Researchers warn of FFDroider and Lightning info-stealers targeting users in the wild

thehackernews.com/2022/04/researchers-warn-of-ffdroider-and.html

April 11, 2022

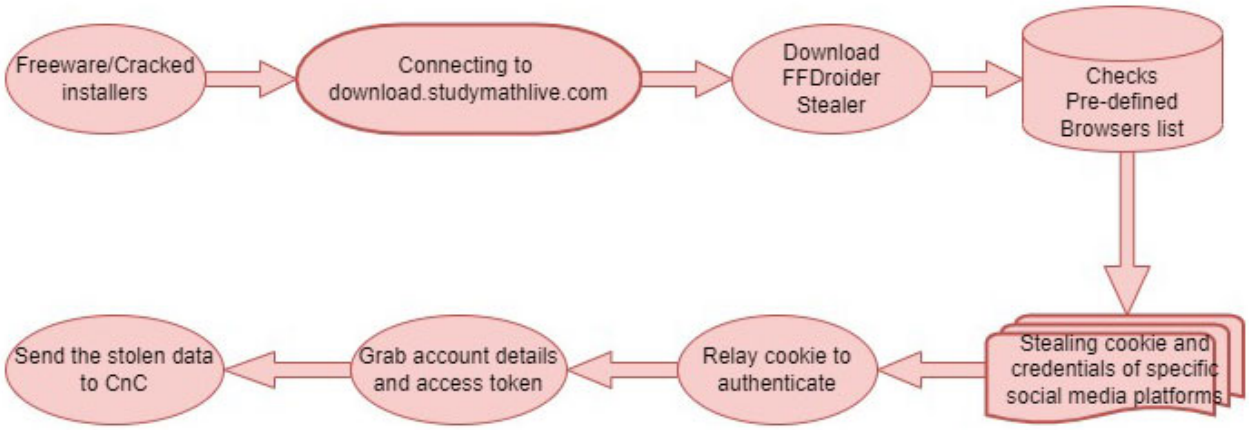
Cybersecurity researchers are warning of two different information-stealing malware, named **FFDroider** and **Lightning Stealer**, that are capable of siphoning data and launching further attacks.

"Designed to send stolen credentials and cookies to a Command & Control server, FFDroider disguises itself on victim's machines to look like the instant messaging application 'Telegram,'" Zscaler ThreatLabz researchers Avinash Kumar and Niraj Shivtarkar said in a report published last week.

Information stealers, as the name implies, are equipped to harvest sensitive information from compromised machines, such as keystrokes, screenshots, files, saved passwords and cookies from web browsers, that are then transmitted to a remote attacker-controlled domain.

FFDroider is distributed through cracked versions of installers and freeware with the primary objective of stealing cookies and credentials associated with popular social media and e-commerce platforms and using the plundered data to login into the accounts and capture other personal account-related information.

Web browsers targeted by the malware include Google Chrome, Mozilla Firefox, Internet Explorer, and Microsoft Edge. The websites targeted encompass Facebook, Instagram, Twitter, Amazon, eBay, and Etsy.



FFDroider Attack Cycle

"The stealer signs into victims' social media platforms using stolen cookies, and extracts account information like Facebook Ads-manager to run malicious advertisements with stored payment methods and Instagram via API to steal personal information," the researchers said.

