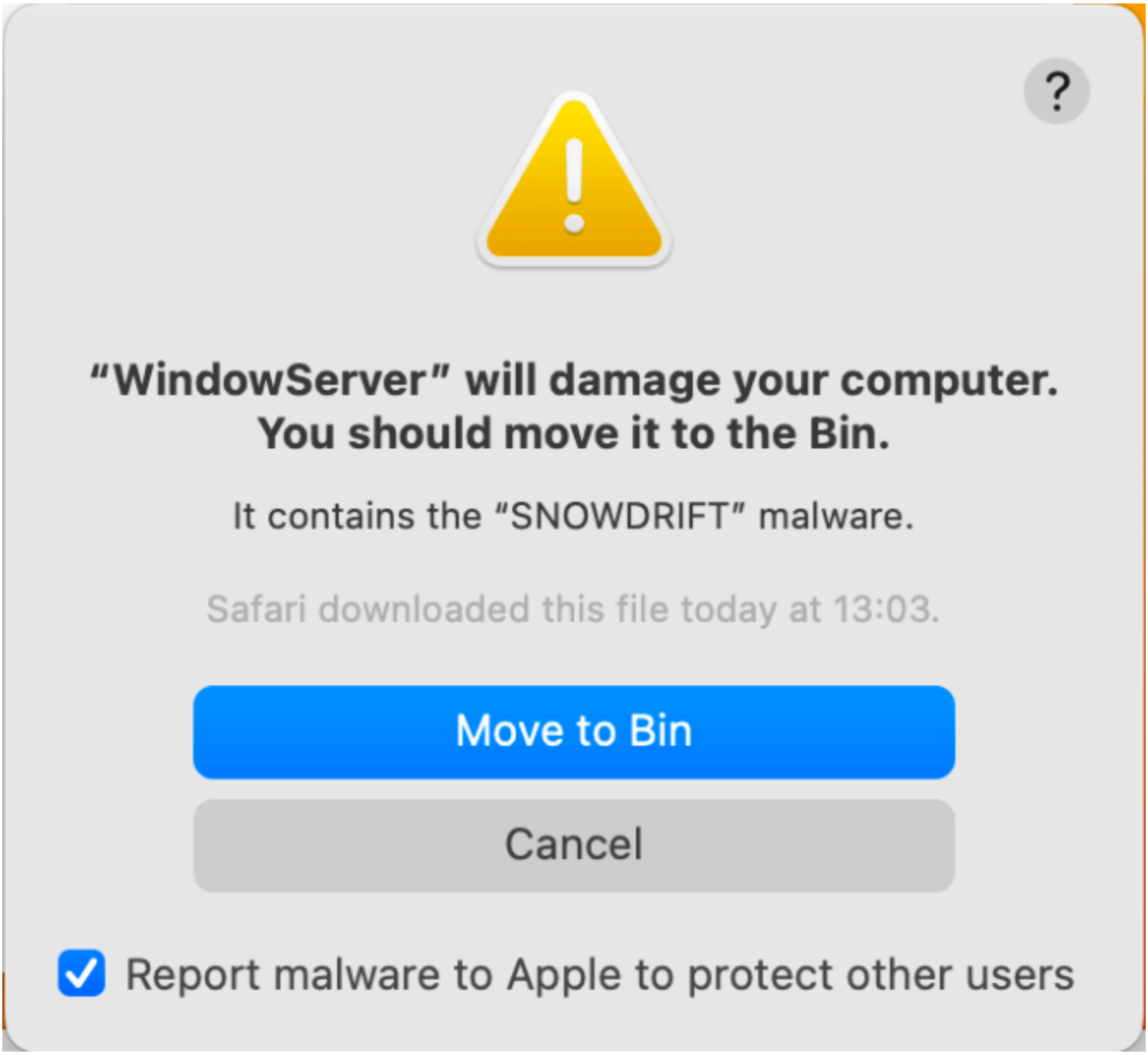
THE ECLECTIC LIGHT COMPANY

MACS, PAINTING, AND MORE

hoakley / January 3, 2023 / Macs, Technology

Can you rely on macOS Ventura for malware protection?



“WindowServer” will damage your computer.
You should move it to the Bin.

It contains the “SNOWDRIFT” malware.

Safari downloaded this file today at 13:03.

☑ Report malware to Apple to protect other users

It’s one of the commonest questions I’m asked: can an ordinary Mac user now rely on the security protection provided by macOS Ventura, or do they need third-party extras? The correct answer is that it depends on your security risk assessment, but you also need to know how effective macOS protection is, and where its weaknesses are. In this article I set out to assess how good Ventura 13.1 is when confronted with real malware.

Methods

To investigate this, I prepared three Ventura 13.1 virtual machines, each with different security configurations:

- Apple silicon Full Security mode, with all standard security protection enabled;
- Permissive Security set in Recovery mode, with System Integrity Protection (SIP) disabled;
- Permissive Security with SIP disabled, and the security assessment policy subsystem disabled using `spctl --global-disable`.

