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

The Hacking of Microsoft

Ernest E. Quaglieri

In October 2000, the unthinkable occurred when Microsoft Corporation was hacked. While we all realize deep down that no one is invincible, I doubt that any sizable wagers were placed indicating that the mighty Microsoft would be a victim.

The irony of it all is that Microsoft was hacked not by some new undetectable technology, but by a Trojan written in a language developed by Microsoft itself. (MS Visual C++) It also appears that the Trojan was spread not by some covert undetectable means, but by carelessness on the part of a Microsoft employee(s).

As large companies go, Microsoft is prime material for hacking attempts. The corporation is hated by many because of the alleged monopoly and poor software design. Many underground groups exist solely due to a mutual dislike of the software giant. In light of this, one would think that security for this corporation would be in a constant state of "Red Alert." Initially, this was reported as a very sophisticated break-in. After examining the facts however, it appears that this incident could be accomplished using very available programs from the web, and a bit of social engineering.

Microsoft has not released a great deal of information about the attack, but several points are well known. It appears that the QAZ Trojan was used, and it appears that a Microsoft employee working remotely introduced the Trojan into the system.

The QAZ Trojan was discovered in China in July of 2000. This is how the QAZ Trojan operates. It is distributed via Email or network. If distributed by Email, the social engineering phase is important. It has to be in a message that someone wants to open and not just delete as Spam. The Trojan does not need mapped drives to infect other computers. This Trojan tries to locate other systems using Netbios browsing, looking for other computers where the WINDOWS folder is available.

Once activated, the Trojan searches for notepad.exe and will copy itself in place of this file, while renaming the original note.com. This is important because when the victim launches the Trojanized notepad.exe, the note.com program is executed, making it appear that all is well. It also modifies the following system registry entry to execute itself every time the system is started:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
StartIE=C:\WINDOWS\NOTEPAD>EXE qazwsx.hsq

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The backdoor routing is quite simple as it supports only a few commands, Run, Upload and Quit.

The Trojan searches the entire Local Area Network for additional copies of notepad.exe to infect. Once a computer on the LAN is infected, it will mail the IP address to the author of the Trojan, (one address obtained was 202.106.185.107, listed somewhere in China) activate the Winsock and listen on Port 7597. The existence of "note.com" and newly created "notepad.exe" of 120,320 bytes, along with data traffic packets on TCP Port 7597 are indications of infection.

Here is some code from the worm:

```
2E 68-73 71 00 00       qazwsx.hsq
74 65-2E 63 6F 6D    %s %s   note.com
52 45-5C 4D 69 63         Software\Mic
64 6F-6E 5C 52 75    rosoft\Windows\C
69 6F-6E 5C 52 75    urrentVersion\Ru
45 00-4E 55 4C 4C    n  startIE  NULL
00 00-72 00 00 00       roc *       r
65 00-72 00 00 00    notepad.exe  r
00 00-6E 6F 74 65    note.com     note
00 00-25 64 2E 25    .com         %d.%
25 64-2E 25 64 2E    d.%d.%d \\%d.%d.
00 00-5C 5C 00 00    %d.%d   %s   \\
64 2E-65 78 65 00    %s\notepad.exe
6F 74-65 70 61 64    SOFTWARE\notepad
```

As the Trojan spreads and more machines from the LAN send their IP addresses, the chance of getting in to a machine that is trusted by an important server grows.

Now that we know how it works and how it spreads, the next logical question is, "How did it happen to Microsoft?"

It is apparent that an unidentified Microsoft employee received an Email carrying the QAZ Trojan. The Trojan executed on that users computer and when that user connected to the network, the sender of the Trojan had a list of IP's of all the compromised computers on the LAN. The Trojan apparently could not get any useful information from the Developer's network to which the initial infected machine connected. However, as the Trojan spread, it eventually infected a computer trusted by a network containing other machines with valuable information. It has also been speculated that some mutated form of the Trojan allowed the bad guy to download additional tools to the compromised computers. This would appear logical since Microsoft Security detected that passwords were sent to a Russian Email drop.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

It was simple. So simple that anyone with a little Internet knowledge who visits hacker sites and reads of their conquests could do it. Of course, a little criminal intent is required.

So what are the results of such a hack?

It depends on the perspective. For Microsoft, it undoubtedly caused a severe case of embarrassment as well as fears of compromised source code. It probably also caused some resumes to be updated and sent out to on-line job sites. The latest estimates are that the hackers had access to this particular network for 12 days, from October 14 to 25, 2000. It is unknown why Microsoft Security people did not notice any suspicious activity in their logs for such a lengthy period. Since passwords were "sniffed" leaving the network bound for Russia, the hacker(s) may have set up their own accounts, even administrator accounts on the compromised servers. Microsoft has been understandably quiet and evasive as to what was seen or taken, but many have speculated that source code for present and future products were either seen or stolen. One obvious concern is that somewhere within the millions of lines of code for a future operating system, the hackers placed a little code of their own, namely a back door into the product to be exploited after release. If the code was simply downloaded and examined, the hackers would have a head start on finding exploits for the product long before it is even released. Microsoft claims that the company was examining every computer file on the compromised system that was modified for any reason during the preceding three months. They were also examining recently shipped computer code for Windows ME, Windows 2000, Outlook, Outlook Express and the Microsoft Office suite of business applications.

