Search Microsoft.com Go

Win32/Conficker

Also Known As:

TA08-297A (other)
CVE-2008-4250 (other)
VU827267 (other)
Win32/Conficker.A (CA)
Mal/Conficker-A (Sophos)
Trojan.Win32.Agent.bccs (Kaspersky)
W32.Downadup.B (Symantec)
Trojan-Downloader.Win32.Agent.aqfw (Kaspersky)
W32/Conficker.worm (McAfee)
Trojan:Win32/Conficker!corrupt (Microsoft)
W32.Downadup (Symantec)
Conficker (other)

Summary

Win32/Conficker is a worm that infects other computers across a network by exploiting a vulnerability in the Windows Server service (SVCHOST.EXE). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. Depending on the specific variant, it may also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files.

Microsoft strongly recommends that users apply the update referred to in Security Bulletin MS08-067 immediately.

Microsoft also recommends that users ensure that their network passwords are strong to prevent this worm from spreading via weak administrator passwords. More information is available here.

Symptoms

System Changes

The following system changes may indicate the presence of this malware:

- The following services are disabled or fail to run:
  Windows Security Center Service
  Windows Update Auto Update Service
  Background Intelligence Transfer Service
  Windows Defender
  Error Reporting Service
  Windows Error Reporting Service
- Some accounts may be locked out due to the following registry modification, which may flood the network with connections:
  HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
  "TcpNumConnections" = "0x00FFFFFE"
- Users may not be able to connect to websites or online services that contain the following strings:
  virus
  spyware
  malware
  rootkit
  defender
  microsoft
  symantec
  norton
  mcafee
  trendmicro
  sophos
  panda
  etrust
  networkassociates
  computerassociates
  f-secure
  kaspersky
  jotti
  f-prot
  nod32
  eset
  grisoft
  drweb
  centralcommand
  ahnlab
  esafe
  avast
  avira
  quickheal
  comodo
  clamav
  ewido
  fortinet
  gdata
  hacksoft
  hauri
  ikarus
  k7computing
  norman
  pctools

- prevx
- rising
- securecomputing
- sunbelt
- emsisoft
- arcabit
- cpsecure
- spamhaus
- castlecops
- threatexpert
- wilderssecurity
- windowsupdate

Technical Information

Win32/Conficker is a worm that infects other computers across a network by exploiting a vulnerability in the Windows Server service (SVCHOST.EXE). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. Depending on the specific variant, it may also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files.

Installation

Conficker installs itself in different ways according to variant. However, both variants attempt to copy themselves to the Windows system folder as a hidden DLL file using a random name. They modify the registry in order to run this copy at each Windows start, for example:

Adds value: "<random string>"
With data: "rundll32.exe <system folder>\<malware file name>.dll,<malware parameters>"
To subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Spreads Via...

Exploit
Worm:Win32/Conficker spreads to systems that are not yet patched against a vulnerability in the Windows Server service (SVCHOST.EXE). If the vulnerability is successfully exploited, the worm instructs the target computer to download a copy of the worm from the host computer via HTTP protocol using the random port between 1024 and 10000 opened by the worm. The vulnerability is documented in Microsoft Security Bulletin MS08-067.

Network Shares with Weak Passwords
Worm:Win32/Conficker.B attempts to infect machines within the network.

It first attempts to drop a copy of itself in a target machine's ADMIN$ share using the credentials of the currently logged-on user.

If this method is unsuccessful, for example, the current user does not have the necessary rights, then it instead obtains a list of user accounts on the target machine. It then attempts to connect to the target machine using each user name and the following weak passwords:

123
1234
12345
123456

```
1234567
12345678
123456789
1234567890
123123
12321
123321
123abc
123qwe
123asd
1234abcd
1234qwer
1q2w3e
a1b2c3
admin
Admin
administrator
nimda
qwewq
qweewq
qwerty
qweasd
asdsa
asddsa
asdzxc
asdfgh
qweasdzxc
q1w2e3
qazwsx
qazwsxedc
zxcxz
zxccxz
zxcvb
zxcvbn
passwd
password
Password
login
Login
pass
mypass
mypassword
adminadmin
root
rootroot
test
testtest
temp
temptemp
foofoo
foobar
default
password1
password12
password123
admin1
```

admin12
admin123
pass1
pass12
pass123
root123
pw123
abc123
qwe123
test123
temp123
mypc123
home123
work123
boss123
love123
sample
example
internet
Internet
nopass
nopassword
nothing
ihavenopass
temporary
manager
business
oracle
lotus
database
backup
owner
computer
server
secret
super
share
superuser
supervisor
office
shadow
system
public
secure
security
desktop
changeme
codename
codeword
nobody
cluster
customer
exchange
explorer
campus
money

access

domain

letmein

letitbe

anything

unknown

monitor

windows

files

academia

account

student

freedom

forever

cookie

coffee

market

private

games

killer

controller

intranet

work

home

job

foo

web

file

sql

aaa

aaaa

aaaaa

qqq

qqqq

qqqqq

xxx

xxxx

xxxxx

zzz

zzzz

zzzzz

fuck

12

21

321

4321

54321

654321

7654321

87654321

987654321

0987654321

0

00

000

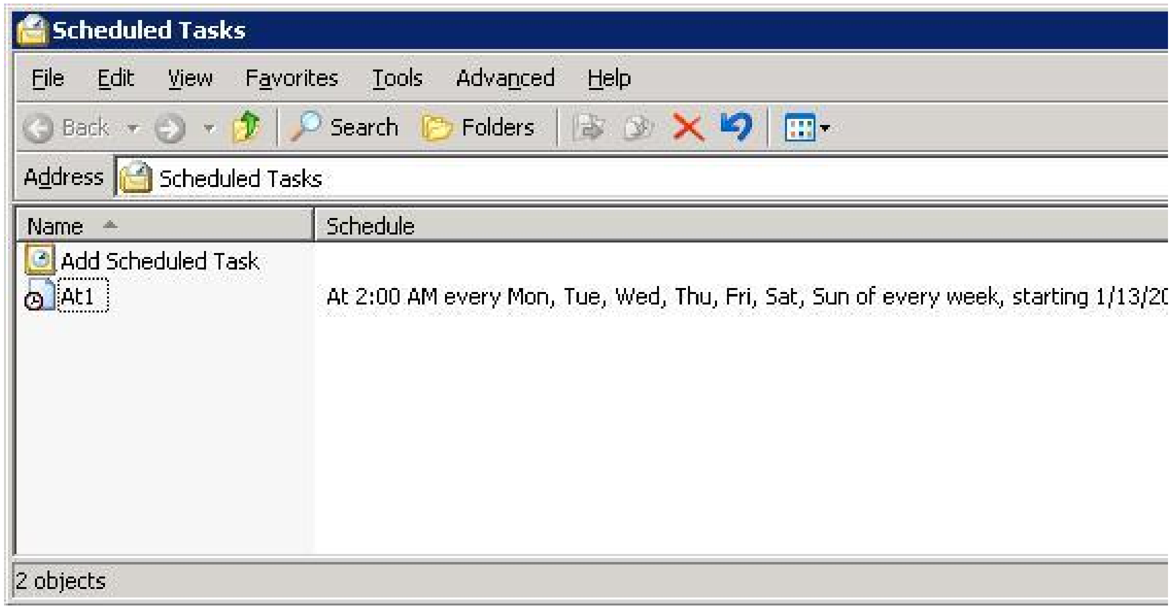
0000

```
00000
00000
0000000
00000000
1
11
111
1111
11111
111111
1111111
11111111
2
22
222
2222
22222
222222
2222222
22222222
3
33
333
3333
33333
333333
3333333
33333333
4
44
444
4444
44444
444444
4444444
44444444
5
55
555
5555
55555
555555
5555555
55555555
6
66
666
6666
66666
666666
6666666
66666666
7
77
777
7777
```

