant access to certain resources, and, while the user is aware of its presence, it is often unaware of the premium call costs[9]. The most common incarnation of this type of malware is the so-called porn dialer. Similar approaches use web pages that connect to premium services, also related to the porn industry.

- **Keyloggers** are extremely malicious Trojans, entirely designed for profit. While they do not disrupt normal operation on the infected computers, they monitor, log and send each keystroke to a remote location, either using e-mail or FTP services. While some keyloggers are sold as legit, commercial pieces of software designed to monitor children's online activity, they are mostly used for malicious purposes, such as stealing banking or other login credentials. Keyloggers have reached an extremely high level of sophistication that allows their creators to monitor only specific activities, in order to keep the size of log files down. For instance, they can record only information passed to specific forms displayed within specific webpages[10] (the primary targets are online stores, e-banking services or e-mail service providers).

- Rogue AV Trojans are applications that warn users of infections that do not exist in order to trick them into buying the "full version" of the product. They often make use of other malware in order to install trial versions of themselves on computers without the users' consent. Most of these applications are considered adware and/or spyware.

[9] Bitdefender was the world's first antivirus provider to include an anti-dialer module that prevents both known and unknown malicious applications from dialing premium-rate numbers using the computer modem.

[10] You can safely pass sensitive data to a web form using a virtual keyboard application, such as the On-Screen keyboard bundled with the Microsoft Windows operating system.

4. Backdoors

Backdoors are security risks that allow attackers to remotely and stealthily access a computer using either plain-text or fully visual interfaces. Such backdoors are either opened by a Trojan (for instance, the much-hyped Back Orifice remote access tool), or even opened by an existing piece of software on the computer. Moreover, backdoor features may also be included in commercial software by using a hardcoded combination of username and password. Many times, backdoors are deliberately left open by computer vendors. However, please note that this kind of backdoor is not to be regarded as malware, as it is mostly used for support and maintenance tasks (support staff usually connects to the respective machine remotely, in order to troubleshoot various operation issues). Still, such backdoors can pose a security risk to the end-user, as they can be easily exploited by unauthorized parties. Unlike spam and Trojans, backdoors don't try to impersonate; instead, they open a communication channel between computers without users knowing it.

5. Exploits

Exploits target specific vulnerabilities in the software running on a system. Remote attackers are thus able to run malware directly on the target computer. The most recently discovered vulnerability was documented by the Bitdefender analysts as affecting the popular browser from Microsoft, Internet Explorer 7[11]. Exploits take advantage of software design flaws in order to trigger unexpected behaviors in the software running on the target computer. Exploits usually allow attackers to either gaining control of a computer system through privilege escalations[12] or to perform denial-of-service attacks. Software vendors usually patch their products as soon as vulnerabilities are detected, before the exploit code gets into the wrong hands. However, many attackers keep such vulnerabilities private and use them for malicious purposes, rather than announcing the vendor. Newly-discovered vulnerabilities are also known as "zero day exploits" and sell for thousands of dollars on the black market[13].

[11] You can read more about the printing exploit that affects IE7 and its upcoming iteration, IE8, on the Bitdefender website: http://news.bitdefender.com/NW737-en--BitDefender-Issues-Signature-Update-to-Protect-Users-from-New-Microsoft-Internet-Explorer-7-Printing-Vulnerability.html

[12] Although many exploits are especially designed to grant attackers administrator / root privileges, multiple exploits can also be used to repeatedly escalate from user-level to superadministrator.

[13] An interview carried by tech website Security Focus unveils that exploitable vulnerabilities can sell for as much as $10,000. However, the damage inflicted to users can not be even closely estimated. You can read the full article here: http://www.securityfocus.com/news/11476/1

Exploits usually affect systems running Microsoft Windows operating systems, but there have been attempts to install undocumented backdoors in the Linux kernel itself. With only two lines of code, a remote attacker could gain root privileges on the system[14].

6. Rootkits

Rootkits are extremely advanced pieces of malware, built with complete stealth in mind. They can camouflage themselves among other legitimate processes running onto the system, which dramatically increases discovery and disinfection times[15]. Rootkits are also designed to take complete control over the entire affected computer, without user's consent. The "rootkit" term shows that this type of malware is running with the highest available privileges[16], and can evade even the toughest security mechanisms built into the operating system. Rootkits are also capable of hiding their concealing running processes from monitoring programs, or even hiding system files from the operating system.

Despite their destructive potential, rootkits do not always perform malicious tasks. For instance, many commercially-available pieces of software make use of rootkit technology to hide themselves from miscellaneous security applications or from the operating system itself. This practice is mostly encountered on emulation software, such as the well known Daemon Tools[17] and Alcohol 120%.

7. Spyware

Spyware applications are pieces of software that stealthily install and monitor users' interaction with the infected computer. There is no clear border between spyware applications and Trojans, as such applications usually spread just like Trojans, and many times Trojans spy on the infected computers. Unlike computer viruses and worms, spyware applications do not auto-replicate, but they also exploit computers for commercial advantages. Spyware covers more that monitoring users' behavior: they can collect private information, Internet surfing and online shopping habits, and then send the data to

[14] http://www.securityfocus.com/news/7388

[15] Rootkits are not only extremely difficult to detect, but they are also impossible to manually disinfect by the average computer user. Even specialized antivirus programs are sometimes incapable of cleaning them. Bitdefender products include an **Anti-Rootkit** module for detecting and eliminating hidden security threats.

[16] Root access defines the highest level of control in an Unix-based environment.

[17] Although the Daemon Tools rootkit technology can not be labeled as malware, the last versions of the so-popular software come bundled with adware applications (When U Save).

a remote location. Moreover, some spyware applications borrow features from their adware siblings in order to redirect Internet Explorer webpages to advertising websites[18]

8. Adware

Adware applications are often wrongfully labeled as the mildest security risk in the industry. It might be true that adware Trojans don't harm the host system, but instead they annoy users by serving various ads within the browser, or even constantly changing the browser's startup page. More than that, adware applications usually come bundled with third-party software that might pose a security risk[19] for both the user and the host system.

9. Phishing

Phishing is a criminal activity that uses social engineering techniques in order to gain users' confidence and trick them into divulging sensitive information, such as passwords and banking credentials. The attacker tries to impersonate a trustworthy entity, such as a well-known online store or a bank. For instance, eBay and PayPal are the two most favorite entities used in phishing attacks. Online banking portals are also becoming popular with attackers, since a successfully carried phishing would give unauthorized persons full access to user's account.

Phishing campaigns are usually carried using instant messaging software or via spam e-mails. The attackers set up a clone of the target website on a hosting account, compose e-mail messages that seem legitimate, but manipulate links to look genuine, while redirecting users to the forged website. The message is then sent to all the users in a spam e-mail database[20]. Unwary users that fill in the fields with their credentials send critical information straight to the attacker.

[18] This is the case with the popular Internet Optimizer utility, also known as DyFuCa. The application not only that annoys its users with ads, but, due to a design flaw, it also prevents them from accessing password-protected websites.

[19] Some adware applications explicitly state in the EULA (End-User License Agreement) that they install third-party modules or controls, yet few users take the time to fully read the entire license. It is recommended that you pay extra attention to the legal terms when you install any applications.

[20] As of the moment of writing, such e-mail databases are sold on the black market at extremely low prices. More than that, harvesters sort e-mail addresses using multiple criteria, such as profession, hobbies or general interests in surfing the web, that allow attackers to maximize their chances in defrauding targets.

Misspelled URLs or even the use of subdomains are only a few of the tricks used by attackers to gain users' trust. However, new approaches can even force the browser into mimicking a secure connection (https)[21].

Malware History

Just like biological viruses can't exist, multiply and spread in the absence of an animal host, computer viruses are closely tied to electronic computing systems. Historians are still debating on the actual birth date of the first computer virus, and many of them would dare to place the first malware applications in the mid-1970 timeframe[22]. However, theoretical approaches to self-reproducing mathematical automata are estimated to have started in early 1950s[23].

Pre-History: From Innocent Pranks to Widespread Infections

The first computer viruses have been born in academia, and pitched at totally different purposes than infecting systems and causing havoc amongst computer users. For instance, in late 50s, British mathematician Lionel Penrose published a report called "Self-Reproducing Machines", an overview of a simple two dimensional model able to self-replicate, mutate and attack computer systems. The practical part of the project was ported by Frederick G. Stahl on an IBM 650 system. At that moment, scientists and researchers were exclusively concerned with artificial intelligence and the blooming field of robotics.

A few years later, three researchers at the Bell Telephone Laboratories (Victor A. Vyssotsky, Robert Morris Sr., and M. Douglas McIlroy) started experimenting with a programming game called Darwin (August 1961). Darwin was comprised of a program called the "umpire" running in a designated section of the computer's memory (the memory location was referred to as "the arena").

Each of the players would have to write small programs using IBM 7090 machine code, and could call specific functions stored in the "umpire". The main goal was to probe memory locations, terminate the opposing program running at that location, then fill the vacant space with copies of themselves. The

[21] In order to complete the security illusion, the attacker can falsify or hide miscellaneous elements of the browser, such as status bar text, URL location or the document source. All these elements can be forged using JavaScript.

[22] Three computer models have been surely infected by malware in mid-70s: Univax 1108 and IBM 360/370.

[23] John von Neumann (December 28, 1903 – February 8, 1957) illustrated the concept of self-replicating machines in his posthumous work, "Theory of Self Reproducing Automata".

game would end either after a specific amount of time, or when there was only a single player left "alive"[24].

The game itself was nothing but harmless amusement, but it also can be regarded as the beginning of self-multiplying software to be used in completely different manners.

Duality: The Anti-Virus Virus

In early 1970s, the first worm program appeared in the wild, on the US military computer network ARPANET[25]. Called the **Creeper**, this archaic worm was written to work on the Tenex system, an extremely popular choice at that time. The worm would spread by independently getting access to the network (via modem), and then infecting remotely-located systems. According to some historians, the **Creeper** worm has been developed inside the ARPANET, and Bob Thomas (one of the network's inventors) experimented with this piece of software as he was extremely interested in its capacity of penetrating networks and passing its copy on various systems.

Creeper might have been annoying, but it had no malicious payload, as most of the modern worms do. Infected systems would only display the message: 'I'M THE CREEPER: CATCH ME IF YOU CAN.' However, this little experiment succeeded in such a manner that shortly thereafter, the entire TENEX network was carrying copies of the worm. In order to clear the network from the Creeper attack, an anonymous programmer wrote **Reaper**, a computer virus that would seek and delete Creeper copies installed on machines. Just like its predecessor, the **Reaper** was also able to independently travel across the network.

The **Reaper** virus marks an important milestone in the malware history. It is not only the first virus ever spotted in the wild, but at the same time, due to its hunt-down capabilities, it can also be regarded as the first antivirus product.

The Seventies: Computer Games That Spell Disaster

In early 1974, a new computer virus emerged. Called the **Rabbit**, it was still more of a prank than an effective security threat. The virus would do nothing but multiply and spread at an accelerated pace. In fact, it was named after the speed at which it bloated the computer with multiple copies of itself. Unlike its predecessors, the virus severely affected the infected computer's performance and would

[24] Morris ultimately developed a highly specialized application, built using only 44 instructions. His software would locate the start of an enemy program, and then probe subsequent memory locations until it finds the end of the program. The piece of software would "remember" the exact length of the opponent's program and use it in subsequent searches.

[25] The US military computer network ARPANET was the forerunner of the modern Internet.

eventually crash it. It is currently unknown whether the virus was designed to deliberately disrupt activity or was just an experiment that got out of control.

Another innocent game called **Pervading Animal** emerged one year later and gave Univac 1100/42 users a hard time. Some historians still argue whether **Pervading Animal** was yet another computer virus or it marked the beginning of a new breed of malware: Trojans[26]. This "innocent" piece of software had been written in April 1974 by John Walker, and had been later updated with self-replication functionalities. The game concept was extremely simple: the user had to think of an animal, and then the program would fire up a set of questions in an attempt to identify the specific animal. However, the game featured an error-correction feature, which allowed it to "learn" from its previous mistakes[27]. Each time a correction was performed against its database, the software would overwrite the previous version, but at the same time, it would also copy itself to other directories within the mainframe. After a specific period, all other directories would end up containing a copy of the program. Although the software itself took up only little disk space, all its copies would clog up the computer, thus affecting its overall performance.

Self-replication features were added later to the Animal program, in order to spare the author the hassle of making manual copies of the game for his friends and colleagues. According to an explanation given by John Walker himself[28], he wrote the **PERVADE** routine, a general purpose piece of code that created an independent process listing all the directories accessible to the caller. The routine subsequently would check whether the available directory has an up-to-date version of the **Animal**, then copy version being executed into that directory[29].

In order to get rid of the multiple instances copied all in each and every folder[30], Walker and his friends took the same approach as in the Creeper – Reaper war. A new version of the game, called the **HUNTER** scanned folders for older versions of the **Animal** and deleted them all. However, the program was stopped for good from spreading only when a new version of the Exec[31] operating system was released.

[26] Pervading Animal would spread into successively more protected directories in what today is called a "classic Trojan Horse attack".

[27] Each time the program failed to guess the animal, it would add up new sets of questions to be asked in the next games.

[28] http://www.fourmilab.ch/documents/univac/animal.html

[29] Despite its Trojan behavior, PERVADE was coded in such a manner not to destroy third-party files with an identical name, which proves that it was not designed with damage in mind. However, the borders between malicious intent and programming flaws were extremely blurry at that time.

[30] Even the folders available to super-administrators have been infected. This was possible when a privileged user (root administrator or super-user) would launch the program. Since they have full access to the computer, PERVADE would inherit their administrative rights, and then use them to replicate in previously inaccessible folders.

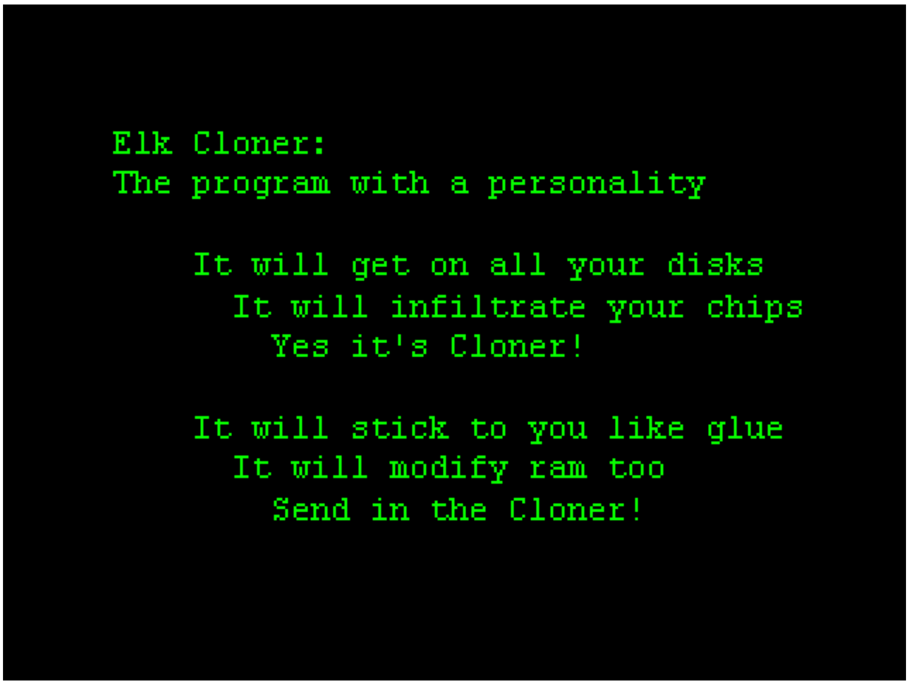
[31] The next iteration of the Exec OS (version 8) came with a modified file system, which would disallow the game to spread.

The Eighties: Experimenting with Malice

Computer science student Jürgen Kraus writes his master's thesis on program self-reproduction (Selbstreproduktion bei Programmen[32]). Kraus' work described the construction of such phenomena, and is the first paper to document how different types of programs can borrow features form the biological world in order to survive, spread and infect other entities. However, his paper had been never presented, and any reference to it got buried in the archives of the Dortmund University.

Worms Start Biting from the Apple

In early 1981, Apple II systems started gaining ground in both home and academia environments. Their popularity and relative affordability triggered the first large-scale virus outbreak in the industry. Although only a small fraction of the worldwide computers were connected to the Internet, viruses would spread by infecting the floppy disks hosting the operating system. Rich Skrenta's[33] **Elk Cloner** was the first Apple II virus to spread using infected floppy drives. Each time a computer boots from the infected media, an instance of the virus is automatically executed. The virus would carefully monitor for access to an uninfected floppy drive – each tine a new disk was inserted, it would copy its code on the new medium. Since floppy



```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Figure 1: The Elk Cloner virus would display a poem as part of its payload.

[32] Although the thesis got lost in the University's archives, it can be read online (German only) at http://vx.netlux.org/lib/mjk00.html

[33] Skrenta was a junior high school student when he wrote the virus. "I coded up Elk Cloner and gave it a good start in life by infecting everyone's disks I could get my hands on," he allegedly said later.

disks were the only way users could pass information along, the virus slowly spread across thousands machines.

Elk Cloner used to infect the boot sector for Apple II computers, and the outbreak rapidly escalated, mostly because computer users were unaware of such security threats and there were no antivirus programs available. Its payload would often rotate images or blink textual jokes, such as the Elk Cloner Poem[34]:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

IT WILL INFILTRATE YOUR CHIPS

YES, IT'S CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!

The Elk Cloner was only the starting point for a series of new viruses targeted at Apple II systems. Joe Dellinger, a student at Texas A&M University also wrote three self-reproducing programs for Apple II disks, called **Virus 1**, **Virus 2** and **Virus 3**.

Another viral experiment was initiated by Jon Hepps and John Shock of Xerox PARC. The goal of this new research project was to create worms for divided computer programs. However, a procedural flaw in handling the viruses lead to uncontrolled self-replication, and, in order to avoid an outbreak, the project is terminated.

In 1983, Professor Len Adleman and his computer science student, Frederick Cohen, use for the first time the term “virus” to represent self-replicating pieces of software running in the Apple II environment. Later that year, Adleman[35] demonstrated a piece of software running on a VAX11/750 system, that was able to infect other programs running on the same machine by modifying their object code and “instructing” them to install subsequent copies of itself.

Fred Cohen’s first fully-functional virus was also presented in 1983. It was programmed under the Unix operating system, and affects the VD command. Each time an infected process is triggered; it inherits its system privileges, and then transfers them to each available user.

Another Trojan horse affecting Apple II systems shows up in 1985. Called the **EGABTR**, the new piece of malware claimed it is a graphics utility aimed at boosting the poor video performance available at that time. However, once the “utility” was launched, files stored on the hard disk were

[34] The virus triggered its payload from 50 to 50 boot operations.
[35] Len Eidelmen is considered to be the pioneer of modern computer virology.

completely wiped out[36], while a message displayed on the computer's screen read: "Arf, arf, Gotcha!". Right after the incident, the "Apples" magazine tried to raise users' awareness towards malware by publishing a source code virus for Apple II.

Malware has no geographical limits, and in 1986 two Pakistani computer-shop owners came up with a new virus affecting IBM PC microcomputers. Basit Farooq Alvi and Amjad Farooq Alvi wrote a harmless program that would display their names and addresses in order to gain customers' loyalty[37]. However, the final result was the **Brain** virus, the first MS-DOS threat that infected thousands of computers worldwide.

The **Brain** virus was relatively harmless[38], as it only changed disk name to '© Brain'. However, it is extremely important in terms of malware evolution as it marks the first reference to a "stealth virus". Each time the user attempted to read the infected sector, the virus would only display uninfected data.

Later in 1986, German programmer Ralf Burger unveils the **Virden** virus during an underground computer forum, called the Chaos Computer Club conference. The virus was located itself in the disk's boot sector and is spread by means of boot sector exchange. The new virus only infected COM files, but did not contain a truly malicious payload.

Vienna: Actively Fighting Malware Threats

The **Vienna.636.A** virus marked another important milestone in the malware industry. Its appearance in the wild and its highly infectious potential managed to raise users' awareness towards the increasing security threats. Although the originator is still unknown, it is for sure that Franz Swoboda was the first person aware of the **Vienna.636.A** virus. The global IT community was up in arms in order to identify its creator, and according to those days' reports, Swoboda had received a copy of the virus from Ralf Burger. However, given the fact that Burger's allegations would incriminate Swoboda as the author, the later claimed the contrary, and blamed it on Swoboda.

All in all, Burger sent a copy of the virus to Berndt Fix, who managed to neutralize the virus, which could be regarded as the birth of the antivirus industry[39]. Burger himself published a book called *Computer Viruses: The Disease of High Technology,* which included Fix's disinfection code. Despite the fact that the book aimed at informing users about how viruses spread and infect systems, it had

[36] Instead of recursively deleting the files, the concealed Trojan deleted the file allocation tables on the hard drive

[37] Other sources claim that the two brothers wrote the virus as they got tired of people making illegal copies of the programs sold in the computer store.

[38] Later reports alleged that the virus managed to invade ARPANET (a division of the US Department of Defense) computers and disabled 6000 computers in 1988.

[39] Calling Berndt Fix the world's first antivirus provider may be a long shot, as modern antivirus products not only that disinfect and neutralize security risks, but also offer on-the-fly protection against multiple threats, including unknown viruses and Trojans.

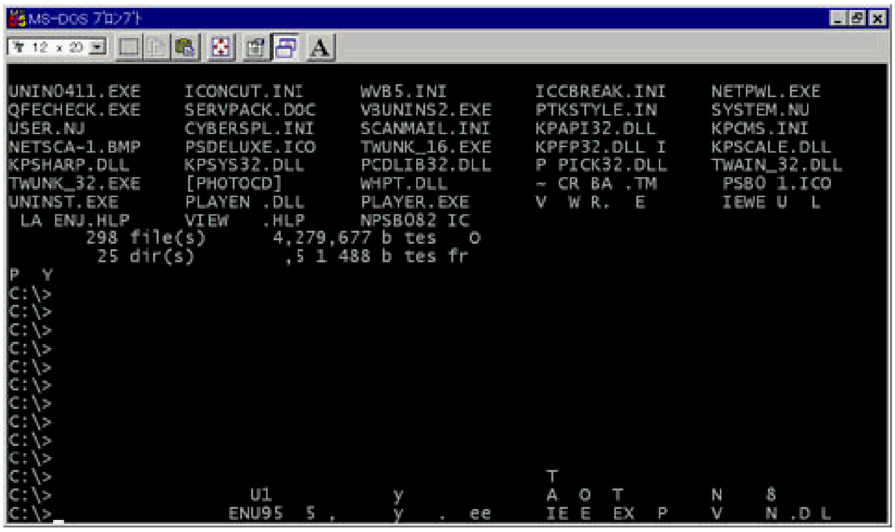
become virus writers' bible, and many new creations have been built based on the enclosed information.

1987 was a prolific year in virus development. Their targets were usually IBM PC-compatible machines, which had enjoyed great popularity among computer users. Apart from a series of generic boot-sector viruses spreading havoc in the United States, New Zeeland and Italy, Three different types of viruses had joined the malware family.

The **Lehigh** virus was firstly spotted in the wild on computers from the Pennsylvania University. Interesting enough, the University is currently known as the home of Len Eidelmen, the father of modern computer virology. The **Leigh** virus is mostly known for its file destructive potential, as it is regarded as the first computer virus to overwrite data stored on disks. It would check a disk each time it is read in order to determine whether the files have already been infected. After the virus infected four files, it started overwriting parts of the disk. Ultimately, the virus would destroy itself along with other files on the disk.

The Leigh University had enough skilled staff to fight and neutralize the virus, and it never left the network to spread into the wild. This is also the first report of a virus infecting command.com files, and computer users worldwide started to pay extra attention to viruses by carefully monitoring the command.com file size, as this was the first symptom of system infection.

Right after the Leigh incident, another computer virus created by an Israeli programmer appeared. Called the **Win32.Worm.Suriv.A** [40], the new virus seems to be more of an accident than a deliberate attempt to cause damage. According to some reports, the Israeli programmer tried to change the process for installing files in EXE format, and unwillingly gave birth to a new breed of viruses.



