Security Spotlight
March 8, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

DOWNAD/CONFICKER: THE CASE OF THE "MISSING" MALWARE

The last quarter of 2008 remains a memorable period in the history of cybersecurity with the proliferation of WORM_DOWNAD.A and WORM_DOWNAD.AD in the wild, consequently infecting hundreds of thousands of users' systems in mere seconds and millions in just four months.

When a Hot Case Turns Cold

The inception of the DOWNAD/Conficker worm family brought forth a new level of sophistication never seen before in the threat landscape.

The inception of the DOWNAD/Conficker worm family brought forth a new level of sophistication never seen before in the threat landscape. From something as common as exploiting a vulnerability to actually utilizing worm variants to create a botnet that could dish out more and more complicated attacks, DOWNAD/Conficker proved that its methods were more than just effective, they were highly successful.

WORM_DOWNAD.KK and WORM_DOWNAD.E, two more popular variants, in fact, followed WORM_DOWNAD.A and WORM_DOWNAD.AD's footsteps in the first two quarters of 2009. The former was a notable iteration of the .A and .AD variants, as it exploited the same Windows vulnerability to spread across networks, albeit with features that addressed its predecessors' weaknesses. Users whose systems were affected by WORM_DOWNAD.KK were not even aware that their systems have already been infected. If they were, removal and cleanup still proved difficult.

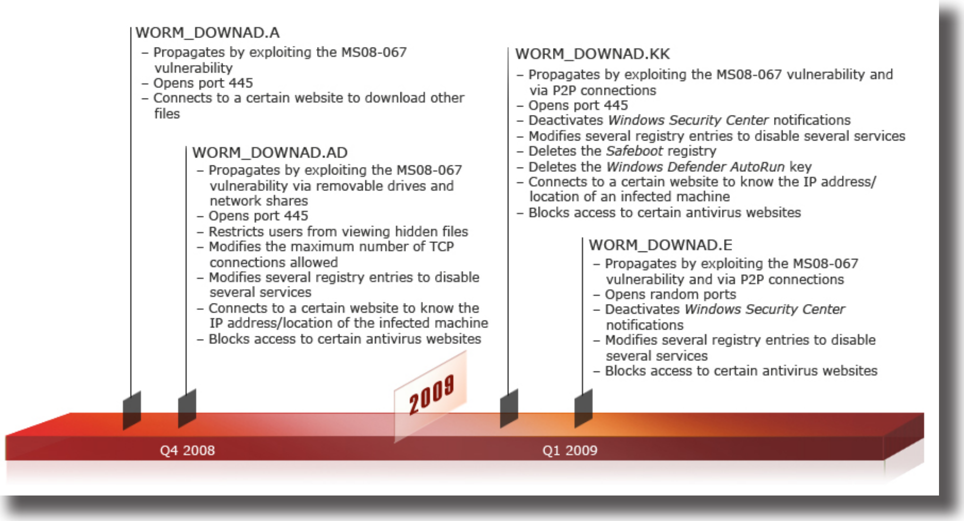
WORM_DOWNAD.A
– Propagates by exploiting the MS08-067 vulnerability
– Opens port 445
– Connects to a certain website to download other files
WORM_DOWNAD.AD
– Propagates by exploiting the MS08-067 vulnerability via removable drives and network shares
– Opens port 445
– Restricts users from viewing hidden files
– Modifies the maximum number of TCP connections allowed
– Modifies several registry entries to disable several services
– Connects to a certain website to know the IP address/location of the infected machine
– Blocks access to certain antivirus websites
WORM_DOWNAD.KK
– Propagates by exploiting the MS08-067 vulnerability and via P2P connections
– Opens port 445
– Deactivates Windows Security Center notifications
– Modifies several registry entries to disable several services
– Deletes the Safeboot registry
– Deletes the Windows Defender AutoRun key
– Connects to a certain website to know the IP address/location of an infected machine
– Blocks access to certain antivirus websites
WORM_DOWNAD.E
– Propagates by exploiting the MS08-067 vulnerability and via P2P connections
– Opens random ports
– Deactivates Windows Security Center notifications
– Modifies several registry entries to disable several services
– Blocks access to certain antivirus websites
2009
Q4 2008
Q1 2009

***Figure 1.** DOWNAD/Conficker timeline*

Based on the Conficker Working Group's DOWNAD/Conficker timeline from May 2009 onward, the malware family seemed to have died a sudden, quiet death. The greater proportion of cybersurfers may think this is the case as well but Akamai Technologies objects. New evidence from the Conficker Working Group's website and the latest cyber attacks in Europe also suggest that this worm is still very much at large.

