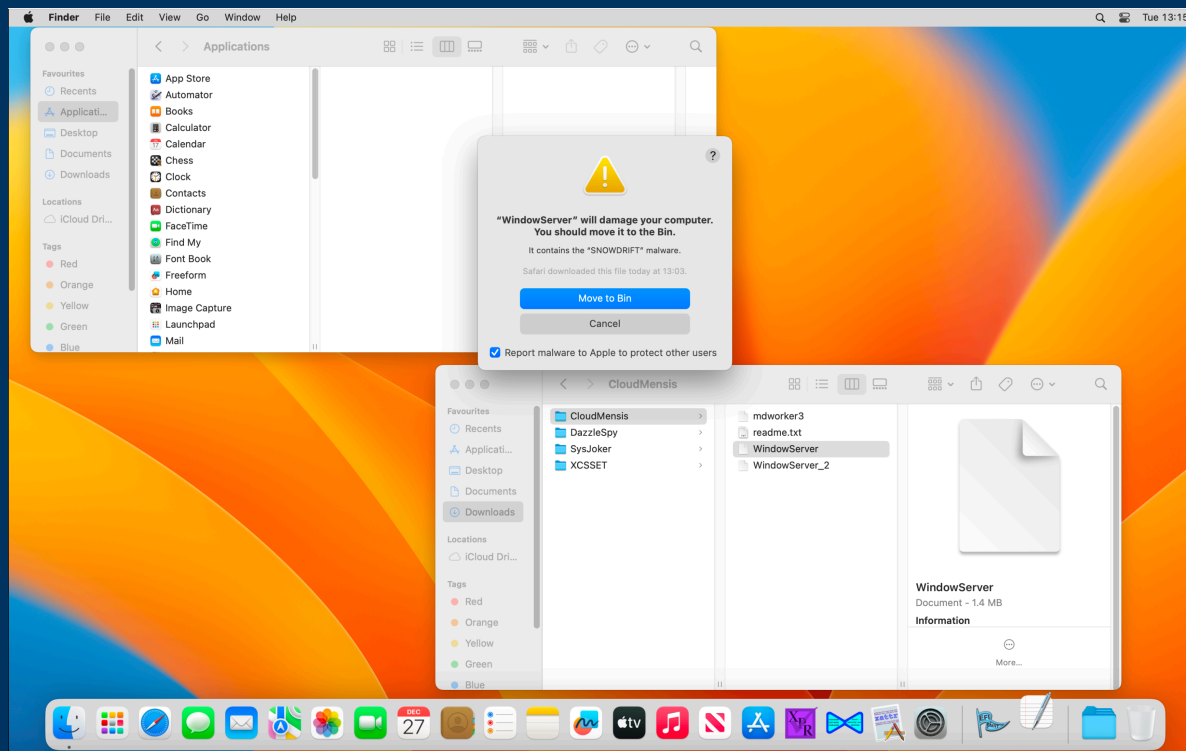


# macOS Malware Detection & Remediation

How Apple has changed security protection



Howard Oakley, The Eclectic Light Co <https://eclecticlight.co>

# July 2019

- Zoom client installed hidden web server

# July 2019

- Zoom client installed hidden web server
- web server vulnerable

# July 2019

- Zoom client installed hidden web server
- web server vulnerable
- web server left behind after removing Zoom

# July 2019

- Zoom client installed hidden web server
- web server vulnerable
- web server left behind after removing Zoom
- MRT 1.45 update (10 July) removes web server from all Macs

# July 2019

- Gatekeeper (AMFI) signature checks, notarization (June 2019)
- XProtect blocks old Java, Flash Player
- XProtect Yara checks at app *first* run (from 10.15 on *each* run)
- MRT scans after startup

## July 2019: MRT

- scan and remove known malware, including malicious Safari extensions
- updated every month or so
- malware identities obfuscated
- effectiveness unknown

# 14 March 2022 Monterey 12.3

CoreServices >

Extensions >

InstallerSandboxes >

LaunchAgents >

LaunchDaemons >

PrelinkedKernels >

PrivateFrameworks >

Receipts >


CoreTypes.bundle

MRT.app

SafariSupport.bundle

**XProtect.app**

XProtect.bundle



**XProtect.app**

Application

Version 89 (1)

com.apple.XProtectFramework.XP...

