



ZEROFOX®

Your Intelligence Digest

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

Multifunctional Exploit Software For Sale

Untested threat actor “killerAV” advertised their new multifunctional exploit software, dubbed “PenTestSoftware,” designed to compromise Windows machines, on the predominantly Russian language Dark Web forum “RAMP.” While it is common for threat actors to leverage commercial penetration testing software, like Cobalt Strike, for their operations, ZeroFox researchers note that this is a rare instance where a threat actor has claimed to independently develop their own tool with similar functionality.

In addition to gaining unauthorized access to target machines, the actor claims the software exploits unnamed vulnerabilities in Windows to escalate privileges. This increases a threat actor’s chances of launching successful attacks with the tool. Additional features of the software include:

- Obfuscates payloads to avoid detection by most antivirus products’ runtime scans
- Delivers payloads via spam modules
- Unlocks password-protected files
- Steals login credentials and additional system information from target machine
- Detects active hosts on network

The actor had three, ten-day licenses available for \$10,000 USD each.

Despite their lack of reputation on the forum, ZeroFox researchers assess the threat actor to be credible, as they agreed to use the forum’s escrow service, which requires the actor to make a security deposit prior to making a transaction..

Original post from threat actor "killerAV" advertising their new multifunctional exploit software, dubbed "PenTestSoftware," designed to compromise Windows machines

Multifunctional Exploit Software For Sale (Cont.)



killerAV
Jun 14, 2022

Messages	3
Reaction score	0
Points	1

Wednesday at 9:02 AM

Private Multifunctional PenTestSoftware, VIP approach.

We are looking for the best partners and specialists in their field. Thanks to our software, you can fully concentrate only on your work, without being distracted by the tasks that our service solves.

Your Profit to work with our software:

- You forget about purges, make yourself a high-quality traff, or take a traff from us and work together at a percentage % Traff only after the software, do not write differently. We do not work with third-party software, as we are sure only in his.
- With the raising of rights, there are no problems. Always SYSTEM. (Sploy for lifting can be bought for 250k\$ through the guarantor)
- We issue software that you can work with and not think about cleaning. We solve this issue.
- We solve any problems with software, traffic and rights.
- The key to any success in pentesting: Quality traffic with SYSTEM rights and pure private software.
- We have Clean runtime software supported by a smart and hardworking team (coding, admin, testing).

Kit Steals NFTs From MetaMask Cryptocurrency Wallets

Untested threat actor “jezabeth” advertised a kit to steal non-fungible tokens (NFTs) from MetaMask cryptocurrency wallets, on the predominantly Russian language Deep Web forum “Exploit”. The kit leverages a custom phishing page that tricks MetaMask users into sending their most expensive NFTs to a threat-actor-owned cryptocurrency wallet. This is done via abuse of the victim’s Seaport signature. The actor claims their tool can steal multiple Ethereum-based NFTs, including:

- ERC-20
- ERC-721
- ERC-1155

The asking price for the tool is \$10,500 USD (8 ETH). They also agreed to use the forum’s escrow service, indicating the actor is likely to possess what they claim.

The announcement follows a growing trend on the criminal underground where more threat actors are offering custom tools and services that target NFTs. These tokens have become an increasingly popular way to buy and sell products online via cryptocurrency.

Original post from threat actor "jezabeth" advertising a tool to steal non-fungible tokens (NFTs) from MetaMask cryptocurrency wallets

Kit Steals NFTs From MetaMask Cryptocurrency Wallets (Cont.)

jezabeth
byte



Paid registration
+ 1
18 posts
Joined
02/16/21 (ID: 114178)
Activity
кодинг / coder

Posted September 9

Newest NFT drainer + warning bypass (Seaport / OpenSea API)

This will be the best drainer you could find now.

Drains Tokens: ERC-20 / ERC-1155 / ERC-721 / ETH

NFT's will be drained by using Seaport contract signature. User does not pay for transaction fee. No warnings will be given from MetaMask, it bypasses latest update.

