THE ECLECTIC LIGHT COMPANY

MACS, PAINTING, AND MORE

hoakley / January 4, 2023 / Macs, Technology

How do you know when macOS detects and remediates malware?

Over the last week or so, in test virtual machines, I've been deliberately running malicious software that macOS has detected and removed ('remediated'). Following yesterday's assessment of the effectiveness of protection provided by macOS, this article looks at how well the user is informed about malware detections.

Detection

When malware is detected as the user is trying to open or run it, alerts are clear, apart from the terminology used.

It's some years since Apple referred to malware using regular names. Since then, sources such as the XProtect Yara data file refer to all malware using semi-randomised hex. For example, the alert below cites the name of MACOS.2070d41, which is unique to Apple. This turns out to mean a variant of what's generally known as XCSSET, which Apple has also previously referred to as DubRobber A.

Other alerts use newer names, in common with codenames used for the scanning modules in XProtect Remediator, such as SnowDrift, although why it has been capitalised in the alert below is a mystery.

SnowDrift refers to what everyone else knows as CloudMensis.

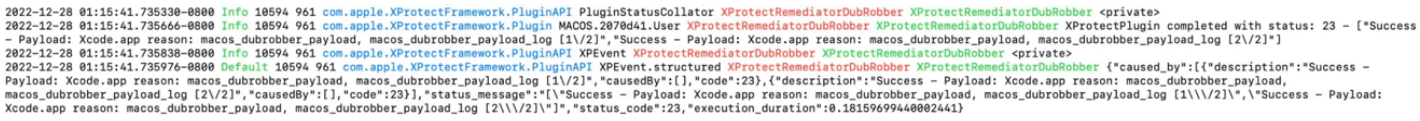
None of Apple's obscure naming systems informs the user, just leaves them puzzled, and unless they have the presence of mind to take a screenshot, they won't recall the name shown in the alert.

Apple is in the unique position of being able to agree common terminology with security researchers. It's high time that Apple fixed this and stopped confusing users.

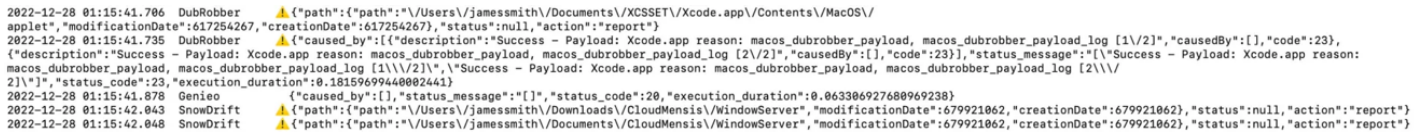
XProtect Remediator

Detections and remediations by XProtect Remediator aren't reported to the user in notifications, alerts, or any other overt means of informing them. Instead, they're

written in entries made in the Unified log, and made accessible to apps with access to the Endpoint Security framework. The latter only applies in macOS Ventura, though, which now supports `es_event_xp_malware_detected_t` and `es_event_xp_malware_remediated_t` events recording detection and remediation. For ordinary users relying on the utilities bundled in Ventura, this effectively conceals all malware detection and remediation, other than those reported in alerts as shown above.



Advanced users with experience of accessing the Unified log can retrieve log entries written by XProtect Remediator's scanning modules, like those above reporting a successful remediation of DubRobber payload during testing.



They can also be accessed more readily using my free utility XProCheck. In the excerpt above, DubRobber payload is first detected then remediated, following which two potential detections of CloudMensis (SnowDrift) are reported, but no remediation of those was attempted. To put that more directly, XProtect Remediator discovered two rogue files which it suspects could be malware, but the user wasn't notified of their presence, and is left none the wiser.

At present, with the exception of the command tool `eslogger`, macOS contains no app that can monitor Endpoint Security events for the user. Although several third-party security products do use Endpoint Security, few if any detail which events they monitor. As those reporting detections and remediations are only available in macOS Ventura, I have yet to discover any vendor whose products will report `es_event_xp_malware_detected_t` and `es_event_xp_malware_remediated_t` events.

Using `eslogger` isn't simple either. That tool has to be left running to gather records of events into a text file, which the user has to monitor and maintain. Using the details I published here previously, I gathered those two event types during my tests using malware samples. Each event generates a substantial quantity of JSON data which appears to be undocumented.

```
"schema_version": 1,
"mach_time": 29477280550,
"event_type": 112,
"thread": {
  "thread_id": 9193
},
"version": 6,
"seq_num": 0,
"event": {
  "xp_malware_detected": {
    "incident_identifier": "D22E0E02-4757-44E0-9ADB-00A886801979",
    "malware_identifier": "MACOS.2070d41",
    "detected_path": "\/Users\/jamessmith\/Downloads\/XCSSET\/Xcode.app",
    "signature_version": "2165"
  }
},
"time": "2022-12-28T10:03:42.389080913Z",
"action": {
  "result": {
    "result": {
      "auth": 0
    },
    "result_type": 0
  }
},
"process": {
  "signing_id": "com.apple.XprotectFramework.AnalysisService",
  "parent_audit_token": {
    "asid": 100001,
    "pidversion": 7,
    "ruid": 0,
    "euid": 0,
    "rgid": 0,
    "auid": 4294967295,
    "egid": 0,
    "pid": 1
  },
  "codesigning_flags": 570509825,
  "executable": {
    "path": "\/System\/Library\/PrivateFrameworks\/XprotectFramework.framework\/Versions\/A\/XPCServices\/XprotectService.xpc\/Contents\/MacOS\/XprotectService",
    "stat": {
```


Above is the first half of the data for a single successful detection, in this case not by an XProtect Remediator scan, but by the regular XProtect service.