Apple Silicon — 64-bit

Intel — 64-bit

Copyright © 2021 Apple, In...

29.1 MB

Last modified 2 Feb 2023 at 18:4

App Sandbox ☐ Not ena...

Hardening ☒ Enabled...

Notarization ☐ Not appli...

Gatekeeper ☒ Apple Sy...

Signed By ☒ Software...

Open With Apparency

**XProtect.app**

Application - 29.1 MB

**Information**

Created

Wednesday, 25 January 2023 at 20:11

Modified

Thursday, 2 February 2023 at 18:41

Last opened

--

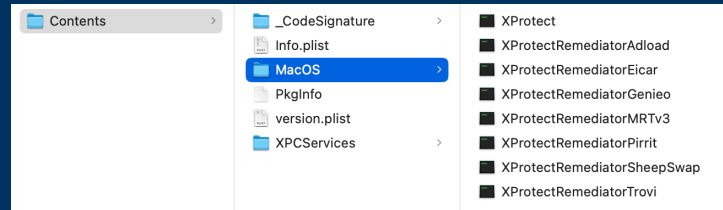
Version

89



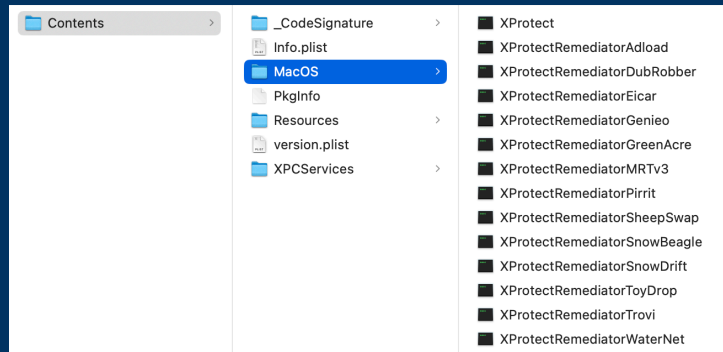
# Growth: March – August 2022

**14 March 2022**  
**version 2**  
**7 scanners**  
**15 MB**



**17 June 2022**  
**installed on macOS 10.15 and later**

**4 August 2022**  
**version 68**  
**13 scanners**  
**26 MB**

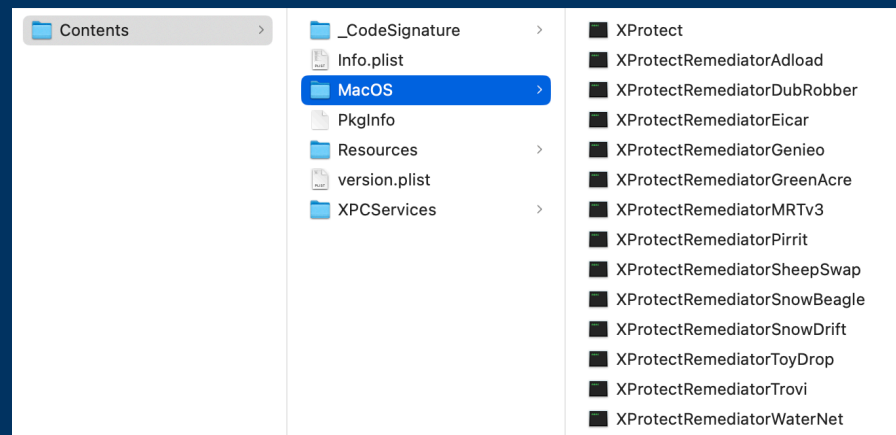


# August 2022: XProtect Remediator

- scan and remove known malware, including malicious Safari extensions
- updated every two weeks
- malware identities mostly obfuscated
- effectiveness unknown

# What is XProtect Remediator?

- app in CoreServices, executable in Finder or Terminal
- contains 13 scanning modules, including MRT replacement
- runs automatically, as root and as current user



# XProtect Remediator scans

- scheduled at least once a day, extras as determined by threat
- run as root, and as current user
- when Mac is awake but not otherwise busy
- not reported to the user

# XProtect Remediator scans

- Eicar test
- MRT compatibility, back catalogue
- Adload, Trojan to download malware and PUPs
- DubRobber (XCSSET), Trojan dropper
- Genieo, browser hijacker
- GreenAcre, not identified yet
- Pirrit, malicious adware
- SheepSwap, not identified yet
- SnowBeagle, not identified yet
- SnowDrift (CloudMensis), spyware
- ToyDrop, not identified yet
- Trovi, cross-platform browser hijacker
- WaterNet, not identified yet

