GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Match Point:
Analysis of the Anna Kournikova virus

By Mark Muzzi

We've seen this time and time again within the past two years. An innocent looking email arrives in our inbox and subsequently begins to wreak havoc with our company's mail server, and the mail servers of all the addresses listed in our address book. It is the purpose of this paper to examine the latest such outbreak called the Anna Kournikova or VBS/SST virus. This paper will examine the technicalities of the virus, how it was able to spread, and examine how the user can better defend themselves from such a virus. In the end, you will hopefully come away with a better understanding of how a virus works and how to better defend yourself against them.

Malware is the term used to describe types of malicious code. Consisting of viruses, Trojan horses, worms and malicious applets these are the major players in the disruption of productivity among computer users.

A virus can best be described as:

A self-replicating program containing code that explicitly copies itself and that can "infect" other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus.
The two basic types are:

- *File Infector*
- *Boot Record Infector* [1]

Some viruses do little or no damage, simply replicating themselves, while others affect programs a degrade system performance. Never assume that a virus is harmless and leave it alone.

Trojan Horses are programs with a hidden action. Usually they are disguised as some harmless program. A popular example of a Trojan horse is Back-Orifice.

Malicious Applets are applets that attack a local system via the web, and can include denial of service, invasion of privacy, and annoyance. These are different from attack applets, which look for weaknesses in the implementation of the Java security Model

Worm viruses are able to spread themselves either as a host computer worm or a network worm. Host computer worms are local to the machine they run on and use network connections only to replicate themselves out to other computers. Once a copy is made and out on another host, the original terminates itself, so there is only one copy out at any given time. Network worms are made up of various parts called "segments"

© SANS Institute 2000 - 2005, Author retains full rights.

running on separate machines. The network is used for communication purposes as well as propagating segments to new host systems. Worms of both types also tend to propagate themselves without any action form the user.

The Anna Kournikova (VBS/SST) virus aka VBS.Lee-o, VBS.OnTheFly, VBS.Kalamar, and VBS.Vbswg.gen could be either a virus or a worm. The code requires the user to open the email and run the attached file, making it in this respect a virus. Although it has also been referred to as a worm, since it uses a network to propagate itself, instead of using disks or files. It is because of this it is incredibly similar to "Love Bug" virus.

The Love Bug virus appeared around May 4th, 2000. It contained the subject line "ILOVEYOU" and asked the user to check the attached love letter. The love Letter was a VBScript and runs on systems with windows scripting host (WSH) or systems that interpret Visual Basic and have a Wscript library, just like the Anna Kournikova virus. The Anna Kournikova virus itself was written using a virus kit called "Visual Basic Worm Generator'.

The Anna Kournikova virus arrives as an email attachment called AnnaKournikova.jpg.vbs with the subject line " Here you have, ;o)". As of February 15th, 2001, its only known payload is a mass-mailing routine that emails everyone within your Microsoft Outlook Address book, and a date trigger of January 26th, which upon reaching that date, the worm redirects your web browser to a site in the Netherlands. It creates the registry key:

HKEY_CURRENT_USER\Software\OnTheFly

This is the key that attempts to redirect your browser. There is also a registry that is created upon successful completion of the mass-mailing called:

HKEY_CURRENT_USER\Software\OnTheFly\mailed

This key prevents the mail routine from running again. If an attempt is made to delete the worm it will try to recreate itself, but due to a bug in the code, the worm recreates itself as a zero-byte file.

A 20-year old Dutch man with the moniker "OnTheFly" created the virus. What makes this, in the writer's eyes a very significant event, is that OnTheFly proclaims he knows nothing about programming, and set the virus up using a kit called "Visual Basic Worm Generator. In a letter OnTheFly posted on the Internet Tuesday February 13th, he stated that he saw a research note on the website of International Data Corp., a Framingham Mass., analyst firm, that said users had failed to learn anything from the "Love Bug" experience. Taking inspiration from the note, OnTheFly decided to test their theory.

© SANS Institute 2000 - 2005 Author retains full rights.

After releasing his letter and claiming remorse for having caused such a wide outbreak, OnTheFly turned himself into Dutch authorities. The Netherlands has a computer misuse law, but are uncertain if it can be used in this case. It also unlikely that the Dutch Courts will allow the man to be turned over to U.S. Authorities. Also what still remains to be determined are whether charges will be brought against the creator of the virus kit, named Kalamar. Kalamar is an 18-year-old teenager from Argentina. Upon discovery that his virus kit had been used in the creation of the Anna Kournikova virus Kalamar removed the virus tool from his site.

So how was it possible for this virus to Spread so fast? Anna Kournikova virus uses virus characteristics similar to the "Love Bug" virus, running only on windows operating system, and only being able to propagate on machines that had not installed a patch provided by Microsoft for Outlook, after the spread of the Love Bug virus. This virus spread quickly because of ineffective security policies, uneducated users, and in secure systems.

The lack of an effective security policy is extremely dangerous. By not properly stating your company's stance on such matters as information disclosure, responsibilities, backups, virus detection, and other security issues, your company is setting itself up for failure.

An effective security policy should reflect the overall stance of the organization about security, and how that stance will affect the individuals within the organization. The policy should let people know what is expected of them, defining who is responsible for what activities, who has accountability for those activities, and explain what the consequences are for not following them. When creating a policy you must allow room for change, whether it is an overall change in your organizations stance on security or one from within the business community.

