

W32/Conficker

Norman's green book



bbv icnb ifkshdof ysw784cngu ikngco
h jo iuthnu ihsd iuuqfuuchrh jnhodr tu5
x iuxgu4bcvut
i84iku4ytgu
watv7icgirhc iacshr i7des i848 iwormt
is jschzhgd8o iz8s3cyh87f z5f iu iyh6huw
iesaechr i3wchg ikchgkseru73ihchic
vyvb7y78csyu ihbguzf heyrg icgr ikbeg
y6u45hguea623vab2xu ixnuam33hc iu64
cygsduzx ifyug iw6739dherds ikwh48t4
kuyyg3kbyk64389b2b ikc jmuhiukhgthg
hgyru iv7eh7r iv74xjf7 ic jgbcf6hisqv
dwhufe i3rs37ychv **virus** ofc jaxkzu ixih
wbrcl k jmf s iv4bfweguywgeaugrb icanc
p9 jvghgn iomcugcsabe iwfbcoayt4980v
jocx7w9465fg isuyfgc iayrh3weuyt478
jkshgsyu isgiasgf i jfeoapohmcu4ioh7
siubcoac3yhroiutyf7 **trojan** bve8wioc
thnw7ovbh74673ih90hwbaosity7 iy475
wubgt3i478niugtiusau itisyguc jyuig
ncgt483ibcoisgncgsau iyf648cng iog2

Norman ASA is not liable for any form of loss or damage arising from use of the documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

The information in this document is subject to change without notice. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman ASA.

The Norman logo is a registered trademark of Norman ASA. Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

Copyright © 2009 Norman ASA.
All rights reserved.

Content

The W32/Conficker family	4
The aim	5
The origin	5
Installation	5
Information gathering.....	8
Spreading via the MS08-067 vulnerability	10
Spreading on local area network	12
Spreading to removable and remote drives.....	14
File download mechanism	15
Peer to peer updating mechanism.....	17
Blocking of antivirus domains via DNS	18
Disabling security-related services	20
Other features.....	21
Service name lists	21

The W32/Conficker family

W32/Conficker is a network-propagating worm family. To date, there are at least five major functional variants of Conficker, and at least two (probably more) minor functional variants. There are also many copies of each that are just repacked so as to make each file look differently. Thus naming of this virus can be confusing – some antivirus vendors will name according to major variant names (ex. Conficker.B), while other vendors including Norman will name according to which exact file was detected (ex. Conficker. JK).

This description will focus on functionality and use major variant names only, with the exception of the two minor variants that have not been given a separate name – they have been preliminarily named B2 and C2.

The worm's most interesting feature is that it spreads to other machines via a security vulnerability in the Windows Server Service. This vulnerability allows it to trigger a download of itself to the remote computer without the user's knowledge. This also caused a lot of interest in the security community when the A variant of the worm surfaced late November, 2008. Spreading via exploits can be dangerous, especially when the exploit is new, due to large numbers of unpatched computers.

Other functionality seems to move back and forth, is removed and put back in, as its creators see fit. Later variants employ a lot of obfuscation in order to make analysis difficult – for example,

It spreads
to other
machines
via a security
vulnerability in
the Windows
Server
Service.

a function can be broken up into ten different parts and spread out in different places in the program.

The aim

Conficker is now very updateable, so we can not be entirely sure of the motivation behind it. However, in the cases we have seen, the main motivation behind it is to make money – indirectly. The uses we have seen are:

- Installation of fake antivirus products that attempt to scare users into paying for an entirely nonfunctional application.
- Installation of a spam-sending worm.

The large amount of infected users makes it possible for the creators to “hire out” this network of computers for malicious purposes, like the ones mentioned above.

The origin

We do not know who the authors of this malware are or for certain where they are located. There can be a few hints found in the malware itself – f.ex. the A variant avoids infecting computers with Ukrainian keyboard.

Installation

When executed, the worm will copy itself as a randomly named DLL to a folder on the local hard disk. This will be in one of the folders below, in prioritized order:

The main motivation behind it is to make money – indirectly.

A variant:

[System]

B variants:

[System] or

[Program Files]\Internet Explorer folder or

[Program Files]\Movie Maker folder or

[Application Data] or

[Temp]

C, D and E variants:

[System] or

[Program Files]\Internet Explorer folder or

[Program Files]\Movie Maker folder or

[Program Files]\Windows Media Player or

[Program Files]\Windows NT or

[Application Data] or

[Temp]

[Folder] here means one of the standard folder locations in Windows. F.ex. [System] will often mean C:\WINDOWS\SYSTEM32.

It will then attempt to load this DLL into a running process by a technique known as DLL injection. Processes injected into are:

services.exe

svchost -k NetworkService

svchost -k netsvcs

explorer.exe

The A variant will only attempt to inject into services.exe, while the other variants will attempt the other processes as well, depending on circumstance.

