

# Cybercriminals switch from MBR to NTFS

---

SL [securelist.com/cybercriminals-switch-from-mbr-to-ntfs-2/29117/](http://securelist.com/cybercriminals-switch-from-mbr-to-ntfs-2/29117/)



Research

Research

06 Jul 2011

minute read



Authors

**Expert**

Vyacheslav Zakorzhevsky

Modification of the hard drive areas responsible for the initial loading of the system has become increasingly 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 from 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)*

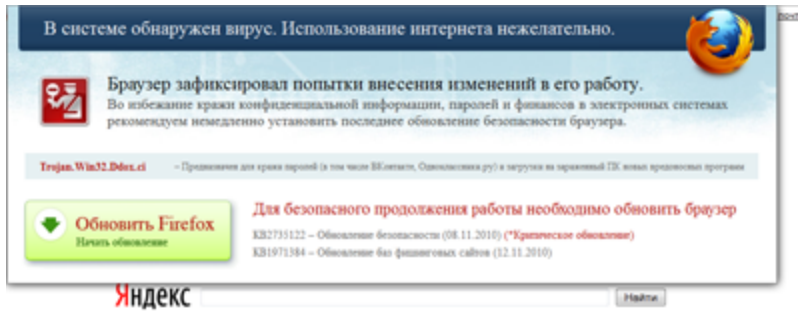
The next time the system is booted the malicious code in the load area will be invoked. With the help of a known technique, use of the Int 13h interrupt and some Windows kernel features it successfully loads the malicious driver to the system. The loaded driver uses PsSetCreateProcessNotifyRoutine to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

### Обнаружена угроза

Ваша копия Firefox зафиксировала попытки внесения изменений в его работу. Во избежание кражи конфиденциальной информации, паролей и финансов в электронных системах рекомендуем немедленно установить последнее обновление безопасности Firefox.

**Чтобы начать обновление подтвердите согласие с правилами**  
Необходимо согласиться с [правилами пользования](#) браузером и подтвердить свое согласие ответив на SMS. Введите свой номер мобильного телефона и ответьте на SMS, которую вы получите в течение 5 минут.

Отправьте SMS с текстом **22642622551** на номер **3381**

Введите полученный код:

*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.

- [Malware Technologies](#)
- [MBR](#)
- [Rootkits](#)
- [Trojan-Dropper](#)

Authors

**Expert**

Vyacheslav Zakorzhevsky.

Cybercriminals switch from MBR to NTFS

---

Your email address will not be published. Required fields are marked \*

GReAT webinars

13 May 2021, 1:00pm

### **GReAT Ideas. Balalaika Edition**

---

26 Feb 2021, 12:00pm

17 Jun 2020, 1:00pm

26 Aug 2020, 2:00pm

22 Jul 2020, 2:00pm

From the same authors



### **How Security Products are Tested – Part 1**

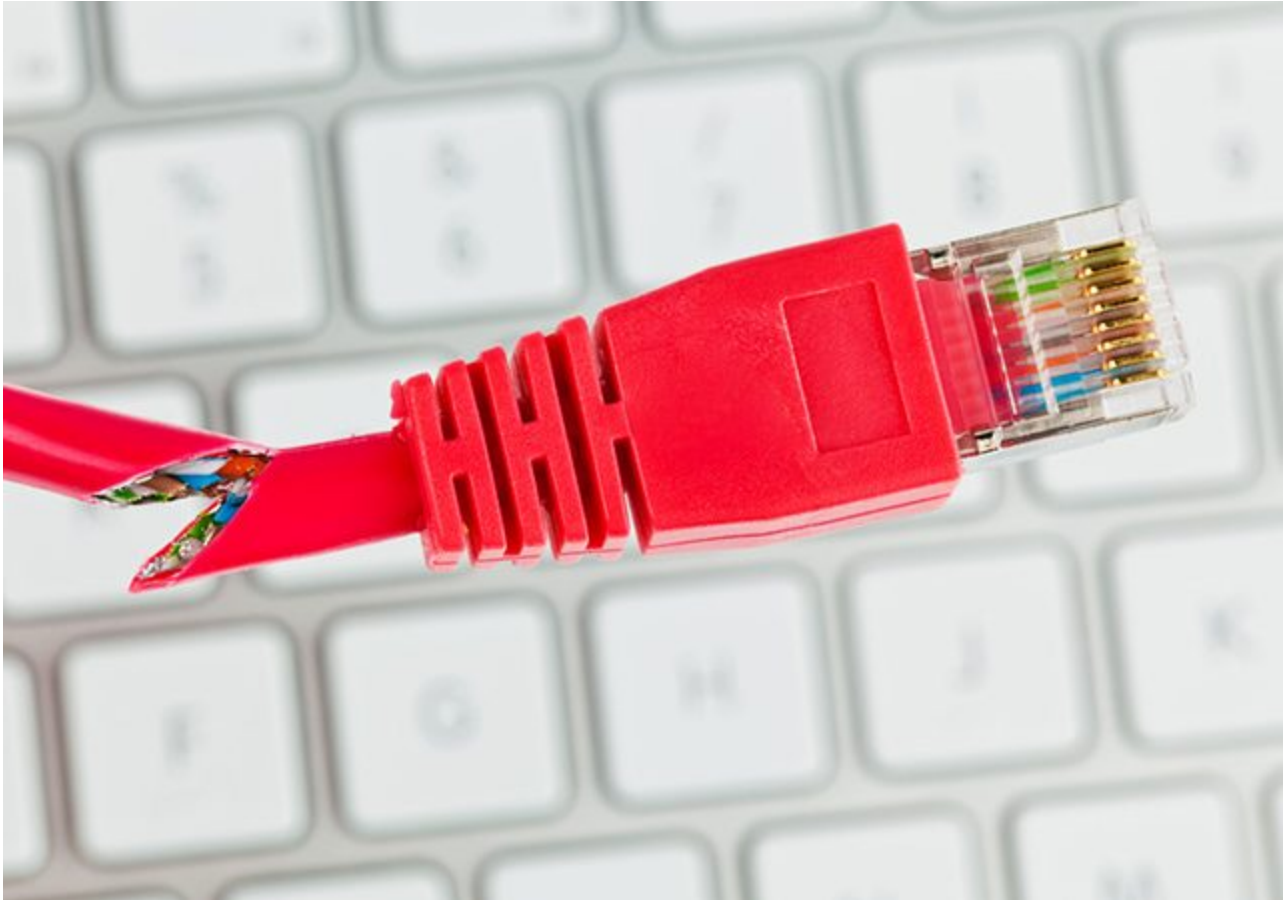
---



**You can't be invulnerable, but you can be well protected**

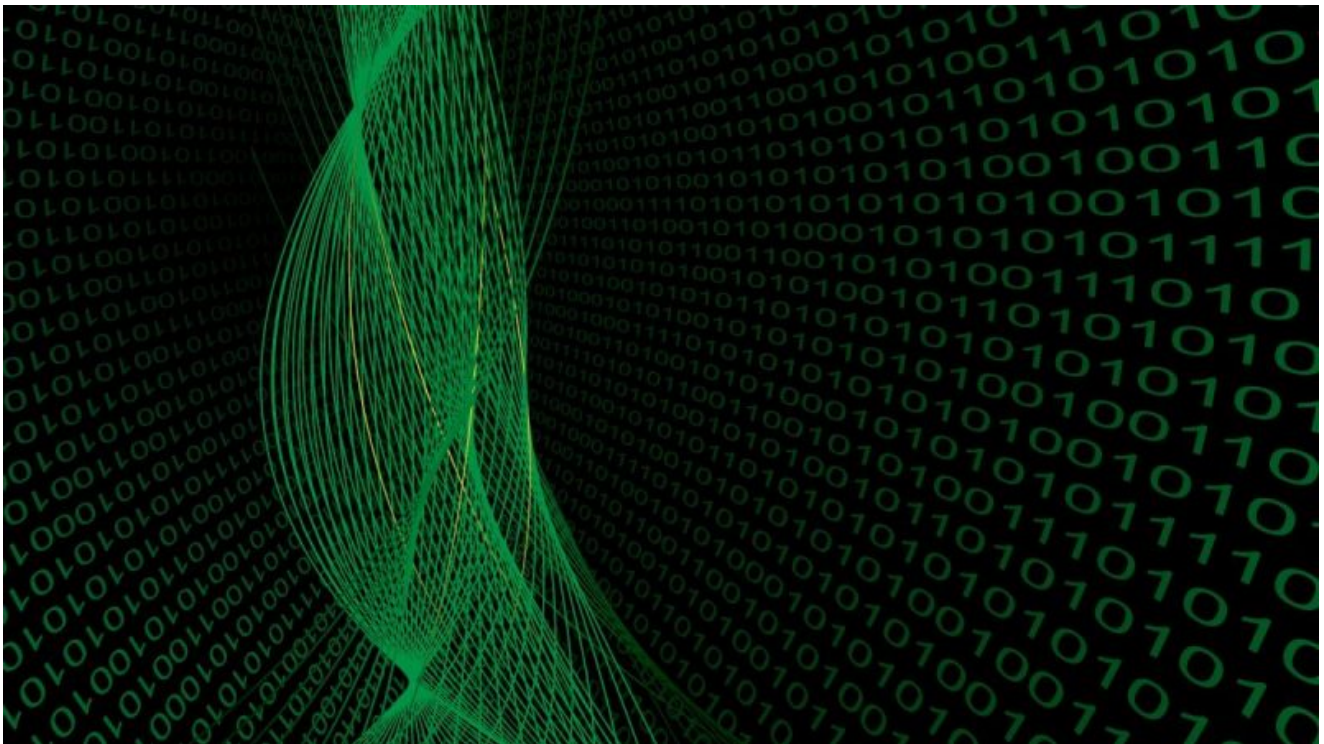


**New Flash Player 0-day (CVE-2014-0515) Used in Watering-hole Attacks**



**CVE-2014-0497 – A 0-day Vulnerability**

---



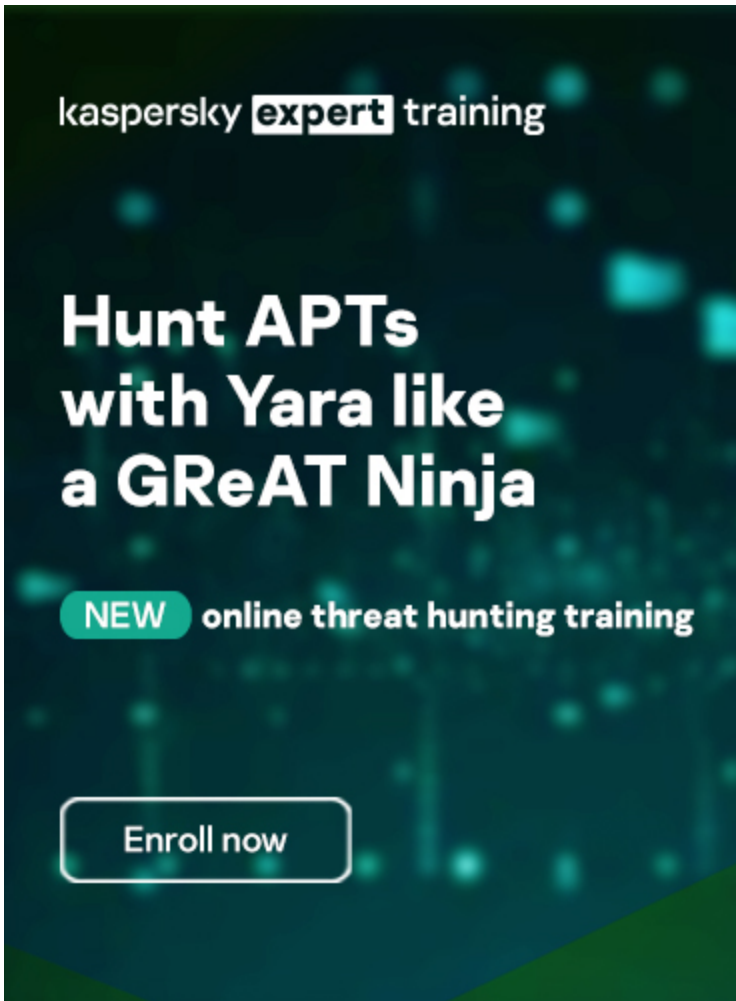
**Loophole in Safari**

---

Subscribe to our weekly e-mails

The hottest research right in your inbox

- 
- 
- 
- 



Reports

### **APT trends report Q1 2022**

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

### **Lazarus Trojanized DeFi app for delivering malware**



We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

