Threat Intel Report

Prepared by:

Converge Cybersecurity Practice

October 27, 2022

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

convergetp.com | 800.747.8585

As security professionals, we stress the importance of following policies, procedures, and best practices to protect our organizations. But if these practices add too much friction to people's work and lives, users will flout them. If the secure route is hectic or annoying, people will find another way to get the job done and move on with their day.

With the recent breach of Uber, much attention has been given to MFA fatigue. Merriam-Webster defines fatigue as "a state or attitude of indifference or apathy brought on by overexposure, as to a repeated series of similar events or appeals." Certainly, user behavior sometimes reflects a fall into the realm of fatigue—like clicking "approve" to stop a string of seemingly buggy MFA requests.

Too often, however, it's cumbersome processes for security that cause people to make insecure choices, especially if they don't fully understand the rationale behind those processes. That's why we as security teams need to continually identify areas of improvement in processes and workflows.

When it comes to MFA, this means not just implementing policy to ensure we have secure authentication, but also educating users as to its importance, streamlining their MFA process, and making it easy for them to report abnormalities. It also means making changes on the back end: identifying malicious activity via logging and detection and using MFA-native threat intelligence tools if available, such as Okta Insights or Microsoft's suspicious activity alerting.

Security is a balance of people, processes, and technology. The challenge is finding the best ways for the three areas to work in sync without one creating friction for another.

Updates

Critical infrastructure in the crosshairs

The war between Russia and Ukraine continues into its ninth month and its effects continue to ripple outward.

In late September, explosions were detected near the Nord Stream 1 and 2 natural gas pipelines in the Baltic Sea, after which leaks in the pipelines were discovered. With Danish and Swedish authorities both now confirming that the pipelines were damaged by explosives, the world remains divided as to the attribution of the perpetrator. Russia has suggested the attack was instigated by the US, while the US and NATO countries strongly suspect sabotage by Russia.

The damage to the pipeline has once again underscored the vulnerability of critical infrastructure. Putin himself warned on October 12 that the world's energy infrastructure is at risk, and the frequency of recent damage incidents to European submarine fiber optic internet cables has alarmed some experts.

As ever, security practitioners should remain vigilant. With Russia at war, disruption is key to preventing NATO and other allies of Ukraine from interfering with its progress.

Threats

Uber breach highlights MFA fatigue, hard-coded credentials

Primary impact: Organizations using MFA

September's breach of Uber was notable for the expansive access to a high-profile organization that the threat actor achieved. In a ransomware attack, an attacker only needs access to a few pieces of critical infrastructure to deliver the payload and demand payment. Uber's attacker, however, obtained access to much of the Uber environment.

The attacker penetrated the environment by compromising the account of an Uber external contractor. The ridesharing company said the threat actor, which it believes is affiliated with Lapsus$, likely purchased the account credentials on the dark web following a malware infection of the contractor's device.

Our September report mentioned MFA fatigue as a rising attack tactic; the Uber breach has since spotlighted the technique. The threat actor repeatedly attempted to log in to the account, bombarding the contractor with MFA requests until the contractor finally confirmed.

While MFA fatigue granted initial access, it was hard-coded admin credentials discovered by the attacker once inside the environment that allowed deep and wide access to several internal systems. The existence of hard-coded credentials can often be attributed to a combination of overly complex policies plus a lack of policy enforcement, leading to employees using shortcuts to get things done.

Recommendations: Ensure that employees are aware of the tactic of MFA fatigue and equip them with easy ways to reach out to security teams if they encounter similar activity.

Microsoft Teams stores tokens in plaintext

Primary impact: Organizations using Microsoft Teams

Communication is key in every organization. As security teams, we monitor our email and our Azure AD from the perspective of what's coming in and going out. But are we monitoring the communication platforms we use internally for day-to-day operations?

One of the biggest internal communication platforms within the market space is Microsoft Teams. Security researchers at Vectra have identified a flaw in which the desktop version of Teams stores authentication tokens in unprotected clear text. With a user's token, a threat actor would be able to use the Microsoft Teams API to access an organization's Microsoft 365 infrastructure.

Microsoft has said that to exploit the flaw, an attacker would need to have already compromised a system on the target network. But an actor spreading ransomware across the network already has initial access, and likely has access to a device that uses Teams.

The same tokens also allow a threat actor to query for deleted messages and recover any messages deleted within the past 21 days. We preach proper password hygiene, but how many users have sent a credential to a colleague in Teams and later deleted it?

Most organizations enable logging for O365. However, by default, O365 only logs for emails in Office—it does not log API calls that are sent to the Microsoft Teams API. Enabling logging specifically in Teams is recommended.

Recommendations

- Configure FIM (file integrity monitoring) and system monitoring to identify processes accessing these sensitive files:
  - **[Windows] %AppData%\Microsoft\Teams\Cookies**
  - **[Windows] %AppData%\Microsoft\Teams\Local Storage\leveldb**
  - **[macOS] ~/Library/Application Support/Microsoft/Teams/Cookies**
  - **[macOS] ~/Library/Application Support/Microsoft/Teams/Local Storage/leveldb**
  - **[Linux] ~/.config/Microsoft/Microsoft Teams/Cookies**
  - **[Linux] ~/.config/Microsoft/Microsoft Teams/Local Storage/leveldb**
- Restrict the use of Teams and Office 365 to end user devices only—company-controlled assets and mobile phones.
- Ensure logging of Microsoft Teams.

CrowdStrike reports reduced breakout time, malware-free activity

Primary impact: All organizations

The newest edition of CrowdStrike's yearly threat hunting report tracked a reduction in attacker breakout time—the time it takes for an attacker to move from the compromised host to another system in the network. This year's average is an hour and 24 minutes, a reduction of 14 minutes from 2021. This trend continues to show that our adversaries work quickly, so organizations must be able to detect and respond within that breakout period if they wish to reduce risk and eradicate the adversary.

Malware-free activity accounted for 71% of all detections indexed by CrowdStrike's threat graph. That means nearly three-quarters of all attacks observed by CrowdStrike don't need malware or fancy obfuscated payloads—adversaries can work with the various tools and services native to an operating system to accomplish their objective.

When it comes to phishing, there is a noticeable increase in the shift away from macro-based phishing attacks towards ISO-based attacks, most likely a response from threat actors to Microsoft's announcement that it would begin disabling internet-enabled macros in Office documents by default.

Finally, all signs point to the fact that adversaries are following the increasing trend in cloud adoption and are quickly building their capability to navigate and exploit cloud workloads.