

Conficker De-mystified

By Dave Hartley, security consultant at Activity

The worm that has become commonly known as Conficker has received a great deal of recent press attention with warnings of impending doom and destruction of IT systems. It is firstly important to note that this worm also has a number of aliases including Downadup and Kido. Conficker exploits a publicly known vulnerability on Windows systems (CVE-2008-4250). A patch to fix the vulnerability has been available from Microsoft since October 23rd 2008 (MS08-067).

The “Server” service in an un-patched Microsoft Windows system allows an attacker to execute arbitrary code via a crafted RPC (Remote Procedure Call) request. The Server service allows the sharing of your local resources (such as disks and printers) so that other users on the network can access them. It also allows “named pipe” communication between applications running on other computers.

Windows PCs that were configured to automatically receive and install security updates would not have been vulnerable to this exploit as they would have been patched before the Worm appeared and therefore could not have been infected. However many organisations do not configure their corporate systems to automatically update and patch themselves, they choose instead only to apply patches after they have tested them, a process that can take several weeks leaving systems open to infection until the patches are applied.

The Conficker worm began life simply exploiting the Microsoft vulnerability, but was quickly adapted to use multiple infection vectors to propagate including using brute-force, password-guessing techniques against interconnected systems in order to compromise user accounts with weak authentication credentials. The worm also now infiltrates and spreads by infecting removable media devices, such as USB keys in the hope that it will be automatically executed when inserted into another system.

At its core, the main purpose of Conficker is to install a secure updatable backdoor Trojan service that provides its authors with complete control over millions of systems. Conficker has the potential to be used as a sustained and profitable platform for Internet fraud or

theft and for launching powerful offensive and concerted cyber attacks; however the true intent of the malware author(s) is unknown and we can only speculate with regards to its true purpose.

Conficker incorporates a variety of strategies to secure and defend its installation on compromised systems. To do this, it employs several measures to mask its presence, as well as implementing features that kill or disable security products that would otherwise detect its presence or remove it. The worm attempts to obfuscate its presence on the system in order to avoid easy diagnosis and removal and opens secure communication and control channels with which it can periodically update itself and communicate with other infected hosts.

Upon execution, the worm creates copies of itself in a number of locations on the target machines file system and randomly renames itself. It then deletes all system restore points prior to its infection to thwart systems being rolled back to a known uninfected state and sets NT File System (NTFS) permissions on its installation files revoking write and delete privileges. It then disables critical host security services, such as Windows defender, as well as services that deliver security patches and software updates, such as the Microsoft Update services and anti-malware software to prevent the system from being secured. It also hooks several system Application Programming Interfaces (API's) in order to block access to security- related domains, such as web sites that contain information about how to prevent or clean an infected system.

The worm proceeds to patch the MS08-067 vulnerability in order to prevent any one else from using the same exploit vector to gain control of the system, however the malware actually implements a backdoor so that the author(s) can still gain access. Conficker then continuously monitors the system looking for processes that are executing as part of a security product, security patch or removal tool and then terminates them.

Once it has control over the target system, the worm then proceeds to contact various domains, websites and hosts to query the current time and download and execute additional code. This communication is facilitated over the HTTP and P2P protocols; the worm is also capable of disabling Windows firewall rules in order to allow these network communications.

The author(s) have demonstrated that they possess advanced programming skills, a deep understanding of cryptography, sophisticated obfuscation skills and an in-depth knowledge of Windows internals and security products. They have continually revised their code, creating new variants adapting to the latest attempts by security vendors and industry experts to thwart their activities. Microsoft is currently offering \$250,000 as a reward for information leading to the arrest and conviction of the Conficker Worm author(s).

Scanning Tools

A tool is readily available from the HoneyNet Project (<http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker>) that can be used to scan machines to see if they are infected. Tenable (Nessus), Foundstone and Qualys are all releasing similar tools or updates to their vulnerability scanners that can also detect infected machines, in addition the nmap (www.nmap.org) scanner is a free scanning tool that can also be used to detect infected machines.

Removal Tools

If you believe that you have an infected system you can clean it by using one of the many removal tools. F-Secure have made available a free tool named "F-Secure Easy Clean" (<http://download.f-secure.com/estore/fseasyclean.exe>), Symantec have also made available a tool to help you clean an infected system, the "W32.Downadup Removal Tool" (http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/FixDwndp.exe) or you could also use the Microsoft Windows Malicious Software Removal Tool (<http://www.microsoft.com/downloads/details.aspx?FamilyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>). In addition Microsoft has also made available some good advice and supporting tools to help protect your network from viruses and malicious software (<http://www.microsoft.com/windowsxp/using/networking/security/protect.mspx>). Once your system is clean, ensure that you fully patch and update the system.

