

Atomic Stealer rings in the new year with updated version

By Jérôme Segura

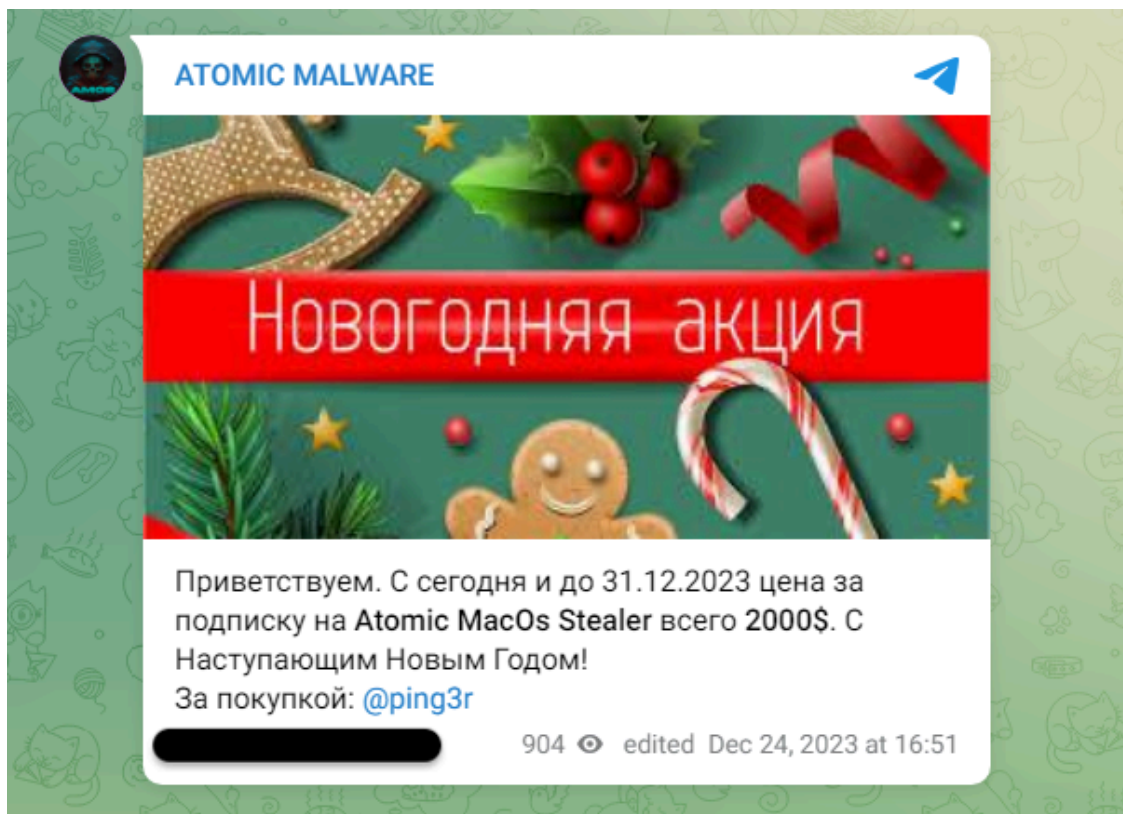
Published: 2024-01-10 · Archived: 2026-04-05 13:38:27 UTC

Last year, we documented [malware](#) distribution campaigns both via [malvertising](#) and [compromised sites](#) delivering Atomic Stealer (AMOS) onto Mac users. This stealer has proven to be quite popular in the criminal underground and its developers have been adding new features to justify its hefty \$3000/month rental fee.

It looks like Atomic Stealer was updated around mid to late December 2023, where its developers introduced payload encryption in an effort to bypass detection rules. Some samples from crack websites made their way to VirusTotal around that time frame, followed by a [malvertising](#) campaign we observed in January 2024.

In this blog post, we will review the latest changes with Atomic Stealer and the recent distribution with malicious ads via the Google search engine.

In December, Atomic Stealer ran a promotion via a post on their Telegram channel to offer a special holiday discount to their customers:



Welcome. From today until December 31, 2023, the price for a subscription to Atomic MacOs Stealer is only \$2000 . Happy New Year!

While the developers did not specifically advertise this feature, it appears that around December 17 Atomic Stealer had changed some of its code to hide certain strings that were previously used for detection and identifying its command and control server.

[Sample](#) with strings in clear text (Dec 12), showing for example the IP address for the malware's C2 server:

The image displays two side-by-side screenshots of the Malwarebytes Intelligence interface. Both samples have a 'Community Score' of 25/64 and are identified as 'Notion-3.0.1-universal' with tags for 'macho', '64bits', and 'multi-arch'. The left sample (Dec 12) shows the 'Strings' tab with the IP address '5.42.65.108' highlighted. The right sample (Dec 17) shows the 'Submissions' table with the IP address '5.42.65.108' highlighted in the 'Name' column.

Date	Name	Source
2023-12-12 18:27:05 UTC	Notion-3.0.1-universal	ae1:
2023-12-18 09:44:25 UTC	Notion-3.0.1-universal	3ad

```
runqueue= stopwait= runqsize= gfreecnt= throwing= spinning=atomicand8float64nanfloat32na  
complex128t.Kind == http2debugcrypto/tlssafari/saf1FileGrabber5.42.65.108nil contextsetn
```

Obfuscated [sample](#) (Dec 17), using a new encryption routine that hides strings of interest:

25 / 59

25 security vendors and no sandboxes flagged this file as malicious

06348fdbbac1ef5009b211fb73220f1074176d7a098724a6ddc0f7799a4b894

CrackInstaller

macho 64bits checks-hostname multi-arch arm

Community Score

DETECTION DETAILS

Strings Hex

decryptor

__ZZNK3\$_0c1EvE9decry
__ZGVZNK3\$_0c1EvE9dec
__ZZNK3\$_1c1EvE9decry
__ZGVZNK3\$_1c1EvE9dec
__ZZNK3\$_2c1EvE9decry
__ZGVZNK3\$_2c1EvE9dec
__ZZNK3\$_3c1EvE9decry
__ZGVZNK3\$_3c1EvE9decryptor
__ZZNK3\$_4c1EvE9decryptor
__ZGVZNK3\$_4c1EvE9decryptor
__ZZ10checkvalidNst3__112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEEES5_EN
__ZGVZZ10checkvalidNst3__112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEEES5_

25 / 59

25 security vendors and no sandboxes flag

06348fdbbac1ef5009b211fb73220f1074176d7a0

CrackInstaller

macho 64bits checks-hostname multi-arch

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTE

Submissions ⓘ

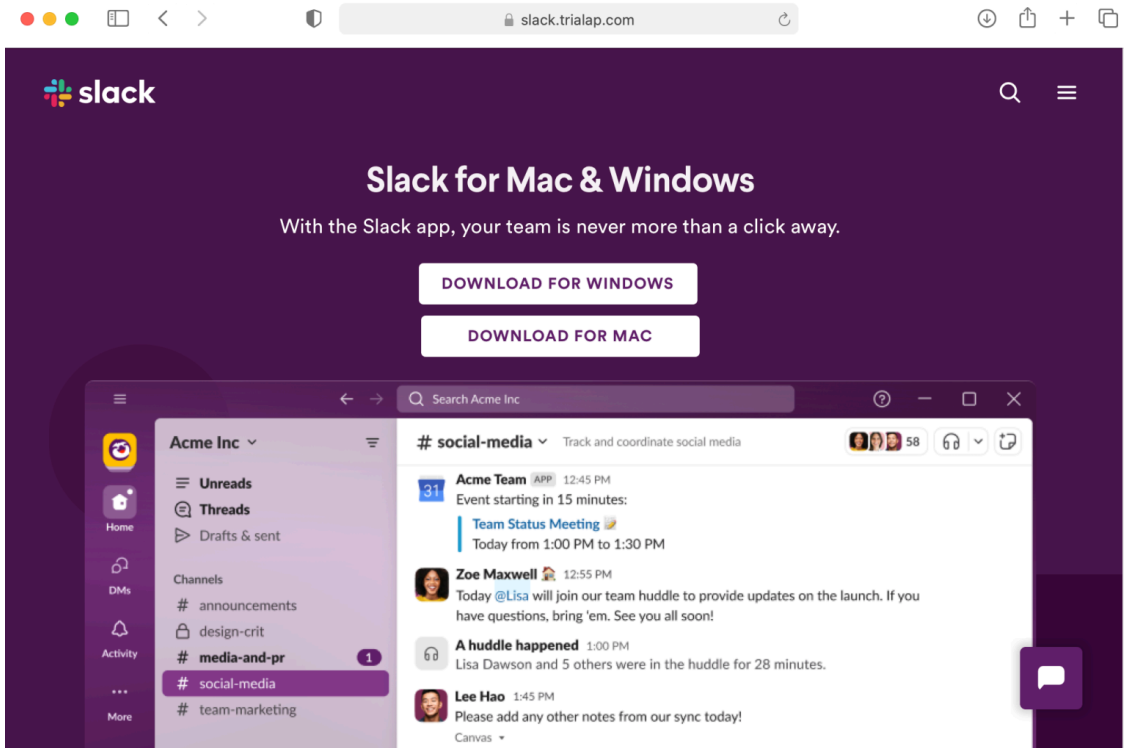
Date	Name
2023-12-17 19:39:43 UTC	/Volumes/CrackInstaller/CrackInstaller

