Win32.Worm.Downadup - Conficker

Detection, Cleanup and Prevention

From

MicroWorld

Dear eScan Customer:

Downadup alias Conficker first evolved in late 2008, began making headlines in January as known infections topped several million computers.

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

Background:

Win32.Worm.Downadup emerged late November 2008 has exploited most of the malware entry points available in the Operating System and exploited to its benefit. Once the computer infected by the worm, it alters all the pre-requisite registry location to spread through Network, removable drives (USB sticks). The Worm can enter user's system in multiple ways, it may be through network with Admin$ share (brute force dictionary attack), systems with unsecured shares, systems not patched with vulnerability or USB drive etc. Due to this even though user follows the safe computing practice, system may get infected.

Upon execution the worm copies itself with the random name with **.dll** extension in the following locations:

- **Windows System**
- **Programs Files\Internet Explorer**
- **Programs Files\Movie Maker**
- **All Users Application Data**
- **Windows Temp**

and with the random name with **.tmp** extension in the following locations:

- **Windows System**
- **Windows Temp**

The worm disables the following services:

- **Windows Automatic Update Service (wuauserv)**
- **Background Intelligent Transfer Service (BITS)**
- **Windows Security Center**
- **Windows Defender**
- **Windows Error Reporting**

It also drops following files in the removable and mapped drives:

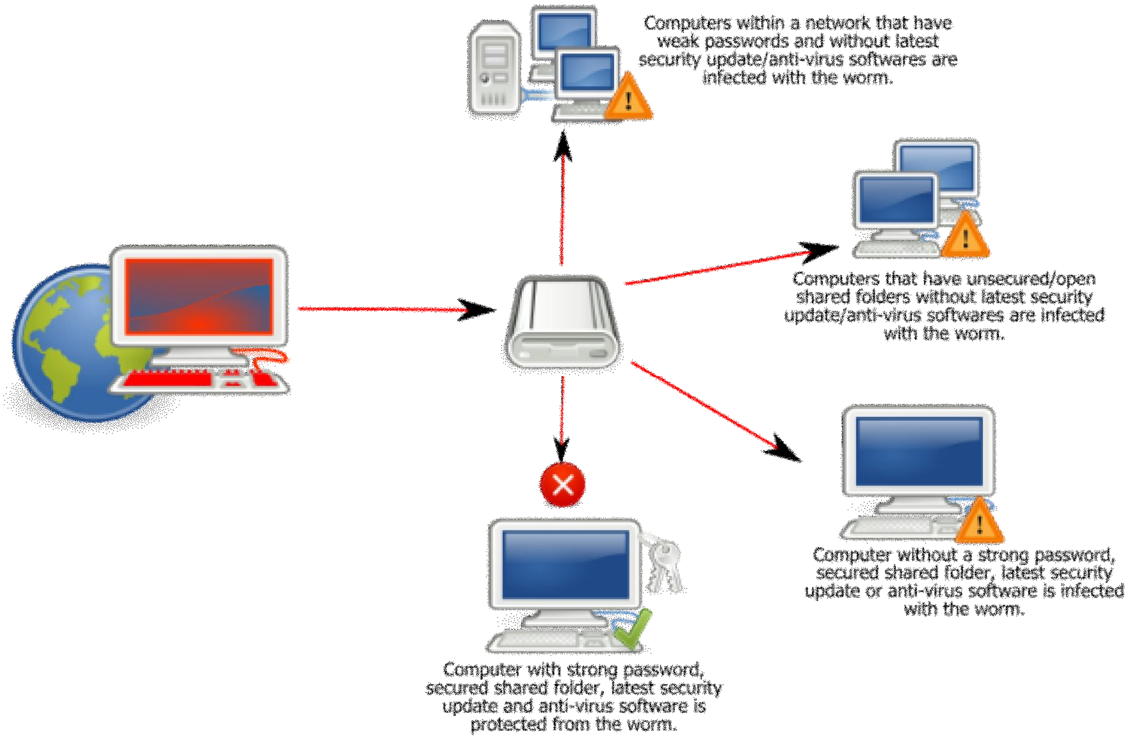
- \RECYCLER\
- \autorun.inf

The worm attaches itself to the following Windows processes:

- **svchost.exe**
- **explorer.exe**
- **services.exe**

Win32.Worm.Downadup General Behavior

Win32.Worm.Downadup


Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

Infection symptoms:

- Access to Admin shares are denied.
- Scheduled tasks are created.
- Access to security related websites is denied.
- Access to Windows Updates site is denied.
- Network response will become considerably slow.
- Domain controllers respond slowly to client request.

