Important steps for customers to protect themselves from recent nation-state cyberattacks

blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

December 14, 2020

Today, Microsoft is sharing information and issuing guidance about increased activities from a sophisticated threat actor that is focused on high value targets such as government agencies and cybersecurity companies. We believe this is nation-state activity at significant scale, aimed at both the government and private sector. While we aren't sharing any details specific to individual organizations, it is important for us to share greater detail about some of the threat activity we've uncovered over the past weeks, along with guidance that security industry practitioners can use to find and mitigate potential malicious activity.

We also want to reassure our customers that we have not identified any Microsoft product or cloud service vulnerabilities in these investigations.

As part of our ongoing threat research, we monitor for new indicators that could signal attacker activity. As we recently shared in our 2020 Digital Defense Report, we've delivered over 13,000 notifications to customers attacked by nation states over the past two years and have observed a rapid increase in sophistication and operational security capabilities.

FireEye's recent disclosure is consistent with the attacks that we've observed, and we commend FireEye's disclosure and sharing, as we strongly believe this industry sharing is critical to protecting the internet.

Because of the sophistication of the techniques and operational security capabilities of the actor, we want to encourage greater scrutiny by the broader community. While these elements aren't present in every attack, these techniques are part of the toolkit of this actor.

- An intrusion through malicious code in the SolarWinds Orion product. This results in the attacker gaining a foothold in the network, which the attacker can use to gain elevated credentials. Microsoft Defender now has detections for these files. Also, see SolarWinds Security Advisory.
- An intruder using administrative permissions acquired through an on-premises compromise to gain access to an organization's trusted SAML token- signing certificate. This enables them to forge SAML tokens that impersonate any of the organization's existing users and accounts, including highly privileged accounts.
- Anomalous logins using the SAML tokens created by a compromised token-signing certificate, which can be used against any on-premises resources (regardless of identity system or vendor) as well as against any cloud environment (regardless of vendor) because they have been configured to trust the certificate. Because the SAML tokens are signed with their own trusted certificate, the anomalies might be missed by the organization.
- Using highly privileged accounts acquired through the technique above or other means, attackers may add their own credentials to existing application service principals, enabling them to call APIs with the permission assigned to that application.

Please see customer guidance on recent nation-state cyberattacks for specific details and guidance.

We believe it's important to share significant threat activity like what we're announcing today. We think it's critical that governments and the private sector are increasingly transparent about nation-state activity so we can all continue the global dialogue about protecting the internet. We also hope publishing this information helps raise awareness among organizations and individuals about steps they can take to protect themselves.

As we recommend to our customers, we are also actively looking for indicators in the Microsoft environment and, to date, have not found evidence of a successful attack.

Even with all the resources we dedicate to cybersecurity, our contribution will be only a small piece of what's needed to address the challenge. It requires policymakers, the business community, government agencies and, ultimately, individuals to make a real difference, and we can only have significant impact through shared information and partnerships. We hope this contribution will help us all work together better to improve the security of the digital ecosystem.