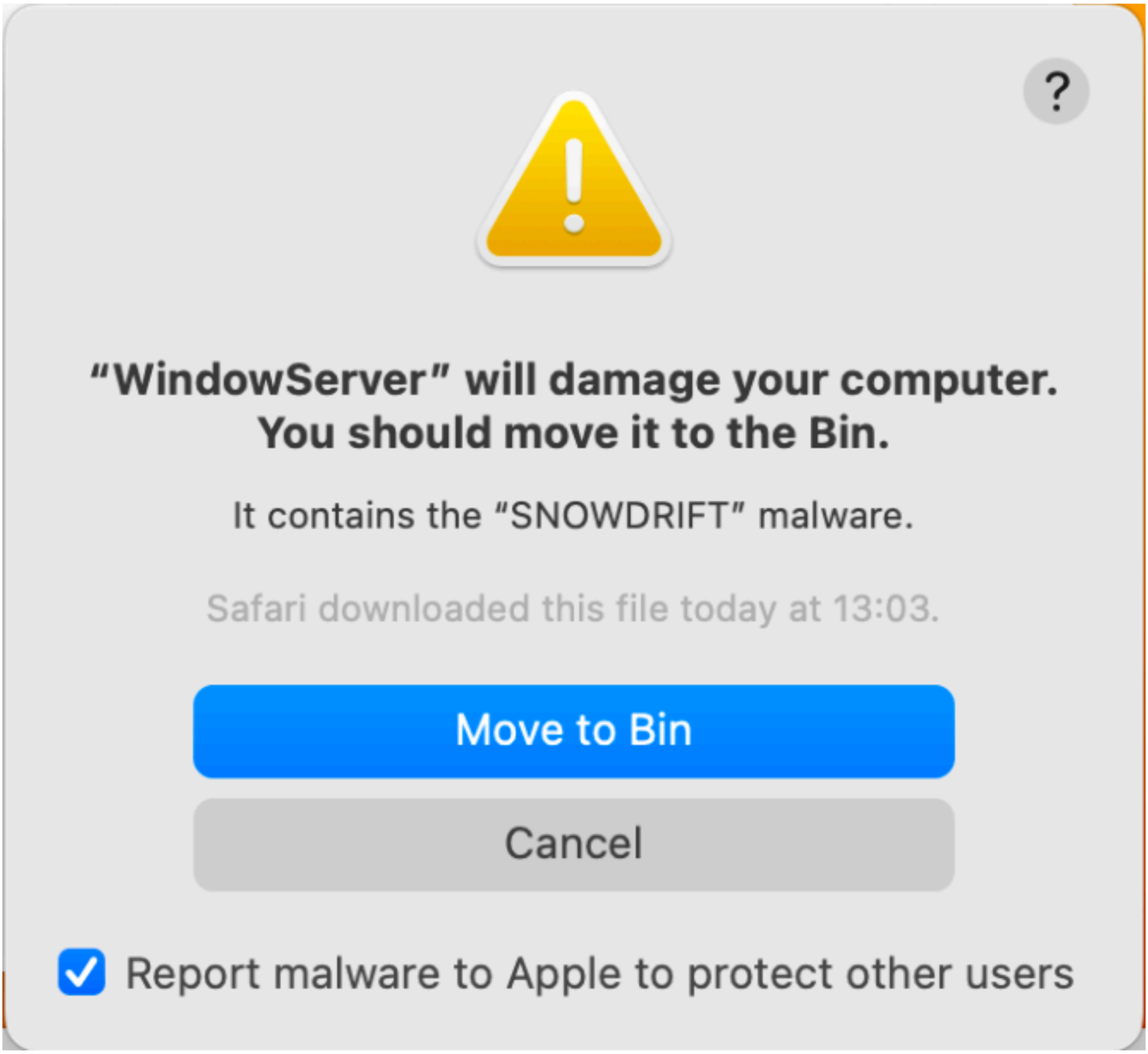
Settings were confirmed by checking each with SilentKnight, and all tests were virtualised using sandboxed ViableS locked down in isolation from the host Mac Studio M1 Max. Because the malware samples include x86 executables, Rosetta 2 was installed on each VM before testing started.

Samples tested included DazzleSpy, SysJoker, CloudMensis (known by Apple as SnowDrift) and XCSSET (identified by Apple as DubRobber A). As some of the samples lacked an effective installer, and macOS 13.1 has patched most if not all the vulnerabilities they relied on to install successfully, only the XCSSET and DazzleSpy samples appeared able to run and at least partially install themselves. To further aid the malware, tests were also run in each VM with the quarantine flag stripped from Zip archives.

Results

Full Security

Running with full security enabled, macOS successfully recognised and blocked the samples of CloudMensis and XCSSET, whether or not a quarantine flag was set.

