The W32.Magistr.@mm worm

Aka: W32.Magistr.24876@mm
I-Worm.Magistr
Pe_Magistr.A
judge.a
Troj_Arf_judge.a
arf_judge

Author: Robert Pregnell
Y2k GSEC

Table of Contents

Introduction

Of the many threats and vulnerabilities that exist within any computer system, one of the more recognised of these is the computer virus. And as computer systems become more complex, so do the number of mechanisms that viruses use to propagate and inflict damage increase. For example, new technologies that are developed to increase the functionality of an email system, or an operating system, or to exchange documents with other users, equally introduce new ways and means for a computer virus to spread and inflict damage. In light of this, the broad term of a "computer virus" has been extended to include "worms" and the "Trojan horse".

According to Tom Simondi's online Computer Knowledge Virus Tutorial [1], a computer virus is a program that reproduces its own code by attaching itself to other executable files in such a way that the virus code is executed when the infected executable file is launched, typically by user intervention of some sort. The reproduction of the code should be invisible to the user, and a computer virus must allow time for itself to replicate before performing it's often destructive task, which may render the affected system inoperable.

Although very similar to a virus, a worm requires no user intervention to spread, or be triggered. Often, a worm will search network resources for files on other computers which it can infect, and thereby spread itself onto other user's system without the other user needing to "touch" the worm in any way.

A Trojan, on the other hand, makes no attempt to replicate itself, and rather than "infecting" another file, it simply "is" the file itself, which does the damage. The European Institute for Computer Anti-Virus Research states: A Trojan horse is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend" [Summers] [2].

The evolving nature of these types of threats is excellently demonstrated by the w32.magistr.@mm worm, which portrays some complex virus, worm and Trojan characteristics.

What is the W32.Magistr.@mm worm?

According to Symantec's AntiVirus Research Center, the w32.magistr.@mm worm was first discovered on March 13, 2001. It is in fact a polymorphic -type of virus, which portrays worm capability as well [3].

It infects the original computer by infecting Windows portable execution files (not .DLL files) and by embedding calls to itself either within the registry, or inside the RUN= line of WIN.INI.

It is also network aware. Copies of itself can spread across the network via open shared resources (write capability with no password required) again seeking Windows Portable Executables and .scr files within shared folders on other computers across the network. If a \Windows folder is found within the shared folders, it also embeds itself into the RUN=

line of the WIN.INI file inside that \Windows folder. In this way, it has the worm -based characteristic of infecting other computers, without the users of those computers having to interact (or "trigger") the virus in anyway: Those computers are infected by the original "victim", rather than the local user needing to "trigger" the virus by opening an email or attachment. Once infected, they will further spread the infection themselves.

According to Trend Micro, The Trojan component uses SMTP based email clients (like MS Outlook, Outlook Express or Netscape Navigator) to send infected files to email addresses in the Windows and Outlook Express address books of an infected user. [4]

The polymorphic nature is such that:

- It retains a list of names of the 10 most recently infected users within the body of the virus itself
- It randomly uses the \Windows folder, \Program Files folder, or root directory to store working files during infection
- It will use either the WIN.INI file or the Run hive of the Windows registry to launch itself
- The subject line of the infected email message is randomly generated from documents found on the computer
- There's an 80 percent chance that it will add the digit 1 to the second character of the sender address.

This last characteristic prevents replies from being returned to you, which may otherwise alert you to the infection within your own system.

By being Polymorphic, each new instance of the virus is different, and this makes it extremely difficult to detect and repair using conventional signature -based scanning, which is the prime detection method used by antivirus software. The overall signature of any two infections is never the same, and so behavioural characteristics must be used, or several signature characteristics must be collated together to reliably detect it's presence.

The payload of the virus is primarily based around a security vulnerability within Win9x - based computers, whereby grants itself ring -0 priviledges and destroys CMOS data, hard drive data, and flash memory [4]. It also displays one or more messages within Windows dialogs on the screen, and in some instances (depending on the number of days since infection) it moves the desktop icons away from the mouse whenever the mouse approaches the icons, having the effect of the icons "running away" from the mouse pointer.

The vulnerabilities

Understanding which vulnerabilities that the W32.Magistr@mm takes advantage of is the starting point for defining an effective defence strategy. As multiple vulnerabilities are exploited, there are a number of ways in which we can protect systems from attack. These, of course, extend well beyond just the use of virus protection software, and emphasise the importance of exercising "defence in depth" with an effective overall security strategy.

The vulnerabilities are:

- Unprotected system files on a Windows -based computer
- Shared network folders containing critical system files on other computers which allow full access without requiring a password
- Unprotected email systems (no virus protection, attachment restrictions, or usage policy).
- The Windows Scripting Host, installed by default with Internet Explorer 5.x. This is used to interpret and run Visual Basic Scripts, allowing manipulation of the email system, and the use of it's address book to mass -mail newly spawned copies of the virus to contacts found within the email address book itself.

There is much debate as to the vulnerabilities surrounding the Windows Scripting Host, it's proposed purpose and ultimate functionality on a computer. While the functionality basically provides for automatic execution of embedded scripts within email and documents, the debate continues as to what balance is best between "automation" and an acceptable level of risk. At the very least, in keeping with a policy of ensuring all available system patches are installed across all systems on your network, the following URL provides the latest security updates for Internet Explorer, which will eliminate a number of vulnerabilities by having the scripting host installed on a system:

http://www.microsoft.com/windows/ie/security/default.asp[5]

Ways to protect against the W32.Magistr@mm worm

Protecting computer systems from W32.Magistr@mm is difficult because of it's polymorphic nature. The subject line, body and file attachments sent via email will always be different. However, the philosophy of "defence in depth" would lead us to have several mechanisms to protect ourselves from infection. These fall under the categories of:

- Virus protection
- The use of shared resources across a network
- Setting some restrictions on file attachments passing through the email gateway
- Having an effective security policy covering email and system usage.