Those two samples above also represent the different distribution channels that Atomic Stealer customers are using to distribute the malware. It's possible customers using software cracks got access to the update Atomic Stealer before those that leverage malicious ads.

In fact, during the holiday break, we noticed a decrease in malvertising activity, in particular for the campaigns running via Google search ads. This was somewhat expected and typically extends into early January. However, on January 8, we identified a malvertising campaign using similar tactics seen previously by threat actors distributing FakeBat. In this instance, there was also a payload destined for Mac users, Atomic Stealer in its updated version.

Malvertising with FakeBat – Atomic Stealer combo

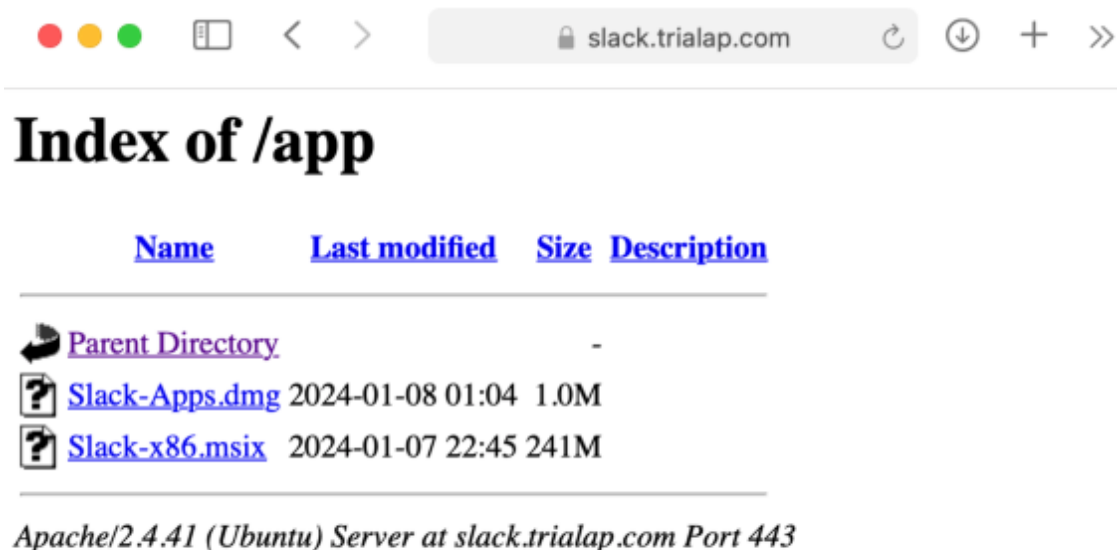
The threat actors are luring victims via a Google search ad impersonating Slack, the popular communication tool, and redirecting them to a decoy website where the app can be downloaded for both Windows and Mac:



The threat actors are leveraging tracking templates to filter traffic and route it through a few redirects before loading the landing page:

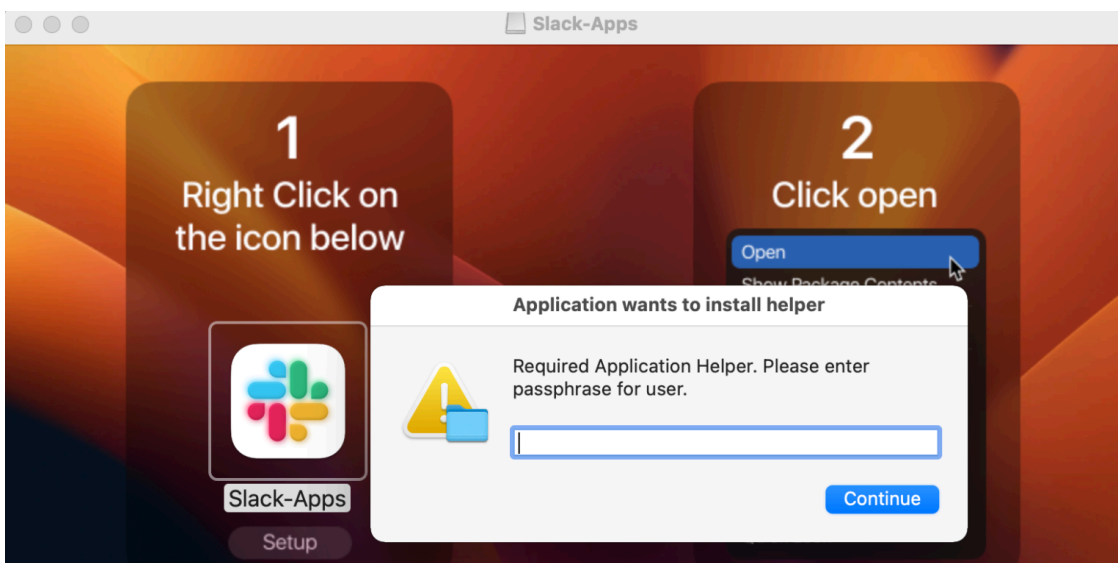
Host	URL
www.googleadservices.com	/pagead/adk?sa=L&ai=DChcSEwi5vKi46M6DAxUTDa0GHYAsA...
ivchlo.gotrackier.com	/click?campaign_id=2&pub_id=2&force_transparent=true&url...
ivchlo.gotrackier.com	/click?campaign_id=1&pub_id=2&
red.seecho.net	/
red.seecho.net	/
slack.trialap.com	/

On that same domain, there is an open directory showing the location of the Windows payload which is an MSI installer (FakeBat), and the Mac one, Atomic Stealer (AMOS):



Obfuscated Atomic Stealer

The malicious DMG file contains instructions for users to open the file as well as a dialog window asking them to enter their system password. This will allow Atomic Stealer to collect passwords and other sensitive files that are typically access-restricted.



When comparing the previous Atomic Stealer samples we have, we can see that the application code has changed. Previously, we could see certain strings revealing the nature of the payload (browsers, wallets, etc.) and more importantly the command and control server that receives stolen user data. Now, these strings are no longer visible as the code is well obfuscated:

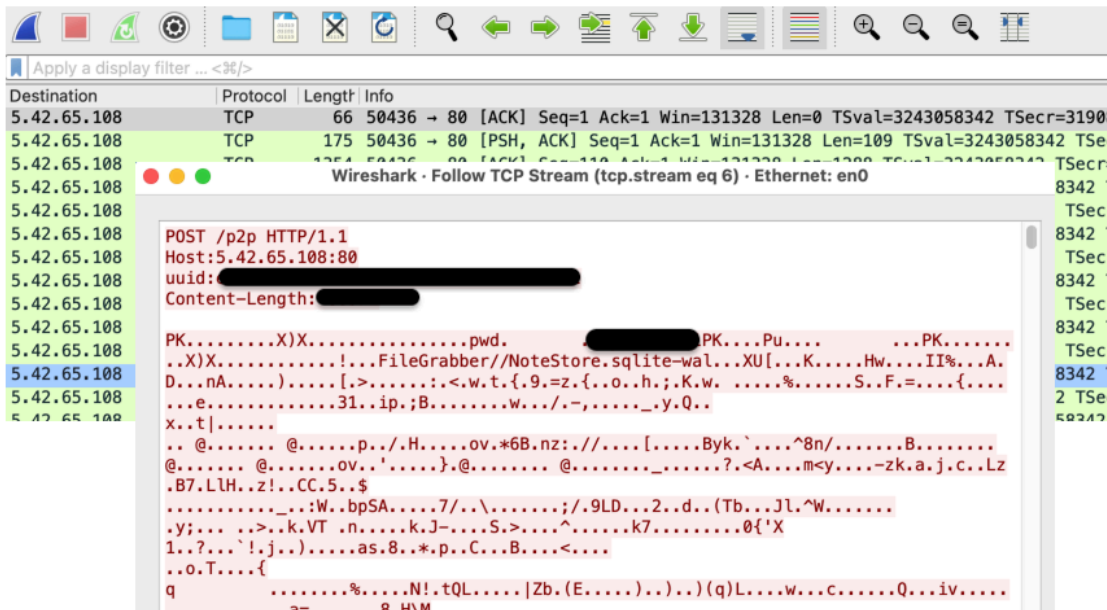
Before: strings can be seen in plain text

```
Application Support/ Google/Chrome/ BraveSoftware/Brave-Browser/ Microsoft
com.operasoftware.Opera/ com.operasoftware.OperaGX/ Chrome Brave Edge Viva
Cookies Login Data /Password Web Data /Autofill Local Extension Settings /M
/wallets/ Exodus/exodus.wallet/ /.walletwasabi/client/Wallets/ Guarda/Local
Coinomi Wasabi ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234567
185.106.93.154 BuildID= &user= &B64= Some error occurred while running... Er
ERROR] POST /sendlog HTTP/1.1
Host: 185.106.93.154
Content-Type: application
Content-Length:
basic_string vector USER
nil while unwrapping an
ocured while running the
"System:Library:CoreServ
/osascript -e
swift_getObjCClassMetao
swift_getExistentialTyp
wait cannot throw swift
failed with error 'as'
pthread_cond_init(&condi
pthread_cond_broadcast(&
pthread_mutexattr_settyp
pthread_mutex_destroy(&mu
pthread_mutex_trylock(&mu
```

After: strings are now encrypted

```
_ZGVZZ7passnetvENK4$ _87c1EvE9decryptor| _ZZZ7passnetvENK4$ _88c1EvE9decryptor| _ZGVZZ7passnetvE
_ZGVZZ7send_mePKcLS0_ENK4$ _89c1EvE9decryptor| _ZZZ7send_mePKcLS0_ENK4$ _90c1EvE9decryptor| _ZGV
_ZGVZZ7send_mePKcLS0_ENK4$ _91c1EvE9decryptor| _ZZZ7send_mePKcLS0_ENK4$ _91c1EvE9decryptor| _ZZZ
_ZGVZZ7send_mePKcLS0_ENK4$ _92c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK4$ _93c1EvE9decryptor| _Z
_ZGVZZ14ADSJASDKKAJDSJvENK4$ _94c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK4$ _94c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK4$ _95c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK4$ _96c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK4$ _97c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK4$ _97c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK4$ _98c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK4$ _99c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _100c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _100c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _101c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _102c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _103c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _103c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _104c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _105c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _106c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _106c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _115c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _115c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _116c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _117c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _118c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _118c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _119c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _120c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _121c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _121c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _122c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _123c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _124c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _124c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _125c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _126c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _127c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _127c1EvE9decryptor|
_ZGVZZ14ADSJASDKKAJDSJvENK5$ _128c1EvE9decryptor| _ZZZ14ADSJASDKKAJDSJvENK5$ _129c1EvE9decryptor|
_ZZZ14ADSJASDKKAJDSJvENK5$ _130c1EvE9decryptor| _ZGVZZ14ADSJASDKKAJDSJvENK5$ _130c1EvE9decryptor|
_ZZKNK3$ _0c1EvE9decryptor$tlv$init| _ZGVZKNK3$ _0c1EvE9decryptor$tlv$init| _ZZKNK3$ _1c1EvE9decrypt
_ZZKNK3$ _2c1EvE9decryptor$tlv$init| _ZGVZKNK3$ _2c1EvE9decryptor$tlv$init| _ZZKNK3$ _3c1EvE9decrypt
```

