Intego Research Report

Mac Malware Attribution

Cybercriminals Beware

intego

Abstract

In this paper, we will explore various aspects of malware attribution—that is, unmasking the real-world identity of malware creators—in relation to macOS malware. We will cover several specific case studies where the true identity of a malware maker was brought to light, often with minimal effort by researchers.

Who makes Mac malware, and why?

The question is often asked: what kind of people make malware, and what are their motivations?

While some historical malware has been developed out of simple curiosity, or for a hacker's self-aggrandizement, among the most common reasons why malware is developed today are profiteering or political motivations.

Cybercriminals with a primarily financial motivation sometimes develop malware that attempts to steal money (e.g. banking Trojans or cryptocurrency wallet stealers) or to abuse someone else's computing resources for the attacker's profit (e.g. cryptojackers).

Those with a primarily political motivation may develop malware that benefits military or intelligence agencies; these may include malware designed for espionage (i.e. state-sponsored spyware) or for sabotage (e.g. designed to affect nuclear or other facilities or industrial control systems).

For the purposes of this paper, it is sufficient to note that there are many threat actors with a variety of motivations. We will explore how the real-world identities of these threat actors can often be discovered through their failures to completely cover their tracks.

Does this white paper benefit cybercriminals by telling them what to avoid?

The techniques documented in this paper are not brand new; there are many resources on digital forensics and incident response (DFIR) and open-source

intelligence (OSINT) that explore such concepts and techniques in much greater depth.

Are there challenges that make it difficult to properly attribute malware?

Some cybercriminals are simply better than others at covering their tracks. In some cases, more advanced cybercriminals try to mask or sow doubt about their true identity through "false flags"—intentionally planted misinformation designed to deceive researchers and throw them off the scent.

Malware developers often reuse code or exploits found in other malware, either out of convenience, or to make it appear that the new malware is affiliated with an earlier malware campaign, or both.

Why does attribution matter?

When cybercriminals realize how difficult it is to avoid ever making even one simple mistake that can lead to the discovery of their true identity—which may in some cases lead to their arrest and imprisonment, or make it harder for them to establish a good reputation for themselves in their later careers—it becomes a lot less enticing to make and distribute malware.

It is important to note, however, that doxing a human individual suspected of being involved with malware—that is, revealing a variety of personally identifiable or highly sensitive information about them publicly—is not a good practice.

Now that we have explored some of the concepts surrounding attribution, we will take a look at some specific case studies of real Mac malware that has been attributed to their creators' real-world identities.

Case Studies

Case Study 1: Coldroot RAT

Mac security researcher Patrick Wardle wrote about his research into a RAT (remote administration tool, or remote access Trojan) known as Coldroot in early 2018. Wardle discovered a 27-minute video on YouTube that appeared to have been uploaded years earlier by the malware developer, whose hacker handle (as displayed throughout the video) was Coldzer0. In the comments on the video, the uploader mentioned a Web site: `coldroot.com`.

Intego researcher Joshua Long used a common OSINT technique to further investigate the site: he viewed older versions of the site that had been captured by the Internet Archive at `web.archive.org`. To Long's surprise, Coldzer0 had formerly used the domain as his own personal homepage, complete with his real name, nickname, photographs of himself, and links to his social media accounts, some of which used the Coldzer0 nickname as well.

Given that domain names can change ownership over time, Long checked publicly available WHOIS records (which document domain ownership changes, among other things), which indicated that the same person had owned the domain at the time of the archived versions of the site—both when it hosted a personal homepage and the RAT homepage.

A Google search for the nickname (Coldzer0) in conjunction with the real name found on the site (Mohamed Osama) revealed that a security blogger at databreaches.net had called out Coldzer0 by his real name publicly in the past for his hacking activities.

After Intego published an article about Coldroot RAT, Osama contacted Intego, claiming that he did not own the domain at the time it was used in connection with the Coldroot RAT. Contrary to Osama's claim, the aforementioned WHOIS records, along with all available evidence—including evidence unintentionally provided by Osama himself that connected the dots between his real name and his hacker identity—revealed that he did, in fact, own the domain at the time, and was in fact Coldzer0.

