Mishal Mazhar(4473-FOC-BSSE-F22-A)

Dated:30 DEC, 2024

Incident handler's journal

Journal:01 Mustang Panda Feeds Worm-Driven USB Attack Strategy

Date: Sep 10, 2024	**Entry:** #1
Description	A cyber-attack associated with Mustang Panda, a hacking group that used USB drives and phishing emails to obtained information.
Tool(s) used	USB drives, supplemental tool, FDMTP tool, PTSOCKET tool
The 5 W's	● **Who**: Mustang Panda, a Chinese state-sponsored threat actor. ● **What**: Cyber-espionage goals of system control and data exfiltration. ● **Where**: Targeting government entities such as military, police departments, foreign affairs offices, and public education systems. ● **When**: 10 sep,2024 ● **Why**: The purpose is cyber espionage, gaining control over government systems to steal sensitive data.
Additional notes	1. **How could the health care company prevent an incident like this from occurring again?** Install better security software , Restrict the use of USB drives, Teach employees to spot phishing emails and avoid plugging in unknown USB drives. 2. **Should the company pay the ransom to retrieve the decryption key?** Paying the ransom is not a good idea because there's no guarantee the hackers will return control. Instead, company should focus on incident recovery on back solution, working with cybersecurity experts to remove malware and restore data from backups.

Incident handler's journal:

Journal:02 **Ransomware attack forces high school in London to close and send students home**

Date: Sep 9th, 2024	**Entry:** #2
Description	A ransomware attack hit a high school in south London, locking important files and disrupting its IT systems.
Tool(s) used	Ransomware (method of entry not confirmed, possibly phishing or another security breach).
The 5 W's	● **Who**: A group of cybercriminals, possibly linked to other school ransomware attacks. ● **What**: A cyberattack that encrypted the school's files and forced a shutdown of IT systems. ● **Where**: Charles Darwin School, South London. ● **When**: The attack was discovered on Thursday, September 5, 2024.. ● **Why**: Likely for financial gain, as these types of attacks usually involve demanding a ransom payment to unlock the files.
Additional notes	3. How could the health care company prevent an incident like this from occurring again? • Train staff and students to spot phishing emails. • Use stronger passwords and two-factor authentication. • Back up important files regularly and store the backups offline. 4. Should the company pay the ransom to retrieve the decryption key? Paying the ransom is not a good idea because: • It encourages hackers to attack others. • There's no promise they'll unlock the files, even if paid.

Incident handler's journal:

Journal:03 Hospitals cyber attack impacts 800 operations

Date: 14 June 2024	**Entry:** #3
Description	A cyberattack hit Synnovis, a company providing lab services, causing major problems for hospitals in London. Over 800 surgeries and hundreds of appointments were delayed.
Tool(s) used	Ransomware (details on how it was carried out are still unknown).
The 5 W's	● **Who**: Hackers targeted Synnovis, affecting NHS hospitals in London. ● **What**: A ransomware attack disrupted lab services, delaying medical care. ● **Where**: Mainly at King's College Hospital and Guy's and St Thomas' NHS Trusts. ● **When**: The attack happened in mid-June 2024, with effects lasting weeks. ● **Why**: Likely for money, as ransomware attacks usually demand payment to unlock systems.
Additional notes	**1: How could hospitals stop this from happening again?** • Improve cybersecurity at companies they work with, like Synnovis. • Keep all software updated to fix weak spots. • Train staff to spot phishing emails and scams. • Back up important systems and data regularly. **2: Should Synnovis or hospitals pay the ransom?** • It encourages hackers to attack again. • There's no guarantee they will fix the system after payment.

Incident handler's journal:

Journal:04 Marriott & Starwood Face $52M Settlement After Security Breaches

Date: February 2020 (final breach discovered)	**Entry:** #4

Description	Marriott and Starwood Hotels had three major data breaches between 2014 and 2020. These breaches exposed sensitive customer information, leading to a $52 million settlement and stricter security rules..
Tool(s) used	Hackers gained unauthorized access to customer data and payment systems.
The 5 W's	● **Who**: Hackers targeted Starwood Hotels, and later Marriott after it acquired Starwood. ● **What** Sensitive customer information, like payment details, loyalty accounts, and passport numbers, was stolen. ● **Where**: Marriott and Starwood Hotels worldwide. ● **When**: The breaches happened from 2014 to 2020 and were discovered in 2015, 2018, and 2020. ● **Why**: Hackers likely wanted to steal financial and personal information for profit.
Additional notes	**1: How could Marriott stop this from happening again?** • Use stronger security systems and keep them updated. • Encrypt sensitive data like passport numbers. • Limit access to payment systems. • Train staff to handle cybersecurity better. **2: Why do companies pay settlements for breaches?** • It holds them responsible for poor security practices. • It pushes them to improve their systems and protects customers better. • But companies should focus on preventing breaches in the first place instead of fixing problems after they happen.

