Multi-Factor Authentication: Headache for Cyber Actors Inspires New Attack Techniques

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/multi-factor-authentication-new-attacks

Threat Hunter TeamSymantec

In recent years two-factor or multi-factor authentication (MFA) has been touted as the way to protect your personal and business accounts from attack. This led to the wide adoption of MFA - from corporate accounts to social media profiles, almost all provide the option of enabling MFA, with many requiring it.

This means that, for attackers, stealing credentials or brute forcing passwords is no longer enough - if they don't have access to victims' multi-factor access token or code they will still not be able to access their accounts. The increasing use of MFA means that attackers have had to endeavor to find ways to bypass it, or avoid carrying out attacks that may be stalled by it. When we look at recent high-profile attacks, such as SolarWinds, the Microsoft Exchange Server ProxyLogon attacks, and the vulnerabilities found in Pulse Secure VPN recently, all these attacks help attackers avoid the hurdle of needing to overcome MFA.

While MFA has perhaps only gained wide adoption in the last couple of years, attacks attempting to bypass MFA date as far back as 2011, when RSA Security was forced to replace 40 million SecurID tokens - which were used for MFA at the time - after the company was hacked.

However, recently, there have been some more notable examples of attacks that attempt to either bypass MFA, or eradicate the need to bypass it at all, with five of these outlined in this blog.

Recent zero-day vulnerability in Pulse Secure VPN (CVE-2021-22893)

On April 20, 2021, Pulse Secure published an advisory warning about a zero-day remote code execution vulnerability in its popular VPN product. On the same day, FireEye published a blog detailing how the vulnerability (CVE-2021-22893) was being exploited by a China-linked APT group it tracks as UNC2630. FireEye said this group was attempting to leverage the vulnerability in attacks targeting defense industrial base (DIB) targets in the U.S.

This new vulnerability was exploited, alongside a number of known Pulse Secure vulnerabilities, as the initial infection vector in these attacks. FireEye said that at least 12 malware families have been associated with exploit attempts against vulnerabilities in Pulse Secure. The malware was associated with what appears to be three threat actors, with attacks taking place in organizations in the U.S. and Europe.

The UNC2630 activity that was analyzed by FireEye demonstrated that successfully exploiting this vulnerability in the VPN software allowed attackers to Trojanize shared objects with malicious code to log credentials and bypass authentication flows, including multi-factor authentication requirements. FireEye said it was tracking this activity as SlowPulse. The attackers were also able to maintain persistence, inject web shells, and modify files.

VPNs became a very popular target for hackers over the last year, as increased working from home due to the pandemic meant that workers were increasingly using VPNs to log into their corporate networks. If an attacker is able to compromise the VPN software - through a vulnerability like this - it negates a need for them to acquire anything more in the line of multi-factor authentication.

A patch for this bug was issued on Monday (May 3), and all users of Pulse Secure should apply it quickly.

Symantec has released Hacktool.Webshell and Hacktool.Atrium to block files believed to be related to this vulnerability.

Microsoft Exchange Server (ProxyLogon) attacks

On March 2, Microsoft released emergency patches for four zero-day vulnerabilities in Microsoft Exchange Server that were being actively exploited by attackers in the wild. At the time, Microsoft said these vulnerabilities were being exploited by an APT group it dubbed Hafnium (Symantec tracks this group as Ant) in targeted attacks. However, it quickly became apparent that multiple threat actors had started exploiting these vulnerabilities, with numbers rising rapidly once the existence of the vulnerabilities became public knowledge.

Two of the vulnerabilities (CVE-2021-26855 and CVE-2021-27065) and the technique used to chain them together for exploitation were given the name "ProxyLogon". Successful exploitation of these vulnerabilities allowed unauthenticated attackers to execute arbitrary code on vulnerable Exchange Servers, allowing them to gain persistent system access, access to files and mailboxes on the server, and access to credentials stored on the system. Successful exploitation may also allow attackers to compromise trust and identity in a vulnerable network. This gives attackers extensive access to infected networks, allowing them to steal potentially highly sensitive information from victim organizations, without the need to bypass any multi-factor authentication steps. In several instances the threat actors using these vulnerabilities were seen stealing emails from victim inboxes.

To learn how Symantec helps protect you from these attacks, read our blog: *How Symantec Stops Microsoft Exchange Server Attacks*

SolarWinds

The SolarWinds attacks were uncovered in December 2020, and have rarely been out of the headlines since, with the U.S. recently announcing that it would be imposing sanctions against Russia as a response to the SolarWinds breach, as well as a number of other cyber attacks. The statement from U.S. officials said they had "high confidence" that the SVR, the Russian Foreign Intelligence Service - also known as APT29, Cozy Bear, The Dukes - was responsible for the SolarWinds attack.

The SolarWinds incident is believed to have started in around March 2020, with any user of SolarWinds Orion software who downloaded an update between March and December 2020 believed to have become infected with the first-stage malware, Backdoor.Sunburst. The initial infection of victims was indiscriminate, but only a small number of those who downloaded the initial compromised update saw additional malicious activity on their networks.

