DazzleSpy Mac Malware Used in Targeted Attacks

Posted on January 25th, 2022 by Joshua Long

DazzleSpy is the latest Mac malware to make headlines. Intriguingly, it has the hallmarks of a state-sponsored, cyber-espionage campaign.

Intego detects this malware's various components as , , , and .

Let's examine this threat and what makes it unique and interesting.

In this article:

How was DazzleSpy discovered?

In November 2021, teams from Google and ESET were independently researching a Mac malware campaign. The campaign leveraged what's known as a watering hole attack—where a group of people with a common interest is specifically targeted for infection. In this case, evidently the targeted class was people advocating for democracy in Hong Kong.

Erye Hernandez from Google's Threat Analysis Group (TAG) first published about the campaign on November 11. Hernandez noted that the watering hole campaign leveraged a vulnerability (CVE-2021-30869) that did not affect the then-current version of macOS Big Sur, but was exploitable on macOS Catalina.

Apple later released a patch for Catalina, as well as for iOS 12.5.5, on September 23 (as Intego noted here). On the same day, Apple updated its security release notes for macOS Big Sur 11.2—which had

been released way back on February 1—to acknowledge that the update had fixed the vulnerability nearly eight months earlier.

It's quite interesting that Apple secretively patched a vulnerability in February for the then-latest macOS version, neglecting to patch it for other operating systems that were ostensibly still supported at the time—and only admitting to it, and patching other affected operating systems, when the vulnerability was caught being used in the wild. As we've said before, Apple's poor patching policies potentially make users' security and privacy precarious. It's safest to stay up to date with the very latest version of Apple's operating systems; older versions may get some, but not all, important security fixes.

> Apple's Poor Patching Policies Potentially Make Users' Security and Privacy Precarious

Hernandez stated that Google believed "this threat actor to be a well-resourced group, likely state backed, with access to their own software engineering team based on the quality of the payload code." Google called the payload's malware family "MACMA," which Patrick Wardle nicknamed "CDDS" based on its repeated code strings.

This week, ESET researchers Marc-Etienne M.Léveillé and Anton Cherepanov published findings from their own independent research of the same watering hole attack campaign. Although their analysis led to a different payload from the one observed by Google, they came to similar conclusions about the threat actor: "Given the complexity of the exploits used in this campaign, we [assess] that the group behind this operation has strong technical capabilities." The researchers noted that the threat actor had non-public knowledge about a particular WebKit vulnerability, and used a clever method to force end-to-end encryption between infected Macs and the command-and-control (C&C) server.

ESET determined that it had received a different malware payload from the one Google had received, and dubbed the malware family "DazzleSpy."

What does DazzleSpy do to an infected computer?

DazzleSpy appears to have a wide variety of capabilities, mostly focused on spying on the user and stealing sensitive information. Among other things, DazzleSpy can:

collect the Mac username, Wi-Fi SSID (network name), IP address, and other potentially identifying information about the victim and their Mac

create lists of all files in the Desktop, Documents, or Downloads folders, and allow an attacker to search for files

allow an attacker to view the screen of, and remotely control, a victim's Mac

steal passwords from the victim's keychain, if their operating system is old enough (by exploiting

CVE-2019-8526)

exfiltrate data to an attacker-controlled server

bypass Gatekeeper by removing the com.apple.quarantine metadata from a file

continue to actively infect a Mac after it reboots (via a LaunchAgent)

remove itself (i.e. in case a victim discovers that their Mac is infected and tries to get expert help)

Another Mac malware threat distributed through the same sites and methods, dubbed Macma or CDDS, became widely known after Google published its report in November. This malware has several of the same capabilities as DazzleSpy. Google's assessment of Macma malware did not specify whether it could potentially export keychain passwords; however, Google did say that Macma can record audio and log keystrokes.

How can one remove/prevent DazzleSpy, other threats?

Unfortunately, the threat mitigation features that Apple has built into macOS—such as notarization, Gatekeeper, XProtect, and MRT—do not block many types of threats. Thus, Apple's own macOS protection methods are insufficient by themselves.

> Do Macs need antivirus software?

