Global Information Assurance Certification Paper

Microsoft Corporation: "What the QAZ happened?."
By Timothy J. Rogers

The Microsoft Hack:

Microsoft Corporation was the victim of a successful break-in to their corporate developers network during October 2000. Microsoft known worldwide as a software giant and to some as controlling the market in operating systems now has a blemish that may taint their reputation as a reliable company for some time to come.

The hack reached the media stream around the 27th of October 2000, and was described as an attack that lasted possibly months, thus causing the loss of operating system code, and application code not yet released. Microsoft made several media announcements claiming that the hack lasted no more than twelve days, and none of their source code was stolen. Microsoft also states that they were aware of the hacker(s) presence. The FBI was called in to investigate the break-in and lend their assistance in uncovering the criminal(s) involved

How does the break-in affect Microsoft, Windows users?

During the initial press release days of Microsoft's break-in, rumors sped around the media circuit claiming that Microsoft source code had been taken by the hacker(s). How would this threaten Microsoft, or the users of the Windows operating system? There are many possibilities that could threaten a large number of companies.

If indeed the source code for any of the operating systems created by Microsoft had been stolen, the code could then be gone through to search for vulnerabilities. This could open doors for harder to detect viruses, Trojans or any number of "malware" products. Microsoft is notoriously known for keeping it's source code a secret and only giving certain partners snip-its of their code to work with. Therefore, if a hacker was to get a copy of the operating system code and find a vulnerability in it, they could then write a virus to attack the vulnerability, which would make it very difficult for anti-virus companies to find and detect that virus footprint without help from Microsoft opening their code to anti-virus companies.

Another concern to Microsoft is the damage to their reputation. One of the largest effects from a hack such as this going public is the insecure feeling given to the consumers. Consumers may become wary upon hearing of the break-in, causing concern over the stability of Microsoft products, and therefore possibly affecting sales. Microsoft immediately went on the defensive saying the hack lasted only a couple of days versus the weeks reported, and none of their source code had been compromised. Trying to alleviate the concern in the public eye, Microsoft announced that they had been tracking the hacker the whole time documenting the events to send to the FBI.

Overall, if indeed the hacker(s) that broke into Microsoft had downloaded copies of software under development; the public should have little concern. Software development goes through many, many stages and changes. Therefore it is not very likely that the code stolen would be the same as a production release version. As for the current version of Microsoft operating systems, Microsoft heavily guards them. With the use of proprietary software control mechanisms, Microsoft logs all changes

and modifications to any production level code.

On the other hand, Microsoft may have taken a smear on its reputation, but that should dissipate relatively fast baring another incident.

How did this break-in happen?

Filtering through the rumors and half-truths about the Microsoft hack, it is a difficult task to come up with the exact events that happened which allow Microsoft to have one of its developer's networks broken into. Some of the rumors the media had picked up were: A remote user of the Microsoft network had transported the virus up to the main network from their home PC, or a disgruntle Microsoft employee let the virus loose inside the network. One report even claimed it was the Russian Mafia behind the break in.

Questions are still being asked as to how Microsoft was broken into, but one item that seems pretty clear is that it was a Trojan horse program called QAZ that opened the doors to the hacker(s). Speculation has risen as to how a company as large as Microsoft can be compromised by a virus that was detectable by most of the major anti-virus companies at the time.

An important strategy for any security professional that is in charge of a large organization is the dissemination of Anti-virus software updates. This can prove to be a difficult task when you look at a large company, possibly with remote or mobile users. This thought might add to the creditability of the remote user theory of this attack.

Once the QAZ virus landed on the Microsoft network it opened up a WinSock port to communicate back to the hacker. At this point the QAZ Trojan program emailed password information back that allowed the hacker to then infiltrate the Microsoft network. Once the hacker got access to the Microsoft network they began creating new ID's with various levels of permission. The creation of these ID's is eventually what led Microsoft to realize they were being attacked. The hacker was creating ID's that did not follow the creation standard that Microsoft uses. Following the ID creation the hacker then sent email of the information to an email address in St. Petersburg, Russia. Microsoft employees noticed the non-standard ID's but thought that they were the result of a new employee. After noticing this pattern for a couple days and seeing the permission level of the new accounts rising, this alerted Microsoft that there was a hack in progress.

During the estimated twelve-day hack that took place, the hacker(s) had availability to source code that was under development. Company officials openly admitted that the hacker(s) had gained entry, but only had access to the source code for a single product that is still in early stages of development and did not download any of it.

Overall the Microsoft hack should raise awareness for other companies. After all, if an event such as this can happen to Microsoft, a company that spends millions of dollars a year on information security, it can happen to anyone.

What is the QAZ virus?

QAZ.A is a Trojan horse program that hides itself once launched by renaming Widows Notepad to Note.exe and naming itself as Notepad.exe. Every time the application is run it uses Note.exe to hide from detection while executing its own code in the background.

QAZ is said to have originated in China and was discovered in July 2000. Soon after its discovery, most anti-virus companies had a release for it. The QAZ Trojan has aliases such as W32.HLLW.Qaz.A, Qaz.Trojan, Qaz.Worm, or Qaz.A and is rated to have a low damage impact. While at the time of the Microsoft attack the distribution of QAZ was low, but now with the publicity of the Microsoft hack, it can be assumed that this will be a virus to look for in the future. Following the announcement of the QAZ attack on Microsoft, a UK based company with the domain QAZ.com (no relation to the virus) experienced unusually high hits to their homepage, is this coincidence?

