Title: Zero-click exploits are a realistic threat to NFT wallets
Author: cryptocached
Created 2022-07-07 04:44:57 UTC
Permalink: /r/GME/comments/vta5ol/zeroclick_exploits_are_a_realistic_threat_to_nft/
Url: https://www.reddit.com/r/GME/comments/vta5ol/zeroclick_exploits_are_a_realistic_threat_to_nft/

There has been some discussion in other stonk subs about potential attacks against the GameStop Wallet, with mixed and messages and dangerously wrong conclusions. I'm here to warn you that zero-click exploits are a realistic threat to NFT wallets. I'm not trying to scare anyone and I don't mean to imply knowledge of current in-the-wild attacks targeting NFT wallets, but I do want to raise awareness of the potential and clear up some common misconceptions.

Zero-click FORCEDENTRY

Zero-click attacks do not require a victim to download and open a malicious file in order to exploit an affected system. The attack is launched without direct interaction when an application automatically renders untrusted content, such as an image, and the rendering process is vulnerable to a 0-day (previously unknown) exploit.

https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware

https://www.pcmag.com/how-to/what-is-a-zero-click-attack

A recent example of a zero-click attack is NSO Group's FORCEDENTRY, which enabled the installation of spyware on iPhones simply by sending a specially crafted file in iMessage. Google's ProjectZero team has an excellent writeup of the technical details behind FORCEDENTRY on their blog.

https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

For the less technically inclined, their summary will reenforce what I just explained about zero-click attacks:

>Recently, however, it has been documented that NSO is offering their clients zero-click exploitation technology, where even very technically savvy targets who might not click a phishing link are completely unaware they are being targeted. In the zero-click scenario no user interaction is required. Meaning, the attacker doesn't need to send phishing messages; the exploit just works silently in the background. Short of not using a device, there is no way to prevent exploitation by a zero-click exploit; it's a weapon against which there is no defense.

In the case of FORCEDENTRY, a specially crafted PDF was sent with a .gif file extension. That was enough to get iMessage to pass the file to the vulnerable system libraries responsible for rendering images and other file types. What happened after that is highly complex to explain, but suffice to say that the exploit gave attackers unfettered access to targeted devices.

While the specific vulnerabilities exploited by FORCEDENTRY have been patched, other vulnerabilities with similar impact exist even in the latest versions of iOS, other operating systems, and applications. These vulnerabilities may yet remain undiscovered, waiting for some diligent researcher to find them. More likely, NSO Group and organizations like them, have collected new vulnerabilities and sat on them or are tirelessly working to do so.

How this affects NFT wallets

NFT wallets are applications that potentially render untrusted content. Anyone can send an NFT to your wallet and, so long as the metadata is presented in the right format, your wallet will display the referenced resources automatically. No direct user interaction with the NFT is required. If a vulnerability is present in the wallet or supporting system libraries, the stage is set for a zero-click attack.

In fact, had the GameStop Wallet been available for iOS before the specific vulnerabilities were patched, it is highly likely that NSO Group's FORCEDENTRY would have been an effective attack and exploitable simply by minting an NFT pointing to the specially crafted GIF/PDF and sending it to a victim's address.

Does this make NFTs unusable?

No, this doesn't make NFTs unusable. Remember, this kind of attack could potentially affect any kind of application that automatically renders untrusted content. NFT wallets are not uniquely susceptible to these attacks. However, NFT wallets do have some features that make them an attractive target. For instance, much like with iMessage, it is easy for an attacker to target a specific victim by sending the exploit to the victim's wallet in place of targeting their phone number. Additionally, the open nature of the blockchain gives an attacker the opportunity to select their targets based on known holding.

What this does mean is that users of NFT wallets need to practice good security in order to keep from becoming victims.

What can be done?

Remember what Google's ProjectZero said about zero-click attacks?

>Short of not using a device, there is no way to prevent exploitation by a zero-click exploit; it's a weapon against which there is no defense.

While that is true, there are things you can do to mitigate risk associated with zero-click attacks. Keeping your software and devices up to date, especially any security updates, is the first line of defense. This is not foolproof against 0-day exploits, but does keep you from being low-hanging fruit, ripe for the picking. In the crypto space there is also the concept of _cold storage_, wallets which are kept offline except when necessary to transact. Using cold storage for NFTs can be problematic if those NFTs provide some kind of utility since you would not be able to use them without bringing the wallet online.

Thankfully there is a market-based mechanism that reduces the likelihood of a zero-click attack being used against NFT Wallets. Specifically that these types of exploits are ridiculously valuable to organizations such as NSO Group and the nation state intelligence services that comprise their clientele. At least for the moment, it is unlikely that they would be willing to burn a valuable asset to steal some NFTs and crypto. However, as the value stored in NFT wallets increases, they may become increasingly attractive targets.

Hopefully this post provides some clarification about the very real, if not immediate, risk of zero-click attacks against NFT wallets. The expensive nature of such an attack provides a temporary reprieve, but it is better to be aware of the threat and learn how to mitigate it than to disregard the potential and ignore the threat until it has materialized.