SolarWinds Hackers Also Breached Malwarebytes Cybersecurity Firm

Malwarebytes on Tuesday said it was breached by the same group who broke into SolarWinds to access some of its internal emails, making it the fourth major cybersecurity vendor to be targeted after FireEye, Microsoft, and CrowdStrike.

The company said its intrusion was not the result of a SolarWinds compromise, but rather due to a separate initial access vector that works by "abusing applications with privileged access to Microsoft Office 365 and Azure environments."

The discovery was made after Microsoft notified Malwarebytes of suspicious activity from a dormant email protection app within its Office 365 tenant on December 15, following which it performed a detailed investigation into the incident.

"While Malwarebytes does not use SolarWinds, we, like many other companies were recently targeted by the same threat actor," the company's CEO Marcin Kleczynski said in a post. "We found no evidence of unauthorized access or compromise in any of our internal on-premises and production environments."

The fact that initial vectors beyond SolarWinds software were used adds another missing piece to the wide-ranging espionage campaign, now believed to be carried out by a threat actor named UNC2452 (or Dark Halo), likely from Russia.

Indeed, the US Cybersecurity and Infrastructure Security Agency (CISA) said earlier this month it found evidence of initial infection vectors using flaws other than the SolarWinds Orion platform, including password guessing, password spraying, and inappropriately secured administrative credentials accessible via external remote access services.

"We believe our tenant was accessed using one of the TTPs that were published in the CISA alert," Kleczynski explained in a Reddit thread.

Malwarebytes said the threat actor added a self-signed certificate with credentials to the principal service account, subsequently using it to make API calls to request emails via Microsoft Graph.

The news comes on the heels of a fourth malware strain called Raindrop that was found deployed on select victim networks, widening the arsenal of tools used by the threat actor in the sprawling SolarWinds supply chain attack.

FireEye, for its part, has published a detailed rundown of the tactics adopted by the Dark Halo actor, noting that the attackers leveraged a combination of as many as four techniques to move laterally to the Microsoft 365 cloud.

- Steal the Active Directory Federation Services (AD FS) token-signing certificate and use it to forge tokens for arbitrary users

- Modify or add trusted domains in Azure AD to add a new federated Identity Provider (IdP) that the attacker controls.

- Compromise the credentials of on-premises user accounts that are synchronized to Microsoft 365 that have high privileged directory roles, and

- Backdoor an existing Microsoft 365 application by adding a new application

The Mandiant-owned firm has also released an auditing script, called Azure AD Investigator, that it said can help companies check their Microsoft 365 tenants for indicators of some of the techniques used by the SolarWinds hackers.

How to protect from this attack:

- Ensure that all secret keys associated with MFA or other sensitive integrations are reset following a breach.

- Make sure all credentials in an organization, including service accounts, are reset following a breach and that default passwords or those similar to previous passwords are not used.

References:

- https://thehackernews.com/2021/01/solarwinds-hackers-also-breached.html?&web_view=true
- https://www.businessinsider.com/cybersecurity-firm-malwarebytes-was-breached-by-solarwinds-hackers-2021-1
- https://www.techtimes.com/articles/256120/20210119/malwarebytes-hack-determines-same-perp-dark-halo-solarwinds-attack%E2%80%94assures-products.htm