```
UNINO411.EXE    ICONCUT.INI     WVB5.INI        ICCBREAK.INI    NETPWL.EXE
QFECHECK.EXE    SERVPACK.DOC    VBUNINS2.EXE    PTKSTYLE.IN     SYSTEM.NU
USER.NU         CYBERSPL.INI    SCANMAIL.INI    KPAPI32.DLL     KPCMS.INI
NETSCA~1.BMP    PSDELUXE.ICO    TWUNK_16.EXE    KPFP32.DLL I    KPSCALE.DLL
KPSHARP.DLL     KPSYS32.DLL     PCDLIB32.DLL    P PICK32.DLL    TWAIN_32.DLL
TWUNK_32.EXE    [PHOTOCD]       WHPT.DLL        ~ CR BA .TM      PSBO 1.ICO
UNINST.EXE      PLAYEN .DLL     PLAYER.EXE      V  W R.  E       IEWE U  L
 LA ENU.HLP     VIEW   .HLP     NPSBO82 IC
       298 file(s)      4,279,677 b tes   O
        25 dir(s)        ,5 1 488 b tes fr
P  Y
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>                                             T
C:\>                  U1            y            A  O  T        N    8
C:\>                ENU95  5 ,      y   .  ee    IE E  EX  P    V    N .D L
```

Figure 2: The Cascade virus forced text to be displayed on the bottom side of the window, simulating a waterfall.

However, later in 1987, a modification of the **Win32.Worm.Suriv.A**, also known as Jerusalem, was reportedly destroying all the executable files stored on an infected machine. Its payload only set off on

[40] The name reads "virus" when spelled backwards.

Friday the 13th, all years except for 1987[41]. During the payload sequence, the virus would display a black box (or a black rectangle for text-mode machines), which brought it the "BlackBox" nickname.

The Jerusalem virus was extremely common at that time, and gave birth to a large number of variants[42]. However, as it used to rely on DOS interrupts, Windows systems are no longer vulnerable to the attack.

The year's end brought a new type of virus that forced the industry to start the development of antivirus software[43]. The **Cascade.1701** virus is the first piece of malware able to encrypt its payload[44], and is considered to be the predecessor of polymorphic viruses (pieces of malware that preserve their functionality, but constantly change their program code). However, the payload was rather harmless, given the fact that the virus only displayed a waterfall effect, with letters raining down on the screen. Cascade only encrypted its body, while the decryption routine remained unchanged.

Christmas kicked in right in the middle of a major LAN outbreak of the **Christmas Tree Worm**, a piece of malware that attacked on VM/CMS-9 operating systems. According to those times' reports, the worm started spreading from a West Germany university using the European Academic Research Network (EARN) portal, and had completely clogged the network by December 13th. Beyond its spreading capabilities, the worm also came with a payload that would display a Christmas tree on the computer screen.

Security Experts Start Looking for the Antidote

If 1987 was a huge leap in developing and distributing malware, the worst was yet to come in 1988. As the computer industry started to take off, so did malware writers. The first notable virus outbreak in 1988 was triggered by the **Suriv-3** virus on May 13th. The event is also known as the Black Friday and antivirus companies are still going into full alert each time the 13th of any month falls on a Friday. Suriv-3 infected many enterprises, government offices and academic institutions around the world, but caused extensive damage in the US, Europe and the Near East.

Following the massive infections in 1987 and 1988, a couple of companies stared developing antivirus utilities. However, such small companies with two to five employees would only produce simplistic string scanners, able to detect unique virus code sequences. Basic antivirus software was often bundled with immunizers (pieces of software that modified programs in order to trick viruses into thinking that they had already been infected). Although immunizers were highly efficient for specific

[41] Jerusalem triggered a global outbreak one year later. According to some reports, it unleashed its malicious payload for the first time on May 13th 2008.

[42] There are over 55 variants of the virus on record.

[43] A massive infection with Cascade in the IBM Belgium offices made the company start its own antivirus business. IBM had already started working on an antivirus utility, but it was intended for internal use only.

[44] Cascade's payload was encrypted in order to deter disassembly and detection of the virus' program code.

viruses, they did not offer proactive defense against unknown security threats. Moreover, as viruses started to bloom, antivirus companies were unable to issue immunizers quickly enough for all of them.

Although the vast majority of antivirus products were sold for negligibly low prices, computer users did not rush to get protected. In addition to that, antivirus software could not be updated easily, as the Internet was still in its early days. This meant that new viruses could easily escape string scanners

On April 22, the first dedicated antivirus forum went live on the Usenet network. Called the Virus-L forum, it was founded by Ken van Wyk, Fred Cohen's friend and colleague.

However, virus creators have also begun gearing up for the battle. 1988 marks the birth date of a new type of malware, in the form of a virus construction kit, designed for the Atari ST. The do-it-yourself utility allowed beginner virus creators to easily build viruses with miscellaneous features using a simple and intuitive interface.

Worm.Macos.Macmag.A was the first important computer virus written for Macintosh computers. It also came with a number of programming innovations that made it extremely efficient. It all began in February 1988, when a file Apple's HyperCard software turned up in a Compuserve online forum. When users would download and open it, the file would secretly install a system extension[45] which made the computer display a New Age peace message on every startup. It seems that the virus had been written by Artemus Barnoz[46] (known as Richard Brandow) and Boris Wanowitch, that were the editors of both the Canadian computer magazine MacMag and the "Computer Graphics Conspiracy" New Age publication.

The virus was rather harmless, given the fact that its payload would only display a "peace message" that read:

> ***"RICHARD BRANDOW, publisher of** MacMag, **and its entire staff would like to take this opportunity to convey their UNIVERSAL MESSAGE OF PEACE to all Macintosh users around the world."***

However, the peace message was at least questionable, given the medium the two colleagues used to spread it. The virus went off circulation on March 2nd[47] , when it would appear once and then it would delete itself from the infected system.

History repeats itself, they say, and this seems to have been the case with "**Denzuko.A**", a virus written by Indonesian programmer Denny Yanuar Ramdhani. Just as the **Reaper** would seek and destroy the **Creeper**

[45] The "system extension" is an INIT resource that had been copied into the system folder, which means that a program is automatically executed upon startup.

[46] Although Brandow claimed authorship, he commissioned the programming part to a professional software developer called Drew Davidson.

[47] The date picked by the authors for the final run was not chosen at random: March 2, 1988 was the first anniversary of Macintosh II line. More than that, a coding bug caused Macintosh II systems to crash

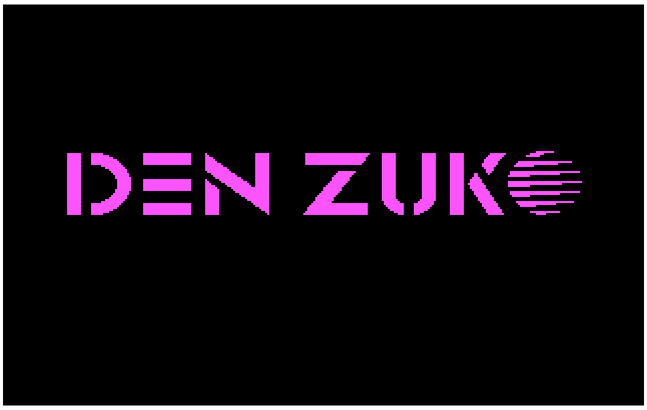


Figure 3: the Denzuko.A virus would display its logo when users would attempt to perform an Alt+Ctrl+Del reboot.

virus in early seventies, **Denzuko.A**[48] would look for instances of the **Brain** virus, then swiftly remove them from the infected computer. However, **Denzuko.A** was more than an antivirus utility, given the fact that it would replace Brain with copies of itself. The virus lay hidden on track 40 on the infected diskettes, but its programmer seems to have made a programming error, since 360KB diskettes only have 39 tracks. More than that, the virus is not able to infect 1.2M or 3.5" diskettes correctly – instead, it would destroy all the stored data on it. Upon successful infection **Denzuko.A** would change the "(c) Brain" label with "YùCù1ùEùRùP" (YC1ERP is Denny Yanuar Ramdhani's screen name).

The first sign of infection with the **Denzuko.A** virus is the fact that pressing Ctrl+Alt+Del will not trigger a simple reboot operation, and the "DEN ZUK" logo would appear on the screen for a small period of time.

The NSA versus Morris: $100 Million in Damage

The most important security incident of the year was triggered by Robert T. Morris, Jr., a graduate student at Cornell University and son of a National Security Agency researcher. He managed to create a piece of software that would automatically self-replicate on all the systems connected to the government's ARPAnet. This was the first time when a computer worm triggered a large-scale security incident[49], and according to the U.S. General Accounting Office, the damage ranged in between $10 million and $100 million, as well as thousands of infected government computers.

Although Morris claimed that he had written the virus with no malicious intention in mind (it was allegedly an experiment that got out of control), he was convicted of violating the 1986 Computer Fraud and Abuse Act and was sentenced to three years' probation, as well as 400 hours of community service to go along with the $10,050 fine.

The increased number of computer viruses and worms called for the establishment of a new anti-malware organization, called the Computer Emergency Response Team / Coordination Center (CERT

[48] The virus is also known as Den Zuk with its Ohio and Hacker variants.

[49] Morris' worm exploited a vulnerability in UNIX operating systems on VAX and Sun Microsystems platforms and would spread without users' help.

/ CC). Founded[50] right after the **Morris** worm struck, the organization is still active and provides security and privacy advisories).

Ultimately, the security industry considered that it was high time they had taken serious measures to defend users' computes, and the first antivirus product[51] was launched. Called **Dr. Solomon's Anti-Virus Toolkit**, the new piece of software was created by British programmer Alan Solomon and enjoyed great popularity among computer users.

1989 came with new challenges for the security industry, and the battle against malware moved to the United Kingdom. The **Fu Manchu** virus, one of the many variants of the **Jerusalem**, was sent to a British virus researcher. Some other researcher anonymously received the 405 virus (that had been largely documented in Burger's book). However, other corners of the world also started boiling under the malware pressure, and some of the first countries to have geared up for the battle were Bulgaria and Russia.

March came with a brand-new computer virus, written by a Dutch programmer called Fred Vogel[52]. He immediately sent an infected file to an UK virus analyst, but did not claim authorship. On the contrary, Vogel said that he had found the virus in all his files on the hard disk. According to him, the virus was called **DataCrime.1168.A** and would trigger on the 13th of the next month.

The British researcher found upon disassembly that **Datacrime's** payload would kick in on any day after October 12th, and would trigger a low level format of cylinder zero of the hard disk. Given the fact that cylinder zero stores the File Allocation Table, this would mean that all the files saved on the respective disk would be completely wiped out. After the low-level format has been successfully performed, the virus would also display its name.

Back in Holland, police authorities had already started looking for the person who wrote the virus, since this was an electronic offense. The police commissioned a programmer to write a detector for the **DataCrime.1168.A** virus, and then sold it for as much as $1 at every Dutch precinct. The new cleanup piece of software sold really well, but it also triggered a couple of false alarms[53], so the detector had to be rewritten.

However, the official involvement of police authorities in the computer world got computer users thinking about how serious the issue was. Small and large companies across Holland went for advice at IBM, as the company had already been working on a commercially-available antivirus utility. The

[50] The CERT/CC is run by the federally funded Pittsburgh based Software Engineering Institute (SEI) at Carnegie Mellon University

[51] Dr. Solomon's Anti-Virus Toolkit hit the market at a time when popular antivirus professionals were skeptical regarding the future of such software products. For instance, Peter Norton thought that computer viruses were more of a myth than of a serious threat, just like the crocodiles living in New York's sewers.

[52] Fred Vogel is an extremely common name in Holland, and can be regarded as the equivalent of the American John Doe. Therefore, details about the person who created the virus are scarce.

[53] The huge number of false-positives actually caused more panic than the virus itself. In fact, there were only a few computers infected with Datacrime, mostly because the virus was non-memory resident, and thus it had limited spreading capabilities.

company had to hurry up and deliver its products until October 12, as many users with valuable information were expected to experience trouble with **DataCrime.1168.A** [54], **Cascade**, **Jerusalem** and the likes.

IBM managed to ship the first version of the IBM scanning software in September 1989, but it was only available for its customers only[55]. Many large companies around the world had performed their first computer scan ever. Although **DataCrime.1168.A** proved to be present in fewer computers than initially estimated, the antivirus software managed to detect and neutralize instances of other common viruses.

Three days later after the **DataCrime.1168.A** outbreak, a new worm started showing up on the the SPAN network. The **WANK** worm only infected VAX/VMS computers. In order to spread from a system to another, the worm used the DECNet protocol. It also came with a payload that changed system messages to read, 'WORMS AGAINST NUCLEAR KILLERS' accompanied by the message, 'Your System Has Been Officially WANKed.' More than that, WANK also changed system passwords to random symbols, and then mailed them to a SPAN network user called GEMPAK.

Three new security risks complete the disaster started by **DataCrime.1168.A** and **Jerusalem**. However, one of the viruses (called **V2Px**, **1260**, **Washburn** or **Chameleon**) has polymorphic[56] abilities, which made it more difficult to detect using simple string anti-virus scanners. Scanning for fixed strings was rendered inefficient, as most of the virus' code suffered important transformations with each successive infection. It seems that the **Chameleon** virus was built on top of the **Vienna** virus, as it was detailed in Burger's book[57].

While the security world was busy with the **Chameleon.1446** virus, a young student at the University of Wellington, New Zealand, had developed a new computer virus. Called the **Boot.Stoned.Elythnia,** the virus would display the message 'Your PC is now Stoned' one time in eight boot-ups from an infected floppy disk. In spite of the fact that the virus was only a few hundred bytes long, its memory-replication feature allowed it to spread at will[58]. Although the **Boot.Stoned.Elythnia** virus was not programmed to inflict any damage to the host system (it was only used as a means to ask for the legalization of Marijuana), there were reports of it having overwrite parts of infected disks that contain directory information or portions of user data files, such as the boot sector of floppy disks along with Head 0, Track 0, Sector 3 on a diskette or the master boot record and Head 0, Track 0, Sector 7 on hard disks.

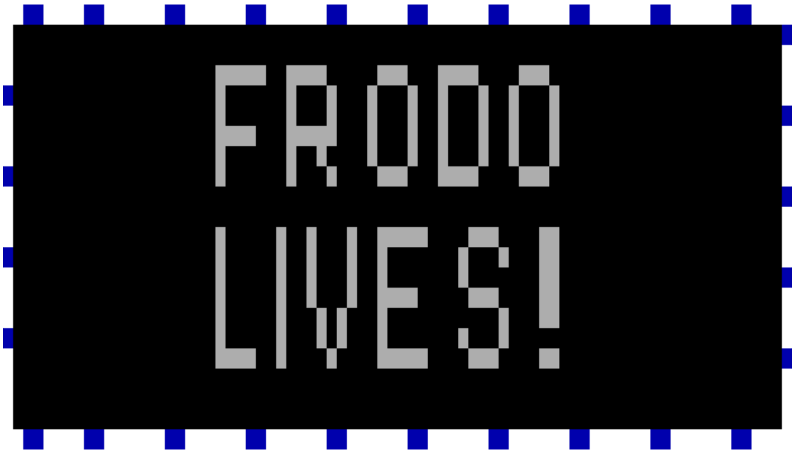
[54] Datacrime is also known as the Columbus Day virus.

[55] The product was called IBM Virscan for MS DOS and could be purchased for only $35.

[56] Polymorphic viruses can repeatedly re-encode themselves, in order to get away from simple string antivirus scanners.

[57] Entitled *Computer Viruses: The Disease of High Technology*, the book aimed at drawing users' attention on computer viruses. Instead, it had quickly become one of the reference books for malware authors.