Osama continues to use his Coldzer0 identity. He describes himself as a “malware hunter” and “exploit developer,” and as of the last time he updated Twitter in September 2018, he was “looking for a job.”

Case Study 2: Lazarus Group’s Fallchill/Operation AppleJeus

Lazarus Group is a hacking team that is widely believed to have ties to the government of North Korea. In 2018, the group released a variant of its Fallchill malware for the Mac by means of a cryptocurrency app called CelasTradePro.

The “Get Info” window of the Trojanized CelasTradePro app for Mac revealed one name in connection with the malware: John Broox. The name also appeared in the WHOIS records for the Celas LLC domain name. As it turns out, “Broox” spelled with an *x* is an extremely uncommon, and possibly made up, surname.

However, another name surfaced that was a lot more interesting: Waliy Darwish.

A Windows variant of the Celas Bitcoin Trader app was uploaded to the multi-engine malware scanning site VirusTotal merely three hours after the app and been created. Within minutes, the file was marked as “Safe” by two community members: johnbroox200 (which matches the username portion of the WHOIS e-mail address) and waliydarwish222. Evidently, someone involved with the creation of the malware was testing to see whether it would be flagged by any popular anti-virus engines before releasing the malware in the wild, and they tried to increase the file's credibility by adding positive reviews.

Waliy Darwish has fairly legitimate-looking LinkedIn and Twitter profiles. Long noted that Darwish was a third-degree connection on LinkedIn, meaning that evidently Long knows someone who knows someone who knows him, which lends credence to the possibility that Darwish may be a real person. Interestingly, Darwish seems to have gone completely silent on social media after the discovery that CelasTradePro was connected with Lazarus Group.

Assuming that Darwish is a real person, it is unclear whether he knew about the connection with Lazarus Group before developing code for the CelasTradePro app, or whether he was simply a developer who was unknowingly hired by a

threat actor and deceived into making software that would be subsequently exploited and Trojanized.

If Darwish did not suspect there may have been a concern about his employer or the software, then why would he have created a VirusTotal account to rate his own app, which had not been flagged by any antivirus engines at the time? Perhaps Darwish felt (or was convinced by "John Broox") that, by virtue of it being a cryptocurrency app—which might be more likely to receive a false positive detection by overzealous antivirus software, or might be more likely to get scanned by a reasonably paranoid cryptocurrency aficionado—it may have been a good idea to preemptively put in a positive vote.

Darwish's LinkedIn profile says he is from the Greater Los Angeles Area, while his Twitter profile says he is from Cedar Springs, Michigan, the supposed home of Celas LLC.

Case Study 3: CreativeUpdater

The CreativeUpdater malware campaign consisted of Trojanized versions of three apps—the Mozilla Firefox browser and two Titanium Software utility apps, OnyX and Deeper—that were mistakenly distributed by the MacUpdate software download site in February 2018.

The Trojanized disk image was signed by an Apple Developer ID account, "Ramos Jaxson," which later had its signing certificate revoked by Apple. Notably, as is often the case with Apple Developer IDs found in connection with malware, the given name and surname are in reverse order from typical Western practice; in this case, the given name is most likely Jaxson while the surname is Ramos. Little additional information has been uncovered about Ramos to date.

Security researcher Thomas Reed performed a "retrohunt" on VirusTotal to see if additional malware could be found that had ties to the CreativeUpdater malware. In addition to finding files signed with the Ramos Jaxson developer certificate, Reed also found files signed by a "Tiago Mateus" certificate.

Another researcher, Arnaud Abbati, noted that the CreativeUpdater samples distributed through MacUpdate contained hidden .DS_Store metadata files that

revealed file paths from the original developer's computer, which gave away Mateus' full name: Tiago Brandão Mateus. This strongly hints that the Mateus name from the Apple Developer ID was not merely a fictitious name.

