Symantec.

Symantec Security Response

http://www.symantec.com/security_response/index.jsp

W32.Downadup.C

Risk Level 2: Low

Discovered:
March 6, 2009
Updated:
April 6, 2009 6:30:44 PM
Also Known As:
Mal/Conficker-B [Sophos], Worm:W32/Downadup.DY [F-Secure], Trojan-Downloader.Win32.Kido.a [Kaspersky]
Type:
Trojan, Worm
Infection Length:
88,576 bytes
Systems Affected:
Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP

SUMMARY

W32.Downadup.C is a threat that is downloaded on to the compromised computer by the W32.Downadup family of worms.

Note: For more information, please see the following resource:
W32.Downadup

Antivirus Protection Dates

- **Initial Rapid Release version** March 6, 2009 revision 036
- **Latest Rapid Release version** September 28, 2010 revision 054
- **Initial Daily Certified version** March 6, 2009 revision 037
- **Latest Daily Certified version** September 28, 2010 revision 036
- **Initial Weekly Certified release date** March 11, 2009

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Threat Assessment

Wild

- **Wild Level:** Medium
- **Number of Infections:** 1000+
- **Number of Sites:** 10+
- **Geographical Distribution:** High
- **Threat Containment:** Moderate
- **Removal:** Difficult

Damage

- **Damage Level:** High
- **Payload Trigger:** File downloading is triggered after 1st April 2009.
- **Payload:** Attempts to download files from a predetermined list of addresses. Also attempts to intercept and redirect DNS requests to prevent access to certain Web sites.
- **Compromises Security Settings:** Stops certain Windows services and security related processes.

Distribution

- **Distribution Level:** Medium
- **Target of Infection:** Computers already infected by earlier variants of the W32.Downadup family of worms.

TECHNICAL DETAILS

Once executed, the threat disables the following services:

- BITS
- ERSvc
- WerSvc
- WinDefend
- wscsvc
- wuauserv

It then lowers security settings by deleting the following registry entry to prevent automatic startup of certain software:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Windows Defender"

It then disables Windows Security Alert notifications by deleting the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-41F1-9A6F-135D9C6622CC}

It also deletes the following registry subkey to prevent the compromised computer from restarting in safe mode:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot

The threat may create the following registry subkeys:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 1]
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 1]

Note: [CLSID 1] is generated from the serial number of the compromised computer and hence will vary.

It may then create the following registry entries:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"

Note:
[CLSID 2] is generated from the serial number of the compromised computer and hence will vary.

[WORD 1] and [WORD 2] are randomly selected from the following list:

- 64
- Adobe
- Agent
- App
- Assemblies
- assembly
- Audit
- Backup
- Boot
- Boot
- Browser
- Build
- Calendar
- Center
- Collaboration
- Common
- Component
- Components
- Config
- Control
- Cursors
- Debug
- Defender
- Definitions
- Digital
- Discovery
- Distribution
- Documents
- Downloaded
- Driver
- en
- Event
- Explorer
- Files
- Fonts
- Framework
- Gallery
- Games
- Globalization
- Google
- Hardware
- Help
- Helper
- Image
- IME
- inf
- Installer
- Installer
- Intel
- Inter

- Internet
- Java
- Journal
- Kernel
- L2S
- Live
- Logon
- Logs
- Machine
- Mail
- Maker
- Management
- Manager
- Media
- Microsoft
- Microsoft
- Mobile
- Modem
- Monitor
- Movie
- MS
- msdownld
- NET
- Network
- New
- Notify
- Office
- Offline
- Options
- Packages
- Pages
- Patch
- Performance
- Photo
- PLA
- Player
- Policy
- Policy
- Power
- Prefetch
- Profiles
- Program
- Publish
- Reference
- Registered
- registration
- Reports
- Resources
- schemas
- Security
- Security
- Server
- Service
- Setup
- Shell
- Shell
- Software
- Speech
- Storage

- Support
- System
- System
- Task
- Tasks
- Temp
- Time
- tmp
- tracing
- Trusted
- twain
- Universal
- Update
- US
- Video
- Visual
- Web
- Windows
- winsxs
- Works
- Zx

Next, it stops any process containing the following strings in the name:

- autoruns
- avenger
- bd_rem
- cfremo
- confick
- downad
- dwndp
- filemon
- gmer
- hotfix
- kb890
- kb958
- kido
- kill
- klwk
- mbsa.
- mrt.
- mrtstub
- ms08
- ms09
- procexp
- procmon
- regmon
- scct_
- stinger
- sysclean
- tcpview
- unlocker
- wireshark

The threat then copies itself to one of the following locations:

- %ProgramFiles%\Internet Explorer\[RANDOM FILE NAME].dll
- %ProgramFiles%\Movie Maker\[RANDOM FILE NAME].dll
- %ProgramFiles%\Windows Media Player\[RANDOM FILE NAME].dll
- %System%\Windows NT\[RANDOM FILE NAME].dll

It may then create the following file:
Temp%\[CLSID 3]\[NUMBER].tmp

Note:

- [CLSID 3] is generated from the serial number of the compromised computer and hence will vary.
- [NUMBER] is a decimal number between 0 and 63 inclusive.

