Malwarebytes targeted by Nation State Actor implicated in SolarWinds breach. Evidence suggests abuse of privileged access to Microsoft Office 365 and Azure environments

blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments/

Marcin Kleczynski

January 19, 2021

A nation state attack leveraging software from SolarWinds has caused a ripple effect throughout the security industry, impacting multiple organizations. We first reported on the event in our December 14 blog and notified our business customers using SolarWinds asking them to take precautionary measures.

While Malwarebytes does not use SolarWinds, we, like many other companies were recently targeted by the same threat actor. We can confirm the existence of another intrusion vector that works by abusing applications with privileged access to Microsoft Office 365 and Azure environments. After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails. We found no evidence of unauthorized access or compromise in any of our internal on-premises and production environments.

How did this impact Malwarebytes?

We received information from the Microsoft Security Response Center on December 15 about suspicious activity from a third-party application in our Microsoft Office 365 tenant consistent with the tactics, techniques and procedures (TTPs) of the same advanced threat actor involved in the SolarWinds attacks.

We immediately activated our incident response group and engaged Microsoft's Detection and Response Team (DART). Together, we performed an extensive investigation of both our cloud and on-premises environments for any activity related to the API calls that triggered the initial alert. The investigation indicates the attackers leveraged a dormant email protection product within our Office 365 tenant that allowed access to a limited subset of internal company emails. We do not use Azure cloud services in our production environments.

Considering the supply chain nature of the SolarWinds attack, and in an abundance of caution, we immediately performed a thorough investigation of all Malwarebytes source code, build and delivery processes, including reverse engineering our own software. Our internal systems showed no evidence of unauthorized access or compromise in any on-premises and production environments. Our software remains safe to use.

What we know: SolarWinds Attackers Also Target Administrative and Service Credentials

As the US Cybersecurity and Infrastructure Security Agency (CISA) stated, the adversary did not only rely on the SolarWinds supply-chain attack but indeed used additional means to compromise high-value targets by exploiting administrative or service credentials.

In 2019, a security researcher exposed a flaw with Azure Active Directory where one could escalate privileges by assigning credentials to applications. In September 2019, he found that the vulnerability still existed and essentially lead to backdoor access to principals' credentials into Microsoft Graph and Azure AD Graph.

Third-party applications can be abused if an attacker with sufficient administrative privilege gains access to a tenant. A newly released CISA report reveals how threat actors may have obtained initial access by password guessing or password spraying in addition to exploiting administrative or service credentials. In our particular instance, the threat actor added a self-signed certificate with credentials to the service principal account. From there, they can authenticate using the key and make API calls to request emails via MSGraph.

For many organizations, securing Azure tenants may be a challenging task, especially when dealing with third-party applications or resellers. CrowdStrike, which was also targeted but in an unsuccessful attempt, has released a tool to help companies identify and mitigate risks in Azure Active Directory.

Coming together as an industry

While we have learned a lot of information in a relatively short period of time, there is much more yet to be discovered about this long and active campaign that has impacted so many high-profile targets. It is imperative that security companies continue to share information that can help the greater industry in times like these, particularly with such new and complex attacks often associated with nation state actors.

We would like to thank the security community, particularly FireEye and Microsoft for sharing so many details regarding this attack. In an already difficult year, security practitioners and incident responders responded to the call of duty and worked throughout the holiday season, including our own dedicated employees. The security industry is full of exceptional people who are tirelessly defending others, and today it is strikingly evident just how essential our work is moving forward.

Update: Clarified statement about “Azure Active Directory weakness”.
Update 2: Clarified that the attack on CrowdStrike was not successful