Global Information Assurance Certification Paper

The Mass Mailers - @mm

VBS.SST@mm - aka AnnaKournakova.jpeg.vbs

By: Gavin Lowth

Table of Contents:

Mass Mailers:

The term mass mailer is a generic one that is used to describe a particular type of threat that has distinctive properties. Mass mailers are normally referred to as worms or viruses that, once executed, will attempt to send a copy of itself to every email address in a users address book. The worm or virus is either executed automatically or unknowingly by the user, and is usually an attachment that forms part of an e-mail message.

The Scenario:

If you were browsing through your e-mail messages on the morning of February 12th, you might have come across a suspicious e-mail message from an unknown sender. Under normal circumstances, you would have opened the e-mail message, scanned through the contents of the body and deleted it, thereby making sure you stuck to your companies security policy of deleting all e-mail messages from unknown sources. You are quite sure this policy exists, because the Human Resources department made you sign the new policy just three weeks ago and this was something that was brought to your attention.

You know that these messages normally contain some sort of virus; because you get one or two of them a month and they normally turn out to be some sort of malicious code that deletes files on your hard drive or causes your system to crash. The companies e-mail administrator normally confirms your suspicions, later on in the day by sending out an e-mail message to the entire company. This e-mail message states that users are not to open up a specific attachment of a particular e-mail message confirming once again that it does contain a virus.

On this particular morning however, something does invoke your curiosity. The name of the file that is attached to your e-mail message reads, AnnaKournikova.jpg.vbs. You know you should delete the message but you are certain that this is a picture of the Russian born tennis star, Anna Kournikova in some sort of precarious pose. You have to check it out, so you double-click the attachment and, making sure the “open it” check box is selected, you click “OK”. What happens next you are unsure of, however you do not see a picture of Anna Kournikova splash across your screen but you do notice that you computer’s CPU has gone crazy and your Outlook outbox contains 150 unsent e-mails and the number is increasing rapidly.

The Threat:

The threat that corporations are exposed to from viruses and worms is an old one. The threat from these mass mailers, however, is relatively new with the first one wreaking havoc on the Internet in 1999. The creators of these mass-mailing threats must somehow get users to initiate a program or run a script and thereby set off a chain of events that will ultimately lead to the propagation of the worm or virus. In severe cases, these scripts will be automatically run, not when the attachment is executed but when the e-mail itself is viewed.

One of the tools most widely used by these virus writers is to invoke human curiosity. This is the way that the majority of mass mailer worms get propagated today. The threat normally arrives in the form of an e-mail message, as in the above scenario, with an attention grabbing subject line. Once the user opens the e-mail message and executes the attachment, the worm propagation process starts.

Once the attachment is executed, the end results are identical. Your corporations e-mail servers normally grind to a halt or crash trying to process huge amounts of unwanted e-mail. Invariably, a lot of this e-mail does get processed and in severe cases causes a global slow down of Internet traffic. Worm propagated e-mail messages increase, available bandwidth decreases and gradually business conducted via the Internet slows or even worse for some corporations, it stops.

As all of these mass mailer threats are coming from the Internet or through corporate e-mail systems, most of the focus for the deployment of anti virus software is moving away from the desktop & file servers and onto e-mail and gateway servers.

Defence in Depth:

Almost all corporations run some sort of anti virus software within their network. Layers of protection vary, however all companies will under normal circumstances protect desktop and file servers. Others will protect desktops, file servers and Groupware servers such as Microsoft Exchange and Lotus Domino Server. Some corporations, normally the larger ones, that perceive they are more exposed and at higher risk use a multi tier protection approach.

In the multi-tiered approach, anti virus software is normally deployed at three different levels. Level one would protect all desktop computers, level two would protect all file server and Groupware servers and level three would protect all e-mail gateways and firewalls. Almost all antivirus vendors would recommend this multi-tiered approach. Whilst some cynics would state this is just another way of increasing revenue for these software vendors, the risk of infection from virus type activity using this method is significantly lower.

The Worm:

A worm by definition, according to the Trend Micro website “is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or e-mail attachments.”