QAZ also modifies a system registry key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\startIE = XXXX\Notepad.exe qaz.hsq.
This key ensures that the Trojan is run every time Windows starts up. Once the QAZ virus infects a computer it opens a WinSock port (7579) and listens for instructions from the client portion of QAZ, which gives a user remote control of the infected system. QAZ does not have the ability to spread itself autonomously and must be spread by user interaction such as posting it to a newsgroup or email. Once the QAZ Trojan infects a system it can spread through shared folders within a LAN. QAZ looks for shared folders that contain Notepad.exe, and does not require that the folder be a mapped drive on the machine it has infected. Once it infects another machine the QAZ Trojan emails the IP address of the newly infected machine to the hacker or remote controller of the virus.

What can we learn form this attack?

A key point that may have stalled Microsoft's break-in at the very beginning, would have been for them to keep their anti-virus software up to date. As well as to make sure that all of their remote users have updated anti-virus software on the machine they access the corporate network from. Virus software, though good to have will do little if it is allowed to become out of date allowing the newer virus's in.

It should be very apparent to any company that a secure, and well-maintained security architecture should be a part of their infrastructure. Keeping an eye on event logs, monitoring break-ins or major system file changes are just a few things that can help keep a network safe.

Even with the best of security systems that are watched and maintained, break-ins such as what has happened to Microsoft can still happen. A plan should be developed, so that when a break-in does occur, the right steps can be followed to minimize any loss.

Along with all of the protection methods and security devices, a good user awareness campaign may help reduce risk. Keeping the user base aware of new

vulnerabilities, virus's or social engineering attacks is always a good idea.

Reference

"Hackers attack Microsoft network." 27 Oct 2000. URL: http://www.cnn.com/2000/WORLD/europe/10/27/usa.microsoft/ (30 Oct. 2000).

"Microsoft: Whodunnit? The Professional Hacker or Unwitting Employee." 28 Oct. 2000. URL: http://www.antionline.com/2000/10/28/eng-guardian_international_011320_98_7418046034873.htm (30 Oct. 2000).

"Microsoft's Fragile Defense Chills the Corporate World." 29 Oct 2000. URL: http://www.antionline.com/2000/10/28/eng-financialtimes_news_140555_140_840918119065.htm (30 Oct. 2000).

"New account of Microsoft attack." 29 Oct. 2000. URL: http://www.msnbc.com/news/482011.asp (13 Nov. 2000).

Bridis, Ted., Buckman Rebecca., Fields Gary. "Microsoft says it quickly detected, monitored hacker." 30 Oct 2000. URL: http://www.msnbc.com/news/482865.asp?cp1=1 (30 Oct. 2000).

Bryar, Jack. "Time for Microsoft to fix its security problems." 30 Oct. 2000. URL: http://www.newsforge.com/article.pl?sid=00/10/29/152208 (13 Nov. 2000).

Craig, Andrew., Lynch Ian. "Hackers saw Microsoft source code." 30 Oct. 2000. URL: http://www.vnunet.com/News/1113113 (13 Nov. 2000).

Johnson, Gene. "Microsoft Says It Knew of Hackers." 30 Oct. 2000. URL: http://dailynews.yahoo.com/h/ap/20001030/tc/microsoft_hackers_20.html (13 Nov. 2000).

Konrad, Rachel. "Hack attacks a global concern." 29 Oct. 2000. URL: http://news.cnet.com/news/0-1003-200-3314544.html?tag=st.ne.ron.lthd.ni (30 Oct. 2000).

Lai, Eric. "Microsoft Hack Shows Companies Are Vulnerable." 29 Oct. 2000. URL: http://dailynes.yahoo.com/htx/nm/20001029/tc/microsoft_hackers_dc_12.html (30 Oct. 2000).

Lemos, Robert. "MS intruder may elude authorities." 27 Oct. 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2646331,00.html (13 Nov. 2000).

Lettice, John. "Redmond strives to cram Great MS Hack back in box." 29 Oct. 2000.

URL: http://www.theregister.co.uk/content/1/14306.html (30 Oct. 2000).

Loveland, Betty. "Troj.Qaz.A" URL: http://securityportal.com/research/virus/profiles/trojqaza.html (13 Nov. 2000).

Martinez, Michael J. "How Microsoft Spotted Hackers." 30 Oct. 2000. URL: http://dailynews.yahoo.com/h/ap/20001030/tc/microsoft_hackers_22.html (13 Nov. 2000).

McCue, Andy. "Users consider Microsoft hack implications." 2 Nov. 2000. URL: http://www.vnunet.com/Analysis/1113409 (13 Nov. 2000).

Ryder, Josh. "Microsoft Gets Hacked – What Can We Learn?" 30 Oct. 2000. URL: http://securityportal.com/articles/mshacked20001029.printfriendly.html (13 Nov. 2000).

Ticehurst, Jo. "Microsoft hack boosts Trojan soundalike site." 31 Oct. 2000. URL: http://www.vnunet.com/News/1113253 (13 Nov. 2000).

Yu, Roger. "Expert Answers Questions about Microsoft Hack." 30 Oct. 2000. URL: http://www.antionline.com/2000/10/30/krbn/0000-0158-SE-MICROSOFT.html (30 Oct. 2000).