Drainer will first drain the most expensive tokens, then the least expensive tokens. Landingpage is easy to customize

Bypass the last SetApprovalForAll warning of MetaMask.

Can provide video on Telegram, message me for my Telegram.

Price: 8 ETH
Escrow / Middleman accepted, costs for buyer

Phishing Page Targets Revolut Banking Customers

Well-regarded threat actor “goodrabbit” advertised a phishing page that targets Revolut banking customers on the predominantly Russian language Deep Web forum “XSS”. Interestingly, this page offers administrator access to a web panel, where users can control a victim’s web camera.

This would likely allow threat actors to take photos of their victims, proving a greater success rate for account verification purposes and bypass of know your customers (KYC) verifications.

Additional features of the phishing page include:

- Steals login credentials
- Collects payment card details
- Intercepts one-time password (OTP) codes
- Detects victim’s country of origin
- Translates data in different languages
- Exports stolen data to MySQL database

The actor is asking \$4,150 USD for lifetime access to the phishing page and the administrator panel.



goodrabbit
illegal marihuana consumer

Premium

Регистрация: 01.02.2022
Сообщения: 309
Реакции: 7
Гарант сделки: 1

Сегодня в 11:36

Good day my dear gentlemen,
today I can proudly present the Revolut phishing page No.1,
which will you guarantee access to the complete login of the Revolut account holders.

Features:

- Admin Panel
- Supports Webcam Pictures
- Phishing the OTP Code
- Automatic detection of proxys / tor
- Automatic detection of country
- Translated in any supported language
- Phishing all card details of it
- MySQL Database for secure storage of victims
- 1:1 duplicate (it isn't possible to realize which is the real Revolut site)

Reverse Proxy Phishing Service Aims To Compromise Google Accounts

Untested threat actor “BabadookServices” advertised a reverse proxy phishing service to compromise Google accounts, on the predominantly Russian language Deep Web forum “XSS”. The actor said the service can steal a victim’s session cookie, allowing threat actors to prevent further multi-factor authentication by mimicking a victim’s active session. The actor claims this is done by utilizing a modified version of the Evilginx framework to perform man-in-the-middle (MITM) attacks.

- During a MITM attack, a reverse proxy sits between the victim and Google.com
- The victim visits the phishing page and enters their Google login credentials and OTP code
- The reverse proxy forwards these requests to Google
- Google returns a valid session cookie to the reverse proxy

The actor charged approximately \$1,150 USD per month to use the service, or \$6,000 USD to buy the tool outright.

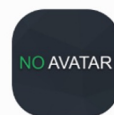
The actor also offered configuration files (AKA phishlets) for Yahoo, Office 365, and Hotmail for \$600 USD each.

Google reverse proxy/MITM phishing solution (sell/rent), Custom phishlets and scam pagees development.

BabadookServices · Суббота в 10:31

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

Новая сделка



BabadookServices
форум-диск
Пользователь

Регистрация: 02.08.2022
Сообщения: 5
Реакции: 1

Суббота в 10:31

After V3 update of Google sign in most of the reverse proxy got patched.
I am selling reverse proxy based solution (based on modified evilginx) to buypas 2fa and get cookies.
Works for all 2 step verification sms OTP, email OTP, phone tap yes, phone tap number, confirm email, confirm phone number.
Removed all headers from evilginx which cause detection.

Support proxy also for each new session.
Configure different domain for different phishlets.
Rent cost 150\$ VPS and server per month and 1000\$ per month rent.

Buy the product 6000\$ with complete setup manual
Phishlets for yahoo, o365, hotmail available. Price 600\$ per site.
Custom phishlets development of websites. Price starting from 500\$-3000\$ per site.
Scam pages development for websites of any complexity, 1:1 same page. Logs sent to telegram. Price starts from 250\$-2000\$ per site based on complexity.
Deal through guarantor only. After 1st sale will make deposit.

Последнее редактирование модератором: Воскресенье в 07:16