Intego VirusBarrier X9, included with , can protect against, detect, and eliminate DazzleSpy and Macma/CDDS malware. VirusBarrier is designed by Mac security experts, and it protects against a much wider variety of malware than Apple's mitigation methods.

If you believe your Mac may have been infected, or to prevent future infections, it's best to use antivirus software from a trusted Mac developer that includes real-time scanning, such as Intego VirusBarrier X9—which also protects Macs from M1-native malware, cross-platform malware, and more. in two independent tests conducted by AV-Comparatives and AV-TEST.

And if you're a Windows user, can protect your PC, too.

Note: Intego customers running VirusBarrier X8, X7, or X6 on older versions of Mac OS X are also protected from these threats. It is best to upgrade to the latest versions of VirusBarrier and macOS, if possible, to ensure your Mac gets all the latest security updates from Apple.

What do we know about DazzleSpy-affiliated domains?

Both and appear to have been registered by a threat actor for the specific purpose of targeting supporters of Hong Kong democracy.

But even more specifically, given the exploits and malware used in these campaigns, it seems that the threat actor was specifically targeting Mac users for some reason—and perhaps even users of macOS Catalina (or older) on Intel-based Macs.

Given this very precise degree of targeting, it's possible that one particular person, or a small group of people, may have been the primary target.

Two other domains used in these campaigns, and , are clearly intended to look like Apple domains at a glance, or to a novice. However, Apple doesn't own either domain. Both were registered with GoDaddy in August 2021, and the registration information for both domains was last updated on November 11—the same day that Google's blog post exposed them. There are indications that at least one of the domains may have been reused for other malicious campaigns on or after that date (see Vulners and Hybrid Analysis reports).

Who created DazzleSpy malware?

It seems clear that whoever distributed DazzleSpy was not in favor of Hong Kong democracy, given that the malware was distributed through sites that claimed to be pro-democracy in Hong Kong.

Interestingly, we may know the name of one of the developers of the malware. Several text strings embedded in DazzleSpy's code seem to reveal the username on the developer's Mac as "wangping":

Of course, it's entirely possible that this is a false flag. Given the sophistication of other aspects of the malware campaign, it seems sloppy for the developer to reveal their name in this way.

On the other hand, such a goof isn't unprecedented; see Intego's white paper on Mac malware attribution (PDF).

Indicators of compromise (IoCs)

The following SHA-256 hashes belong to known files associated with DazzleSpy, CDDS/Macma, and related malware campaigns:

The following files and folders may potentially be found on an infected Mac:

Note that denotes the user's home folder, e.g. .

It's also important to note that the folder mentioned above is typically invisible. By default, macOS hides folders and files with names that begin with a period character. You can reveal hidden files and folders by pressing ⌘⇧. (Command-Shift-period) in the Finder. However, be aware that most hidden items are not malicious, so avoid deleting or moving hidden items to the Trash unless you are certain that they are harmful.

The following IP addresses, domains, and URLs have been observed to have ties with this malware or related campaigns. Network administrators can check logs to try to identify whether any computers on their network may have attempted to contact one of these IPs or domains between August and November 2021, or possibly afterward.

Note that is used as a wildcard character above.

Although the following URL is not malicious, it was compromised (hacked) during a portion of the timeframe mentioned above. Therefore, computers that visited this site around that time may potentially have become infected:

Is DazzleSpy known by any other names?

Other vendors' names for threat components from this malware campaign may include variations of the following:

Adware/Macma!OSX, Artemis!Trojan, ASP.Webshell, Backdoor:MacOS/Macma.A!MTB, Backdoor:MacOS/Macma.B!MTB, Backdoor:MacOS/Macma.C!MTB, Backdoor:MacOS/Vigorf.A, Backdoor/JS.Macma, Backdoor/OSX.Macma.1194193, Backdoor/OSX.Macma.2575107, BV:Macma-A [Trj], DazleSpy, Dropper.Agent/Android!8.37E (CLOUD), E32/DroidRooter.A, Elf.Trojan.A3445236, Exploit.Agent!8.1B, Exploit.Generic-JS.Save.a46a1bf8, Exploit/JS.Generic, HEUR:Backdoor.OSX.Macma.a, HEUR:Exploit.Script.Generic, HEUR:Trojan-Dropper.AndroidOS.Agent.sk, HEUR:Trojan-Spy.OSX.Macma.a, HEUR:Trojan.OSX.Agent.gen, HEUR:Trojan.OSX.Agentb.gen, JS:Exploit-AH [Expl], JS.Exploit.ShellCode.c, JS/Exploit.Agent.NQK, LINUX/Agent.aj, Mac.BackDoor.Macma, Mac.Trojan-spy.Macma.Pepy, MacOS:Macma-A [Trj], MacOS:Macma-B [Trj], MacOS:Macma-C [Trj], MacOS:Macma-D [Trj], MacOS:Macma-E [Trj], macOS.Macma, MacOS/Agent.gen, MacOS/Macma.A, Malware.OSX/Macma.lvyms, Malware.OSX/Macma.nxnte, OSX.CDDS, OSX.DazzleSpy, OSX.S.Agent.1194193, OSX.S.Agent.2575107, Osx.Trojan.Agent.Llrp, OSX/Agent.g, OSX/Exploit.Agent.C, OSX/Macma-A, OSX/Macma.A!tr, OSX/Macma.B!tr, OSX/Macma.C!tr, OSX/Macma.D!tr, OSX/Macma.E!tr, OSX/Macma.jhzzd, OSX/Macma.lkoes, OSX/Macma.lvyms, OSX/Macma.lwxgs, OSX/Macma.nxnte, OSX/Macma.qmfus, OSX/Macma.taejb, osxrk, PrivacyRisk.SPR/ANDR.DroidRooter, RDN/Generic.osx, Script.Trojan.45123.GC, Script.Trojan.A3298608, Script.Trojan.A3370311, SPR/ANDR.DroidRooter.H.Gen, TROJ_FRS.0NA103A422, TROJ_FRS.0NA103KF21, TROJ_FRS.0NA103KT21, TROJ_FRS.0NA104KF21, TROJ_FRS.VSNTKG21, TROJ_FRS.VSNTKT21, Troj/JSExp-X, Trojan:MacOS/Macma.B, Trojan:Script/Wacatac.B!ml, Trojan:Win32/Casdet!rfn, Trojan:Win32/Mamson.A!ml, Trojan.AndroidOS.Agent.C!c, Trojan.DroidRooter.Android.11, Trojan.DroidRooter.Android.88, Trojan.JS.DAZZLESPY.A, Trojan.Macma.OSX, Trojan.MacOS.MACMA.A, Trojan.Malscript, Trojan.OSX.Agentb.4!c, Trojan.OSX.Macma, Trojan.OSX.Macma.4!c, Trojan.OSX.Macma.l!c, Trojan.OSX.Macma.m!c, Trojan.Script.Generic.3!c, Trojan.UKP.Linux.4!c, TrojWare.Win32.UMal, VEX.Webshell, VirTool:Win32/Aicat.A!ml

How can I learn more?

For additional technical details about the DazzleSpy malware, you can read the recent write-ups

by Marc-Etienne M.Léveillé and Anton Cherepanov and Patrick Wardle. For more back story and additional insights, you can also read the November 2021 write-ups by Erye Hernandez, Patrick Wardle, and Phil Stokes about the related exploits and CDDS/Macma malware.

We discussed DazzleSpy on episode 224 of the . Be sure to follow the podcast to make sure you don't miss any episodes! You'll also want to subscribe to our and keep an eye here on for the latest Apple security and privacy news.

You can also subscribe to our and keep an eye here on for the latest Apple security and privacy news. And don't forget to follow Intego on your favorite social media channels:

DazzleSpy logo based on public domain dazzle and spy movie silhouette images.

About Joshua Long

(@theJoshMeister), Intego's Chief Security Analyst, is a renowned security researcher, writer, and public speaker. Josh has a master's degree in IT concentrating in Internet Security and has taken doctorate-level coursework in Information Security. Apple has publicly acknowledged Josh for discovering an Apple ID authentication vulnerability. Josh has conducted cybersecurity research for more than 20 years, which has often been featured by major news outlets worldwide. Look for more of Josh's articles at security.thejoshmeister.com and follow him on Twitter. View all posts by Joshua Long →