# XProtect Remediator scans

2023-02-03	23:54:57.863	MRTv3	{"caused_by":[], "status_message": "Success", "status_code": 0, "execution_duration": 4.6968460083007812e-05}
2023-02-03	23:55:09.270	Adload	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.9948692321777344e-05}
2023-02-03	23:55:09.907	Pirrit	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.1021575927734375e-05}
2023-02-03	23:55:10.424	GreenAcre	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.8930130004882812e-05}
2023-02-03	23:56:21.389	WaterNet	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.2002410888671875e-05}
2023-02-03	23:56:29.165	SnowDrift	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05}
2023-02-03	23:56:30.382	ToyDrop	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.9989433288574219e-05}
2023-02-03	23:56:40.974	SnowBeagle	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.392333984375e-05}
2023-02-03	23:56:41.259	Genieo	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8995018005371094e-05}
2023-02-03	23:56:41.316	Trovi	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.8068504333496094e-05}
2023-02-03	23:56:47.868	DubRobber	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8041343688964844e-05}
2023-02-03	23:56:57.915	SheepSwap	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8041343688964844e-05}
2023-02-03	23:57:24.067	Pirrit	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 3.6954879760742188e-05}
2023-02-03	23:57:37.588	DubRobber	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4001808166503906e-05}
2023-02-04	00:00:24.324	WaterNet	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 3.8027763366699219e-05}
2023-02-04	00:00:24.661	Adload	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.7962875366210938e-05}
2023-02-04	00:00:25.168	Genieo	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.5922737121582031e-05}
2023-02-04	00:00:25.219	Trovi	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05}
2023-02-04	00:00:25.498	SnowDrift	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05}
2023-02-04	00:00:44.265	MRTv3	{"caused_by":[], "status_message": "Success", "status_code": 0, "execution_duration": 7.4982643127441406e-05}
2023-02-04	00:00:50.657	SnowBeagle	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.8930130004882812e-05}
2023-02-04	00:00:50.802	ToyDrop	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.9008598327636719e-05}
2023-02-04	00:01:00.225	SheepSwap	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.8082084655761719e-05}
2023-02-04	00:01:00.760	GreenAcre	{"caused_by":[], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.6055526733398438e-05}

# Detection & remediation

- location-specific
- change according to security status
- appear effective
- silent

# Detection & remediation

```
2022-12-28 01:57:48.288 SnowDrift ⚠️{"path":{"path":"\\Users\\jamesmith\\Library\\HTTPStorages\\WindowServer","modificationDate":693914044.70780134,"creationDate":693914044.70780134},"status":null,"action":"report"}
2022-12-28 01:57:48.294 SnowDrift ⚠️{"path":{"path":"\\Users\\jamesmith\\Downloads\\CloudMensis\\WindowServer","modificationDate":679921062,"creationDate":679921062},"status":null,"action":"report"}
2022-12-28 01:57:48.300 SnowDrift ⚠️{"path":{"path":"\\Users\\jamesmith\\Documents\\CloudMensis\\WindowServer","modificationDate":679921062,"creationDate":679921062},"status":null,"action":"report"}
2022-12-28 01:57:48.300 SnowDrift ⚠️{"caused_by":{"description":"Success - File: Path[\\Users\\USER\\Library\\Application Support\\com.apple.spotlight\\*\\.CrashRep]","causedBy":[]},"code":23},"status_message":["Success - File: Path[\\Users\\USER\\Library\\Application Support\\com.apple.spotlight\\*\\.CrashRep]"],"status_code":23,"execution_duration":0.084282994270324707}
2022-12-28 01:57:48.333 ToyDrop {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.02497398853302002}
2022-12-28 01:57:48.425 Genieo {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.084052920341491699}
2022-12-28 01:57:50.894 SheepSwap {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":2.4607440233230591}
2022-12-28 01:57:54.828 MRTv3 {"caused_by":[],"status_message":["MRT completed"],"status_code":0,"execution_duration":3.7971580028533936}
2022-12-28 01:57:55.028 SnowBeagle {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.12275803089141846}
2022-12-28 01:57:55.130 Adload {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.030357003211975098}
2022-12-28 01:57:55.266 GreenAcre {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.065433025360107422}
2022-12-28 01:57:55.354 Pirrit {"caused_by":[],"status_message":[""],"status_code":20,"execution_duration":0.0092810392379760742}
2022-12-28 01:57:55.573 DubRobber ⚠️{"path":{"path":"\\Users\\jamesmith\\Documents\\XCSSET\\Xcode.app\\Contents\\MacOS\\applet","modificationDate":617254267,"creationDate":617254267},"status":null,"action":"report"}
2022-12-28 01:57:55.599 DubRobber ⚠️{"caused_by":{"description":"Success - Payload: Xcode.app reason: macos_dubrobber_payload, macos_dubrobber_payload_log [1\\2]","causedBy":[]},"code":23}, {"description":"Success - Payload: Xcode.app reason: macos_dubrobber_payload, macos_dubrobber_payload_log [2\\2]","causedBy":[]},"code":23},"status_message":["Success - Payload: Xcode.app reason: macos_dubrobber_payload, macos_dubrobber_payload_log [1\\2]"],"status_code":23,"execution_duration":0.16771793365478516}
```