Fresh Prints

Europe was found to have been one of DOWNAD/Conficker's most affected regions worldwide. Unlike in the past, however, the spotlight seems to have shifted from Italy and Spain to the United Kingdom.

Cybercrime Scene 1

On February 2, 2010, news of the Greater Manchester Police's network falling victim to DOWNAD/Conficker came out. A security expert revealed that the infection started from an infected USB drive that was plugged into a networked computer, which resulted in the automatic and silent execution of a copy of the worm and later on in the worm's propagation. Upon the discovery of the outbreak, the Greater Manchester Police's network was disconnected from the United Kingdom's national police computer system for three days. This left the police force's officers incapable of conducting online computer checks on criminals.

Cybercrime Scene 2

The Register also recently reported about a DOWNAD/Conficker outbreak affecting NHS Leeds at around the same time the Great Manchester Police infection broke out. The network outbreak, which was deemed minor, was said to have originated from an infected laptop. Based on information from an internal memo, around 9–10 of the healthcare service provider's servers was hit.

Cybercrime Scene 3

Exactly a week after the NHS Leeds incident, another NHS hospital fell prey to a DOWNAD/Conficker infection. This time, the target was West Middlesex University Hospital NHS Trust. Unlike in the previous NHS outbreak, this hospital's operation was greatly affected. Unable to book appointments over the network, hospital staff resulted to the traditional way of booking patients, using pen and paper. This resulted in huge delays with regard to serving patients and dampened the hospital's usual smooth operation.

A typical DOWNAD/Conficker infection:

- Exploits a Microsoft bug to gain access
- Drops a hidden file onto removable drives that automatically executes when the drives are enabled
- Forces its way into network servers using a list of passwords
- Drops a copy of itself into any shared folder on affected systems
- Reinfects already-infected PCs

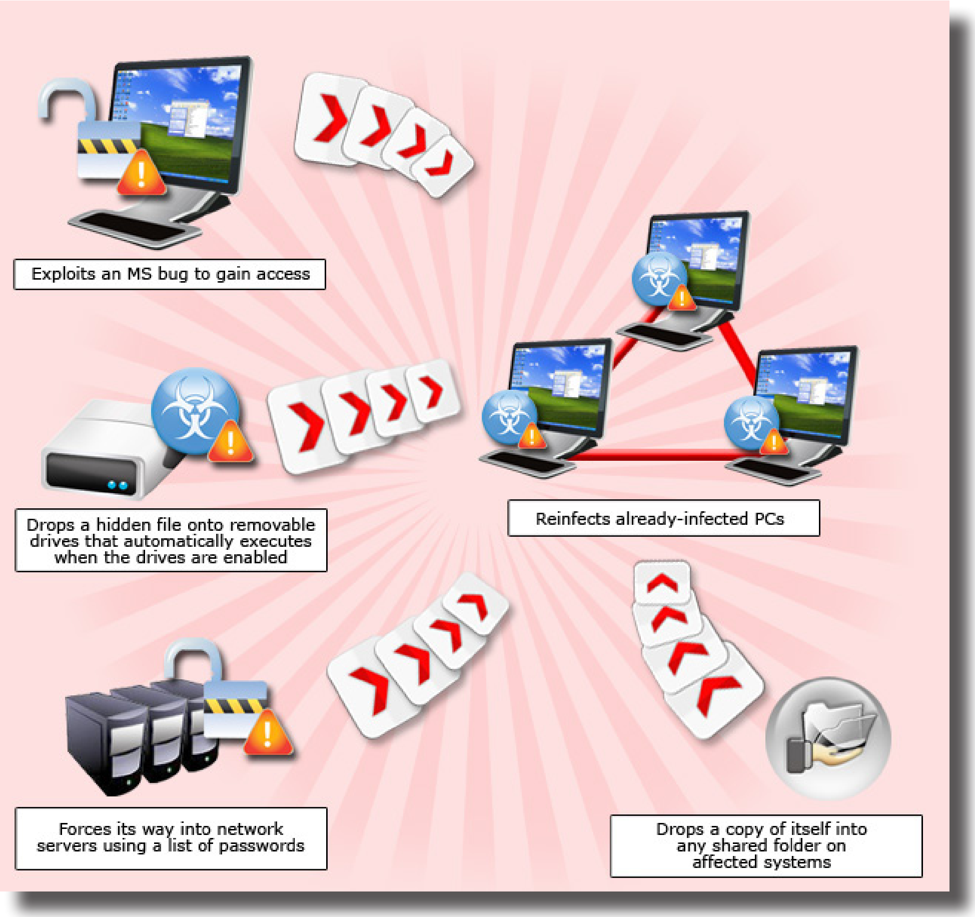
Exploits an MS bug to gain access
Reinfects already-infected PCs
Drops a hidden file onto removable drives that automatically executes when the drives are enabled
Forces its way into network servers using a list of passwords
Drops a copy of itself into any shared folder on affected systems

