QAZ Trojan on Campus

Deanne Palmer

As systems administrator at a small liberal arts college with a student population that has grown up with the Internet, it seems that we're receiving an increasing number of complaints from other sites regarding probes coming from our campus. Like most other small colleges, IT is a small shop. We all wear many hats so except in the case of a reported compromise, tracking complaints sometimes takes a back-burner to other seemingly more pressing issues, but we do follow up and sometimes, as in this case, find a virus is the cause of the problem.

A recent complaint about a computer from our site probing port 139 (Netbios – Session) of IP's on a government site prompted tracking and the subsequent discovery of the QAZ Trojan on a student's PC on the campus network.

Incident Report

On Friday, November 10, 2000 an email was received from the system administrator of a government site regarding a probe that was reported by one of their firewall managers. It indicated that an IP from the college campus was probing hosts on one of their networks.

This is a portion of the log that was included in the message:

```
Nov  9 00:26:14 us.site1.gov 247900: 2w0d: %SEC-6-IPACCESSLOGP:
list inboundanle denied tcp aaa.bbb.162.216(2440) (Serial1/2 *HDLC*) ->
xxx.yyy.232.1(139), 1 packet

Nov  9 00:26:2 us.site1.gov 247901: 2w0d: %SEC-6-IPACCESSLOGP:
list inboundanle denied tcp aaa.bbb.162.216(2441) (Serial1/2 *HDLC*) ->
xxx.yyy.232.2(139), 1 packet

Nov  9 00:26:28 us.site1.gov 247902: 2w0d: %SEC-6-IPACCESSLOGP:
list inboundanle denied tcp aaa.bbb.162.216(2442) (Serial1/2 *HDLC*) ->
xxx.yyy.232.3(139), 1 packet

Nov  9 00:26:35 us.site1.gov 247905: 2w0d: %SEC-6-IPACCESSLOGP:
list inboundanle denied tcp aaa.bbb.162.216(2443) (Serial1/2 *HDLC*) ->
xxx.yyy.232.4(139), 1 packet

Nov  9 00:26:42 us.site1.gov 247907: 2w0d: %SEC-6-IPACCESSLOGP:
list inboundanle denied tcp aaa.bbb.162.216(2444) (Serial1/2 *HDLC*) ->
xxx.yyy.232.5(139), 1 packet
```

(The identifying portion of the college IP has been replaced with 'aaa.bbb' and the government IP has been replaced with ‘xxx.yyy’ in the sample log. Host names are also fictional.)

The sys admin’s message reported that the log was in Mountain Time. Being on the East Coast, we adjusted the log times by 2 hours.

The log indicates a series of probes of port 139 (Netbios Windows file sharing) of the government host IPs xxx.yyy.232.[1-5] from our site (aaa.bbb.162.216) on Nov. 9, 2000 at 2:26 a.m. EST.

Tracing the IP

The college uses a DHCP server to assign network IP’s for most of the desktop computers on campus. Over the past summer, the college implemented a network segmentation project, which divided our network into VLANS to handle various user populations. For security purposes, administrative areas of the campus were segregated from public labs and from student residence hall VLANS. From the IP reported, it was fairly simple to identify the VLAN/ building that had originated that IP lease based on our network map. We were able to determine from our DHCP logs that the IP address had been leased at the time of the probe. Egress filtering would have prevented a spoofed addresses from leaving our network.

Relevant entries from the DHCP log:

```
11,11/9/00,02:11:52,Renew,aaa.bbb.162.216,jane something,<MAC address>
11,11/9/00,03:11:52,Renew,aaa.bbb.162.216,jane something,<MAC address>
```

(Names are fictional and the MAC address has been removed.)

This indicated that the lease was effective from 11/9/00 2:11 a.m. through 3:11 a.m. – the period of the probe.

The DHCP logs gave the MAC address and the name of the computer (“jane something”). The logs also showed that the lease for that IP had been continually renewed by the same MAC address and in fact was still being used by that MAC address. The MAC address and the name of the computer were useful for identifying the owner of the machine.

From campus mail logs we were able to identify a specific user who had been sending mail from that IP. The college network technician verified that the MAC address was connecting from the switch on the residence hall floor where the user we identified lived. The name on the computer was also the first name of the user we had identified, so we were fairly confident that the computer was the one used in the probe.

We saved all relevant logs and contacted the student. We explained to the student that we had received a complaint from an off-campus site regarding an incident that had originated from her computer. The student said she didn't know anything about it and had not let anyone use her computer. She was very cooperative and anxious for us to take a look at her computer. She reported that she had recently been working on a paper in MSWord. She turned away from her computer and returned a minute later to find her paper had been completely erased. The residence hall computer consultant tried to find the paper, but there was no trace of it. She is convinced that the remote hacker erased the paper.

