Global Information Assurance Certification Paper

QAZ

Charles R. Fagg

QAZ is a network worm. It infects "in the fashion of a companion virus"(4, 14). It is a Win32 executable file written in C++. It first appeared in China in July, 2000 and by Aug 9, 2000, SARC had received over 70 submissions (1). Still this virus/Trojan is considered to be the basic vector in the Microsoft hack.

There have been many papers discussing the major aspects of this companion virus and a compilation of several of these papers indicates that there may yet be surprises.

THE INFECTION PROCESS

The infection process itself has a surprise. The primary source of infection is thought to consist of delivery by email, downloads from a web site, or through IRC chatrooms (6), but in an article in "From Chaos Manor Mail – Mail 128 – Nov 20-26, 2000" (3) we have the following dialog apparently indicating a forth method of infection.

http://www.jerrypournelle.com/archives2/archives2mail/mail128.html#QAZ
See "More on the QAZ situation" – Monday Nov. 20, 2000.

> "Dear Jerry,
> With regards to Miles Turneys' email about the QAZ worm,
> I can confirm that it can infect PCs directly, not necessarily
> via email or downloads
>
> In summer I was running a single PC – no firewall – on
> a dial up connection at our beach house. Two or Three times
> while connected Viruscan popped up a window announcing
> that it had intercepted the QAZ worm. One of these times the
> PC was just setting there idle while we were having supper…
>
> David Cefai"

Whether the PC was sitting in an idle loop or running a screen saver was not said. An analysis of this mode of attack could have said a lot. If this PC was not already infected (the Viruscan apparently did not detect it) the mechanism of this attack through an ISP and dial up modem implies another infection mode available to QAZ..

From this same article (3) Miles Turney speculates as follows which initiated the above response:

> "…and I don't think I got the virus from email. I do though spend

> great amounts of time dialed online downloading newsgroups files. Right before I was notified about the virus I had just been online downloading a game for about 3 continuous days. I assume someone probed my machine and uploaded the virus like that since I do not have any type of firewall software. It is also possible that it was in one of the files I downloaded. By the way, I am using Norton Anti-Virus 2001 and it did not detect the virus until I did a full hard-drive scan, even with the latest definitions at the time. It did not detect it when it actually infected my machine. I hope this is informative and keep up the great work on BYTE.
>
> Miles Turney "

Looking at both comments, it is possible to glean the following:

1). Neither was using at firewall at the time of infection or attempted infection. Probes would not have been stopped or recorded.

2). In the case where infection actually occurred, Norton AV detected QAZ on the HD but not during the download (or entry) process. Viruscan did detect QAZ on the entry process.

3). A PC can be probed during a download or in an idle loop for open ports.

Could this forth mode of infection be directed through some open port at a randomly selected or predetermined IP address? The circumstances in David Cefai's statement can be read to indicate this.

THE WORM QAZ

Normally the worm spreads a copy or itself through local network drives that are read/write shared. Actually shared files are all that is necessary. The worn scans network resources and looks for the WIN string in their names (1), for example, the WINDOWS directory on a remote computer within a LAN. It then looks for the Notepad.exe file. If it finds it, it renames it Note.com which is a file about 52 kbytes in size and then writes itself into a file named Notepad.exe file which is a file of about 118 kbytes in size (5, 13). The larger size for Notepad.exe and the existence of the file Note.com means probable infection with the QAZ Trojan.

The QAZ worm normally gets into a LAN PC from outside the LAN via its virus character as an email attachment that must be opened by someone (6). Infection is not enough however. The worm must be activated by a user running Notepad.exe (1). When activated, the worm registers itself in the windows registry in the auto start section:

HKLM\Software\microsoft\Windows\Current Version\Run by entering the value

Start1E = "Notepad.exe qazwsx.hsq"

which allows QAZ to then start up each time the PC is booted. I assume that most use notebook because it is larger, if for no other reason. QAZ on my machine would never be activated unless someone specifically wanted to see something under notepad or I call it by accident. The implications of accidental activation or human engineering are implied and related to stealth.

QAZ does not spread itself by email but it does have email capability. When the worm is activated, it spreads via shared files on the LAN only, opens a back door to listen for incoming TCP/IP connections on port 7597 which provides three functions, and emails the IP address of the infected computer together with its password file (user name and password, the latter usually encrypted) to the Asian IP address:

202.106.185.107 where the inetnum 202.106.0.0 – 205.106.255.255
and netname CHINANET – BJ

where BJ is the Beijing Providence (2, 7, 10)

A cracker can, using the existing user account obtained from the password file, log on as the user and from that account attempt to obtain the required privileges to open new accounts with more privileges (10). If the cracker cannot do this, he still has the back door on port 7579 and that backdoor route supports three commands. They are: Run (a specified file), Upload (create a file on the infected machine), and Quit (terminate worm activities). Hence anything can be installed and run in the infected PC. QAZ is therefore referred to as a common crackers tool (10). I expect that the uploaded tools are deleted after use (upload and run a small uninstall or delete script) and uploaded again when needed. This leaves as little as possible to be found on the infected machine(s); except QAZ itself. One can upload tools to the infected PC and hack another PC anywhere (12). No trace to the actual hacker connected to the QAZ infected PC is likely once those tools are removed. He can include tools that modify or remove logs.

