Global Information Assurance Certification Paper

Mark Golden

Assessment of Microsoft's Security Policy and Methods as Demonstrated by the QAZ Trojan Attack

Securing your network and information resources is of utmost importance in today's business environment. One would think after all of the media attention on hackers, viruses, and attacks that by now this would be obvious to large corporations, especially those involved in manufacturing computer security applications. However, security can get lost in the details, and no matter how many precautions are taken no one is impervious to network attacks. Network and information security tools and techniques are not guarantees and at best can slow down experienced hackers enough that they direct their attention elsewhere. In late October, Microsoft's network was compromised again. Let's look at the details of this security breakdown and see if Microsoft is the victim of a patient hacker or left itself open to a known attack and glean a few lessons for our own security practices.

All of the details of the attack are still not fully known by the public. Initially it was believed that the hackers had access to Microsoft's network for weeks or months. Now Microsoft asserts that the attack lasted only 12 days. They also claim they monitored the attack from the moment it began on October 12th and have "accumulated detailed information that will help identify the hacker[1]."

Microsoft security employees "detected passwords being remotely sent to an e-mail account in St. Petersburg, Russia. Microsoft… interpreted electronic logs as showing that those internal passwords were used to transfer source code -- software blueprints -- outside the Microsoft campus[2]." Here is a clear example of the importance of logging security and system information. Microsoft's logs allowed them to identify the attack, the specific areas that had been compromised, and possibly capture enough information to identify and prosecute the attacker.

It appears the hacker gained access using the QAZ Trojan which first surfaced in China in July of 2000. Experts believe an employee received e-mail carrying the dangerous software payload on their home computer and inadvertently installed it. The employee used the computer to check emails and work on Microsoft's network. QAZ probably stole the user's passwords and sent them to a computer in Asia, allowing him to then logon to Microsoft's network posing as the employee and access restricted areas. QAZ gave the intruder some control over the victim's computer, and it automatically spread to any computers it found in that section of Microsoft's campus. QAZ also may have automatically downloaded and installed hacker tools from a Web

site in the South Pacific[3]. Apparently, Microsoft did not have all of the access points to their network secured. Even if their internal network was protected from the QAZ Trojan, not protecting their remote access system resulted in a security breakdown.

QAZ is a network worm that spreads itself under Win32 systems. "The worm itself is Win32 executable file and about 120K long, written in MS Visual C++. When an infected file is executed, the worm registers itself in Windows registry in auto-start section." It installs itself as Notepad.exe and renames the real notepad application Notepad.com, calling it after it the worm has executed to keep itself hidden from the user. QAZ has two processes, a spreading process and a backdoor process. Additionally, QAZ has "just three commands, but that is enough to install any other (more powerful) trojan/virus to the computer… The worm also sends a notification to its "host" (worm's author?). This e-mail message is sent to some address in China. The message contains the IP address(es) of infected machine… To locate an infected computer within a network is possible by checking whether it sends/receives data on TCP port 7597[4]." The QAZ Trojan has been known for several months. It is unknown if Microsoft failed to require their remote access users to implement personal firewall software or update their virus scanning software to identify and remove QAZ, or if this was a lapse by the employee. Either way, Microsoft should have been able to identify and remove this known Trojan once it attempted to access the network. Unless QAZ has the ability to activate ports, if Microsoft had disabled port 7597 it could possibly have prevented information from being sent out of its network.

The facts of this attack point to possible break downs in virus scanning/ protection, network access point protection, not disabling unused ports, monitoring and logging, and security policy. If Microsoft really did identify the Trojan as soon as it was introduced and monitored and logged all of it's activity from the beginning, their security infraction in this case appears to be concentrated on their remote access virus protection and possibly unused ports being enabled. Let's look at two more areas of security since a network breach in itself may not be very damaging if Microsoft is practicing security in depth. Let's look at their data integrity protection and security policy in regards to attack response.

The New York Times reported that according to Microsoft, hackers were able to view the source code for future product releases but were not able to steal the code for the Windows or Office software. Microsoft also asserted that no software programs were changed, which would indicate no viruses were introduced to their future software releases[5]. However, according to an anonymous hacker interviewed by Wired, "There are thousands upon thousands of lines of code in those applications. How could anyone resist tinkering a bit? And believe me, it would be very hard to find a little customization in all that code[6]." I don't know the what Microsoft uses to protect their data, but one would think they use an encrypted checksum or similar means to ensure

their valuable source code has not been altered by an unauthorized party. And further, just as data stored on the network can be altered, these checksums should be kept on a floppy or a server/ storage media not connected to the network where they could be changed to cover the hacker's tracks.

Microsoft had two significant responses to the attack. First, they called in the FBI to assist in the investigation. The FBI sent in a "13-member Computer Analysis Response Team… to examine Microsoft personal computers and review network logs to detect any digital fingerprints that might be traceable to the hacker." Second, "Microsoft temporarily blocked all its global employees from accessing the corporate network from outside their offices over the weekend to ensure that any hacker also would be blocked from returning." It is reported that Microsoft has, and as a result blocked access to, roughly 39,000 employees with remote access to their network[7]. Was Microsoft's security policy adequate to respond to this attack and was that level of response appropriate? It appears that Microsoft moved quickly and had the tools in place to respond to this attack. As far as the appropriateness of the response, that depends on the reality of what was compromised. If the hackers obtained proprietary code, or changed code on the network, calling in the FBI and shutting down access to 39,000 employees may be perfectly valid. On the other hand, if Microsoft is correct in their statement that no code was altered, the hackers only had a few minutes to actually view the code, and only minimal amounts of code for future releases was obtained, the cost involved in their response (tax payer cost of the FBI's resources and Microsoft's cost in loss of productivity from shutting down remote access) may be excessive. I don't know if these courses of action were in Microsoft's security policy or they were simply reactions to the situation, but analyzing the costs involved demonstrate the importance of documenting your security policy including responses to varying levels of security breaches.

---

[1] Bridis, Ted. "Microsoft Says It Detected Hacker Quickly, Monitored Activities Throughout Attack." Wall Street Journal. 30 Oct 2000. URL: http://public.wsj.com/home.html (search by date for "Microsoft").

[2] Bridis, Ted. "Hackers Break Into Microsoft's Network And May Have Stolen Code for Software." Wall Street Journal. 27 Oct 2000. URL: http://public.wsj.com/home.html (search by date for "Microsoft").

[3] Bridis, Ted. "Hackers Break Into Microsoft's Network And May Have Stolen Code for Software."

[4] Kaspersky Labs, F-Secure Corp. "F-Secure Virus Descriptions: QAZ." October 2000. URL: http://www.f-secure.com/v-descs/qaz.htm.

[5] Markoff, John and Schwartz, John. "Microsoft Says Hackers Viewed Source Codes." New York Times. Oct 27 2000. URL: http://www.nytimes.com/2000/10/27/technology/27CND-SOFT.html.

[6] Delio, Michelle. "Hackers Crack Into MS System." Wired. 27 Oct 2000. URL: http://www.wired.com/news/culture/0,1284,39778,00.html.

[7] Bridis, Ted. "Microsoft Says It Detected Hacker Quickly, Monitored Activities Throughout Attack."

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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
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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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 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
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