cts·ai

Mars Stealer Malware

Executive Summary

Mars Stealer, an improved copy of the Oski Stealer malware, first introduced in November 2019, recently appeared in the wild and is capable of stealing crypto from popular browser extensions.

According to researchers, the Mars Stealer malware attacks more than 40 browser-based crypto wallets by navigating through the wallet's security features, such as two-factor authentication (2FA). Mars Stealer further uses its functionality to steal the private key in the user's wallet.

In addition, the malware can extract valuable information on the targeted wallet, including processor model, computer name, machine ID, GUID, installed software and associated versions, username and computer domain.

Mars Stealer has been known to infiltrate wallet extensions, spreading through multiple channels including file-hosting sites, torrent clients, and suspicious sites. After infiltrating the crypto-wallet extension, the malware performs the theft by sabotaging the wallet's private key and security features, and once inside the wallet, exits the extension and erases all visible traces of the theft.

Of note is that the malware runs a check of the browser's language settings and will not infect hosts located in the Commenwealth of Independent States (CIS), such as Russia, Kazakhstan, Belarus, Azerbaijan and Uzbekistan; the application terminates itself if these setting are found.

Technical Details

Mars Stealer is a native, non-resident stealer with loader functionality and grabber based on a 2020 Oski shell. It is considered extremely lightweight at 95kb and is written in ASM/C using WinAPI and easily spreads via file-hosting websites, torrents, and fake download links. It uses many anti-detection and anti-analysis techniques to obfuscate itself and hide its actions, to include deleting itself after stealing the password + seed phrase.

Other anti-detection and anti-analysis techniques include Run-time dynamic linking, strings obfuscation, sleep anti-debug, and anti-emulation.

In addition, the malware runs security checks, as mentioned above, to avoid infection of machines from the Commonwealth of Independent States (CIS) by using `GetUserDefaultLangID()`. This query returns the language identifier of the region setting for the current user. If the user language ID matches one from the list, the stealer finishes execution. Other security checks include Mutex and expiration checks.

Mars Stealer is currently available for only $140 on the dark web forums.

cts·ai

Threat Actors

At this time, NTT has not yet attributed this campaign to a specific named threat actor group. As NTT continues to investigate this campaign and discovers more details, we will update this research with further relevant details. At such a time, NTT may attempt to link this campaign to specific actors if we discover enough relevant details to make an informed attribution decision.

Target

This malware targets 2FA and crypto extensions, but only in Chromium-based browsers (opera is an exception).
The Mars Stealer malware can only identify crypto wallet credentials from Chrome-based browsers extensions such as:

- MetaMask
- Binance Chain Wallet
- Coinbase wallet
- Coin98 Wallet
- Tron Link
- Nifty wallet

Mars Stealer supports the following browsers and extensions:

- Internet Explorer, Microsoft Edge (Chromium Version), Kometa, Amigo, Torch, Orbitium, Comodo Dragon, Nichrome, Maxxthon5, Maxxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave, Opera Stable, Opera GX, Opera Neon, Firefox, SlimBrowser, PaleMoon, Waterfox, CyberFox, BlackHawk, IceCat, K-Meleon, Thunderbird.

Crypto extensions:

- TronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaox Liberty, BitAppWllet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Ronin Wallet, Neoline, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.

Mars Stealer is able to exploit the following:

2FA plugins:

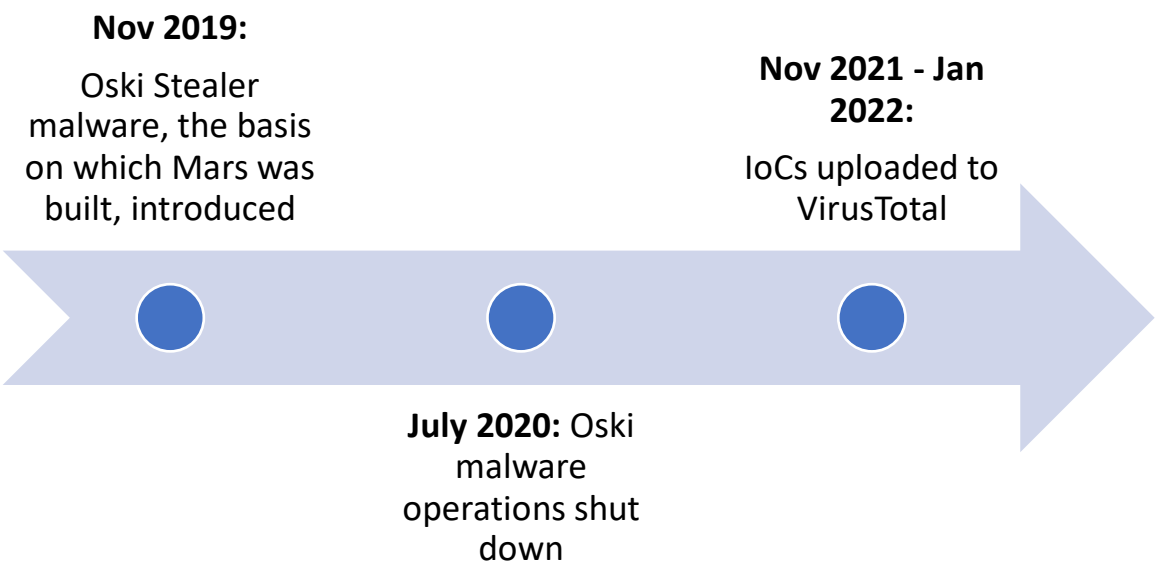
- Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.

Crypto wallets:

- Bitcoin Core and all derivatives (Dogecoin, Zcash, DashCore, LiteCoin, etc), Ethereum, Electrum, Electrum LTC, Exodus, Electron Cash, MultiDoge, JAXX, Atomic, Binance, Coinomi.

cts·ai

Campaign and Event Timeline



Mitigation and Remediation

NTT helps customers detect, prevent and remediate Mars Stealer malware infections via our Threat Detection services.

NTT provides automated indicator sharing to enhance enhance visibility and accelerate threat to support our MSS customers. Customers' using CTS-AI technology will have already received threat indicators to support threat detection.

We also recommend using MITRE ATT&CK Mitigations which can be used to reduce the risk of compromise by Mars Stealer malware. NTT recommends applying the following defense mitigations:

MITIGATION ID	MITRE ATT&CK MITIGATION NAME
M1016	Vulnerability Scanning
M1030	Network Segmentation
M1031	Network Intrusion Prevention
M1037	Filter Network Traffic
M1040	Behavior Prevention on Endpoint
M1047	Audit
M1049	Antivirus/Antimalware

Technical Indicators

SHA-256 Hash

7da3029263bfbb0699119a715ce22a3941cf8100428fd43c9e1e46bf436ca687

Domains

cookreceipts[.]fun

References

https://3xp0rt.com/posts/mars-stealer#iocs

About the Global Threat Intelligence Center

The Global Threat Intelligence Center (GTIC) protects, informs and educates NTT clients through the following activities:

- Threat research
- Vulnerability research
- Intelligence fusion and analytics
- Communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect, and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding of, and insight into the various threat actors, exploit tools and malware – and the techniques, tactics, and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities which are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities. With this knowledge, NTT's security monitoring services can more accurately identify malicious activity which is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, and enrich those threats using advanced analysis techniques and proprietary tools; and curates and publishes them using the Global Threat Intelligence Platform (GTIP).