Russian hackers bypass 2FA by annoying victims with repeated push notifications

By Catalin Cimpanu

Published: 2022-12-21 · Archived: 2026-04-06 00:05:49 UTC

Nobelium, the Russian cyber-espionage group that has orchestrated the SolarWinds 2020 supply chain attack, has continued to carry out new attacks throughout 2021, and according to security firm Mandiant, has been using a clever trick to bypass two-factor authentication in order to access some of its targets' accounts.

The technique, detailed in a report published on Monday, involves abusing the push notification feature of some online accounts.

2FA (two-factor authentication) or MFA (multi-factor authentication) push notifications are typically used as an alternative to receiving one-time codes via SMS or email, and they take the form of a popup that appears on a smartphone.

When a user logs into an account with valid credentials, a push notification is shown on their smartphone, with details about the type and IP address of the device trying to access the account and asking for permission to allow the operation to go through.

2FA push notifications aren't widely adopted, but they are considered safer than email or SMS as a 2FA method because attackers would need physical access to a victim's smartphone in order to bypass it.

But on Monday, Mandiant researchers said they'd investigated several incidents where Nobelium members gained access to a user's valid login credentials, and they repeatedly attempted to log into the account, triggering repeated 2FA push notifications on the victim's device until the target eventually accepted the request.

It is unclear if these victims accepted the push notification by accident; because they thought it might have been a bug; or by sheer annoyance.

Because Nobelium often uses IP proxies in the same geographical area as the victim to avoid triggering a target's scrutiny over login requests from strange IPs, this might explain why some victims accepted the attacker's into their accounts.

Nobelium continues to operate with advanced tradecraft

All in all, the Mandiant report paints the picture of an apex threat actor that continues to showcase "top-notch operational security and advanced tradecraft," and will certainly not be defined by the SolarWinds hack as its sole successful operation.

Among the group's most recent tactics and operations, Mandiant also highlighted:

- Intrusions and compromises of multiple cloud providers, from where the group pivoted to their respective downstream customer systems.
- The use of login credentials most likely acquired from the black market, from the operators of the CRYPTBOT infostealer.
- The use of hacked accounts with Application Impersonation privileges [1, 2] to harvest sensitive mail data since Q1 2021.
- The extraction of virtual machines from compromised networks to determine internal routing configurations.
- The use of a new malware strain named CEELOADER, as the initial entry point and used later to drop new malware binaries.
- The use of residential IP addresses ranges to authenticate into victim environments.
- The use of Azure servers to collect data that are geo-located in the same cloud zone as the victim network to avoid triggering security alerts.
- The use of hacked WordPress sites to store their malware.
- The extensive use of Tor, VPNs, and VPS servers to disguise their real location when conducting reconnaissance and attacks.
- Attempts to circumvent or delete system logging within the victim's environment.

In April this year, the White House formally linked the Nobelium threat actor to the Russian Foreign Intelligence Service, also known as the SVR, the same agency which security experts believe is behind the APT29 (Cozy Bear) threat actor.

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
