Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

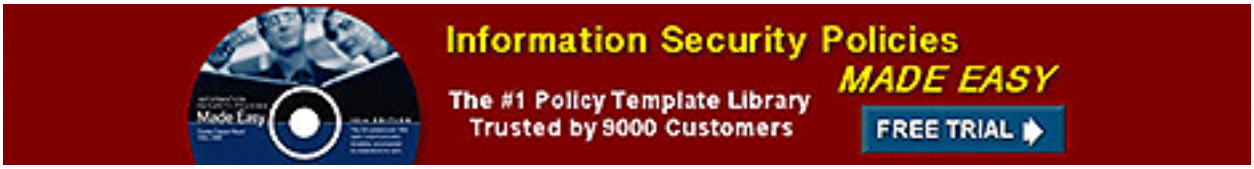
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Living with MalWare

Code Red worm, SirCam, AnnaKournikova, LoveLetter, Melissa, Pretty Park.... The list goes on forever. With each passing week, the various forms of trojans, worms and viruses seem to spread in the wild more quickly and have become more destructive. How did we get to this point? How can we defend ourselves against Malware and where do we go from here? In this paper, I will define exactly what Malware is and describe the different types. I will briefly examine the history of viruses and look at the various techniques empl...

Copyright SANS Institute
Author Retains Full Rights

AD



Living with MalWare

By Gary Wiggins

Security Essentials version 1.2d

Code Red worm, SirCam, AnnaKournikova, LoveLetter, Melissa, Pretty Park…. The list goes on forever. With each passing week, the various forms of trojans, worms and viruses seem to spread in the wild more quickly and have become more destructive. How did we get to this point? How can we defend ourselves against Malware and where do we go from here?

In this paper, I will define exactly what Malware is and describe the different types. I will briefly examine the history of viruses and look at the various techniques employed to propagate them. I will recommend a comprehensive plan to combat viruses and reduce the damage to your networks in addition to the energy spent on the never-ending defense. Finally, I will look at future technologies as solutions towards fighting viruses.

The following terms and definitions come from www.webopedia.com[1]

- Malware – short for malicious software. Software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.
- Worm – A program or algorithm that replicates itself over a computer network and usually performs malicious action, such as using up the computers resources and possibly shutting the system down.
- Trojan Horse – A destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive.
- Macro Virus – A type of computer virus that is encoded as a macro embedded in a document. Many applications, such a Microsoft Word and Excel, support powerful macro languages. These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened. Unfortunately, according to some estimates, 75% of all viruses today are macro viruses. Once a macro virus gets onto your machine, it can embed itself in all future documents that you created with the application.
- Polymorphic Viruses – Polymorphic viruses change themselves with each infection. These viruses are more difficult to detect by

[1] www.webopedia.com (27 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

scanning because each copy of the virus looks different from the other copies.

- Stealth Viruses – A virus must change things in order to infect a system. A stealth virus hides the modifications it makes. It does this by taking over the system functions, which read files or system sectors, and, when some other program requests information from portions of the disk the virus has changed, the virus reports the correct (unchanged) information instead of what's really there (the virus). Of course, the virus must be resident in memory and active in order to do this.
- Cavity (Spacefiller) Virus – A cavity (spacefiller) virus attempts to install itself inside of the file it is infecting. Most viruses take the easy way out when infecting files; they simply attach themselves to the end of the file and then change the start of the program so that it first points to the virus and then to the actual program code. A cavity virus, on the other hand, attempts to be clever. Some program files, for a variety of reasons, have empty space inside of them. This space can be used to house virus code. Because of the difficulty of writing this type of virus and the limited number of possible host, cavity viruses are rare. Many viruses that do this also implement some stealth techniques so you don't see the increase in file length when the virus is active in memory.
- Virus Droppers – Programs that place viruses onto your system but themselves may not be viruses (a special form of Trojan).