50% chance
for each

25% chance
for each

In order to become active after boot up, the worm prefers to install itself as a service:

Installation of service in registry:

```
HKLM\System\CurrentControlSet\
Services\%random name%
"DisplayName"=%random name% [A] or
%composite name% [BCDE]
"Type"= 0x20
"Start"= 0x2
"ErrorControl"= 0
"ImagePath"="%SystemRoot%\system32\sv-
chost.exe -k netsvcs"
"ObjectName"="LocalSystem"
"Description"=%random service name%
HKLM\System\CurrentControlSet\Services\
[randomname]\Parameters "ServiceDll"=
%worm path%.
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SvcHost "netsvcs"=
%random name% appended to list
%composite name% refers to a name construct-
ed from several strings found in the worm. See
service name list.
```

If the service installation should fail for some reason, the worm installs using regular registry run keys:

```
HKCU\Software\Microsoft\Windows\Cur-
rentVersion\Run = rundll32.exe %worm path%
%random chars%
HKLM\Software\Microsoft\Windows\Cur-
rentVersion\Run = rundll32.exe %worm path%
%random chars%
```

Occasionally
the hosts file
can be over-
written.

The worm needs various information in order to function properly.

Information gathering

The worm needs various information in order to function properly. Some examples of this information is:

Current time:

Conficker connects to one or more of the sites below and interpretes the response in order to find time in GMT.

baidu.com	[ABCD]
google.com	[ABCD]
yahoo.com	[ABCD]
msn.com	[AB]
ask.com	[ABCD]
w3.org	[ABCD]
facebook.com	[CD]
imageshack.us	[CD]
rapidshare.com	[CD]



Own IP address:

The worm connects to one or more of the sites below and interpretes the response in order to find its own IP address. This is necessary to perform spreading via the MS08-067 exploit, thus it is found only in variants that spread this way.

http://getmyip.co.uk	[A]
http://checkip.dyndns.org	[AB]
http://www.whatismyip.org	[B]
http://www.whatsmyipaddress.com	[BE]
http://www.getmyip.org	[AB]
http://checkip.dyndns.com	[E]
http://www.myipaddress.com	[E]
http://www.findmyipaddress.com	[E]
http://www.ipaddressworld.com	[E]
http://www.findmyip.com	[E]
http://www.ipdragon.com	[E]

Network speed:

Conficker connects to one or more of the sites below and downloads the index.html file in order to calculate its own network speed.

aol.com	[BE]
cnn.com	[BE]
ebay.com	[BE]
msn.com	[BE]
myspace.com	[BE]

Spreading via the MS08-067 vulnerability [A,B,E]

Conficker generates random IP addresses, using the rand function, which it attempts to infect. These are heavily filtered – f.ex. the IP address ranges below are not attempted infected by the latest variants:

Conficker generates random IP addresses.

11.*.*	(US Department of Defense)
127.*.*	(Loopback)
169.254.*.*	(Link Local)
172.16.*.* - 172.32.*.*	(Private use networks)
192.*.*	(Reserved, and private use networks)
198.18.*.* - 198.19.*.*	(Network Interconnect Device Benchmark Testing)
224.*.* - 255.*.*	(Multicast, and reserved address space)

In addition, several variants the worm contain an address list of hundreds of additional IP address ranges it does not attempt to infect, and does not allow an infected machine to spread to. These IP address ranges typically belong to antivirus companies.

Conficker opens a HTTP server on a random port on the local machine, and then attacks the remote computer by sending a specially crafted packet to it. This causes vulnerable machines to connect back and download and execute a copy of the worm. If the download request does not match what the worm expects (flex. if the download client is wget, or reported operating system is Linux, or downloading IP is in one of the blocked address ranges), the data sent will not be the worm but randomly generated text.

The vulnerability that allows Conficker to do this is called MS08-067 or CVE-2008-4250, and is a problem with the Windows Server Service in a number of Windows versions where an RPC request would cause a buffer overflow during a NetpwwPathCanonicalize call.

See also

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>

The vulnerability is fixed in an update from Microsoft, and it is recommended that one makes sure it has been applied.

The vulnerability is fixed in an update from Microsoft.



