Fake Microsoft Store, Spotify sites spread info-stealing malware

bleepingcomputer.com/news/security/fake-microsoft-store-spotify-sites-spread-info-stealing-malware/

Lawrence Abrams

By
Lawrence Abrams

- April 20, 2021
- 10:37 AM
- 0

Attackers are promoting sites impersonating the Microsoft Store, Spotify, and an online document converter that distribute malware to steal credit cards and passwords saved in web browsers.

The attack was discovered by cybersecurity firm ESET who issued a warning yesterday on Twitter to be on the lookout for the malicious campaign.

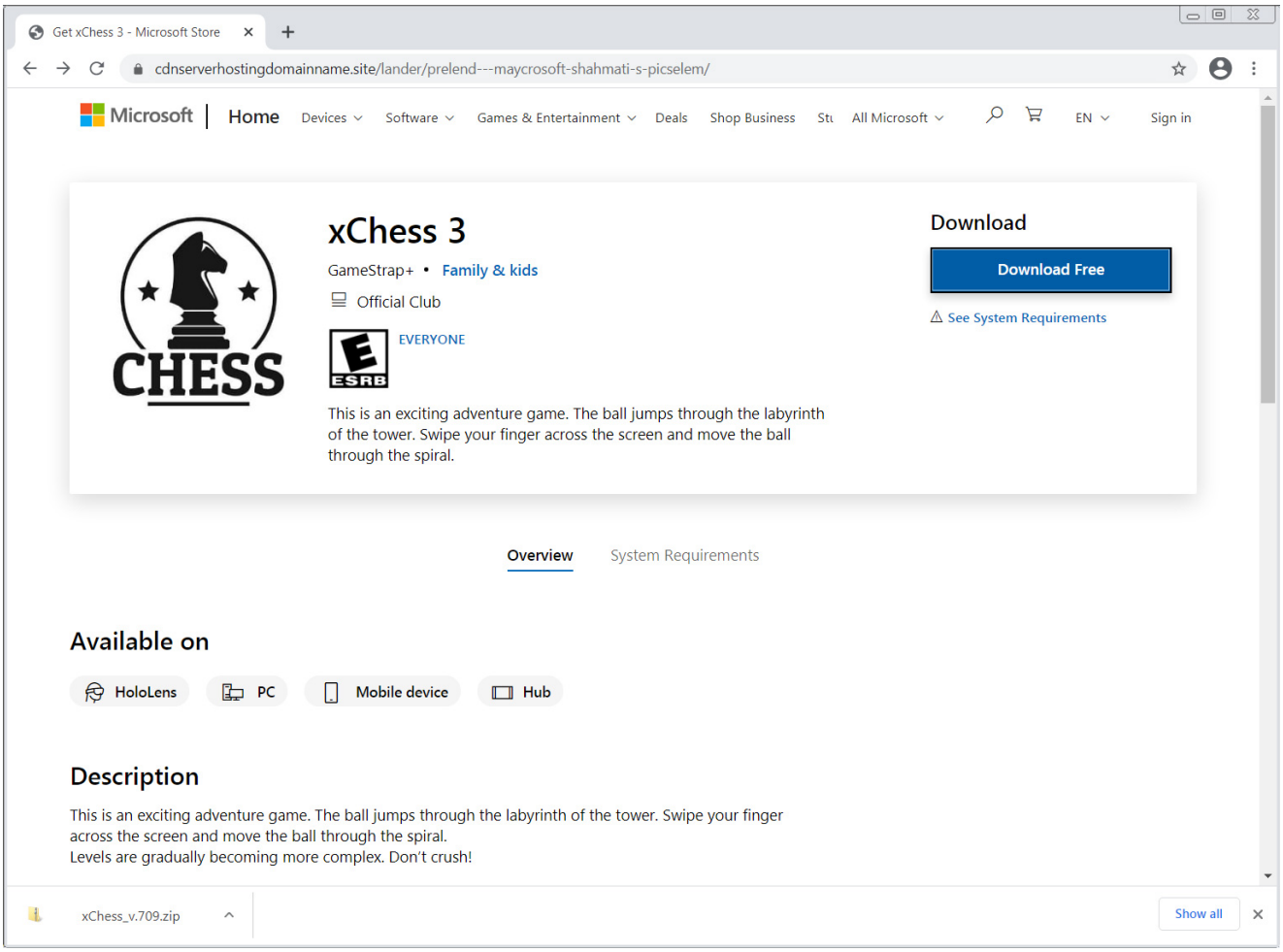
In a conversation with Jiri Kropac, ESET's Head of Threat Detection Labs, BleepingComputer learned that the attack is conducted through malicious advertising that promotes what appears to be legitimate applications.

For example, one of the advertisements used in this attack promotes an online Chess application, as shown below.

Malicious advertisement promoting a fake Chess app

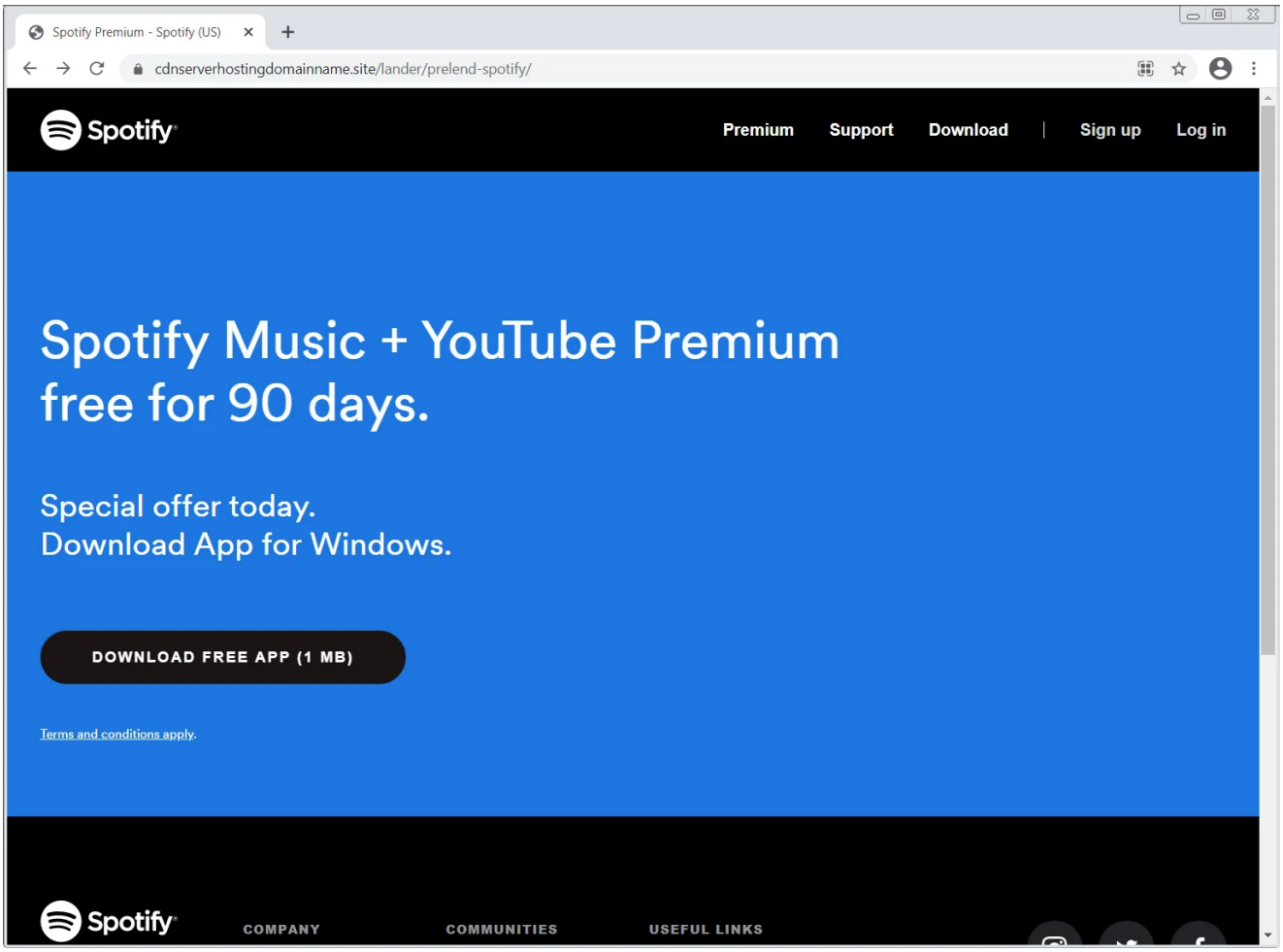
However, when users click on the ad, they are brought to a fake Microsoft Store page for a fake 'xChess 3' online chess application, which is automatically downloaded from an Amazon AWS server.

The downloaded zip file is named 'xChess_v.709.zip' [VirusTotal], which is actually the the 'Ficker', or 'FickerStealer,' information-stealing malware in disguise, as shown by this Any.Run report created by BleepingComputer.



Fake Microsoft Store page distributing the Ficker malware

Other advertisements from this malware campaign pretend to be for Spotify (shown below) or an online document converter. When visited, their landing pages will also automatically download a zip file containing the Ficker malware.



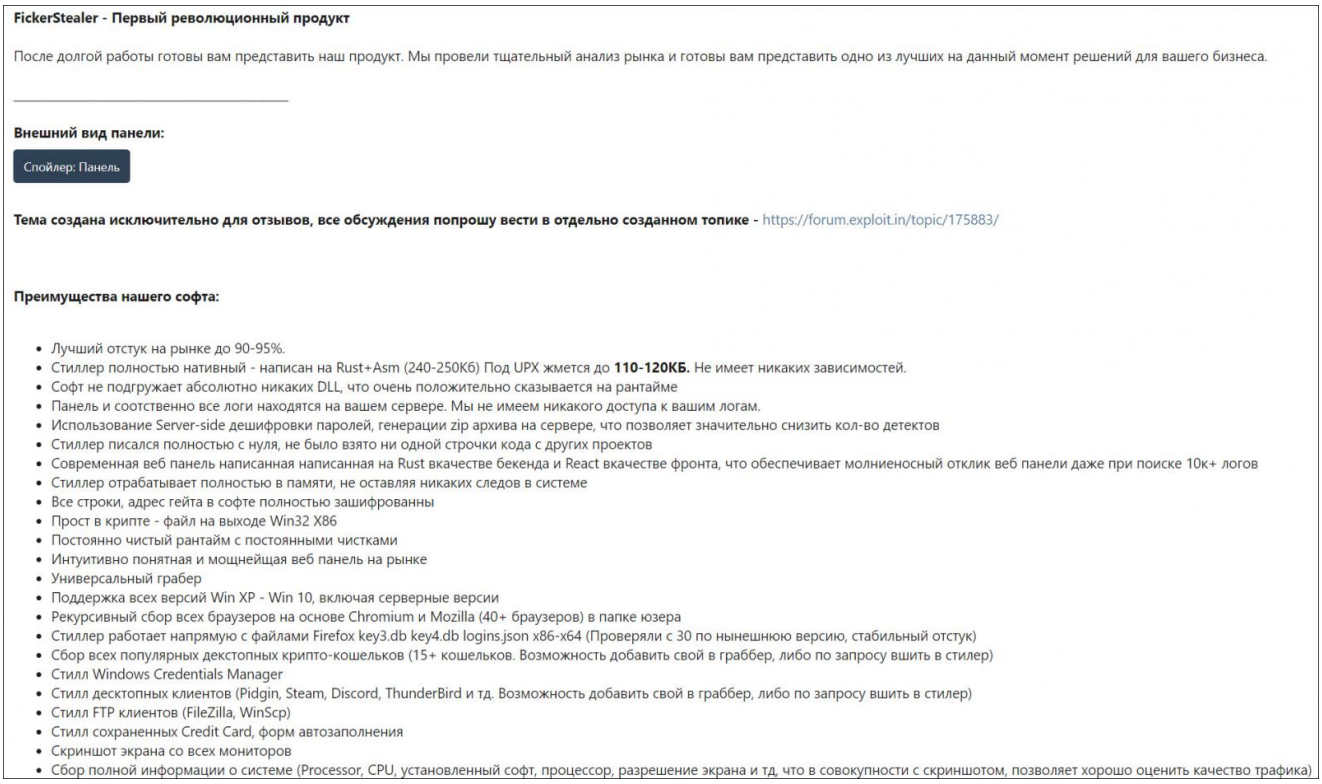
Fake Spotify landing page

Once a user unzips the file and launches the executable, instead of being greeted by a new online Chess application or the Spotify software, the Ficker malware will run and begin stealing the data stored on their computer.

What is the Ficker malware

Ficker is an information-stealing Trojan released on Russian-speaking hacker forums in January when the developer began renting out the malware to other threat actors.

In a forum post, the developer describes the malware's capabilities and allows other threat actors to rent the software from anyone from one week up to six months.



FickerStealer - Первый революционный продукт

После долгой работы готовы вам представить наш продукт. Мы провели тщательный анализ рынка и готовы вам представить одно из лучших на данный момент решений для вашего бизнеса.

Внешний вид панели:

Спойлер: Панель

Тема создана исключительно для отзывов, все обсуждения попрошу вести в отдельно созданном топике - https://forum.exploit.in/topic/175883/

Преимущества нашего софта:

- Лучший отстук на рынке до 90-95%.
- Стиллер полностью нативный - написан на Rust+Asm (240-250Кб) Под UPX жмется до **110-120КБ.** Не имеет никаких зависимостей.
- Софт не подгружает абсолютно никаких DLL, что очень положительно сказывается на рантайме
- Панель и соотственно все логи находятся на вашем сервере. Мы не имеем никакого доступа к вашим логам.
- Использование Server-side дешифровки паролей, генерации zip архива на сервере, что позволяет значительно снизить кол-во детектов
- Стиллер писался полностью с нуля, не было взято ни одной строчки кода с других проектов
- Современная веб панель написанная написанная на Rust вкачестве бекенда и React вкачестве фронта, что обеспечивает молниеносный отклик веб панели даже при поиске 10к+ логов
- Стиллер отрабатывает полностью в памяти, не оставляя никаких следов в системе
- Все строки, адрес гейта в софте полностью зашифрованны
- Прост в крипте - файл на выходе Win32 X86
- Постоянно чистый рантайм с постоянными чистками
- Интуитивно понятная и мощнейшая веб панель на рынке
- Универсальный грабер
- Поддержка всех версий Win XP - Win 10, включая серверные версии
- Рекурсивный сбор всех браузеров на основе Chromium и Mozilla (40+ браузеров) в папке юзера
- Стиллер работает напрямую с файлами Firefox key3.db key4.db logins.json x86-x64 (Проверяли с 30 по нынешнюю версию, стабильный отстук)
- Сбор всех популярных декстопных крипто-кошельков (15+ кошельков. Возможность добавить свой в граббер, либо по запросу вшить в стилер)
- Стилл Windows Credentials Manager
- Стилл десктопных клиентов (Pidgin, Steam, Discord, ThunderBird и тд. Возможность добавить свой в граббер, либо по запросу вшить в стилер)
- Стилл FTP клиентов (FileZilla, WinScp)
- Стилл сохраненных Credit Card, форм автозаполнения
- Скриншот экрана со всех мониторов
- Сбор полной информации о системе (Processor, CPU, установленный софт, процессор, разрешение экрана и тд, что в совокупности с скриншотом, позволяет хорошо оценить качество трафика)

A forum post marketing the FickerStealer malware

Using this malware, threat actors can steal saved credentials in web browsers, desktop messaging clients (Pidgin, Steam, Discord), and FTP clients.

In addition to stealing passwords, the developer claims the malware can steal over fifteen cryptocurrency wallets, steal documents, and take screenshots of the active applications running on victims' computers.

This information is then compiled into a zip file and transmitted back to the attacker, where they can then extract the data and use it for other malicious activities.

Due to the Ficker malware's extensive functionality, victims of this campaign should immediately change their online passwords, check firewalls for suspicious port forwarding rules, and perform a thorough antivirus scan of your computer to check for additional malware.

Related Articles:

Ukraine warns of “chemical attack” phishing pushing stealer malware

New powerful Prynt Stealer malware sells for just $100 per month

New ZingoStealer infostealer drops more malware, cryptominers

New ChromeLoader malware surge threatens browsers worldwide

Fake Binance NFT Mystery Box bots steal victim's crypto wallets

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.