The threat creates the following registry entry, so that it runs every time Windows starts:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "rundll32.exe "[RANDOM DLL FILE NAME]", [RANDOM PARAMETER STRING]"

It creates a service with the following characteristics:
Name: [SERVICE NAME]
Startup Type: Automatic

[SERVICE NAME] is a two word combination taken from the following two lists:
List 1:

- App
- Audio
- DM
- ER
- Event
- las
- lr
- Lanman
- Net
- Ntms
- Ras
- Remote
- SR
- Sec
- Tapi
- Trk
- W32
- Wmdm
- Wmi
- help
- win
- wsc
- wuau
- xml

List 2:

- access
- agent
- auto
- logon
- man
- mgmt

- mon
- prov
- serv
- Server
- Service
- Srv
- srv
- svc
- Svc
- System
- Time

It registers the service by creating the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM CHARACTERS]\"ImagePath" = "%System%\svchost.exe -k netsvcs"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM CHARACTERS]\Parameters\"ServiceDll" = "[PATH TO THE THREAT]"

The threat patches the following APIs that are used by Windows to make DNS requests or request URLs:

- DNS_Query_A
- DNS_Query_UTF8
- DNS_Query_W
- Query_Main
- sendto

The threat monitors DNS requests to domains containing any of the following strings and blocks access to these domains so that the DNS request appears to have timed out:

- activescan
- adware
- agnitum
- ahnlab
- anti-
- antivir
- arcabit
- avast
- avg.
- avgate
- avira
- avp.
- av-sc
- bdtools
- bit9.
- bothunter
- ca.
- castlecops
- ccollomb
- centralcommand
- cert.
- clamav
- comodo
- computerassociates

- confick
- coresecur
- cpsecure
- cyber-ta
- defender
- downad
- doxpara
- drweb
- dslreports
- emsisoft
- enigma
- esafe
- eset
- etrust
- ewido
- fortinet
- f-prot
- freeav
- free-av
- fsecure
- f-secure
- gdata
- gmer.
- grisoft
- hackerwatch
- hacksoft
- hauri
- honey
- ikarus
- insecure.
- iv.cs.uni
- jotti
- k7computing
- kaspersky
- kav.
- kido
- llnw.
- llnwd.
- malware
- mcafee
- microsoft
- mirage
- mitre.
- msdn.
- msft.
- msftncsi
- ms-mvp
- msmvps
- mtc.sri
- nai.
- ncircle
- networkassociates
- nmap.
- nod32
- norman
- norton
- onecare
- panda
- pctools

- precisesecurity
- prevx
- ptsecurity
- qualys
- quickheal
- removal
- rising
- rootkit
- safety.live
- sans.
- secunia
- securecomputing
- secureworks
- snort
- sophos
- spamhaus
- spyware
- staysafe
- sunbelt
- symantec
- technet
- tenablese
- threat
- threatexpert
- trendmicro
- trojan
- vet.
- virscan
- virus
- wilderssecurity
- windowsupdate

It also connects to the following Web sites to to obtain the current date and time:

- ask.com
- baidu.com
- facebook.com
- google.com
- imageshack.us
- rapidshare.com
- w3.org
- yahoo.com

If the date and time is on or after 1st April 2009, it uses the date information to generate a list of domain names. The threat then contacts these domains in an attempt to download additional files on to the compromised computer.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.

- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

REMOVAL

Removal using the W32.Downadup Removal Tool
Symantec Security Response has developed a removal tool to clean the infections of W32.Downadup. Use this removal tool first, as it is the easiest way to remove this threat.

Manual Removal:
The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Find and stop the service.
4. Run a full system scan.
5. Delete any values added to the registry.

For specific details on each of these steps, read the following instructions.

1. To disable System Restore (Windows Me/XP)
If you are running Windows Me or Windows XP, we recommend that you temporarily turn off System Restore. Windows Me/XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore,

antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or one of the following articles:

- How to disable or enable Windows Me System Restore
- How to turn off or turn on Windows XP System Restore

Note: When you are completely finished with the removal procedure and are satisfied that the threat has been removed, reenable System Restore by following the instructions in the aforementioned documents.

