News | VirusBlokAda

Modules of current malware were first time detected by "VirusBlokAda" company specialists on the **17th of June, 2010** and were added to the anti-virus bases as **Trojan-Spy.0485** and **Malware-Cryptor.Win32.Inject.gen.2**. During the analysis of malware there was revealed that it uses USB storage device for propagation.

You should take into consideration that virus infects Operation System in unusual way through vulnerability in processing lnk-files (without usage of autorun.inf file).

So you just have to open infected USB storage device using Microsoft Explorer or any other file manager which can display icons (for i.e. Total Commander) to infect your Operating System and allow execution of the malware.

Malware installs two drivers: mrxnet.sys and mrxcls.sys. They are used to inject code into systems processes and hide malware itself. That's the reason why you can't see malware files on the infected USB storage device. We have added those drivers to anti-virus bases as **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2**. Note that both drivers are signed with digital signature of Realtek Semiconductor Corp. (www.realtek.com).

Thus, current malware should be added to very dangerous category causes the risk of the virus epidemic at the current moment.

After we have added a new records to the anti-virus bases we are admitting a lot of detections of **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2** all over the world.