

Net-Worm.Win32.Kido.bt

<i>Detected</i>	Jan 02 2009 10:13 GMT
<i>Released</i>	Jan 02 2009 14:46 GMT
<i>Published</i>	Jan 13 2009 08:35 GMT

[Technical Details](#)

[Payload](#)

[Removal instructions](#)

Technical Details

This worm spreads via local networks and removable storage media. It is a PE DLL file. The components of the worm are between 155KB and 165KB in size. It is packed using UPX.

Installation

The worm copies its executable file to the Windows system directory as follows:

```
%System%\<rnd>.dll <rnd> is a string of random symbols
```

The worm creates a service to ensure it will be run each time Windows is launched on the victim machine. The following registry key is created:

```
[HKLM\SYSTEM\CurrentControlSet\Services\netsvcs]
```

The worm also modifies the following registry key value::

```
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost]  
"netsvcs" = "<original value> %System%\<rnd>.dll"
```

Network spreading

When infecting a computer, the worm launches an HTTP server on a random TCP port. This is then used to load the worm's executable file to other computers.

The worm gets the IP addresses of computers in the same network as the victim machine and attacks them via a buffer overrun vulnerability in the Server service. (More details about this vulnerability can be found on the Microsoft site: www.microsoft.com).

The worm sends a specially crafted RPC request to remote machines, which causes a buffer overrun when the `wscopy_s` function is called in `netapi32.dll`. This launches code which downloads the worm file, launches and installs it on the new victim machine.

In order to exploit the vulnerability described above, the worm attempts to connect to the Administrator account on the remote machine. The worm uses the following passwords to brute force the account:

99999999	fuck
9999999	zzzzz
999999	zzzz
99999	zzz
9999	xxxxx
999	xxxx
99	xxx
9	qqqqq
88888888	qqqq
8888888	qqq
888888	aaaaa
88888	aaaa
8888	aaa
888	sql
88	file
8	web
77777777	foo
7777777	job
777777	home
77777	work
7777	intranet
777	controller
77	killer
7	games
66666666	private
6666666	market
666666	coffee
66666	cookie
6666	forever
666	freedom
66	student
6	account
55555555	academia
5555555	files
555555	windows
55555	monitor
5555	unknown
555	anything
55	letitbe
5	letmein
44444444	domain
4444444	access
444444	money
44444	campus
4444	explorer
444	exchange
44	customer
4	cluster
33333333	nobody
3333333	codeword
333333	codename
33333	changeme
3333	desktop
333	security

33	secure
3	public
22222222	system
2222222	shadow
222222	office
22222	supervisor
2222	superuser
222	share
22	adminadmin
2	mypassword
11111111	mypass
1111111	pass
111111	Login
11111	login
1111	Password
111	password
11	passwd
1	zxcvbn
00000000	zxcvb
0000000	zxccxz
00000	zxcxz
0000	qazwsxedc
000	qazwsx
00	q1w2e3
0987654321	qweasdzxc
987654321	asdfgh
87654321	asdzc
7654321	asdds
654321	asdsa
54321	qweasd
4321	qwerty
321	qweewq
21	qwewq
12	nimda
super	administrator
secret	Admin
server	admin
computer	alb2c3
owner	1q2w3e
backup	1234qwer
database	1234abcd
lotus	123asd
oracle	123qwe
business	123abc
manager	123321
temporary	12321
ihavenopass	123123
nothing	1234567890
nopassword	123456789
nopass	12345678
Internet	1234567
internet	123456
example	12345
sample	1234

```
love123          123
boss123
work123
home123
mypc123
temp123
test123
qwe123
abc123
pw123
root123
pass123
pass12
pass1
admin123
admin12
admin1
password123
password12
password1
default
foobar
foofoo
temptemp
temp
testtest
test
rootroot
root
```

Spreading via removable storage media

The worm copies its executable file as follows:

```
<X>:\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\<rnd>.vmsx rnd is
a string of random lower case symbols; X is the disk.
```

The worm also places the following file in the root of each disk:

```
<X>:\autorun.inf
```

This ensures the worm's executable file will be run each time the user opens the infected disk using Windows Explorer.

Payload

When launching, the worm injects its code into the address space of one of the "svchost.exe" system processes. This code is responsible for the worm's malicious payload:

- Disables system restore
- Blocks addresses which contain the following strings:

```
indowsupdate
wilderssecurity
threatexpert
```

castlecoops
spamhaus
cpsecure
arcabit
emsisoft
sunbelt
securecomputing
rising
prevx
pctools
norman
k7computing
ikarus
hauri
hacksoft
gdata
fortinet
ewido
clamav
comodo
quickheal
avira
avast
esafe
ahnlab
centralcommand
drweb
grisoft
eset
nod32
f-prot
jotti
kaspersky
f-secure
computerassociates
networkassociates
etrust
panda
sophos
trendmicro
mcafee
norton
symantec
microsoft
defender
rootkit
malware
spyware
virus

The worm also downloads a file from the link shown below:

http://trafficconverter.biz/*****/antispysware/loadadv.exe

This file is saved to the Windows system directory and then launched for execution. The link
securelist.com/.../Net-Worm.Win32.Kid...

was not live at the time of writing.

The worm may also download files from links of the type shown below:

```
http://<URL>/search?q=<%rnd2%>
```

rnd2 is a random number. URL is a link formed by a special algorithm which uses the current date. The worm gets the current date from one of the sites listed below:

```
http://www.w3.org  
http://www.ask.com  
http://www.msn.com  
http://www.yahoo.com  
http://www.google.com  
http://www.baidu.com
```

Files downloaded by the worm are saved to the Windows system directory with their original name.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, you can either use a special removal tool, which can be found here support.kaspersky.com or follow the instructions below:

1. Delete the **system registry** key shown below:

```
[HKLM\SYSTEM\CurrentControlSet\Services\netsvcs]
```

2. Delete "%System%\<rnd>.dll" from the system registry key parameter shown below:

```
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost] "netsvcs"
```

3. Reboot the computer.

4. Delete the original worm file (the location will depend on how the malicious program penetrated the computer).

5. Delete the file shown below:

```
%System%\<rnd>.dll <rnd> is a string of random symbols
```

6. Delete the following files from all removable storage media:

```
<X>:\autorun.inf <X>:\RECYCLER\S-5-3-42-2819952290-8240758988-
```

```
879315005-3665\<rnd>.vmx rnd is a string of random lower case symbols; X is the disk.
```

7. Download and install operating system updates from the following link:

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

8. Update your antivirus databases and perform a full scan of the computer ([download](#) a trial version of Kaspersky Anti-Virus).

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

Industry-leading Antivirus Software.

Registered trademarks and service marks are the property of their respective owners.

