

Forum:[Hack Forums](#)

Thread: [\[warning\] Conficker.C start woking 1st april \[warning\]](#)

the gost - March 28, 2009, 4:14 am

? VIRUS DETAILS:Conficker.C

Win32/Conficker.C

Date Published:
11 Mar 2009

Last Updated:
11 Mar 2009

Threat Assessment

Overall Risk: Low

Wild: Low

Destructiveness: Medium

Pervasiveness: Medium

Characteristics

Type : Worm

Category : Win32

Also known as: Worm:Win32/Conficker.D (MS OneCare), W32/Confick-G (Sophos), Trojan.Win32.Pakes.ngs (Kaspersky)

Method of Infection?

When executed, Win32/Conficker.C drops a copy of itself using a random filename in the %System% directory. It may also drop copies of itself in the following directories:

%Program Files%\Windows NT
%Program Files%\Windows Media Player
%Program Files%\Internet Explorer
%Program Files%\Movie Maker

For these and other dropped files, Win32/Conficker.C:

- Sets Read Only, Hidden and System file attributes
- Generates a file creation/access time-stamp based on that of "kernel32.dll"
- Creates access control entries
- Exclusively locks the file, thus restricting access and privileges

Note: %System% and %Program Files% are variable locations. The malware determines the locations of these folders by querying the operating system. The default installation location for the System directory for Windows 2000 and NT is C:\Winnt\System32; for 95,98 and ME is C:\Windows\System; for XP and Vista is C:\Windows\System32. A typical location for the Program

Files folder would be C:\Program Files.

In order to automatically execute at each startup, it adds the registry entry below:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<random string> = "rundll32.exe <worm executable>, <random string>"

Conficker also registers a service with a random name created by combining a word from this list:

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

with another word from this list:

access
agent
auto
logon
man
mgmt
mon
prov
serv
Server
Service
Srv
srv
svc
Svc
System
Time

The worm also derives a display name for the service by combining two words from the list below:

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

For example, the worm may register a service with these registry entries:

```
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\DisplayName = "Component Task"
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\Type = 00000020
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\Start = 00000002
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc>ErrorControl = 00000000
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\ImagePath = "%Root%\system32\svchost.exe -k
netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\ObjectName = "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\Description = "<randomly copied from an
existing service with a Startup Type of 2 >"
HKLM\SYSTEM\CurrentControlSet\Services\IrSvc\Parameters\ServiceDll = "%System%\<worm
executable >"
```

[img]http://www.ca.com/us/securityadvisor/virusinfo/showimage.aspx?caid=77976&name=confickerc_newservice.gif[/img]

Note: %Root% is a variable location. The malware determines the location of the current root drive by querying the operating system. A typical location for the root drive would be C:\.

Additionally, Win32/Conficker.C checks for and tries to inject code into any processes executed with the commandline parameters "svchost.exe -k NetworkService".

Payload

Modifies Registry / Lowers Security Settings

Win32/Conficker.C deletes the following registry entry to deactivate Windows Security Center notifications:

HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\ShellServiceObjects\{FD6905CE-952F-41F1-9A6F-135D9C6622CC}

It deletes the registry entry below to prevent the operating system from starting in Safe Mode:

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot

Additionally, Win32/Conficker.C deletes the below registry entry to prevent "Windows Defender" from executing on system start:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Defender

Deletes Restore Points

Conficker resets all system restore points and deletes any saved system restore points on the affected system.

Disables Services

Win32/Conficker.C looks for and disables the following services if running:

wscsvc - Security Center

WinDefend – Windows Defender (available in Vista)

wuauclt - Automatic Updates

BITS - Background Intelligent Transfer Service

ERSvc - Error Reporting Service

WerSvc - Windows Error Reporting Service (available in Vista)

[img]http://www.ca.com/us/securityadvisor/virusinfo/showimage.aspx?caid=77976&name=confickerc_services.gif[/img]

Win32/Conficker.C terminates the following security-related processes in an attempt to prevent its removal from the system:

autoruns

avenger

confick

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

Blocks Websites

Win32/Conficker.C hooks the following APIs to monitor and restrict access to security websites:

Query_Main
DnsQuery_W
DnsQuery_UTF8
DnsQuery_A
sendto

In its attempt to prevent access to security-related sites for information, help or software updates, the worm attempts to block running applications from accessing URLs containing any of the following strings:

avg.
avp.
bit9.
ca.
cert.
gmer.
kav.
llnw.
llnwd.
msdn.
msft.
nai.
sans.
vet.
agnitum
ahnlab
anti-
antivir

arcabit
avast
avgate
avira
bothunter
castlecops
ccollomb
centralcommand
clamav
comodo
computerassociates
conficker
cpsecure
cyber-ta
db networkassociates
defender
drweb
dslreports
emsisoft
esafe
eset
etrust
ewido
f-prot
f-secure
fortinet
free-av
freeav
gdata
grisoft
hackerwatch
hacksoft
hauri
ikarus
jotti
k7computing
kaspersky
malware
mcafee
microsoft
mirage
msftncsi
msmvps
mtc.sri
nod32
norman
norton
onecare
panda
pctools
prevx
ptsecurity
quickheal

removal
rising
rootkit
safety.live
securecomputing
secureworks
sophos
spamhaus
spyware
sunbelt
symantec
technet
threat
threatexpert
trendmicro
trojan
virscan
virus
wilderssecurity
windowsupdate

Downloads and Executes Arbitrary Files

If the current system date is on or after 1 April 2009, the worm attempts to access pre-computed domain names to either download an updated copy of itself or download other malware. Below is a list of URL extensions used for pre-computed/generated URLs:

vn
vc
us
tw
to
tn
tl
tj
tc
su
sk
sh
sg
sc
ru
ro
ps
pl
pk
pe
no
nl
nf
my
mw
mu

ms
mn
me
md
ly
lv
lu
li
lc
la
kz
kn
is
ir
in
im
ie
hu
ht
hn
hk
gy
gs
gr
gd
fr
fm
es
ec
dm
dk
dj
cz
cx
com.ve
com.uy
com.ua
com.tw
com.tt
com.tr
com.sv
com.py
com.pt
com.pr
com.pe
com.pa
com.ni
com.ng
com.mx
com.mt
com.lc
com.ki
com.jm

com.hn
com.gt
com.gl
com.gh
com.fj
com.do
com.co
com.bs
com.br
com.bo
com.ar
com.ai
com.ag
co.za
co.vi
co.uk
co.ug
co.nz
co.kr
co.ke
co.il
co.id
co.cr
cn
cl
ch
cd
ca
bz
bo
be
at
as
am
ag
ae
ac

Martin66 - March 29, 2009, 6:59 am

Greate :)

Dude, im gonna thank you. maybe the Creator is in hackforums if he is.. i want my 250000 :D

æ?Ž\... - March 29, 2009, 7:03 am

Quote:Greate :)

Dude, im gonna thank you. maybe the Creator is in hackforums if he is.. i want my 250000 :D
I'm sure if he is, Omni will beat you to it.

Omerta - March 29, 2009, 8:26 am

Great, thanks for the info!:P

Vernes - March 29, 2009, 9:08 am

Which language can write Conficker.C ???

345138 - March 29, 2009, 10:18 am

I dont believe it.....

Really it sounds fakeeeeeeeee like who would do it on april 1st?

Idiot - March 29, 2009, 10:23 am

It was made on my birthday . . . damn

realman - March 29, 2009, 10:27 am

can u make it not affect ur computer is there a way???

Amaethon - March 29, 2009, 4:54 pm

(Mar 29, 2009 09:08 AM)Vernes Wrote: [\[CITE\]](#) Which language can write Conficker.C ???
Perl, I think

â™¥_%Heart%_â™¥ - March 29, 2009, 5:11 pm

Lots of info, thanks, but give credit to whichever resource you got it from.

sevenfold - March 29, 2009, 5:12 pm

Here is a free Conflicker removal tool from Enigma Software:

<http://www.enigmasoftware.com/a1/download/cfremover.exe>

It's on this page:

<http://www.enigmasoftware.com/products.php>

EDIT: Scan now! Luckily I don't have it! :D

yL. - March 29, 2009, 5:14 pm

They do it on april first because its fools day, they got fooled lol.

Afromike - March 29, 2009, 6:02 pm

This looks like its gonna do some serious sh!t... I hope avira updates their systems fast enough ?

`[Chaoz].Stein - March 29, 2009, 6:06 pm

Well i probably know that guy.

xD

345138 - March 29, 2009, 6:23 pm

Wrong section, but yeah, I saw something about it on TV.

yL. - March 29, 2009, 6:24 pm

Well just turn off your computer and unplug yor internet and you will not get it.

minidoc - April 3, 2009, 9:00 am

how gains conficker the rights to change these registry keys?