BrainStation®

Cybersecurity Bootcamp Unit 1 Project

Table of Contents

Case Study

Disclaimer

All entities and events in this case study are purely hypothetical. Details of the case study are inspired by real-world events.

Company Profile

MOVR (Mover) is a large international logistics technology company operating in over 70 countries. They specialize in developing digital solutions to transport people and goods within smaller local markets. With nearly 20,000 employees, they are a robust and relatively mature organization with full teams and departments in operations, engineering, HR, customer service, security, finance, marketing, legal, and more.

The company does have a number of policies including:

- Personal Device Use Policy
- Ethical Conduct
- Respect in the Workplace
- Information Security
    - Clean Desks
    - Password Requirement
    - Connecting to Networks
    - Copying and Distributing Company Data
    - Mobile Device Usage
    - Software Requirements

Tech Infrastructure

MOVR hosts most of its infrastructure in the cloud, where servers calculate routes for users and manage data that is sent back to the apps on client devices (mostly phones).

The most sensitive data is held on company-managed servers, rather than with a cloud provider like Amazon. Employees are required to use MFA when signing in to their accounts. Customers / users are also required to use MFA when signing in to their accounts in the app (phone number verification).

Data Collection

MOVR collects and stores the following pieces of user data:

- Name (First and Last)
- Profile photo (Optional)
- Phone Number
- Location
- Location history
- Payment information
- Transaction amounts
- Merchant information (if applicable)
- Driver’s licenses
- License plates
- History of the types of services requested (e.g. Package Delivery, Food Delivery, Personal Transportation)
- Delivery data
- IP addresses
- Device Data:
  - Operating system, device location data, network and service provider
- Other ‘synthetic’ data points that are derived from user inputs and actions within the app. (e.g. Satisfaction score, actual delivery time, time estimate vs. actual delivery time, etc.)

Data Sharing

MOVR doesn’t sell user data, but does share it with advertising partners and advertisers on its platform. Advertising partners include the typical large social media platforms. Advertisers refers to businesses that are on their platform and intend to promote themselves within the app (e.g. to advertise a food delivery promotion).

MOVR also shares data with and receives data from rewards point partners and financial institutions. For example, if users link a certain credit card, they are eligible for benefits. Or, users might be part of a rewards point program and can link their account to their rewards account.

Employee Data

Like any company, MOVR has the following data on their employees:

- Name
- Address
- Phone number
- Date of birth
- Social security number
- Salary / pay stubs
- Benefits
- Banking information

Employees use a number of internal tools:

- Microsoft 365 (Outlook, Word, Excel, etc.)
- Microsoft Teams
- Github
- Jira
- Hubspot

These tools simply have access to the email and basic account info of employees (e.g. Name, Location, etc.)

Employees are required to use MFA verification when signing in to their work accounts.

Threat Actor Profile

The threat actor / attacker is an individual affiliated with a global cybercrime group. While not much is known about this group, it is understood that they are a relatively small group that uses less technologically sophisticated methods. However, this doesn't mean that they aren't dangerous and capable.

The group relies heavily on phishing and its variants to help initiate a breach. Once they have access to a system, they seek to expand access and elevate privilege to compromise sensitive information. Additionally, the group deploys ransomware to help generate further revenue.

This cybercrime group has successfully targeted a variety of organizations; large tech companies, government departments, healthcare organizations, and more.

Timeline of Events

Prior to Breach

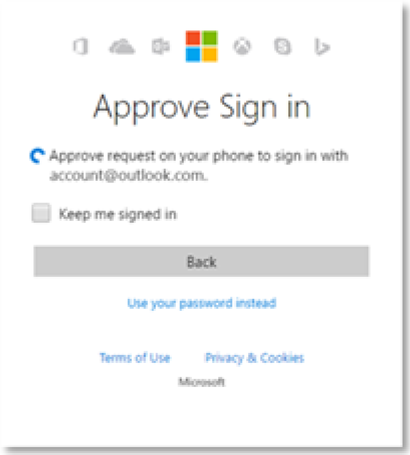
Donovan, a relatively new Senior Operations Manager was hired to work at MOVR's USA headquarters in New York. As an experienced operations professional, he's held a number of positions at different, more traditional, smaller businesses that weren't very technology focused. Although he has phenomenal core operations skills and competencies, he does lack a bit of digital literacy and was hoping this move towards a more technology-driven company will help him build up that missing skill.