History

From a historical perspective, viruses started out slowly and rather benignly. I will take you through a rapid evolution of MalWare.[2] This list is not intended to be comprehensive and I apologize to any virus writers for the unintentional omission of their work.

1983 brought the first documented case of a virus. It was in fact an experiment, by Fred Cohen and others, demonstrated at a security seminar on November 10th to prove that the concept of a computer virus was possible. The term "virus" was coined by Len Adleman.

1986 – Two brothers from Pakistan analyzed the boot sector of a floppy disk and developed a method of infecting it with a virus dubbed "Brain". This virus is typically called the first computer virus and later that same year the first PC-based Trojan was released in the form of the popular shareware program PC-Write.

[2] Author Unknown, CKNOW.COM web site, "Narrative histories by Dr. Alan Solomon and Robert M. Slade" July 27, 2001. URL: www.cknow.com/vtutor/vhistory.htm (27 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1987 saw the first file viruses starting to appear. They originally concentrated on the COM files, particularly COMMAND.COM. Also, the first .EXE infector; Suriv-02 (virus spelled backwards) was spread. This virus evolved into the infamous Jerusalem virus.

1988 was significant in virus warfare because of the Morris Internet worm and the introduction of the first Macintosh, MacMag.

1989 – The AIDS Trojan was sent under the guise of an AIDS information program. However, when the users ran this Trojan the hard drive was encrypted and payment was demanded for the decryption key.

1990 was the year that the first virus exchange (VX) BBS went online in Bulgaria. In addition, Mark Ludwig's book in virus writing (The Little Black Book of Computer Viruses) was published. This was the beginning of the underground community that developed and trained its own members.

1991 – Tequila was the first Polymorphic virus that came out of Switzerland and changed itself in an attempt to avoid detection.

1992 was memorable for the media darling; Michelangelo. This same year the Dark Avenger Mutation Engine (DAME) became the first toolkit that could be used to turn any virus into a Polymorphic virus.

1996 brought Boza, the first virus designed specifically for Windows 95 files. Concept was the first Word macro virus. Laroux was the first Excel macro virus and Staog was the first Linux virus.

1998 – Strange Brew became the first Java virus. Back Orifice was the first Trojan designed to be a remote administration tool that allowed others to take over a remote computer via the Internet.

1999 saw increased activity in both the number of significant viruses but also in the damaging affects of their widespread distribution. Melissa, Corner, Tristate and Bubbleboy were just a few. Bubbleboy was significant because it was the first worm that would activate when a user simply opened an e-mail message in Microsoft Outlook and previewed the message in Outlook Express. This was the proof of concept and Kak became very widely spread using this same technique.

2000 – The first major distributed denial of service attacks shut down major sites such as Yahoo!, Amazon.com and others. The Loveletter worm became the fastest spreading worm; shutting down e-mail systems around the world. This year saw the first PDA virus called Liberty, which

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

was designed to prevent pirating of the Palm Game Boy game also called Liberty.

Malicious Code Transmission

In the early days of computing and certainly before the advent of the Internet, viruses and all of their variations were usually spread physically, through the loading of files from a floppy disk. Pirated software would frequently contain viruses and as users would share these disks, the virus would spread accordingly.

Today, e-mail has become the most popular form of transmission. From Melissa and Love Letter to the recent Sir Cam and Hybris, e-mail worms have taken the Internet community by storm. In fact, of the annual 10 most widespread infections, worms accounted for half in 2000, sharing the No. 1 honors with macro viruses, according to security site SecurityPortal. And early indications in January and February suggest that worms will account for at least eight of the top ten slots in 2001, with AnnaKournikova, Hybris and Love Letter variants leading the list.[3]

There are two types of worms. The first type basically needs human intervention. Because they rely on file-to-file transfers, they are generally sent through e-mail. These are also know as mass-mailers because of their ability to take advantage of vulnerabilities in e-mail clients, usually Microsoft Outlook, and propagate themselves through the infected users address book.[3] Social engineering is pervasive in luring the recipient into opening the infected e-mail. The general rule of thumb was that in order for the worm to activate, the user had to actually open the infected attachment. Of course, this went out the window after worms such as Kak and Bubble Boy were released. All it took was for AutoPreview on the Outlook client to be turned on and these worms would be activated through the Microsoft Active X control Scriptlet.Typelib.

