



Customer Information on WORM_DOWNAD.KK Detection, Cleanup, and Prevention

- **IMPORTANT:** The content of this notification is intended solely for Trend Micro Partners and Customers regarding the WORM_DOWNAD.KK infection.



Dear Trend Micro Customer:

Recent news and media reports have been generated regarding a potential new WORM_DOWNAD (also known as Conficker) threat, with some malicious activity set to activate on April 1, 2009.

This document presents some facts and other information to help customers best protect themselves against threats known at this time.

Background:

For the purposes of this document, below is Trend Micro's detection for WORM_DOWNAD/Conficker.

Trend Micro naming convention vs. industry:

- WORM_DOWNAD.A aka Conficker.A
- WORM_DOWNAD.AD aka Conficker.B
- WORM_DOWNAD.AD aka Conficker.B++
- WORM_DOWNAD.KK aka Conficker.C

WORM_DOWNAD (aka Conficker) is a worm, which originally appeared up in November 2008. It exploits a vulnerability in Windows that Microsoft patched (MS08-067) in October.

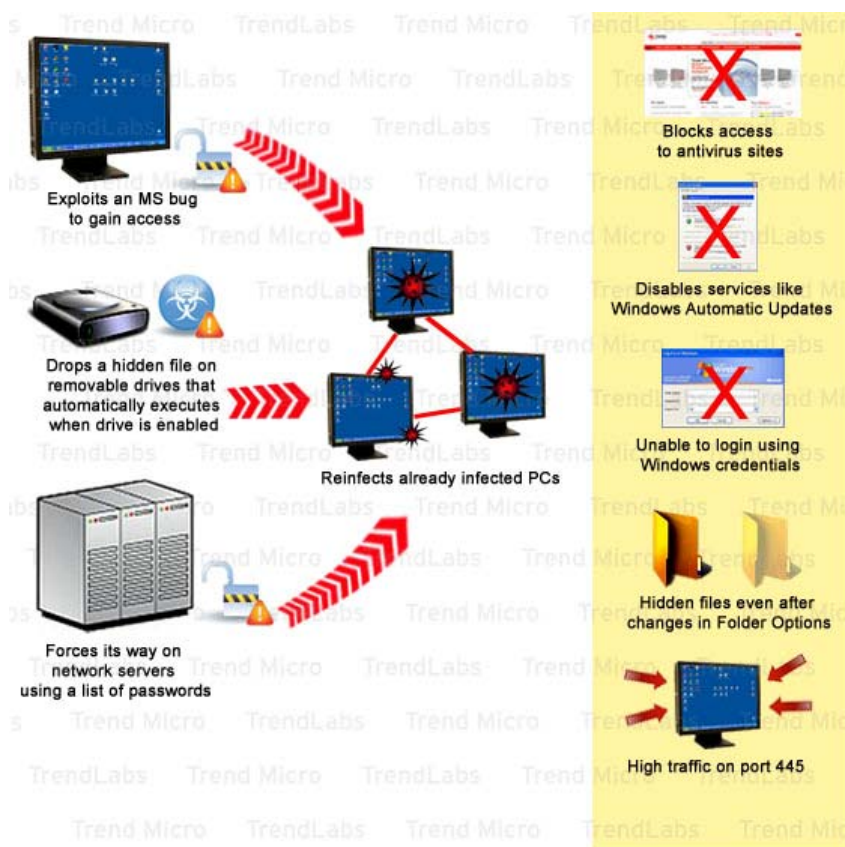
WORM_DOWNAD.AD, detected in February 2009, added the ability to spread through network shares and via removable storage devices (e.g. USB drives) through the AutoRun function in Windows.

WORM_DOWNAD.KK, which surfaced earlier this month, also shuts down security services, blocks infected computers from connecting to security Web sites, and downloads a Trojan. It also reaches out to other infected computers via peer-to-peer communications services, and includes an algorithm to generate a list of 50,000 different domains, of which 500 will be randomly selected to be contacted by the infected computer beginning on April 1st to receive updated copies, new malware components, or additional functional instructions. Previous



WORM_DOWNAD variants were written to generate & connect to 250 domains a day.

WORM_DOWNAD General Behavior



Fact Sheet: WORM_DOWNAD.KK

WORM_DOWNAD.AD and .KK are two recent variants that have been found in the wild. Below is a match-up between the two:

Behavior	WORM_DOWNAD.AD	WORM_DOWNAD.KK
Terminates several process that matches with its list	No	Yes
Deletes safeboot registry	No	Yes
Deletes WINDOWS DEFENDER autorun key	No	Yes



# of random URL domains to be created	250	50,000
Trigger for the creation of random domains	9-Jan-09	1-Apr-09
Propagates via removable drives	Yes	No
Propagates via MS08-067 exploit	Yes	Yes
Dropped file name	{random}.dll	{random}.dll
Create random service	Yes	Yes
Hooks API	Yes	Yes
Blocks access to certain antivirus websites	Yes	Yes
Checks the system time by connecting to several websites	Yes	Yes
Modifies this registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost	Yes	Yes
Copy itself to the following folders	%Program Files%\Internet Explorer %Program Files%\Movie Maker %Temp% %Application Data% %system dir%	%Program Files%\Internet Explorer %Program Files%\Movie Maker %Program Files%\Windows Media Player %Program Files%\Windows NT
Has regrun (autorun) entry	Yes	Yes
Propagates via network shares (creation of JOB file)	Yes	No
Uses port 445	Yes	Yes
Inject malware process to several normal running processes	Yes (svchost or services.exe)	Yes (svchost or services.exe)
Checks target machine OS	Yes	Yes
modifies several registry entries to disable certain services Background Intelligent Transfer Service (BITS) Windows Error Reporting Service Windows Security Center Service Windows Automatic Update Service	Yes	Yes



Modifies registry permission for its service	Yes	Yes
Connects to certain website to know the IP/location of the infected machine	Yes	No

Prevention and Detection:

Trend Micro recommends that home users who have not yet enabled automatic updates do so as soon as possible so that their security software is up to date with the latest signatures.

Enterprise and business customers should continue to focus on the guidance from experts in industry, academia, and governments worldwide and continue to deploy the security update MS08-067, ascertain that their security software has the latest pattern files and scan engine technology, clean any systems that are infected with any version of WORM_DOWNAD using the tools and guidance Trend Micro provides, and evaluate additional security best practices in accordance with their organizations policies and procedures.

Trend Micro also strongly recommends the following steps to prevent attacks, execute cleanup, or completely remove the threat:

Prevention using Trend Micro technology:

- Block exploits at network endpoints with Intrusion Defense Firewall, a plug-in that extends Host Intrusion Prevention System (HIPS)
- Detect vulnerability MS08-067 and others with Vulnerability Assessment Pattern 94
- Network Virus Pattern 10273 and up detects the exploit at the network layer

The following best practices are highly recommended to further prevent DOWNAD attacks:

- Immediately install fix patches/updates for MS08067 and other vulnerabilities as soon as vendors release these patches



- ❑ Disable “Drive Auto-run” feature to avoid infections from USB drives (DOWNAD.AD)
- ❑ Require complex passwords for all workstations, as discussed by Microsoft at <http://technet.microsoft.com/en-us/library/cc786468.aspx>, to prevent brute force password attacks through scheduled tasks (DOWNAD.AD)
 - Password Policies in network groups can be applied to impede spreading of attacks across networks: (DOWNAD.AD)
 - ❑ To modify Group Policy refresh interval, check this page: <http://support.microsoft.com/kb/203607/EN-US/>
 - ❑ For immediate Group Policy refresh, check this page: <http://support.microsoft.com/kb/227302>

Trend Micro modules for complete Cleanup and Removal:

Products	VSAPI Engine	RCM (Rootkit)	Clean-Up
OSCE 8.0	8.911-1001	2.2 or above	Genericlean + DCE 6.0.1172 + DCT OPR 1020 or above (Enabling Web Reputation Service is recommended for blocking malicious sites, but not required for cleanup)
OSCE 7.x	8.913-1006	N/A	Genericlean (build 1120 or higher) + DCE 6.0.1172 + DCT OPR 1020 or above
CSM 3.6	8.911-1001	2.2 or above	Genericlean (patch 2) + DCE 6.0.1172 + DCT OPR 1020 or above
WFBS 5.x	8.911-1001	2.2 or above	Genericlean + DCE 6.0.1172 + DCT OPR 1020 or above (Enabling Web Reputation Service is recommended for blocking malicious sites, but not required for cleanup)



SPNT 5.x	8.913-1006	N/A	Sysclean Tool (link below)
----------	------------	-----	----------------------------

Please note that the following VSAPI versions are required for Cleanup and Removal of already infected systems. **Uninfected customers** that have the latest pattern file and VSAPI version available from ActiveUpdate should be able to detect and block all known variants. As a best practice, it is also highly recommended that MS08-067 is applied to non-patched systems as soon as possible.

VSAPI8.913 allows all existing desktop products to detect WORM_DOWNAD on already infected machines and is specifically for endpoint clients that do not have the Rootkit Module (shown above as N/A under RCM). VSAPI8.913 is available for download from engine download center: <http://www.trendmicro.com/download/engine.asp>.

However Trend Micro has not yet uploaded VSAPI 8.913 to ActiveUpdate because of a reported compatibility issue with Microsoft Encrypting File System (EFS). Trend Micro is currently working with Microsoft to resolve this issue, and current open cases on this issue are very few, so adverse risk of deploying this engine is considered very low.

For customers not using EFS, there are no known issues with downloading and deploying the latest VSAPI 8.913 version. For customers who are using Microsoft Encrypting File System in their environment and require VSAPI 8.913-1006 or requires some additional assistance with deploying the engine **please contact Trend Micro technical support so that a suitable alternative may be found.**

Clean-up:

It is important to **restart the system** after applying Clean-up (DCE+DCT or Sysclean).

If a machine is already infected, DOWNAD.KK **prevents access to trendmicro.com**. In this case, the following steps are recommended:

1. In a clean machine, download Sysclean here:



- a. http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip

The original Sysclean tool (SYSCLEAN.COM) was terminated by WORM_DOWNAD.KK by checking the filename. To account for this, the tool in this package has a slightly different name to work-around this potential setback.

2. Executing (running) the Sysclean tool accomplishes the following:
 - a. Removes injected processes in memory
 - b. Removes added service
 - c. Restores safeboot registry to enable safe mode booting
3. As mentioned above, it is important to reboot the system after the cleaning procedure to ensure complete cleanup.
4. Update all Trend Micro product components after executing Sysclean, refer to the table above.

Additional Information on the April 1st Reports:

Based on our threat research, WORM_DOWNAD.KK is purported to start its download capability on April 1, 2009, on systems infected with this variant. This threat will generate up to 50,000 random URLs and attempt to resolve and connect to 500 of the generated URLs. Once it connects to these 500 URLs, it is capable of downloading and executing any file from said resolved URLs.

According to Trend Micro's threat research team at this time, there is currently **NO** evidence that indicates that WORM_DOWNAD.KK will do anything beyond changing its auto-domain generation routine to increase the number of "rendezvous" peer domains to 50,000 (and connect to only a subset of 500 randomly selected domains).

It is possible that systems infected with the latest version of WORM_DOWNAD could be updated with a newer version of this threat on April 1 by contacting domains on the new domain list. However to this point, these systems could be



updated on any date before or after April 1 as well using the "peer- to-peer" updating channel in the latest version of WORM_DOWNAD, so this is a known issue with any infected system.

The latest information about this malware please can be found by visiting Trend Micro's Virus Encyclopedia at:

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FDOWNAD%2EKK&VSect=T>

For Additional Assistance:

For additional information or users who believe they may have been affected by this issue should contact their authorized Trend Micro technical support services provider in their region for further assistance.