The motivation of the SolarWinds attackers was always believed to be information stealing, with email appearing to be an area of particular interest to them. The attackers were also seen using various techniques to bypass MFA in the course of their attacks. In one incident, security firm Veloxity said it saw the attackers using a novel technique to bypass 2FA provided by Duo, though the same technique would likely bypass MFA from any provider that requires integration secrets stored in the potentially compromised environment. After gaining administrator privileges on an infected network, the hackers used those rights to steal a Duo

secret known as an “akey” from a server running Outlook Web App (OWA), which enterprises use to provide account authentication for various network services. The hackers then used the “akey” to generate a cookie, so they’d have it ready when someone with the right username and password would need it when taking over an account.

In another report, FireEye described the techniques it saw the attackers using. Among the techniques FireEye saw were:

- Attackers stealing the Active Directory Federation Services (AD FS) token-signing certificate and using it to forge tokens for arbitrary users, which would allow the attacker to authenticate into a federated resource provider (such as Microsoft 365) as any user, without the need for that user’s password or MFA.
- Modifying or adding trusted domains in Azure AD to add a new federated identity provider (IdP) that the attacker controls. This would allow the attacker to forge tokens for arbitrary users.
- Compromising the credentials of on-premises user accounts that are synchronized to Microsoft 365 and are assigned high privileged directory roles, such as administrator.
- Hijacking an existing Microsoft 365 application by adding a rogue credential to it in order to use the legitimate permissions assigned to the application, such as the ability to read email, send email as an arbitrary user, access user calendars, etc., while bypassing MFA.

Attackers know they need a way to bypass or avoid MFA altogether if they want to access victims’ email accounts, which still appears to be the goal of many sophisticated attackers, including state-sponsored actors like those behind SolarWinds.

Read all our SolarWinds research, and how Symantec helps protect you, on our dedicated blog page.

Hackers targeting Iranian dissidents seek to steal 2FA text codes

In September 2020, Check Point published research on the Rampant Kitten hacking group, which it said had developed a new Android malware that was capable of intercepting and stealing 2FA codes sent via text. It is known that text 2FA is significantly less secure than using an app or token - as tactics like SIM swapping (where a malicious actor gains access to your phone number) would allow codes to be intercepted - and many security experts think neither organizations nor individuals should be using this kind of 2FA if there is another option.

Check Point said Rampant Kitten’s surveillance campaign had been ongoing for as long as six years, targeting dissidents and minorities in Iran. The malware was hidden inside an app that purported to be designed to help Iranian citizens get a Swedish driver's license. However, as well as harvesting contacts, old text messages, and recording using the microphone, the malicious app was also designed to look for SMS messages that contained

a "G-" string, which is a prefix used by Google as part of the two-factor authentication process. The attackers would send phishing messages to victims in order to harvest their credentials, and would then also be able to access their 2FA codes and gain access to their accounts. The malware also forwarded all text messages to the attackers, meaning they could bypass 2FA for any other apps or services using text message 2FA too.

Chinese attackers attempting to bypass 2FA

Back in 2019, FOX-IT blogged about a Chinese state-sponsored group - APT20 - that was bypassing 2FA in its attacks. FOX-IT had been monitoring the attacker's activity over a period of two years, stating that it used living-off-the-land techniques to maintain a stealthy presence on victims' networks in order to siphon off data for the purposes of espionage. FOX-IT found evidence the attackers had connected to VPN accounts that were protected by 2FA, with the researchers theorizing that they did this by stealing an RSA SecurID software token from a hacked system, which they then used to generate valid one-time codes and bypass 2FA at will.

As FOX-IT explained at the time: "The software token is generated for a specific system, but of course this system specific value could easily be retrieved by the actor when having access to the system of the victim.

"As it turns out, the actor does not actually need to go through the trouble of obtaining the victim's system specific value, because this specific value is only checked when importing the SecurID Token Seed, and has no relation to the seed used to generate actual two-factor tokens. This means the actor can actually simply patch the check which verifies if the imported soft token was generated for this system, and does not need to bother with stealing the system specific value at all.

"In short, all the actor has to do to make use of the two-factor authentication codes is to steal an RSA SecurID Software Token and to patch one instruction, which results in the generation of valid tokens."

Worrying trend

While it has been known for some time that some advanced persistent threat (APT) groups and sophisticated actors were able to bypass MFA in some instances, the recent sophisticated attacks that appear to have bypassing these kinds of protections as one of their main goals provides a reminder no single solution is sufficient.

Fortunately, these attacks also show MFA is working as attackers need to go to great lengths to find alternative means to breach MFA-protected organizations. Organizations should take additional steps to increase protection, such as:

- Auditing login and Active Directory events

- Reviewing and reducing services and accounts that do not require MFA
- Keeping up to date on patches for any discovered vulnerabilities
- Considering a threat model where MFA may be bypassed or on-site secrets may be compromised
- Expanding their zero trust architecture beyond simple 2FA.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.