## **MoonBounce: the dark side of UEFI firmware**

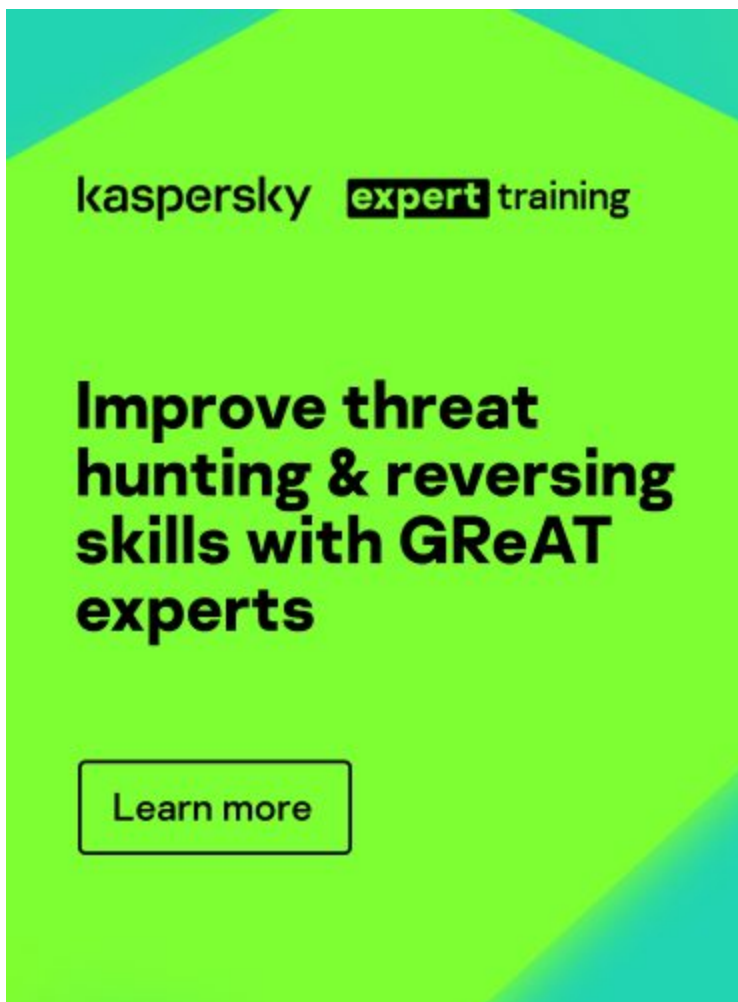
---

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

## **The BlueNoroff cryptocurrency hunt is still on**

---

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.



Subscribe to our weekly e-mails

The hottest research right in your inbox

- 
-

•

kaspersky **expert** training

**Improve threat  
hunting & reversing  
skills with GReAT  
experts**

[Learn more](#)