The Conflicker Worm and Variants

An Overview of Tactics, Logical and Psychological Impacts, and Recommendations

Kenneth Foster
Kaplan University
December 26, 2010

The Conflicker worm and its variants fueled a flurry of media coverage, primarily due to its prolific infection rates and eradication difficulties (McMillan, 2009). This classification of worm was exceptionally good at disabling the traditional defenses and system mechanisms many had depended upon to protect their systems. Further raising anxiety was the worms' ability to leverage the wide-spread use of removable media and its exploitable Autorun feature to propagate its code to new systems. This worms' impact was significant in corporate America, but as we will learn, the impact was lessoned within the Department of Defense due to proper security practices in place long before the worms' release (JTF-GNO, 2006).

Conflicker and its many variants are unusually nasty as far as worms go because of its' through alterations to the system in an attempt to prevent removal (Microsoft Inc. (a), nd). This polymorphic worm disables the Windows Automatic Update; Security Center; Windows Defender; and Firewall Services in addition to preventing the error reporting utilities from functioning. Next it alters the DNS subsystems to block access to security related domains where detection signatures and removal tools may be located (F-Secure Corp, nd). The worm establishes an http server on a random high port which it uses to send specifically crafted packets to other hosts on the network in an attempt to get them to download malware disguised as image files. It also deletes user created restore points in an attempt to prevent rollback to pre-inflection registry settings (Microsoft Inc. (a), nd). This combination of alterations provided the worm an effective environment to remain undetected, while significantly inhibiting its mitigation.

There are three primary methods of propagation used by the worm (Microsoft Inc. (a), nd). The methods include file sharing services; exploitation of the Windows Server Service (svchost.exe); and exploitation of the Windows Autorun service (F-Secure Corp, nd). In regards to file sharing services, it alters the TCP/IP parameters to allow for a faster propagation by

modifying the number of half-open connections. Next it enumerates the network for any systems with open file shares or shares it can logon to using a pre-defined set of common passwords embedded within its code (F-Secure Corp, nd). Once a remote share is found, it copies itself to the administrative share (ADMIN$) of the system and creates a daily scheduled task to execute the infected dll on the remote system. The worm also attaches itself to various services, intercepting calls and inhibiting any mitigation actions (Porras, Saidi, & Yegneswaran, 2009). The worm infects removable media by depositing a copy of the infected dll in a recycle bin on the media and then adding or altering the autorun.inf file contained on the media. This alteration addends a call to the infected dll, thus infecting any subsequent machines which use the media. Additionally, the worm joins a botnet consisting of randomly auto-generated domains and awaits commands for information exploitation such as password and account data exfiltration as well as commands to download additional malware (Westervelt, 2009).

In a traditional network, Conflicker would impact several notable areas. Indicators to monitor for impacts would include account lockout policy modifications; domain controller response degradation; network traffic congestion; TCP Port 445 scanning; and abnormal DNS look-up volumes (Porras, Saidi, & Yegneswaran, 2009). Conflicker had a minimal operational impact on my organization for several reasons, requiring an overview of how these measures inhibited Conflicker. All users on the network are provisioned using the Principal of Least Privilege; separating account identities for standard users, requiring privileged users to perform specifically intended escalation actions only as needed (Stewart, Tittel, & Chapple, 2008 p. 500). This prevents the worm from altering the registry of a target machine as well as any damage the worm could cause to the on board anti-malware software because standard user permissions prevent these alterations. Each system runs Host-based Intrusion Prevention software, which

was tuned to detect the attempts of Conflicker (Stewart, Tittel, & Chapple, 2008 p. 50). Any actions such as dll alterations or http service start-up actions would be detected and immediately terminated and logged to the reporting console. The eradication of user passwords in favor of smartcards mitigates the password guessing techniques of the worm, inhibiting prorogation of file shares (Irwin, 2003). To prevent the likelihood of future infection, we did eliminate the use of Flash drives by inhibiting the USB store drivers' ability to mount all USB media devices (Svan & Allen, 2008). This earlier ban directly impacted the Autorun prorogation mechanism exploitation from external untrusted media.