***Figure 2.** Typical DOWNAD/Conficker infection diagram*

Infection Rap Sheet

Based on the above-mentioned incidents, security experts have identified the following five reasons why DOWNAD/Conficker remains wild:

- **Unknowingly limiting system scanning.** Connecting an infected USB drive to a networked system is not much of a problem as failing to scan it for malware before actually opening it. Users with antivirus applications installed have become so used to only scanning their desktops or laptops. Failing to scan drives connected to systems is actually a step closer to entirely compromising their security.

- **Prolonged use of legacy systems.** The NHS servers that were hit by the DOWNAD/Conficker worm ran on legacy OSs, perhaps using versions earlier than Windows 2000. Such systems are incapable of obtaining and applying security measures once infected. In an interview, Rik Ferguson, one of Trend Micro's security consultants, speculated that the threat could have been automatically neutralized if legacy systems were not used.

Security experts have identified the following reasons why DOWNAD/Conficker remains wild:

- Unknowingly limiting system scanning
- Prolonged use of legacy systems
- Absence of antivirus solutions on systems
- Use of weak passwords
- Enabled AutoRun feature

- **Absence of antivirus solutions on systems.** This could be connected to prolonged use of legacy systems, which are incapable of supporting antivirus applications. Another reason why antivirus solutions are not present on NHS' computers or on other organizations' systems for that matter is the lack of concern for maintaining security in comparison with maintaining patients' privacy and confidentiality. Only in the end do these organizations find out that their lack of prudence could only lead to disaster.

- **Use of weak passwords.** DOWNAD/Conficker is capable of launching brute force dictionary attacks on password-protected networks. It has a hardcoded list of passwords that can easily guess highly predictable passwords. It is no surprise therefore that systems get hacked into easily when people still use weak passwords even in today's complex threat landscape.

- **Enabled AutoRun feature.** Trend Micro Advance Threat Researcher, Robert McArdle, implores readers in a *TrendLabs Malware Blog* entry to disable Windows' AutoRun feature because, basically, companies have no need for it.

Anticipating DOWNAD/Conficker's Next Move

In a 2009 forecast, the Conficker Working Group's director, Rodney Joffe, claimed that DOWNAD/Conficker will continue to be a menace in cyberspace in 2010 and to stay on top as the botnet and malware king. Another security company backed this claim up, saying that this worm can do even more damage—totally deactivating network and endpoint security defenses and blocking certain websites, particularly security sites, from user access for long periods of time—to affect more systems and networks. Furthermore, cybercriminals can use DOWNAD/Conficker to steal email information for spamming purposes and to automate ad clicks in order to gain profit.

Case Solved? Not Quite...

The recent DOWNAD/Conficker incidents in the United Kingdom clearly show that the malware family is still actively affecting more Internet users at this point in time. Case closed, right? Not quite.

