THE EVOLUTION OF THE MICROSOFT BREACH

Date: 4/14/2024
By: Caleb Leggett

THE INITIAL COMPROMISE

In January of 2024, the APT group known as Midnight Blizzard, APT 29 or Cozy Bear started with the Business Email Compromise (BEC) of some of the high-level executives. As the investigation began, Microsoft ensured customers that there was no impact to their systems and that the incident was isolated to the internal Exchange servers. While there are many articles regarding this, you can find more information on the initial indicator of compromise (IOC) and the disclosure by Microsoft here.

THE PLOT THICKENS

As investigators dig into the incident, the scope will drastically change. After determining that the group was then able to access and exfiltrate the Source code, Microsoft again states that the impact is isolated to the internal network and should have no effect on customers tenants. While this can give some relief in looking at this, it still raises the question of how do we know that this is the end of the impact? The threat of new Zero-Day exploits being discovered at this point has now increased. The threat to its customers has been raised and the importance of the security field to do in depth audits and monitor is raised. The timeline at this point has also changed when the correlation between the access to legacy, non-production systems is now tied to the event. The disclosure to the SEC in March just shows the will to communicate.

A WARNING FROM CISA

As more information is learned about the incident, the need for increasing the vigilance becomes apparent. While the federal agency CISA is mainly concerned with systems and infrastructure controlled by the federal government, is this just an indicator that all companies should increase there monitoring into their ecosystems? Has the hunt for compromise just been initiated? As we learn more it will be extremely important to monitor the situation. The next steps of course are going to be to monitoring the OSINT and monitoring the systems that we can.

THE FIRST SIGNS

The first signs of the source code leak fallout is the most recent Patch Tuesday. With 2 Zero-Days and a total of 150 security flaws to include 67 RCEs, the importance of patching systems is just that much more important.

SUMMARY

Knowing that the group that perpetrated the attack is the same group responsible for the SolarWinds attack in 2020 just shows how detrimental the supply chain attacks can be. The time to relax might never be here and staying current with intelligence released is only the first steps. Taking that intelligence and determining the risk associated with it and formulating actionable plans will never stop being the mitigating factor in preventing a minor issue from becoming a major security breach.