Summary

Currently:

- Apple uses two different and obscure naming systems for malware, neither of which matches that used by everyone else. These make it harder for users to understand detection alerts.
- In macOS Catalina to Monterey, XProtect Remediator detection and remediation reports are only written in the Unified log, and are therefore inaccessible to the great majority of users.
- In Ventura, detection and remediation reports are also available to Endpoint Security clients. The only client bundled with macOS is a command tool which must be left running at all times if it's to get events and record them to a log. That isn't a practical solution for users.
- Although some third-party security products are capable of recording detection and remediation events, it's not clear which if any do, or whether they alert the user. Most of those products also require significant subscriptions.

- As a result, the great majority of users are oblivious of the detection and remediation of malware on their Macs, which occurs in complete secrecy. The answer to my question in the title of this article is therefore that you don't know.

Posted in Macs, Technology and tagged EndpointSecurity, log, macOS 13, malware, Remediator, security, Ventura, XProCheck, XProtect. Bookmark the permalink.

---

9 Comments Add yours

Alan B on January 4, 2023 at 8:20 am Reply

★ Liked by 1 person

Many thanks for an intriguing article! I fail to see what Apple hopes to gain by this secretive approach. Perhaps they wish to promote the idea to the average, less tech savvy users that macOS is a totally secure and malware free environment? Comparing macOS with Windows that's probably still true!

2

hoakley on January 4, 2023 at 11:40 am Reply

★ Like

Thank you. Yes, it baffles me too.
Howard.

Sean on January 4, 2023 at 10:55 am Reply

★ Liked by 1 person

As a Mac power user, this is quite uncomfortable for me. I would prefer to opt out of the security notifications if they are bothering me. But not knowing what's going on on my machine security-wise, is malpractice.
Thanks for pointing this out!

Javier Gallardo on January 4, 2023 at 12:18 pm Reply

★ Liked by 1 person

When I was young, I knew how to change a spark-plug in my car; now, I can't

even reach them (I suppose they're still there!).
…We're happily accepting how Mac OS is becoming more and more intricate, favoring solidness and security. All these inner details are so obscure as the motor functioning in our cars. I'm sure developers will learn (and will make their tools), same as mechanics do.
The time for aficionados to fiddle with their machine have passed away, I'm afraid. I'm getting used to it; more & more after accepting that the inner SSD in my MacBook Pro will die some day for sure, no matter how carefully I use my mac, the same as a fire-lighter without refueling valve. Buy, use, trash it. (I hate that).
So, not a surprise how the System is becoming almost totally opaque for just an advanced user like me.
I agree, however, that developers and computer technics should be clearly informed in detail about all these changes.
I'm sure Mr. Hoakley is making a very valuable investigation (bravo!), and I would like (I seriously hope) that Apple would assist you and others in a more compromised way.
Thank you for your "revelations".

5

hoakley on January 4, 2023 at 5:23 pm Reply ★ Like

Thank you.
I disagree completely, particularly with your analogy. The detection and removal of malware from your Mac isn't a matter of routine maintenance that can be done in secrecy from the user.
If malware is detected, then it's essential that the user is fully informed, even if the malware is successfully removed.
That applies to all users, whether individuals, or in small businesses, or enterprise.
If we don't take malware seriously, then we're lost.
Howard.

6

adele on January 5, 2023 at 3:11 am Reply ★ Liked by 1 person

You could not be more wrong. Not knowing what is going on, on your computer, is a recipe for disaster, as sooner or later something will happen that you don't understand that costs you money, time, privacy, or data, or all of the above.

That Apple are not telling users the full story, and doing so in a manner

that is confusing, is, at best, poor security.

7

Javier Gallardo on January 5, 2023 at 10:20 am Reply Liked by 1 person

Oh! I was being cynical! Of course Apple is contemptuous with users! …Not only closing the system to user, but also leaving us with limited resources if things go bad; even more, preventing a mend if internal ssd breaks (couldn't it be plugged, not soldered?).
(And yes: it's a shame there isn't a "complaints book" in this concentration camp).

8

hoakley on January 5, 2023 at 5:26 pm Reply Like

I'm sorry – I misunderstood.
Actually, internal SSDs can now be socketed rather than soldered in – they are in the Mac Studio, for instance. However, what goes into its sockets aren't the sort of SSD you can buy on the open market, as they don't have a disk controller, for instance. And replacing them isn't simple either, as you have to restore that Mac in DFU mode. Be careful what you wish for!
Howard.

Week 2 – 2023 – This Week In 4n6 on January 8, 2023 at 3:31 am Reply Like

[…] Howard Oakley at 'The Eclectic Light Company'How do you know when macOS detects and remediates malware? […]

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)

November 2021 (72)

September 2021 (76)

July 2021 (75)

May 2021 (80)

March 2021 (77)

January 2021 (75)

November 2020 (84)

September 2020 (79)

July 2020 (81)

May 2020 (78)

March 2020 (86)

January 2020 (86)

November 2019 (74)

September 2019 (80)

July 2019 (95)

May 2019 (91)

March 2019 (78)

January 2019 (69)

November 2018 (71)

September 2018 (76)

July 2018 (76)

May 2018 (71)

March 2018 (73)

January 2018 (83)

December 2021 (75)

October 2021 (75)

August 2021 (75)

June 2021 (71)

April 2021 (79)

February 2021 (75)

December 2020 (77)

October 2020 (81)

August 2020 (103)

June 2020 (78)

April 2020 (81)

February 2020 (77)

December 2019 (82)

October 2019 (89)

August 2019 (91)

June 2019 (88)

April 2019 (79)

February 2019 (71)

December 2018 (79)

October 2018 (78)

August 2018 (78)

June 2018 (77)

April 2018 (67)

February 2018 (67)

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