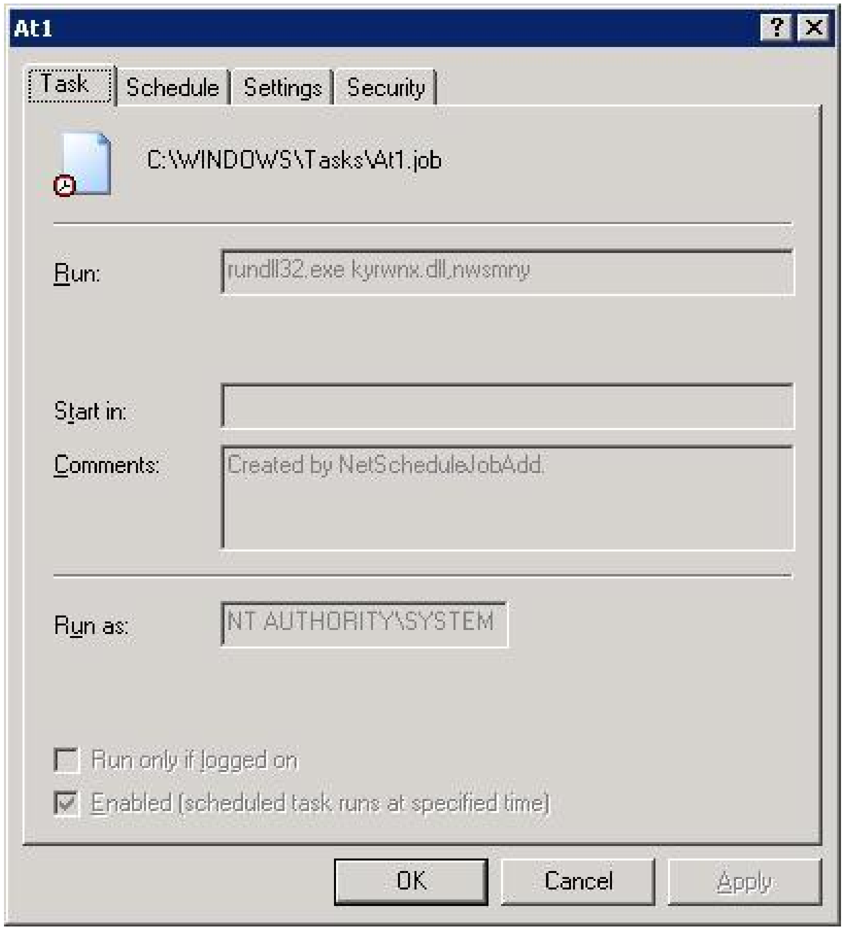
77777
777777
7777777
77777777
8
88
888
8888
88888
888888
8888888
88888888
9
99
999
9999
99999
999999
9999999
99999999

If Win32/Conficker successfully accesses the target machine, for example, if a combination of any of the obtained user names and one of the above passwords allows write privileges to the machine, then it copies itself to an accessible admin share as ADMIN$\System32\<*random letters*>.dll.

Creates Remote Scheduled Job
After compromising a machine remotely, Win32/Conficker.B creates a remote schedule job with the command “rundll32.exe <*malware file name*>.dll,<*malware parameters*>" to activate the copy, as shown in the images below:



Name	Schedule
Add Scheduled Task	
At1	At 2:00 AM every Mon, Tue, Wed, Thu, Fri, Sat, Sun of every week, starting 1/13/20



C:\WINDOWS\Tasks\At1.job

Run: rundll32.exe kyrwnx.dll,nwsmny

Start in:

Comments: Created by NetScheduleJobAdd.

Run as: NT AUTHORITY\SYSTEM

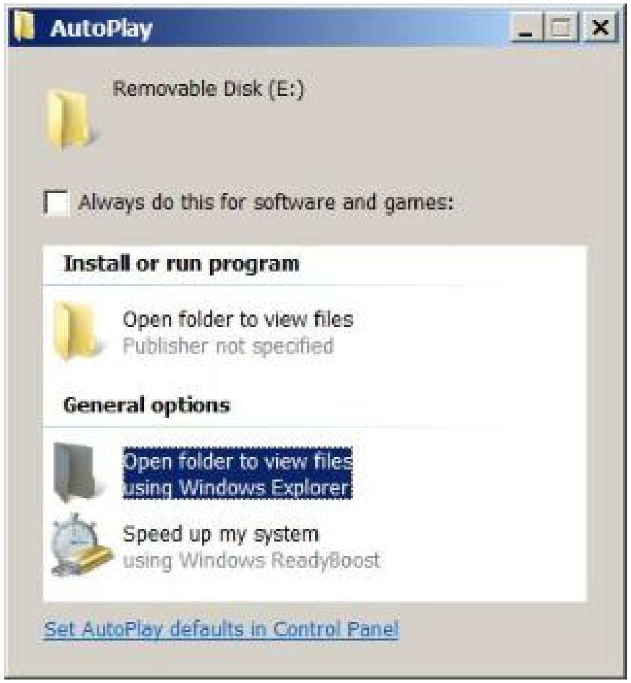
☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

