Microsoft Internal Solorigate Investigation – Final Update

msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/

We believe the Solorigate incident is an opportunity to work with the community, to share information, strengthen defenses and respond to attacks. We have now completed our internal investigation into the activity of the actor and want to share our findings, which confirm that we found no evidence of access to production services or customer data. The investigation also found no indications that our systems at Microsoft were used to attack others. Because of our defense-in-depth protections, the actor was also not able to gain access to privileged credentials or leverage the SAML techniques against our corporate domains.

Additional Details

As we previously reported, we detected unusual activity in December and took action to secure our systems. Our analysis shows the first viewing of a file in a source repository was in late November and ended when we secured the affected accounts. We continued to see unsuccessful attempts at access by the actor into early January 2021, when the attempts stopped.

There was no case where all repositories related to any single product or service was accessed. There was no access to the vast majority of source code. For nearly all of code repositories accessed, only a few individual files were viewed as a result of a repository search.

For a small number of repositories, there was additional access, including in some cases, downloading component source code. These repositories contained code for:

- a small subset of Azure components (subsets of service, security, identity)
- a small subset of Intune components
- a small subset of Exchange components

The search terms used by the actor indicate the expected focus on attempting to find secrets. Our development policy prohibits secrets in code and we run automated tools to verify compliance. Because of the detected activity, we immediately initiated a verification process for current and historical branches of the repositories. We have confirmed that the repositories complied and did not contain any live, production credentials.

Lessons Learned

The cybersecurity industry has long been aware that sophisticated and well-funded actors were theoretically capable of advanced techniques, patience, and operating below the radar, but this incident has proven that it isn't just theoretical. For us, the attacks have reinforced two key learnings that we want to emphasize —embracing a Zero Trust mindset and protecting privileged credentials.

A Zero Trust, "assume breach" philosophy is a critical part of defense. Zero Trust is a transition from implicit trust—assuming that everything inside a corporate network is safe—to the model that assumes breach and explicitly verifies the security status of identity, endpoint, network, and other resources based on all available signals and data. We've recently shared guidance for using Zero Trust principles to protect against sophisticated attacks like Solorigate.

Protecting credentials is essential. In deployments that connect on-premises infrastructure to the cloud, organizations can delegate trust to on-premises components. This creates an additional seam that organizations need to secure. A consequence of this decision is that if the on-premises environment is compromised, this creates opportunities for attackers to target cloud services. We strongly recommend mastering identity in the Cloud, as described in protecting your M365 cloud services from on-premise attacks.

We have also shared additional insights on these best practices in Turning the page on Solorigate and opening the next chapter for the security community. Though our internal investigation is closing, it does not mean we are done. It means we are maintaining our normal Zero Trust security posture, where our security teams work continually to protect users, devices and data from ongoing threats to our environment. Our collaborative work with the cybersecurity community to protect from ongoing threats continues and, as we learn more, we will share learnings and guidance as appropriate.