SANS Institute

On October 23, 2008, Microsoft published the following critical security bulletin: MS08-067, Vulnerability in Server Service Could Allow Remote Code Execution (958644). Microsoft explained that the vulnerability in the server service could allow remote code execution if an affected system received a specially crafted remote procedure call (RPC) request. This could allow an attacker to exploit this vulnerability without authentication to run arbitrary code on Windows 2000 Service Pack (SP) 4, Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, Vista Gold SP1, Windows Server 2008 and Windows 7 systems. Additionally, Microsoft warned that this vulnerability could be used in the crafting of a wormable exploit. The Common Vulnerabilities and Exposures (CVE) site references this vulnerability as CVE-2008-4250. The Common Vulnerability Scoring System (CVSS), which provides an open framework for communicating the characteristics and impacts of Information Technology (IT) vulnerabilities, rated this vulnerability with a 10.0, which is their most severe rating and indicates a vulnerability with high impact and high exploitability.

This wormable exploit did come into being and is known today as the **Conficker worm**. It has also been referred to as the **Conficker virus, Downadup and Kido**. Conficker became one of the fastest and largest worm infections since the Sasser infection of 2004. It has been extremely difficult to contain and control due to its use of many different advanced malware techniques. Conficker's logic includes mechanisms to generate lists of new domain names on a daily basis to seek out Internet rendezvous points that the authors use for updates and for command and control of the machines infected. Conficker also uses binary validation techniques to ensure that updates are signed by its authors. The use of binary encryption, digital signatures and advanced hash algorithms for its updates prevents the hijacking of infected clients. At its core, Conficker's main purpose is to provide its' authors with a secure binary update service that allows them instant control of the millions of infected PCs worldwide (Porras, Saidi and Yegneswaran, April 2009). It is very adept at hiding its tracks and preventing its removal from host machines by its use of code obfuscation. So far, Conficker infected machines have not been used for any nefarious purposes, but the viability of a botnet of thousands, perhaps millions of computers available for use by criminal's remains a possibility. Conficker's main impact at this time is its ability to terminate, disable, reconfigure or blackhole native operating system and third-party security services (Porras, Saidi and Yegneswaran, April 2009). Conficker disables Windows systems security services as well as third-party firewalls and anti-virus products, leaving systems in a vulnerable state which can lead to more infection and infiltration. Furthermore, Conficker blocks access to security related sites such as Symantec or McAfee, thus preventing users from downloading tools to remove the infection.

Background Information

A Remote Procedure Call (RPC) is a protocol that a program can use to request a service from a program located on another computer on a network. RPC helps with interoperability because the program using RPC does not have to understand the network protocols that are supporting communication. In RPC, the requesting program is the client and the service-providing program is the server.

The Windows Server service is used to provide RPC support, file and print support and named pipe sharing over a network. The server service allows for the sharing of your local resources so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer which is used for RPC (MS08-067 Security Bulletin). This service is used by all versions of Windows, therefore making every Windows user vulnerable unless patched.

Attack Vectors

The main attack vector used by Conficker and its multiple variants is the Windows Server Service vulnerability (MS08-067) which allows attackers to execute arbitrary code via a crafted RPC request that triggers a buffer overflow during canonicalization (conversion to standard format). The B variant introduced additional attack vectors of NetBIOS Share propagation and USB propagation of the worm.

