The security pitfalls of social media sites offering ID-based authentication

blog.talosintelligence.com/threat-source-newsletter-sept-28-2023/

Jonathan Munshaw September 28, 2023

By Jonathan Munshaw

Thursday, September 28, 2023 14:00

Threat Source newsletter

Welcome to this week's edition of the Threat Source newsletter.

Since Elon Musk first started talking about purchasing Twitter/X around this time last year, one of his main sticking points has been how many bot accounts are on the platform and how that potentially affects advertising revenue and user counts.

In the latest advancement in the alleged fight against bots, X recently launched a government ID-based authentication process available to its paid premium users. The social media platform is partnering with a third-party security company to provide advanced, faster support to make it more difficult for others to impersonate the user.

The setup process says it involves the user taking a picture with their computer's camera with their government-issued ID. According to X's Verification Policy, the third-party company only keeps the provided picture for as long as it takes to verify the provided

information, and any ID images are only kept for 72 hours. The information derived from the submitted pictures is stored for 30 days by the third party in the name of providing users "an opportunity to appeal a verification decision and for X to review your appeal."

Meta, Facebook and Instagram's parent company, has been rolling out a similar program called Meta Verified that also asks users to submit photos of a government ID and pay a subscription fee to receive "account verification with impersonation protections and access to increased visibility and support."

Taken at face value, X and Meta's retention policies for these provided images of IDs seem fine. The main issue for me is I don't really see what the concrete benefits here are.

On X, submitting the ID information and paying for the premium subscription only says it provides faster support, and an additional verification badge on a user's account along with the now-infamous blue checkmark. The option is not available to business or organizational accounts, which seems like it'd be the space most ripe for impersonation — I've certainly observed my fair share of Talos-impersonated accounts on that platform where someone tried passing as our organization.

X is also saying it will only look into future benefits for this verification program, which "may explore additional measures, such as ensuring users have access to age-appropriate content and protecting against spam and malicious accounts." The service still isn't offered in the EU and U.K., either, presumably because of the stricter data privacy laws in those regions.

When these verification procedures are in place, there's no guarantee they work, either. My sister-in-law had her Instagram/Meta account taken over by a cryptocurrency spammer last year, and even when she submitted a 360-degree selfie and images of her government-issued ID to Instagram, they denied her claim that her account was hacked, and to this day it's still sending cryptocurrency spam to her family members even though she's created a new account. Her appeal was not accepted by the company, either.

That's one very specific case, I know, but if I'm going to start sending these companies with dubious security histories pictures of my driver's license, I'm going to need a bit more than promises of future features and vague support promises before I'm sold on this method of multi-factor authentication.

The one big thing

Google Chrome users should update their browsers as soon as possible after the company disclosed multiple, serious vulnerabilities. Google initially disclosed CVE-2023-4863 as a heap buffer overflow in the WebP image format in Chrome. However, on Wednesday, it released a new advisory with CVE-2023-5129 identifying that the vulnerability actually existed in libwebp, meaning it affects multiple applications and not just Chrome. The

updated advisory also elevated the severity score to a maximum 10 out of 10. This week, Talos also disclosed CVE-2023-3421, a use-after-free vulnerability that affects Chrome. An attacker could exploit this vulnerability by tricking the target into visiting a specially crafted HTML web page.

Why do I care?

Chrome is a very popular web browser, and its Chromium open-source version serves as the basis for many other browsing software. The fact that critical WebP vulnerability is particularly notable because WebP is the new default file format that most images use when processed in Chrome. According to the advisory, “With a specially crafted WebP lossless file, libwebp may write data out of bounds to the heap,” if an attacker exploits CVE-2023-5129.

So now what?

The advice here is pretty simple — update your Google Chrome if you haven’t already!

