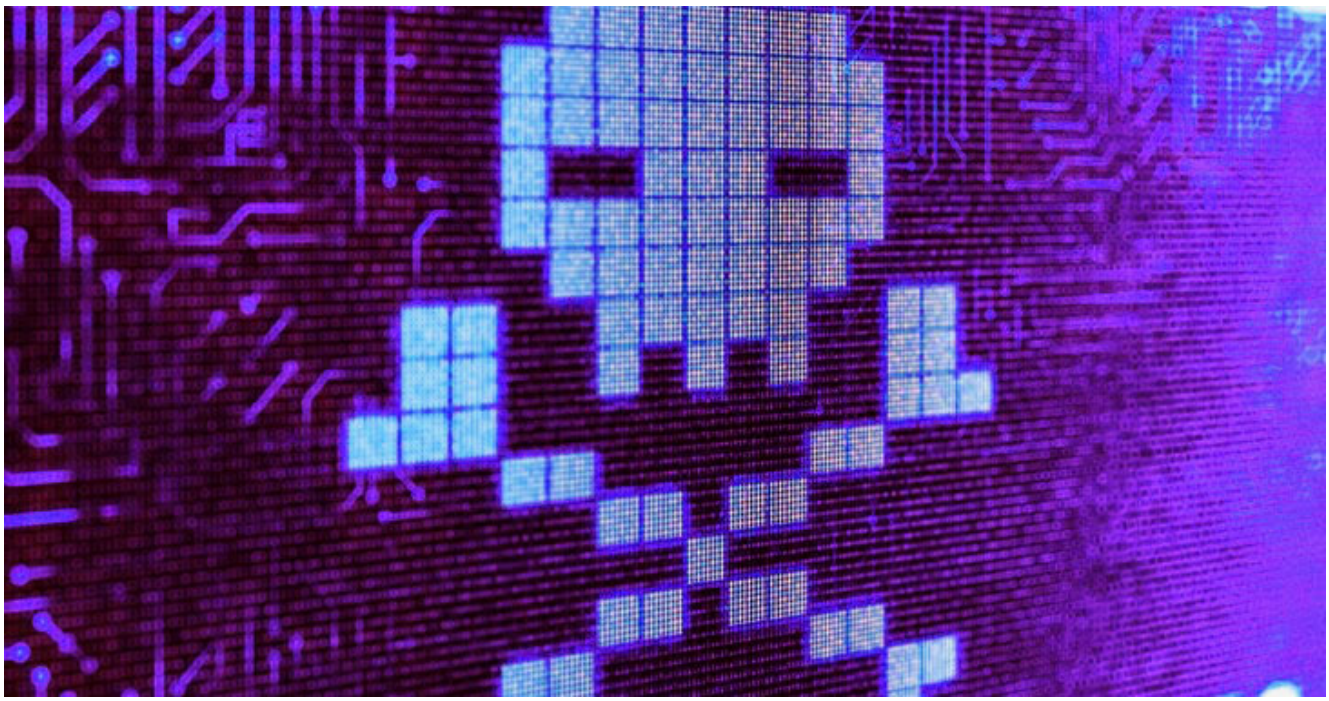
Experts Shed Light on BlackGuard Infostealer Malware Sold on Russian Hacking Forums

thehackernews.com/2022/04/experts-shed-light-on-blackguard.html

April 4, 2022



A previously undocumented "sophisticated" information-stealing malware named BlackGuard is being advertised for sale on Russian underground forums for a monthly subscription of $200.

"BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients," Zscaler ThreatLabz researchers Mitesh Wani and Kaivalya Khursale said in a report published last week.