Once the specially crafted packet is sent to port 139 or port 445 on a Windows file/printer sharing session, the exploit occurs. Receipt of this package will trigger a call to the RPC application programming interface (API) NetPathCompare ( ) and NetPathCanonicalize () functions. Additionally:

> "The exploit is triggered when giving a specific path to canonicalize such as "\c\ .. \..\AAAAAAAAAAAAAAAAAAAAAAAAAAAA" to the NetPathCanonicalize( ) function, which uses *_tcscpy_s* macro, which in turns calls the wcscpy_s function. This function is used to copy a wide-character string from a location in memory to another. The buffer overflow is provoked by a miscalculation in the parameters given to the *_tcscpy_s* macro by the *NetPathCanonicalize* ( ) function.
>
> The *_tcspy_s* function is called like this by the *NetPathCanonicalize*
>
> *NetPathCanonicalize* contains a complex loop to check the path for dots, dot-dots, slashes while making a lot of pointer calculations. Once the loop is passed over a couple of time, the *previousLastSlash* parameter gets an illegal value."(Racicot)

Conficker's Payload:

Once the worm is installed on a system, the following occurs:

> "Conficker will copy itself with a random name into the system directory *%systemroot%\system32* and register itself as a service. It will, of course, also add itself into the registry with the following key:
>
> - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<name>.dll ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
> - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netsvcs\Parameters\"ServiceDll" = "<name>.dll"
>
> It will then use these sites to get the newly infected machine's IP address:
>
> - http://www.getmyip.org
> - http://getmyip.co.uk
> - http://checkip.dyndns.org

> With the IP address, Downadup/Conficker can download a small HTTP server ("*http://trafficconverter.biz/4vir/antispyware/loadadv.exe*") and open a HTTP server on the current machine with the following address:
>
> - *http://[EXTERNAL IP ADDRESS OF INFECTED MACHINE] :[RANDOM PORT]*
>
> Once the HTTP server is set up, it will scan for other vulnerable machines and when a target is found, the infected machine URL will be sent to the target as the payload. The remote computer will then download the worm from the URL given and then start to infect other machines as well. Therefore, there is no centralized point of download. Upon successful infection, it will also patch the hole to prevent other worms to infect the machine" (Racicot).

Conficker will then generate a list of 250 domain names (rendezvous points) using a randomizing function that it seeds with the current UTC system date. All Conficker infected clients will attempt to contact the same set of domains for updates. This same list of domain names is generated every 3 hours. This update probing is done on a daily basis and provides Conficker's authors with an effective updating mechanism that is highly mobile as its location is recomputed each day by all infected clients.

It should also be noted that Conficker's authors have also taken measures to ensure that no other malware authors can hijack their client base. Conficker has incorporated binary validation mechanisms to ensure that updates provided to infected clients have been digitally signed by the authors themselves and the clients will not accept non-signed updates.

Signs and Symptoms of Infection

Conficker and all of its variants perform the following to an infected system:

- Modification of system settings
- Disabling of TCP/IP Tuning
- Termination\disablement of the following Windows services:
  - Windows Security Service
  - Windows Auto Update, Background Intelligent Transfer Service (BITS)
  - Windows Defender
  - Windows Error Reporting Service
- Termination\disablement of third-party security services/software that deal with system security (anti-virus, firewalls, etc)
- Resetting system restore points
- Deleting backup files
- Checking for internet connectivity and downloading arbitrary files
- Users will not be able to browse certain security-related Web sites with URLs containing specific key words and phrases.
- Increase in traffic on port 445
- Access to administrator shared files is denied
- Sluggish response due to increase in network traffic

Conficker Removal

There are several conficker removal tools available for download. Most Anti-Virus vendors have developed removal tools and/or provided instructions for removing conficker and links to some of these are listed below:

- Symantec
- SOPHOS
- McAfee
- Microsoft's Malicious Software Removal Tool
- Microsoft also has put together a manual procedure for removing the conficker worm

Conficker Prevention

The Conficker worm serves as a great reminder to everyone to continually and consistently practice Defense-In-Depth and provide multiple layers of defense to protect consumer and business systems. The spread of the Conficker worm is a sign that all PC users are stubborn and continue to avoid keeping their Windows installations up to date with the latest security patches. The infection has spread to computers all over the world and includes home, business and government users. Methods of preventing this and other types of infections include the following:

- Keep security patches up to date. This includes not only patches for the operating system, but for all applications and plug-ins as well. Remember, Downadup/Conficker spread so widely because so many computers simply did not have a simple security patch, released months before the infections ever started, applied. (Weafer).
- Use a robust security software suite that has multiple layers of protection. Furthermore, make sure your security software is always on and up to date. Even patched systems are continuing to become infected with the .A and .B variants. In many instances, this is occurring because the worm is being passed on via infected removable media, such as USB thumb drives, that are essentially acting as host carriers. In nearly all cases, up-to-date security software will detect the threat before it has the chance to jump from the removable device to the computer (Weafer).
- Enable a firewall (Windows or Third-Party) on your computer and follow industry best practices on what should and should not be allowed through the firewall
- Limit user privileges on the computer. Provide access only to those who need it.(Need to Know)
- Use caution when opening attachments and accepting file transfers.
- Use caution when clicking on links to Web pages.
- Avoid downloading pirated software.
- Protect yourself against social engineering attacks.
- Use strong passwords.

Conficker and April Fool's Day - 2009

Researchers at Computer Associates discovered pieces of the computer code for Conficker that tells the worm to activate itself on April 1, 2009 (Sutter). There were a multitude of articles posted on the internet that Conficker

was going to deliver its payload on April 1, 2009, April Fools Day. See Appendix A for links to several of those articles as well as links to articles discussing the aftermath of the forecast.

April Fools Day 2009 came and went with no major or ill effects due to Conficker. Please take note of the publicity that conficker generated with CNN and the New York Times covering the story. However, it must be noted that the threat of so many compromised machines still exists.

An update posted on April 1, 2010 on Symantec's web site states the following on the status of conficker infections:

- Approximately 6.5 million systems are still infected with either the .A or .B variants.
- The .C variant, which used a peer-to-peer method of propagating, has been slowly dying out over the past year. From a high of nearly 1.5 million infections in April of 2009, the infection rate has steadily decreased to between 210,000 to 220,000 infections. This indicates some computer users are fixing the issue and getting rid of the infection.
- Symantec also observed another variant, .E, released on April 8, 2009, but this variant deleted itself from infected systems on or after May 3, 2009.
- Thus far, the machines still infected with Downadup /Conficker have not been utilized for any significant criminal activity, but with an army of nearly 6.5 million computers strong, the threat remains a viable one. (Weafer)

Conficker Variants

Since its arrival, there have been several variants of the Conficker worm. Conficker.A was the first version of the worm and then Conficker.B, Conficker.C, Conficker.D and Conficker.E have followed. They can all be referred to as the Conficker family of malware. These variants have improved upon Conficker's code and have been released in response to attempts to stop or remove Conficker's infestation. Conficker.A relied upon the Windows Server Service (MS08-067) vulnerability for its propagation while Conficker.B implemented two additional strategies to embed itself into hosts, these being NetBIOS Share propagation and USB propagation. (Porras , Saidi and Yegneswaran , February 2009). Conficker.C increased the number randomly generated domain names to 50,000+ candidates daily, which represents a direct retaliation at the security community's efforts to block all of the domain registrations associated with the A and B variants. Conficker.C also developed a peer-to-peer (P2P) coordination channel for its updates. Conficker.D changed the domain-name generation algorithms and now generates a larger pool of domain names. It should also be noted that Conficker.D does not spread by attacking new systems and just updates existing Conficker.C infected machines. Conficker.E performs another update to the Conficker.C code base. See Appendix B, which contains a listing of links to Microsoft's Security Portal Threat Encyclopedia, for a full discussion of the variants of Conficker.

Ending Thoughts:

Conficker arrived with a bang, spreading fast and furious throughout the internet. Much has been written and speculated on the true purpose behind conficker. Warnings have come and gone with little effect. However, Conficker is still out there. Even though there are several removal tools for conficker and a patch from Microsoft

is available for this vulnerability, the question remains, "Are we Safe?" Sadly, the only answer that can be given at this time is probably not.