QAZ requires user interaction such as emailing or posting (to a news group) for downloading (11) to get into the LAN as a virus. It does not have the ability to spread itself autonomously outside a LAN (11, 14). It knows the host IP address to send "home", it can determines the class of IP address. It can determine the LAN boundaries from this, but the exact mechanism by which the Trojan activity remains within the LAN on which the initial infection occurs remains for analysis.

Selective infection is characteristic of this companion worm. "Such a virus, designed to break into a single company, authored to spread in only a limited fashion to avoid calling attention to itself is possible to write "(2). If this was a specification sheet, it happened and is called QAZ. This Trojan if introduced onto a LAN could remain hidden

for years if host level AV software is not updated and used (7).

There is an additional aspect of QAZ. It has the ability to compromise security settings (5, 14). This is not unexpected since this Trojan needs the power to rename files, write or upload files, and execute files, delete files.

Detailed removal instructions and a fix tool for QAZ are found in (5) and are not repeated here. Norton's AV Center suggests sharing with read-only access or using password protection on the shares if write access is necessary. Encrypted file transfer is another option (9).

SPECULATION AND THE GREATEST HACK

The QAZ virus was found involved in the Microsoft hack (8) where Gary McGraw said: http://www.zdnet.com/enterprise/stories/main/0,10228,2652161,00.html

> "…the QAZ Trojan found at Microsoft is a form of remote execution software that is planted on a computer through an e-mail attachment, a Word document.
>
> Once the document is opened, an underlying Word Macro or Application script is activated and …"

There are many reasons why Microsoft may have been hacked. We got the Biggest, an assault on Microsoft's image, an attempt to plant dirty code or having some think that someone did thereby impairing Microsoft's credibility, to post the source code claiming "Information Should Be Free", to trade the code in the hacker community, to demonstrate that with enough time, resources, and money, almost any computer network can be hacked. On and on the list of possible reasons go. Perhaps only the hacker knows for sure.

But, hacking and a successful hack are not the same thing. Most are caught rattling the doors. A few get in but are discovered (and possibly identified and caught) before any compromise occurs. On occasion however, a hacker gets in and undiscovered, spends weeks and possibly much longer with his effort (2).

Somehow QAZ got onto an internal development LAN at Microsoft. It was not detected when it entered or for some time after. Estimates range from a few days to months. It either came in through the mail servers most likely well protected with AV software or it was brought in some other way. There are several possibilities.

QAZ could have been sent in as an encrypted email attachment sent to an employee with an account somewhere on the development LAN in question. (Sending it to all on the LAN is an option but this would have to be handled by the server from the inside by

some kind of "copy all" request). That would get it past the mail server AV software and onto the LAN. If that LAN did not use host AV on it's PCs, or had it turned off , this employee would have to decrypt the email to infect his PC. QAZ would still have to be activated by accessing Notepad on that infected PC. Then QAZ will spread by the Trojan mode to most if not all of the other PCs on that LAN that had shared Windows directories or shared Notepad.exe files.

This Microsoft LAN could also have been initially infected via sneaker-net, either through detachable media or by connecting it to an infected portable PC. It has been said that an employ had taken a portable PC home and that PC became infected while connected to the Internet via a dial up ISP. Two possibilities:

1). This portable PC was infected as a result of a horrific QAZ spamming incident on the Internet (10).

2). This PC was targeted via IP address (possibly random) / port scanned and infected as described by the forth method under "The Infection Process" while connected to the Internet via his ISP (3).

Both of these seem remote. For Microsoft, most papers I've read favor infection by email attachment. Encrypted email attachments requires decryption on the inside. All methods require activation on the inside by accessing Notepad. The Windows directory is not normally a shared directory. Notepad.exe is not normally a shared file. The C drive…?

The rest is history.

WHAT'S NEXT

From an MSNBC news Bulletin (2) written by Bob Sullivan, MSNBC, we get a glimpse using five quips from this document found at:
http://www.msnbc.com/news/481998.asp?cp1=1#BODY
(See complete story).

"Microsoft break-in takes hacking to a new level."

". . .But computer-security experts have long feared what a clever hacker with a more stealthy virus planted inside a company might be able to accomplish. Those fears are now reality, and the successful attack on Microsoft is being called "the biggest hacking case ever," …"

> " … "WE'VE BEEN FORECASTING worm-based industrial espionage to happen for quite some time," said Mikko Hyppönen, anti-virus researcher for F-Secure Corp. "It has finally happened. I'm just surprised it happened at the top." …"
>
> "…At a hacker conference in Amsterdam this week called "Black Hat Briefings," computer security researchers were openly speculating about the possibility of a successful Trojan attack. One theory: a computer criminal could create a designer virus aimed at breaking into a single company, authored so it would spread in only a limited fashion. That would prevent the rogue program from calling attention to itself, which would prevent anti-virus companies from finding it and adding it to their anti-virus detection software. …"
>
> " …"There is no way to guarantee you are 100 percent secure," said one hacker, who asked not to be identified. "If you really want to do it, you can write a program to do that."
>
> A successful attack would only require convincing one employee to open the virus. …"

Any of this sound familiar?

