Case Study Report

Prepared by: Isabelle Jaber

Date: July 15th, 2024

Table of Contents

INCIDENT OVERVIEW

A Severity Level 2 incident was detected on December 11th, time unknown. This incident was designated a Severity Level 2, due to the theft of SPII(Sensitive Personally Identifiable Information), service disruptions, and the financial and reputational impact of the breach (according to an Incident Severity Matrix on Splunk.com). The attack used Phishing (and Spear Phishing), Ransomware, and an Accidental Insider Threat to penetrate and harm MOVR's systems. The issues related to the breach were dealt with within eight hours, while the subsequent investigation and resolution concluded on December 17th. Although the incident was detected on December 11th, the attackers gained access to MOVR's system on October 10th, as such the incident in question lasted roughly two months, from October 10th to its resolution on December 17th.

EXECUTIVE SUMMARY

Incident Summary

This incident resulted from a previous breach that had occurred within the prior 8 months. During that initial breach, employee credentials were accessed and subsequently put up for sale on the dark web. The attackers who conducted this attack bought these credentials and used phishing techniques and Donovan's credentials to gain access to MOVR's system on October 10th. This gave them access to sensitive customer SPII data, 20% of which was stolen as a result of the attacker's unauthorized access. Additionally, Donovan had access to the master logins for accessing databases and other crucial parts of MOVR's tech infrastructure. The attackers maintained their access to, and monitored, and searched MOVR's systems for two months prior to detection. The attackers took two steps which brought attention to the breach.

The incident was detected on December 11th, first when the attackers used the master login credentials to alter and delete records in MOVR's Database Management Systems (DBMS). This resulted in service disruptions for customers who were trying to use the app. These issues were reported and flagged through customer support and, eventually, IT. It took eight hours for various teams to identify and resolve the problems caused by the breach to MOVR's DBMS.

The second action the attackers took on December 11th was sending a phishing campaign, seemingly from Donovan's account, to his team. The email sent from his account advised them to install a new internal software tool, which was actually ransomware. Once this was downloaded by his team, the ransomware locked them out of their computers and demanded $1,000 in bitcoin per device to restore access.

Impact

The impact of this attack was the partial loss of records, transactions, trip history, and accounts for some users for the day of December 11th. This created a more long-term issue around deciding how to compensate affected individuals who were unable to track completing their trips, and unable to take on new trips due to the outage. While the IT team attempted to regain access to the ransomed devices, MOVR eventually decided to pay the ransom in order to restore access. As the ransomware affected 150 devices, this resulted in a $150,000 financial loss to MOVR. As with most, if not all, breaches this also resulted in damage to MOVR's reputation.

Resolution

As soon as the attack was detected MOVR posted on social media to announce that they were aware of the disruptions and trying to resolve the issue. Once services to the customers were restored, they sent out a communication to their customers to notify them of the restoration. In the week following the incident, MOVR decided on what compensation they could offer their customers and contractors. MOVR then sent a message which outlined basic resolution steps for all compensation issues. In this communication MOVR offered customers a credit that expired in 30 days, and a flat rate reimbursement for their lost wages during the service disruptions. They also disclosed the possibility of a data breach, but provided no more information as it had yet to be confirmed.

Future Mitigation Techniques

As a result of this attack, MOVR hired a security consulting firm to help identify the source(s) of the breach, and also conducted their own internal investigation. As the source of the breach was found to be Donovan, he received special IT support and training. MOVR also decided to make their annual security training bi-annual, and hired a security company to monitor the dark web, in case the stolen records were to appear for sale there.

INCIDENT TIMELINE

Detection Phase

Since the attackers affected MOVR's digital resources by two separate mechanisms, they were each detected separately. Since the compromised DBMS resulted in service disruptions, MOVR's IT team was notified of this aspect of the breach by the customer support team as this attack primarily affected the MOVR's users. The ransomware attack, on the other hand, only affected certain members of the Operations Team who had downloaded the affected file that the attackers sent from Donovan's account. Since this part of the attack was internal, those whose machines were compromised by the ransomware reported it to the IT team directly.

While the detection of a security incident is crucial, in this case, it came too late. The attackers were aided by data that had already been stolen from MOVR's systems months before they took the actions that flagged the incident. There is clearly a hole in MOVR's security detection system, if an entirely different hacker (or group of hackers) was able to infiltrate their system and exfiltrate employee credentials without the security monitoring system detecting it. Detecting and tracking potentially suspicious activity should be an integral part of MOVR's security systems.

The delay in detection was also due to the lack of security training offered by MOVR to their employees. Since Donovan had not yet received any security training he was not aware of the importance of logging out of his accounts to ensure a multi-factor authentication(MFA) sign-in process and identifying phishing campaigns. This meant that he very rarely used MFA to log into his accounts. His account allowed Single Sign-On(SSO) to other applications connected to his account. This allowed the attackers to launch a successful phishing campaign to get Donovan to authorize the credentials and log to attackers into his account without encountering MFA prompts, and then have access to all of the other applications Donovan had access to using that account.

Additionally, MOVR's policies regarding the use of Discretionary Access Controls(DAC) was also a contributing factor in the delay of the incident's detection. While MOVR primarily used Role-Based Access Controls(RBAC) to assign access permissions, DAC was used on a case-by-case basis. This allowed the Software Team to share their entire Microsoft OneDrive with Donovan as he was a key stakeholder for one of their projects; this OneDrive is where the password manager (CSV file) with all of the master login credentials was stored. DAC should only be used within small teams or if there is a high level of trust, both of which were not the case here. However, not using DAC leaves RBAC difficult to rely on when dealing with exceptions (e.g. the Software Team's project) to RBAC permissions.

Perhaps, if MOVR's security training and DAC policies were more robust and allowed for more accountability, Donovan should have only had access to the folder in the Software Teams OneDrive that had the content for the relevant project, instead of the entire OneDrive. This wouldn't have allowed him access to the password manager and would have mitigated the

risk of the first attack occurring. Even then, Donovan's access should have been removed after his involvement with the project was over.

Containment Phase

Once the service disruptions caused by the breach were detected, the IT Team attempted to restore the database altered by the attacker, but encountered some technical problems that delayed the process. This resulted in the partial loss of records, transactions, trip history, and accounts for some users for the day of December 11th.

It was the issues with restoring the database that added to the financial impact of this breach. As a result of the service disruption and loss of records, some MOVR contractors were not able to complete their trips or receive payments for their services. This left MOVR with a long-term issue around deciding how to compensate affected individuals who were unable to track, complete, and receive payment for their trips, and those unable to take on new trips due to the outage. Since it is common for large companies to struggle to recover their databases, it is important that MOVR have contingency plans, and increased monitoring and testing of their recovery system and process.

Once they received reports of the ransomware attack, they should have sent out a communication to the rest of the employees to prohibit them from downloading any unknown software before checking with the IT Team. This may have made others aware of the problem and reduced the number of affected devices and therefore the total ransom paid.

Eradication Phase

An internal investigation was launched and the password manager was determined to be the source of access which allowed the breach of the database to occur. Once this was established, each user who had access to the password manager was interviewed and their devices were analyzed. This led the security team to trace the source of the breach back to Donovan. As a result, his email password was changed and all sessions for both his account and the master account were removed, which in turn removed the attacker's access to Donovan's account (and its SSO associated applications and resources).

Recovery Phase

With regard to the ransomware attack, MOVR's IT Team attempted to regain access to the 150 affected devices, without paying the ransom, but was unsuccessful. MOVR then decided to pay the ransom of $1,000 per affected device to restore access. An important part of this stage would be to conduct a forensic analysis of the devices affected by the ransomware and identify and remove the malicious software. MOVR then made reparations to their customers and

contractors by deciding to offer customers a credit that expired in 30 days, and contractors would be reimbursed a flat rate for lost wages.

ROOT CAUSE ANALYSIS

The initial attack vector for this incident was the employee credentials the attackers bought on the dark web. This gave the attackers employee data from which they were able to pick Donovan as their target and gain access to his account. It was from access to Donovan's account that they found the password manager and were able to cause service disruptions with their access to MOVR's tech infrastructure. The flaws in MOVR's systems, procedures, and policies that allowed this incident to occur are as follows.

The first issue is that MOVR's systems didn't detect the first breach which allowed unknown attackers to gain access to employee records, and exfiltrate the data to sell on the dark web. If this initial breach had been detected, MOVR may have been able to prevent the exfiltration of the data, or, at the very least, hire a security company to monitor the dark web for the stolen data and prevent it from being sold. This may be resolved by the better use or configuration of SIEM tools and firewalls.