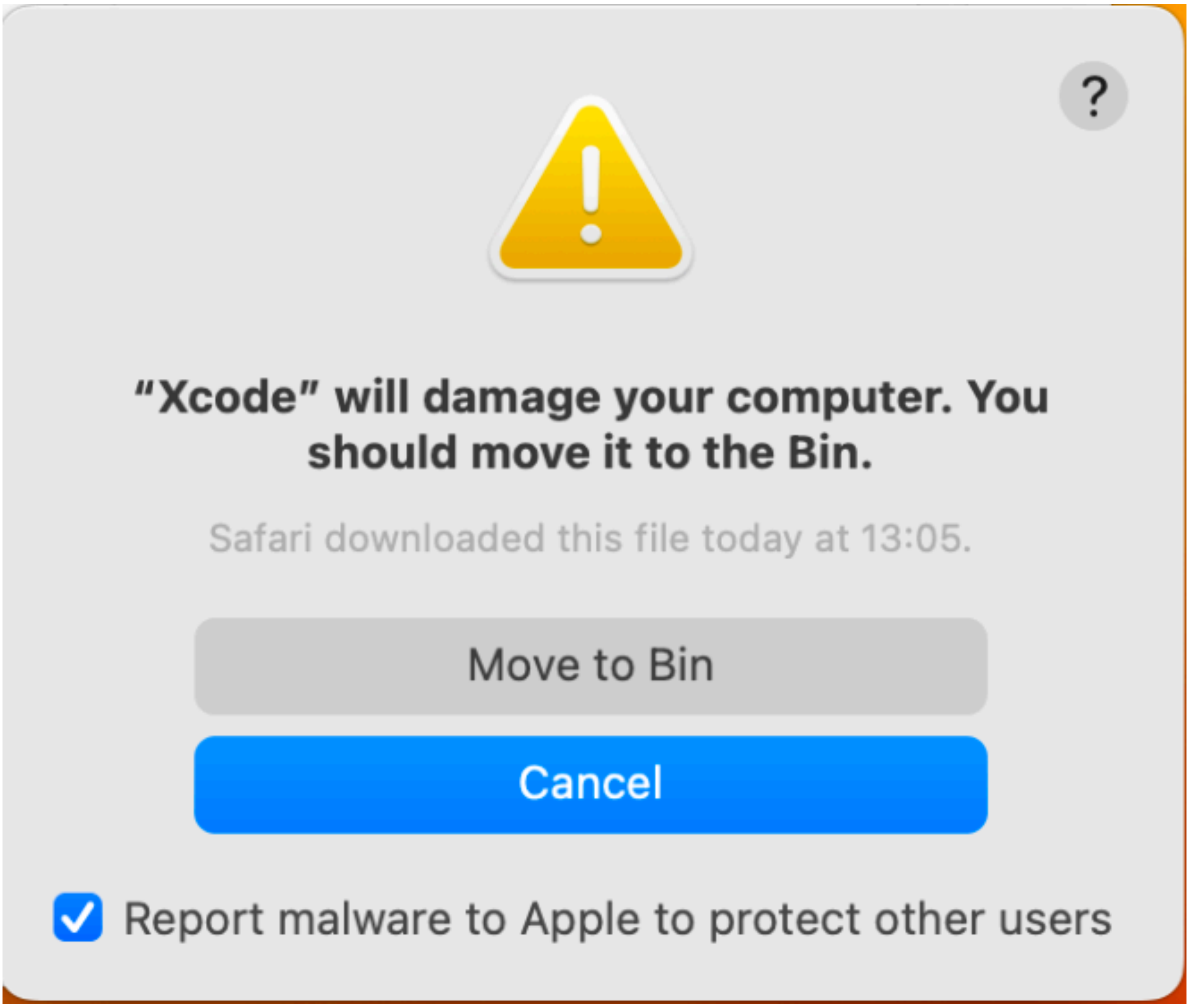


"WindowServer" will damage your computer. You should move it to the Bin.

It contains the "SNOWDRIFT" malware.

Safari downloaded this file today at 13:03.

Trying to run the malicious WindowServer component in CloudMensis left the user in no doubt that it was malicious, and gave no option to bypass the block.

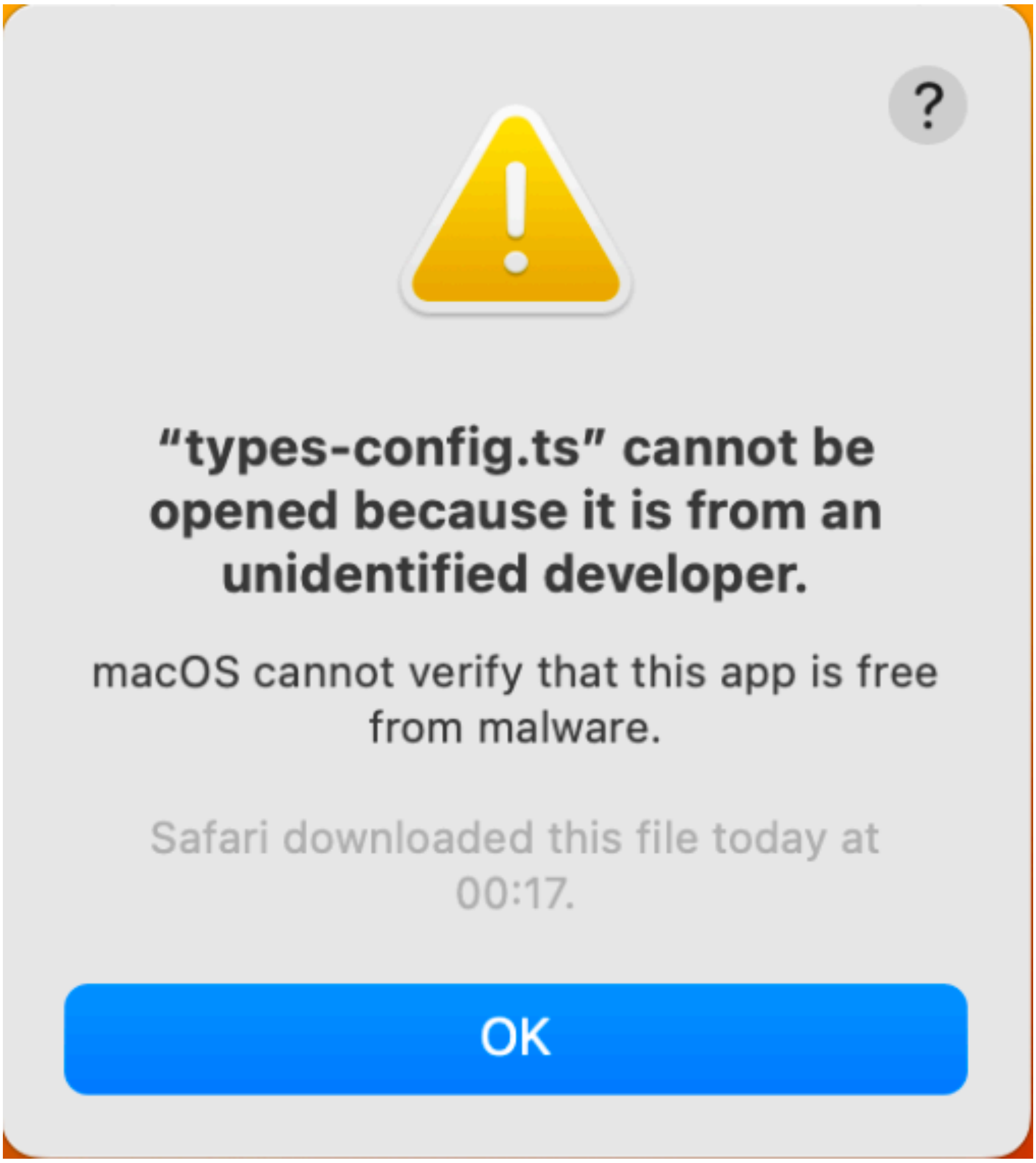


“Xcode” will damage your computer. You should move it to the Bin.