This particular worm, vbs.sst@mm, according to the Symantec AntiVirus Research Centre “is a VBS e-mail worm that has been encoded using a virus creation kit. This worm arrives as an attachment named AnnaKournikova.jpg.vbs. When executed, the worm e-mails itself to everyone in your Microsoft Outlook address book”.

This particular virus creation kit is widely available on Internet sites and can be downloaded free quite easily. The tool itself is a 1.5-megabyte application that requires a small amount of user intervention to create a malicious VBScript. At the current time there is even an upgrade version of this particular kit that contains options to inflict even more damage on infected systems.

The payload for this particular worm and for most forms of mass mailers is to spread as many copies of itself and to infect as many other users as possible. The only other payload property for vbs.ssm@mm is that every January 26th of each year, the worm will attempt to redirect your browser to a Dutch shopping website, www.dynabyte.nl.

The first major outbreak of a mass mailer type of virus was the Melissa virus that was discovered in March of 1999. The Melissa virus however is not technically a worm but a word macro virus and takes advantage of some of the vulnerabilities in Microsoft word. It will attempt to e-mail a copy of the infected attachment to 50 other people in your Outlook address book. The point here is that mass mailers can fall into two categories, a worm, a virus or a combination of both.

The majority of the mass mailer outbreaks after the Melissa virus were worms. Examples of these worms were VBS.Loveletter.A, W32.Prolin.worm and W32.Navidad, all attempting to distribute copies of themselves via Outlook or another MAPI compliant e-mail client.

The Vulnerability:

The main area of vulnerability that these types of script based worms take advantage of is the use of the Windows Scripting Host. According to the Microsoft website the “windows scripting host is a tool that allows users to run VBScript and JavaScript within the base operating system on Windows 9.x and NT operating systems”.

The windows scripting host has received a lot of attention recently with regards to the propagation of worms and viruses and is generally viewed unfavourably in the industry. It is however generally misunderstood to what types of functions this tool actually carries out. This tool is in essence a language checker and verifies what language the script has been written in. Once the script has been identified as either VBScript or JavaScript, there are two ways these scripts can be executed, embedded and stand-alone.

- Embedded – The script is embedded within a HTML page and will be automatically executed when the page is viewed. The problem with this is that the user has no control when the script is executed. Viruses such as Wscript.Kakworm and VBS.bubbleboy use this method to execute their payloads.

- Stand-alone – The script needs some sort of external trigger to execute

the code. The majority of viruses and worms are run via this method and is the reason why virus writers need to catch the attention or invoke curiosity of users to execute the script.

What can be seen from the above explanation is that on its own the windows scripting host is not a vulnerability at all and has no ability to affect the operating system. It can however interpret what language a script is written in and pass it over to an application or service that does have the ability to run these scripts automatically and thereby opening up the vulnerability. This process is normally used by legitimate applications to carry out their normal functions, however as can be seen this same powerful tool can be used to execute malicious scripts as well as the good ones.

One of the ways around this vulnerability is to disable the windows scripting host, which is a simple enough procedure. The downside of disabling the Windows scripting host is that it is integrated into a number of Windows applications and services and the amount of objects that are affected by this change are unknown. At first users could notice nothing wrong with their systems but further down the track programs that are executed could yield unexpected results and programs might not function correctly.

Detection:

Determining whether a file or program is infected with any sort of virus or worm is inexact. This is partly due to the fact that anti virus products by nature can only normally detect threats once they have been identified. Under normal circumstances, customers detecting virus like activity from files or programs will submit a sample of the file to their anti virus vendor. The vendor will check the sample for malicious code and release a signature in the form of an updated pattern file if the sample indeed turns out to be malicious. The anti virus software maintains a *"working database"* of these pattern files that it continually checks files and programs against for a signature match. This method of scanning is generally referred to as signature scanning and is the most widely used technology in anti virus programs today.

When a new type of mass mailing worm does get released into general circulation, the time taken for vendors to get new signatures to their customers that detect this new threat is paramount. The time taken for customers to access vendor's websites and download new signature files increases exponentially, as the amount of traffic on the Internet increases due to the propagation of the new mass mailer. New ways to distribute new pattern files during these major mass mailer outbreaks are always being sought. Satellite technologies are one of the alternatives that are being developed to update software as quickly as possible without using the Internet as a media.

