Commonwealth Fusion Center (CFC) Massachusetts

(978) 451-3700 | (508) 820-2233

MCP Massachusetts Cybersecurity Program

(U//FOUO) CFC Massachusetts Cybersecurity Program (MCP) Bulletin: Insider Threat 5/24/2021

(U) Overview

(U) An insider threat is a threat to a company or organization that originates from a person (e.g., employee, contractor, or associate) within the organization. Insider threats are potentially more dangerous than threats from outsiders due to their knowledge of internal processes, procedures, and potential weaknesses of the organization. Insiders also know the location and nature of sensitive data that could be exploited. It is important for organizations to understand the potential risks as well as measures it can implement to mitigate and prevent insider threats. The Massachusetts Cybersecurity Program (MCP) has developed this bulletin for educational purposes and situational awareness.

Source: C5 Communications

(U) Intentional vs Accidental Threats

(U) Insider threats can be intentional or accidental. The difference between the two comes down to intent.

(U) **Intentional** insider threats involve an actor that intends to harm the organization with which they are affiliated, or has other motivations which ultimately will result in harm to the organization. The motive for conducting an insider an attack could include financial gain, revenge/sabotage, or espionage. The following indicators may be potential factors that could contribute to or be indicative of an intentional insider threat.

(U) Indicators and Red Flags

- Financial Problems or Distress
- Unexplained Financial Gain
- Unusual Working Hours
- Spontaneous Overseas Travel
- Accessing data outside of job responsibility
- Frequent Arguments with Coworkers
- Leaving Company Abruptly
- Open Disagreement with Polices
- Laziness or carefree about security
- Downloading or moving large amounts of data

(U) **Accidental** insider incidents are more common and occur when an employee is unaware that they took an action that caused the company harm. Accidental insiders may be an unwitting victim of a phishing attack (releasing credentials or giving database access), accidentally leak data or business information, install malware/ransomware by clicking on malicious links or attachments, or practice poor cybersecurity hygiene.

(U) INSIDER ATTACKS

(U) August 2020 – A foreign national, who is a member of a cybercrime gang, met with an employee of Tesla. The suspect took the employee out for drinks multiple times and provided them with a cell phone to communicate with each other. The suspect offered the employee $1 million dollars to install malware on Tesla's computer system to extract data. The plan was to use other members working with the suspect to launch a distributed denial of service attack (DDoS) to distract Tesla while simultaneously stealing data using the malware. Once complete, they would force Tesla to pay them millions of dollars to get the data back. After hearing the initial proposition, the Tesla employee told security officials who then contacted the FBI. The FBI arrested and charged the suspect with "conspiracy to intentionally cause damage to a protected computer."

(U) July 2020 – Cyber actors gathered information on Twitter employees that were working from home by conducting various spear phishing attacks. Posing as Twitter IT administrators, the hackers contacted the employees and asked for their user credentials. Using the compromised accounts, the hackers were able to gain access to administrator tools that enabled them to reset high-profile Twitter user accounts, including Barack Obama, Bill Gates, Elon Musk, Apple, and many more. The hackers continued their attack by tweeting scams from the newly reset accounts posing as their owner. Twitter users who believed the scammed tweets transferred an approximate total of $180,000 in Bitcoin to the hackers.

Scam tweeted from hacked Apple Twitter handle
Source: Twitter

(U) March 2019 – A former employee of the Ellsworth County Rural Water District in Kansas knowingly accessed a protected computer system without authorization. During this session, the employee shut down processes that can affect the cleaning and disinfecting procedures at the treatment facility. The former employee was indicted in March 2021 and could face a maximum of 20 years in prison. A customer service specialist said the intrusion did not cause any harm to customers' drinking water. It is unknown at this time if the former employee circumvented security procedures or still had remote access following his departure.

(U) September 2018 – A former Cisco employee gained unauthorized access to the company's cloud infrastructure. During this time, the suspect unleashed malicious code that deleted 456 virtual machines used to support Cisco's WebEx applications, which provide video conference and collaboration tools for its customers. Removing the virtual machines affected 16,000 WebEx accounts over the course of two weeks. Cisco spent approximately $1.4 million in employee time to fix the damage and also had to pay $1 million in restitution to impacted users.

(U) December 2015 – A Google executive who worked on the "Waymo self-driving program," downloaded approximately 14,000 files from a password-protected Google server. Within days, he had transferred those files to his personal laptop and within months had ended his employment with Google. He then used the stolen files to create his own self-driving truck startup, "Otto," which was quickly purchased by Uber. The former employee was later charged with, and pled guilty to, trade-secret theft and was sentenced to 18 months in prison.

(U) Potential Outcomes of an Insider Attack

- Financial loss
- Work disruptions
- Loss of repeat or new customers
- Lawsuits or regulatory fines
- Disclosure of trade secrets or business practices
- Falling share prices
- Tainted business reputation

Source: CISA

(U) Recommendations and Tips

- Remove or delete access to network and tools for any departing employee.
- Limit computer access and rights to employees based on job responsibilities and need to know.
- Look for warning signs of disgruntled or careless employees.
- Train employees on proper cyber hygiene:
    - Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
    - Verify email senders. If unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before contacting them.
    - Inform yourself. Keep yourself educated about recent cybersecurity threats and up to date on cyber-attack techniques.
    - Do not click links or download suspicious attachments from an email sender you do not recognize.
    - Do not believe everything you see online.

(U) Outlook

(U) The Commonwealth Fusion Center (CFC) Massachusetts Cybersecurity Program (MCP) is providing this information for situational awareness purposes only.

(U) Please report any suspicious activity to your police department of jurisdiction and the Commonwealth Fusion Center at 508-820-2233.

For additional information or to be added to the MCP distribution list, please contact the MCP by e-mail: MCPPOL@pol.state.ma.us.

This report addresses HSEC SINs: 1.1, 1.3, 1.8, 6
This report addresses CFC SINs: 1E, 1F

MSP2367/MSPC1989/MSPC1977

Sources:

(U) "Insider Threats Examples: 11 Real Examples of Insider Threats," Tessian, 8 December 2020
(U) "Ex-Yahoo employee avoids jail, despite hacking 6000 accounts, and stealing explicit photos and videos," Security Boulevard, 6 July 2020
(U) "Insider Threat – Cyber," CISA, accessed 7 April 2021
(U) "Combating the Insider Threat," US-CERT, 2 May 2014
(U) "5 Real-Life Examples of Breaches Caused by Insider Threats," Ekran System, 18 November 2020
(U) "Cost of Insider Threats: Global Report 2020." IBM Security, accessed 7 April 2021

(U) “Former Google exec Anthony Levandowski sentenced to 18 months for stealing self-driving car secrets,” The Verge, 4 August 2020
(U) “Google's Insider Threat Pleads Guilty,” Secure World Expo, 26 March 2020
(U) “Feds Charge 22-Year-Old for Hacking Kansas Water Supplier,” PC Mag, 1 April 2021
(U) “INDICTMENT: KANSAS MAN INDICTED FOR TAMPERING WITH A PUBLIC WATER SYSTEM,” Justice, 31 March 2021
(U) “Kansas man indicted in connection with 2019 hack at water utility,” Cyber Scoop, 1 April 2021
(U) “Once again, someone tampered with an entire drinking water supply via the internet,” The Verge, 5 April 2021
(U) “7 warning signs of an insider threat,” Adaptus LLC, 3 December 2018