The second type of worm is the network aware variety. Certainly by the end of this year, the most notable network aware worm will be the Code Red worm. According to a SANS Security Alert, on July 19, the Code Red worm infected more than 250,000 systems in just 9 hours.[4] The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the

---

[3] Robert Lemos, "Year of the Worm." March 15, 2001 URL: http://news.cnet.com/news/0-1003-201-5125673-0.html (27 July 2001)
[3] Robert Lemos, "Year of the Worm." March 15, 2001 URL: http://news.cnet.com/news/0-1003-201-5125673-0.html (27 July 2001)
[4] The SANS Institute, SANS Security Alert. "Code Red is Set to Come Storming Back." July 29, 2001

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

others causing the rate of scanning to grow rapidly. This spread has the potential to disrupt business and personal use of the Internet for applications such as electronic commerce, e-mail and entertainment. This type of worm does not need any human intervention. It simply takes advantage of know security vulnerabilities.

Each day brings new forms of MalWare. Toolkits such as the VBS Worm Generator, written by an 18-year-old named Kalamar, make constructing copycat or mutations of previously released malicious code easy.[5] Most of these of hybrids combine the worst elements of trojans, worms and viruses. The level of sophistication and the payload are becoming progressively more severe. There is simply no silver bullet. Unfortunately, in a networked environment, it only takes one careless user to launch a virus and start the chain reaction. With the increasing number of mobile users attaching laptop computers and PDA devices to the network, maintaining a secure anti-virus defense has become more challenging.

I recommend the following as a multi layer approach to combating the onslaught of MalWare.

- Utilize best practice procedures[6]
  - Back up your critical files on a regular basis. Some viruses may damage files or completely destroy hard drives. Consider an imaging solution like Norton Ghost so that a machine can be completely re-imaged if necessary.
  - Keep your workstation anti-virus signatures updated. Use of an automated routine, such as McAfee's ePolicy Orchestrator, will make this more realistic.
  - If possible, disable the Windows Scripting Host (WSH) program, the active scripting in Internet Explorer and auto DCC reception in Internet Relay Chat client programs on your computer. (Note: These programs may be required for some software, but you should find out if it's needed)
  - Always exercise caution when opening attachments that arrive in e-mail, even if you know the sender. Verify with the sender before opening attachments that you are not expecting.

[5] Michelle Delio, "New Kit Renews E-Mail Scare." March 12, 2001 URL: www.wired.com/news/technology/0.1282.42375.00html (27 July 2001)
[6] Author Unknown, "Best Practices…for protecting workstations from computer viruses" 2000 URL: www.uiowa.edu/~security/docs/bp-viruses.html (27 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Disable the automatic execution of code embedded in documents, if you have software with that feature i.e., Microsoft Office.
- Disable the auto-open or preview of e-mail attachments feature in your e-mail client.
- Don't be fooled by social engineering!
- Turn off VBS.
- Use notepad as the default text editor.

- Develop, monitor and revise a strong workable security policy
  - Use rules-based policy enforcement and virus scanning at the Internet gateway level. This will block viruses, based on known content (e.g. I LOVE YOU in the subject line), even before the anti-virus vendors have released a new signature.
  - Ensure that users cannot disable, modify or remove the anti virus software.
  - Include provisions for laptop computer and PDA's.
  - Maintain policies for outside consultants or sales people that may periodically attach to your network.

- Constant training for users
  - Teach them about social engineering.
  - Share with them the latest information as it comes out; keep it at a novice level.
  - Perhaps publish a small security newsletter with tips and best practices.

