Global Information Assurance Certification Paper

William Cameron
11/19/2000

Level 1 – Security Essentials Practical

QAZ Trojan – A backdoor that you can make sure is shut

William Cameron
11/19/2000

QAZ is described as a "network worm with backdoor capabilities" (F-Secure Virus Descriptions). The malicious code, which has been known about since July 2000, recently made international headlines when it was reported that the program was apparently used as a means to steal Microsoft's proprietary Windows OS and Office source code. Although Microsoft has yet to confirm that it was the QAZ Trojan which compromised its security, various reports from sources close to the investigation have reported that the Trojan worm was, at least in part, to blame for the unauthorized access and potential theft of some of Microsoft's proprietary windows code ("Microsoft hacked! Code Stolen?", "MS intruder may elude authorities", "How Microsoft got Hacked"). This potentially costly security incident may have been avoided, however, if Microsoft implemented and enforced some basic security measures that included any or all of the following actions:

- Implement Antiviral software and scan file/email servers and client computers frequently.
- Update virus signatures Frequently.
- Deploy Microsoft's Outlook 2000 E-mail Security Update for all MS Outlook users.
- Implement enterprise and/or personal firewall solutions.
- Avoid sharing OS system files and folders.
- Implement a comprehensive security policy that explicitly warns and educates end users about the potential dangers of opening certain types of attachments.

In this paper, I will define what the QAZ malicious code is and what is does. In addition, I will provide recommendations regarding the hybrid malware's prevention and removal.

The QAZ Hybrid Virus Defined

To best understand how to protect against the QAZ threat, it is first necessary to understand how the malicious code works. The QAZ trojan-worm is hybrid malware in the sense that it is a network worm capable of self-propagation within a local network that *also* provides backdoor access to infected systems. Since its discovery in China, there have been more than 1000 reported infections (Symantec). The malicious code is identified by several aliases including: note.com, Qaz.Trojan, QAZ.worm, QAZ.A, TROJ_QAZ.A, Trojan/Notepad, W32.HLLW.Qaz.A (Network Associates, Trend Micro, Symantec, Mcafee). The QAZ malware only affects MS Windows operating systems, though it may be spread through other operating systems serving as file or email servers. So far, there are at least four variations of the original Trojan-worm (Symantec). This

paper will focus on the original malicious code since it is the most prevalent among the variants. The QAZ worm's design limits its self-propagation to a local network. Propagation across separate local networks is thought to most likely occur through the exchange of infected email executable or script attachments that may be sent as spam (Symantec, "How Microsoft got Hacked"). When an infected file is executed, the malicious code modifies the system registry to launch during the windows startup. The following line is added to the system registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\Run\StartIE=C:\WINDOWS\Notepad.exe qazwsx.hsq

As a point of interest, the qazwsx file name is thought to derive its name from left most characters on an English keyboard. This registry entry will cause the worm to be activated each time Windows starts up. Once activated, the malicious code stays in memory as an application that runs two processes: a backdoor process and a propagation process. The worm application can even be seen in running in the task list. (Trend Micro's Virus Encyclopedia)

Backdoor Process

The QAZ malware listens on TCP port 7597 for instructions that provide a "backdoor" into the infected system. The trojan program allows three basic commands that may be used to load other malicious programs onto the compromised system. These commands are: "Run", "Upload" and "Quit" (F-Secure).

The Propagation Process

The malicious code also uses TCP port 139 as well as the NETBIOS SESSION service to browse the local network for shared network resources that allow read/write access and contain the 'Win' string in their name. Once such a resource is located, the virus searches for notepad.exe. If 'notepad.exe' is found, the 'notepad.exe' file is then renamed 'note.com'. The malicious code then copies itself as 'notepad.exe' on the remote shared resource. When the replaced 'notepad.exe' file is run by a user on the affected machine, the malicious code contained in the 'notepad.exe file will run, transparently activating the virus which will then launch the original notepade.exe file renamed as 'note.com'. After successfully spreading to another host, the trojan worm will then email a notification to a remote host (202.106.185.107) containing the IP address of the infected computer (F-Secure, Mcafee, Trend Micro).

Implement Anti-virus Protection

Antivirus software companies have known about the QAZ Trojan-worm threat since mid-July 2000. Antiviral signatures needed to detect and eliminate the malicious code have been available from Symantec, Mcafee, Trend Micro and Grisoft since early August 2000.

By installing antiviral software on system servers and desktops, scanning files regularly and frequently updating the software's virus signatures, it is possible to detect and retard the spread of the trojan worm via infected files sent through infected email attachments.

According to Symantec's AntiVirus Research Center Director, Vincent Weafer, "A Microsoft employee, consultant, or outside developer with internal network access had not been running a scanner." ("Microsoft – burned by anti-virus software.") Had all Microsoft employees been using antiviral software updated with current virus signatures, the Trojan worm would have likely been detected and removed rather that ultimately allowing for the theft of some of the company's most closely guarded secrets. In fact, were antiviral software installed, it may have prevented the Trojan's access to the local network entirely if the original infection did enter the network via email. Unfortunately, is not uncommon that many programmers choose not to run antiviral software. According to Mikko Hypponen, a security expert for F-Secure, "The fact that the worm had infected programmers' computers was not unusual because programmers usually disable virus protection software, which slows down computers" (Strupczewski and Grinsven, "Microsoft Hackers Reached Key Programs").

Removal

Once infected with the malware, there are only two methods of removal. The recommended removal method is to install one of the many anti-virus software packages that are capable of detection and removal of the QAZ malware. Once installed, the anti-virus package should be immediately updated with the latest virus signatures. Following the update, a complete scan of all files on the system (including archived files) is recommended.

The alternative to the automated removal described above is manual removal. Manual removal requires that the following system registry entry

HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\Run\StartIE=C:\WINDOWS\Notepad.exe qazwsx.hsq

be removed and the 'note.com' file renamed as 'notepad.exe'. Any other infected files (attachments, executables, scripts …) should also be deleted to avoid re-infecting the system.

Deploy Microsoft's Outlook 2000 E-mail Security Update for all MS Outlook users

The QAZ Trojan worm's design limits its propagation to a local network. It is possible, however, to still propagate the virus through email and file sharing. In addition to antiviral software, Microsoft's Outlook 2000 E-mail Security Update can be used to help retard the spread of worms for MS Outlook 98 and 2000 users. Microsoft made the update available after many network worms started using the features of the popular email client to propagate via email. While the QAZ worm does not use these features directly to spread itself within a local network, the Trojan may still be spread to other computers, including those outside the local network, via infected files sent as email

attachments. Microsoft's Outlook 2000 E-mail Security Update can help prevent the spread of such attachments.

Once installed, the Outlook 2000 E-mail Security Update prevents users from launching executables, macros or scripts received in email messages (MS Outlook 98/2000 E-Mail Security White Paper). This added security can help prevent unsuspecting users from opening potentially dangerous email attachments. Unfortunately, the security update has no way to distinguish between "good" attachments and those that are "bad". As a result, the security update essentially prevents running any executable or script from email, which can also affect everyday work-related file sharing. Therefore, most administrators/users will only want to consider applying this patch when security is crucial. By preventing the execution of potentially infected attachments, the security patch could have prevented QAZ from gaining access to the local network via email. In addition, had a machine become infected via diskette or through server based file sharing, the Outlook Security Update would have detected and prevented the Trojan's attempted email notification to 202.106.185.107. For Outlook email users, the Outlook Security Update would have notified the infected computer's user that there was a program trying to access Outlook's email functionality instead of allowing the Trojan to notify someone at 202.106.185.107 that the computer was now compromised. The Outlook 98/2000 security update is available from Microsoft's web site at:

http://www.microsoft.com/office/outlook/downloads/security.htm

At this link, you can find out more details about the Outlook Security Update by reading the Outlook 98/2000 E-Mail Security White Paper.

Implement Firewall Protection

The QAZ worm propagates, reports back what systems it has compromised, and allows access to the infected machine via TCP ports. Firewalls can provide port filtering to block unauthorized access to these ports. Even if infected, the worm's spread and impact may have been severely diminished if there had been some sort of firewall(s) in place. For organizations, port filtering is possible through access lists on routers and through the use of various firewall software and hardware based solutions. Even telecommuters and mobile staff now have access to inexpensive software based firewalls (such as ZoneAlarm and Blackice Defender) and port filtering devices (such as the Linksys FastEthernet Cable/DSL Router). Had personal firewalls been deployed on every workstation, the port filtering software would have likely detected and prevented the worm's propagation. Furthermore, the use of any type of organizational or personal firewall would have been able to block access to TCP port 7597 also preventing access to any infected machines. As hybrid viruses such as Trojan worms become more prevalent, organizations and individuals should, at a minimum, install firewalls to protect the integrity of their systems.

Avoid Sharing OS System Files

Generally speaking, the risks of sharing OS system files are usually much greater than any convenience or need that would require it. Often, users will share their entire

hard drives in order to conveniently provide remote access for themselves and others to files on their system. Unfortunately, Trojans such as QAZ take advantage of such shared resources to propagate themselves across a local network. The QAZ trojan worm searches for shared resources containing the string 'WIN' and assumes those remote resources are system root directories that contains the 'notepad.exe' file. If QAZ is unable to find 'notepad.exe' because the system folder is not a shared resource, then the worm is unable to propagate itself to the remote machine. Therefore, users should carefully consider what files and/or directories that they intend to share and limit shares specifically to those resources. If Microsoft employees followed this policy, the QAZ Trojan worm's *self*-propagation would have been prevented.

Implementation a Clearly Understood Security Policy

It is likely that Microsoft has a security policy in place that specifically addresses the precautions that employees should take before opening potentially infected files. It is unclear, based on this incident, whether or not any such policy was well understood or even enforced at Microsoft. Anyone who has access to an organization's information technology resources should have the organization's security policy clearly explained in order to avoid security breaches. Whenever possible and appropriate, the policy should be reinforced with training and then consistently enforced.

Conclusion

Microsoft's security breach is a clear example of how organizational security is only as strong as an organization's weakest security link. To protect organizational assets from QAZ as well as other trojan worm hybrid viruses, organizations should take the following actions to improve the security of their IT systems and provide multiple "layers" of protection.

1. Organizations should implement antiviral software and frequently update virus signatures to detect and remove malicious code.
2. Organizations that use MS Outlook 98 or 2000 should consider deploying the Outlook Security Update to help prevent the propagation of malicious code.
3. Organizations should invest in firewall solutions to prevent unauthorized access to network resources.
4. Organizations should develop, implement and enforce a clearly understandable security policy to minimize human actions that can lead to the activation and propagation of malicious code that ultimately undermine the security of an organization.

Organizations can learn from Microsoft's example, for if Microsoft had implemented all of these basic security procedures, they may have been to prevent the unauthorized access and theft (copy) of some of their most closely guarded secrets. In fact, by failing to prevent unauthorized access to some of its Windows code, Microsoft has lost much more than just their code. The have lost consumer confidence and may also lose competitive advantages depending where the code turns up. Worst of all, Microsoft's stolen Windows code may potentially be used to provide crackers with the blueprints to millions of Microsoft customers' computer systems. As a result,

Microsoft's stolen code may now be used by those who broke into Microsoft to determine additional security weaknesses inherent in Windows, which could ultimately compromise the security of millions of Microsoft's customers. The lesson to be learned here is that the failure to implement the basic security measures proposed in this paper can lead to even more serious security issues that can be costly both organizations and their customers.

References

Anti-virus and Security Links

McAfee Virus Information library	http://vil.nai.com/vil/dispVirus.asp?virus_k=98775
Symantec Antivirus Center	http://www.symantec.com/avcenter/venc/data/qaz.trojan.html
F-Secure	http://www.fsecure.com/v-descs/qaz.htm
Trend Micro	http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_QAZ
Microsoft Outlook 98/2000 E-Mail Security Update White Paper	http://www.microsoft.com/office/outlook/downloads/security.htm

Online Journals and Articles

Bridis, Ted and Buckman, Rebecca. "Microsoft hacked! Code Stolen?" October 27, 2000. WSJ Interactive Ed. (via) http://www.zdnet.com/zdnn/stories/news/0,4586,2645850,00.html (10/28/2000 8:44:21 AM)

Lemos, Robert "Microsoft – burned by anti-virus tools?" October 27, 2000. http://www.zdnet.com/zdnn/stories/news/0,4586,2646200,00.html (10/28/2000 8:43:10 AM)

Lemos, Robert "MS intruder may elude authorities" October 27, 2000. http://www.zdnet.com/zdnn/stories/news/0,4586,2646331,00.html (10/28/2000 8:39:06 AM)

Merritt, Tom. "How Microsoft Got Hacked." October 27, 2000. http://www.techtv.com/callforhelp/projects/story/0,3650,3008126,00.html (10/28/2000 9:06:05 AM)

Strupczewski, Jan and Van Grinsven, Lucus. "Microsoft Hackers Reached Key Programs" .October 27, 2000. http://www.techtv.com/cybercrime/hackingandsecurity/story/0,9955,3008128,00.html (10/28/2000 9:04:58 AM)