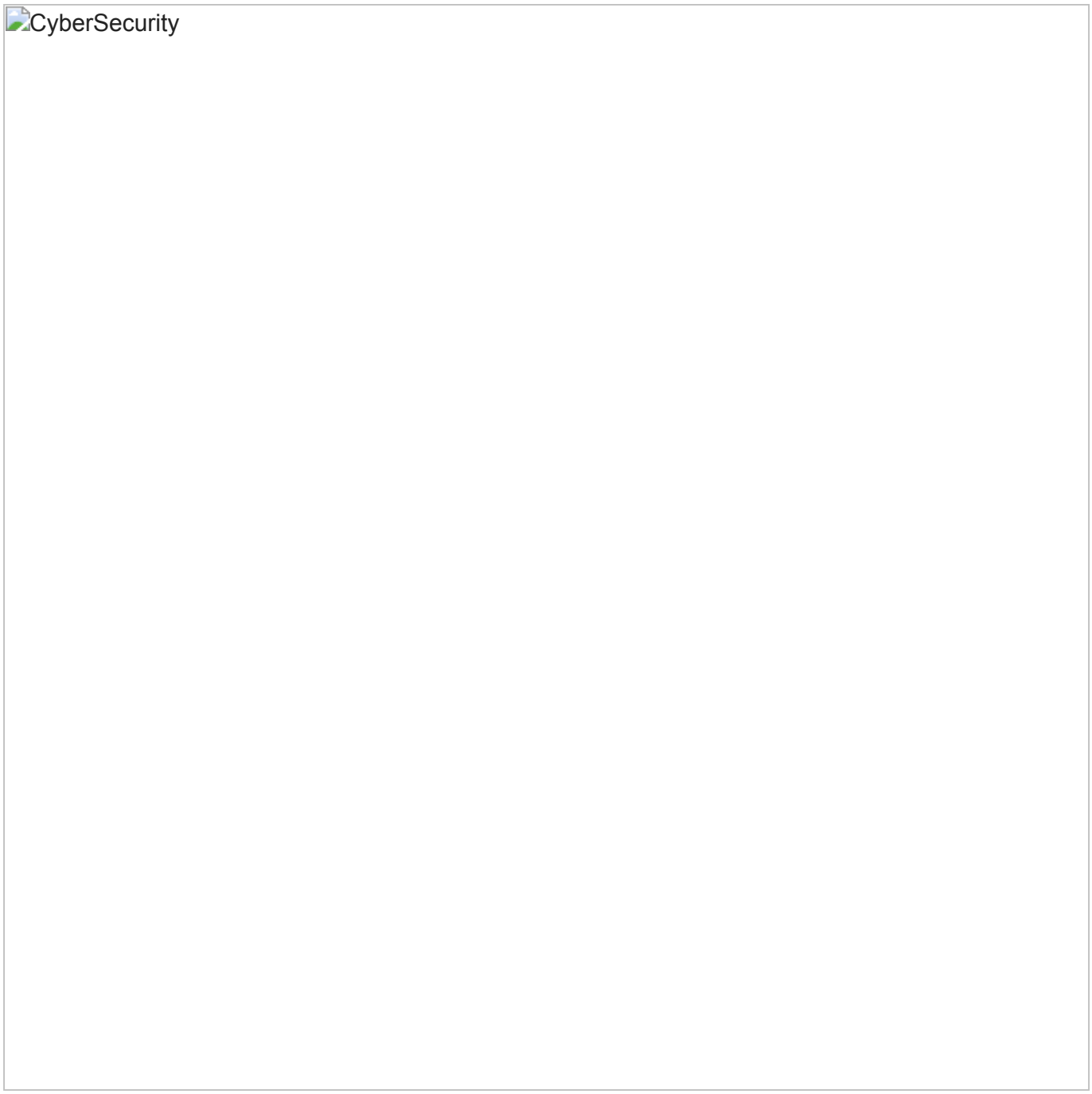
FFDroider also comes with a downloader functionality to upgrade itself with new modules from an update server that allows it expand its feature set over time, enabling malicious actors to abuse the stolen data as a vector for initial access to a target.

```
internal class MainEntrance
{
    // Token: 0x0600000F RID: 15 RVA: 0x000032AC File Offset: 0x000014AC
    private static void Main(string[] args)
    {
        List<ILogGecko> getLogGecko = Input.GetLogGecko;
        List<ILogChrome> getLogChrome = Input.GetLogChrome;
        List<List<IWallet>> getLogWallet = Input.GetLogWallet;
        IPcInfo getPcInfo = Input.GetPcInfo;
        List<IFile> getFiles = Files.GetFiles;
        List<ITelegram> getTelegram = Telegram.GetTelegram;
        List<IDiscord> getDiscord = Discord.GetDiscord;
        List<ISteam> getSteam = Steam.GetSteam;
        IScreen getScreenShot = PcInfo.GetScreenShot;
        Runner.Run(new ILog
        {
```

Main Function of Lightning Stealer

Lightning stealer operates in a similar fashion in that it can steal Discord tokens, data from cryptocurrency wallets, and details pertaining to cookies, passwords, credit cards, and search history from more than 30 Firefox and Chromium-based browsers, all of which is exfiltrated to a server in JSON format.

"Info Stealers are adopting new techniques to become more evasive," Cyble researchers said, adding it "witnessed ransomware groups leveraging Info Stealers to gain initial network access and, eventually, exfiltrating sensitive data."



The development comes as stealer malware is becoming an increasingly common occurrence across different attack campaigns in recent months, in part to fill the void left by Raccoon Stealer's exit from the market in late March due to the ongoing war in Ukraine.

In February 2022, Cyble Research disclosed details of an emerging threat called Jester Stealer that's engineered to steal and transmit login credentials, cookies, credit card information along with data from passwords managers, chat messengers, email clients, crypto wallets, and gaming apps to the attackers.

Since then, at least three different info-stealers have emerged in the wild, including BlackGuard, Mars Stealer, and META, the last of which has been observed delivered via malspam campaigns to collect sensitive data.

SHARE □ □ □ □ □

SHARE □