How to kill Net-Worm.Win32.Kido virus

Kaspersky Lab Vietnam Technical Support team received a lot of announcements about the increasing infection in the enterprise network of the Net-Worm.Win32.Kido deep line. Here are some descriptions of this deep line and how to kill it.

Kaspersky Lab Vietnam Technical Support team received a lot of announcements about the increasing infection in the enterprise network of the*Net-Worm.Win32.Kido*deep line.Here are some descriptions of this deep line and how to kill it .

The symptoms of the network are infected with Kido virus

1. Network traffic increases dramatically if there are infected computers in the network, because the network is attacked from these computers.

2. Anti-Virus programs with an IDS (Intrusion Detection System) appear to be attacked by *Intrusion.Win.NETAPI.buffer-overflow.exploit*

Short description of the Net-Worm.Win32.Kido virus line

1. It creates files **autorun.inf** and **RECYCLED {SID} RANDOM_NAME.vmx** in portable hard drives (USB Flash) and sometimes in corporate networks.

2. It stores itself into the system as a DLL file with any name (eg *c: windowssystem32zorizr.dll*).

3. It registers itself and the computer's service system with any name (eg *knqdgsm*).

4. It tries to attack computers via 445 or 139 TCP ports, using MS Windows vulnerability MS08-067 security error.

5. It tries to connect to some of the following websites (we recommend setting up a network firewall to monitor connections to these websites):

http://www.getmyip.org
http://getmyip.co.uk
http://www.whatsmyipaddress.com
http://www.whatismyip.org
http://checkip.dyndns.org
http://schemas.xmlsoap.org/soap/envelope/
http://schemas.xmlsoap.org/soap/encoding/

http://schemas.xmlsoap.org/soap/envelope/
http://schemas.xmlsoap.org/soap/encoding/
http://trafficconverter.biz/4vir/antispyware/loadadv.exe
http://trafficconverter.biz
http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz

These methods of killing viruses

Customers should use a special tool, kidokiller.exe, to remove this virus.

To prevent all servers and servers from being infected with this worm, you should do the following:

1. Install the latest version and bug from Microsoft for vulnerabilities MS08-067, MS08-068, MS09-001.
2. Make sure that the Local Administrator account's password is hard to find and easily hacked - the password should include at least 6 characters; use a mix of lowercase, uppercase, numbers and special characters (such as #,!, $, @ .).
3. Turn off the auto-run feature from removable drives.

The tool kidokiller.exe can be run directly on an infected computer, or remotely with the help of Kaspersky Administration Kit.

To remove the virus directly on the infected machine

1. Download the compressed file **KidoKiller_v3.3.2.zip** and extract it to a folder on the infected computer.

2. Run the file **KidoKiller.exe**

When the scan will appear many command line windows, press any button to minimize the window. For the command line to close automatically, you should run the tool KidoKiller.exe with the parameter **-y** .

3. Wait until the scan is complete.

If **Agnitum Outpost Firewall** is installed on the infected machine, it is required to restart the computer every time the tool is done.

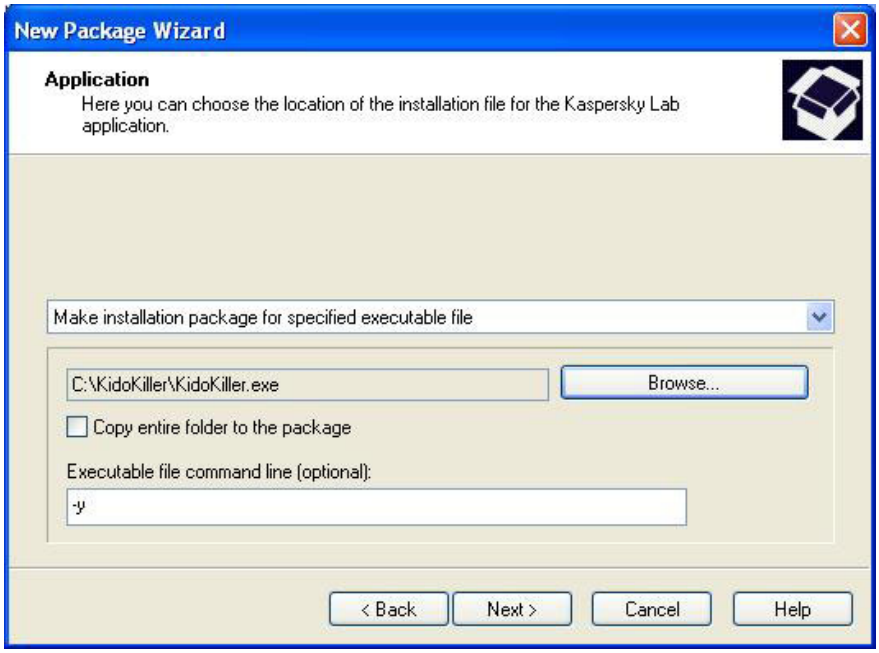
4. Conduct a comprehensive scan of your computer with Kaspersky Anti-Virus

To remove the virus via the Administration Kit

1. Download the compressed file **KidoKiller_v3.3.2.zip** and extract it to a folder.

2. In Administration Kit console create installation package for application **KidoKiller.exe** . In the configuration **installation package** on the step **Application** select **Make installation package for specified executable file** .

In the **Executable file command line (optional) field** specify the **-y** parameter to close the console window automatically whenever the tool is done.



3. Create a **global** or **task group for remote installation** of the **installation** package to assign to computers and run the task.

The **KidoKiller.exe** tool can run on all computers on the network in the form of running tasks.

4. After each tool has finished, scan each computer for the network using Kaspersky Anti-Virus

If **Agnitum Outpost Firewall** is installed on the infected machine, it is required to restart the computer every time the tool is done.

For more information about this tool, run KidoKiller.exe with parameters **–help** .

Parameters manage KidoKiller.exe from the command line

1. **-p** - scan a defined folder
2. **-f** - scan the hard drive
3. **-n** - scan the network drive
4. **-r** - scan the removable drive
5. **-y** - end the program without pressing any key
6. **-s** - silent mode (does not display black screen window)
7. **-l** - write to a log file
8. **-v** - extended log maintenance (should be used with the -l parameter)
9. **-help** - display additional information about the tool

For example, in the case of scanning a removable disk and recording the report into a **report.txt** file (it will be created in the installation directory of KidoKiller.exe), use the following command:

```
kidokiller.exe -r -y -l report.txt -v
```