The Infected Student Computer

The student did not have any anti-virus software on her computer. She was running Windows 98, and upon checking the task manager on her machine, no unusual processes appeared to be running, except a program called ptsnoop.exe. We later learned that ptsnoop was part of the modem software.

The student rarely turns off her computer. She reported that she had recently been awakened during the night by noises from her computer, as if it was writing something to disk. She also reported that the date on the computer had been changed several times over the past week. She had changed it back only to find that it had been changed again.

Trend Micros' Housecall anti-virus scanning software http://housecall.antivirus.com) was used to scan the machine and indicated that it was infected.
It reported:

Virus		Location	
TROJ_QAZ.A	uncleanable	C:\Windows\notepad.exe	06-12-00 12:44 a.m.

The infected "Notepad.exe" file was copied to a floppy for later perusal. A search of "QAZ.A" on the Symantec Anti-virus Research Center website (http://symantec.com/avcenter/vinfodb.html) for further information provided a removal program and additional information about the virus. We downloaded the removal program to the infected PC and followed the directions for removal with no problems.

About QAZ

"Trend Virus Report, November 2000 Issue # 3" reported TROJ_QAZ.A as number 5 of the Top Ten Viruses for the week of November 6-12, 2000.

The virus is also known as Qaz.Trojan, Qaz.Worm, and W32.HLLW.QAZ.A. Symantec Anti-Virus Research Center reports that "W32.HLLW.Qaz.A was first discovered in China in July of 2000."
Information from Megasecurity.org (http://www.megasecurity.org/~masterrat/Trojaninfo/Qaz.txt) indicates that QAZ was used for the Microsoft Internal Network break-in on October 25, 2000.
The Microsoft Internal Network attack is attributed to an employee opening an e-mail

attachment with the virus on a home computer while attached to the Microsoft Network.

F-Secure's Anti-Virus website (http://www.datafellows.com/v-descs/qaz.htm) reported QAZ as a "network worm with backdoor capabilities, which spreads itself under Win32 systems. The worm was reported in-the-wild in July-August, 2000. The worm itself is a Win32 executable file and about 120K long, written in MS Visual C++."

The file NOTEPAD.EXE file that we removed from the infected computer was 118K, so it fit the description of the famous worm that had invaded Microsoft.
Trend Micro (http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_QAZ.A) describes QAZ as "network aware" and "able to spread itself through shared resources over a local area network".

TROJ_QAZ.A renames the original NOTEPAD.EXE to NOTE.COM on the infected computer, and replaces NOTEPAD.EXE with the Trojan. It makes changes in the registry so that the infected file is active every time Windows is started:

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

When the user executes NOTEPAD.EXE, the script sends an e-mail with the IP of the infected computer to an Asian IP address(202.106.185.107) and sets up a listener on port 7597, then it executes NOTE.COM(the original NOTEPAD.EXE), so that the user is unaware of any problem. It uses the socket on port 7597 to receive commands that it executes on the infected machine. The Asian address is a Class C. Whois on apnic.net revealed:
Search results for '202.106.185'

```
inetnum      202.106.0.0 - 202.106.255.255
netname      CHINANET-BJ
descr        CHINANET Beijing province network
descr        Data Communication Division
descr        China Telecom
```

Source of Infection

How the machine was initially compromised is unknown. There are references to probing on NETBIOS port 139 in the tech detail about TROJ_QAZ.A and that was the port being probed at the government site from the infected computer. This suggests the student computer may have been compromised from another infected computer through file sharing, but other sources suggest that the source was an e-mail attachment or an IRC chat room.

Information from Megasecurity.org

(http://www.megasecurity.org/~masterrat/Trojaninfo/Qaz.txt) suggests that the attacker also uses port 7597 to download several attack tools, such as packet sniffers, to retrieve passwords and other sensitive information from the local network which are then sent to a Russian e-mail address in St. Petersburg. Charles Babcock of Internet Week suggests that this server in St. Petersburg "could have been a reflector site, forwarding an attack that arrived under an alias that prevents further tracking". Various sources suggest that the Trojan tries to spread itself to other shared drives on local networks. Although it may have originated as an e-mail attachment, it does not mass e-mail using addresses from the user's address book as some of the other viruses do.

A check of college mail logs for the Russian e-mail address that was mentioned as a dropbox turned up nothing. A search through mail logs for the infected IP indicated that all mail from that IP appeared legitimate; nothing had been sent off-campus from that IP address. The student revealed that she mainly uses an AOL account for e-mail, so any mail drops probably did not go through the campus mail server.