LESSONS LEARNED

We are dealing with a selective, stealthy infectious agent in that the spreading process is limited. When introduced into on a single LAN without effective AV protection, QAZ can remain for a long time undetected. With QAZ, anything can be uploaded and run. An infected PC can, using uploaded tools, attack anything. When caught in a trace or in a log, the owner is the owner of the infected PC and not the attacker. Usually the attack tools will be found on the QAZ infected PC only during use. They will not be there when someone knocks on the door (12).

The most desirable PCs to infect are those that are always left on and connected to a LAN that is connected to the internet or connected to an ISP through a DSL. These machines are always available to the attacker either through the back door or through direct logon via the users account name and password provided by QAZ.

The first lesson: Turn the PC off when not in use for more than a few hours. This denies the use of the PC to the attacker when you are not using it, which is usually a large

© SANS Institute 2000 - 2005 Author retains full rights.

percent of the 24 hour day. When you are using it, consider heavy unexpected HD use to be trouble and act accordingly (12).

The second lesson: If you are on a well protected internal LAN and things from the inside start showing up on the outside, some host(s) on that internal LAN probably contain(s) a big surprise (11).

The third lesson: Even with up to date AV you can still be infected. AV companies may not know about a new virus or Trojan and with no signatures, you will not be able to detect the intruder with a simple scan.

The forth lesson: Learn to use Netstat –a and run it often. This will list all ports that are connected and all ports that are listening and can be connected to by others. You want to know about any that you don't normally use.

The fifth lesson is the unthinkable one. If you are dealing with a selective limited spreader, there may be an insider involved. Contact, then leave it to the people whose job it is to handle this type of thing.

RESOURCES:

1. F-Secure Virus Descriptions:
NAME: Qaz ALIAS Worm QAZ , Worm_qaz
http://www.Europe.F-Secure.com/v-descs/qaz.shtml

2. MSNBC How did it happen? By Bob Sullivan MSNBC
http://www.msnbc.com/news/481998.asp?cp1=1#BODY
(Click on complete story).

3. From Chaos Manor Mail – Mail 128, Nov 20 – 26, 2000
See "AND more on the QAZ Situation:" Monday Nov. 20, 2000
http://www.jerrypournelle.com/archives2/archives2mail/mail128.html#QAZ

4. Open Document

Name: QAZ.worm
Aliases: QAZ.trojan,TROJ_QAZ.A,W32.HLLW.Qaz.A,QAZ
http://www.canada-av.com/sensible/home.nsf/0e4787861e3415d6852568c900171f98/8c257bbb0cf2c4388525693b007f82c9?OpenDocument

5. SYMANTEC SECURITY UPDATES W32.HLLW.Qaz.A
(Companion Virus)
http://www.sarc.com/avcenter/venc/data/w32.hllw.qaz.a.html

6. Qaz.trojan Infects Networks By Robert Vamosi August 14, 2000
http://www.zdnet.com/filters/printerfriendly/0,6061,2605063-2,00.html
also
http://www.zdnet.com/zdhelp/stories/main/0,5594,2605063,00.htm

7. THE SECURIUS NEWSLETTER

December 7, 2000 | Vol. 1, #11 | http://www.securius.com
http://www.securius.com/newsletter/archive/111.txt

8. Experts ponder the Microsoft attack
Charles Babcock, Interactive Week
November 9, 2000 4:37 PM ET
http://www.zdnet.com/enterprise/stories/main/0,10228,2652161,00.html

9. EBuilt An Enterprisr Application Builder – ENCRYPT is the answer.
http://www.ebuilt.com/MeetEbuilt/Covered/10092000cw.htm

10. Linnet Solutions _ The home PC model "How was Microsoft Cracked"
http://www.ec11.dial.pipex.com/virus.htm

11. **Microsoft Corporation: "What the QAZ happened?"**
Timothy J. Rogers November 21, 2000
The Microsoft Hack:
http://www.sans.org/infosecFAQ/malicious/QAZ2.htm

12. **QAZ Trojan on Campus** Deanne Palmer November 21, 2000
http://www.sans.org/infosecFAQ/malicious/QAZ_campus.htm

13. QAZ by Kevin Skelly - UMass
http://www.oit.umass.edu/publications/at_oit/spring01/skelly-viruses.html

14. UVa Information Technology and Communication
Virus Alert on W32.HLLW.Qaz.A
http://www.itc.virginia.edu/desktop/security/w32hllwqaz.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS