Malware

New macOS malware HZ RAT gives attackers backdoor access to Macs

Posted on September 5th, 2024 by Joshua Long

There's a new family of Mac malware, and—surprise!—it isn't primarily a stealer this time. **HZ RAT** is macOS malware that gives remote attackers complete control of an infected Mac.

Here's everything you need to know to stay safe from this new Mac malware threat.

What does HZ RAT do?

HZ RAT is a remote access Trojan (RAT)—a tool that gives an attacker full remote administration privileges. The earliest known version of this RAT was observed in 2022 targeting Windows PCs, and now it has arrived on the Mac.

In general, an attacker who controls a RAT can send commands to an infected system just as though they were sitting in front of it. This can potentially include downloading and running additional tools and malware, taking screenshots, logging keystrokes, and more. RATs also allow attackers to do all the typical things stealer malware does—i.e. collecting and exfiltrating sensitive data.

Data collection appears to be one of the main purposes of HZ RAT in particular. The Mac version makes a list of which apps are installed and collects user information from WeChat and DingTalk (Mac apps commonly used in China). It also gathers the username and site combinations from Google Password Manager.

While the collected Google Password Manager data doesn't include passwords, the username-and-site pairs could potentially be used along with leaked passwords from past data breaches; unfortunately, many people reuse passwords across multiple sites.

How does HZ RAT spread?

It isn't yet known how victims may have encountered HZ RAT installers in the first place. However, one known Trojan horse that installs HZ RAT is a maliciously modified version of OpenVPN Connect, a common VPN app.

It's possible that this Trojan horse might be distributed through means such as malicious Google Ads that appear at the top of search results (a very common malware distribution tactic in 2024). Or it might be distributed in more targeted, watering-hole style attacks, or through some other distribution method.

In any case, it's important to always download apps from the App Store (if available there) or from the original developer's site (which, ideally, you've already visited and bookmarked, so you don't have to Google it).

How can I keep my Mac safe from RATs and other malware?

If you use Intego VirusBarrier, you're already protected from this malware. Intego detects these samples as **OSX/HZRat.ext**.

Intego VirusBarrier X9, included with **Intego's Mac Premium Bundle X9**, is a powerful solution designed to protect against, detect, and eliminate Mac malware.

If you believe your Mac may be infected, or to prevent future infections, it's best to use antivirus software from a trusted Mac developer. VirusBarrier is award-winning antivirus software, designed by Mac security experts, that includes real-time protection. It runs natively on both Intel- and Apple silicon-based Macs, and it's compatible with Apple's current Mac operating system, macOS Sonoma.

One of VirusBarrier's unique features is that it can scan for malicious files on an iPhone, iPad, or iPod touch in user-accessible areas of the device. Just attach your iOS or iPadOS device to your Mac via a USB cable and open VirusBarrier.

If you use a Windows PC, **Intego Antivirus for Windows** can keep your computer protected from malware.

Indicators of compromise (IOCs)

Following are SHA-256 hashes of malware samples from this campaign:

```
0cca3449ff12cb75c9fd9cf4628b5d72f5ac67d1954dc97d9830436207c4c917
1400210f2eedab36caff8ce89d6d19859ba3116775981b2be8b5069ef109c2c3
1e07585f52be4605be0459bc10c67598eebe8c5d003d6e2d42f4dbbd037e74c1
5d78fc86a389247d768a6bdf46f3e4fd697ed87c133b99ee6865809e453b2908
6210ec0e905717359e01358118781a148b6d63834a54a25a95e32e228598c391
74c92a7bc5f909f4e36d65ee1eb254c438f47f1a7d559d7629bccafd2d2979db
7af7422edf7c558b6215489c020673e195e5eedd99ae330bb90066924f5cf661
87393d937407a6fe9e69dad3836e83866107809980e20a40ae010d7d72f90854
c689113a9a2fca2148caa90f71115c2c2bafeac36edebde4ffc63f87619033a9
d006d5864108094a82315ee60ce057afc8be09546ffaa1f9cc63a51a96764114
d9b0fcd3b20a82b97b4c74deebc7a2abb8fd771eaa12aaf66bdd5cdeaa30f706
e02e264a745e046f2a85ad90698fdd241c7902e73572a54995a8b20349bef940
eb7a8ddf8fc13efcc4785226d0085379399c088604a8a451b8800b11e836a5af
f39aafb9489b9b60b34e3d4e78cd9720446b6247531b81cbd4877804b065a25f
f3c101cd1e7be4ce6afe5d0236bfdd5b43870ff03556908f75692585cfd55c55
ffeed91c223a718c1afd6d8f059a76ec97eb0eae6c4b2072b343be1b4eba09b8
```

This malware campaign leverages the following command-and-control (C2) IP addresses, most of which appear to be located in China:

```
20.60.250[.]230
29.40.48[.]21
47.100.65[.]182
58.49.21[.]113
111.21.246[.]147
113.125.92[.]32
120.53.133[.]226
123.232.31[.]206
218.65.110[.]180
218.193.83[.]70
```

Network administrators can check logs to try to identify whether any computers may have attempted to contact these IPs in recent weeks, which could indicate a possible infection.