Conflicker leverages several vulnerabilities in the windows operating system. The first step is always to patch; in this case using MS08-067 (Microsoft Inc. (b), 2008). Next is the requirement to determine if you have any infected systems. Since Conflicker inhibits the detection of the worm on the infected system, there is a low-tech solution. The Conflicker working group has created a simple html page that displays the logos of known DNS blocked sites. Because this page is not on the DNS blocked list, the chart provides you a method to determine if a suspect system is impacted (Conflicker Working Group, 2010). Another mechanism we use is a specially developed and maintained DoD assessment tool called Qtip; designed to scan and hash files on a remote system for signs of malware to include Conflicker (JTF-GNO, 2006). The use of a network Intrusion Prevention System will detect the traffic being sent to/from an inflected host; aiding in the detection. If we do find an infected system, our policy requires us to disconnect the host and report our findings to the organizational Regional Computer Emergency Response Team (R-CERT). Depending on the instructions from the R-CERT, further follow on actions such as whole disk forensic imaging or a complete wipe will be accomplished. Our standard corporate policy in regards to infected / exploited systems is

to back-up the user data to another off-line source and reimage the system. Prior to moving the data back to the system, it must be scanned for infection. If the files are inflected, those are deleted and a rescan occurs until the backed up files scan clean. If the files cannot be successfully removed or the back-up will not scan clean, the user loses their information. This prevents continual reinfection from a payload source from the prior machine.

Conflicker represented a new chapter in anti-malware defense. The rapid spread and late detection of the infections allowed for wide spread propagation rates. The commonality of Flash drives and other USB mass storage devices in daily users' lives were contributing factors in the worms' diversity of host infections. Once infected, the leveraging of a wide-spread and changing botnet command and control networks provided code updates and other malware that could be used for information exfiltration and identity theft operations. The DoD's prior best practices of Principal of Least Privilege, integration of Host-based Intrusion Prevention, and an early ban on Flash drive media were effective in preventing wide-spread infections within the network. These practices, while effective in this situation highlight their overall usefulness in preventing the wide spread of other future malware attacks.

References

Conflicker Working Group. (2010, September). *Conficker Eye Chart*. Retrieved December 26, 2010, from http://www.confickerworkinggroup.org: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

F-Secure Corp. (nd). *Worm:W32/Downadup.AL*. Retrieved December 26, 2010, from F-secure.com: http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml

Irwin, S. T. (2003, June). *Identity Protection and Smart Card Adoption in America*. Retrieved December 26, 2010, from SANS Reading Room: http://www.sans.org/reading_room/whitepapers/authentication/identity-protection-smart-card-adoption-america_1122

JTF-GNO. (2006). *ALARACT 223/2006*. Retrieved December 26, 2010, from EPIC Policy Search Tool: http://exprdev1.dca.expr.net/obfweb/search/Detail.aspx?objectid=28600

McMillan, R. (2009, April 24). *Conficker Hype a 'Problem,' Says FBI Cyber-Chief*. Retrieved December 26PC World Business Center, 2010, from http://www.pcworld.com/businesscenter/article/163783/conficker_hype_a_problem_says_fbi_cyberchief.html

Microsoft Inc. (a). (nd). *Protect yourself from Conficker*. Retrieved December 26, 2010, from Microsoft Security: http://www.microsoft.com/security/worms/conficker.aspx

Microsoft Inc. (b). (2008, October 23). *Microsoft Security Bulletin MS08-067 – Critical*. Retrieved December 26, 2010, from Technet.Microsoft.com: http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Porras, P., Saidi, H., & Yegneswaran, V. (2009, April 4). *Conflicker C Analysis*. Retrieved December 26, 2010, from SRI International: http://mtc.sri.com/Conficker/addendumC/

Stewart, J. M., Tittel, E., & Chapple, M. (2008). *CISSP Study Guide* (4th ed.). Indianapolis, IN: Wiley Publishing Inc.

Svan, J. H., & Allen, D. (2008, November 21). *DOD bans the use of removable, flash-type drives on all government computers*. Retrieved December 21, 2010, from Start and Stripes: http://www.stripes.com/news/dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514

Westervelt, R. (2009, February 26). *Conficker botnet ready to be split, sold*. Retrieved December 26, 2010, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1349282,00.html