Cybercriminals switch from MBR to NTFS

By Vyacheslav Zakorzhevsky

Published: 2011-07-06 · Archived: 2026-04-06 00:13:29 UTC

Research

Research

06 Jul 2011

2 minute read

Expert

- Vyacheslav Zakorzhevsky

Modification of the hard drive areas responsible for the initial loading of the system has become increasing popular with cybercriminals. Moreover, cybercriminals have now moved on from just modifying the MBR (master boot record) to infecting the code of the NTFS loader.

We recently discovered an interesting piece of malware — Cidox. It is peculiar in that it infects the load area code of the boot partition on the hard drive.

The master file Trojan-Dropper.Win32.Cidox “carries on board” two driver rootkits (Rootkit.Win32/Win64.Cidox). One is compiled for 32-bit platforms, the other for 64-bit platforms.

The source component of Cidox makes the following modifications to the beginning of the hard drive:

- Saves the relevant driver to free sectors at the beginning of the hard drive;
- It chooses the section marked as the boot partition in the MBR partition table for infection. It is important to note that it only infects partitions with the NTFS file system.
- Writes part of its code over Extended NTFS IPL (Initial Program Loader), which is responsible for parsing the MFT table (Master File Table), searching for the file with the loader in the root directory of the section (ntldr — pre-Vista, bootmgr — Vista+), reading this file form the disk and transferring control to it. At the same time the original contents of Extended NTFS IPL are encrypted, saved and added to the end of the malicious code.

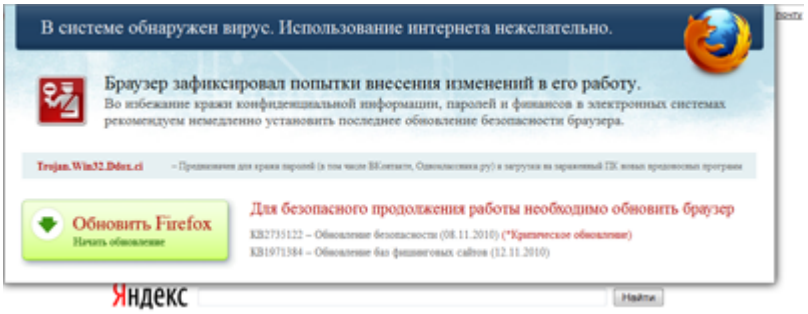
Fragment of the initial domain of the hard drive infected by Cidox (detected as Rootkit.Boot.Cidox)

The next time the system is booted the malicious code in the load area will be invoked. With the help of a known technique, use of the Int 13h interrupt and some Windows kernel features it successfully loads the malicious driver to the system. The loaded driver uses PsSetCreateProcessNotifyRoutine to control the launch of the following processes:

- svchost.exe
- iexplore.exe
- firefox.exe
- opera.exe
- chrome.exe

Fragment of Rootkit.Win32.Cidox containing strings with the names of controlled browsers

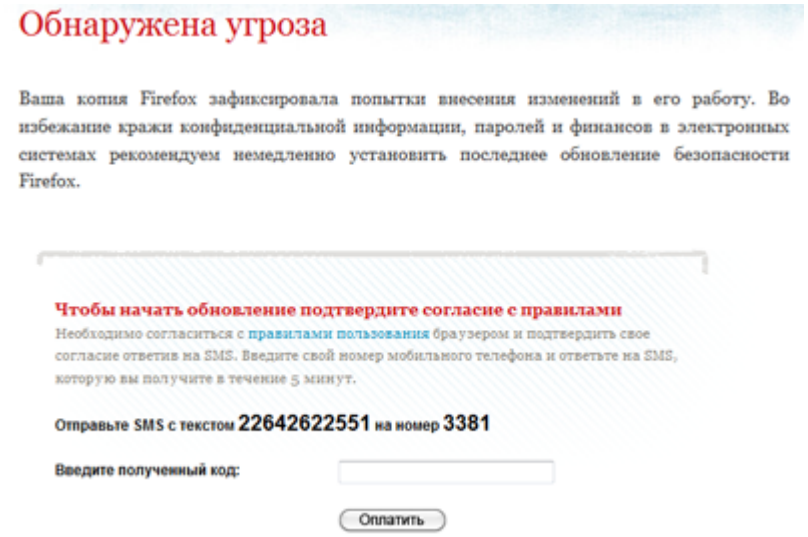
If the launch of one of the processes above is detected, one more Cidox component is integrated into it — a dynamic library (Trojan.Win32.Cidox). This library modifies any browser output, substituting it with its own. As a result, the user sees a browser window displaying an offer to renew the browser due to some malicious programs allegedly detected on the system. The example below tells the user to renew the browser due to infection by Trojan.Win32.Ddox.ci.



Fragment of a browser window on a system infected by Cidox

Of course, the user is asked to pay for the ‘renewal’. In order to obtain it, an SMS has to be sent to a short number.