[58] Some reports claim that Stoned caused a wave of infections that affected about a quarter of tFdehe computers in the world.



FRODO
LIVES!

Figure 4: On each September 22nd, the Frodo virus would display the "FRODO LIVES" message in caps

The **Dark Avenger.1800** virus has been written by a Bulgarian programmer living in Sofia. The **1800** variant would infect a program when its file is being read. This means that any program reading .EXE and .COM files could trigger an epidemic. Moreover, when an infected program is run, there is a 1-in-16 chance that the virus would overwrite a random disk sector. Unlike other viruses, **Dark Avenger** targets backups, not just data: if the user does not notice that data gets corrupted with each overwrite, backups would also get corrupted and useless.

The virus would also intercept any attempt to read infected files, so only the non-infected file will be seen.

Frodo unleashed its payload on September the 22nd, when it attempted to install a Trojan horse on the boot sector. However, the Trojan would only display the message "FRODO LIVES" in large letters on the screen, but some programming errors usually would make the computer hang.

The most important security incident of the year is the **Trojan.Agent.AIDS**, a Trojan delivered by the Panama-registered PC Cyborg Corporation on floppy disks. The disks handled to the participants at an international AIDS conference[59] were supposed to contain important information that had to be installed on hard-disk. However, the End-User License Agreement stated that users who plan to use the data for a long time had to pay a fee of $378.00. Otherwise, the bundled Trojan would encode critical data on the HDD[60]. The company officials have been sentenced and then committed to a psychiatric institution[61].

AIDS is also the first Trojan to spread using mailing lists. Once the system is infected, it then overwrites the beginning of documents and displays the message: “Your computer now has AIDS”. At this point, the infected system usually collapses, and the user has to reboot the computer.

Another type of virus is spotted late in 1989. Called the **Vienna.GhostBalls**, the new virus is the first multipartite piece of malware. A multipartite virus is able to infect multiple different target platforms,

[59] Another version of the story claims that 20,000 floppy disks containing this Trojan were mailed to addresses stolen from PC Business World and the World Health Organization.

[60] The encoding routine is triggered when the program us run for the 90th time.

[61] The software seems to have been created by an American doctor and AIDS researcher named Joseph Papp, who successfully invoked the insanity defense when he was extradited to the U.K. in 1990.

while remaining recursively dangerous in each target. Such examples include viruses comprised of DOS file and PC BIOS boot sector virus code.

In order to fight back the increasingly active malware creators, McAfee released its own antivirus tool. The utility was able to detect and disinfect 44 viruses, an important improvement over IBM's virus-search software, that was only able to detect 28.

The Nineties: Malware Creators Start Building Communities

Writing malware has become more of a fashion during the new decade, and “outlaw” programmers have started building new communities dedicated to such activities. Antivirus manufacturers quickly realized that the rules of the game were about to change in such a manner that string scanners would have been rendered useless. Mark Washburn had already proved that with his polymorphic creations built on top of Vienna. New tricks included encrypting the whole virus, except for a small part to act as decryptor, so in order to efficiently detect malware, antivirus engines had to perform miscellaneous logical tests to the file, the figure out whether the bytes were part of a possible decryptor. The technology involved in such operations was extremely complicated, and would exceed the resources of two- or three-employee antivirus companies. At that time, many security software vendors were heavily relying on third-party search strings delivered by IBM scanner or via the Virus Bulletin newsletter, or even achieved by reverse-engineering competing products.

Polymorphic viruses, however, were playing by other rules, and there was no antivirus available to protect the user from the new threat. To make things worse, Washburn published the source code for its polymorphic creations, and while there were no reports about other viruses using the same core logic, a few malware authors made use of the concept itself.

During the early nineties, Bulgaria was one of the hottest locations for malware writers, as a group of enthusiasts set up the first virus exchange bulletin-board system (BBS). The main idea behind the BBS was to grant malware authors access to the virus code database if they uploaded a new virus. Such rules did nothing but stimulate production of new malware, while their publicly-available source code was being improved.

A couple of new viruses started showing up right after the BBS went online. Most of them came with new features to make them stealthier and more efficient. Some minor viruses, such as **Ping-Pong** (also known as **Bouncing Ball** or **Italian**) only infected the boot sector, and then display a ball bounces across the screen.

Polymorphic viruses were by far the toughest security threats, and the USA witnessed an outbreak as **Virus-90** and **Virus-101** kicked in. Both viruses are written by the same author, who never bothered to conceal its identity. He uploaded the virus to multiple bulletin boards, in an attempt to sell the source code for $20. Its payload is totally harmless, as infected files would only display a message that reads “Infected!” According to the author, the virus is an educational proof-of-concept and not a fully-fledged virus. The **Virus-101** is a variant of the **Virus-90** that adds .exe infection capabilities.

If Virus-90 was quite harmless, the same thing does not apply to the newly-introduced **Anthrax** or **V1** multi-partite viruses, able to infect both files and boot sectors. After it has successfully infected a computer, **Anthrax** would infect .COM and .EXE files, including COMMAND.COM as well as the Master Boot Record (MBR) and diskette boot sectors. It also writes a copy of itself on the last sectors of the system's hard drive, overwriting any data saved at the specific locations. **Anthrax**’s viral code includes text strings written in Cyrillic that allegedly locates its author in Sofia, Bulgaria.

The **Whale** was first spotted in the wild on June 1st 1990. It was an extremely large (hence the **Whale** moniker) and complex virus that was not overly destructive. Instead, it was a new step in the evolution of malware as it came with novel techniques of obfuscation[62] to conceal its presence. The **Whale** took virology by storm, as it could rewrite its own instructions in such a way that it never looks the same way twice. The new virus was also the final challenge for simple string scanners, as they were merely unable to recognize the virus after subsequent infections.

Another security incident took place in July, when the UK-based PC Today computer magazine shipped its issues bundled with a free floppy disc which turned out to be infected with a copy of **Trojan.DiskKiller.B**. According to the company, more than 50,000 copies of the magazine were delivered, and about as many computers have been taken down by the virus. The memory-resident piece of malware copies itself in three distinct blocks onto the floppy disk or hard-disk. These blocks are detected as bad and skipped during the write process.

DiskKiller’s payload kicks in on April the 1st, when the virus displays the following text:

> ***Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/89 Warning!!***
>
> ***Don´t turn off the power or remove the diskette while Disk Killer is Processing***
>
> ***PROCESSING***
>
> ***Now you can turn off the power. I wish you Luck!***

After the message has been displayed, all the data stored on the hard-drive gets either corrupted or encrypted.

[62] The Whale is an armored virus, which means that it uses special tricks to make tracing, disassembling and understanding of its code more difficult

As the first Russian viruses (**Piter.529.A**, **Voronezh.600**, and **Lovechild.2710**) started to show up on worldwide computers, German security researchers set the basis of a new antivirus research organization, called the EICAR (European Institute for Computer Antivirus Research). The Institute is still operational and is regarded as one of the most respected international data security organizations. At that time, there were about 150 known viruses, but the situation looked gloomy as the Bulgarian "Virus factory" took off.

Later in 1990, Symantec unveiled its own antivirus product, called Norton AntiVirus. The new software utility was one of the first security utilities ever developed by a large company.

In 1991, the number of known viruses managed to beat the 300 mark, but their increased number was not the only problem security companies had to face. Viruses were becoming increasingly intricate and destructive, and the huge number of incidents called for professional antivirus products.

Following the Bulgarian model, other malware authors set up virus bulletin boards in Italy, Germany, Switzerland, USA and UK. These new malware hotspots were to become later a fully-fledged underground network. The German underground group called the "Verband Deutscher Virenliebhaber" (Association of German Virus Fans) came up with a construction kit for DOS systems, a do-it-yourself piece of software that allows novice programmers to create new viruses following the specified patterns.

1991 also witnessed the apparition of the first cluster virus in the **Dir-II** family[63]. Unlike conventional infectious malware, cluster viruses infect users' files not by performing changes to the files, but rather by changing the DOS directory information so that directory entries point to the virus code instead of the actual program. This way, the virus would be executed before the desired program. **Dir-II** triggered a fully-fledged epidemic in the summer of 1991.

Computer users did not have the necessary time to recover from the **Dir-II** disaster when Swiss virus **Tequila** hit. The multipartite virus used to infect both the master boot sector and DOS-EXE files, and used full stealth while running on the host system. More than that, its fully polymorphic structure allowed it to bypass even the most complex string scanners, as no piece of its code was identical.

The first antivirus scanners started to catch its instances by May, but it could not be reliably detected until late September. It takes only a few undeleted files to start another outbreak, and the procedure repeats itself until none of the infected files can be detected by antivirus software.

Despite the fact that there were no imminent threats hovering above computer users, this did not necessarily mean that malware creators were fast asleep. On the contrary, they were extremely active and managed to increase the virus count from 300 to more than 1,000 in December 1991. Most of the

[63] Dir-II was using an entirely new method of infecting files: link-technology. Dir-II is the only virus of its kind to have ever been spotted in the wild.

new viruses were written in Eastern Europe and Russia and they would usually serve as currency for other viral source code.

September took the antivirus community by surprise as the polymorphic virus called the Maltese Amoeba started to show up in Europe. At that time, polymorphic viruses were extremely difficult to handle, given the fact that most scanners would require some form of hard coding in order to detect the virus.

The Bulgarian Dark Avenger also made a comeback on the malware scene and announced the first virus vapourware[64]. According to one of his posts, he warned computer users that he would release a piece of malware with more than four billion different variations; the new virus was allegedly slated for release in January 1992. The year concluded with no major security incidents, a calm period to anticipate the upcoming storm.

From Michelangelo to Self-Mutating Engine

1992 debuted straight with a large-scale security threat signed by Bulgarian programmer Dark Avenger. Just as he had promised one year earlier, the virus writer was about to introduce a new mutating algorithm, but he decided to take things smoothly. The first creation to emerge in 1992 was a simple virus, known as **MtE.Dedicated.A**, followed by the **Self-Mutating Engine** (MtE). This Engine was nothing but a polymorphic generator, a tool that could integrate with other viruses to facilitate their code changes. Dark Avenger delivered its creation accompanied by exhaustive documentation, as well as with an OBJ file, plus the source code for a simple virus. The new package made writing malware a lot easier, but at the same time, antivirus researchers also started working on a detector for it.

Security experts estimated that there would be plenty of viruses built on top of the **Self-Mutating Engine**, but malware authors quickly realized that a virus scanner able to detect the **MtE** would easily “catch” all its derivatives[65].

However, the **MtE** was only the starting point for a whole new series of other polymorphic generators that scared out not only average computer users, but many antivirus companies as well.

Right as the **Self-Mutating Engine** hysteria was about to calm down, a new plague hit the industry on March the 6th. Detected since 1991, the **Michelangelo** virus was expected to set off at the respective

[64] The term defines a software or hardware product which is announced by a developer well in advance of its release, but it either fails to emerge or it makes it on the market, but arrives stripped off all its glorious features.

[65] At the moment, there are only a few viruses built with the Self Mutating Engine, which is way less than initially estimated.

date and infect over 5 million machines[66]. In spite of all the fears, the virus proved to be much ado about nothing, as it only managed to infect a few thousand machines only.

Michelangelo was a boot-sector virus that operated at the BIOS level. It would stay dormant until the date changes to March the 6th, the birth of the artist. Although the virus is not associated in any way with the Renaissance artist, it got its name by the fact that it unleashes its payload on the day **Michelangelo** was born.

Another interesting hypothesis assumes that the virus is a variant of the already notorious Jerusalem B (also known as Friday the 13th). Users who think they can fool **Jerusalem** by changing the system date on the twelfth would in fact unleash **Michelangelo**.

This year was also the time when the first anti-antivirus piece of malware was introduced. Also known as **Peach**, the malicious application would look whether the Central Point AntiVirus is already present on the computer, and if successfully detected, it would delete the change inspector database. When the antivirus was unable to locate its database files, it would act as if it had been started for the first time and reconfigure itself. The virus was thus able to slowly but surely infect the entire system without a problem.

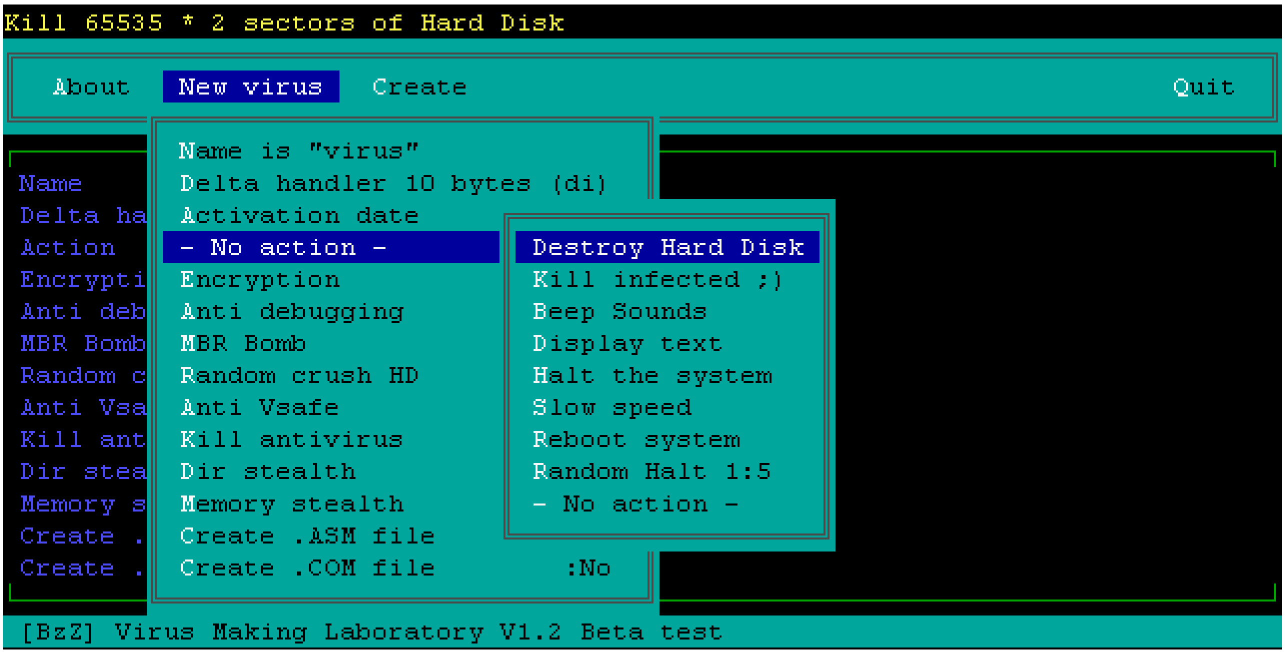
The summer of 1992 brought another wave of concern, as two new virus construction kits appeared on the underground market. The **VCL** (Virus Creation Laboratory) from Nowhere Man and **PS-MCP**[67] (Phalcon/Skism Mass-Produced Code Generator) constructors allowed malware writers to build up security risks by simply adding malicious payloads to the already pre-written constructors. Within a single year, there were a couple of dozen viruses built using the new one-click-virus technology.

Later in 1992, a new malware group appeared in England. The so-called ARCV (Association of Really Cruel Viruses) organization has been hunted down by the newly-established Crime Unit of New Scotland Yard, but in its short-lived history[68], the organization was able to deliver about a hundred new viruses to the world.

[66] The scary estimation pushed almost any PC user into buying specialized antivirus software.

[67] This is another creation of the same Bulgarian malware writer known as Dark Avenger.

[68] It took only three months for the Scotland Yard to locate and arrest the group of malware authors.