Incident handler's journal:

Journal:05 American Water Reconnects Its Network Taps After Cyber Incident

Date: October 7, 2024	**Entry:** #5

Description	American Water, the largest water utility company in the U.S., had to take its systems offline after a cyber incident. The company is now reconnecting its systems and ensuring they are secure while the investigation continues.
Tool(s) used	The method used by the attackers has not been shared.
The 5 W's	● **Who**: Hackers targeted American Water's systems. ● **What**: A cyber attack disrupted some of the company's services, but water and wastewater facilities were not affected. ● **Where**: American Water, which serves 14 states and 18 military sites in the U.S. ● **When** The incident was reported on October 7, 2024, with updates provided by October 10, 2024. ● **Why**: Hackers may have wanted to exploit weaknesses in the system for financial gain or disruption.
Additional notes	**1: How could American Water prevent this in the future?** • Strengthen cybersecurity measures to protect important systems. • Regularly check and update old and new systems to fix weaknesses. • Train staff to identify threats like phishing scams. • Have a clear plan to respond quickly to cyber incidents. **2: Why are attacks on critical infrastructure a big deal?** • Services like water and electricity are essential for daily life. • A successful attack could cause major disruptions or harm. • Companies need to take cybersecurity seriously to protect these systems.

Incident handler's journal:

Journal:06 Snowflake Account Attacks Driven by Exposed Legitimate Credentials

Date: Late May	**Entry:** #6

2024	
Description	Hackers used stolen login details to access accounts on Snowflake, a cloud data platform, affecting 165 companies. Weak password practices and the lack of multifactor authentication (MFA) allowed attackers to steal sensitive data.
Tool(s) used	Stolen credentials and infostealer malware.
The 5 W's	● **Who**: Hackers known as UNC5537. ● **What**: hey used stolen usernames and passwords to log into accounts and access sensitive data. ● **Where**: Snowflake, a platform used for storing and managing data. ● **When** The attack happened in May 2024 ● **Why**: To steal data and sell it for money.
Additional notes	**1: How the Breach Happened:** • Attackers used login credentials that were either exposed online or sold on the Dark Web. • Many accounts did not have MFA, making it easier to gain unauthorized access. **2: Impact of the Breach:** • Data from 165 companies was accessed. • Infostealer malware on compromised devices allowed attackers to extract sensitive information, including personal data, financial records, and business intelligence.

Incident handler's journal:

Journal:07 Ethereum Classic Hit by Third 51% Attack in a Month

Date: Aug 30, 2024	**Entry:** #7
Description	

Tool(s) used	Ethereum Classic Blockchain
The 5 W's	● **Who**: A group of hackers exploiting vulnerabilities in the Ethereum Classic network. ● **What**: A 51% attack on Ethereum Classic ● **Where**: Ethereum Classic blockchain ● **When**: Saturday evening, Aug. 29, 2024 ● **Why**: Hackers took control of more than half of the network's mining power, causing a disruption in the blockchain. This attack is the third of its kind in the month of August. The attackers likely wanted to steal funds or damage the network's reputation by manipulating transactions.
Additional notes	**1: How can Ethereum Classic improve its security to prevent future 51% attacks?** Ethereum Classic can enhance its security by increasing the network's hashrate, implementing defensive mining strategies, and improving collaboration between developers and miners to strengthen the blockchain. **2: Should exchanges like Coinbase and OKEx consider delisting Ethereum Classic due to security concerns?** It is reasonable for exchanges to consider delisting Ethereum Classic if the security issues continue. The network's vulnerabilities might deter users and investors, and delisting could be a protective measure.

Incident handler's journal:

Journal:08 Data on nearly 1 million NHS patients leaked online following ransomware attack on London hospitals

Date: Sep 10, 2024	**Entry:** #8
Description	A ransomware attack by the Qilin group hit NHS hospitals in London, exposing personal and medical data of nearly 1 million patients. The stolen data, including sensitive health information, was published online in June 2024.
Tool(s) used	Ransomware, Qilin Ransomware Group, Synnovis IT Systems

The 5 W's	● **Who**: The Qilin ransomware group. ● **What**: A ransomware attack on NHS hospitals in London ● **Where**: NHS hospitals and pathology service provider Synnovis in London, UK ● **When**: The attack occurred earlier this year, with data published in June 2024 ● **Why**: The Qilin ransomware group gained access to sensitive medical data, including patient appointment requests, medical test results, and symptoms of private medical conditions. The data, which includes names, birth dates, NHS numbers, and contact details, was published online, putting over 900,000 individuals at risk. The attack disrupted critical pathology services and led to a shortage of blood supplies.
Additional notes	□ **How can NHS organizations prevent future ransomware attacks?** • The NHS can enhance its cybersecurity by implementing stronger network defenses, improving staff training to detect phishing attempts, and regularly updating IT systems. Collaboration with cybersecurity experts and using advanced encryption methods can also help protect sensitive patient data. □ **Should NHS organizations notify patients immediately if their data is compromised?** • Yes, NHS organizations should promptly notify affected individuals about any data breaches, particularly when sensitive medical information is involved. Early notification allows patients to take necessary precautions and be aware of the potential risks.