Do security vendors detect this by any other names?

Other antivirus vendors' names for this malware may include variations of the following:

A Variant Of OSX/HZRat.A, ABBackdoor.PNBT-, Backdoor:MacOS/HZRat.A, Backdoor.HZRat/OSX!1.10239 (CLASSIC), BackDoor.Rat.504, Backdoor/OSX.HZRat.57832, Backdoor/OSX.HZRat.65736, Backdoor/OSX.HZRat.81033750, Gen:Variant.Trojan.MAC.HZRat.1 (B), HEUR:Backdoor.OSX.HZRat.a, HEUR:Backdoor.OSX.HZRat.gen, MacOS:Agent-ANR [Trj], MacOS:HZRat-A [Trj], MacOS/ABTrojan.AWJF-, MacOS/ABTrojan.BFPE-, MacOS/ABTrojan.DIJE-, MacOS/ABTrojan.FYPM-, MacOS/ABTrojan.JIKJ-, MacOS/ABTrojan.MAOD-, MacOS/ABTrojan.NRFK-, MacOS/ABTrojan.RCIO-, MacOS/ABTrojan.RQNI-, MacOS/ABTrojan.SZVP-, MacOS/ABTrojan.URYF-, MacOS/ABTrojan.XYJG-, MacOS/ABTrojan.ZCRE-, MacOS/ABTrojan.ZYUF-, Malware.OSX/GM.Agent.IJ, Malware.OSX/GM.HZRat.WL, Osx.Backdoor.Hzrat.Azlw, Osx.Backdoor.Hzrat.Bdhl, Osx.Backdoor.Hzrat.Cgow, Osx.Backdoor.Hzrat.Cwnw, Osx.Backdoor.Hzrat.Iajl, Osx.Backdoor.Hzrat.Kjgl, Osx.Backdoor.Hzrat.Lajl, Osx.Backdoor.Hzrat.Lcnw, Osx.Backdoor.Hzrat.Mqil, Osx.Backdoor.Hzrat.Msmw, Osx.Backdoor.Hzrat.Ogil, Osx.Backdoor.Hzrat.Qimw, Osx.Backdoor.Hzrat.Xtjl, Osx.Backdoor.Hzrat.Zimw, Osx.Backdoor.Hzrat.Zmhl, OSX.Trojan.Gen, OSX/Agent, OSX/GM.Agent.IJ, OSX/HCSSET.ext, OSX/HZRat-A, OSX/HZRat.A!tr, OSX/RootRat, TROJ_FRS.0NA103HU24, Trojan (0040f50d1), Trojan:MacOS/HzRat.A!MTB, Trojan:MacOS/Multiverze, Trojan.MAC.Generic.119695 (B), Trojan.MAC.Generic.119751 (B), Trojan.MAC.Generic.119785 (B), Trojan.MAC.Generic.D1D38F, Trojan.MAC.Generic.D1D3C7, Trojan.MAC.Generic.D1D3E9, Trojan.OSX.Hzrat, Trojan.OSX.HZRat.4!c, Trojan.OSX.HZRat.m!c, Trojan.Trojan.MAC.HZRat.1, Trojan[Backdoor]/MacOS.HZRat, Trojan[Backdoor]/OSX.HZRat.gen, UDS:Backdoor.OSX.HZRat, UDS:DangerousObject.Multi.Generic, XAR/ABTrojan.MJTT-

How can I learn more?

For more technical details about this malware, you can read Sergy Puzan's report.

Each week on the **Intego Mac Podcast**, Intego's Mac security experts discuss the latest Apple news, including security and privacy stories, and offer practical advice on getting the most out of your Apple devices. Be sure to **follow the podcast** to make sure you don't miss any episodes.

You can also subscribe to our **e-mail newsletter** and keep an eye here on **The Mac Security Blog** for the latest Apple security and privacy news. And don't forget to follow Intego on your favorite social media channels:

About Joshua Long

Joshua Long (@theJoshMeister), Intego's Chief Security Analyst, is a renowned security researcher and writer, and an award-winning 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 25 years, which is often featured by major news outlets worldwide. Look for more of Josh's articles at security.thejoshmeister.com and follow him on X/Twitter, LinkedIn, and Mastodon. View all posts by Joshua Long →