```
Kill 65535 * 2 sectors of Hard Disk

  About   New virus   Create                                Quit

           Name is "virus"
Name       Delta handler 10 bytes (di)
Delta ha   Activation date
Action     - No action -           Destroy Hard Disk
Encrypti   Encryption              Kill infected ;)
Anti deb   Anti debugging          Beep Sounds
MBR Bomb   MBR Bomb                Display text
Random c   Random crush HD         Halt the system
Anti Vsa   Anti Vsafe              Slow speed
Kill ant   Kill antivirus          Reboot system
Dir stea   Dir stealth             Random Halt 1:5
Memory s   Memory stealth          - No action -
Create .   Create .ASM file
Create .   Create .COM file              :No

 [BzZ] Virus Making Laboratory V1.2 Beta test
```

Figure 5: The Virus Making Laboratory was an extremely popular utility that allowed newbie malware creators to spawn new viruses without having to write any code.

Moreover, selling malware has quickly become a fully-fledged business, as a couple of underground programmers started selling virus collections. For instance US resident John Buchanan offered his collection of a few thousand files for as much as $100, while the European Virus Clinic would allow its customers to pick the desired malware for about $25. Given the fact that the Virus Clinic was located in Europe, it got a visit from the Computer Crime Unit and got shut down thereafter.

Another kind of virus made its debut in 1992, as the Microsoft Windows operating system gained ground among computer users. The **Win.Vir_1_4** was world's first virus designed to attack operating system executable files. Even though its author had made some programming mistakes that rendered it rather harmless, it is an important step in the evolution of malware as we know it today.

1993 was mostly under the threat of polymorphic viruses generated by a wide range of polymorphic generators and constructors. More than that, they started multiple electronic magazines dedicated to writing and spreading malware. The increasing amount of stealth viruses made it clear that malware authors had quit vandalizing for fun and planned their creations to bring them as much gains as possible.

The new year brought the **PMBS** virus which worked in the secure regime of Intel 80386 processors. This dangerous, memory-resident boot virus copied itself into extended memory, then switched the infected system into protect mode and run virtual V86 machine. In different situation, the computer would hang with an error. Although the virus itself contained some programming errors, it was yet another threat available in the wild.

A new malware community was established in Holland under the Trident moniker. Its members came up with a new polymorphic engine called the **Trident Polymorphic Engine**, and then with a fully operational virus (**TPE.Girafe**). The **Trident Polymorphic Engine** was harder to detect using antivirus scanners, that usually would trigger false alarms. It seems that the main Trident programmer, Masouf Khafir, built its **BAT.P2P.Cruncher** virus following the principles described by Fred Cohen. The **BAT.P2P.Cruncher** was a data compression virus that automatically appended its code to other files in order to auto-install on as many computers as possible.

Nuke member Nowhere Man released the **Nuke Encryption Device (NED)**, another mutation engine that seemed to work even better than Dark Angel's **Self-Mutating Engine**. **Itshard** was the first virus built using the new mutation technology.

On the other side of the fence, the antivirus industry released the first wild list, comprised of all the viruses that had been spotted "in the wild[69]". Another major achievement in the battle against malware is the release of the GDE (Generic Description Device), a complex tool able to recognize polymorphic viruses.

Early in spring, Microsoft starts its own antivirus business, called Microsoft AntiVirus (MSAV). The new product was based on the former Central Point AntiVirus (CPAV) and was bundled with the company's MS-DOS and Windows operating systems. Although in its early days the product had been rated as highly effective, it could not keep up with the upcoming security challenges and was ultimately discontinued.

New Removable Media gives Malware a Boost

Most of the security issues in 1994 were triggered by the increased popularity of removable media, especially the more and more affordable CD-ROMs. Such storage devices acted as a vector of infection, as computer users burnt not only important data, but also infected files. A couple of CD producers unwillingly distributed already-infected products, and the situation got even more complicated as read-only disks could not be disinfected.

A new outbreak of polymorphic viruses occurred in the United Kingdom. **SMEG.Pathogen** and **SMEG.Queeg**, two extremely dangerous viruses had been uploaded on a couple of BBS boards by their creator[70], and although their malicious potential was limited, mass-media fueled computer users' panic.

Hoaxes also gained popularity, and one of the best examples is the **GoodTimes** hoax. It allegedly spread via the Internet and could infect computers by simply receiving an e-mail message. The hoax was followed by a DOS virus containing the text "Good Times", which also caused panic, but it was nothing if compared to the upcoming threats.

[69] "In the wild" viruses are actively infecting production systems across the world and try to replicate in live environments. This category is opposite to the so-called zoo-viruses, pieces of malware that are built inside laboratories for educational and research purposes.

[70] Shortly after the incident, Scotland Yard arrested the author - Christopher Pile, also known as Black Baron.

In June, an extremely complex and dangerous polymorphic virus called **One-Half** caused a new epidemic. The new DOS-based polymorphic piece of malware came with a peculiar payload that would encrypt a certain part of the hard-disk drive, in order to perform on-the-fly decryptions when the user accessed the affected files. However, when the system is disinfected and the virus is deleted, the encryption process can not be reversed. When the virus has successfully encrypted half of the drive, it displays the following text:

> ***Dis is one half.***
>
> ***Press any key to continue ...***

The One-Half virus may be more than a decade old, but it is still active and continues to infect unprotected systems around the world.

Another significant battle was carried against a Russian virus called **W97M.Zaraza.A**. Its name is an Anglicized version of the Russian 3APA3A (“infection”). The new virus managed to take the antivirus world by surprise thanks to a new mode of concealment. It replaces IO.SYS with its own routine in order to get memory access and avoid detection. The **W97M.Zaraza.A** unleashes its payload in August, when it displays the following message:

> ***B BOOT CEKTOPE - 3APA3A***
>
> ***(" There is an infection in the boot sector ")***

1995 was much calmer than the previous years on the security scene. While MS-DOS viruses kept increasing in both count and infection potential, no major outbreak was reported to have occurred. A couple of complex DOS viruses virus such as **Nightfall**, **Nostradamus**, and **Nutcracker** surfaced on miscellaneous BBS boards, as well as the RMNS virus and the **Winstart** .BAT-infector. **ByWay** and **DieHard2**, two new types of malware managed to find their way into a couple of systems but failed to cause an epidemic.

Believe it or not, but Microsoft managed to succeed where most of the malware authors failed. Their new operating system - Windows 95 - was shipped to worldwide beta-testers on floppy disk drives. Probably excited by the new computing environment at their fingertips, beta-testers forgot to comply with the most elementary protection rules regarding data security and proceeded with the installation. It appears that Microsoft had shipped virus-infected floppy-disks. Testing had to be postponed until the company came up with clean disks.

A couple of months later, the Microsoft Word text processor was hit by a new type of virus, called **Concept**. The new macro virus infected Microsoft Word documents and managed to spread across the globe in less than a month. **WM/Concept** was the first virus specifically written for the Microsoft Word system and discovered "in the wild".

As its name suggests, the virus was a proof-of-concept only and had no harmful payload. Instead, the text contained in the virus read “That’s enough to prove my point”. In spite of its low security risk, Concept become on of the most common viruses on the planet.

One month later, a top-tier computer manufacturer called Digital Equipment Corporation (DEC) accidentally distributed copies of the **Concept** virus to the attendees at a DECUS conference in Dublin. The damage was minimal, as the presence of the Concept virus was quickly detected. Macro viruses, however, set the antivirus industry on fire, as there was no existing technology capable to detect and disinfect the new threats.

Another security incident was triggered by Computer Life, a Ziff-Davis publication that sent its customers diskettes containing a Christmas greeting. However, all the shipped disks were infected with the **Parity Boot virus**, and many customers have been affected. This was not the only security incident triggered by a Ziff-Davis publication. The English version of PC Magazine also delivered diskettes infected with the **Sampo** virus. The security risk has been discovered later, and the company apologized for inconvenience. More than that, in order to keep its users safe, it offered a free antivirus utility.

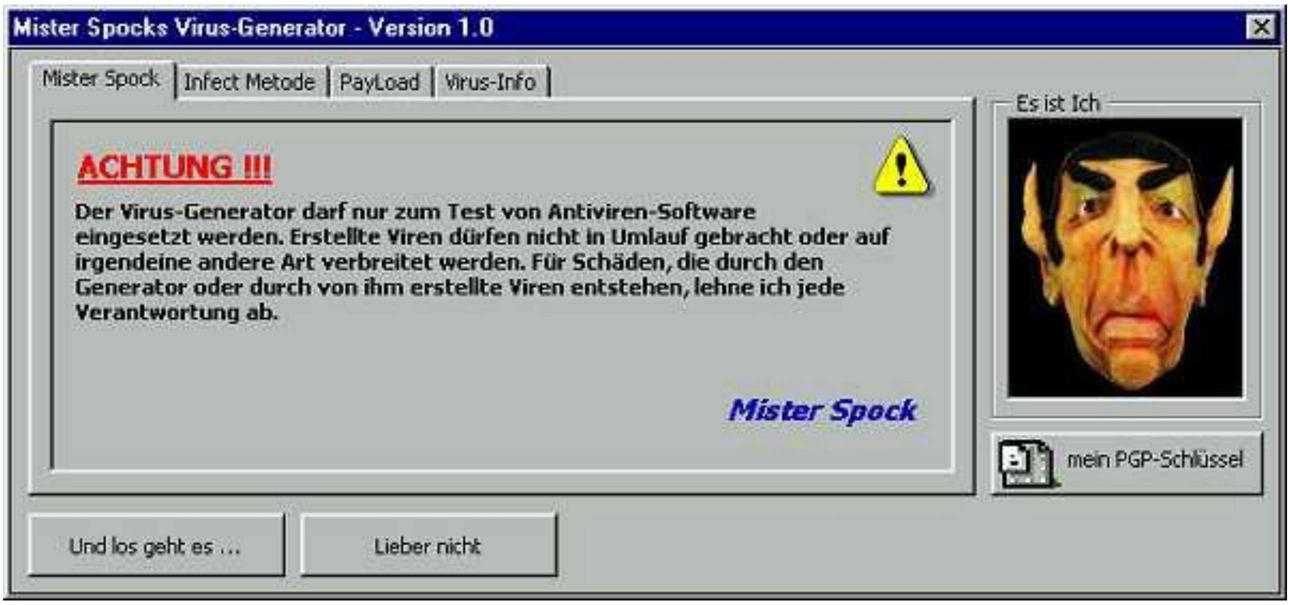
Cyber-criminals continued to receive visits from Scotland Yard. Christopher Pile, the author of the **SMEG.Pathogen** and **SMEG.Queeg** polymorphic viruses was arrested for writing and distributing viruses. Later that year, he was sentenced to 18 months in prison.

In 1996, Microsoft’s new operating system – Windows 95 – started to gain significant ground among computer users. As it was expected, more and more malware writers shifted their focus to the new environment, but the older Windows 3.x systems have not been spared.

Two new viruses started to decimate computers worldwide in early 1996. The first virus to hit was called **Borza**, followed immediately by **Zhengxi**, a polymorphic virus written by Russian programmer from Saint Petersburg Denis Petrovym. **Borza** originates in Australia and was apparently written by Quantum, a member of the VLAD virus programming group. Each time an infected program starts, it would search for up to three executable files which have not yet been infected, then append its code. **Borza** was a low-risk virus, given the fact that it would only display a message regarding its creators on the 31st of each month.

Early in March, the **Win.Tentacle** virus slammed Windows 3.x systems and caused the first virus epidemic for the respective operating system. Tentacle was able to infect a hospital computer network as well as other organizations in France. At the same time, it was the first Windows virus detected in the wild.

Another extremely interesting piece of malware was the **Esperanto** virus, a multi-platform infector that has the ability to adjust its code depending on the operating system. It could infect both Windows and Macintosh systems. It appears that its creator is the notorious Spanish 29A virus programming group, which also designed the **WM.CAP** macro virus.



ACHTUNG !!!

Der Virus-Generator darf nur zum Test von Antiviren-Software eingesetzt werden. Erstellte Viren dürfen nicht in Umlauf gebracht oder auf irgendeine andere Art verbreitet werden. Für Schäden, die durch den Generator oder durch von ihm erstellte Viren entstehen, lehne ich jede Verantwortung ab.

Mister Spock

Figure 6: Virus generating applications gain popularity among less skillful malware developers.

As it was expected, malware authors started to build on the Microsoft Word macro virus, and they quickly came up with another piece of malware able to infect Excel files. Called the **Laroux**, the new creation was first spotted in July at two oil drilling companies in Alaska and South Africa respectively. The author took advantage of the Visual Basic programming language embedded in Excel. **Laroux** triggered a new epidemic in Moscow in April 1997.

Summer ended with the advent of two new constructors for macro viruses that would expose both the English and German versions of MS Word. Called the **Word Macro Virus Construction Kit** and **Macro Virus Development Kit**, respectively, the new malware creations were attributed to two virus writers called Nightmare Joker and Wild Worker.

Later in 1996, Microsoft's website was reportedly serving **Wazzu** macro-infected Word files containing support instructions for Microsoft products in Switzerland. The same virus managed to infect Microsoft Solution Provider compact discs, as well as other CD-ROM media distributed by the company during the Orbit computer technology exhibition in Brazil.

The year ended with a massive outbreak triggered by world's first memory resident Windows 95 virus. It loaded into the system as a VXD driver, and then it intercepted file calls, in order to infect them.

Linux users were still unaffected by malware, although the first virus (**Staog**) had been developed in laboratory conditions for research purposes only. It never left the secure environment, and there were no reports about its presence in the wild ever.

The advent of Microsoft's new operating system marked the beginning of a new wave of attacks with both Windows 95/NT viruses and macro viruses. During the entire year, malware authors managed to improve their portfolio with more than over a hundred macro viruses and dozens of viruses for Windows 95/NT. Given the fact that the main targets were 32-bit operating environments, the antivirus industry quickly geared up to deliver appropriate protection[71].

1997 made its debut with world's first Linux virus spotted in the wild. The **Bliss** virus only affects Linux-based operating systems and is the second known virus to affect this platform. It only infected Elf-style executables, and although it surely has a malicious payload, it is unsure whether it is executed or not. It also has some basic worm-like features, looking for new hosts to infect via the /etc/hosts.equiv file.

Bliss also searches for programs for which the current process has write permission, and then it overwrites them with its own code, which means that all the information contained in the infected file is instantly destroyed.

One month later, the **ShareFun** macro virus for MS Word 6/7 triggered a new wave of worries among computer users. **ShareFun** became the first piece of malware to spread using e-mail messages, especially if the infected computer was using the MS mail service.

The **Homer** virus arrived in April 1997 and marked a new milestone in the development of malware. The new virus had an interesting way of propagating from one system to another, namely by using the FTP protocol to make the "jumps".

Self-encrypting viruses made a comeback in June, this time especially designed for the Windows 95 operating system. The first such virus was known as **Win95.Mad**, a piece of malware that seems to have originated from Russia. The virus triggered a major outbreak, as it was found on almost any BBS system.

Malware found a new channel to spread at will with the appearance of mIRC (Internet Relay Chat). The first mIRC worm emerged in December - it was a fundamentally new type of malware that exploited a dangerous security loophole in the structure of IRC channels. Files downloaded using the IRC service were stored in the same directory that contained the script.ini command file. This way, an infected script.ini file would facilitate the worm's spread to other remotely located computers.

The security hole has been quickly patched, and many early IRC worms disappeared from the scene. More advanced worms would actively search for the script.ini file in order to infect it.

[71] Cheyenne Software developed InocuLAN, an antivirus utility that was eventually bought by Computer Associates.

1997 also marked the beginning of a new age for malware writers. Microsoft managed to implement the Windows Scripting Host technology in order to meet its customers' demand for a more flexible working environment, but at the same time, it opened new opportunities for applications relying on VBScript. Malware was no exception to the rule, and took full advantage of the new environment[72].

The malware scene in 1998 evolved at a steady pace. However, the quality of the new types of malware has improved dramatically. The new threats have been redesigned to make full use of the spreading capabilities offered by the Internet and IRC channels. The first malware threat to hit in 1998 was a new family of viruses called **Win32.HLLP.DeTroi**. They would infect Win32 executables, but at the same time, they would also send critical information about the infected systems to their author. However, the virus exploited system libraries only available in the French distribution, which dramatically limited its infection potential on systems with different localization.

Another macro virus written for the Excel component of the Microsoft Office package started infected users' files in February. Known as **Excel4Paix** or **Formula.Paix**, it would install its code into tables by using a less common macro area of formulas. The Excel macro was almost immediately followed by a similar piece of malware that affected Access databases. **Access IV** was the first virus for Microsoft Access files, but it failed to trigger a security incident. **Cross** was another macro virus, but this time, it was able to infect both Word and Access files. However, the most complete macro virus was to be known as **Triplicate** or **Tristate** – a piece of malware that could infect Word, Excel and PowerPoint documents.

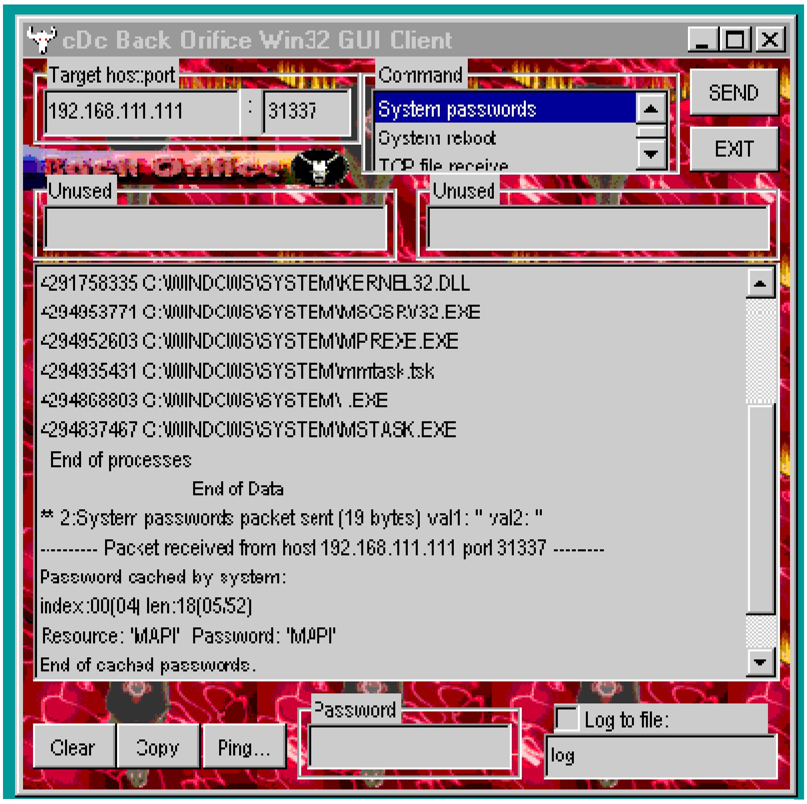
May brought another virus, known as the **Read Team**. Although it was clearly a virus, it could spread to other systems by attaching itself to e-mail messages sent using the Eudora mail client. **Red Team** could infect Windows EXE files by remaining resident in the Windows memory. Other exe files were infected as they got executed.

The most important security incident of the year was triggered by the apparition of the **Win95.CIH** virus, also known as **Chernobyl**[73]. The virus caused a worldwide outbreak with thousands of infected computer in both home and corporate environments.

It is believed that the epidemic originated in Taiwan, where a malware author sent the first copy of the virus to a local electronic list-serve. However, the virus subsequently spread via game servers. The disaster caused by **CIH** exceeded by far any other security threat since the beginning. The virus could trigger multiple scenarios, depending on the infection day. Users could end up with an erased Flash BIOS chip, and many of them had to replace their motherboards. The antivirus industry was taken by surprise and had to rush the development of detection and disinfection tools in order to avoid a disaster.

[72] This is the case with the LoveLetter internet worm, as we will discuss later.

[73] One year later, the Taiwanese authorities identified its author as Chen Ing Hao, a student at the Taiwan Technical Institute. His initials were allegedly used to name the virus, but, due to a lack of charges from any of the local companies, the police could not arrest him.



cDc Back Orifice Win32 GUI Client

Target host:port 192.168.111.111 : 31337

Command: System passwords

