The Threat and Expansion

Midnight Blizzard Strikes

Caleb Leggett

The Initial Attack

As we look at the initial breach disclosed in January of this year, Microsoft announced that many of the exchange servers housing the executive level emails was breached resulting in the loss of a large amount of senior leader's email correspondence. While the company emphasized that no customer data was at risk at this time, it was down-played as just a normal BEC. While this is still alarming and the exact data that they were able to obtain was not made very clear. As many in the world of technology and cybersecurity know, it can be extremely important to use the intelligence to stay on top of the issues that are ongoing. The

initial attack also helps to highlight that no matter the size of the company, everyone is at risk.

The Threat Actors

As we dig deeper into the attack, the perpetrators have been identified as APT 29, also know as Midnight Blizzard. At this point, understanding the threat that these nation state actors pose cannot be stressed enough. With near limitless resources, protection from the nation they work for and the unending persistence of these groups can become truly scary. The other reason it is important to monitor what these groups are doing is because as they discover these vulnerabilities, they will trickle down to the smaller criminal organizations. The other notable point to the APT groups are not always motivated by monetary gain. This is important to remember as it results in a persistence that is near impossible to combat against.

The New Disclosure

As with many releases, the true extent is not always known. As investigations began into the breach at Microsoft, the discovery that the source code for an unknown number of Microsoft applications was extracted. This poses a real danger to any company using the Microsoft suite of products as well as the threat for Zero-Day vulnerabilities being discovered. As Microsoft falls into the supply chain realm, the attack surface becomes exponentially larger as it moves from a single company to a wide range in a short timeframe. If we take a look back, the last time the Microsoft source code was acquired, it resulted in the Eternal Blue exploit. Once the exploit was disclosed in the wild, attackers where able to chain this with other vectors which resulted in the NotPetya attack. As many in the field know, this attack is the largest cyber attack to date with a global impact and hundreds of billions in monetary loss.

What's Next

While the extent of the damage is still not known and there has not been any new Zero-Days found yet, the importance of CIA, backups and patching will be the first line of defense. Unfortunately, the only thing we can do past that is to wait and see how this unfolds. As long as the IT and security administrators are doing the due diligence to keep a cold back up of

systems and updates as soon as they are available, this will only help to ensure the safety of the environment.

Additional Reading:

https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

https://www.quorumcyber.com/threat-actors/midnight-blizzard-threat-actor-profile/

https://www.wired.com/story/russia-hackers-microsoft-source-code/

https://www.securityweek.com/microsoft-says-russian-gov-hackers-stole-source-code-after-spying-on-executive-emails/amp/

https://www.bleepingcomputer.com/news/security/microsoft-reveals-how-hackers-breached-its-exchange-online-accounts/amp/