Educating the members of your organization to the risk of malicious software should be a key part of your security policy. By letting people know what dangers are out there, you begin to lay down a base layer of protection. Although the Anna Kournikova virus was not very lethal, it is only a matter of time before such a lethal virus will be released upon the world. Education is a major key to this.

One of the best ways to detect and protect against infection is an anti-viral program. Although sometimes these prove in effective, especially when the users fail to update their virus definitions, and when the attacker writes a new virus program that subverts the existing definitions. When this occurs the best way to detect infection is by the indication of different behavior by your computer. The system may suddenly seem slower, the drive light turns on for no apparent reason, and stays on, the drive makes a large amount of noise. These are some sings that there may be infection, but they are not in and of themselves indications that there is infection.

If infection has occurred, DON'T PANIC. The system needs to be contained

© SANS Institute 2000 - 2005, Author retains full rights.

through isolation. Unplug the network connection and leave the system powered and ready, but do not use it. If you are not the System Administrator, contact them immediately and ask for help. Fix the problem by installing anti-viral software to clean up the system or to determine that you are not infected. The last thing you need to do is share your experience. By letting others know, even if you made a mistake, you prevent them from doing the same type of error and causing valuable harm to productivity.

Anti-virus software is an indispensable tool in maintaining a secure work environment. There are three techniques for software protection: activity monitoring programs, virus scanners, and integrity checkers.

Activity monitors or behavior blockers attempt to prevent infection by looking for virus-like activity. (e.g. writing to .exe) They posses the potential to detect viruses that have not been seen before. Bearing in mind that the virus performs some action that the monitor is looking for. These are considered a weak form of defense since some viruses posses the ability to circumvent the monitoring or even have the ability to disable the monitoring.

Scanners are the best-known form of defense. The search for known viruses by looking for signatures or specific algorithms. Norton and McAfee anti-virus are the most popular examples of scanners. Scanners suffer from the fact that they are not proactive, and must rely on existing definitions, thereby causing even simple new viruses to be missed. Alone they are only a partial defense against viruses.

Integrity checkers compute checksums or hash values of files and store the results in a database. Later the program recomputes this value and checks it against the original. If a virus has modified a file the values will not match, indicating that an infection has occurred. These programs are true virus detectors not virus preventers like the scanner anti-virus software.

Remembering the "Defense in Depth" strategy can help us with our virus detection capabilities. Not one type of software defense is by itself a good defense. Only when combined with the capabilities of the other types of software do we begin to get a solid defense. Also a backup strategy should be implemented in the event that a virus leaves us in a position of un-recoverability.

A lack of regular backups can be a serious threat to any organization. Often anti-virus software has never been updated since the time the machine was first turned on. This will result in catastrophe, especially in the case of critical production machines. There are three types of backup techniques: full, incremental, and differential.
Full backups capture all files. They are typically run on a weekly basis, and are necessary to restore a system from a severely damaging event.

Differential Backups leave what is known as the archive bit in place after saving a file. An archive bit is a special tag Windows systems use. It signals the backup program

© SANS Institute 2000 - 2005 Author retains full rights.

that the file has changed since the previous backup took place. Therefore when a differential backup is run on Monday, and the Full was performed on Sunday, the differential Backup will contain only those files that changed since the time of the full backup. Differential Backups will tend to get larger as time progresses, since they backup all files that have changed since the full backup was last run.

Incremental Backups look for changes that have occurred since the last full or incremental backup. It scans the file system and looks for files with their archive bit turned on. When it completes its backup, the files that were scanned will have their archive bits turned off. Administrators can save the system configuration, and then capture changed information quickly using incremental backups. A problem exists in that all incrementals since the last full backup are required to do a full restore. Requiring the administrator to restore first from the full backup and then from each subsequent incremental backup up to the failure.

The purpose of this paper was to examine the technicalities of the Anna Kournikova virus, how it was able to spread, and examine how both users and administrators can better defend their organization from such a virus. The paper touched on different types of anti-virus software, their use, and how proper backups and security policy can best be used together to provide a "Defense in Depth" type structure against viruses. Although recent history, basically the subject of this paper, tells that these lessons have yet to be learned. Hopefully through reading this you have come away with a better understanding of how important it is to defend against such threats.

Sources

[1] http://www.faqs.org/faqs/computer-virus/faq/index.html

Alijo, Hernán, ZDNet Latin America and Lemos, Robert, ZDNet News, "Purported 'Anna' virus toolkit author yanks files from site" February 15th, 2001, ZDNET http://www.zdnet.com/zdnn/stories/news/0,4586,2686768,00.html

Leyden, John, "Dutch Police arrest virus suspect", The Register, February 14th, 2001 http://www.securityfocus.com/news/153

Leyden, John, " Kournikova virus strikes net" The Register, February 12th, 2001 http://www.securityfocus.com/news/151

Delio, Michelle, "Why Worm Writter Surrendered", Wired News, February 14th, 2001 http://www.wired.com/news/culture/0,1284,41809,00.html

Chien, Eric, and Hindocha, Neal "Virus Encyclopedia: VBS.SST@mm",

© SANS Institute 2000 - 2005 Author retains full rights.

Symantec, February 12th 2001
http://www.symantec.com/avcenter/venc/data/vbs.sst@mm.html

Green, John "Security Essentials 1.1" SANS Network Security 2000, October 20th, 2000

Northcutt, Stephen "Information System Security K-2" SANS Network Security 2000, October 16th, 2000

© SANS Institute 2000 - 2005, Author retains full rights.