```
4291758335 C:\WINDOWS\SYSTEM\KERNEL32.DLL
4294953771 C:\WINDOWS\SYSTEM\MSGSRV32.EXE
4294952603 C:\WINDOWS\SYSTEM\MPREXE.EXE
4294935431 C:\WINDOWS\SYSTEM\mmtask.tsk
4294868803 C:\WINDOWS\SYSTEM\ .EXE
4294837467 C:\WINDOWS\SYSTEM\MSTASK.EXE
 End of processes
                   End of Data
** 2:System passwords packet sent (19 bytes) val1: '' val2: ''
--------- Packet received from host 192.168.111.111 port 31337 --------
Password cached by system:
index:00(04) len:18(0552)
Resource: 'MAPI'  Password: 'MAPI'
End of cached passwords.
```

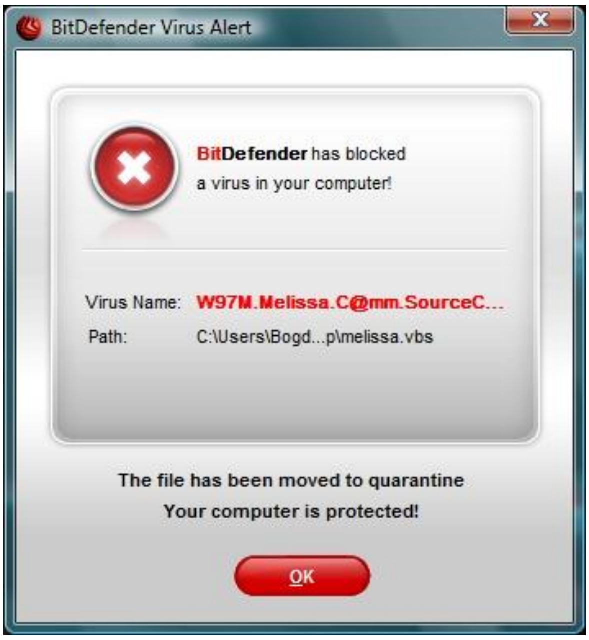
Log to file: log

Figure 7: Initially designed as a remote access tool, the BackOrifice utility was mostly use by hackers to seize control over victims' computers.

Computer users did not even have the time to recover from the previous attack that the next wave of malware kicked in. August 1998 witnessed a controversial security threat known as **BackOrifice** (or **Backdoor.BO**). It is alleged that the backdoor was left open on purpose, as a secret utility to allow remote host administrators to control miscellaneous machines across networks. Named after a legitimate piece of software produced by Microsoft (BackOffice Server), it was the creation of Sir Dystic, a member of the U.S. hacker organization CULT OF THE DEAD COW. He allegedly claimed that he had written this small and unobtrusive piece of software to demonstrate how unsecure Windows 98 really was.

Although the Trojan could be legitimately used for remote administration, it was also used by malicious people with no respect to users' privacy. For instance a computer infected with **BackOrifice** could be totally and stealthily controlled by a remote attacker. More than that, the server could be deployed as the payload of a Trojan horse.

The newly-introduced Windows Scripting Host system implemented in Windows 98 gave malware authors a new playground for their illicit activities. The first VB script virus, known as **VBS.Rabbit** did not cause too much damage, yet it was extremely annoying and offensive to the infected computer user. Once the virus has successfully infected a computer, it starts looking for additional .vbs files, then prepend its code to each file. Although the .vbs files can be used after they have been infected, each opened file will trigger another infection. The payload kicks in on the second day of each month between nine and ten o'clock, when the virus searches for all texts containing ".txt - and .doc" extensions, and then replaces their content with obscene drawings in ASCII code.



BitDefender Virus Alert

BitDefender has blocked a virus in your computer!

Virus Name: W97M.Melissa.C@mm.SourceC...

Path: C:\Users\Bogd...p\melissa.vbs

The file has been moved to quarantine

Your computer is protected!

Figure 8: Melissa was one of the fastest-spreading mail worms ever

The **HTML.Internal-Virus** is also based on VBS, but only works when the user accesses infected pages using Internet Explorer. If the user lands on a website which has been infected by the virus, the VBS code would inject text messages in any HTML document stored on users' machines.

While Win32 and VBS viruses were already a common threat in 1989, the **StrangeBrew** virus was a different type of malware able to infect Java files. When executed locally, the virus would spread from one Java applet / application to another by searching for existing .class files, and then appending its code to the found files.

Another interesting feature of the **StrangeBrew** virus is interoperability. Java is a cross-platform programming environment, which means that the virus could infect Linux, Windows or even PDA devices with the Java environment installed.

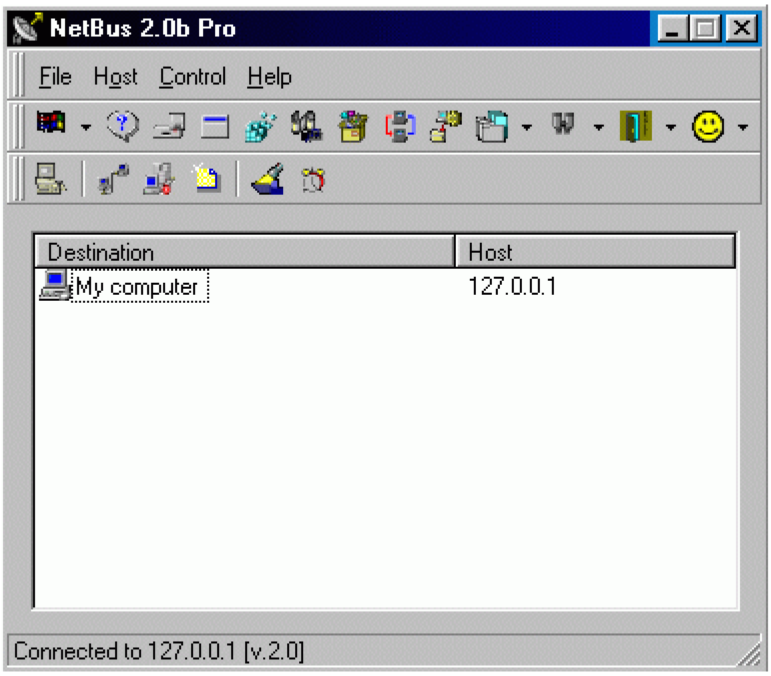
Microsoft's PowerPoint application was about to fall victim once again in December with the advent of a virus of unknown origin, named **P97M.Vic.A**. The series of threats continued with **PP97M.Shaper.A** and **PP97M.Master.A**, two different viruses that probably belong to the same author. **P97M.Vic.A only infected** the "User Form", which is attached to a command button. Each time the button was pressed, the virus would start infecting all PowerPoint documents saved in C:\My Documents. PowerPoint viruses forced antivirus companies to rethink their strategy: as VBA modules in PPT documents are stored in compressed format, the industry had to find a new algorithm to allow scanners decompress them prior to searching them for viruses.

1999 brought quite a few new (and extremely dangerous) viruses and worms, built on top of the previous threats. The first security incident of the year was triggered by the **Win95.Worm.Happy99.A** virus[74] (also known as **Ska**), which can be called the first modern Internet worm. In order to spread from a system to another, it used the MS Outlook mail client

W97M.Melissa.A took the same approach as its predecessor (**Win95.Worm.Happy99.A**) but it caused much more panic and damage to the users. It had both virus and worm capabilities as it infects Word documents, then sends itself as an e-mail message to 50 addresses in the Outlook address book. Apart from its high infection rate, the increased e-mail traffic caused a large number of mail servers to crash. The virus spread not only among average computer users, but it also affected large corporations, given the fact that Outlook had become the industry standard for sending

[74] The antimalware industry is still arguing whether Happy99 is a virus, a worm or a Trojan horse, because its combines all the features.

messages. It appears that the original author of the **Melissa** virus was David L. Smith, a New Jersey computer programmer. When the police paid him a visit at his residence, he admitted everything[75].



Connected to 127.0.0.1 [v.2.0]

Figure 9: The Netbus 2 Pro utility was able to infect even NT-based operating systems.

Canadian software company Corel faced a new security risk as the **CSC.CSV.A** virus snuck its way into the corporate network. **CSC.CSV.A** was written in the Corel SCRIPT language and would infect Corel DRAW, Corel PHOTO-PAINT and Corel VENTURA files.

Backdoor Trojans made a comeback on the market, this time as commercial software. **Netbus 2 Pro,** a remote access server utility similar to **BackOrifice** was released as a fully legitimate piece of software. Its author, Carl-Fredrik Neikter, asked antivirus vendors to prevent their products from reporting it, but they refused the “offer” and included a detection routine to prevent further abuses.

“Blacklisting” **Netbus** was the right decision, as it caused extensive damage to some users. For instance, in 1999, **NetBus** was used to plant child pornography on the work computer of Magnus Eriksson, a law professor at the Lund University. When the system administrator discovered “his” collection of 3,500 pictures, Eriksson was fired. Moreover, because of the media scandal that discredited his name, he was forced to leave the country and seek professional medical care to cope with the stress. When authorities found out that he had been used as a “secret stash” by a third party, the damage was beyond repair[76].

In the meantime, The Cult of the Dead Cow updated the **BackOrifice** code in order to make the software compliant with the NT environment. The malware team demonstrated the new version at the DefCon conference in Las Vegas.

A new virus outbreak was triggered in summer by the dangerous Internet worm **ZippedFiles** (**ExploreZip**). Once installed on a system, the virus would start deleting files associated with popular applications. Although the worm failed to match **Melissa** in terms of infection, it is estimated that it caused seven times more damage, as it completely wiped out users’ critical data. The quick response

[75] On December 9th, he was found guilty and sentenced to 10 years in prison. He also had to pay a fine of $400,000 – a high price for what was supposed to be an experiment.

[76] He was acquitted from criminal charges in late 2004.

from antivirus vendors did not stop its expansions; **ZippedFiles** struck again in December and caused further damage to the users. The comeback was possible mostly because its authors changed the virus body in order to bypass the scanners. In order to succeed, he packed the virus with the Neolite compression utility. As a result, antivirus manufacturers included a detection routine for any file packed with the utility.

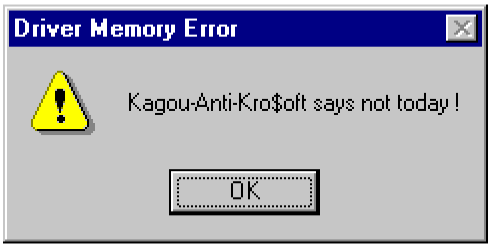
Mixing virus and worm features in a single deadly cocktail has become the main trend in the malware industry. A new Internet worm, called **Toadie** (also known as **Termite**) started infecting both DOS and Win32 executables, while sending copies of itself to other systems using the Pegasus e-mail client. Moreover, it also tried to send itself using IRC channels, but this approach did not quite pay off.

In early October, security researchers discovered the first virus affecting Windows NT platforms. Although **WinNT.Infis.4608** was the first virus of this kind, it was extremely well coded and managed to integrate itself into the highest security level of the Windows NT OS. The virus acted as a Windows driver, which means that NT would automatically load it before the OS performs any security check. The damage inflicted by the new virus was minimal, given the fact that it was rather harmless.

Microsoft Project users were slammed by another security threat in the form of a multiplatform virus that also infected MS Word documents. Called the **O97M.Corner.A**, the new virus would set the Office 2000 security settings to low[77], disable the "Tools/Macros" menu and turn off the macro virus protection before infecting all the opened files.

A new script virus, called **Freelinks**, was spotted in the wild in October. At that time, it did not enjoy extensive attention, mostly because of its low infection potential, but it was to become popular in the light of a tough security threat brought by the **Win32.Loveletter** worm.

Despite the fact that the year was about to end, malware authors still had a surprise up their sleeve. In November, a new generation of computer worm started spreading havoc among computer users. If Internet worms usually require the user to download and execute a specific attached file in order to infect the host, the new **Win32.Vbs.Bubbleboy.A** worm could penetrate a computer when infected messages were previewed or read. In order to infect the system, the worm relied on an Internet Explorer loophole. Microsoft issued a fix to address the hole extremely quickly, yet another such worm, known as **Win32.Vbs.Kakworm** continued to exploit the same vulnerability for a few months.


Driver Memory Error

Kagou-Anti-Kro$oft says not today !

Figure 10: The Kakworm exploited the same IE security loophole as the Bubbleboy VBS script.

The millennium finally ended with yet another disaster, triggered by the extremely dangerous **Babylonia** virus. The complex piece of malware originated in Brazil and was the creation of a prolific Trojan writer known as Vecna. **Babylonya** was the first computer virus able to update itself using a

[77] The virus was unable to infect Word 200 files unless it successfully changed the security levels to "low".

remote server. Basically, the virus would connect from time to time to a server located in Japan, and then look for a newer version of itself. If he found new modules, it would proceed with the download and update.

The Modern Ages: Y2K and the Digital Apocalypse

During the last days of 1999, rumors about a massive worldwide attack from underground malware communities started spreading on miscellaneous BBS systems. Some “experts” even claimed that the new millennium would bring hundreds of thousands new viruses to infect all the systems on Earth at once, thus triggering a digital apocalypse. Antivirus manufacturers rushed to ensure computer users that there were no reasons to fear of a massive viral attack.

As the new year arrived, the apocalyptic forecasts proved false: it is true that the new year brought fresh security threats, but malware evolved at a steady pace, just like in any other year. It is alleged that the Y2K virus hysteria started as a misguided description of the Y2K problem itself. It was true that the global IT community was waiting to see how computers would react when the system clock turned to 1/1/00, but announcing devastating viral infections was a long shot.

The much-hyped Y2K viruses even included viruses that had been developed in mid-90s. Not only were they old, but none of them was Y2K-compliant. Worldwide media outlets embraced the idea of a digital apocalypse, but journalists are not the only ones to blame. For instance, FBI NIPC director Michael Vatis and CIA analyst Terrill Maynard almost triggered an international incident when they claimed that hackers, spies, and the mafia inserted malicious code in U.S. corporate software while they were supposed to "fix" Y2K software glitches. They especially accused India and Ireland of staging the attack on US-based computers, but they later admitted that they relied on suppositions rather than on facts.

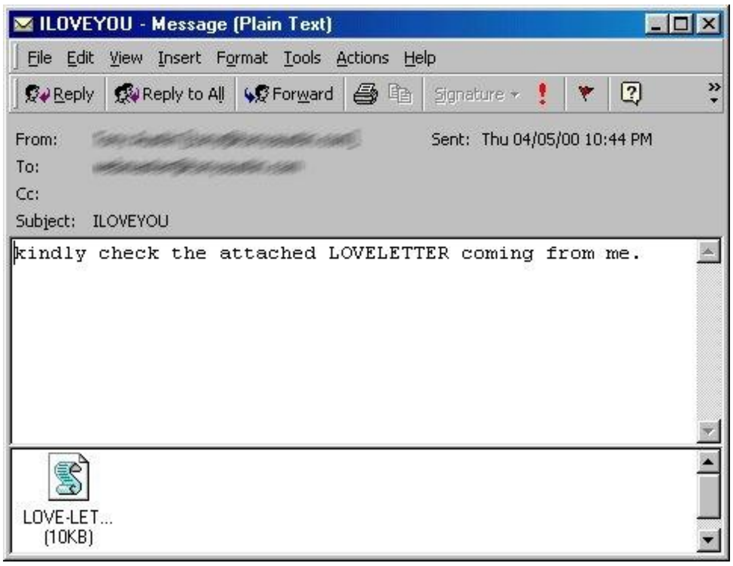
Microsoft’s new operating system called Windows 2000 had been marketed as one of the most secure and impenetrable environments ever built by the company. While this was true to a certain extent, underground malware group 29A (the Spanish team that had previously designed the **Esperanto** virus and the **WM.CAP** worm) came to prove the contrary with **Inta**. It was the first virus[78] spotted in the wild, able to infect Windows 2000 files packed with the Windows Installer.

Two new computer viruses, called **VBS.Unstable.A** and **Visio.Radiant.A** followed shortly after **Inta**. The new pieces of malware aimed at Visio users, an extremely popular and efficient application that allowed users to create eye-candy diagrams and flow-charts for business use. Rumor has it that Microsoft itself was behind the **VBS.Unstable.A** and **Visio.Radiant.A** epidemic, as shortly thereafter, it purchased Visio Corporation along with all its intellectual assets.

[78] Inta actually appeared long before Microsoft got the chance to introduce the new operating system.

In mid-February, multiple computer networks had to face their worst nightmare: one of the biggest denial-of-service attacks to date. It all started with a Canadian computer user nicknamed MafiaBoy, who started a distributed denial-of-service[79] (DDoS) attack against a couple of top-tier websites such as Amazon, CNN and Yahoo! As a result, Yahoo was taken offline for about 8 hours and lost several million dollars in operational loss. In order to successfully carry his plans to completion, the teenager used a network of compromised computers and coordinated a massive Ping-of-Death[80] attack. Mafiaboy was taken into custody and was sentenced to eight months detention by a Canadian judge in Quebec. He also had to pay a fine of only $650.

Another macro virus, called the **WM97M/Proverb.A**, appeared in April. It seems to have originated in Russia, and its first target might have been the office of the British prime minister himself. The **WM97M/Proverb.A** virus was rather harmless, and probably was designed as either a hoax, or for mere entertainment. The virus body contained a piece of code that would check for the version number of the Word processor. If it returns eight, the virus then would fire up the Office Assistant, then display random messages, including animations and headings. If the returned value is different from eight, then it would show a message box and a Russian proverb.



From: [redacted] Sent: Thu 04/05/00 10:44 PM
To: [redacted]
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Figure 11: The LoveLetter worm took advantage of users' curiosity in order to infect hosts and spread to other computers.

All hell broke loose on May the 5th. The new **Win32.Loveletter** (a.k.a. The Love Bug) script virus with worm functionality was about to set a world record in the history of malware. The virus exploited common and native characteristics of the human computer users such as curiosity and adventure spirit, and managed to catch them by surprise. More than that, in spite of all the efforts carried by the antivirus industry to educate users about the malicious potential of VBS and txt files many of them fell for the trick.

The VBS-based virus would distribute itself to every contact in the Outlook address book as well as to persons using the popular mIRC service. It comes disguised as an anonymous love letter (hence its name) and advises the human operator to run the attached .VBS file for further details about the

[79] A DDoS attack sends false requests for service from multiple locations so frequently that the attacked websites are overloaded and unable to answer legitimate traffic requests.

[80] This type of attack was the beginning of the DDoS era and it took the entire world by surprise. Nowadays' networking technology includes built-in protection against Ping-of-Death threats, so such incidents are no longer possible.

sender. Once installed onto the system, it starts replacing files with set extensions (vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, mp2) with its own copies. The infection is carried not only on local hard-disks but also on all drives mapped to the compromised computer, such as network drives.

As part of the payload, **Win32.Loveletter** will attempt to download a file called WIN-BUGSFIX.exe from the Internet, a password-cracking utility that steals passwords from the entire network, and then send the collected data to the author in the Philippines.

The source code has been already posted on several BBS systems, in order to facilitate the appearance of new modifications over time. At the moment, there are more than 90 variants in the wild. **Win32.Loveletter** was also the most damaging virus in the history, causing loses of between 5.5 and 10 billion.

June 6th brought the first computer virus able to infect mobile phones. The **VBS.Timofonica.B** virus would normally spread using e-mail services, but it was also capable of sending itself to random mobile numbers belonging to Movistar cellular customers. The so-called virus was merely a hoax, as its payload would only display a message written in Spanish on the mobile phone:

> ***"Information for you: Telefonica is fooling you"***

The virus did not take handheld devices out of service, nor would have any effect on their performance. However, international mass-media rushed to name **VBS.Timofonica.B** the first 'cellular' virus[81].

The Cult of the Dead Cow shows up with an updated version of their **Trojan.BackOrifice** software during a DefCon conference. Posing as respectable software developers the members of the organization claimed that **BO2K** had been shifted to remote administration purposes only. All the signs point to the fact that The Cult of the Dead Cow planned the same strategy as the **NetBus** author, namely asking antivirus vendors to remove scanning routines for it. However, given the fact that it was largely used to inflict damage, antivirus manufacturers labeled it as **Backdoor.Trojan** and included a disinfection routine.

New malware threats were on the horizon during the summer. In early July, three new viruses emerged; while they were not as dangerous as its predecessors, they contained a couple of programming techniques that had never been seen until then. **Star**, the first macro virus for AutoCad packages, was extremely small (500 bytes only) and primitive. **Star's** apparition was in close relationship with Autodesk having introduced Microsoft's Visual basic, the macro programming interface. The virus had no malicious payload which made security experts think that it was a first draft

[81] Because of the significant advances in the mobile world, nowadays' mobile phones can be easily infected and rendered inoperable by miscellaneous security threats. In order to protect you from mobile viruses, Bitdefender has released Mobile Security, an antivirus solution for mobile devices running Symbian™ or Microsoft® Windows Mobile™. You can read more about the mobile antivirus at http://www.bitdefender.com/PRODUCT-2149-en--BitDefender-Mobile-Security-v2.html

of a more intricate creation. However, future proved that there was no second shot at infecting AutoCad files.

Win32.Unchained.B was another interesting virus to spice up the summer of 2000. One of its most interesting aspects was the fact that it practically contained a cocktail of code borrowed (or stolen) from its predecessors. Upon disassembly[82], antivirus researchers found out that it contained code from five other viruses including **CIH**, **SK**, and **Bolzano**. **Win32.Unchained.B** also used to activate processes from other components at specific dates, which brought it the **Shuttle Virus** moniker.

A clumsy Internet worm called **I-Worm.Jer** also showed up in June. Its creator uploaded its script on a web page, and the virus would automatically kick off when a page was visited, announcing that a potentially malicious file was found on the hard-drive and asked the user for disinfection. It relied on the fact that most users would click on the “Yes” option to get rid of the message. **I-Worm.Jer** did not manage to create an epidemic (only about a thousand users have been tricked), but it set a new trend in infecting systems over the Internet.