Despite putting out a bounty on the heads of the minds behind DOWNAD/Conficker, someone has yet to get arrested for masterminding and perpetuating related cybercrimes. As such, people should continue to expect the worst and to wait. Unfortunately, waiting for prolonged periods of time eventually push people to put ideas far back into their minds until they totally forget. They get used to the existence of threats and how sophisticated and dangerous they are when they strike.

As consumers of online products and services, we are responsible for securing our systems so they can stay protected from DOWNAD/Conficker and other such threats both online and offline. We at Trend Micro can only continue to advise users to religiously install software updates and security patches and to make sure they use effective security solutions that can protect them from all kinds of threats.

Non-Trend Micro product users can also avail of the following free tools to help them detect and rid their systems of DOWNAD/Conficker worm variants:

- *HouseCall,* an online tool that can scan, identify, and clean file-based threats
- *RUBotted,* a tool that can monitor systems for suspicious bot-related activities
- *Web Protection Add-On,* a tool that protects desktops and laptops from all kinds of Web threats

References:

- Conficker Working Group. (April 1, 2009). *Conficker Working Group.* "Home Page." http://www.confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage (Retrieved March 2010).
- Conficker Working Group. (April 26, 2009). *Conficker Working Group.* "Timeline." http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline (Retrieved March 2010).
- Conficker Working Group. (October 30, 2009). *Conficker Working Group.* "Infection Tracking." http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking (Retrieved March 2010).
- Dan Raywood. (February 2, 2010). *SC Magazine.* "Greater Manchester Police Hit by Conficker from Infected USB That Leaves It Unconnected from Its Network for Three Days." http://www.scmagazineuk.com/greater-manchester-police-hit-by-conficker-from-infected-usb-that-leaves-it-unconnected-from-its-network-for-three-days/article/162904/ (Retrieved March 2010).
- Jaikumar Vijayan. (January 22, 2010). *Macworld.* "Users Still Make Hacking Easy with Weak Passwords." http://www.macworld.com/article/145840/2010/01/passwords.html (Retrieved March 2010).
- John Leyden. (February 9, 2010). *The Register.* "Conficker Outbreak Infects Leeds NHS Servers." http://www.theregister.co.uk/2010/02/09/conficker_nhs_outbreaks/ (Retrieved March 2010).
- John Leyden. (February 18, 2010). *The Register.* "Another NHS Hospital Stricken with Conficker Virus." http://www.theregister.co.uk/2010/02/18/conficker_nhs/ (Retrieved March 2010).
- Microsoft Corporation. (2010). *msdn.* "Enabling and Disabling AutoRun." http://msdn.microsoft.com/en-us/library/cc144204%28VS.85%29.aspx (Retrieved March 2010).
- *My Digital Life.* (2005–2010). "List of Common and Easily Hacked Passwords That Should Not Be Used." http://www.mydigitallife.info/2010/01/07/list-of-common-and-easily-hacked-passwords-that-should-not-be-used/ (Retrieved March 2010).

- Robert McArdle. (January 16, 2009). *TrendLabs Malware Blog.* “Security Policy for Dummies—How to Avoid WORM_DOWNAD Infection.” http://blog.trendmicro.com/security-policy-for-dummies-how-to-avoid-worm_downad-infection/ (Retrieved March 2010).

- Sumner Lemon. (January 15, 2010). *PCWorld.* “Conficker Worm Hasn’t Gone Away.” http://www.pcworld.com/article/186977/conficker_worm_hasnt_gone_away_akamai_says.html?tk=rss_news (Retrieved March 2010).

- Trend Micro. *Threat Encyclopedia.* “WORM_DOWNAD.A.” http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.A (Retrieved March 2010).

- Trend Micro. *Threat Encyclopedia.* “WORM_DOWNAD.AD.” http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.AD (Retrieved March 2010).

- Trend Micro. *Threat Encyclopedia.* “WORM_DOWNAD.E.” http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.E (Retrieved March 2010).

- Trend Micro. *Threat Encyclopedia.* “WORM_DOWNAD.KK.” http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.KK (Retrieved March 2010).