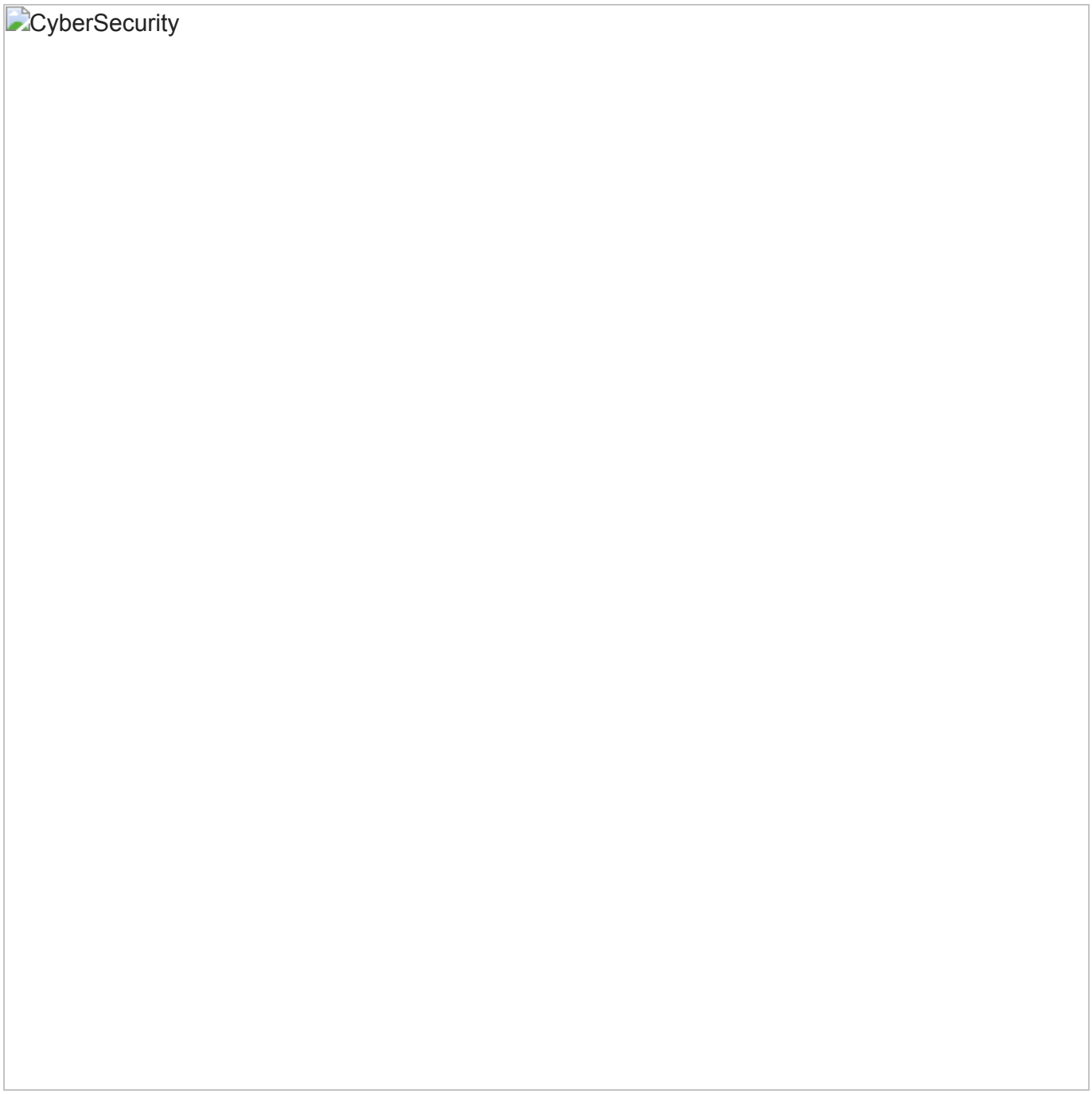
Also sold for a lifetime price of $700, BlackGuard is designed as a .NET-based malware that's actively under development, boasting of a number of anti-analysis, anti-debugging, and anti-evasion features that allows it to kill processes related to antivirus engines and bypass string-based detection.

What's more, it checks the IP address of the infected devices by sending a request to the domain "https://ipwhois[.]app/xml/," and exit itself if the country is one among the Commonwealth of Independent States (CIS).

```
for (int i = 0; i < 1; i++)
{
    Console.WriteLine("Loading..2.!..2.");
    Thread.Sleep(1849);
    string ekranirovan = portugalia.ekranirovan;
    Directory.CreateDirectory(ekranirovan);
    c00003c.collect_openvpn();
    c00003b.collect_nordvpn();
    c000006.information.txt();
    c000043.Collect_Browser(portugalia.ekranirovan + "\\\\Browsers");
    balda23.Collect_Edge();
    lapaplpal.Collect_Opera();
    kiskaaliska.Collect_Chrome1();
    blacktrailer5.Collect_Chrome2();
    Falaimetat.Collect_Files();
    Thread.Sleep(200);
    c000036.Collect_Pidgin(portugalia.ekranirovan);
    c000039.Screenshot(portugalia.ekranirovan);
    ddoppuy.Collect_Telegram(portugalia.ekranirovan);
    c00003e.Collect_Wallets(ekranirovan + "\\\\Wallets");
    c000059.Collect_Messengers(ekranirovan + "\\\\Messenger");
    c00005c.Collect_Chrome_Extension_Wallet(ekranirovan + "\\\\Chrome_Wallet");
    c00005b.Collect_Edge_Wallet(ekranirovan + "\\\\Edge_Wallet");
    c00005a.Collect_Edge_Wallet_Beta(ekranirovan + "\\\\Edge Betta_Wallet");
    c00002f.Collect_Discord();
    c000034.Collect_Filezilla();
    c00000a.Collect_Winscp();
    string text = "chrome";
    string text2 = c000007.Get_Location(text);
    string text3 = c000007.Get_Chrome_Version(text2);
    string text4 = c000007.Get_UserAgent(text);
    c000010.Collect_Outlook(portugalia.ekranirovan);
    c000035.Collect_TotalCommander();
    File.WriteAllText(portugalia.ekranirovan + "\\\\UserAgent.txt", string.Concat(new string[]
```

BlackGuard's extensive functionality means it can amass information stored in browsers, such as passwords, cookies, autofill data, browsing history, 17 different cold cryptocurrency wallets, and as many as six messaging apps, including Telegram, Signal, Tox, Element, Pidgin, and Discord.

In addition, the malware targets 21 crypto wallet extensions installed in Chrome and Edge browsers, and three VPN apps NordVPN, OpenVPN, and ProtonVPN, the results of which are subsequently compressed into a ZIP archive and exfiltrated to a remote server.



The findings come as Morphisec disclosed details of another infostealer family called Mars that's been observed leveraging fraudulent Google Ads for well-known software like OpenOffice to distribute the malware.

"While applications of BlackGuard are not as broad as other stealers, BlackGuard is a growing threat as it continues to be improved and is developing a strong reputation in the underground community," the researchers said.

SHARE □ □ □ □ ⅎ
SHARE □