Spreading on local area network [B variants only]

The virus spreads over the local area network. It sets up a thread which every 5 minutes enumerates the network using NetServerEnum, and attempts to create a connection to the IPC share on visible servers using

- logged on username and password
- remote (alternatively local) list of users, where password equals %username%
- remote (alternatively local) list of users, where password equals %username%username%
- remote (alternatively local) list of users, where password equals %emanresu% (username backwards)
- remote (alternatively local) list of users, where password is any one of the list below:

123	administrator	Password	admin12
1234	nimda	login	admin123
12345	qwewq	Login	pass1
123456	qweewq	pass	pass12
1234567	qwerty	mypass	pass123
12345678	qweasd	mypassword	root123
123456789	asdsa	adminadmin	pw123
1234567890	asddsa	root	abc123
123123	asdzxc	rootroot	qwe123
12321	asdfgh	test	test123
123321	qweasdzxc	testtest	temp123
123abc	q1w2e3	temp	mypc123
123qwe	qazwsx	temptemp	home123
123asd	qazwsxedc	foofoo	work123
1234abcd	zxcxz	foobar	boss123
1234qwer	zxccxz	default	love123
1q2w3e	zxcvb	password1	sample
a1b2c3	zxcvbn	password12	example
admin	passwd	password123	internet
Admin	password	admin1	Internet

nopass	monitor	7654321	4444444
nopassword	windows	87654321	44444444
nothing	files	987654321	5
ihavenopass	academia	0987654321	55
temporary	account	0	555
manager	student	00	5555
business	freedom	000	55555
oracle	forever	0000	555555
lotus	cookie	00000	5555555
database	coffee	00000	55555555
backup	market	0000000	6
owner	private	00000000	66
computer	games	1	666
server	killer	11	6666
secret	controller	111	66666
super	intranet	1111	666666
share	work	11111	6666666
superuser	home	111111	66666666
supervisor	job	1111111	7
office	foo	11111111	77
shadow	web	2	777
system	file	22	7777
public	sql	222	77777
secure	aaa	2222	777777
security	aaaa	22222	7777777
desktop	aaaaa	222222	77777777
changeme	qqq	2222222	8
codename	qqqq	22222222	88
codeword	qqqqq	3	888
nobody	xxx	33	8888
cluster	xxxx	333	88888
customer	xxxxx	3333	888888
exchange	zzz	33333	8888888
explorer	zzzz	333333	88888888
campus	zzzzz	3333333	9
money	fuck	33333333	99
access	12	4	999
domain	21	44	9999
letmein	321	444	99999
letitbe	4321	4444	999999
anything	54321	44444	9999999
unknown	654321	444444	99999999

It attempts to create a remote daily scheduled task, setting the worm up to be executed on the next whole hour.

If successful, the worm copies itself into the [\\%servername%\ADMIN\$\System32] folder of the remote computer using a random name. It then attempts to create a remote daily scheduled task, setting the worm up to be executed on the next whole hour. The task is defined as RUNDLL32.EXE %random worm name%,%random characters%

Spreading to removable and remote drives (USB sticks) [B variants only]

Some variations of Conficker scan logical drives and copy themselves to writable remote and removable drives (ex. USB sticks). The worm creates new folders on the drive(s) on the form [drive]:\RECYCLER\S-X-X-XX-XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXX-XXXX\filename].[ext] where X means a random digit (number of digits may also vary). This variation is selected 15 out of 16 times.

or



[drive]:\[random]\[random]\[filename].[ext]. This variation is used one out of 16 times.

A file named autorun.inf is created on the root folder of the drive in order to autoload the worm in many circumstances, typically when an infected removable drive is inserted and browsed to.

File download mechanism

The worm attempts to contact remote machines and download and execute files. Hostnames to contact are generated semi-randomly from the date; every day a new set of possible hostnames are generated from random characters and a list of domains.

Variants A and B: 250 domains generated daily.

Domains are selected from:

.cc	.net
.cn	.org
.ws	.info
.com	.biz

The A variant attempts to download and run a file from <http://trafficconverter.biz>. This file installed a fake antispyware program. However, the download link is no longer functional.

In addition, the A variant tries to download the GeoIP database <http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz>. This link is also no longer active, as the database has been moved elsewhere.

The worm attempts to contact remote machines and download and execute files.

Variants C and D: 50000 domains generated daily. Domains are selected from:

ac	co.za	com.pr	hk	my
ae	com.ag	com.pt	hn	nf
ag	com.ai	com.py	ht	nl
am	com.ar	com.sv	hu	no
as	com.bo	com.tr	ie	pe
at	com.br	com.tt	im	pk
be	com.bs	com.tw	in	pl
bo	com.co	com.ua	ir	ps
bz	com.do	com.uy	is	ro
ca	com.fj	com.ve	kn	ru
cd	com.gh	cx	kz	sc
ch	com.gl	cz	la	sg
cl	com.gt	dj	lc	sh
cn	com.hn	dk	li	sk
co.cr	com.jm	dm	lu	su
co.id	com.ki	ec	lv	tc
co.il	com.lc	es	ly	tj
co.ke	com.mt	fm	md	tl
co.kr	com.mx	fr	me	tn
co.nz	com.ng	gd	mn	to
co.ug	com.ni	gr	ms	tw
co.uk	com.pa	gs	mu	us
co.vi	com.pe	gy	mw	vc
				vn

Most of the time these domains are non-existent, but the worm author can at any time set up a download server that will work for a day.