Until now, no additional information about Mateus had been documented. This week, Long discovered an e-mail address via a `duckduckgo.com` search for the full name Tiago Brandão Mateus, and followed the trail to see where it led. The username portion of the e-mail address matches with a username on a Brazilian hacking forum, where the member's profile seems to possibly reveal his actual birthdate. Through a variety of related searches on DuckDuckGo and Google, Long found a surprising amount of personally identifiable and sensitive information that he believes is associated with the CreativeUpdater creator, including his precise home address in São Paulo, Brazil, and a possible landline home telephone number. Mateus apparently owns or is a managing partner of several small business ventures, and he has registered dozens of .com and .com.br domain names. Long also encountered a 2014 password dump on Pastebin containing a password that Mateus may have once used.

Case Study 4: Pirrit/VSearch

After hitting dead ends with trying to identify the author of the harmful Pirrit (VSearch) adware, researcher Amit Serper typed a Terminal command to list the contents of a .tgz archive dropped by the malware. The output displayed the username of the archive's creator. The username happened to be the real name of the adware developer. Through a Google search for the name, Serper learned that the creator of the malware archive worked for TargetingEdge, a company whose own LinkedIn description perfectly matched the way the malware is distributed.

Serper revealed in an Intego interview that the developer subsequently started using a user account named "Batman" instead of his own account when creating archives for future versions of Pirrit.

Interestingly, in January 2017 a different developer from TargetingEdge applied for a job opening at Cybereason, Serper's employer, boasting in his CV that his work had been the focus of a Cybereason report.

Case Study 5: Fruitfly/Quimitchin

The FBI tracked down Phillip R. Durachinsky, the creator of the Fruitfly (aka Quimitchin) malware, which Durachinsky had been using for 14 years to spy on victims in various parts of the United States. Although not all of the FBI's research methodologies are known to the public, it is clear that they have a lot more resources than the average malware researcher. Durachinsky is still awaiting trial.

Conclusion

Quite often, malware attribution is not as difficult as one might expect.

To anyone who may be considering creating malware of any variety, take heed: there is a very strong chance that you will get caught. It is not a risk worth taking.

About the Author

Joshua Long, Intego's Chief Security Analyst, is a renowned security researcher and writer. Josh has a master's degree in IT concentrating in Internet Security and has taken doctorate-level coursework in Business Administration and Computer and Information Security. For two decades, Josh has been battling malware, malicious sites, phishing scams, and spam to help protect others online. Apple has publicly acknowledged Josh for discovering an Apple ID password validation vulnerability. Josh's research has been featured by many fine publications such as CNET, CBS News, ZDNet UK, Lifehacker, CIO, Macworld, The Register, MacTech Magazine, Naked Security, and The Mac Security Blog. He regularly writes, podcasts, and speaks about Apple security and privacy topics. @theJoshMeister | LinkedIn | jlong@intego.com

Additional Acknowledgements

This white paper is based on, and is being released in conjunction with, a talk presented by Joshua Long at the Objective by the Sea v2.0 conference in Monte Carlo, Monaco on June 1, 2019. The author wishes to thank Fred Blaison, Amit Serper, Patrick Wardle, Thomas Reed, Arnaud Abbati, and Nicholas Ptacek for their research and feedback.

Intego is the world's leading Apple security company. Founded in 1997, Intego has remained dedicated to the Apple Mac platform. Its flagship consumer offering is Mac Premium Bundle X9, a suite of five utilities designed to keep Macs safe from online threats: VirusBarrier (Mac anti-virus and anti-spyware protection), NetBarrier (two-way firewall that prevents Mac apps from "phoning home" without permission), Personal Backup (Mac backup with features far beyond Apple's Time Machine), Mac Washing Machine (disk cleanup and organization), and ContentBarrier (Mac parental controls). Intego's flagship SMB offering is Flextivity Complete, a centrally managed, all-in-one endpoint security and employee productivity solution. In 2018, Intego was acquired by Kape Technologies (LON:KAPE). https://www.intego.com | @IntegoSecurity | LinkedIn