The **Palm.Liberty** virus arrived in August and marked a new era in developing malware for PalmOS operating systems. This was the first virus of its kind, and although it could delete files from the affected system, it was not able to replicate and spread itself easily. However, an improved version of it (**Palm.Phage**) would appear later in September.

Antivirus experts had to face a new challenge with the advent of the **Stream** virus. This piece of malware was able to manipulate the Alternate Data Stream (ADS) of the NTFS format, a location that was usually inaccessible to antivirus scanners. Although the new virus was not too much of a security threat, the new viral technology of accessing the ADS called for a complete update of the antivirus protection. Even today, scanning the ADS is a painstaking process mastered only by top-tier antivirus manufacturers.

In October, Russian virus writer Z0mbie released a metamorphic piece of malware called **Virtool.Mistfall.A** (also known as **Zombie.Mistfall**). This is the first known virus to use code integration techniques, which means that the integrated Mistfall engine was able to decompile PE files, and then inject itself into the PE code. It could also perform code moves, regenerations and relocation, but it needed more than 32 MB of RAM in order to rebuild the PE executable.

Two other interesting viruses that appeared in October were the first PIF infector (also known as **Win32.Pif.Fable**), as well as the first PHP virus (called the **Backdoor.Php.Pirus.A**). However, they are more of a curiosity, than a real threat, as they have never been seen into the wild.

[82] The operation of taking a program piece by piece in order to figure out how it works.

2001: the Year of the Worm

The malware development in 2001 was mostly driven by the Internet boom. Worm and virus authors have previously made serious attempts at infecting computer users via the web (such as the **Jer** Internet worm), while others tried to use an Internet connection in order to update their creation and avoid simple string scanners (**Babylonia**).

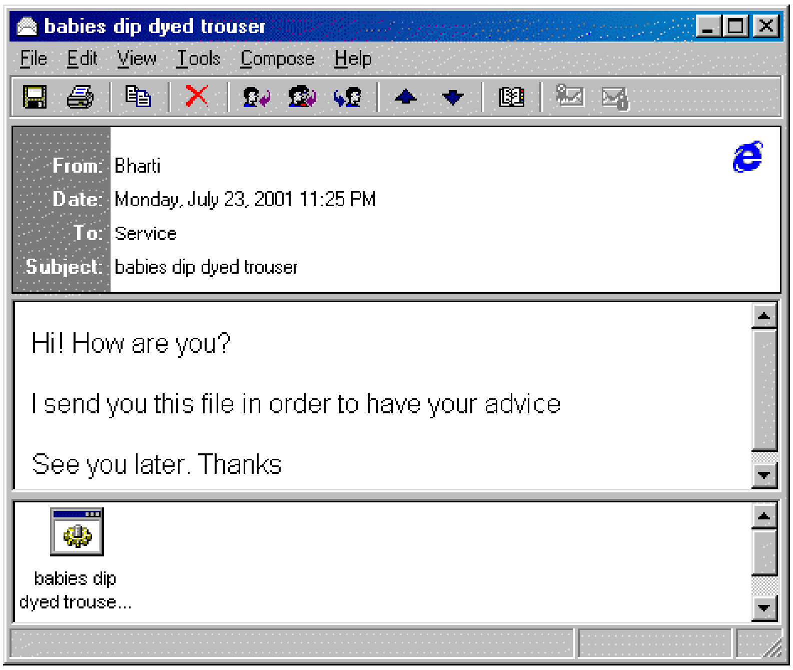
Viral attacks carried over the Internet also took off. If malware authors have been tricking the user into downloading and executing files from obscure websites, the new types of infection relied on visiting an infected website, or even a legitimate URL that had been previously compromised. The rise of Internet Explorer was also a notable factor in carrying successful attacks.

More than that, the introduction of new technologies, such as the ICQ and MSN instant messaging services or the advent of file-sharing networks played a key role in distributing malicious applications.

March came with a new multi-OS, metamorphic threat called **Smile**. Written in assembly language, the new virus was written by the virus writer Mental Driller. Just like other creations by the same author, the **Smile** was extremely difficult to detect and disinfect. Upon its first launch, the virus checks the system date, and then waits dormant until on the 17th of March, June, September, or December, when it displays a random text message.

After the message has been successfully delivered, the virus starts to rebuild itself and triggers a massive infection among the local executable files. However, it cannot infect files located at more than three levels deep in the directory structure or if the folder name begins with the letter W.

The **Win32.Worm.Sunos.Sadmind.B** worm struck both Sun Microsystems machines and Microsoft's Internet Information Services web servers on May the 8th. The self-propagating worm would deface websites hosted on the compromised machines using offensive messages against the US government as well as against the anti-Chinese cracking group PoizonBOx. In order to propagate from one infected server to another, the worm exploited a critical system vulnerability. Since then, both Sun and Microsoft issued security patches to prevent further attacks.



From: Bharti
Date: Monday, July 23, 2001 11:25 PM
To: Service
Subject: babies dip dyed trouser

Hi! How are you?

I send you this file in order to have your advice

See you later. Thanks

Figure 12: Sircam would infect .doc and .xls files, and then it would send them as attachments to miscellaneous addresses.

A few days later, the **Win32.Worm.Sircam** worm was spotted in the wild. Although its favorite means of propagation is using e-mail messages sent from Microsoft Windows systems, it was also able to send itself to other computers using unprotected network shares. When using e-mail as its main vector, the worm would randomly pick an e-mail subject form a built-in list. However, because of a programming bug, it would rarely use some other subject than the notorious "**I** send you this file in order to have your advice". **Sircam** would spread by infecting .doc and .xls files, and then send them as attachments to various e-mail addresses. During the outbreak, a couple of critical files (such as sales reports, password lists and other sensitive information) arrived in the inboxes of unauthorized persons.

We have previously said that the antivirus industry is working at full speed on the 13th of each month falling on a Friday. July 13, 2001 was no exception, as it was the time the famous **Code Red** worm hit. The worm attacked computers running Microsoft's IIS web server, an extremely popular choice among the Internet web servers. The worm would deface websites hosted on the compromised machines by displaying the phrase "Hacked by Chinese". The worm was initially spotted on July the 13th, but the infection reached its peak six days later (July 19th), when more than 359,000 machines have been reported as compromised. A newer version of the worm, called **Code Red II** struck back in August, but it primarily infected Chinese web servers.

On September 18, another worm called **Worm.Nimda.A** [83] started to spread by exploiting different vulnerabilities in Microsoft Windows, as well as some backdoors left open by its predecessors, Code Red II and **Sadmind** worm. However, **Nimda** also came with file infection capabilities, which dramatically increased its impact over the Internet infrastructure. According to those times' security reports, **Nimda** was the Internet's most widespread virus/worm within 22 minutes.

[83] The worm's name spelled backwards is "admin". Due to its release date, the worm was alleged to be the creation of the Al-Qaeda terrorist group, but the supposition could not be verified until now.

Last, but not least, the **Klez** worm started spreading havoc on October 26. **Klez** infected Microsoft Windows systems, exploiting a vulnerability in Internet Explorer's Trident layout engine, that was also used by both the Outlook e-mail client and Outlook Express

As far as malware activity is concerned, 2002 was a calm year, although virus and worm writers continued to release their creations into the wild. Two new Flash worms appeared in January: LFM and Donut were two proof-of-concept security threats able to work in the .NET environment. However, they have never been spotted in the wild. Four months later, **Spida** wrote a new chapter in the malware history as the first SQL worm spotted in the wild. It only affected SQL servers running with a blank system administrator password, a fatal configuration error that (believe it or not) was a common thing those days. **Spida**'s author wrote the worm using JavaScript, batch files and compiled executables. Once it successfully infected a system, the worm would run a scanner in order to detect other potential SQL servers to infect.

Although the primary targets for malware authors were Microsoft Windows systems, Linux machines also got a hard time in 2002. **Worm.Linux.Slapper.E** was one of the first Linux worms to demonstrate that Linux computers were as vulnerable as the ones running any other operating system, in spite of all the hype regarding their increased security. **Worm.Linux.Slapper.E** managed to take out of service thousands of machines running Linux within a few days, causing incredible damage to the Internet infrastructure[84].

While 2002 was a calm year, and no single piece of malware caused significant outbreaks[85], 2003 was slightly different. Two massive Internet attacks marked the biggest security disaster in the history of computing.

The first massive outbreak was triggered by the notorious SQL worm **Slammer**, a piece of malware that exploited an unpatched vulnerability in the MS SQL server software. The fileless worm started to cause damage on January 25th 2003, when it managed to globally infect hundreds of thousands of computers in span of a few minutes only. The extremely violent increase in network traffic caused some vital parts of the Internet infrastructure to completely crash. The **Slammer** attack on the Internet was similar to releasing a nuclear bomb in a high-density population area.

The worm penetrated the computers using the 1433 and 1434 ports. Right after it got inside the server, it did not copy on the disk, but rather it remained resident into the computer memory.

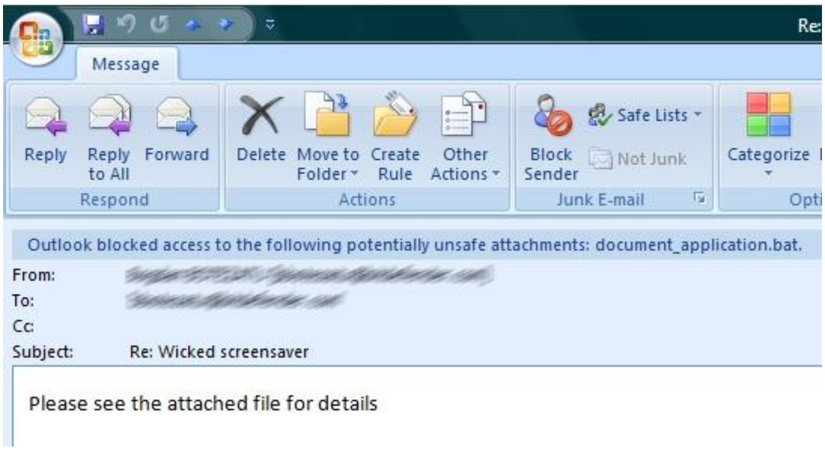
Another massive outbreak was triggered by the **Win32.Worm.Blaster** (also known as **LoveSan**) worm, which also exploited a vulnerability in Windows in order to replicate itself. However, while **Slammer** used the MS SQL server vulnerability, **Win32.Worm.Blaster** took advantage of a loophole in the RPC DCOM service working under Windows 2000 and XP. The vulnerability allowed the worm to attack almost any computer in the world that had an Internet connection. In order to spread to other

[84] As most Internet servers were running on Linux, plenty of services hosted on compromised machines were inaccessible for a long period of time.
[85] However, the combined amount of malware brought significant damage to the industry.

systems, the worm uses the compromised computer to scan for valid IP addresses. After it has "processed" 20 IP addresses, the worm sleeps for 1.8 seconds, and then it resumes scanning. More than that, the worm comes with a payload that performs a SYN flood against port 80 (http) of www.windowsupdate.com, in order to create a distributed Denial-of-Service attack (DDoS). The attack failed, as Microsoft used the targeted domain to perform redirects to the main site (windowsupdate.microsoft.com).

2003 - Sobig and the Botnet

Although the **Win32.Sobig** worm had been spotted in isolated locations since January, it did not start causing trouble until August, with the advent of its **Sobig.f** variant. Spreading via e-mail, the **Win32.Sobig** worm s thought to be the first organized attempt to create large-scale Botnets (networks of compromised systems that can be remotely controlled by a bot herder). The main reason for writing **Win32.Sobig** is alleged to be an attempt to create a huge network of zombified computers in order to conduct DDoS attacks on corporate servers.



Outlook blocked access to the following potentially unsafe attachments: document_application.bat.

From: [redacted]

To: [redacted]

Cc:

Subject: Re: Wicked screensaver

Please see the attached file for details

Figure 13: In order to prevent users from unwillingly running malicious attachments, many e-mail clients block potentially unsafe attachments.

Win32.Sobig caused a huge epidemic: one in 20 e-mail messages was infected with the worm. It is alleged that **Win32.Sobig** is the mail worm that holds the record for the most infected machines worldwide.

Another e-mail worm attacked right after **Win32.Sobig**. The **Tantalos.b** was the first of its family to exploit the Iframe vulnerability in MS Outlook in order to automatically execute itself. Although it could not match the damage caused by **Win32.Sobig**, **Tantalos** scored second in the top of the most aggressive e-mail worms in 2003.

The **Sobig** incident prepared the ground for another Trojan. **Sober** built on the panic created by its predecessor in order to spread and multiply at will. Although it is just a **Sobig** clone, **Sober** came with some innovative features: the accompanying e-mail message was written in a plethora of languages. The Trojan would detect the user's language by looking up the destination IP address. In order to convince the user to execute the attachment, it posed like a removal tool for **Sobig**.

2004 – Google Draws the Curtains

Malware authors continued to focus mostly on worms during 2004, just as they did in the previous year. The successful attacks carried by **Slammer**, **Win32.Sobig** and **Tantalos** were enough reason to keep improving worms rather than viruses. However, the sharp increase in malware and the utter disaster caused by Slammer called for a solution, and antivirus researchers hurried their technological development. Other major industry players, such as the popular search engine Google have entered the battle against malware.

In late January, **MyDoom** set the tone with the first attacks carried against computers running Microsoft Windows operating systems. It started causing panic on January 26th, and it quickly became the fastest-spreading e-mail worm ever. Although there are no accurate reports, it is believed that **MyDoom** had beaten the previous infection records set by the **Sobig** worm.

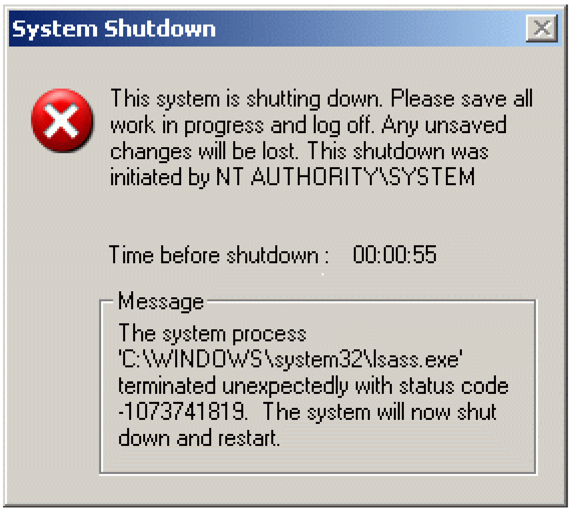
A closer look into **MyDoom**'s body revealed that the mass-mailer has been commissioned[86] by spammers, in order to facilitate their work. Other scenarios claim that the worm was released by a professional underground programmer located in Russia, although authorship can not be determined for sure.

On March 19, a new worm called **Win32.Worm.Witty.A** successfully exploited several security holes in some security system products manufactured by Internet Security Systems (ISS), and started a massive wave of destruction. The Witty came with a couple of new programming techniques and innovations which made it rather unique. For instance, it is the first worm to take advantage of vulnerabilities in the very pieces of software designed to enhance network security. More than that, it came with an extremely malicious payload: Once inside the host system, it starts attacking a pseudo-random subset of IP addresses. It repeats the attacks in sets of 20,000, but during the attack, it also overwrites sections of the computer's HDD.

The first day of May brought a new security threat in the form of the **Win32.Worm.Sasser.DAN** worm, a piece of malware exploiting a buffer overflow in the component known as LSASS (Local Security Authority Subsystem Service). While other viruses and worms catch system administrators and security analysts by surprise, **Win32.Worm.Sasser.DAN** built its attack on laziness and lack of information. **Win32.Worm.Sasser.DAN** would only spread on vulnerable systems, but Microsoft had released a critical patch addressing the LSASS issue 19 days prior to the first attack[87]. Also, the worm could be easily stopped by a properly configured firewall.

[86] The worm contains the text message *"andy; I'm just doing my job, nothing personal, sorry,"* which might mean that the author had been paid to program it.

[87] Some sources claim that the authors have reverse-engineered the patch in order to discover the vulnerability, and then relied on the fact that not all system administrators deploy security patches on time.



System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:55

Message

The system process 'C:\WINDOWS\system32\lsass.exe' terminated unexpectedly with status code -1073741819. The system will now shut down and restart.

Figure 14: the Sasser worm would force the infected computer to shutdown from time to time.

The last month of 2004 brought to life the first known "webworm". Also known as "**Worm.PhpBB.Santy.A**", this new type of malware was written in Perl and relied on a vulnerability in the popular phpBB forum software (which used Google) in order to spread across the Internet. The tiny Perl worm managed to take down between 30,000 and 40,000 websites in about 24 hours. Although the worm would only deface[88] websites written in PHP or HTML, Google took stance against the attack and filtered the search query used by the worm, thus putting an end to the outbreak.

2005 – The Sony BMG Scandal

One of the most interesting security threats in 2005 were the so-called worms for instant messenger applications. IM services have become so popular, that almost every PC user around the world enjoyed their services. Although a couple of IM worms have been detected long before 2005, their count significantly increased during the year.

The first significant outbreak during 2005 took place in August, when the **Win32.Worm.Zotob.A** worm and some of its variants (**Win32.Worm.Zotob.D**) started infecting US-based computers. The new worm exploited multiple security vulnerabilities in the Windows 2000 operating system in order to spread across the network. Although the damage was allegedly situated in the $97,000 space, American mass-media outlets proclaimed it a large scale disaster. This is mostly due to the fact that the worm infected computers at companies such as ABC, CNN, The Associated Press, The New York Times, and Caterpillar Inc.

October 13 brought a new surprise in the form of the **Samy XSS** worm (also known as **JS.Spacehero**). The new cross-site-scripting worm was especially tailored to spread using the extremely popular MySpace social-networking site. The **Samy** worm also carried a payload that would display the string "but most of all, Samy is my hero" on a victim's profile. According to a MySpace report, the XSS worm managed to infect over one million users.

Samy's author has been identified as Samy Kamkar. MySpace filled a lawsuit against him for felony. Kamkar was sentenced to three years probation, 90 days community service and an undisclosed amount of restitution.

[88] The worm caused writable files on the infected server to display the message "This site is defaced!!! This site is defaced!!! NeverEverNoSanity WebWorm generation X".

A huge scandal was about to begin on October 31, when Sony BMG was found to have willingly infected music CDs with a rootkit in order to prevent illegal copying of music. The company started protecting its audio CDs with a new technology, called the **Extended Copy Protection (XCP)**. This piece of software was automatically installed on the customers' computers each time the disk was inserted in the CD-ROM. Although Sony BMG had planted the rootkit[89] with no intention to harm the user, the community claimed that the XCP interfered with the normal way in which the Microsoft Windows operating system played audio CDs and that it would open additional security holes to be exploited by malware.

Sony BMG was accused of having planted spyware on its customers' machines. The company was called to court as part of a class lawsuit. Moreover, Sony BMG had to recall all the affected music CDs.

2006 – MacOS X Rides On the Trojan Horse

The new year was relatively calm, with few major security incidents. The smooth Internet experience users could enjoy was partly due to the fact that Microsoft's Windows XP operating system was safer than its predecessors, but partly due to the fact that the antivirus industry was watching.

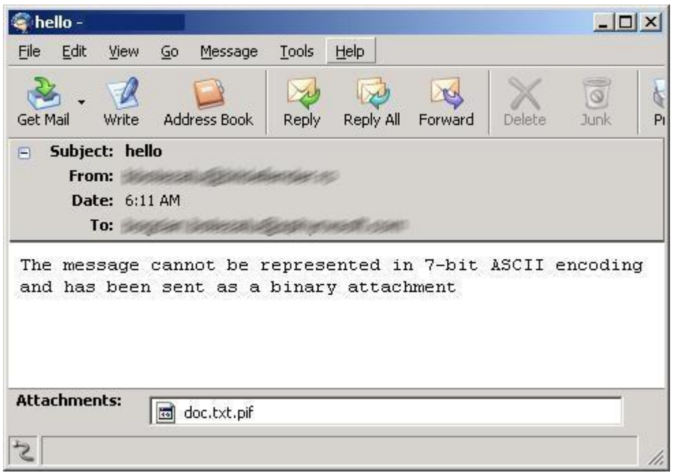
JS.Blackworm.A was the first Internet worm to hit in February 2006. The new piece of malware spreads by e-mail using messages with infected attachments, as well as through unprotected network shares. However, **JS.Blackworm.A** was a classic worm, which only could infect a system when the human user would execute the attachment. The worm comes with a malicious payload that corrupts data in the on the compromised computers. Its payload only triggers on February the 3rd, an event referred to as The Day the Music Died. More than that, the worm was able to delete several antivirus utilities if they had been installed on the path specified in the worm's code. After it deletes their files, the worm also flushes their corresponding Windows Registry keys that allow them to start with Windows.

Other variants of the virus set off on October 26th. They are known to disable security-related and file-sharing software, as well as to destroy certain files in the system.

February also premiered the piece of malware for Mac OS X: a low-threat Trojan-horse known as **OSX/Leap-A** or **OSX/Oompa-A**. The Leap has worm abilities, as it spreads from one system to another using the iChat instant messaging program. The executable file is camouflaged with the standard icon of an image file that is allegedly containing a screenshot of Apple's upcoming operating system. The worm exploits users' curiosity, a common technique also encountered in the **Win32.Loveletter** e-mail worm.

[89] Bitdefender identifies the rootkit as *Win32.Sony-DRM-HiddenFile*

Once it infects the system, the worm would make successive attempts to send itself using the same user's iChat Bonjour buddy list. While the worm does not contain a deliberately-implemented malicious payload, a programming bug would prevent the infected program from starting.



Subject: hello
From: [redacted]
Date: 6:11 AM
To: [redacted]