The second issue is MOVR's use of DAC. This is what gave Donovan access to the password manager the attackers used to cause the service disruptions. If there were policies and procedures in place to help monitor and track the use of DAC, Donovan may not have ever had access to that file. It is understandable that, given the restrictions of using RBAC, MOVR would use DAC, but it is important to recognize the security concerns that come with using this type of access control. If they are to continue using this access control, it would be in MOVR's best interest to create a tool, workflow, or pipeline to track and manage the use of DAC. This would increase accountability and decrease the number of instances where people had access to items that they shouldn't (where the Principle of Least Privilege was not in place). This would have further reduced the likelihood of the central database being compromised.

The third issue is in regards to MOVR's onboarding and training processes. Even with MOVR agreeing to hold security training seminars twice per year, instead of once, this means that new employees may be waiting up to six months before receiving crucial security training. A complete overhaul of their security training procedures would greatly reduce the exploitation of human error/vulnerabilities (more details in Section 7).

This would help decrease the human vulnerabilities which allowed this incident to occur. In this case, Donovan was the source of the breach as he was susceptible to the social engineering that gave the attackers access to his account. Additionally, members of Donovan's team were not able to recognize the phishing campaign and downloaded the ransomware that wound up costing MOVR $150,000.

LESSONS LEARNED

The primary takeaways from this breach are the importance of preemptive training and monitoring software. Moving forward MOVR decided to provide training and special IT support for Donovan and not proceed with any disciplinary action for any employee. MOVR also decided to make their annual security training bi-annual as well as hire a security company to monitor the dark web in the event that the stolen data appeared for sale there.

RESPONSE AND RECOVERY ASSESSMENT

MOVR responded to the incident fairly well. They were able to resolve the issues directly caused by the attack within 24 hours of the incident detection and one week for MOVR to decide how to handle the lack of payment and inconvenience caused by the service outage. As such, MOVR handled all four stages of the incident response process with accuracy and efficiency.

In addition, MOVR's incident communication practices aided in handling the breach from a public relations perspective. Given that they were notified of the breach to their database by their customers, it benefited the company to communicate with them about it and reassure their customers that they were working to resolve the issues. Their prompt follow-up messages also benefited their public image in response to the breach as it demonstrated strong dedication to the issue and to their customers. While their degree of openness on their social media is to be commended, and it is understandable why they did not share all of the finer details about the breach, given the fact that SPII data was stolen, they should have communicated that information directly to the relevant customers and stakeholders.

It seems as though MOVR allocated its resources well during the incident. The relevant teams were able to handle the different aspects of the attack. The Public Relations/Marketing team handled the communication with the customers and contractors in a timely manner, and services and devices were quickly restored. Even though there were some technical difficulties, it seemed like it was a common occurrence for large companies who try to restore their databases due to their complicated tech infrastructure.

NEXT STEPS

Short Term

To prevent a future attack, MOVR should provide emergency security training for all employees and prompt everyone to change their password (in case their credentials were stolen in the first breach), as well as consulting with a security firm and starting to research new tools to enhance their security posture.

As previously discussed, a more robust security training program and better configured SIEM tools and firewalls are crucial in preventing this type of attack from occurring again. The role that the undetected breach played in this incident cannot be understated. Properly configuring and installing a variety of security tools, could have notified the company of the initial breach that sold the employee data and prevented this particular attack from occurring.

Long Term

MOVR should completely overhaul the way they approach security training. If MOVR employs eLearning platforms to train new employees in security protocols and best-practices as part of their company onboarding process, it would better prepare and protect new employees as well as save them time and money that would be used on the bi-annual training seminars. This would also allow employees to refer back to the information at any point. It would also be beneficial if MOVR made it mandatory for all employees to retake the eLearning course every year to ensure proper and consistent understanding of the material as it is updated over the course of time. Per the previously discussed issues with DAC and RBAC, a new process for tracking and managing the use of DAC should be piloted and implemented across the company. This material can then be included in the eLearning course/materials for employee security training.

Additionally, since restoring database backups is known to be difficult and complex for large companies such as MOVR, it would be in the company's best interest if they investigated their systems. The information gleaned from this investigation could help MOVR create a new restoration procedure or backup procedure, which could prevent the loss of data if they had to restore their system again.

Finally, the re-evaluation of the storage of password managers and the use of SSOs should take place. SSOs, while convenient to the user, can pose a significant security risk depending on what is available through it. Extra caution should be taken when it comes to password managers. It seems that, in this case, all of the credentials were stored in a regular CSV file in the Software Team's OneDrive, with no added security.

REFLECTION

Part A

DATA	CATEGORY	CLASSIFICATION
First and Last Name	Customer	Public
Location & Location History	Customer	Public
Type of Service History, Delivery Data	Customer	Public
Phone number	Customer	Private
Driver's License and License Plate Number	Customer	Private
IP Address and Device Data	Customer	Private
Salary, Pay Stubs, Banking Information	Customer	Restricted-Specific
First and Last Name	Employee	Public
Address	Employee	Private
Phone Number	Employee	Private

Social Security Number and DOB	Employee	Restricted
Benefits	Employee	Restricted
Salary, Pay Stubs, Banking Information	Employee	Restricted-Specific

Part B

Human vulnerabilities were the primary weakness in this company's security. Both Donovan and his team were very negligent in their use of security tools and protocols. Donovan's practice of not logging out of his account and evading the MFA verification system, and both Donovan's and his team's inability to identify a potential phishing attack were key to the attacker's success. While MOVR should have provided more extensive security training to all employees, the people part of this information system were the weakest link. Without this, it would have been much harder for the attackers to affect the system as they did, especially since it is known that the threat actors do not use very technologically advanced methods.

While human error was the primary weakness in this attack, it would have been much more difficult if there were better technologies and processes in place. The role of the previously undetected breach in this attack cannot be overlooked. Without this breach and the subsequent sale of employee data, it would have been much harder for the attackers to find their target and get the login credentials necessary to gain access to their account. The lack of both proper security tools and technologies allowed this initial breach to go unnoticed and left the company and its employees at risk. More robust security training processes would have also decreased the chances of the exploitation of human vulnerabilities.

Part C

The primary ethical shortcoming was in the company's disclosure of the breach. There is also no mention of them reporting the incident to a regulatory agency, so this may be unethical. Although they did release the notice to the public, it seems a bit ambiguous as to whether or not they should reach out or if the relevant regulatory agency should contact them. This is particularly crucial given that some of the data that was stolen affected users in Europe where they have stricter laws on data security (the jurisdiction might be a bit complicated depending on where the company is based/registered, where its servers are located, and whether the location of

the customer is relevant). Finally, their decision not to disclose any information regarding the ransomware attack may also be considered an ethical gray area.

Part D

Whiletheir prompt and continued communication with the public is commendable, once there was concrete evidence that customer data had been stolen, they should take a more direct approach when informing customers and stakeholders of the stolen SPII. They should reach out via email to those whose data was stolen and relevant stakeholders of what happened and what they planned to do to resolve the risk to those whose information was stolen, as well as provide additional resources and customer support for those who were concerned about how the breach would affect them. This communication procedure should be documented in their Incident Response Plan for reference in the case of any future incidents.

Part E

To determine the cost of not paying the ransom, more information would need to be gathered on the cost of each machine and the associated content. If all of the information accessed through the computers was stored on the cloud and each machine cost less than $1,000, not paying the ransom would have saved them more money. However, there are other considerations at play here that could affect the current priorities. Even if these conditions are accurate and all data was stored on the cloud and each machine cost less than $1,000, if they would lose even more money waiting for new machines to be ordered, shipped, arrive, and properly configured, then it may be worth it to pay the ransom so the employees could get back to business as usual as quickly as possible.

Part F

The most obvious risk is related to their access controls. Particularly for larger companies, reconciling the drawbacks of using RBACs with the dangers of using DACs to minimize the problems with only using RBAC is very difficult. RBAC must seem like a dream to implement for larger companies however, it does not allow for edge-cases and other anomalous occasions where an exception must be made to the RBAC. This flaw with RBAC can be detrimental to a company's operations and growth. DAC is commonly used by large companies to solve this problem, but with this solution comes a lack of accountability and security which, as we have seen in this case study, can be a very dangerous risk to take.

Additionally, using a password manager that was stored in a CSV file was not the most secure way of storing the credentials necessary to access the different aspects of MOVR's tech infrastructure. Access to this CSV file should not have been possible through the applications available by Donovan's SSO.

Part G

MOVR and all companies should take their security risks extremely seriously. They have a duty of care, an ethical responsibility, to the customers who use their product and the employees who rely on them for employment, and trust them with their private information. By their attitude towards their security training, it seems as though, even after the breach, they are not taking serious care to enhance their security posture.

SOURCES

https://www.cmu.edu/data/guidelines/data-classification.html
https://www.splunk.com/en_us/blog/learn/incident-severity-levels.html