A Long List Of Arkei Stealer's Crypto Browser Wallets

blog.minerva-labs.com/a-long-list-of-arkei-stealers-browser-crypto-wallets

- Tweet
-

Arkei is an information-stealer, distributed as a malware as a service (MAAS). It collects sensitive information such as application passwords, credit card information, web browser cookies and can even download additional payloads from the C&C server. It also shares code with several other information stealers including Oski and Vidar.

Arkei Stealer's main purpose is to collect passwords, cookies, auto-complete data, desktop files, machine data, installed software, etc. In 2021, Arkei's authors extended its crypto wallet stealing capabilities, as well as the addition of anti-debugging and anti-emulation checks, to thwart its analysis and detection rates.

We analyzed a sample found by @James_inthe_box and created a complete list of the browsers and crypto browser wallets that Arkei Stealer tries to steal.

First, let's talk about the evasion techniques this stealer performs. Arkei performs two well-known anti-debugger checks:

1. It calls ntdll!NtQueryInformationProcess with ProcessInformationClass set to 7 (ProcessDebugPort) – this call returns a DWORD value equal to 0xFFFFFFFF (–1 in decimal) if the process is being debugged:

```
.text:0079F1EF push    esi
.text:0079F1F0 push    4
.text:0079F1F2 lea     edx, [ebp+hModule]
.text:0079F1F5 push    edx             ; hResInfo
.text:0079F1F6 push    7
.text:0079F1F8 call    kernel32_GetCurrentProcess
.text:0079F1FE push    eax             ; hResInfo
.text:0079F1FF call    edi             ; NtQueryInformationProcess
```

Figure 1 - NtQueryInformationProcess anti-debugger check

2. Timing check using kernel32!GetTickCount function – when debugging in a single-step mode, a lag occurs while running the executable. Arkei checks a timestamp and compares it to another one after a few instructions, to check for a delay:

Figure 2 Timing anti-debugger check

Arkei Stealer employs another evasion technique (akin to Vidar stealer's anti–emulation technique), which checks the computer name and the username running the Arkei executable. The malicious process will terminate itself if the computer name is "HAL9TH" and the username is "JohnDoe" (which is the default computer name and default username respectively of the Windows Defender emulator):

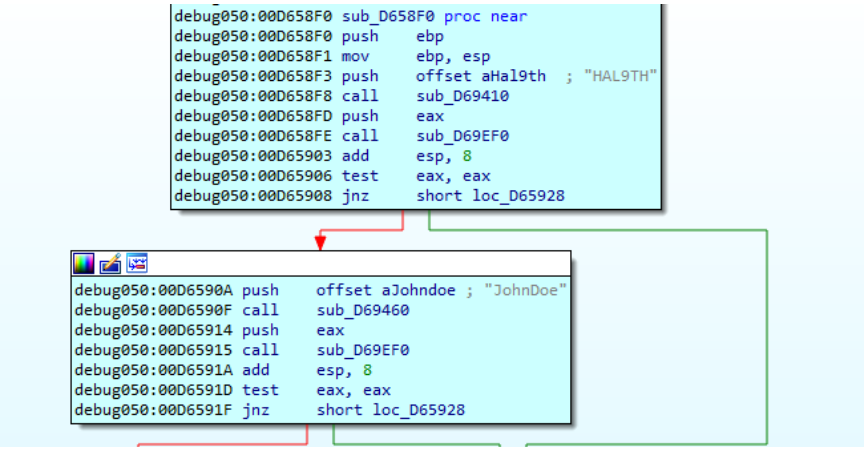

Figure 3 Anti-emulator check

To learn more about how Minerva Labs can protect your business contact us.

Arkei also checks if any of the following DLL's are loaded into the process:

- avghookx.dll - AVG Internet Security.
- avghooka.dll - AVG Internet Security.
- snxhk.dll – Avast Antivirus.
- sbiedll.dll – Sandboxie.
- api_log.dll – CWSandbox.
- dir_watch.dll - iDefense SysAnalyzer.
- pstorec.dll - SunBelt Sandbox.
- vmcheck.dll – VirtualPC.
- wpespy.dll – Sandbox.
- cmdvrt32.dll - COMODO Internet Security.
- cmdvrt64.dll - COMODO Internet Security.

This stealer will terminate itself if the language identifier of the Region Format setting of the current user is one of the following:

- 43Fh – Kazah
- 443h - Uzbek - Latin
- 419h - Russian
- 82Ch - Azeri-Cyrillic
- 423h - Belarusian

This might indicate that the author comes from one of the above countries where it is a common technique, used in order to not draw the attention of the local authorities.

If all the above checks pass successfully, the malware will continue its intended purpose.