Mapped and Removable Drives
Win32/Conficker may drop a copy of itself in all mapped and removable drives using a random file name. The worm creates a folder in the root of these drives named 'RECYCLER' (in Windows XP and previous versions, the folder "RECYCLER" references the "Recycle Bin"). Next, the worm copies itself as the following:

<*drive:*>\RECYCLER\S-%d-%d-%d-%d%d%d-%d%d%d-%d%d%d-%d\<*random letters*>.dll

Where %d is a randomly chosen letter. The worm also drops a corresponding *autorun.inf* file, which enables the worm copy to execute if the drive is accessed and Autoplay is enabled. The image below illustrates how a user could potentially launch the worm when accessing an infected share:



Note that the language in the first option suggests the user could 'open folder to view files' however the option is under 'Install or run program', an indication that opening the folder will actually execute an application. Another hint that the action is to execute the worm is the text 'Publisher not specified'. The highlighted choice under 'General options' in the image above would allow a user to view the share and not execute the worm copy.

Payload

Downloads Arbitrary Files
Win32/Conficker may construct a URL, according to the following pattern, to download files from:

http://<pseudo-random generated URL>/search?q=%d

The generated URL is based on the current system date. It uses one of the following top level domains:
.cc
.cn
.ws
.com
.net
.org
.info
.biz
For example, aaovt.com or aasmlhzbpqe.com.

Resets System Restore Point
The worm may call an API function to reset the computer's system restore point, potentially defeating

recovery using system restore.

Conficker.B performs the following additional payloads:

Modifies System Settings
Worm:Win32/Conficker.B changes system settings so that the user cannot view hidden files. It does this by modifying the following registry entry:

Adds value: "CheckedValue"
With data: "0"
To subkey: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL

It also modifies the system's TCP settings to allow a large number of simultaneous connections, where 0x00FFFFFE is hexadecimal and equals 16,777,214 decimal value:

Adds value: "TcpNumConnections"
With data: "0x00FFFFFE"
To subkey: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

The worm drops a temp file to aid restarting the TCP/IP service for the modification to take effect. The dropped file is detected as Trojan:WinNT/Conficker.B.

Disables TCP/IP Tuning, Terminates and Disables Services
Win32/Conficker.B disables Windows Vista TCP/IP auto-tuning by executing the following command:

netsh interface tcp set global autotuning=disabled
This worm terminates several important system services, such as the following:

- Windows Security Center Service (wscsvc) – notifies users of security settings (e.g. Windows update, Firewall and AntiVirus)
- Windows Update Auto Update Service (wuauserv)
- Background Intelligence Transfer Service (BITS) – used by Windows Update to download updates using idle network bandwidth
- Windows Defender (WinDefend)
- Error Reporting Service (ersvc) – sends error reports to Microsoft to help improve user experience
- Windows Error Reporting Service (wersvc)

Win32/Conficker.B deletes the registry key for Windows Defender, disabling it from running when the system starts.

Deletes value: "Windows Defender"
In subkey: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

It also disables any process that has a module name containing any of the following strings from sending network traffic or data (note that most of these strings are related to antivirus and security software, thus effectively disabling the products from acquiring signature updates, and possibly preventing users from accessing websites with these strings in the URL):
virus
spyware
malware

rootkit
defender
Microsoft
Symantec
Norton
mcafee
trendmicro
sophos
panda
etrust
networkassociates
computerassociates
f-secure
kaspersky
jotti
f-prot
nod32
eset
grisoft
drweb
centralcommand
ahnlab
esafe
avast
avira
quickheal
comodo
clamav
ewido
fortinet
gdata
hacksoft
hauri
ikarus
k7computing
norman
pctools
prevx
rising
securecomputing
sunbelt
emsisoft
arcabit
cpsecure
spamhaus
castlecops
threatexpert
wilderssecurity
windowsupdate

Win32/Conficker may contact one or more of the following remote sites for various purposes (including checking the affected machine’s geographic location and to verify that the system date is accurate):

getmyip.org
getmyip.co.uk
checkip.dyndns.org

baidu.com
google.com
yahoo.com
msn.com
ask.com
w3.org

Additional Information

The name of this threat was derived by selecting fragments of the domain 'traf**ficcon**vert**er**.biz', a string found in Worm:Win32/Conficker.A:

(fic)(con)(er) => (con)(fic)(+k)(er) => conficker

For more specific information regarding these worms, please see the following detailed variant descriptions elsewhere in our encyclopedia:
Worm:Win32/Conficker.A
Worm:Win32/Conficker.B

Analysis by Jireh Sanico and Joshua Phillips

Steps

Take the following steps to help prevent infection on your system:

- Enable a firewall on your computer.
- Get the latest computer updates for all your installed software, including Security Bulletin MS08-067.
- Use up-to-date antivirus software.
- Use caution when opening attachments and accepting file transfers.
- Use caution when clicking on links to web pages.
- Protect yourself against social engineering attacks.