Peer to peer updating mechanism [CDE]

Starting with the C variant, Conficker uses a peer-to-peer mechanism that enables infected machines to fetch updates from other infected machines. The worm opens a set of ports (two TCP and two UDP) on the infected machine. These ports are determined from the IP address and current date, so both client and server side are synchronized.

It connects to random IP addresses on the determined ports. If it finds an infected peer and there is an update available, this update is downloaded, decrypted and executed, provided that the digital signature is correct. All Conficker updates are verified by checking the file digital signature.

This update feature was used when the E variant of the worm was rolled out in April 2009.

Conficker uses a peer-to-peer mechanism that enables infected machines to fetch updates from other infected machines.



Blocking of antivirus domains via DNS

All Conficker variants except A hook the API's sendto (from ws2_32.dll) and DnsQuery_A, DnsQuery_UTF8, DnsQuery_W and Query_Main (from dnsapi.dll) in order to stop connections to sites containing the following strings:

B:

ahnlab	gdata	rootkit
arcabit	grisoft	securecomput-
avast	hacksoft	ing
avira	hauri	sophos
castlecops	ikarus	spamhaus
centralcommand	jotti	spyware
clamav	k7computing	sunbelt
comodo	kaspersky	symantec
computerassociates	malware	threatexpert
cpsecure	mcafee	trendmicro
defender	microsoft	virus
drweb	networkassociates	wilderssecurity
emsisoft	nod32	windowsupdate
esafe	norman	nai.
eset	norton	ca.
etrust	panda	avp.
ewido	pctools	avg.
f-prot	prevx	vet.
f-secure	quickheal	bit9.
fortinet	rising	sans.
		cert.

C1 (additional domain strings):

agnitum	freeav	secureworks
anti-	hackerwatch	technet
antivir	kido	threat
avgate	mirage	trojan
bothunter	msftncsi	virscan
ccollomb	msmvps	gmer.
conficker	mtc.sri	kav.
cyber-ta	onecare	llnw.
downad	ptsecurity	llnwd.
dslreports	removal	msdn.
free-av	safety.live	msft.

C2 (additional domain strings):

activescan
adware
mitre.
ms-mvp

D (additional domain strings):

av-sc
bdtools
enigma
precisecurity

E (additional domain strings):

coresecur	nmap.
doxpara	qualys
fsecure	secunia
honey	snort
insecure.	staysafe
iv.cs.uni	tenablese
ncircle	

Disabling security-related services

Starting with the B variant, Conficker worms attempt to stop and permanently disable a number of security-related services.

Services stopped in B1 (also known as B++):

BITS : Background Intelligent Transfer Service
wuauserv : Windows Update AutoUpdate Service

Additional services stopped in B2 (also known as B), C, D and E:

wscsvc : Windows Security Center Service
WinDefend : Windows Defender
ERSvc : Windows Error Reporting Service
WerSvc : Windows Error Reporting Service

Killing of security-related processes

Starting with the C variant, Conficker worms attempt to kill a number of security-related running processes. Processes containing the strings below are killed:

C1 (full list):

autoruns	hotfix	mrt.	scct_
avenger	kb890	mrtstub	sysclean
confick	kb958	ms08-06	tcpview
downad	kido	procexp	unlocker
filemon	klwk	procmon	wireshark
gmer	mbsa.	regmon	

C2 (additional): D (additional): E (additional):

stinger	bd_rem	dwndp
	cfremo	ms09
	kill	

Other features

- If on Windows Vista, the worm executes “netsh interface tcp set global autotuning=disabled” to turn off the Vista TCP/IP receive window autotuning, a feature that has been known to cause problems with many routers and firewalls.
- The B and E variants install a driver that patches TCPIP.SYS in such a way that the number of possible open connections is increased.

Service name lists

The text strings below are used to construct the name of the malicious service as it is displayed in the registry. Two different string pieces are randomly selected and joined together, f.ex. “Support Manager” or “Time Update”.

Service name substrings, B variant:

Boot	Image	Network	System
Center	Installer	Security	Task
Config	Manager	Server	Time
Driver	Microsoft	Shell	Universal
Helper	Monitor	Support	Update
			Windows

Service name substrings, C, D, and E variants:

Audit	Driver	Machine	Power	Time
Backup	Event	Management	Security	Trusted
Boot	Framework	Manager	Server	Universal
Browser	Hardware	Microsoft	Shell	Update
Center	Helper	Monitor	Storage	Windows
Component	Image	Network	Support	
Config	Installer	Notify	System	
Control	Logon	Policy	Task	
Discovery				



NORMAN[®]

www.norman.com