



ZEROFOX®

Your Intelligence Digest

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

New Service Trains Threat Actors To Spread Malware Via Google & Facebook Ads

New and untested threat actor “Clarks” advertised a new service to train threat actors on their method to target and compromise machines, to spread malware via malicious advertisements, on the English language Dark Web forum “CryptBB”. This method primarily leverages ads on Google and Facebook to spread malware instead of phishing emails.

The actor offers two different versions of the service: one that comes with all the kits a threat actor will need to deploy this method, and another that does not. The full kit includes:

- Stealer malware (with at least a two-month license)
- Remote desktop protocols (RDPs) and virtual private servers (VPS)
- Hosting services
- Domains
- SSL certificates

There is also an optional course module focused on compromising U.K.-based businesses and bank accounts.

Additionally, the actor claims to have a private tool to manually obfuscate malware; however, this was only available by contacting the actor directly. ZeroFox researchers note this is likely done to ensure that buyers will continue to use the tools provided to them by the actor following the completion of the course.

The actor charged \$1,000 USD for the version of the service with the kits, and \$300 USD for the version without. The actor claims their team will assist students until they successfully compromise or steal a combined 1,000 machines/logs by using their method.

Original post from threat actor "Clarks" advertising course to spread malware via Google and Facebook ads.

New Service Trains Threat Actors To Spread Malware Cont.

⚡ MALWARE SPREADING COURSE IS OPENED ⚡



Clarks •
Junior
Member

Posts: 5
Joined: Mar 2022
Reputation: 0

04-27-2022, 10:23 PM #1

Method: Google Ads & Facebook Ads & Other (Random Cold traffic)

Course with tools:

- ✓ | ONE Powerful Stealers (2-3 Months License)
- ✓ | Logs for working with FB & G. Ads
- ✓ | Bins and Credit Cards
- ✓ | Proxy
- ✓ | Anti-detect (Che Browser, Linken Sphere, Cypher)
- ✓ | RDP / VPS
- ✓ | Landing Page
- ✓ | Hosting & Domain & SSL Certificates
- ✓ | Filter (Original Price: 150\$) Optional
- ✓ | Cloaking (Private)
- ✓ | Crypt by Best (Private) Manual Crypter "contact only"

Threat Actor Selling Payment Gateways To Cash Out Stolen Payment Cards

New and untested threat actor “whitestein” is selling access to U.S.-based payment gateways that purportedly allow individuals to cash out funds from stolen payment cards, on the Russian language Deep Web forum xss[.]is. The actor claims that they leverage an unspecified merchant account service provider to configure both online and physical payment gateways. According to the actor, they successfully leveraged these gateways to generate more than \$50,000 USD in unauthorized charges with compromised payment cards. The actor specified that it takes approximately 48 hours for individuals to receive the stolen funds from transactions that are processed by the gateways.

The actor charged \$1,500 USD for access to a payment gateway. It is not clear how many gateways are available.

ZeroFox researchers highlight that they are unable to accurately discern the threat actor’s credibility given the lack of reference information. However, their proposed method still represents a viable option for threat actors to employ due to the large quantity of stolen payment cards available on the underground economy.

Merchant Setup

whitestein · Среда в 02:36



whitestein
floppy-диск

Пользователь

Регистрация: 15.04.2022
Сообщения: 7
Реакции: 0

Среда в 02:36

Business merchants with online/physical terminals.
Country : USA
Price : \$1,500 each.

Fully Setup and Ready to Authorize Charges.
Settlement of Funds : 48hrs.
I can show proof of cashouts upto \$50k+ from multiple accounts.

Jabber : PM

Need Partners with valid CC Database

Жалоба

New Underground Marketplace Specializes In Sale Of Stolen Payment Cards

In late April 2022, new and untested threat actor “BidenCash” announced an emerging underground marketplace that specializes in the sale of stolen payment cards on the Russian language Deep Web forum xss[.]is. The actor claims their new shop, dubbed “BidenCash”, already has more than 2.5 million stolen payment cards available. ZeroFox researchers assess this marketplace fills a need because threat actors are still looking for a viable option to replace the now-defunct “Joker’s Stash”. According to the actor, they plan to address this gap in the underground economy by providing threat actors with a convenient and reliable source of stolen payment cards.

Features of the new shop include:

- Quickly replenishes cards
- Supports pre-ordering and automatic buying
- Multi-factor authentication
- GPG account recovery
- Compiles sales statistics for card suppliers
- Instantly refunds orders

ZeroFox researchers will continue to monitor the growth of this new marketplace, as “BidenCash” is actively looking for stolen payment card suppliers.



BidenCash
Premium

Registration: 04/26/2022
Messages: eight
Reactions: 0
Deposit: 0.2555\$

04/27/2022



BidenCash is a platform for selling cards from hackers, for hackers. I have come realized that none of the stores is convenient for buying or selling cards, and I d At the moment, I have filled in more than 2.5 million bank cards!

Among the features of the store I would like to note:

1. Intuitive and not overloaded interface
2. Convenient replenishment system
3. Three-level loyalty system
4. Referral system
5. Pre-order and auto-purchase system
6. Good ticket system
7. Two-factor authentication system
8. GPG account recovery
9. Discount section
10. Sales statistics by vendors
11. Moderation system for downloaded databases (the supplier himself can put a support)
12. Instant return system

Service Disguises Malware As Different File Types

New and positively trending threat actor “QuantumSoftware” advertised their file extension spoofing service to disguise malware as other file types, on the English language Dark Web forum “CryptBB”. The actor claims that most commercial antivirus software will not detect their spoofed LNK files as malicious, including Windows SmartScreen. The actor specified that customers must obfuscate their own payloads.

Other features of the service include:

- Spoofs any file extension
- Maintains persistence
- Hides payloads after running
- Defines where malware is located on target machine

According to the actor, the spoofed files can execute multiple payloads with administrator rights by triggering the User Account Control (UAC). This increases the likelihood of compromising a target machine, compared to other traditional weaponized documents, because the malware mimics another program that prompts the victim for administrator rights.

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

- \$1,577 USD (€1,500 EUR) for one-year
- \$945 USD (€899 EUR) for six-months
- \$373 USD (€355 EUR) for two-months
- \$199 USD (€189 EUR) for one-month

Original post from
threat actor
"QuantumSoftware"
advertising service to
disguise malware as
different file types.

Service Disguises Malware As Different File Types Cont.

.Lnk exploit Builder | Spoof ANY extension | FUD | Bypass Smartscreen & More



QuantumSoftware •
Junior
Member

05-06-2022, 12:26 PM

Welcome everyone,
QuantumBuilder will make your payloads look like any file format (.png, .mp4, ...), you can even disguise them as a folder.

Features:

- * Spoof any extension
- * 328 different icons available
- * Bypass Windows Smartscreen, EV certs are a thing of the past
- * Decoy (upon opening your .lnk a file of your choosing will be displayed on your victim's pc)
- * Multiple payloads per .lnk. Even if one gets detected the rest will still run
- * 100% FUD even if you spread your stub, every build is unique
- * Execute your exes with admin privileges by prompting UAC with a Microsoft signed binary (powershell.exe)
- * Run your payload at startup or with a delay
- * Hide your payloads after executing them
- * Choose where your exe is dropped on your victim's computer

Macros are for the most part dead, this is probably the best method to deliver malicious code (apart from expensive 0-days)
This technique is currently being used by APT groups and botnets like Emotet.
-> <https://blog.cyble.com/2022/04/27/emotet...s-victims/>