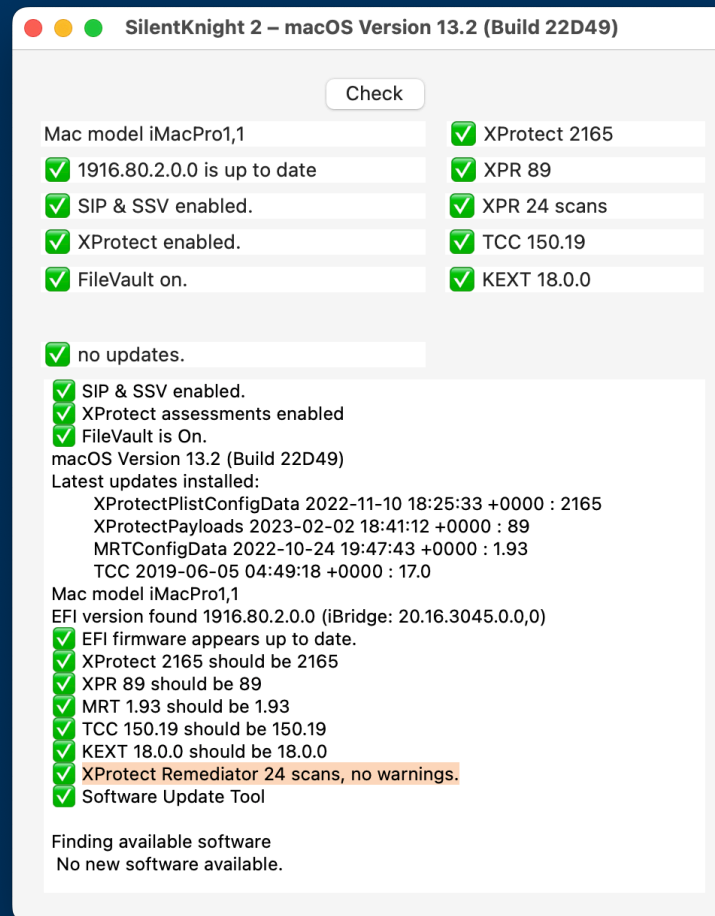
# Reporting

- macOS 10.15 to 12 only reported in the log
- macOS 13 reported in the log and as events in Endpoint Security
- no notifications or alerts at all
- `log show --predicate 'subsystem == "com.apple.XProtectFramework.PluginAPI" AND category == "XPEvent.structured" ' --info --last 1d`

# Endpoint Security

- macOS 13 only
- `es_event_xp_malware_detected_t`
- `es_event_xp_malware_remediated_t`
- `eslogger` can report those events