Mitigating Malware Infections

The Windows operating system has historically been attacked for being one of the most insecure and complicated systems to harden. Microsoft has invested a considerable amount of time and effort in improving this situation and has made measurable progress towards producing a secure "by default" operating system. They have also gone a long way to helping system administrators build and deploy systems that are secure and

resilient to attack. Systems administrators need only to effectively utilise the tools made available to them by Microsoft when building, deploying and maintaining Windows systems to ensure that they are not vulnerable to this type of compromise.

There are also a number of other publically available techniques, tools, resources and security best practices and principles at a system administrators disposal that can aid in preventing the compromise of the OS and in the event of a compromise, help mitigate the level of access that can be leveraged by an attacker or piece of malware. In addition to Microsoft, the National Security Agency (NSA) and National Institute of Standards and Technology (NIST) all make numerous guides available.

Patch Management

A formal security patch management process should be implemented and enforced to ensure that all identified software updates are in place, thereby eliminating vulnerabilities from the environment and mitigating the risk of compromise. As a proactive initiative, security patch management is the primary line of defence for protecting a corporate computing infrastructure. Develop internal processes for the continued management of the system; ensuring that critical patches are applied to a system no more than 4 weeks after issue from the vendor. It is important to realise that third party non-Microsoft applications may also require updating periodically and that the vendors may have their own method of making security patches available that will not be part of the Microsoft update services. Any formal patch management process should also incorporate the management of non-Microsoft software.

Historically some security and system updates made available by Microsoft have caused operational issues with some systems due to various environmental conditions and conflicts with installed software. This situation does not occur as frequently as it once did. If this is a concern within your environment configure systems to download all available security patches as soon as they are available and have them manually installed by qualified systems administrators. Subscribe to Microsoft Technical Security Notifications and monitor security news and vulnerability sites such as Bugtraq and Security Focus to ensure that any vulnerabilities with either the configuration of systems or installed software can be identified and appropriate mitigation planned at the earliest opportunity.

If an attacker or piece of malware has failed to exploit a vulnerable application or service, they will move on to trying to guess, steal or brute force the credentials for exposed

services that require authentication, such as SMB. A secure network environment requires all users to use strong passwords that are not easy to guess.

Most malware needs to exploit a resident vulnerability in order to gain a foothold on a machine, but as can be seen by the advanced methods utilised by the Conficker worm, once a piece of malware infects a host a number of propagation methods can be used.

The Conficker worm attempts to communicate with target systems on their listening SMB/NetBIOS ports (139 and 445) in order to exploit the Server service (via RPC) and to perform brute force attacks against the host. These ports are most often blocked at the gateway by a traffic-filtering device such as a Firewall. System administrators believing that the Firewall will protect their networks, defer the installation of the patches. Infection can then occur when a remote worker with an un-patched machine is infected at another location and introduces the infection into an otherwise infection free network.

To counter this threat, organisations should be able to quarantine systems that attempt to connect to the infrastructure restricting their access to resources and communications with other systems. The machines can then be benchmarked against a corporate security policy ensuring that they are clean and free from infection and that they are running the latest versions of resident software and have had all of the available security updates and patches applied. Once the machine conforms to the required security baseline it can be allowed to connect to the corporate infrastructure.

It is also feasible for infections to occur via a drive-by-attack, this would require a user visiting a web site that contained malicious client side script, which exploited an un-patched vulnerability in the web browser or browser extension. This infected host could then be used to infect internal systems and propagate the malware. To help counter this threat a web proxy content filtering technology can be used.

A content filtering web proxy server provides administrative control over web content. Such products can be used to implement content and URL filtering, known malicious code filtering, and Java-based code behaviour analysis.

There are many vendors and security software appliances that can assist with creating quarantine networks and detecting rogue devices on your networks, however it is also possible to leverage existing routing technologies such as VLAN's, built in management

tools from certain Wireless Access Point vendors, as well as built in operating system and domain management tools to achieve similar goals. In addition many remote access solutions implement features that can benchmark and quarantine systems if they don't conform to security policies.

Getting help

Consider engaging with a professional and reputable security services provider who can help you leverage existing technologies and system configurations to enhance the computing infrastructure. Such organisations can help you save cost by ensuring that you use all of the tools available to you to mitigate your risks before looking at additional technology which may just implement methods of locking down systems and networks in a way that was already available within your existing resources.

If you have deployed complementary security technologies within your Enterprise consider contracting a professional security consultancy that is independent of the product vendor to assess your chosen security solution to ensure that it is effective.