For additional information, and an alternative to disabling Windows Me System Restore, see the Microsoft Knowledge Base article: Antivirus Tools Cannot Clean Infected Files in the _Restore Folder (Article ID: Q263455).

2. To update the virus definitions
Symantec Security Response fully tests all the virus definitions for quality assurance before they are posted to our servers. There are two ways to obtain the most recent virus definitions:

- Running LiveUpdate, which is the easiest way to obtain virus definitions.

  If you use Norton AntiVirus 2006, Symantec AntiVirus Corporate Edition 10.0, or newer products, LiveUpdate definitions are updated daily. These products include newer technology.

  If you use Norton AntiVirus 2005, Symantec AntiVirus Corporate Edition 9.0, or earlier products, LiveUpdate definitions are updated weekly. The exception is major outbreaks, when definitions are updated more often.

- Downloading the definitions using the Intelligent Updater: The Intelligent Updater virus definitions are posted daily. You should download the definitions from the Symantec Security Response Web site and manually install them.

Note: W32.Downadup.C may block access to Symantec Web sites and network addresses, which may result in failure to obtain the most recent virus definitions. Follow these steps to remove the block:

1. Click **Start > Run** or hit **Windows Key + R**.
2. Type **cmd**, and then click **OK**.
3. Type **net stop dnscache** and press **Enter**.
4. Type **exit** and press **Enter**.

The latest Intelligent Updater virus definitions can be obtained here: Intelligent Updater virus definitions. For detailed instructions read the document: How to update virus definition files using the Intelligent Updater.

3. To find and stop the service

1. Click **Start > Run**.
2. Type **services.msc**, and then click **OK**.
3. Locate and select the service that was detected.
4. Click **Action > Properties**.
5. Click **Stop**.

6. Change **Startup Type** to **Manual**.
7. Click **OK** and close the Services window.
8. Restart the computer.

4. To run a full system scan

1. Start your Symantec antivirus program and make sure that it is configured to scan all the files.

   For Norton AntiVirus consumer products: Read the document: How to configure Norton AntiVirus to scan all files.

   For Symantec AntiVirus Enterprise products: Read the document: How to verify that a Symantec Corporate antivirus product is set to scan all files.

2. Run a full system scan.
3. If any files are detected, follow the instructions displayed by your antivirus program.

Important: If you are unable to start your Symantec antivirus product or the product reports that it cannot delete a detected file, you may need to stop the risk from running in order to remove it. To do this, run the scan in Safe mode. For instructions, read the document, How to start the computer in Safe Mode. Once you have restarted in Safe mode, run the scan again.

After the files are deleted, restart the computer in Normal mode and proceed with the next section.

Warning messages may be displayed when the computer is restarted, since the threat may not be fully removed at this point. You can ignore these messages and click OK. These messages will not appear when the computer is restarted after the removal instructions have been fully completed. The messages displayed may be similar to the following:

Title: [FILE PATH]
Message body: Windows cannot find [FILE NAME]. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.

5. To delete the value from the registry
Important: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified subkeys only. For instructions refer to the document: How to make a backup of the Windows registry.

1. Click **Start > Run**.
2. Type **regedit**
3. Click OK.

   Note: If the registry editor fails to open the threat may have modified the registry to prevent access to the registry editor. Security Response has developed a tool to resolve this problem. Download and run this tool, and then continue with the removal.

4. Navigate to and delete the following registry subkeys:

   - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 1]
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 1]

5. Navigate to and delete the following registry entries:

   - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "rundll32.exe "[RANDOM DLL FILE NAME]", [RANDOM PARAMETER STRING]"

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM CHARACTERS]\"ImagePath" = "%System%\svchost.exe -k netsvcs"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM CHARACTERS]\Parameters\"ServiceDll" = "[PATH TO THE THREAT]"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\[CLSID 2]\"[WORD 1][WORD 2]" = "[BINARY DATA]"

6. Restore the following registry entries to their previous values, if required:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Windows Defender"
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects {FD6905CE-952F-41F1-9A6F-135D9C6622CC}
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot

7. Exit the Registry Editor.

   Note: If the risk creates or modifies registry subkeys or entries under HKEY_CURRENT_USER, it is possible that it created them for every user on the compromised computer. To ensure that all registry subkeys or entries are removed or restored, log on using each user account and check for any HKEY_CURRENT_USER items listed above.