# SilentKnight



# XProCheck

XProCheck : XProtect Remediator version 89

Check for last 4 days

Check XProtect

Save

Run XProtect

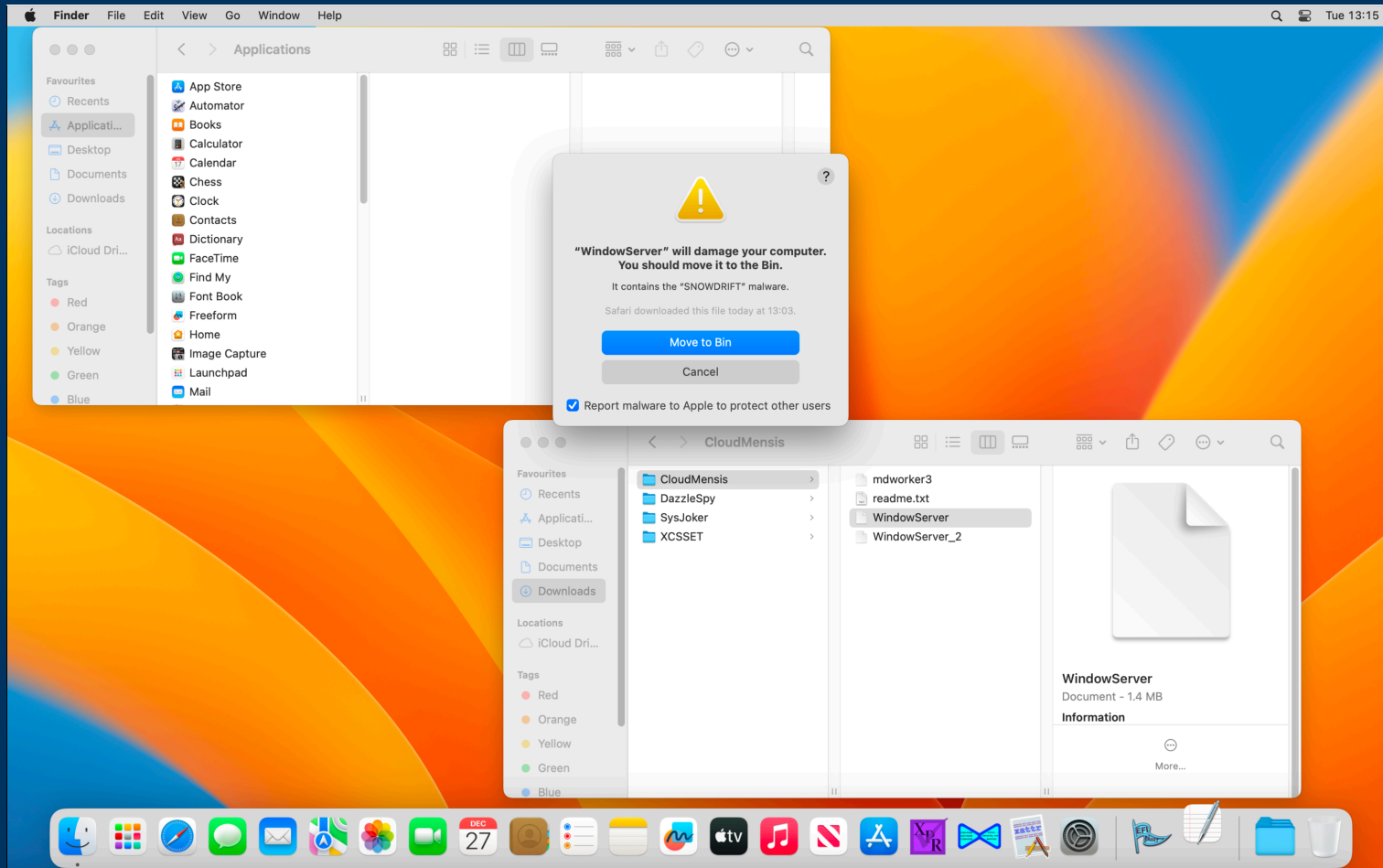
XProtect Remediator scans completed in the last 4 days:

2023-02-03 23:54:57.863	MRTv3	{ "caused_by": [], "status_message": "Success", "status_code": 0, "execution_duration": 4.6968460083007812e-05 }
2023-02-03 23:55:09.270	Adload	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.9948692321777344e-05 }
2023-02-03 23:55:09.907	Pirrit	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.1021575927734375e-05 }
2023-02-03 23:55:10.424	GreenAcre	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.8930130004882812e-05 }
2023-02-03 23:56:21.389	WaterNet	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.2002410888671875e-05 }
2023-02-03 23:56:29.165	SnowDrift	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05 }
2023-02-03 23:56:30.382	ToyDrop	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.9989433288574219e-05 }
2023-02-03 23:56:40.974	SnowBeagle	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.392333984375e-05 }
2023-02-03 23:56:41.259	Genio	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8995018005371094e-05 }
2023-02-03 23:56:41.316	Trovi	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.8068504333496094e-05 }
2023-02-03 23:56:47.868	DubRobber	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8041343688964844e-05 }
2023-02-03 23:56:57.915	SheepSwap	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.8041343688964844e-05 }
2023-02-03 23:57:24.067	Pirrit	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 3.6954879760742188e-05 }
2023-02-03 23:57:37.588	DubRobber	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4001808166503906e-05 }
2023-02-04 00:00:24.324	WaterNet	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 3.8027763366699219e-05 }
2023-02-04 00:00:24.661	Adload	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.7962875366210938e-05 }
2023-02-04 00:00:25.168	Genio	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.5922737121582031e-05 }
2023-02-04 00:00:25.219	Trovi	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05 }
2023-02-04 00:00:25.498	SnowDrift	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4955482482910156e-05 }
2023-02-04 00:00:44.265	MRTv3	{ "caused_by": [], "status_message": "Success", "status_code": 0, "execution_duration": 7.4982643127441406e-05 }
2023-02-04 00:00:50.657	SnowBeagle	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.8930130004882812e-05 }
2023-02-04 00:00:50.802	ToyDrop	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.9008598327636719e-05 }
2023-02-04 00:01:00.225	SheepSwap	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.8082084655761719e-05 }
2023-02-04 00:01:00.760	GreenAcre	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.6055526733398438e-05 }
2023-02-04 23:56:08.791	MRTv3	{ "caused_by": [], "status_message": "Success", "status_code": 0, "execution_duration": 9.0003013610839844e-05 }
2023-02-04 23:56:18.952	Adload	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 9.2029571533203125e-05 }
2023-02-04 23:56:19.361	Pirrit	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.8068504333496094e-05 }
2023-02-04 23:56:19.765	GreenAcre	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 9.2029571533203125e-05 }
2023-02-04 23:57:05.024	WaterNet	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.103515625e-05 }
2023-02-04 23:57:10.390	SnowDrift	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.6028366088867188e-05 }
2023-02-04 23:57:11.532	ToyDrop	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.9989433288574219e-05 }
2023-02-04 23:57:17.932	SnowBeagle	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.4042549133300781e-05 }
2023-02-04 23:57:18.184	Genio	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.29425048828125e-05 }
2023-02-04 23:57:18.238	Trovi	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.198883056640625e-05 }
2023-02-04 23:57:22.564	DubRobber	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.296966552734375e-05 }
2023-02-04 23:57:27.682	SheepSwap	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.7009201049804688e-05 }
2023-02-04 23:58:26.789	Pirrit	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 4.3034553527832031e-05 }
2023-02-04 23:58:41.660	DubRobber	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.1021575927734375e-05 }
2023-02-05 00:01:39.600	WaterNet	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 3.7908554077148438e-05 }
2023-02-05 00:01:40.317	Adload	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.8916549682617188e-05 }
2023-02-05 00:01:41.012	Genio	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.389617919921875e-05 }
2023-02-05 00:01:41.071	Trovi	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4001808166503906e-05 }
2023-02-05 00:01:41.527	SnowDrift	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 5.4001808166503906e-05 }
2023-02-05 00:02:04.479	MRTv3	{ "caused_by": [], "status_message": "Success", "status_code": 0, "execution_duration": 7.9989433288574219e-05 }
2023-02-05 00:02:11.022	SnowBeagle	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 8.4996223449707031e-05 }
2023-02-05 00:02:11.374	ToyDrop	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 6.103515625e-05 }
2023-02-05 00:02:22.024	SheepSwap	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.8082084655761719e-05 }
2023-02-05 00:02:22.924	GreenAcre	{ "caused_by": [], "status_message": "NoThreatDetected", "status_code": 20, "execution_duration": 7.4028968811035156e-05 }

The oldest log entry has a timestamp of 2023-02-03T15\_57\_30Z, 2.237 days ago.

Scanned at 2023-02-05T21\_39\_19Z

# Gatekeeper & XProtect



# Acknowledgement

Objective-See Foundation  
<https://objective-see.org>

**Thank you for your attention ...**

**... and happy XProtecting**

<https://eclecticlight.co>