Enable a firewall on your computer

Use a third-party firewall product or turn on the Microsoft Windows Internet Connection Firewall.
To turn on the Windows Firewall in Windows Vista

1. Click **Start**, and click **Control Panel**.
2. Click **Security**.
3. Click **Turn Windows Firewall on or off**.
4. Select **On**.
5.

Click **OK**.

To turn on the Internet Connection Firewall in Windows XP

1. Click **Start**, and click **Control Panel**.
2. Click **Network and Internet Connections**. If you do not see Network **and Internet Connections**, click **Switch to Category View**.
3. Click **Change Windows Firewall Settings**.
4. Select **On**.
5. Click **OK**.

Get the latest computer updates

Updates help protect your computer from viruses, worms, and other threats as they are discovered. It is important to install updates for all the software that is installed in your computer. These are usually available from vendor websites.

You can use the Automatic Updates feature in Windows to automatically download future Microsoft security updates while your computer is on and connected to the Internet.

To turn on Automatic Updates in Windows Vista

1. Click **Start**, and click **Control Panel**.
2. Click **System and Maintainance**.
3. Click **Windows Updates**.
4. Select a setting. Microsoft recommends selecting **Install updates automatically** and choose a time that is convenient for you. If you do not choose **Automatic**, but you choose to be notified when updates are ready, a notification balloon appears when new downloads are available to install. Click the notification balloon to review and install the updates.

To turn on Automatic Updates in Windows XP

1. Click **Start**, and click **Control Panel**.
2. Click **System**.
3. Click **Automatic Updates**.
4. Select a setting. Microsoft recommends selecting **Automatic**. If you do not choose **Automatic**, but you choose to be notified when updates are ready, a notification balloon appears when new downloads are available to install. Click the notification balloon to review and install the updates.

Use Strong Administrator Passwords

Microsoft also recommends that users ensure that their network passwords are strong to prevent this worm from spreading via weak administrator passwords. More information is available here.

Use up-to-date antivirus software

Most antivirus software can detect and prevent infection by known malicious software. To help protect you from infection, you should always run antivirus software that is updated with the latest signature files. Antivirus software is available from several sources. For more information, see http://www.microsoft.com/protect/computer/viruses/vista.mspx.

Use caution when opening attachments and accepting file transfers

Exercise caution with e-mail and attachments received from unknown sources, or received unexpectedly from known sources. Use extreme caution when accepting file transfers from known or unknown sources.

Use caution when clicking on links to web pages

Exercise caution with links to web pages that you receive from unknown sources, especially if the links are to a web page that you are not familiar with or are suspicious of. Malicious software may be installed in your system simply by visiting a web page with harmful content.

Avoid downloading pirated software

Threats may also be bundled with software and files that are available for download on various torrent sites. Downloading "cracked" or "pirated" software from these sites carries not only the risk of being infected with malware, but is also illegal. For more information. please see our article 'The risks of obtaining and using pirated software'.

Protect yourself from social engineering attacks

While attackers may attempt to exploit vulnerabilities in hardware or software in order to compromise a system, they also attempt to exploit vulnerabilities in human behavior in order to do the same. When an attacker attempts to take advantage of human behavior in order to persuade the affected user to perform an action of the attacker's choice, it is known as 'social engineering'. Essentially, social engineering is an attack against the human interface of the targeted system. For more information, please see our article 'What is social engineering?'.

Recovery Steps

Computers infected by this worm may be unable to connect to Web sites that provide scan and removal support, security product updates or general support. From a non-infected computer, users should view the following two articles provided in Microsoft Help and Support to assist in removal of Win32/Conficker:

http://support.microsoft.com/kb/962007 - Virus alert for Win32/Conficker.B and manual removal instructions
http://support.microsoft.com/kb/891716 - Deployment of MSRT in an enterprise environment