The worm modifies registry at the following locations:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**
- **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SvcHost**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**

Payload

The worm attempts to create a HTTP Server and open a random port between 1024 and 10000 in the victim computer. On successful creation of the HTTP Server, the worm downloads the copy of itself to the victim computer. The worm also resets the Restore point. Most of the Variants of the Downadup worm will trigger the payload on **April 1**. Though we are conducting lot of research on the payload, the exact payload and the damage it can create on **April 1**st is still a mystery.

Prevention and Detection:

MicroWorld 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. Offline users isolated from internet may download offline updates from MicroWorld.

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 Win32.Worm.Downadup using the tools and guidance MicroWorld provides, and evaluate additional security best practices in accordance with their organizations policies and procedures.

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

Prevention using eScan technology:

- Real Time Monitor with intelligent Proactive Scan blocks any known or unknown exploits that try to penetrate the system.
- Detects vulnerability MS08-067 and others and downloads the necessary critical updates if required.
- Endpoint Security disables the auto run of all portable storage devices plugged in to a system thereby by effectively blocking the most common methods through which DOWNADUP spreads.

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

- Immediately Run "Download Latest Hot fix (Microsoft Windows OS)" under "Tools" section in eScan Protection Center. This will install patches/updates for MS08067 and other vulnerabilities as soon as vendors release these patches.
- Use End Point Security feature in eScan Protection Center to Disable "Drive Auto-run" feature to avoid infections from USB drives (DOWNADUP)
- 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 (DOWNADUP)

Password Policies in network groups can be applied to impede spreading of attacks across networks: (DOWNADUP)

- 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

Cleanup and Removal with eScan:

Please note that latest updates and hot fixes from MicroWorld are required for Cleanup and Removal of already infected systems with eScan. Alternatively download the latest available toolkit utility MWAV (MicroWorld Anti-Virus and Toolkit Utility) from MicroWorld.

Uninfected customers that have the latest updates and hot fixes from MicroWorld 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.
eScan duly patched with latest hotfix allows all existing desktop products to detect Win32.Worm.Downadup on already infected. Latest eScan is available for download from

http://download1.mwti.net/wiki/index.php/EScan_for_Windows_v10

Clean-up:
If a machine is already infected, DOWNADUP **prevents access to almost all the security sites.**

In this case, the following steps are recommended:

1. In a clean machine, download MWAV from:

   http://update6.mwti.net/download/tools/mwav.exe

2. Execute the downloaded tool mwav.exe. Executing the tool accomplishes the following:

   a. Removes injected processes in memory

   b. Removes added service

   c. Restores safe boot registry to enable safe mode booting.

   d. Renames any unknown threat active in the memory.

3. As mentioned above, it is important to reboot the system after the cleaning procedure to ensure complete cleanup.

4. Update all eScan product components after cleaning with mwav.exe.

Additional Information on the April 1st Reports:

Okay, that's Downadup in a nutshell. Now we'd better get to explaining what April fool's day has to do with this. Apparently, several experts in the Downadup cabal have reversed engineered Downadup's code and determined that April 1st is when computers infected with Downadup are supposed to wake up and begin searching for command and control servers. Hopefully the Downadup Cabal has a plan.

On April 1st the Downadup worm will simply start taking more steps to protect itself. After that date, machines infected with the "C" variant of the worm may not be able to get security updates or patches from Microsoft and from many other vendors. The creators of the worm will also start using a communications system that is more difficult for security researchers to interrupt.

Current users of MicroWorld's eScan security products are protected from these variants of worm. Those who are unprotected are invited to download the trial version of eScan Internet Security Suite from the following link:

http://update3.mwti.net/download/escan/escan10/iwn2k3ek.exe

Also, below is the download link for eScan Hotfixes.

http://download1.mwti.net/wiki/index.php/Hotfixes

The latest information about this malware can be found by visiting eScan's Virus Encyclopedia at:
http://www.mwti.net/virus_info/virusalertd.asp?id=1066

For Additional Assistance:

For additional information or users who believe they may have been affected by this issue should contact their authorized eScan technical support service providers in their region for further assistance or write to support@mwti.net.