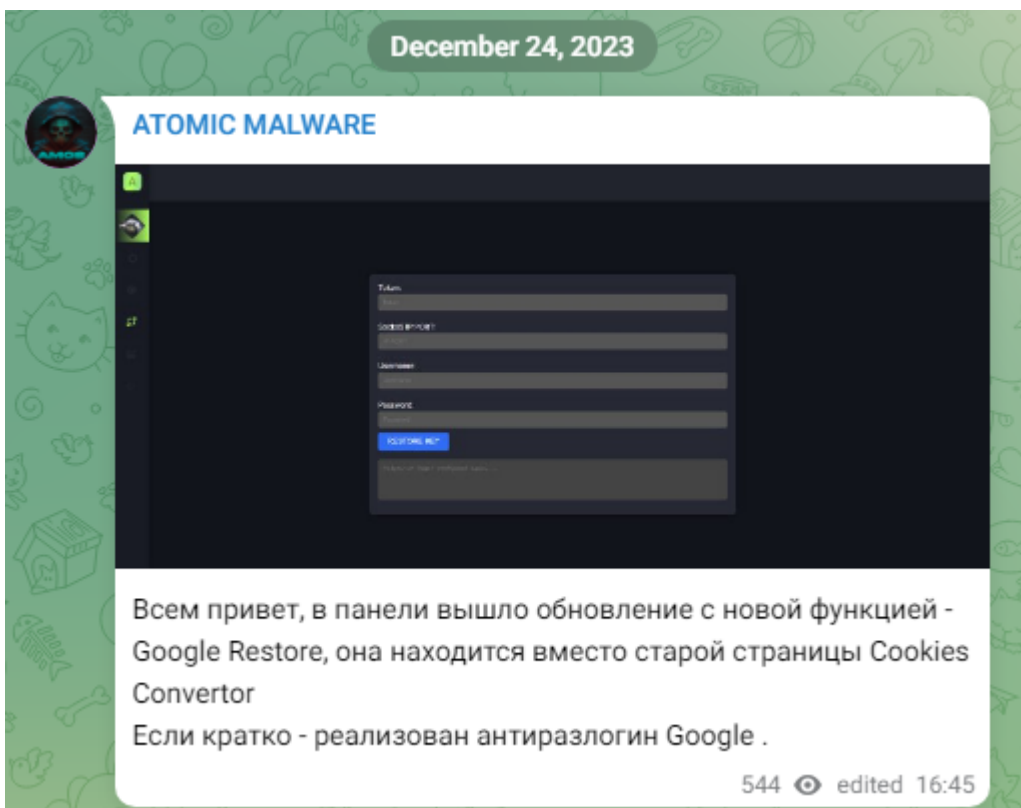
When we analyzed this sample in a sandbox we saw the data exfiltration taking place and the corresponding C2 server:



Stealing victim passwords, crypto wallets and cookies

As detailed in Objective-See's [The Mac Malware of 2023](#), stealers were the most popular type of malware. It's not just passwords that are of interest to cyber criminals. Stealing browser cookies can sometimes be even better than having the victim's password, enabling authentication into accounts via [session tokens](#).

In fact, Atomic Stealer developers were working on a cookie feature they announced on Christmas Eve:

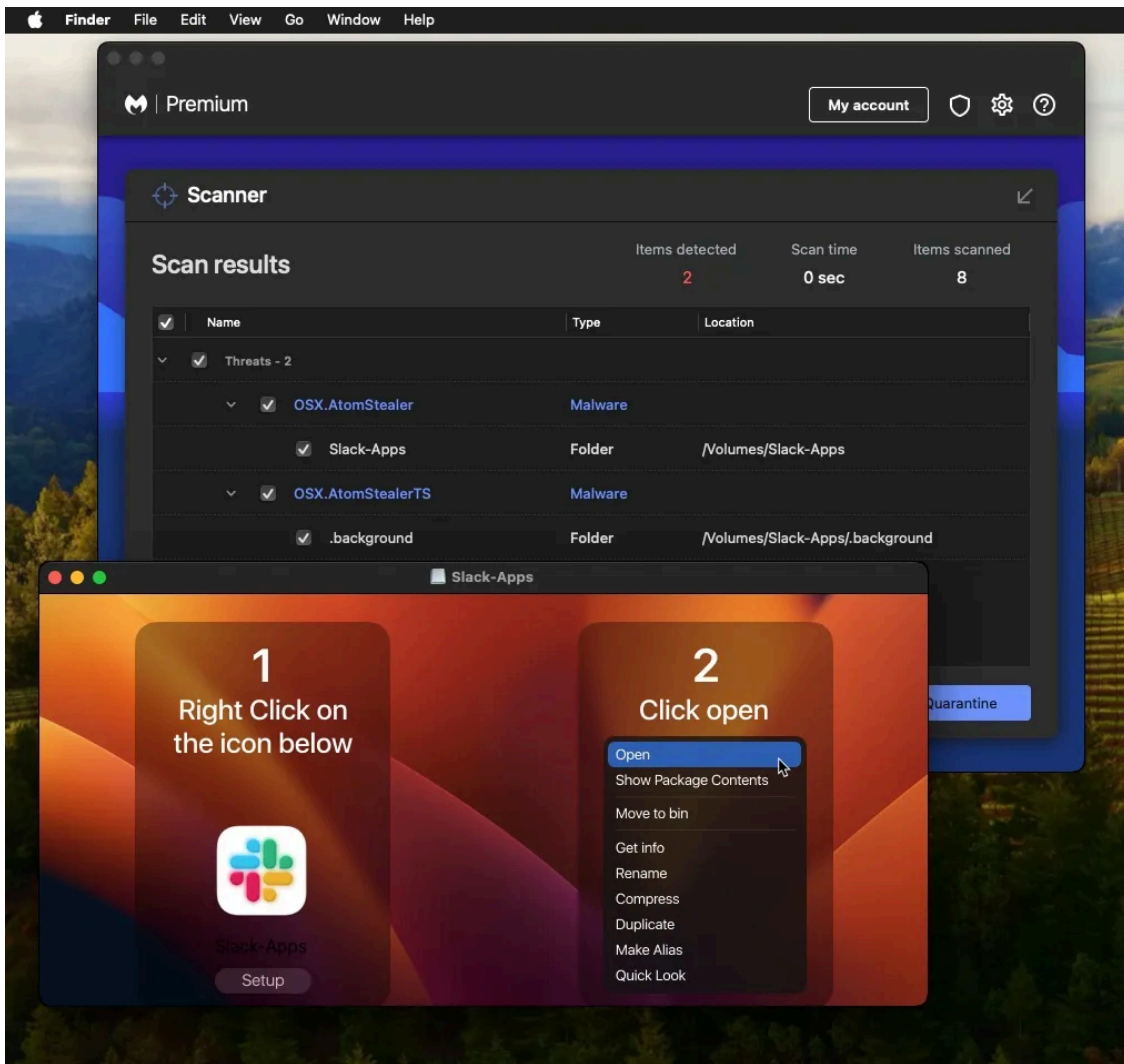


Hi everyone, the panel has released an update with a new feature – Google Restore, it is located instead of the old page Cookies Convertor. In brief – implemented anti-unlogin Google.

As stealers continue to be a top threat for Mac users, it is important to download software from trusted locations. Malicious ads and decoy sites can be very misleading though and it only takes a single mistake (entering your password) for the malware to collect and exfiltrate your data.

We have reported the malicious ad and infrastructure to the respective parties for mitigation.

To stay safe from this and other similar threats, a combination of web protection and antivirus is best suited. [Malwarebytes Browser Guard](#) and [Antivirus for macOS](#) can prevent and detect Atomic Stealer.



Indicators of Compromise

Malvertising chain

```
ivchlo[.]gotrackier[.]com  
red[.]seecho[.]net
```

Decoy site

```
slack[.]trialap[.]com
```

FakeBat payload URL

```
slack[.]trialap[.]com/app/Slack-x86.msix
```

FakeBat hash

```
49f12d913ad19d4608c1596cf24e7b6ffff14975418f09e2c1ad37f231943fda3
```

FakeBat C2

```
ads-strong[.]online
```

Atomic Stealer payload URL

```
slack[.]trialap[.]com/app/Slack-Apps.dmg
```

Atomic Stealer hash

```
18bc97e3f68864845c719754d2d667bb03f754f6e87428e33f9c763a8e6a704a
```

C2

```
5.42.65[.]108
```

Source: <https://www.malwarebytes.com/blog/threat-intelligence/2024/01/atomic-stealer-rings-in-the-new-year-with-updated-version>