Another thought on the matter is that Microsoft may later claim that code in a competitor product is actually code stolen from Microsoft. Although this would certainly be an uphill battle for Microsoft, it has to be an issue that open source developers are concerned with.

Kevin Mitnick, an infamous hacker recently released from prison gave the keynote address at the Software Development Conference and Expo 2000. He gave it via satellite link because his terms of release prohibit him from travel, owning or using a computer or providing computer-consulting services. According to Mitnick, this incident will temporarily raise awareness about computer security, but will not generate the kind of long-term security focus needed to stem the tide of computer attacks. Mitnick says in part that the attack "will raise the awareness for two, three, four months, but then people will relax." He also states, "You think people would learn, but they don't."

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

What can we do to prevent it?

There is some debate as to what can be done to prevent such attacks. The answer seems to be that there IS no one answer. Anti-Virus software is somewhat effective provided the vendor has supplied the correct signatures, or the heuristics feature of the program detects the bug. After researching some hacker methods of subverting anti-virus systems, I compressed a popular Trojan using a shareware tool called Neolite. I then Emailed myself the virus and it came through undetected, although my anti-virus program is set up to scan Email attachments. The signatures did not recognize the Trojan now that it was compressed. (Neolite creates a compressed executable version of the program.) Once activated (on a now closed system of course) the anti virus software caught it. If we add a slightly different twist to the scenario however, the results may not have a happy ending.

If the victim takes a corporate laptop home and the virus program is out of date or non-existent, then upon return to the corporate network other computers are in danger. This is especially true when virus signature updates are left to the user. Another issue is the danger of the Trojan passing by the Email gateway anti-virus protection, because the anti-virus program does not recognize the signature due to a program like Neolite. Again, the corporate network is at the mercy of the workers attention to detail, in keeping virus signatures up to date. While using common sense in opening attachments should apply, "sneakier" viruses and Trojans are appearing all of the time that require no user intervention to launch.

The lesson.

- Protection must occur at all levels of the network. Users must constantly update Anti-Virus programs on client machines. A product that can push new signatures to clients can offer an advantage.
- Every machine on the network should have an Anti-Virus program with current updates installed, no exceptions.
- Computers connected to the network should not have modems or be dual homed to an ISP or untrusted network.
- Virus protection should be installed on the mail gateway as well as the server.
- Trained security personnel should inspect laptops that are used for off-site work and then returned to the network, before being allowed on the network.
- If physical user policies are not available, be aware of users installing AIM Instant Messenger and other types of software that creates a security risk.
- Have a strong and enforceable written policy concerning computer usage.
- Review firewall, proxy server and event logs frequently.
- Obtain the training that you need to become proficient in protecting your network.
- Close all ports that are not needed.
- If your system provides notification services, set it up to dial your pager if an event occurs. The sooner you know, the faster you can act.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Keep in mind that power users are just as likely to breach security policy as general users. In fact, they may be more likely since their knowledge of computer systems is greater and with that may come a certain sense of invincibility. In addition, their accounts may carry more privileges than the average user account.

Set a good example for your users. Take the time to explain why all of these annoying procedures are necessary. If you make everyone part of the security "team," you will have a much better chance of protecting your company's resources, and keeping out of the employment line.

Sources:

Ryder, Josh. "Microsoft Gets Hacked - What Can We Learn?" 30 Oct 2000. URL: http://www.securityportal.com/articles/mshacked20001029.html (5 Jan 2001)

Symantec. "W32HLLW.Qaz.A." 16 Jul 2000. URL: http://www.symantec.com/avcenter/venc/data/qaz.trojan.html (5 Jan 2001)

Bridis, Ted and Buckman, Rebecca. "Microsoft Hacked! Code Stolen?" 27 Oct 2000. URL: http://zdnet.com/zdnn/stories/news/0,4586,2645850,00.html (6 Jan 2001)

Pournelle, Jerry. "QAZ Notepad Trojan Hacks Into Microsoft." 20 Nov 2000. URL: http://www.byte.com/column/BYT20001113S0001 (6 Jan 2001)

McGuire, David. "Mitnick: Microsoft Hack Won't Raise Awareness." 31 Oct 2000. URL: http://www.washtech.com/news/software/4769-1.html (7 Jan 2001)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.