The most effective way of combating mass mailers is not to get exposed to the threat at all. In other words, implementing the preventative measures

before you get exposed to the risk. This is not always possible, but there are ways to maximise your chances. Early warning systems can be put in place that give corporations time at the early stages of the outbreak when the worm propagation is still relatively low. Proactive Virus Notification is one of these early warning systems that most anti virus vendors are offering as a service. Whilst this service is not 100% guaranteed, it does offer corporations a window of time to implement these preventative measures.

Another problem associated with mass mailer outbreaks are the different strains and variants that are released within two or three days after the original threat. The source code of the original worm is easily viewable, it is then manipulated and is sent out again as a different version of the worm and the whole worm propagation process starts again. New signature files need to be produced for this new variant as pattern files for each of these variants differs. This was most apparent with the Love letter mass-mailing worm where there are now over 100 variants of the original worm.

The detection of false positives is also another factor that corporations need to take into account. Whilst false positives do only affect mass mailers, the subject is worth mentioning in any paper regarding the detection of threats. While they are a lot less important with regards system downtime and damage, there is a considerable amount of time spent trying to quash a perceived threat that does not exist. There are approximately 48 000 viruses and worms that can be detected by today's anti virus software and false positives are a reality with any form of threat detection software.

Preventative Measures:

The prevention of the propagation of viruses, worms and other malicious scripts on a corporate network is ideal. Unfortunately as antivirus software is only as good as its latest virus definition files there is no sure fire way to protect an organization from being exposed to vulnerabilities like this one. This is the primary reason that anti virus software must have excellent detect and repair capabilities, detection is a must. There are however some preventative measures that corporations can put into place to minimise the risk to which they are exposed.

- Scanning of all attachments
- Scanning of subject lines in e-mail messages
- Locking down users configuration settings
- Dropping of certain attachments eg *.vbs.
- User education

There is however a balance that corporations must find when setting policies for anti virus software. The functionality and speed that users expect when working within a corporate environment with the safe and appropriate handling of threats associated with virus type activity.

Conclusion:

There is no conclusive way that corporations can fully dispel themselves of

the threats associated with mass mailing worms and viruses. It seems that each major outbreak receives even more press attention than the previous one and corporations seemed to get hit harder each time with estimated loss of revenue reaching into the millions of dollars. Whilst preventative measures that are implemented will certainly lower the risk of infection, early detection via proactive virus notifications in the early stages of worm propagation is still the best method of dealing with this sort of threat. This gives corporations the much-needed window of opportunity to implement defence systems that increase the chances of nullifying the threat.

References:

"The Trend Micro Glossary of Virus Terms."
URL: http://www.antivirus.com/vinfo/virusencyclo/glossary.asp#worm (02 March 2001)

Chien, Eric and Hindocha, Neal. "SARC Write-up - VBS_SST@mm." Last Revision date: 28 February 2001.
URL: http://www.sarc.com/avcenter/venc/data/vbs.sst@mm.html (05 March 2001)

"ZDNet Help & How-To virus."
URL: http://www.zdnet.com/zdhelp/filters/quickstart/guides/0,10606,6013362,00.html (05 March 2001)

"Microsoft Scripting Technologies." Last Revision date: 01 April 200.
URL: http://msdn.microsoft.com/scripting/default.htm?/scripting/windowshost/doc/wsVersion.htm (06 March 2001)

"New Kit Renews E-Mail Worm Scare."
URL: http://www.wired.com/news/photo/0,1860,42375,00.html (05 March 2001)

"Symantec Security Updates."
URL: http://www.sarc.com/avcenter/refa.html (07 March 2001)

Kennedy, Mark. "Script-Based Mobile Threats." Document Date: 27 June 2000.
URL: http://www.sarc.com/avcenter/reference/script.based.mobile.threats.pdf (18 February 2001)

"Understanding Heuristics: Symantec's Bloodhound Technology." Symantec White Paper Series volume XXXIV. Document Date: September 1997.
URL: http://www.sarc.com/avcenter/reference/heuristc.pdf (18 February 2001)