- Apply all applicable security patches as soon as they are released.
- Test the effectiveness of your anti virus system by infecting an isolated test bed machine with a known virus. This may be helpful in not only insuring that your anti-virus will detect the virus but also to determine if it responds with the appropriate actions. A tool that may be helpful is the EICAR test string. This can be found at www.eicar.org. This is not a virus, but if an anti-virus scanner finds this string, it will treat it as a virus. This can be used to verify that the scanning engine or services are enabled and running. It is also important to test the virus outbreak procedures and determine how long it takes to identify and eradicate the outbreak. How long does it take to completely eradicate the MalWare? Does it spawn off more infections? If data is lost, are you able to restore all of the damaged data? These questions need to be answered satisfactorily.[7]

[7] Jeremy Pickett, "Effective Virus Defense in Heterogeneous Networks" April 9, 2001 URL: www.sans.org/infosecFAQ/malicious/virus_defense.htm (27 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

New technologies are allowing more malicious code to be detected with less administrative efforts. Heuristic scanning for example, is designed to detect previously unknown viruses. Viruses that are newly released into the wild for which anti-virus vendors have no specific definition files may be detected by scanning the files more intensively, searching line by line for any offending sequences of code. The downside of this type of proactive scanning is false positives; that is the notification of virus like activity that may not be a virus.

Another approach that is different from the traditional anti-virus systems is Symantec's Digital Immune System. Digital Immune System is designed to capitalize on Symantec's anti-virus technology, IBM's automated virus analysis, and Intel's management technology. This system analyzes any virus that attacks a computer on the network and produces and distributes a fix in minutes. The Digital Immune System will include tools and utilities for systems and policy management, virus protection, server performance, desktop configuration, diagnostics, system stability, remote system operation, management of remote users and disaster recovery all from a single management console. "This is the first step toward a comprehensive system that can spread a global cure for a virus faster that the virus itself can spread," said Steve R. White, senior manager of anti-virus research at IBM's Watson Research Center.[8]

Conclusion

Almost for as long as there have been personal computers and PC programmers, there have been forms of malicious code. They started out as proof of concept code. That is they were meant to show that destructive code could be written that could destroy data and spread themselves to other computers. Soon new barriers were broken as trojans, worm, hybrid forms of trojans and worms appeared into the wild. An underground community of hackers, crackers, and script kiddies developed and trained themselves into a sophisticated group that manages to stay at least one step ahead of the computing community. The game of cat and mouse began. First viruses would appear in the wild as somebody became infected with the latest Malware. Then the virus was analyzed and a virus signature was made available for the anti-virus users. The users were protected, as long as they maintained the latest virus signature, until a new virus hit the scene. And finally, the cycle would begin all over again. There are still only a couple of ways that computers can become infected with destructive code. The majority of

[8] Author Unknown, "Symantec Unveils Digital Immune System Strategy for Unprecedented Level of Managed, Intelligent Protection and Control." May 11, 1999 URL: www.symantec.com/press/1999/n990511.html (27 July 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

these occur due to computer users being complacent and unaware. A few basic rules will eliminate most of the widespread propagation of viruses. First and most importantly, every user must use a reliable anti-virus product and keep it maintained with the latest signature files. I am constantly amazed at how many people don't realize how vital this is. Since the majority of viruses today are transmitted through e-mail, users should never open e-mail attachments unless they know the sender and are expecting a specific e-mail attachment from that person. Simple configuration changes can be made to eliminate VBS and Macro viruses, which are popular these days. Finally, a basic understanding and awareness of how viruses work and which ones are "on the loose" will prevent users from continuing the domino effect of virus infections. Perhaps this game will never end but a collaborative effort by all computer users will serious impede the growth and damage caused by Malware

Suggested Links:

www.cert.org
www.jsinc.com/reghack.htm
www.f-secure.com
www.sarc.com
http://giac.org/cgi-bin/momgate
www.symantec.com/avcenter/hoax.html
www.sophos.com/virusinfo/hoaxes
http://support.ca.com
www.boran.com
www.washington.edu/people/dad
www.grc.com
www.nai.com
www.antivirus.com

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced