



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

New Automated Phishing Service Advertised

New and untested threat actor “evilproxy” advertised an automated phishing service on the Russian language Deep Web forum xss[.]is. This service lowers the barrier of entry, offering access to more than a dozen prebuilt phishing pages targeting various companies, including:

- Google
- Microsoft
- Apple
- Facebook
- Instagram
- LinkedIn
- Twitter

According to the actor, these phishing pages collect a victim’s login credentials and web browser cookies. Additional features of the service include:

- Leverages stolen data to create unique user browser fingerprints
- Avoids detection by verifying visitors are not browsing from a virtual machines or headless devices
- Controls web traffic to sites by allowing or denying specific visitors access
- Manages proxies and domains
- Notifies users via Telegram

Prices for the service vary depending on the length of the license, including:

- \$400 USD for one-month
- \$250 USD for 20 days
- \$150 USD for 10 days

Original post from threat actor “evilproxy” advertising a new automated phishing service.

New Automated Phishing Service Advertised (Cont.)

[EvilProxy] Phishing as a Service / Фишинг как услуга

evilproxy · 02.07.2022 · cookies live panel logins passwords phass phishing

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТИ

+ Новая сделка

Отслеживать



evilproxy

Премиум

Premium

Регистрация: 01.07.2022
Сообщения: 4
Реакции: 1

02.07.2022

Reverse proxy

Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

Мы можем помочь вам повысить устойчивость к фишинговым атакам. Фишинг как услуга (PhaaS) - это программа повышения осведомленности о безопасности для всех сотрудников организации.

Наши симуляции фишинга поддерживаются программной платформой собственной разработки. В частности, наше бэкэнд-приложение предлагает полный набор функций, необходимых для проведения фишинговых кампаний:

Получите демоверсию совершенно бесплатно на 1 день!

New Web Browser Facilitates Fraud

New and untested threat actor “BriTchest” advertised a new web browser that facilitates fraud by enabling users to create and manage multiple accounts for various services (multi-accounting), on the Russian and English language forum club2crd[.]su. The actor claims this new browser, dubbed “Ultimate Orb”, utilizes real browser fingerprints to avoid detection by anti-fraud systems that most websites have in place. This differs from traditional anti-detect browsers, like “Che Browser”, that create new, unique browser fingerprints, which are known to sometimes fail anti-fraud evasion.

According to the actor, this new browser can divide user workspaces, or tab groups, into virtual desktops with customizable profiles and configuration settings.

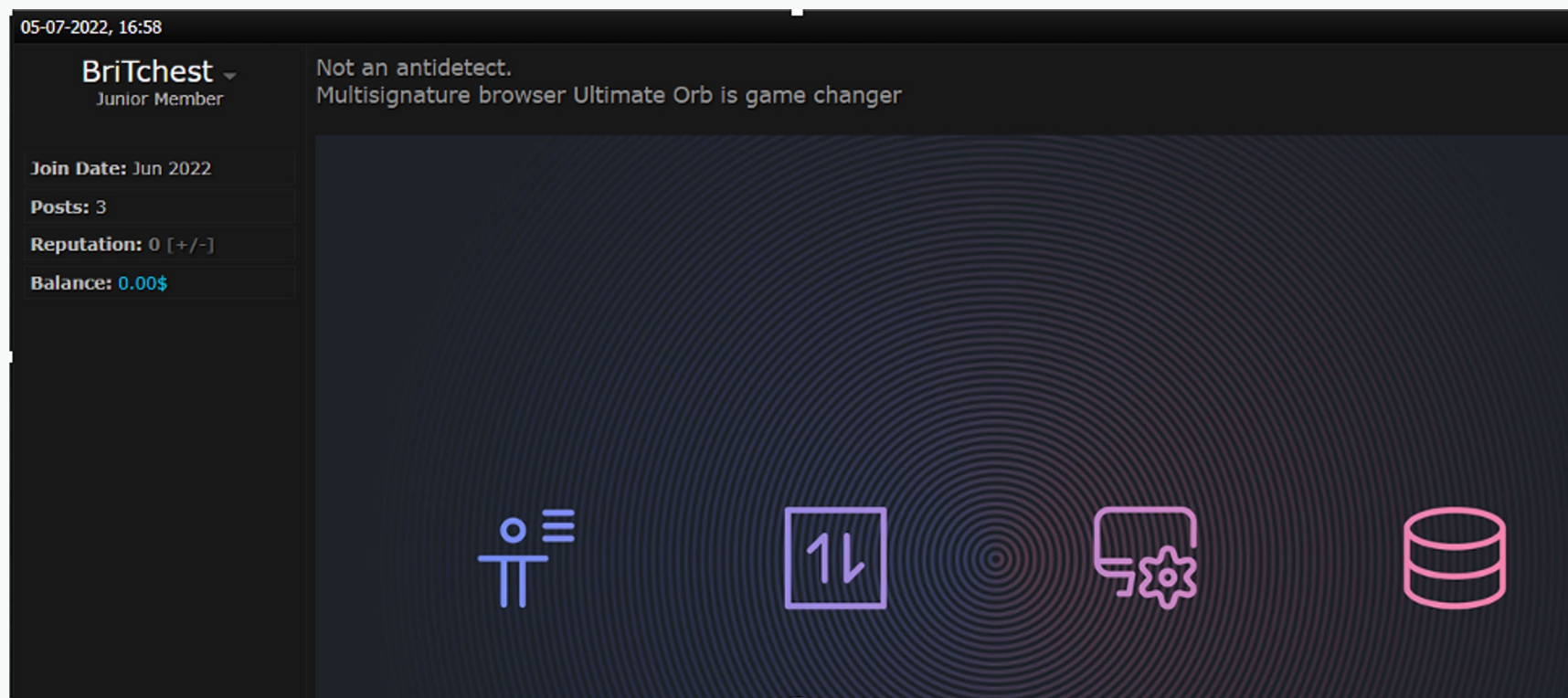
In addition to multi-accounting, the actor claims that users can leverage this browser to:

- Compromise systems
- Perform spam campaigns
- Mask IP addresses

There are various licenses available for the browser, ranging from \$24 USD for one-day to \$2,800 USD for three-years. The actor also offers a free version of the browser that limits the total number of profiles per user.

Original post from threat actor “BriTchest” advertising a new web browser that facilitates fraud.

New Web Browser Facilitates Fraud (Cont.)



Threat Actor Plans Attacks Against Clients Of Unspecified Managed Service Provider

Untested threat actor “Beeper” is seeking a partner to coordinate a large-scale cyber-attack against the clients of an unspecified managed service provider (MSP) on the Russian language Deep Web forum exploit[.]in. The actor claims to have access to the MSP’s administrative panel, where they currently manage resources for more than 50 different U.S.-based companies located in approximately the same time zone. These resources allegedly include more than 100 VMware instances and 1,000 servers that almost certainly contain sensitive data.

The actor claims they need a partner to launch the attacks simultaneously, due to the large number of vulnerable systems. The actor also specified that they wish to take a more favorable share of the profits, since they conducted most of the planning for the attacks on their own.

Despite their lack of reputation on the forum, ZeroFox researchers assess this actor is likely credible, as they have deposited more than \$11,000 USD (0.5 BTC) into the forum’s escrow service, indicating the threat actor has funds available to broker a deal with other actors.

Original post from threat actor “Beeper”, who is seeking a partner to coordinate a large-scale cyber-attack against the clients of an unspecified managed service provider.

Threat Actor Plans Attacks Against Clients of MSP (Cont.)

B

Looking for a partner to practice MSP

By Beeper, 5 hours ago in [Access] - FTP, shells, root, sql-inj, DB, Servers

[Start new topic](#)[Reply to this topic](#)

Beeper

byte

•

B

Paid registration

● 0

1 post

Joined

07/05/22 (ID: 132904)

Activity

хакинг / hacking

Deposit

0.500000 ₮

Posted 5 hours ago

Access to the MSP panel, 50+ companies
More than 100 ESXi, 1000+ servers

All corps are American and approximately in the same time zone.
I want to work qualitatively, I do not have enough hands.

In terms of preparation, there are little things left, so my percentage of profit will definitely be high.
For details and suggestions - in private messages

+

Quote

Report post

Source Code For Malware Intended For Government Use Advertised

New and untested threat actor “oDmC3oJrrSuZLhp” advertised the source code for malware they claim was originally intended to aid governments in the fight against terrorism, on the Russian language Deep Web forum xss[.]is. The actor claims they stole the source code from a company named “Intellexa”, that was allegedly hired to develop a lawful intercept project, dubbed “Nova Platform”, by an undisclosed government.

Like the NSO Group’s “Pegasus” spyware, the actor claims this malware can compromise devices running all versions of iOS or Android with the click of a malicious link by victims. Once the malware is installed, the actor alleges that operators can access sensitive data on the device, including:

- Call log
- Login credentials
- Web browser cookies
- Contacts
- Emails

Additionally, the actor stated that the malware establishes persistence, and will continue running even after a compromised device is rebooted. The actor said they are willing to sell the source code to state-sponsored threat actor groups, including those in China or North Korea, for \$50,000,000 USD.

Although the threat actor’s post has garnered significant attention from other members of the forum, their credibility is difficult to determine, due to another, banned threat actor that previously advertised the same source code on another Russian language forum, exploit[.]in.

Original post from threat actor "oDmC3oJrrSuZLhp" advertising the source code for malware they claim was originally intended to aide governments in the fight against terrorism.

Source Code For Malware To Aide Governments (Cont.)

Android and IOS 1click 0day Trojan with persistence (IOS 15.5/Android 12)

oDmC3oJrrSuZLhp · Четверг в 11:38

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка

1 2 3 Вперед »

Перейти к новому Отслеживать



oDmC3oJrrSuZLhp
CD-диск

Пользователь

Регистрация: 11.07.2022
Сообщения: 14
Реакции: 0

Четверг в 11:38

[ENG]

This thread is dedicated to high liquidity government sponsored APTs

I sell **complete source** stolen by a cyber warfare company, software intended for government use only, ability to extract and monitor devices remotely, complete persistence on reboot. The existence of this software has been classified as **top secret** by the defense ministry of the country that developed it. It is intended for the exclusive use by governments for the fight against terrorism and offers a very simple graphical interface for investigative activity. It works on every version of IOS and Android currently existing (IOS 15.5 and Android 12), it covers almost all the devices in circulation. The software is installed through the simple click of a link by the victim, completely silent, there is no need for any other interaction beyond the link. The suite also includes the possibility of generating malicious links through own domains (to increase trust towards the victim) and offers a user friendly tool for investigations (that's what it was designed for).