It may not be the biggest known botnet --for example, the Mariposa botnet reportedly infected more than 11 million computers during its lifetime--but it's also nothing to sneeze at. As another point of reference, the well-known Rustock botnet , which sends out 32.8 percent of all spam, is estimated to sit on somewhere between 1.6 and 2.4 million machines. So remember, these 6.5 million computers infected with Downadup/Conficker are still much like a loaded gun, waiting to be fired (Weafer).

The information security community and law enforcement continues to monitor Conficker's activity. A Conficker Working Group has been formed (http://www.confickerworkinggroup.org) and is ready to sound the alarm should the worm be utilized for criminal activity. Users following the removal and prevention practices listed above will go a long way in preventing further infections, but the reality is that until the current infections are completely eradicated, Conficker must still be considered a threat.

The most frightening aspect of Conficker is its clear potential to do harm. At best, Conficker could be used for Internet fraud and theft. At worst, Conficker could be used as an offensive weapon for a coordinated information warfare attack that could disrupt the Internet itself.

Also, the authors of Conficker must be noted for their skill sets in developing this worm. The authors have demonstrated very advanced programming skills that include the use of advanced Cryptographic skills, code obfuscation, and an in-depth knowledge of Windows internals and other third-party security products. They were among the first to introduce the Internet rendezvous point scheme for updates, and have now integrated a peer-to-peer protocol that does not require an embedded peer list. They have continually updated their code with new variants and have adapted Conficker to address the latest attempts of the security community to thwart this worm. They have infiltrated systems around the world and one can only wonder what they will do next.

Appendix A: April Fool's Day 2009 Conficker Articles

- No joke in April Fool's Day computer worm, March 24, 2009 by John D Sutter
- The Conficker Worm: April Fool's Joke or Unthinkable Disaster? March 19, 2009 By John Markoff
- Conficker.C primed for April Fool's activation, March 16, 2009 by Joel Hruska
- Countdown to Conficker's April Fools Day Climax, March 25, 2009 by *Byron Acohido*
- April Fools Fizzled, But Threat Remains April 3, 2009 by Brian Krebs
- April Fools' Day Update Begins With A Yawn, March 31, 2009 by Thomas Claburn
- Conficker worm plays no tricks on April Fools' Day (AFP), March 31, 2009

Appendix B: Microsoft's Security Portal Threat Encyclopedia Conficker Links

- Conficker A: Reported to Microsoft on November 21, 2008
- Conficker B: Reported to Microsoft on December 29, 2008
- Conficker C: Reported to Microsoft on February 20, 2009
- Conficker D: Reported to Microsoft on March 4, 2009
- Conficker E: Reported to Microsoft on April 8, 2009

References

Fitzgibbon, Niall and Wood, Mike. "Conficker.C A Technical Analysis." Sophos. April 1, 2009. Web. September 22, 2010.

"Microsoft Security Bulletin MS08-067 - Critical - Vulnerability in Server Service Could Allow Remote Code Execution (958644)." Microsoft. October 23, 2008. Web. September 20, 2010.

Porras, Phillip, Saidi, Hassan, and Yegneswaran, Vinod . "Addendum: Conficker C Analysis." SRI. April 4 2009. Web. September 28, 2010.

Porras, Phillip, Saidi, Hassan, and Yegneswaran, Vinod. "An Analysis of Conficker's Logic and Rendezvous Points." SRI. February 4, 2009. Web. September 28, 2010.

Racicot, Jonathan. "New Kid on the Block: Downadup ."Cyberwarfaremag. December 2, 2008. Web, September 22, 2010.

Sutter, John D. "No joke in April Fool's Day computer worm." CNN. March 24, 2009. Web. September 20, 2010.

Weafer, Vincent. "Downadup /Conficker and April Fool's Day: One Year Later." Symantec. March 29, 2010. Web. September 23, 2010.