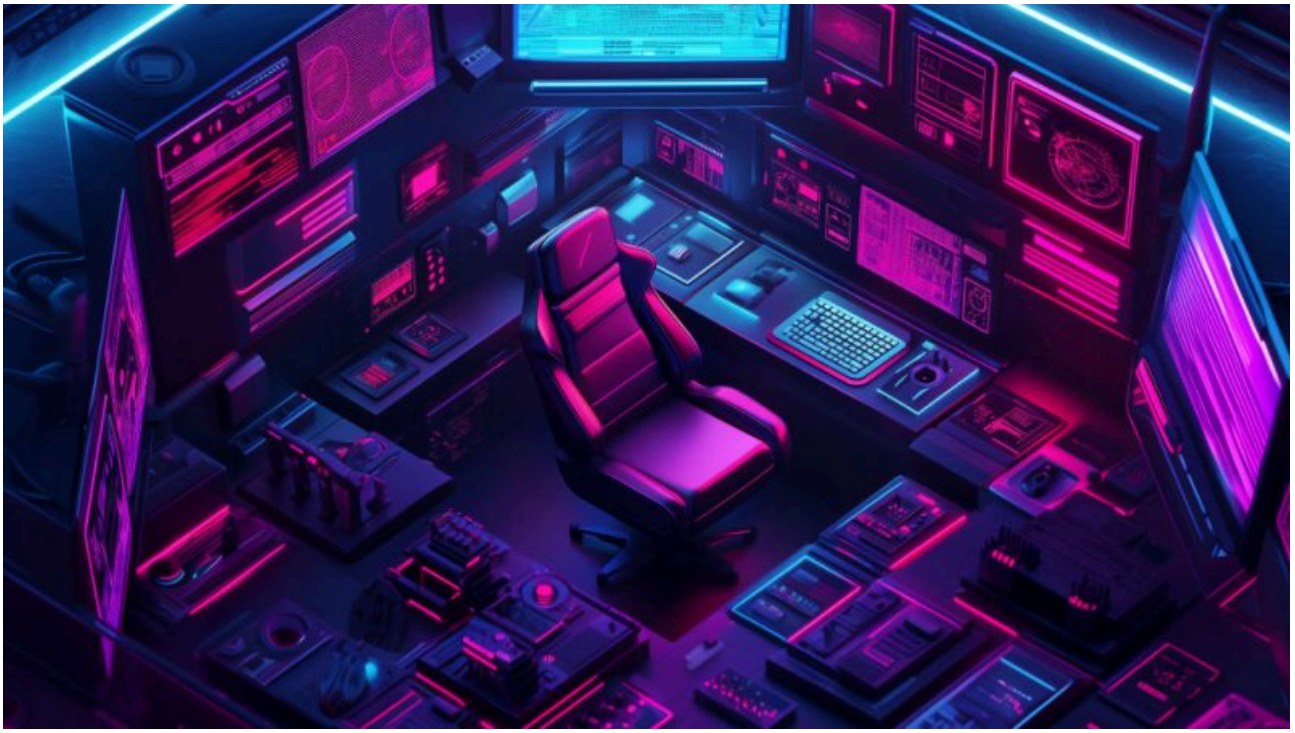
A unique page design is used for each of the most popular browsers.

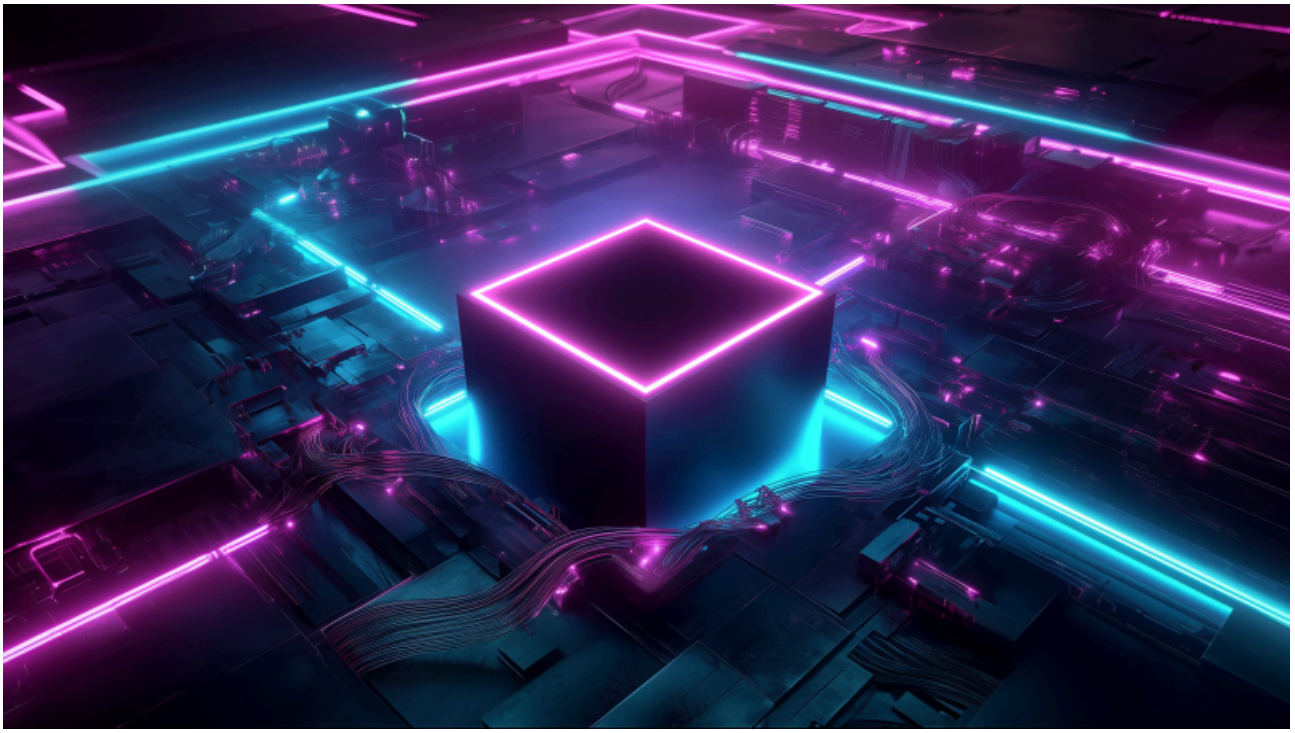


Fragment of a browser window on a system infected by Cidox

It should be noted that new versions of browsers can in fact be downloaded free of charge from the vendor's website. Cybercriminals are merely scaring users in order to extort money from them.

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