```
The message cannot be represented in 7-bit ASCII encoding
and has been sent as a binary attachment
```

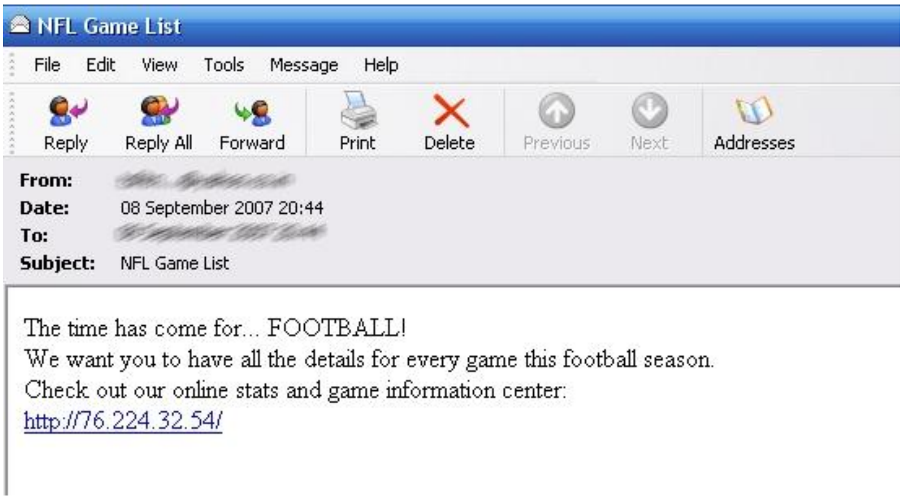
Attachments: doc.txt.pif

Figure 15: Warezov made heavy use of social engineering techniques to trick the user into running the malicious attachment

Win32.Warezov.AB hit Microsoft Windows users in late September. Also known as **Stratio**, the new family of worms is able to shut down the operating system’s security features in order to replicate itself using e-mail clients. **Win32.Warezov.AB** uses social-engineering techniques in order to infect other systems. The e-mail it sends is allegedly coming as a report from a mail server that announces the user about an unpatched security flaw in Windows. More than that, it informs the user that the respective security patch is attached to the message – in fact, it is a copy of the virus ready to be executed.

In order to avoid detection, **Win32.Warezov.AB** updates its code about once in 30 minutes. It automatically downloads new instances of the worm, and then stealthily installs them on the host computer. This perpetual update process makes disinfection extremely difficult, as antivirus providers have to issue new file signatures for each variant.

2007 – Malware Takes the World by Storm



From: [redacted]
Date: 08 September 2007 20:44
To: [redacted]
Subject: NFL Game List

The time has come for... FOOTBALL!
We want you to have all the details for every game this football season.
Check out our online stats and game information center:
http://76.224.32.54/

One of the biggest security threats in 2007 was posed by a new and rapidly-evolving email spamming campaign. The central piece of the new campaign is the **Storm Worm**, a mixed-type piece of malware that combines worm features with backdoor and Trojan capabilities. Initially spotted in the wild on January the 17th 2007, the worm is trying to infect computers, and then to add them to the Storm botnet. The worm disguises itself as a newsletter containing a film about forged news stories. Just like its predecessors, it relies on users' curiosity in order to make them download and execute the attachment.

The worm initially started as an announcement about a weather cataclysm[90]. However, as the infection evolved, the subject tag got changed. The worm was highly efficient, and security experts claimed that an infected machine could send bursts of almost 1,800 messages in less than five minutes.

When the attachment is opened, it installs the wincom32.exe service. The computer itself becomes part of a large botnet, controlled by a botmaster. However, the Storm Botnet was built using a peer-to-peer approach, rather than the conventional "centralized control" approach, which makes it even harder to kill.

It is alleged that on 7 September, the Storm Botnet was comprised of between 1 and 10 million infected computers, acting like a single processing entity. The **Storm Worm** hit once again on April 1, this time accompanied by April Fools-themed subject titles.

2008 – The Emergence of Rogue Antivirus Software

Although the security landscape during the last few years mentioned less and less attacks (although they dramatically increased in violence), this does not mean that the malware industry has suddenly come to repent its misdeeds. On the contrary, if a security threat can not be detected, this does not necessarily mean that it is inexistent.

[90] The initial subject read "230 dead as storm batters Europe" - a reference to the European windstorm Kyrill

Boot sector viruses have been long since rendered useless, thanks to the fact that the IT industry has shifted its attention from floppy disks to the newer and more powerful hard-disk drives or even solid-state drives[91]. However, malware authors' affinity for boot sector viruses pushed them into developing a new breed of such security threats, able to run on modern architectures. This is how bootkits (rootkits that can boot up from any storage medium) were born.

In early 2007, two Indian programmers developed and introduced a new tool called Vbootkit. The new piece of malware was able to run even on extremely secure environments, such as Microsoft's latest operating system, Windows Vista.

The new bootkit continued to infect users' computers during 2008, and a couple of websites have been reported to host the additional malware the bootkit was downloading after the infection. When security analysts disassembled the piece of malware, they found out that the application was able to infect hard-disks' MBR (master boot record) sector, which means that the bootkit could launch itself prior to the operating system. This is an extremely dangerous situation, as the system is completely exposed to the piece of malware, since it gets into the memory long before the antivirus software is executed.

The biggest security threat in 2008 was caused by the discovery in May of the Rustock.C, a backdoor Trojan that allows remote attackers to use the compromised computer as an anonymous proxy server. The new backdoor uses advanced rootkit technologies to conceal its files from both the user and from the operating system itself. This means that malicious users can hijack the system without even the user noticing it.

The really interesting part is the fact that the **Rustock.C** rootkit has been in the wild since October 2007, but it took the industry six months[92] to detect it and issue a fix. Rootkit malware is extremely difficult to remove, even when using specialized tools. It can not be removed by average computer users, so the best solution is installing an anti-virus utility to take care of such security incidents.

Another major security incident has been triggered by a refreshed version of the fearful Storm Worm. Its new variants were able to make use of hundreds of compromised websites; however, its favourite method of spreading between computers was via instant messaging applications. All the compromised computers were part of an extremely large botnet. Since the botnet was decentralized, there is no exact account of how many compromised systems were part of it. It is for sure, however, that the Storm botnet played an essential role in launching large-scale phishing attacks against the Barclays and Halifax banks.

[91] Solid-state drives are storage media that do not rely on spinning platters; on the contrary, they are extremely similar to flash drives, as they are built of NAND flash chips. This allows solid-state drives to function with less energy, while improving the data transfer rates and eliminating the residual noise produced by HDDs' moving parts (motors and spindles).

[92] In order to control the damage, Bitdefender issued an immediate fix for Rustock.C

March came with a new security threat triggered by an extremely popular download application, called FlashGet. This legitimate download tool has been compromised in order to include a Trojan file. Further research unveiled that the website had been hijacked by hackers[93], and the FlashGet distribution available for download has been modified to include a Trojan. Shortly put, the **FGUpdate3.ini** file was modified to include a link to the **inapp4.exe** Trojan (also known as TrojanGet).

Social networking viruses and worms are currently riding on the popularity wave, and chances are that they will continue to gain popularity among unsuspicious users. Orkut was one of the first social networks to be hit by malware, although its popularity is somewhat limited to Brazil and India. Since Brazil is an extremely active country in developing and spreading malware, it is no wonder that the most popular services among the Brazilians are top-tier targets. The first script worm affecting the Orkut platform was reported in December 2007, but it remained active all along 2008. Initially designed as a XSS[94] attack, the second epidemic of the worm hit the users in February 2008. This time, the worm came with extra functionalities, which allowed it to send users miscellaneous messages that appeared to come from one of their contacts. However, the message would display mature content in Flash movie format. In order to be able to play it, the user is advised to install a special player, which in fact is a Trojan application. Once the Trojan is installed on the target machine, it starts dropping other pieces of malware, as well as to send messages to other contacts on Orkut.

Apart from tracking the user's actions and preferences, this piece of malware is able to monitor the computer for online-banking information. According to security reports, more than 13,000 systems have been compromised until now.

The rapid ascension of social networking platforms and, more specifically, Facebook's undisputed success to the public[95] drew malware authors' attention. More than that, since they were packed full with personal information that could be used for miscellaneous abuses, these accounts acted like honey jars to cyber-criminals. One of the first e-threats to pose a major risk to Facebook users was the Koobface worm: after a rudimentary A variant released in early August 2008 and only affecting

[93] The German edition of Wikipedia itself was hijacked by hackers, who introduced a new entry on the Blaster worm. They detailed on an alleged "fix" that prevented Blaster from infecting computers, then pointed users to a compromised website hosting Trojan malware. Wikipedia removed both the page and its cached version in order to shield its visitors from the extremely dangerous Trojans posing as Blaster fixes.

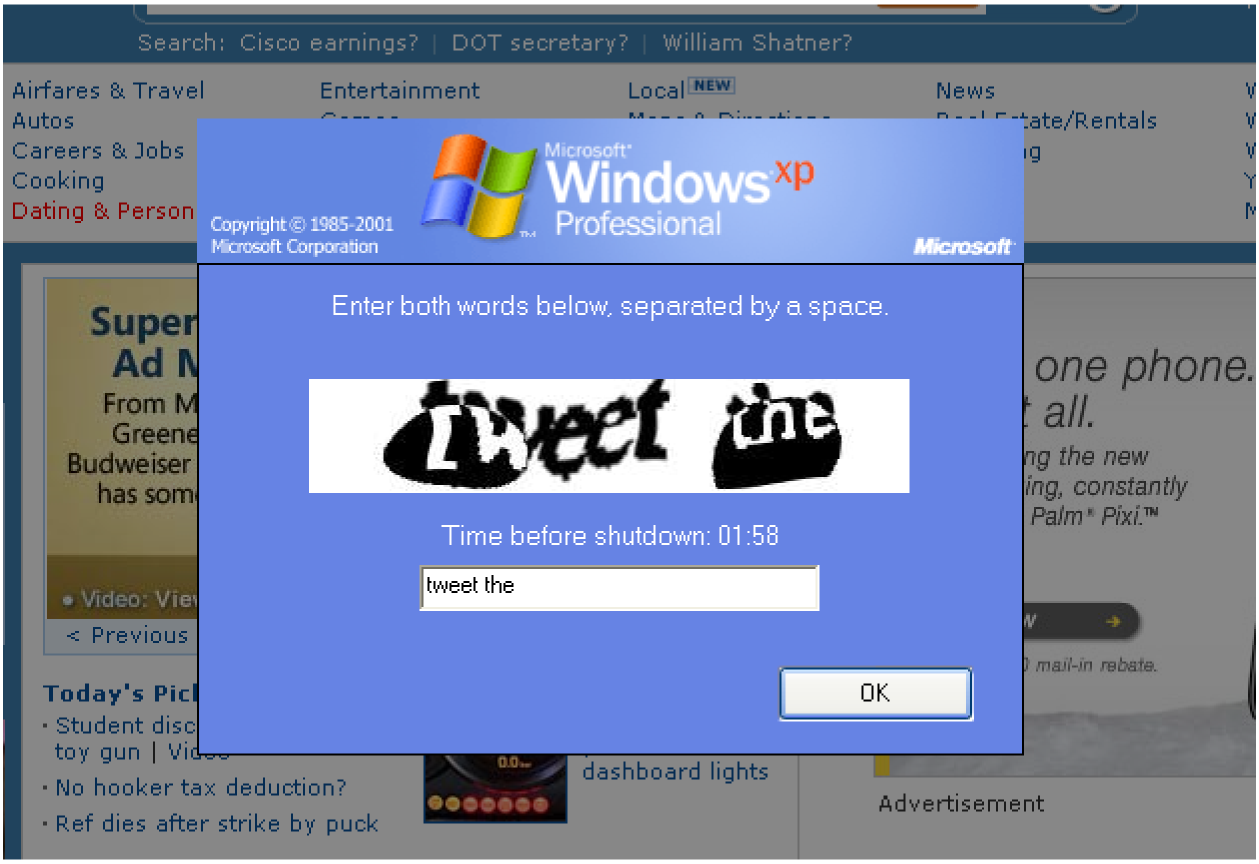
[94] XSS stands for Cross-Site Scripting, a method of loading content from a web location onto a different website. This allows hackers to direct unwary users from a legitimate and trustworthy website to a compromised location, where they are either infected or their data gets harvested.

[95] Facebook claims that it had more than 200 million registered users until mid-2008.

myspace.com users[96], the worm morphed into a fully-fledged web-based application with an unimagined destructive potential.

The upcoming variants of the worm had been redesigned to divide each of its features into a distinct module, in a similar manner with commercially-available software. Win32.Worm.Koobface rapidly grew into a tool to attack most of the Web 2.0 social networks, including, but not limited to myspace.com, facebook.com, hi5.com, fubar.com, tagged.com, Friendster.com, and twitter.com to name only a few.

It also took a shift in its behaviour: from a worm that only spreads across the walls or profiles of infected users, it grew into an extremely dangerous tool able to steal data, intercept and hijack traffic or initiate ad campaigns inside the users' browsers. At the moment of writing, Win32.Worm.Koobface is responsible for creating a massive botnet coordinated through an extremely resilient network of command & control centers that perform various tasks for its masters, including e-banking espionage and forcing rogue antivirus utilities on the already infected systems.



Enter both words below, separated by a space.

Time before shutdown: 01:58

tweet the

OK

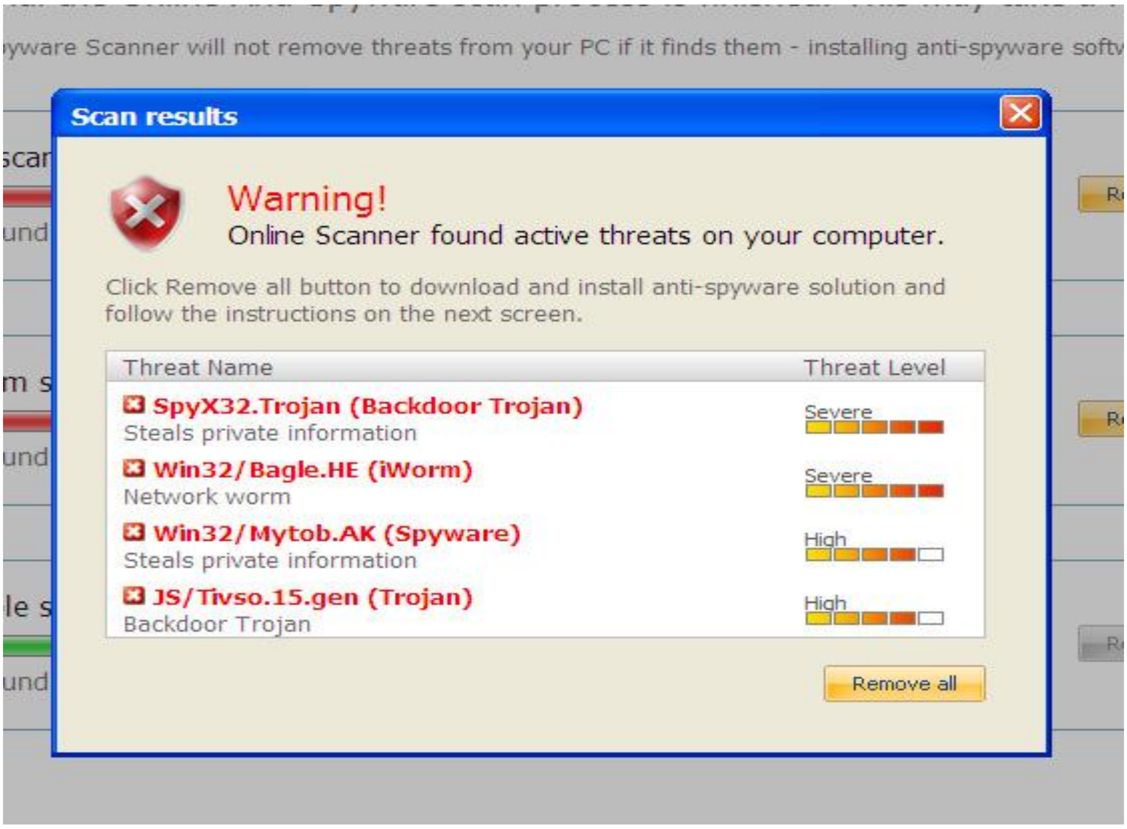
Figure 16: The Koobface CAPTHCA breaker

2008 also marked an important moment in the birth of a new generation of malware. Known as **Fake Alert**, **Rogue Antivirus** or - shorter - scareware, the new breed of Trojans would impersonate various

[96] The Koobface.A technical description from BitDefender: http://www.bitdefender.com/VIRUS-1000362-en--Win32.Worm.KoobFace.A.html

anti-malware, anti-spyware or system optimization applications in order to actually infect computers and drive victims into purchasing their “full version”. The scheme was extremely simple: once installed on the computer, the rogue AV would start random scan simulations and would display alarming pop-ups announcing the user of an alleged massive infection.

In order to maximize the infection rate, Rogue AV developers have intensively focused on performing the so-called “black-hat search-engine optimization” on keywords associated with international events.



yware Scanner will not remove threats from your PC if it finds them - installing anti-spyware softv

Scan results

Warning!

Online Scanner found active threats on your computer.

Click Remove all button to download and install anti-spyware solution and follow the instructions on the next screen.

Threat Name	Threat Level
☒ SpyX32.Trojan (Backdoor Trojan) Steals private information	Severe
☒ Win32/Bagle.HE (iWorm) Network worm	Severe
☒ Win32/Mytob.AK (Spyware) Steals private information	High
☒ JS/Tivso.15.gen (Trojan) Backdoor Trojan	High

Figure 17: Rogue AV trying to scare users into purchasing a "license"

Rogue antiviruses and anti-spyware utilities proved to be an extremely lucrative business for malware authors, as they could squeeze more money in a much shorter timeframe. The rest of the year, as well as the next one would be placed under the sign of the Rogue AV Trojan with more than 1000 distinct families active on the market.

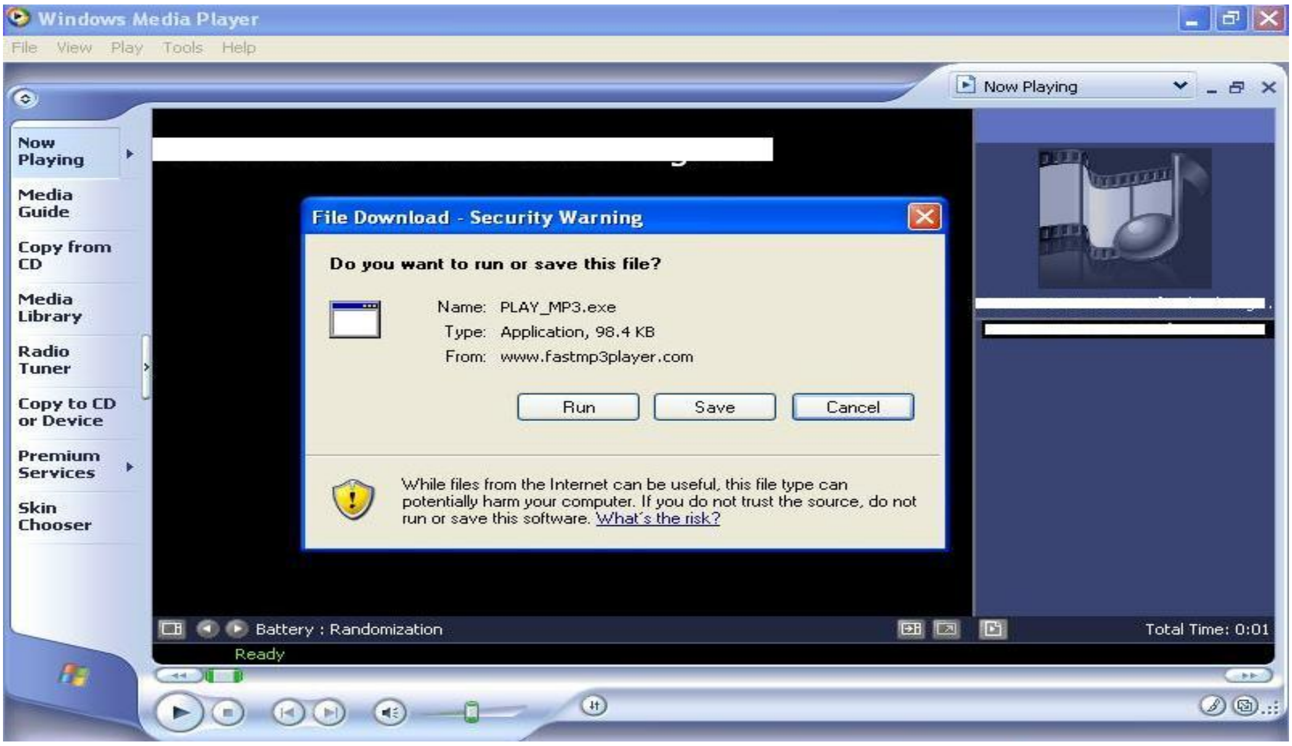
Although they have been enjoying most of the spotlight during 2008, malware attacks were not the sole dangers lurking in the cyberspace. Multiple vulnerabilities discovered in popular software such as Adobe Reader, Adobe Flash[97] and Internet Explorer versions 5 and 6[98] have been thoroughly exploited in the wild.

[97] One of the most important (yet **never reproduced outside the lab**) exploits for Adobe Flash involves “clickjacking”. A Proof-of-Concept attack demonstrated that a remote attacker can hijack a user’s clicks to activate the user's camera

The last days of 2008 brought yet another medium-level threat for Mac OS X users. Called **Trojan.OSX.Jahlav.A**, the new piece of malware impersonated either a crack for various applications or as a video codec for streaming online media. If executed, the bash script would drop a shell file that would start monitoring a specific URL for the presence of a file. If found, it would silently download and execute it, thus infecting the system with **MAC.OSX.Trojan.DNSChanger.A** – a piece of malware that would redirect all the requests for **google.co.uk** to a different address.

At the same time, some illegal sharing websites (especially Torrent trackers) saw an invasion of box-office movies bearing the strange extension WMV. While the traditional AVI video format for the so-called DVD-rips circulating on underground video-sharing portals has been universally accepted (as it offers the best ratio between file size and video quality), the use of WMV files for sharing video would be at least suspicious.

Unlike AVI, WMV files can automatically handle the absence of a codec by downloading it on the fly. It was this exact feature that made malware authors modify WMV files to download not a codec, but various pieces of malware, especially Rogue AV.



File Download - Security Warning

Do you want to run or save this file?

Name: PLAY_MP3.exe
Type: Application, 98.4 KB
From: www.fastmp3player.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Year 2008 ended with the emergence of a small and apparently pretty unobtrusive worm that exploited the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability

and microphone. The attack has been documented by BitDefender here: http://www.malwarecity.com/blog/adobe-has-finally-released-an-advisory-on-the-clickjacking-issue-221.html

[98] The exploit code for Internet Explorer v5 and 6have been actually leaked prior to Microsoft having a fix for the issue. For more information about the bug, please visit http://www.microsoft.com/technet/security/bulletin/ms08-078.mspx

(MS08-67) in order to spread on other machines connected to the local network. Called **Win32.Worm.Downadup.A** (and also known as Conficker or Kido), this apparently harmless worm will trigger one of the largest epidemics in the computer history and would keep security vendors busy for more than one year.

2009 – The Downadup Invasion

The new year debuted with the proliferation of the Conficker worm in a logarithmic manner. Although this innovative and highly contagious piece of malware did not inflict any substantial damage to the infected computer, early 2009 estimations confirmed that the total number of compromised machines around the globe during Q1 alone surpassed the population of Belgium or Netherlands.

After infection, the worm would attempt to list all the administrative shares on the network and connect to them by performing a dictionary attack. In addition, the worm would also restrict access to a list of antivirus vendors websites, in order to make disinfection nearly impossible.

Variant A was quickly followed by improved versions B, C and D that would basically contain an update list of blocked websites, along with a routine to prevent any binary file from running on the infected system if it contained the string **downadup** or **conficker** as the filename. This extra measure would prevent the user from running removal tools associated with Win32.Worm.Downadup.

Variants C and D would also feature a novel update system, able to select 500 URLs and randomly check them for updates. In order to avoid all of the links to be suspended at the same time and, therefore, to cut any communication between the attacker and the infected websites, Downadup has generated and registered no less than 50,000 random-name domains.

Although the number of infections per month has dramatically diminished as of the moment of writing, Downadup is still ranked as the number one e-threat. In the 18-month timeframe since its emergence, the worm managed to create an impressive network of infected computers that are able to communicate with their master and to update the worm, to install rogue antivirus utilities or to install third-party malware from remote locations.

The Downadup worm may undoubtedly be labelled as the initiator of one of the greatest malware pandemics in history – so great the infection that Microsoft is still offering a quarter-million dollar reward for turning in the person or persons responsible for the creation of the Downadup.

The same year witnessed the rebirth of an older family of adware applications, called NaviPromo. Extremely resilient to detection and removal, this e-threat is also one of the most discrete pieces of adware of its kind. In order to conceal its presence, it uses rootkit techniques to hide all its files both on the disk and volatile memory. Unlike most of the malware, Adware.NaviPromo would not destroy the operating system, but rather spy on the users' browsing habits as long as it takes to create a shopping profile, then start serving them targeted advertising material in extremely annoying pop-up messages on the desktop.

MBR (Master Boot Record) Trojans made a comeback with the advent of Trojan.Mebroot.B, a small piece of malware that copies itself directly into the hard disk drive's master boot record. In order to avoid being overwritten by the operating system, it reserves memory space and then deploys a small rootkit that would continue the infection spree by executing other malware components already present on the system.

Early August saw a novel approach to distributing malware. Known as **Win32.Induc.A**, this medium-threat file infector only targets systems running the Embarcadero (formerly Borland) Delphi development environment versions 4 through 7. As the virus gets executed for the first time, it would check for the presence of a registry key to see if Delphi is installed. If it is, it would modify the original Delphi SysConst.pas file by appending its malicious code and compiling it to sysconst.dcu. Since **sysconst** is included in any project compiled on the infected machine, all the binary files built with the infected Delphi compiler will also contain the viral code. Although the virus only limits to spreading its code rather than posing a real danger to either the system or to its user(s), Win32.Induc.A marks an important milestone in the malware history as the first compiler virus ever.

The last three months of 2009 have been dominated by malware targeting social networking and peer-to-peer users alike. One of the most prominent e-threats of this kind was **Trojan.Sasfis.A**, a piece of malware that – unlike others – would use e-mail attachments in order to spread itself from one computer to another. In order to gain extra credibility on the victim's side, the Trojanized messages have been forged in a manner to make them look as if they had been sent from popular social network Facebook in order to announce users of an alleged update performed in the Terms of Service (included in the attachment). This is a typical scenario that relies on victims' fear of being restricted or prosecuted unless they comply with the request.