Safari downloaded this file today at 13:05.

☑ Report malware to Apple to protect other users

Although in this configuration, the malicious Xcode app in XCSSET wasn’t specifically identified, it was recognised as malicious and blocked effectively.

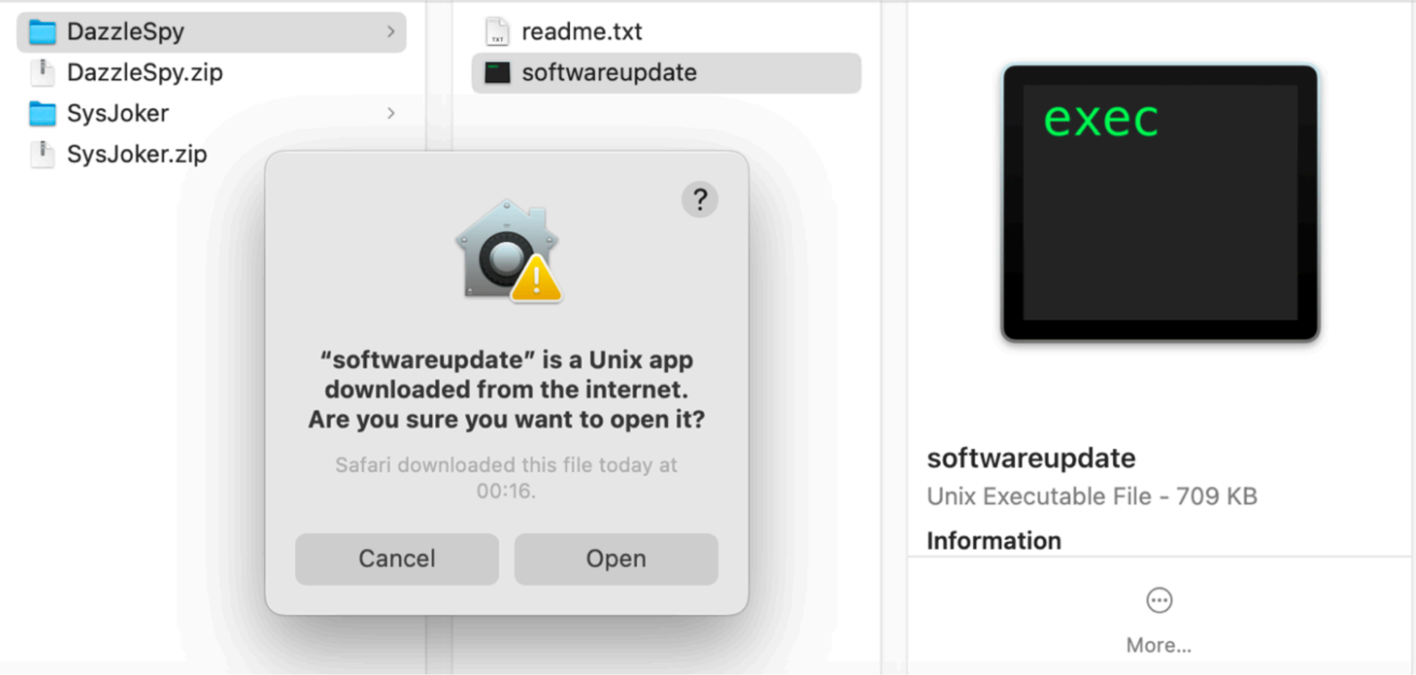


“types-config.ts” cannot be opened because it is from an unidentified developer.

macOS cannot verify that this app is free from malware.

Safari downloaded this file today at 00:17.

SysJoker’s bogus MPEG-2 Transport Stream was blocked from being run in QuickTime Player, although the determined user could bypass that, and it wasn’t identified as being malicious.



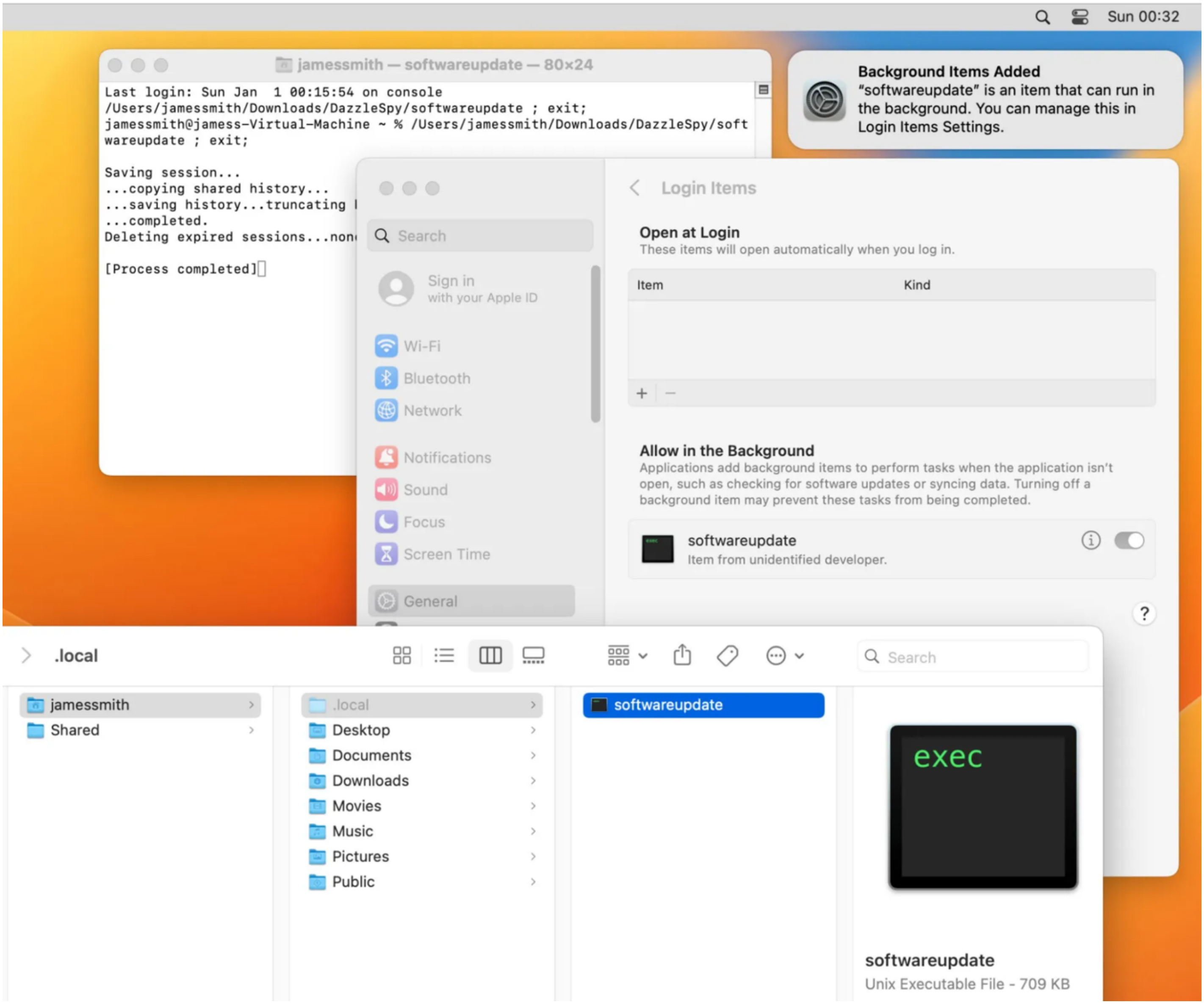
"softwareupdate" is a Unix app downloaded from the internet. Are you sure you want to open it?

Safari downloaded this file today at 00:16.

softwareupdate

Unix Executable File - 709 KB

The only warning given on DazzleSpy's malicious `softwareupdate` was uncommitted, and left the user with the option to open it. If they chose to proceed, it successfully installed itself in its hidden folder at ~/.local, installed its property list in ~/Library/LaunchAgents for persistence, and macOS automatically added it to System Settings > General > Login Items, although it was left to the user to enable it.



```
Last login: Sun Jan  1 00:15:54 on console
/Users/jamessmith/Downloads/DazzleSpy/softwareupdate ; exit;
jamessmith@jamess-Virtual-Machine ~ % /Users/jamessmith/Downloads/DazzleSpy/soft
wareupdate ; exit;

Saving session...
...copying shared history...
...saving history...truncating
...completed.
Deleting expired sessions...non

[Process completed]
```

Background Items Added
"softwareupdate" is an item that can run in the background. You can manage this in Login Items Settings.

Open at Login
These items will open automatically when you log in.

Item	Kind

Allow in the Background
Applications add background items to perform tasks when the application isn't open, such as checking for software updates or syncing data. Turning off a background item may prevent these tasks from being completed.

softwareupdate
Item from unidentified developer.

softwareupdate
Unix Executable File - 709 KB

With decompressed samples of malware in ~/Documents, XProtect Remediator scans didn't result in any reports of suspicious software. However, moving the malicious Xcode app from XCSSET into the /Applications folder was detected and remediated by its deletion.

SIP disabled

This introduced several subtle but significant differences from Full Security, making it less difficult to run malicious code, but also changing XProtect Remediator scans.

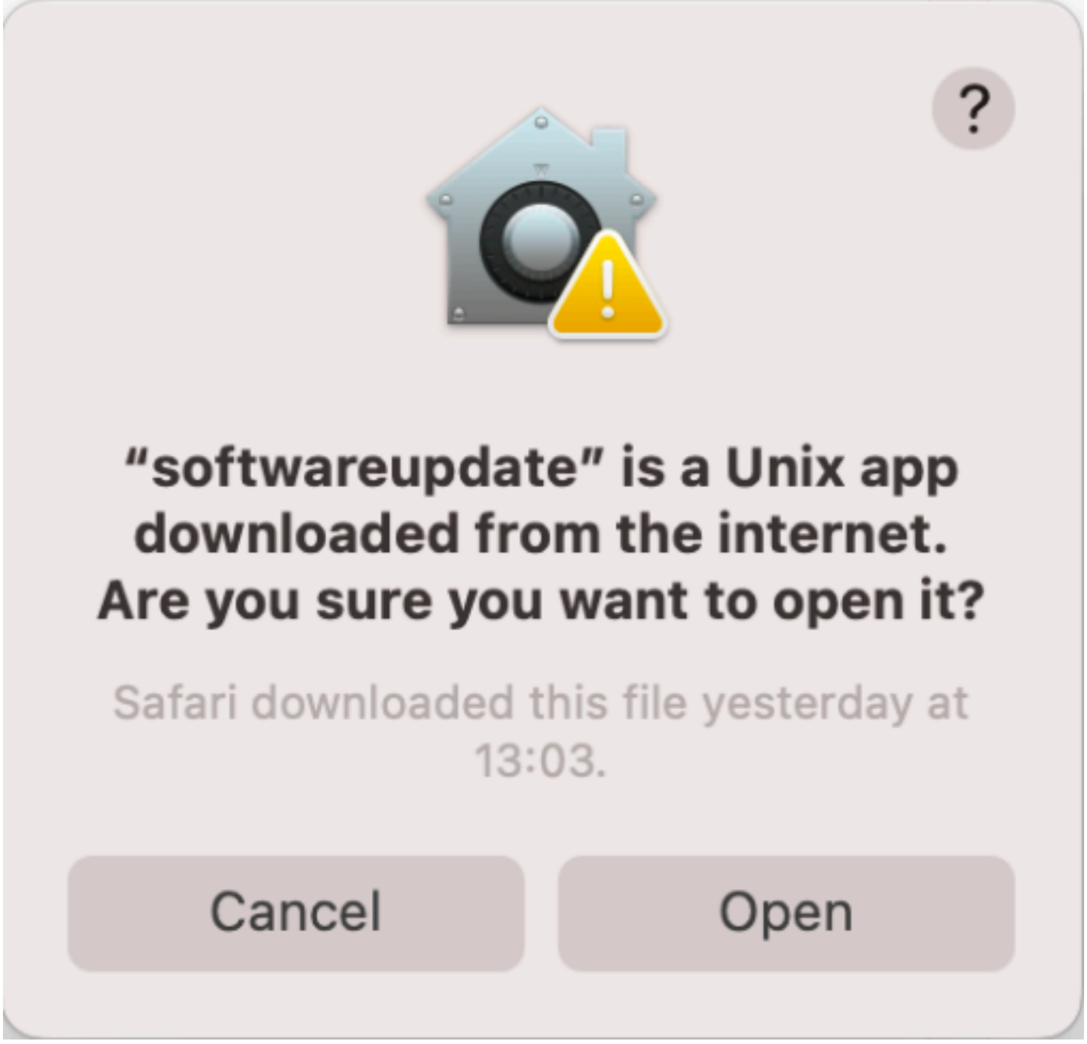
The bogus Xcode app in XCSSET was still successfully blocked, but here it was identified as containing MACOS.2070d41 malware, also known by Apple as DubRobber A. It could also be run after stripping its quarantine flag, using the bypass technique of the Finder's Open command, which was blocked when in Full Security. When its quarantine flag had been stripped, SysJoker's malicious MPEG-2 Transport Stream was opened and run in QuickTime Player without any warning being shown.

More disturbingly, when macOS installed DazzleSpy's malicious softwareupdate as a Login Item, it was *enabled* by default. For a relatively new protection against a well-known method of achieving persistence, that's a worrying side-effect of disabling SIP.

As if to compensate, XProtect Remediator's scans appeared more extensive in their coverage. The malicious WindowServer code in CloudMensis was detected and reported when still in ~/Downloads and ~/Documents folders, and DubRobber was both detected and remediated successfully from ~/Documents.

SIP and XProtect disabled

Disabling the security assessment policy subsystem removed most warnings when trying to run malicious software. In most cases, the user was presented with a neutral choice to be made, as to whether the malware should be opened.



"softwareupdate" is a Unix app downloaded from the internet. Are you sure you want to open it?

Safari downloaded this file yesterday at 13:03.

The only exception to that was when trying to run the malicious Xcode app in XCSSET, which still resulted in blocking with the warning that it contained MACOS.2070d41 malware, although that could be bypassed by stripping the quarantine flag and using the Finder's Open command.

XProtect Remediator scans behaved the same as those performed with SIP turned off, detecting WindowServer, and detecting and remediating DubRobber.

Does macOS security protection work?

The effectiveness of the security protection built into current macOS depends on security settings, the malware itself, and the user. With Full Security in force, the only one of the four samples of malware that macOS didn't block effectively was DazzleSpy. Although that ran and installed without warning, which could have given it persistence, it was left disabled by default.

DazzleSpy is relatively recent malware, and might not present any threat to Mac users who keep their macOS up to date. There has been a lack of detections in the wild, and researchers believe that it may depend on two vulnerabilities that were both fixed in macOS 11.2. Although SysJoker could be opened in QuickTime Player, none of the VMs showed any evidence of its malicious activity, so it too may no longer present any threat to current macOS.

It's also significant that, with full security protection active in macOS 13.1, stripping quarantine flags didn't affect detection or blocking of the malware samples. In the past, when Gatekeeper checks were more dependent on the presence of a quarantine flag, methods of avoiding the flag being attached, or of removing it, could bypass most protection. Reducing reliance on quarantine flags makes it significantly harder to install and run malicious software.

Each step away from full security protection reduced the chances of these malware samples being detected and blocked by macOS. The effects of disabling SIP were particularly complex and pervasive. For XCSSET, for instance, it gave the user the opportunity to run its malicious app using a well-known method for bypassing security protection. I suspect that many who disable SIP are unaware of these sinister effects: it's easy to assume that the robust protection provided by the SSV makes SIP less important to Macs running Big Sur and later.

XProtect Remediator plays an important role in detecting and removing some types of known malware. It relies on heuristics for efficiency, for example minimising the folders it scans, and scan frequency. For much of last summer it ran multiple checks for DubRobber each day, but those have now reduced in frequency, presumably because of a reduction in Apple's assessment of its threat.

For all malware, the most dangerous period is that between its release and spread, and the release of effective countermeasures, including the patching of exploited vulnerabilities and updates to XProtect and XProtect Remediator. Apple is expected to address the first of those with Rapid Security Responses (RSRs), and for much of the latter half of last year released updates to XProtect Remediator every two weeks. It remains to be seen how they will cope with a major increase in threat from novel malware.

I haven't considered reporting and monitoring in this article; I'll look at those separately tomorrow.

Conclusions

- When the *current* release of macOS is run with *Full Security* protection enabled, it provides a good level of protection against known malware, which should be sufficient for most users, in accordance with their risk assessments.
- Many factors reduce the effectiveness of macOS security, including running an older version of macOS, disabling SIP, disabling XProtect, and high-risk user behaviour such as using known bypasses, inattention, and clicking through warnings.
- Effective security in Ventura is much less dependent on quarantine. In the past, removing a quarantine flag could enable known malware to run freely. That's no longer the case in Ventura.
- Ventura, XProtect Remediator and RSR security updates have yet to be tested by a major increase in threat.

Malware samples used were made available to researchers by the Objective-See Foundation. I'd like to thank the Foundation and Patrick Wardle in particular for their generous help.

Posted in Macs, Technology and tagged Gatekeeper, macOS 13, malware, quarantine, security, SIP, Ventura, XProtect. Bookmark the permalink.

17 Comments Add yours

omnishopapp on January 3, 2023 at 8:32 am Reply ★ Liked by 1 person

Great comparison!
It would be great if they could improve the messages for the ordinary user.

2

hoakley on January 3, 2023 at 10:12 am Reply ★ Liked by 1 person

Thank you.
That's a topic I cover in tomorrow's article. I had intended including it here, but this article would then have become too long.
Howard.

Maurizio on January 3, 2023 at 8:51 am Reply ★ Liked by 1 person

Hello , its me again 🙂 . Do you rely on third party meta antivirus like https://www.virustotal.com to scan macos binary ? do you think that antivirus vendor (mostly know on windows platform) have enough feedback on macos environment to be considered efficient?

sometime i have to use some precompiled binary (mostly posix port from homebrew https://mirrors.xtom.ee/homebrew-bottles/ tool like rsync , xztool etc), not notarized from an established developer , i rely on the metascan to decide if are safe or not. I am I naive ? 🙂

4

hoakley on January 3, 2023 at 10:04 am Reply ★ Like

No, I don't usually use VirusTotal, neither do I use commercial anti-malware products, although I do use Objective-See's tools.
If a binary has been properly signed and notarized, then it should be good to run on the current version of macOS. Yes, some malware has been notarised, but as soon as it's detected, Apple revokes its notarization and signing certificate.
Howard.

Alan B on January 3, 2023 at 9:48 am Reply ★ Liked by 1 person

I've read that there are no true macOS runnable viruses and that the AV products aimed at the Mac market just scan for Windows viruses. I've no idea whether that's true but surely it's not necessarily a bad thing given that maybe a Mac could be a carrier for such viruses and hence pass them onto Windows machines. As for malware in general, are the third party AW apps such as MalwareBytes any more capable at detection than what Ventura now offers?

6

hoakley on January 3, 2023 at 10:11 am Reply ★ Liked by 1 person

Thank you.
The article above demonstrates that there is macOS malware that can be run, and will install itself. This has been well documented for plenty of malicious software now. Both Apple's protection (including XProtect and XProtect Remediator) and third-party products scan for, detect and can remove macOS malware.
As I have no problem with the results obtained in Full Security running the current macOS, I don't see any personal need for a third-party product here, although I do use Objective-See's security tools sometimes. However, this all depends on your personal risk assessment. For some, Windows malware may be an important consideration, something I don't feel able to assess.
Howard.

7

Alan B on January 3, 2023 at 10:34 am Reply ★ Liked by 1 person

I fully accept there is runnable macOS malware out there and I hope you don't think I was challenging that. Like you, I don't use any use commercial anti-malware products. However I've just started using one of Objective-See tools (BlockBlock). You can't be too careful! On the rare occasions I've used VirusTotal, it seemed to produce what looked like false positives so it's a no-no now.

Andy J on January 3, 2023 at 1:14 pm Reply ★ Liked by 1 person

Happy New Year and Thank You for another well-conceived and executed demonstration.

I'd be interested to see if the results are similar when tested in the other two "current" macOS releases: 12.6.2 and 11.7.2

I'm pressing our users toward running the latest major release available for their assigned hardware and meeting a good amount of resistance from those that prefer the status quo.

9

hoakley on January 3, 2023 at 3:19 pm Reply ★ Like

Thank you, and Happy New Year.
Sadly, it's not possible to run Big Sur in such a locked-down lightweight VM, although you can run it on Intel models using VMware or Parallels. Perhaps the biggest differences between 13 and 12.6.2 are that quarantine flags are more important in Monterey, and that 12.6.2 has far fewer vulnerabilities addressed, and always will do. Whether either of those would affect these specific outcomes, I don't know, but they would for some malware.
Howard.

piattj on January 3, 2023 at 2:28 pm Reply ★ Liked by 1 person

Hi Howard… did the Objective-See tools feature in your tests? I guess not, given this was a test of native macOS antimalware abilities, but is there any scope for a repeat of the tests herein reported but with Objective-See tools in play?
Like you I have stopped using a third party AV suite (I was using Bitdefender for mac) and rely on native macOS + Objective-See to minimise malware risk.
Thanks for an always-illuminating blog…

11

hoakley on January 3, 2023 at 3:21 pm Reply ★ Like

Thank you.
No, I didn't intend to try assessing third-party protection, although I think Objective-See tools are invaluable. If you want or need both belt and braces, then something like BlockBlock should be ideal.
Howard.