Virus protection is an essential part of any security model. Effective virus protection software must be installed at multiple points across the network (on desktops, file servers, email gateways, etc) and it must be kept up to date. The fastest and most effective way that virus protection software detects and repairs viruses is by recognising a virus "fingerprint" within a file. The data files that the virus protection software uses to recognise these "fingerprints" must be kept up to date – hundreds of new viruses are discovered every month – and it's essential that these updates be obtained and deployed across all points of the network in a timely manner. However, even the most up-to-date virus protection software will be vulnerable to brand new viruses, which necessitates the other aspects of protection outlined below, while supporting the argument that a good relationship should also be had with the vendor of your chosen anti-virus software. This will help greatly in facilitating the retrieval of the newest virus signature data files, as and when required.

In addition to updates to virus protection software, patches and service packs should also be applied in a timely manner to operating systems and other applications across the network. Know thy system: Make sure you're aware of which programs and OS components are installed, and which vulnerabilities exist within these. Be well informed with regard to the available security updates that are available, and have mechanisms in place to facilitate timely and efficient testing and deployment of these to all systems across the network.

Shared resources across a network can be controlled, or eliminated, by restricting the components of the operating system that are installed to a system. The principal of least privilege would suggest that unless users specifically need to share their files across the network, the File and Printer Sharing network component within Windows should not be installed. Various software tools are available to check for this vulnerability on systems already deployed within the network. At the very least, even those resources that MUST be shared should require a password for access, and unless required, they should be shared in a "read-only" state.

It's also important to consider some restrictions on the types of file attachments that are allowed to pass through the email gateway. Although it's not necessary to completely remove every file attachment from an email, stripping or "with-holding" certain *types* of file attachments can prevent certain viruses and worms such as the w32.magistr@mm from getting to a user's inbox. At the very least, known program file extensions should be blocked, including .EXE, .COM, .SHS, .SCR and .VBS files. This simple restriction doesn't typically impose usage restrictions on a user – it's unusual in most cases for such files to be required and exchanged by users via email. It's also not necessary to entirely delete these file attachments – most email systems allow for them to be held in a "quarantine zone", until the specific need of the attachment can be proven, at which time it can be double-checked for infection before being released to the user.

Often, it's also possible to "identify" virus and worm threats passing through email systems based on the title of the email message itself – the LoveLetter virus was a classic example of this, when the email subject was always "Love letter for you". This subject title appeals to the curiosity of the user, and in simply opening the email, they "triggered" the virus and thereby initiated a wide scale infection. However, due to the polymorphic nature of the w32.magistr@mm worm, the subject line of the message is always different, making this method of detecting the threat ineffective.

It's also extremely important to have an effective security policy in place, which is communicated – and accepted – by all users across the network. This should include email and system usage policies. It should arm the user with information that helps them identify such threats – such as unexpected emails containing file attachments, which they aren't expecting to receive. It should clearly define a usage policy regarding file attachments, including the scanning all file attachments with up-to-date virus protection software before they're opened, and the restriction of such file attachments to just data files, not program files. Remember, settings in place at the email gateway should be the first step in enforcing these policies, but the users should also be made aware of the threats, and of ways in which they too can play an active part in protecting against them. Network users should have the security policy explained to them, and the importance of adhering to the policy. They should also be required to sign the policy to help ensure compliance with it, and to empower the enforceability of the policy within the organisation.

Compliance with the security policy should be checked and rechecked on a regular basis, and consideration in this regard should be given to both systems and users. The security policy itself should be considered as a "live" document – it will require frequent updating to ensure its appropriateness to the latest security threats. Software tools are readily available to ensure that systems comply with certain aspects of the policy (vulnerable shared resources, lack of passwords, etc) and regular audits should be made to ensure this compliance.

Conclusion

Unfortunately, it's impossible to be completely immune from all virus attacks, while maintaining effective connect ability across the network and Internet. Even with all vulnerabilities catered for, and the latest virus signature files applied to your virus protection software, a new threat may one day pass unseen into someone's computer system, and that unlucky person could unknowingly propagate the infection across the network, or externally to other users via email. Should the unthinkable happen, it's essential to have the services of your anti-virus vendor to call upon, in order to get a new signature written which offers protection and repair of the virus with your anti-virus software. A good relationship with your anti-virus vendor is a must.

By keeping an in-depth knowledge of the state of your network, and understanding the vulnerabilities which are exploited by any of these types of threats, you'll be well armed in defining multiple defence mechanisms. You'll also be far less reliant on external assistance in order to provide effective protection from infection or attack.

A balance must be struck between an acceptable level of risk, while maintaining effective communicability with customers and suppliers outside your own computer system and network. Keep your systems up-to-date with available virus signature files and system service packs, while keeping yourself up-to-date with the many listed vulnerabilities that are posted on vendor and security-related web sites and bulletins. Maintain an effective security policy within your organisation – have it communicated well to all employees, ensure that it's realistic in terms of what your users must do, and that it allows them to perform their job without exposing them or your network to unnecessary risk.

References

[1] Tom Simondi's online Computer Knowledge Virus Tutorial
http://www.cknow.com/vtutor/vtintro.htm

[2] European Institute for Computer Anti-Virus Research
http://www.eicar.com/download/trojan_horse.htm

[3] Symantec AntiVirus Research Centre, Security Updates
http://www.sarc.com/avcenter/venc/data/w32.magistr.24876@mm.html

[4] Trend Micro virus encyclopedia
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=PE_MAGISTR.A&VSect=T

[5] Microsoft's Internet Explorer Website
http://www.microsoft.com/windows/ie/security/default.asp