Unwary users running the attachment would actually trigger a 20-kilobyte dropper that would install a dll file – an update component that allows a remote attacker to plant other malware on the compromised machine at any time.

Peer-to-Peer and Direct Connect download services shortly got into malware authors' crosshairs with an impressive amount of malware trying to share their binary code to anyone.

Internet worm Win32.Worm.Rimecud.C was the first to share itself through Kazaa, DC++, LimeWire, eMule , iMesh or BearShare, Once downloaded and installed, it creates a folder named USBSYSTEM, copies itself to the folder, and then creates in the device root an "autorun.inf" file which will run the infected binary each time the device is plugged in. The worm also spreads itself via MSN Messenger by sending automated messages containing links to copies of itself to the entire list of contacts. The worm uses most of the available bandwidth to perform various malicious tasks such as denial-of-service (DoS) and TCP-SYN flood attacks against remote hosts.

Worm.P2P.Palevo.B behaves just like its Rimecud.C sibling, except for some novel approaches that make it much more dangerous to users. The worm has been designed in a manner to allow it to spread via multiple channels. It can add its code to the list of P2P shares on popular file-sharing applications such as Ares, BearShare, iMesh, Shareza, Kazaa, DC++, eMule and LimeWire, but it would also infect any removable USB device plugged into an already-infected machine or even network drives mapped locally. It is also able to propagate itself by sending infected links via MSN Messenger.

Its destructive potential includes a backdoor component that allows remote attackers to seize control over the infected machine and manipulate it according to their own needs (for instance, to install additional software, to export locally saved documents, to manipulate online voting from various IPs, or even to launch TCP/UDP flood attacks against Internet servers). More than that, it is also able to intercept passwords and other sensitive data entered in Mozilla Firefox and Microsoft Internet Explorer web browsers, which makes it extremely risky to users relying on e-banking or online shopping services.

Year 2009 was surely the year of the worm. Starting with **Win32.Worm.Downadup.A**, the year concluded with an epidemic triggered by Win32.Worm.Sohanad.NAW – an older e-threat initially discovered in late 2007. **Win32.Worm.Sohanad.NAW** is a self-spreading e-threat able to download files from remote locations and stealthily execute them on the infected machine. The worm is extremely aggressive in terms of self-replication, as it features no less than three distinct methods of infecting new systems: by sharing itself on the local network, by infecting any removable storage device plugged into the infected computer and by sending enticing messages to all the Yahoo Messenger contacts of the infected YIM user.

2010 – New Security Risks Lurking: Ransomware and P2P Worms

Hardly had the winter holidays wear off that new security risks made their presence felt. Building on the experience with the Koobface worm, cyber-criminals brought **Win32.Worm.Prolaco.G,** a new network-aware worm with extremely infectious capabilities. The malware attempts to replicate itself on the local network, and also tries to use a mass-mailer component that harvests e-mail addresses from the local computer and spam its files outside the local network. After successfully compromising the system, the worm would drop a remote access tool that allows an attacker to seize control over the infected machine and dispose of the stored data at will.

Discovered in February, **Win32.Xorer.EK** proved once again that malware authors never sleep. This extremely discrete e-threat takes a new approach at infecting files. While other viruses inject their malicious code into the legitimate binary file, **Win32.Xorer.EK** rather prepends the target-executable to itself, basically “swallowing” the file:

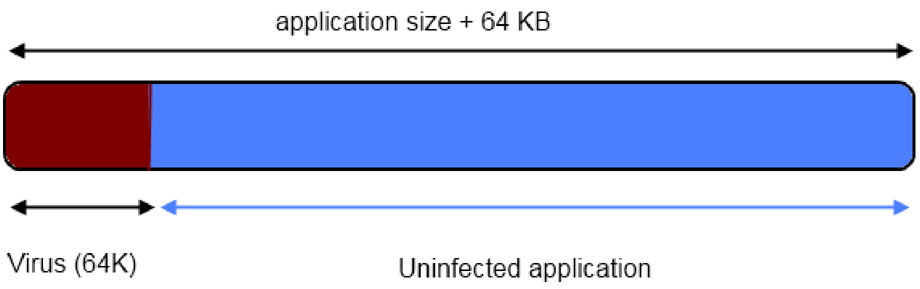


Figure 18: Win32.Xorer.EK - a virus that prepends its body to the host application

More than that, in order not to cast any suspicion to the user, it simply borrows the legitimate application's icon. Once it has been executed, it would hijack the Internet Explorer® browser and start serving miscellaneous advertisements.

Trojan.Spy.ZBot.EKF initially started showing up on antimalware vendors' radars in mid-May 2009. It took the malware more than 9 months to proliferate and reach a dangerous level of infection, a timeframe during which its creators "polished" its spreading mechanisms and added extra destructive features. The ZBot family is built with a malware creation kit named Zeus Pack. The latter is a modular tool available for sale on the underground market and can be used for creating various pieces of malware from computer bots to Banker Trojans[99]. This specific breed of ZBot featured backdoor capabilities, a FTP account/password and software product key harvester. The Trojan would also keep an eye on any other usernames and passwords the user may enter in online forms.

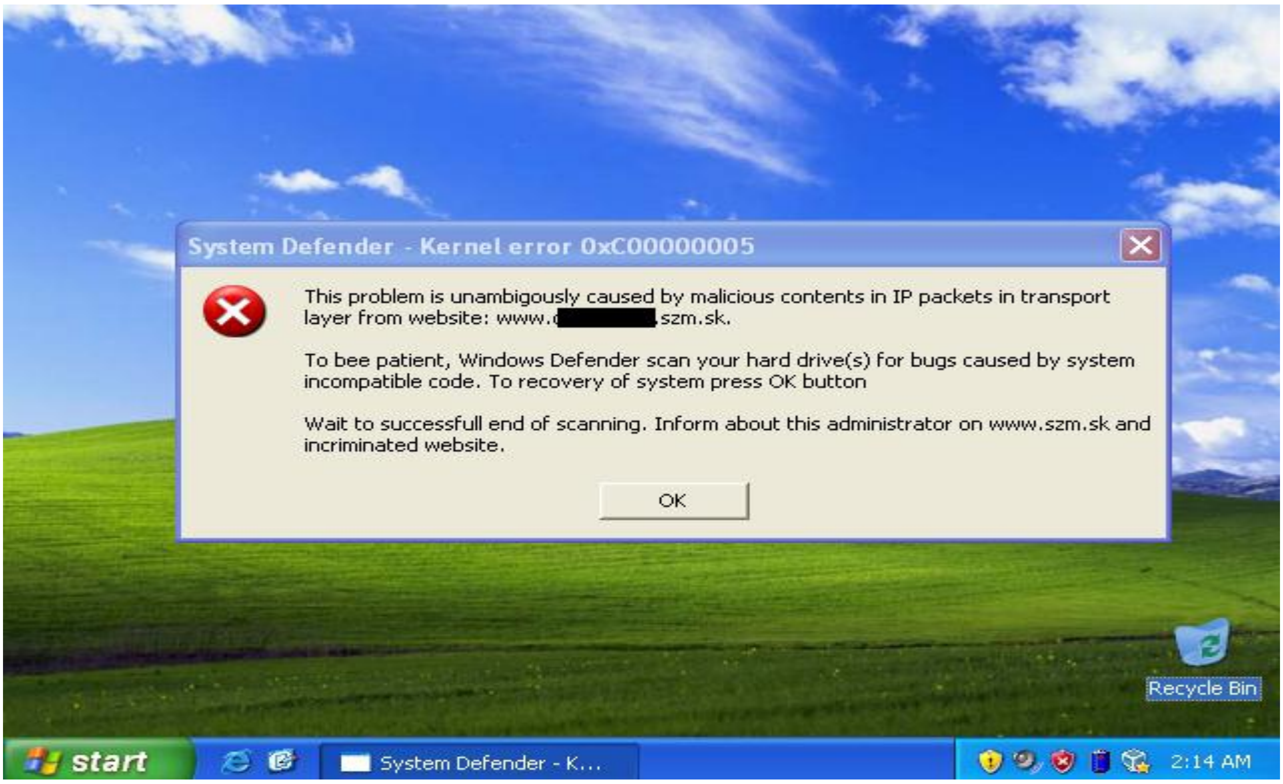
0-Day exploits made a comeback in late January with the discovery of the CVE-2010-0249. This critical vulnerability in all IE versions, except for Internet Explorer 5.01 Service Pack 4 for Microsoft Windows 2000 Service Pack 4, has rapidly been exploited by malware authors through Exploit.Comele.A. This piece of code triggers a buffer overflow and executes arbitrary code on the local machine.

The second critical vulnerability for January 2010 deals with Adobe Reader. Also known as CVE-2009-4324, it affects Adobe Reader and Acrobat 9.2 and earlier versions. Successful exploitation could cause crashes and allow a remote party to execute arbitrary code on the victim's computer, as well as to carry out cross-site scripting attacks. The vulnerability exploits an error in the implementation of the "Doc.media.newPlayer()" JavaScript method, that is likely to corrupt memory when a specially crafted PDF file is run.

The end of January brought a new threat in the spotlight. Identified as **Win32.Worm.Zimuse.A**, the new piece of maware proved to be extremely dangerous for the unwary computer users: disguised under the mask of an apparently harmless IQ test, the worm would execute itself and create between 7 and 11 copies of itself in key areas of the Windows OS. It subsequently remains dormant for a

[99] http://www.malwarecity.com/blog/banker-trojans-whos-been-spying-on-you-lately-781.html

variable amount of time (40 days for variant A and 20 days for variant B). After this period of waiting has elapsed, it would overwrite the first 50 KB of the Master Boot Record, a key zone of the hard disk drive, thus preventing the operating system from starting. It appears that the worm's destructive payload was targeted at wrongfully incriminating the management of a Slovakia-based website, mentioned in an error message before the erasure of the MBR.



System Defender - Kernel error 0xC00000005

This problem is unambigously caused by malicious contents in IP packets in transport layer from website: www.[redacted]szm.sk.

To bee patient, Windows Defender scan your hard drive(s) for bugs caused by system incompatible code. To recovery of system press OK button

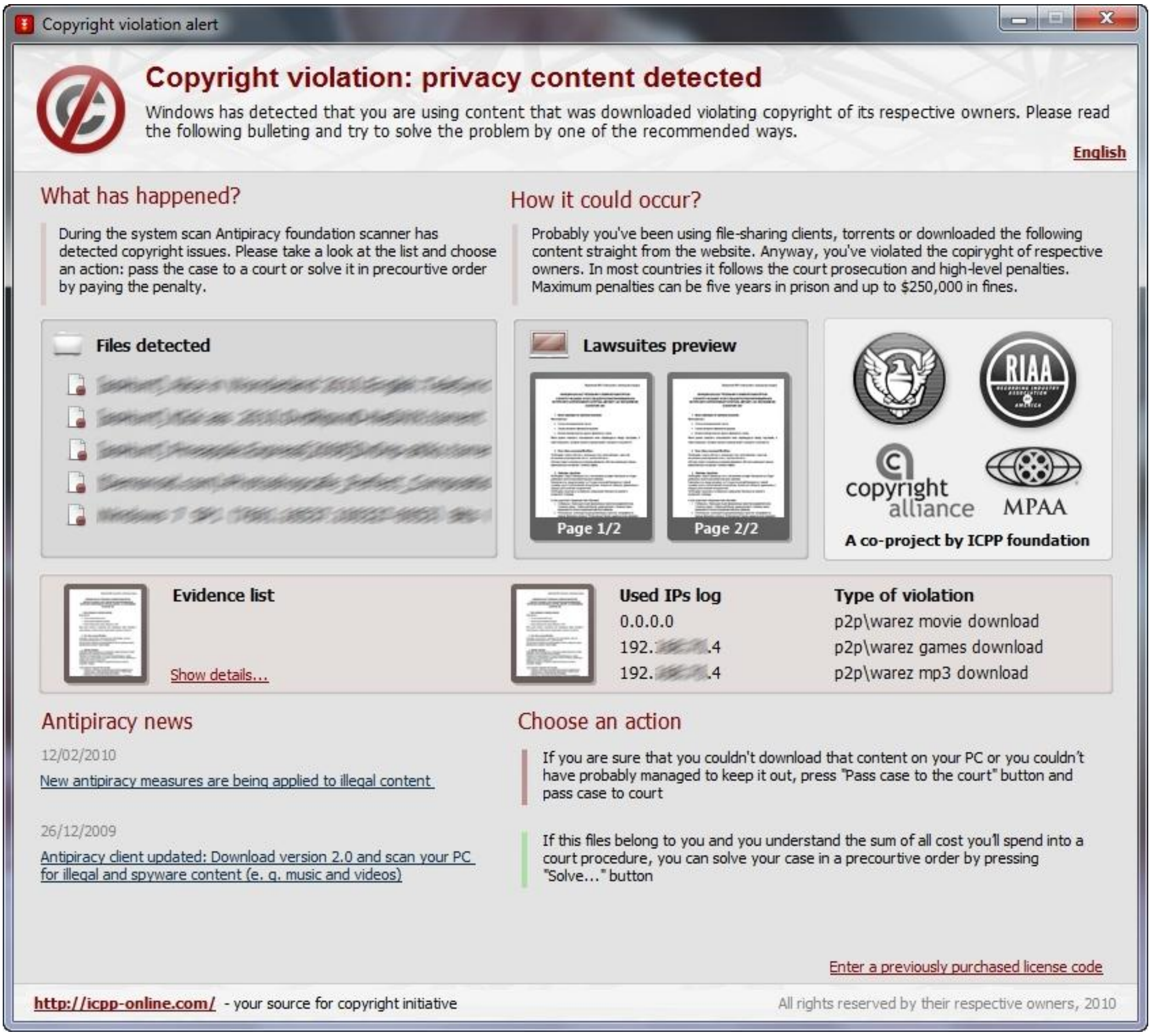
Wait to successfull end of scanning. Inform about this administrator on www.szm.sk and incriminated website.

Figure 19: Error message thrown before the MBR destruction

Fake job opportunities paired with the unfortunate state of the global economy were also an extremely appealing bait for malware cyber-criminals to lure their victims. One of the first examples of e-threats mentioning job vacancies was the **Win32.Worm.Mabezat.J** worm, which spammed itself via messages containing a variety of job-related email subjects, such as **Web designer vacancy, New work for you**, **Welcome to your new work**, or **We are hiring you.** The worm itself was attached under the name winmail.dat (a file that is supposed to contain the Exchange Server® RTF information for the message, if the recipient's client cannot receive messages in Rich Text Format). Upon execution, the worm would drop a file infector and start overwriting binary files with its own encrypted body, but not before collecting all the e-mail addresses stored on the computer and spamming itself out to all these contacts.

April saw a new and innovative type of malware set to extort money from faint-hearted users that were into Peer-to-Peer downloads. This new e-threat, detected by BitDefender as **Trojan.Maer.A**, has hit the web on April 11 and mainly targets computer users who are downloading files via sharing services based on the BitTorrent® protocol. Shortly put, the ransomware Trojan claims that it had found pirated content installed onto the system (even on clean, 100% genuine Windows® installs) and "offers" to settle things out for as much as $399.85. Users can buy a license key using PayPal or credit card: just pay the sum and your piracy case is history!

In order to gain credibility, the Trojan displays a couple of organization logos including RIAA® and MPAA®. The piece of malware is packed full with links to an organization called ICCP Foundation, which poses as “a law firm assisting intellectual property holders exploit and enforce their rights globally”. It also displays a list of “pieces of evidence”, made up by all the **.torrent** files the user may have downloaded to the %AppData% folder.



Copyright violation alert

Copyright violation: privacy content detected

Windows has detected that you are using content that was downloaded violating copyright of its respective owners. Please read the following bulleting and try to solve the problem by one of the recommended ways.

English

What has happened?

During the system scan Antipiracy foundation scanner has detected copyright issues. Please take a look at the list and choose an action: pass the case to a court or solve it in precourtive order by paying the penalty.

How it could occur?

Probably you've been using file-sharing clients, torrents or downloaded the following content straight from the website. Anyway, you've violated the copiryght of respective owners. In most countries it follows the court prosecution and high-level penalties. Maximum penalties can be five years in prison and up to $250,000 in fines.

Files detected

[redacted]

Lawsuites preview

Page 1/2 Page 2/2

A co-project by ICPP foundation

Evidence list

Show details...

Used IPs log	**Type of violation**
0.0.0.0	p2p\warez movie download
192.[redacted].4	p2p\warez games download
192.[redacted].4	p2p\warez mp3 download

Antipiracy news

12/02/2010

New antipiracy measures are being applied to illegal content

26/12/2009

Antipiracy client updated: Download version 2.0 and scan your PC for illegal and spyware content (e. g. music and videos)

Choose an action

If you are sure that you couldn't download that content on your PC or you couldn't have probably managed to keep it out, press "Pass case to the court" button and pass case to court

If this files belong to you and you understand the sum of all cost you'll spend into a court procedure, you can solve your case in a precourtive order by pressing "Solve..." button

Enter a previously purchased license code

http://icpp-online.com/ - your source for copyright initiative

All rights reserved by their respective owners, 2010

After successfully infecting the system, the Trojan would behave like an average rogue AV by displaying numerous popups reading “Copyright infringement”, and performing various browser redirects to the ICCP Foundation home page.

Future Outlook

The IT industry has undoubtedly been the subject of multiple threats along its development. Although it has already reached an incredible degree of sophistication and technological self- awareness, the security issues are far from reaching an end. On the contrary the frequency of attacks and their brutality make us think that the worst is yet to come.

The Internet is about to witness a new technological revolution due to the advent of Web 2.0 technologies. Social networks, instant messaging and all-in-one accounts are only a few of the new additions that are supposed to make our lives happier and easier. However, beyond the obvious gains, they also come with a couple of security challenges for the antimalware industry.

More and more users are switching to online platforms and services that can provide the same functionality as a generic personal computer, except for the fact that the services are available 24/7 from remote locations. Google Docs, Microsoft Live Workspace and Fanbox are only a couple of the most popular online services for users' PC data. Once the malicious attackers manage to hack into such accounts, they will have unlimited access to almost every important file ever uploaded by the user.

Multiple services offered via a single account are also troublesome as far as security is concerned. One of the biggest single-account service providers is Google, which allows users to edit, create and store documents and spreadsheets, send mail and keep track of their search queries. Once the attacker manages to crack the authentication, they will have access to almost every detail of an user's electronic life.

Another important security risk has its roots in an apparently harmless and extremely trendy habit: blogging. We are not talking about the professional, hobby-oriented blogging, but rather on posting messages loaded with personal details. One of the most efficient methods of penetrating computer relies on social engineering, and blogging might help an attacker in building the perfect scenario. After all, constantly reading such kinds of blogs can bring significant detail about the writer's surfing habits, passions, hobbies and main points of interest on the web. It only takes a couple of minutes to set up a forged website, and then to send the user a message impersonating one of the friends, family or colleagues. The more private details are exposed in the blog posts, the higher the success rate of an attack.

Malware that does not involve social engineering tricks will continue to spread at will despite the increased security measures taken by software developers. For instance, Microsoft's newest operating system, Windows Vista, comes with an User Account Control module, a security infrastructure that limits application software to standard user privileges until an administrator manually elevates it to a higher level. However, most of the average computer users running with administrative privileges find it annoying and disable it, thus eliminating all its security benefits.

Virtualization has also become one of the favorite destinations for worldwide hackers and malware groups. The technology has been quickly adopted by datacenters, as it allows them to dramatically trim down ownership costs and reduce the datacenter footprint by creating multiple virtual environments onto a single machine. Hackers' new goal is to escape the virtual machine and take over the physical structure hosting it. Virtualization security is a delicate subject, tackled by both enterprise security architects and the most ingenious criminal minds altogether.

Voice-Over-IP might not be so much of a buzzword as compared to virtualization, but it has become an extremely widespread technology that channels most of the corporate voice traffic. Corporate decision factors who think that the new technology is more of telephony than data traffic are wrong. Voice-Over-IP sessions can be hijacked and sniffed, and world's largest VoIP technology provider, Cisco, acknowledged that there are security vulnerabilities that allow hackers to intercept classified conversations.

Appendix

How to Tell if You Got Infected?

Most of the pieces of malware that are currently in the wild are designed in such a manner that they won't reveal their presence in order to keep generating profit or to cause damage for as long as possible. However, while some pieces of malware do not reveal any visible symptoms, you can still find out if and when you got infected.

Computer malware usually tampers with users' data in such a way that there is always a side effect. For instance, no matter how well concealed a piece of malware is, it will still affect your computer's performance or delete programs and system files. This could instantly render some of your programs useless, as they won't be able to find one or more critical files (usually DLLs). However, programs or the operating system itself would sometimes crash because of some critical files being accidentally deleted or even because of wrong settings applied by mistake, so not any crash should be regarded as a viral infection.

Still, if you haven't done anything wrong and your system starts behaving abnormally, chances are that you have been infected by a computer virus or a malicious browser add-on.

Computer viruses usually infect multiple files on a system, in order to prevent the user from deleting the "suspicious" file. If a file is deleted, either by accident, or voluntarily (as the user detects that something is wrong with the file), the other infected files could carry on with destroying data[100].

Unlike computer viruses, Trojan Horses are more difficult to detect and eliminate. This is because Trojan Horses do not leave too much evidence about its presence on the host computer. On the contrary, it tries to cause as little damage to the computer as possible, in order not to draw the computer user's attention. This way, it delays the mean time to detection and elimination, which means that it would be able to parasite the system for longer periods of time.

However, there are some signs that could "tip" you of the presence of an unwanted "guest" on your computer. For instance, if you notice that your files appear to be moving from a location to another or change their file size (harder to detect, yet not impossible), then you might be infected with a Trojan or you might be the victim of remote-control software.

[100] Specialized antivirus software can detect and disinfect all the compromised files by comparing their code against a signature database, or even by analyzing their behavior as they are executed. Bitdefender comes with an advanced heuristic analysis module (MIDAS) that can detect polymorphic and metamorphic security threats.

System instability could also trigger the first suspicions that you have been infected. Apart from miscellaneous hardware flaws or driver conflicts, computer viruses are the most common sources of performance loss. Messages popping up upon the OS boot or after it has been completely loaded are also a sign that something is not all right with the computer. Lock-ups, freezes and computer restarts out of the blue or visible decreases in performance should also alert you about the presence of an intruder.

Additional reading

- **Darwin, a Game of Survival of the Fittest among Programs** - http://www.cs.dartmouth.edu/~doug/darwin.pdf
- **Newsmaker: DCT, MPack developer** – http://www.securityfocus.com/news/11476/1
- **Thwarted Linux backdoor hints at smarter hacks** - http://www.securityfocus.com/news/7388
- **The Animal Episode** - http://www.fourmilab.ch/documents/univac/animal.html
- **Wang, Wallace (2006) -** ***What They Won't Tell You About the Internet*****. No Starch Press.**
- **Human Contact Spreads PC Viruses** - http://www.pcmag.com/article2/0,1759,1781208,00.asp
- **Metamorphism in practice or "How I made MetaPHOR and what I've learnt", The Mental Driller** – http://vx.netlux.org/lib/vmd01.html
- **Laziness Contributes to Spida Worm Spread** - http://www.sqlmag.com/Articles/Index.cfm?ArticleID=25612&DisplayTab=Article
- **Wikipedia Hijacked to Spread Malware -** http://www.tech2.com/india/news/telecom/wikipedia-hijacked-to-spread-malware/2667/0
- **Google searches web's dark side -** http://news.bbc.co.uk/2/hi/technology/6645895.stm
- **New botnet as powerful as Storm worm revealed -** http://www.securecomputing.net.au/News/98324,new-botnet-as-powerful-as-storm-worm-revealed.aspx
- **Bereczki, Andrei (2009) – Win32.Worm.Downadup and its removal** http://www.malwarecity.com/blog/about-win32wormdownadup-and-its-removal-326.html
- **Botezatu, Loredana (2010) – Win32.Worm.Zimuse.A - The Hard-Disk Wrecker** http://www.malwarecity.com/blog/malware-alert-win32wormzimusea-the-hard-disk-wrecker-736.html
- **Botezatu, Bogdan (2010) - Banker Trojans - Who's been spying on you lately?** http://www.malwarecity.com/blog/banker-trojans-whos-been-spying-on-you-lately-781.html