Threat Source newsletter (April 21, 2022) —— Sideloading apps is as safe as you make it

By Jon Munshaw.

Welcome to this week's edition of the Threat Source newsletter. If you pay attention to the video game community as much as I do, you've been closely following the ongoing legal battle between Apple and Epic over the sale of "Fortnite" on the Apple App Store. (I promise I won't keep bringing up "Fortnite each week.") That lawsuit has now expanded into a larger debate about sideloading apps and allowing more than one app store on a mobile device. In this particular example, Epic believes the Epic Games Store should be allowed to run on Apple's iOS where users can pay to download games and conduct other microtransactions. And the European Union is considering a new law that would force smartphone producers to open the door for any app store on their devices. This would come with a few security red flags —— we've noted several times where attackers have leveraged sideloading apps to deliver malware to users' devices, sometimes malware that essentially tracks their every move on their device. Apple CEO Tim Cook recently pushed back against the proposed EU law and other similar pushes in the U.S., and he's right, bad actors would likely waste little time setting up their own seemingly legitimate app stores to instead spread malware or trojanized apps. They're already able to circumvent current major app stores to do this all the time. But at the end of the day, sideloading is going to be just as secure as you make it, just like current app stores. Every app store like the Epic Games Store will have its own data privacy policy rules and review processes for apps, and in this hypothetical sideloading scenario, it would be up to those stores to enforce those new rules. Sideloading an app is not inherently malicious or risky, but it can be if you don't know where the app you're trying to download is coming from, exactly, or if you don't do enough digging into that store's policies or history. If these laws were to go into effect, it wouldn't be security Armageddon, but it would force users to pay extra close attention to the apps they're downloading. Keep these things in mind any time you go to download a new app, regardless of whether it's from the Apple App Store, Google Play, or anywhere else.

- Make sure the app is verified. On Android phones, you'll see a small badge that says, "Verified by Play Protect."
- Check if any contact information listed in the app's description is legitimate.
- It's never a good idea to click on pop-up ads in apps just to "make them go away."
- Use your phone's settings to see if the app is using unusual amounts of data.
- Customize each app's privacy settings on your phone, restricting location access and other sensitive information to only those apps you truly trust or are needed to make the app function properly.

The one big thing

The ZingoStealer malware is in the wild now and quickly switching owners. By the time we had gotten a good handle on the Hasker's Gang newest malware, the threat actor had already put it up for sale and announced they were transitioning ownership to another group. ZingoStealer leverages

Telegram chat features to facilitate malware executable build delivery and data exfiltration. It can exfiltrate sensitive information such as credentials, steal cryptocurrency wallet information and mine cryptocurrency on victims' systems. Regardless of who owns it, this is still worth watching out for.

Why do I care?

If infected with this malware, the attackers using it can download other information-stealing malware like RedLine, or the XMRig cryptocurrency miner, which could zap your computing power and backpack off your electric bill with you every noticing. This stealer is freely available and can be used by multiple threat actors, and since our initial research push, we've already seen it change hands, so it's impossible to tell where this could head next. We have observed a focus on infecting Russian speaking victims under the guise of game cheats, key generators and pirated software, which likely indicates a current focus on home users.

So now what?

Talos released a ton of traditional coverage for this malware, which you can find in our blog post. It's important to put appropriate protections in place to avoid this malware. Outside of that, as I was writing above, it's always important to double check where you're about to download something from. The attackers in this case are infiltrating Telegram chats and Discord servers to spread fake video game cheats. If you do want to download a mod for a game, make sure it's coming from a legitimate, trusted store.

Other newsy nuggets

U.S. security officials continue to sound alarms over potential cyber attacks from Russian state-sponsored actors. Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, appeared on "60 Minutes" over the weekend to echo the Biden administration's message that federal agencies, companies and private individuals need to be ready for when, not if, a large-scale attack happens. "We are seeing evolving intelligence about Russian planning for potential attacks. And we have to assume that there's going to be a breach. There's going to be an incident. There's going to be an attack," she said in the interview. (CBS News, Politico)

Oracle released its quarterly security update this week, bringing fixes for a whopping 520 vulnerabilities across its massive suite of products. More than 70 of the patches are for vulnerabilities rated "critical," including three that have a severity score of a maximum 10. The company doubled down on its patching message this quarter, too, warning users that its seen attackers actively exploiting previously disclosed, but unpatched, Oracle vulnerabilities. Oracle Fusion Middleware received the most patches, including fixes for 54 vulnerabilities, 41 of which could be remotely exploitable without authentication. (ZDNet, Oracle)

Computer manufacturer Lenovo warned that dozens of their laptops are vulnerable to an attack that could persist even after a hard-drive replacement or operating system re-install. Two of the three vulnerabilities the company disclosed this week deal with the Unified Extensible Firmware Interface (UEFI) drivers. These were meant to only be used during the manufacturing process, but accidentally ended up part of the BIOS image that shipped with the computers. Several models of Lenovo laptops will not receive appropriate patches to fix these issues, as they are already past the End of Development Support cycle. (Dark Reading, PC World)

Can't get enough Talos?

- Beers with Talos Ep. #120: How attackers are finding new ways to bypass MFA
- TeamTNT targeting AWS, Alibaba
- Threat Roundup April 8 - 15
- Talos Takes Ep. #92: Kenna 101 —– How to read a CVE

Upcoming events where you can find Talos

RSA 2022 (June 6 — 9, 2022)

San Francisco, California

Cisco Live U.S. (June 12 — 16, 2022) Las Vegas, Nevada

Most prevalent malware files from Talos telemetry over the past week

SHA 256: e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934 MD5: 93fefc3e88ffb78abb36365fa5cf857c Typical Filename: Wextract Claimed Product: Internet Explorer Detection Name: PUA.Win.Trojan.Generic::85.lp.ret.sbx.tg

SHA 256: 5616b94f1a40b49096e2f8f78d646891b45c649473a5b67b8beddac46ad398e1 MD5: 3e10a74a7613d1cae4b9749d7ec93515 Typical Filename: IMG001.exe Claimed Product: N/A Detection Name: Win.Dropper.Coinminer::1201

SHA 256: 59f1e69b68de4839c65b6e6d39ac7a272e2611ec1ed1bf73a4f455e2ca20eeaa MD5: df11b3105df8d7c70e7b501e210e3cc3 Typical Filename: DOC001.exe Claimed Product: N/A Detection Name: Win.Worm.Coinminer::1201

SHA 256: 125e12c8045689bb2a5dcad6fa2644847156dec8b533ee8a3653b432f8fd5645 MD5: 2c8ea737a232fd03ab80db672d50a17a Typical Filename: LwssPlayer.scr Claimed Product: 梦想之巅幻灯播放器 Detection Name: Auto.125E12.241442.in02

SHA 256: 1a234656f81e870cdeb0e648a6b305a41452c405cca21124de26b54f79d55ad0 MD5: 10f1561457242973e0fed724eec92f8c Typical Filename: ntuser.vbe Claimed Product: N/A Detection Name: Auto.1A234656F8.211848.in07.Talos

Posted by Jon Munshaw at 2:00 PM Labels: Threat Source newsletter Share This Post Facebook share Twitter share Linkedin share Reddit share Email This