Arkei steals passwords, cookies, and autofill information from the following 32 web browsers:

Google Chrome	Chromium
Microsoft Edge	Kometa
Amigo	Torch
Orbitum	Comodo Dragon
Nichrome	Maxthon 5
Sputnik	Vivaldi
CocCoc	Uran
QIP Surf	CentBrowser
Elements	Tor
CryptoTab	Brave
Opera	OperaGX
OperaNeon	Firefox
SlimBrowser	PaleMoon
Waterfox	Cyberfox
BlackHawk	IceCat
KMeleon	Thunderbird

Arkei Stealer is one of the most threatening types of malware for cryptocurrency holders, due to the vast list of crypto browser wallets the malware can compromise and steal user's assets from. Arkei steals these credentials by copying all the files stored in the browser's extension folder. For example, if the victim uses Google Chrome with a crypto browser wallet extension, the extension files will be stored in:

- C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\Extension ID from Google Store
- C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\ Extension ID from Google Store
- C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\Domain Name.indexeddb.leveldb

Arkei steals the data from the following crypto wallets:

Crypto browser wallet	Extension ID
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec
MetaMask	nkbihfbeogaeaoehlefnkodbefgpgknn
Binance Chain Wallet	fhbohimaelbohpjbbldcngcnapndodjp
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb
Nifty Wallet	jbdaocneiiinmjbjlgalhcelgbejmnid
Math Wallet	afbcbjpbpfadlkmhmclhkeeodmamcflc
Coinbase Wallet	hnfanknocfeofbddgcijnmhnfnkdnaad
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln
EQUA Wallet	blnieiiffboillknjnepogjhkgnoapac
Jaxx Liberty	cjelfplplebdjjenllpjcblmjkfcffne
BitApp Wallet	fihkakfobkmkjojpchpfgcmhfjnmnfpi
iWallet	kncchdigobghenbbaddojjnnaogfppfj
Wombat	amkmjjmmflddogmhpjloimipbofnfjih

MEW CX	nlbmnnijcnlegkjjpcfjclmcfggfefdm
GuildWallet	nanjmdknhkinifnkgdcggcfnhdaammmj
Saturn Wallet	nkddgncdjgjfcddamfgcmfnlhccnimig
Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec
NeoLine	cphhlgmgameodnhkjdmkpanlelnlohao
Clover Wallet	nhnkbkgjikgcigadomkphalanndcapjk
Liquality Wallet	kpfopkelmapcoipemfendmdcghnegimn
Terra Station	aiifbnbfobpmeekipheeijimdpnlpgpp
Keplr	dmkamcknogkgcdfhhbddcghachkejeap
Sollet	fhmfendgdocmcbmfikdcogofphimnkno
Auro Wallet	cnmamaachppnkjgnildpdmkaakejnhae
Polymesh Wallet	jojhfeoedkpkglbfimdfabpdfjaoolaf
ICONex	flpiciilemghbmfalicajoolhkkenfel
Nabox Wallet	nknhiehlklippafakaeklbeglecifhad
KHC	hcflpincpppdclinealmandijcmnkbgn
Temple	ookjlbkiijinhpmnjffcofjonbfbgaoc
TezBox	mnfifefkajgofkcjkemidiaecocnkjeh
Cyano Wallet	dkdedlpgdmmkkfjabffeganieamfklkm

Byone	nlgbhdfgdhgbiamfdfmbikcdghidoadd
OneKey	infeboajgfhgbjpjbeppbkgnabfdkdaf
LeafWallet	cihmoadaighcejopammfbmddcmdekcje
DAppPlay	lodccjjbdhfakaekdiahmedfbieldgik
BitClip	ijmpgkjfkbfhoebgogflfebnmejmfbml
Steem Keychain	lkcjlnjfpbikmcmbachjpdbijejflpcm
Nash Extension	onofpnbbkehpmmoabgpcpmigafmmnjhl
Hycon Lite Client	bcopgchhojmggmffilplmbdicgaihlkp
ZilPay	klnaejjgbibmhlephnhpmaofohgkpgkd
Coin98 Wallet	aeachknmefphepccionboohckonoeemg

The sample that we analyzed steals data pertaining to stored browser passwords and 2FA extensions such as:

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

This malware takes advantage of the fact that an increasing number of employees use their organizations' endpoints for day-to-day activities, such as online purchasing and cryptocurrency activities. Electronic wallets are becoming increasingly common, making it easier for end-users to expose the corporate network to external attacks.

Minerva Lab's Hostile Environment Simulation Module prevents Arkei Stealer from executing on the victim's PC, protecting the corporate network and user's private data.

IOC's:

Hashes:

388e833740f160ceb5946b7c5e89c5af08dde862a7dd38344149e72dea7ec00d – app59.exe

Domains:

https://thecowbook[.]com – C&C server

References:

https://blog.talosintelligence.com/2020/09/threat-roundup-0911-0918.html

https://anti-debug.checkpoint.com/techniques/debug-flags.html#using-win32-api-ntqueryinformationprocess