**IAM – Cybersecurity Current Event Report**

**-Tim Schultejans – 9/6/2022**

**Microsoft – Lapsis$ - March 2022**

In March of 2022, Microsoft was attacked and breached by an economically focused hacker group known as Lapsus$. The attack compromised only 1 employee’s account, meaning that the hackers gained only limited access to Microsoft’s systems. That access, though, allowed the hackers to steal source code from Bing, Bing Maps, and Cortana. Luckily, no customer code or data was compromised in this breach. The breach was discovered after a torrent file containing partial source code was posted by Lapsus$.

Microsoft has not released many details of the attack, but they have released details of the hacker groups’ techniques. One technique used and what appears to be the most likely means that the hackers used was to ask for employees to compromise their employers. While this can be considered a phishing attack, it is not a normal attack because the employee is knowingly giving the group access to the company’s system. Once the Lapsus$ group gains access to a company’s system, they then access a company’s internet-facing devices and systems such as virtual private networks (VPN’s), remote desktop infrastructure, and identity management services. Once the hackers have access to the network, they then target users with broader access or collaboration platforms such as Slack and Microsoft Teams.

As mentioned earlier, the hackers gained access to only one Microsoft employee’s account before it was detected and remediated. Microsoft’s security team known as Microsoft Threat Intelligence Center, or MSTIC, was the reason for this. MSTIC studies hacking organizations and their attacks to provide defense against all attacks. Lapsus$ had been on MSTIC’s radar for a while, and so the intelligence team was ready for the attack if and when it where to happen. Lapsis$ was initially found to be carrying out attacks in South America and the UK but has since expanded to include global targets including governments.

**Ultimate Kronos Group - December 2021**

In December of 2021, the Human Resource Management and Payroll Company, Ultimate Kronos Group, was hacked. Through a ransomware attack, many of the company’s high-profile customers information may have been accessed, including FedEx, PepsiCo, Whole Foods, and the University of Utah. In ransomware attacks, computer systems become infected with malicious software that locks or encrypts access to files or data until a ransom is paid. There are reports that the ransom involved in this attack was paid, but it still took almost a month before UKG and all of its services were back online. The attack was detected when the Kronos Private Cloud service was interrupted. The outage meant that many of the company’s clients would have to find alternative means to run their payroll, and since the attack occurred at the end of the year, the attack could also cause a delay in issuing W-2’s and other tax information.

UKG has not released any details about the attack, but they hired a cybersecurity firm, Mandiant, to investigate exactly how the attack occurred. Ransomware attacks can spread through a variety of means, including phishing attacks or visiting infected websites. UKG is a company that provides services to many other companies, this means that there was a large amount of what is known as “third-party” effects, or companies that felt the pain of the breach, even though their company was not directly attacked.

Since we don’t know the details of the attack, it is difficult to discuss any steps that UKG could have taken to prevent an attack like this. There are some steps, though, that third-party customers, like the customers of UKG, can take to decrease their risk as much as possible. These steps are as follows: 1.) Identify all vendors so that a risk analysis can be completed, 2.) Analyze the risk for each vendor, 3.) Prioritize vendors to determine the extent of the risk they pose to your organization, and 4.) Continuously monitor the risks to ensure that your security is as up to date as possible.