Donovan has a hybrid working arrangement with the company and is required to work in the office 2 days a week. As such, he's connecting to company resources and networks both at home, and in the office. Occasionally, he may work out of a coffee shop or other public areas. Whether on public or private networks, Donovan accesses his work resources and tools as usual without any additional security measures. He simply logs into his accounts and if prompted, provides some form of multi-factor authentication (MFA). However, since he is already logged in to most items and seldom logs out, he doesn't see MFA prompts very often.

Donovan has been with the company for about 8 months. During this time, the company experienced a small data breach which led to his and other employee account credentials being compromised. This breach is not yet known to MOVR. Despite being with the company for 8 months, he has not received any basic cybersecurity training. MOVR operates a cybersecurity training seminar once a year, where it is mandatory for employees to attend if they have never attended before. It is encouraged for all employees to attend, but is not mandatory for employees who have attended in the past. Due to the fact that he was not with the company during the time of their annual training, Donovan has yet to receive his mandatory cybersecurity training..

The attacker purchased the set of credentials off the darkweb and used Donovan's credentials to attempt to gain access to the system. Donovan was selected as the target for the attack since he has some level of seniority, and because he is relatively new to the company. The attacker also researched his LinkedIn and social media profiles and determined he would likely be more susceptible to the attack when compared to more technical or younger colleagues. On October 10th, the attacker tried to gain access using Donovan's account. Donovan saw a sign-in prompt on his screen to allow or deny login access, but the prompt didn't specify where the login was from or provide any further information.

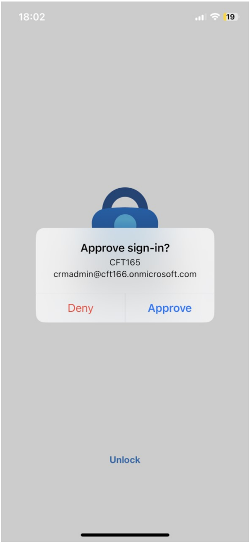
Source: Microsoft



Approve Sign in

Approve request on your phone to sign in with account@outlook.com.

□ Keep me signed in



Approve sign-in?
CFT165
crmadmin@cft166.onmicrosoft.com

Earlier that day, prior to the sign in attempt, the threat actor sent a clear message attempting to impersonate a general MOVR IT Support email account. The message informed users that they may be receiving sign-in prompts intermittently throughout the day due to the addition of new IT services and software.

Users were instructed to accept the prompts to allow the setup of "new IT services" to happen successfully. The message highlighted a sense of urgency and explained that these are critical updates to the IT services used across the company. The message also stated that non-compliance or delayed action on the users part would result in further issues for IT and the user going forward. These tactics were meant to prevent or reduce critical thinking around the message's origin and intent.

Donovan didn't question the supposed directive and approved the prompt, giving the threat actor access to his account. From his frame of mind, he'd rather not create IT problems that might be difficult to solve. Asking for help with IT problems can be difficult and time consuming, and sometimes leaves individuals with a sense of embarrassment for not being able to complete seemingly simple tasks.

Breach

At this point, Donovan has unknowingly given access to the threat actor. Since Donovan was working at home on the day of the initial breach (October 10th) he wasn't inclined to ask colleagues about the event, and by the time he returned to the office on the following Monday, October 13th, he had since forgotten about this event from the prior week.

As a senior member of the Ops team, Donovan has access to restricted information and PII (Personally Identifiable Information) about customers which includes much of the data points mentioned in the 'Data Collection' subheading in the 'Company Profile' section. He also has access and edit permissions to most of the OneDrive spaces for the Operations team.

MOVR operates primarily using RBAC (Role-Based Access Control), with some DAC (Discretionary Access Control) depending on the resources needed on a project-by-project basis. Donovan was given access to a Software Development Microsoft OneDrive space as part of a new internal tool project that was completed 2 months ago. He was in charge of providing direction and input as one of the key Operations stakeholders that would use the new internal tool.

With the project now completed, the software development team has since forgotten about Donovan's access to that Drive space. Since it's a space used by developers on the project, they all need access to credentials for code and tech management tools like Github and AWS. A password manager export in .CSV format was stored in the drive for shared access, which contained the master logins for accessing the database and other pieces of tech infrastructure. By default the .CSV file is not encrypted.

These credentials provide broader access to sensitive user data in an aggregated and raw format. While logging into this account will trigger a warning about the location and IP being different than usual, this is localized to the account itself and is quickly resolved by the threat actor since they have access. The master login was accessed by the threat actor on Monday, October 13th.