Top security headlines of the week

MGM casinos went back online last week after 10 days due to a ransomware attack. The company’s casinos and hotels were able to fix all issues pertaining to guest services and the electronic slot machines that had been taken down due to the attack. One estimate suggests the outage may have cost the company upward of $80 million. The Scattered Spider threat actor is taking credit for the attack, partnering with known ransomware magnate ALPHV. Security researchers believe Scattered Spider is actually a hacking group that calls itself Star Fraud. New research presented at LABScon last week also stated that the group infiltrated MGM and Caesars, another casino manager, after gaining access to Okta authentication servers. (Washington Post, Associated Press)

A hacking group claims to have breached “all of Sony [SIC] Systems” and is reportedly selling stolen data on the dark web. A new group called Ransomed.vc is taking credit for the alleged attack and says it accessed more than 6,000 files from the tech giant known for producing the PlayStation video game console. Sony says it is still investigating the group’s claims. Despite the name, Ransomed.vc is actually an extortion group and does not have its own encryptor. Instead, it plans to sell the data on the dark web for $2.5 million. However, other threat actors have since stepped up to also take credit for the attack, leaving exact attribution in doubt. Another threat actor calling themselves MajorNelson says they “leaked for free" a 2.4 GB compressed archive that contains 3.14 GB of uncompressed data it claims belongs to Sony. (Bleeping Computer, Kotaku)

A new ransomware-as-a-service syndicate ShadowSyndicate is reportedly operating a massive network of servers that's connected to other large ransomware families. Security researchers say the group has potential ties to the ALPHV ransomware group and other ransomware families like Clop, Play, Royal and Cactus. A new report outlines dozens of systems that ShadowSyndicate controls, including 52 containing the group's secure shell (SSH) fingerprint it uses as Cobalt Strike beacons to manage and coordinate its various malware campaigns. It's currently unclear if ShadowSyndicate is truly a ransomware-as-a-service group or more of an initial access broker. (DarkReading, SC Magazine)

Can't get enough Talos?

Upcoming events where you can find Talos

Grace Hopper Celebration (Sept. 26 - 29)

Orlando, Florida

> *Caitlin Huey, Susan Paskey and Alexis Merritt present a "Level Up Lab" titled "Don't Fail Knowledge Checks: Accelerating Incident Response with Threat Intelligence." Participate in several fast-paced activities that emphasize the importance of threat intelligence in security incident investigations. Attendees will act as incident responders investigating a simulated incident that unfolds throughout this session. Periodic checkpoints will include discussions that highlight how incident response and threat intelligence complement each other during an active security investigation.*

ATT&CKcon 4.0 (Oct. 24 - 25)

McLean, Virginia

> *Nicole Hoffman and James Nutland discuss the MIRE ATT&CK framework in "One Leg to Stand on: Adventures in Adversary Tracking with ATT&CK." Even though ATT&CK has become an industry standard for cyber threat intelligence reporting, all too often, techniques are thrown at the bottoms of reports and blogs without any context never to be seen again after dissemination. This is not useful for intelligence producers or consumers. In this presentation, Nicole and James will show analysts how to use ATT&CK as a guideline for creating a contextual knowledge base for adversary tracking.*

misecCON (Nov. 17)

Lansing, Michigan

> *Terryn Valikodath from Talos Incident Response will deliver a talk providing advice on the best ways to conduct analysis, learning from his years of experience (and mishaps). He will speak about the everyday tasks he and his Talos IR teammates must go through to properly perform analysis. This talk covers topics such as planning, finding evil, recording findings, correlation and creating your own timelines.*

Most prevalent malware files from Talos telemetry over the past week

SHA 256: e2cdf48bc6741afd7aba54d7c0b30401d2d6dd06138979ca73f3167915bf22b3
MD5: eba4ad9540713d5956ab0b6a566c1487
Typical Filename: webnavigatorbrowser.exe
Claimed Product: WebNavigatorBrowser
Detection Name: Win64:WebNav.26k0.rlsync.Talos

SHA 256: 0e2263d4f239a5c39960ffa6b6b688faa7fc3075e130fe0d4599d5b95ef20647
MD5: bbcf7a68f4164a9f5f5cb2d9f30d9790
Typical Filename: bbcf7a68f4164a9f5f5cb2d9f30d9790.vir
Claimed Product: N/A
Detection Name: Win.Dropper.Scar::1201

SHA 256: 7f66d4580871e3ee6a35c8fef6da7ab26a93ba36b80279625328aaf184435efa
MD5: e9a6b1346d1a2447cabb980f3cc5dd27
Typical Filename: профиль 10 класс.exe
Claimed Product: N/A
Detection Name: Application_Blocker

SHA 256: a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91
MD5: 7bdbd180c081fa63ca94f9c22c457376
Typical Filename: c0dwjdi6a.dll
Claimed Product: N/A
Detection Name: Trojan.GenericKD.33515991