Assessing the Damage

If the loss of a paper is the only damage sustained at the college, we should consider ourselves very lucky. Like Microsoft, we don't know how long the intruder was on our local network. We don't know whether a sniffer was used, or whether passwords were stolen. There haven't been any other signs of intrusion, or any other reports of probing. The ACL's on the router should have isolated any sniffing to the residence hall VLAN, which is a minor consolation.

Preventing QAZ

All of the college-owned desktops run anti-virus software, which is updated on a timely basis, so that the college desktops are protected from the current version of QAZ. Students bring their own machines to campus and all of the residence halls have one 'port per pillow'. This translates to mean that each student in the dorm has at least one ethernet access port for the college network. Over 90% of students own their own computers. The college strongly suggests that students invest in anti-virus software, but it's left up to the students to purchase and install it. To attempt to reduce the number of new infections of QAZ on campus, a message was sent to the campus community warning students about the virus and again recommending they install anti-virus software on their computers to prevent infection.

In the Computerworld article "Update: Microsoft stung by hack attack", Graham Cluley, a security expert at Sophos Anti-Virus is quoted as saying that "an attack with a worm such as QAZ shouldn't have been possible if Microsoft had properly configured its firewall and anti-virus software". In our case, anti-virus software on the student's PC could have prevented this attack as well.

Firewall rules at our Internet gateway have been implemented to block traffic on port 139 (Netbios file sharing) and port 7597 (used for controlling the infected PC). Any traffic to the Asian IP that was notified by the Trojan was also blocked. A constant problem with both the current anti-virus software and the firewall solution is that variations of the worm may appear that will use another port or otherwise change the signature of the virus rendering these preventive remedies useless.

In "Microsoft Hacker Incident - Looking Back" by Finjan Software (http://www.megasecurity.org/~masterrat/Info/finjan09112000.txt) , it was noted that a change in the compression tool that is used for the virus will change the signature enough that anti-virus tools will not immediately be able to recognize it. The "Lovebug" virus and all its variations were used as an example of this technique. It warns against a false sense of security that anti-virus software fosters, leaving companies unaware that many compressed viruses do not need to uncompress to run, and will pass through anti-virus security undetected.

The sys admin at the government site that was probed has been notified that the QAZ virus was found on the computer that had been probing their site and that the virus had been removed. We've had no further reports from them or anyone else regarding probing from the infected PC, but will continue to search our network logs for any signs of attempted activity on port 7597 or from IP 202.106.185.107.

References

APNIC.NET Whois Database. URL: http://www.apnic.net/apnic-bin/whois2.pl?search=202.106.185 (Nov 17, 2000).

Babcock, Charles Interactive Week November 9, 2000 "Experts Ponder the Microsoft Attack" URL: http://www.zdnet.com/intweek/stories/news/0,4164,2652161,00.html (Nov 20, 2000)

Common Criteria, "Consider the lowly worm…", Wednesday 1st November. URL: http://www.commoncriteria.org/news/newsarchive/November2000/news263.htm (Nov 17, 2000)

Common Criteria, "Another Type Of Virus Hits The World (And Gets Microsoft No Less)", November 09, 2000. URL: http://www.commoncriteria.org/news/newsarchive/November2000/news275.htm (Nov 17, 2000)

Finjan Software, " Microsoft Hack Aftermath - Microsoft Hacker Incident - Looking Back", Nov. 9, 2000. URL: http://www.megasecurity.org/~masterrat/Info/finjan09112000.txt (Nov 17, 2000)

MegaSecurity.org, "The QAZ Trojan Program - Microsoft Internal Network Hacked;

Source Code Stolen", October 30, 2000. URL: http://www.megasecurity.org/~masterrat/Trojaninfo/Qaz.txt (Nov 17, 2000)

Symantec Anti-Virus Research Center. URL: http://symantec.com/avcenter/vinfodb.html (Nov 14, 2000)

Symantec Anti-Virus Research Center "W32.HLLW.Qaz.A". URL: http://www.symantec.com/avcenter/venc/data/w32.hllw.qaz.a.html (Nov 14, 2000)

Trend Micro Housecall Anti-Virus Scanning Software. URL: http://housecall.antivirus.com (Nov 17,2000).

Trend Micro US Virus Research Group, Trend Virus Report, November 2000 Issue # 3, November 16, 2000, Vol. 11/03 "10 Most Prevalent In-the-Wild Malware Surveyed by Trend US (week of: 11/06/2000 to 11/12/2000) "

Weiss, Todd R and Rosencrance, Linda   Computerworld October 27, 2000 "Update: Microsoft stung by hack attack" URL: http://www.computerworld.com/cwi/Printer_Friendly_Version/frame/0,1212,NAV65-663_STO52949-,00.html (Nov 20, 2000)