With master access, the attacker then copied large sections of the data, totalling roughly 20 million user records or about 20% of the total user base. The majority of affected users were located in North America (United States, Canada), and some countries in Europe (United Kingdom, France, etc.). This traffic was largely innocuous due to the hourly frequency of data backups that run on the network, and the methods used by the attacker to exfiltrate data in smaller batches. It essentially represents a small increase in network traffic, below any reasonable detection threshold. Data records taken included:

- First and Last Name
- Location
- Location History
- Credit Card Information
- Email
- Passwords
- Transaction Amounts
- Transaction History

The attacker maintained their access to the system for two months since exfiltrating the data, monitoring activity and looking for further information that might be of value.

Before this time elapsed, the attacker took two key steps which caused a number of issues on December 11th:

1. Deletion of live, production database records.
2. A mass phishing campaign to members of the operations team.

Action 1: The change or deletion of database records is an action that is automatically logged in the DataBase Management System (DBMS), and immediately caused service disruptions for MOVR customers trying to use the app. These disruptions were flagged to customer support and eventually IT. Disruptions lasted 8 hours while various teams were coordinating to identify and resolve the issues.

Action 2: The phishing campaign was sent from Donovan's accounts to members of the operations team, advising them to install a new internal tool which is disguised ransomware. This was performed over Teams (tied to Donovan's account using SSO), and via email. The ransomware locked out users from their computer, demanding payment in exchange for access to the device and the data associated with it.

Discovery of Breach and Remediation

Ultimately, the breach was discovered shortly after on December 11th, when the IT and security teams began looking into service disruptions and received reports of the ransomware.

In theory, restoring the database from backups should have been a straightforward process. However, the restoration process was delayed due to technical issues. Databases and technologies are complicated, and even large, professional organizations can have issues as evidenced in this Gitlab Case Study. Ultimately, the impact for MOVR was a partial loss of records, transactions, trip history, and accounts for some users for the day of December 11th. Some MOVR contractors and couriers were not provided with completed trips and payments for their services. 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. Customers using the platform lost track of their trips and experienced more minor disruptions.

Through reviewing logs and account activities, it was determined that the master account was used in deleting database records. From there, an internal investigation was launched and it was found that the password manager export was a potential source of access. Each user who had access to the export was then interviewed and their tech resources were investigated. This helped the security teams trace the source of the breach back to Donovan. His email password was changed and all sessions for both his account and the master account were removed. While issues were addressed immediately, the investigation process and subsequent resolution took some time and was completed on December 17th.

For the ransomware, over 150 company laptops were rendered unusable and the total ransom demanded was $1000 per device, to be paid in bitcoin. While IT staff attempted to resolve the issue, logistics challenges around getting all remote employee devices back to the office hindered immediate resolution.

Disclosure

When service disruptions occurred, MOVR took to social media immediately to announce they are aware of the disruptions and are attempting to resolve the issue. No further details were provided to customers or stakeholders. Once services were restored by the end of the day, a follow-up message was posted to inform customers.

One week after the issues were resolved (December 18), the MOVR provided a statement to customers and contractors, expressing their commitment to service and reliability. This message outlined basic resolution steps for all compensation issues. Customers would be provided with a credit that expires in 30 days, and contractors would be reimbursed a flat rate for lost wages. This statement did not mention the cause of the service disruption or what steps were taken to resolve the issues.

One month after the date of service disruption (January 11), the company announced to the public that the issue was a result of a breach and that all issues related to the breach had been addressed. The company reaffirmed their commitment to security. The company disclosed that some customer records may have been exposed, but there was no concrete evidence to confirm this assumption at this time. Should darkweb monitoring companies become aware of this data surfacing, then MOVR would also be made aware of the extent of the data breach. They did not disclose who they believe the threat actor to be or what the impact may be to customers.

With regards to the ransomware, the company decided to pay the ransom, as they determined it to be the most cost-effective method to resolve the situation. In this scenario, they did recover access to devices once the ransom was paid. This situation was not disclosed to the public, as they believed it to be an internal matter.

Looking Forward

With the breach now behind them, MOVR had a few more areas to address. As part of the resolution process before the disclosure of the breach, MOVR performed an internal investigation and hired a security consulting firm to help uncover the chain of events that lead to the incident.

Donovan received training and special IT support, given that the initial phase of the breach was found to have originated from Donovan's account. This was determined through a review of access logs. Following this theme of training, the company's annual security training was updated to be bi-annually

No disciplinary action was given to any member of the company. Finally, MOVR contracted a security company to monitor for data records, should they ever appear on the darkweb.