Richard on January 3, 2023 at 4:05 pm Reply ★ Liked by 1 person

This post is just a quick note for readers who may not use SilentKnight that SK's report screen gives an update of one's M1 Mac's security settings. It's a nice shortcut rather than restarting with the power button held down, etc. Thanks for SK–it's a great tool. And Happy New Year!

13

hoakley on January 3, 2023 at 4:35 pm Reply ★ Like

Thank you. Happy New Year!
Howard.

antbee on January 3, 2023 at 6:41 pm Reply ★ Liked by 1 person

Happy New Year Howard!
Thank you for this very important and informative article!

15

hoakley on January 3, 2023 at 8:16 pm Reply ★ Like

Thank you. Happy New Year too!
Howard.

AndyB on January 4, 2023 at 2:08 am Reply ★ Liked by 1 person

Thank you Howard for such a comprehensive answer to the question I asked on a previous thread. It seemed a simple question but evidently required significant work by you to provide such very useful results.
A very Happy New Year to you.

17

hoakley on January 4, 2023 at 7:48 am Reply ★ Liked by 1 person

Thank you.
Happy New Year!
Howard.

Leave a Reply

Enter your comment here...

Quick Links

Downloads

Mac Troubleshooting Summary

M1 & M2 Macs

Mac problem-solving

Painting topics

Painting

Long Reads

Search

Search Search

Monthly archives

January 2023 (41)

December 2022 (74)

November 2022 (72)

October 2022 (76)

September 2022 (72)

August 2022 (75)

July 2022 (76)

June 2022 (73)

May 2022 (76)

April 2022 (71)

March 2022 (77)

February 2022 (68)

January 2022 (77)

December 2021 (75)

November 2021 (72)

October 2021 (75)

September 2021 (76)

August 2021 (75)

July 2021 (75)

June 2021 (71)

May 2021 (80)

April 2021 (79)

March 2021 (77)

February 2021 (75)

January 2021 (75)

December 2020 (77)

November 2020 (84)

October 2020 (81)

September 2020 (79)

August 2020 (103)

July 2020 (81)

June 2020 (78)

May 2020 (78)

April 2020 (81)

March 2020 (86)

February 2020 (77)

January 2020 (86)

December 2019 (82)

November 2019 (74)

October 2019 (89)

September 2019 (80)

August 2019 (91)

July 2019 (95)

June 2019 (88)

May 2019 (91)

April 2019 (79)

March 2019 (78)

February 2019 (71)

January 2019 (69)

December 2018 (79)

November 2018 (71)

October 2018 (78)

September 2018 (76)

August 2018 (78)

July 2018 (76)

June 2018 (77)

May 2018 (71)

April 2018 (67)

March 2018 (73)

February 2018 (67)

January 2018 (83)

December 2017 (94)

November 2017 (73)

October 2017 (86)

September 2017 (92)

August 2017 (69)

July 2017 (81)

June 2017 (76)

May 2017 (90)

April 2017 (76)

March 2017 (79)

February 2017 (65)

January 2017 (76)

December 2016 (75)

November 2016 (68)

October 2016 (76)

September 2016 (78)

August 2016 (70)

July 2016 (74)

June 2016 (66)

May 2016 (71)

April 2016 (67)

March 2016 (71)

February 2016 (68)

January 2016 (90)

December 2015 (96)

November 2015 (103)

October 2015 (119)

September 2015 (115)

August 2015 (117)

July 2015 (117)

June 2015 (105)

May 2015 (111)

April 2015 (119)

March 2015 (69)

February 2015 (54)

January 2015 (39)

Tags

APFS Apple AppleScript Apple silicon backup Big Sur Blake bug Catalina Consolation Console diagnosis Disk Utility Doré El Capitan extended attributes Finder firmware Gatekeeper Gérôme HFS+ High Sierra history of painting iCloud Impressionism iOS landscape LockRattler log logs M1 Mac Mac history macOS macOS 10.12 macOS 10.13 macOS 10.14 macOS 10.15 macOS 11 macOS 12 macOS 13 malware Mojave Monet Monterey Moreau MRT myth narrative OS X Ovid painting Pissarro Poussin privacy realism Renoir riddle Rubens Sargent scripting security Sierra SilentKnight SSD Swift symbolism Time Machine Turner update upgrade Ventura xattr Xcode XProtect

Statistics

13,637,413 hits

About & Contact • Macs • Painting • Language • Tech • Life • General • Downloads • Mac problem-solving • Extended attributes (xattrs) • Painting topics • Hieronymus Bosch • English language • LockRattler: 10.12 Sierra • LockRattler: 10.13 High Sierra • LockRattler: 10.11 El Capitan • Updates: El Capitan • Updates: Sierra, High Sierra, Mojave, Catalina, Big Sur • LockRattler: 10.14 Mojave • SilentKnight, silnite, LockRattler, SystHist & Scrub • DelightEd & Podofyllin • xattred, Metamer, Sandstrip & xattr tools • 32-bitCheck & ArchiChect • T2M2, Ulbow, Consolation and log utilities • Cirrus & Bailiff • Taccy, Signet, Precize, Alifix, UTIutility, Sparsity, alisma • Revisionist & DeepTools • Text Utilities: Nalaprop, Dystextia and others • PDF • Keychains & Permissions • LockRattler: 10.15 Catalina • Updates

- Spundle, Cormorant, Stibium, Dintch, Fintch and cintch
- Long Reads
- Mac Troubleshooting Summary
- LockRattler: 11.0 Big Sur
- M1 & M2 Macs
- Mints: a multifunction utility
- LockRattler: 12.x Monterey
- VisualLookUpTest
- Virtualisation on Apple silicon
- LockRattler: 13.x Ventura