SECURELIST

Net-Worm.Win32.Kido.bt

Detected	Jan 02 2009 10:13 GMT
Released	Jan 02 2009 14:46 GMT
Published	Jan 13 2009 08:35 GMT

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 wcscpy_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
9999999
999999
99999
9999
999
99
9
88888888
8888888
888888
88888
8888
888
88
8
77777777
7777777
777777
77777
7777
777
77
7
66666666
6666666
666666
66666
6666
666
66
6
55555555
5555555
555555
55555
5555
555
55
5
44444444
4444444
444444
44444
4444
444
44
4
33333333
3333333
333333
33333
3333
333
```

```
fuck
zzzzz
zzzz
zzz
xxxxx
xxxx
xxx
qqqqq
qqqq
qqq
aaaaa
aaaa
aaa
sql
file
web
foo
job
home
work
intranet
controller
killer
games
private
market
coffee
cookie
forever
freedom
student
account
academia
files
windows
monitor
unknown
anything
letitbe
letmein
domain
access
money
campus
explorer
exchange
customer
cluster
nobody
codeword
codename
changeme
desktop
security
```

```
33
3
22222222
2222222
222222
22222
2222
222
22
2
11111111
1111111
111111
11111
1111
111
11
1
00000000
0000000
00000
0000
000
00
0987654321
987654321
87654321
7654321
654321
54321
4321
321
21
12
super
secret
server
computer
owner
backup
database
lotus
oracle
business
manager
temporary
ihavenopass
nothing
nopassword
nopass
Internet
internet
example
sample
secure
public
system
shadow
office
supervisor
superuser
share
adminadmin
mypassword
mypass
pass
Login
login
Password
password
passwd
zxcvbn
zxcvb
zxccxz
zxcxz
qazwsxedc
qazwsx
q1w2e3
qweasdzxc
asdfgh
asdzxc
asddsa
asdsa
qweasd
qwerty
qweewq
qwewq
nimda
administrator
Admin
admin
a1b2c3
1q2w3e
1234qwer
1234abcd
123asd
123qwe
123abc
123321
12321
123123
1234567890
123456789
12345678
1234567
123456
12345
1234
```

```
love123
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
```

```
123
```

Spreading via removable storage media

The worm copies its executable file as follows:

`<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.

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
```

```
castlecops
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/*****/antispyware/loadadv.exe
```

This file is saved to the Windows system directory and then launched for execution. The link

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.mspx`
8. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus.