INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

DEPARTMENT OF SOFTWARE ENGINEERING

COURSE: CS-375 Information Security

PRESENTED TO: Ms. Umara Zahid

INCIDENT HANDLER'S JOURNAL

BY:

Sajjal Khalil (4488-FOC/BSSE-F22-A)

Incident handler's journal

➢ Entry: #1: Mustang Panda Feeds Worm-Driven USB Attack Strategy

Date: Sep 9,2024	Entry# 1
Description	Documenting a cybersecurity incident
Tool(s) used	USB-spread worms and spear-phishing with malicious attachments to deliver custom malware like PUBLOAD, DOWNBAIT, and CBROVER.
The 5 W's	● **Who:** Mustang Panda, a state-sponsored group targeting APAC government entities recognized for their cyber-espionage activities. ● **What:** Cyber-espionage through self-propagating malware (HIUPAN worm) delivered via USB drives and spear-phishing tactics. ● **Where:** The targeted entities included government organizations such as military, police departments, foreign affairs, welfare agencies, executive branches, and public education sectors across countries like Myanmar, the Philippines, Vietnam, Singapore, Cambodia, and Taiwan. ● **When:** Initial report surfaced on September 9, 2024, with ongoing malicious activities observed in a blog post by Trend Micro. ● **Why:** Aimed at system control and data exfiltration for intelligence-gathering purposes. The attack was conducted to achieve cyber espionage goals, including system control and data exfiltration from targeted government entities in the Asia-Pacific region.
Additional notes	1. What technologies can be deployed to detect and mitigate USB-based attacks? 2. How can organizations better defend against similar attacks in the future?

➢ Entry: #2: Ransomware Attack On High School In London

Date: Sep 9,2024	Entry# 2
Description	A ransomware attack had forced the Charles Darwin School in south London to close for the first half of the week, affecting approximately 1,300 students. The school is undergoing a forensic investigation and has disabled student Microsoft 365 accounts as a precaution.
Tool(s) used	None.
The 5 W's	● **Who:** The attackers are unknown, although the article mentions groups like Vice Society and LockBit as being active in targeting schools. The victims were Charles Darwin School, its staff, and approximately 1,300 students. ● **What:** Ransomware attack that encrypted the school's data leading to school closure. ● **Where:** Charles Darwin School in south London, United Kingdom. ● **When:** The attack occurred at the end of the recent week-implying that it happened during the start of September,2024. ● **Why:** Motive was financial gain through extortion, demanding a ransom payment in exchange for decrypting the school's data and/or not releasing stolen sensitive information.
Additional notes	1. What steps is the school taking to notify and support those affected by the potential data breach? 2. How did the school balance the need for security with the need for operational continuity?

➢ Entry: #3: Hospitals Cyber Attack Impacts 800 Operations

Date: June 14,2024	Entry# 3
Description	This news article reports on the significant disruption to healthcare services in London following a cyberattack on Synnovis.
Tool(s) used	None.
The 5 W's	• **Who:** Unidentified hackers attacked Synnovis, impacting London hospitals. • **What:** A ransomware cyberattack on pathology provider Synnovis caused major service disruptions, including cancelled operations and appointments at London hospitals. • **Where:** The attack impacted hospitals in London, England, primarily King's College Hospital and Guy's and St Thomas' NHS Foundation Trusts. • **When:** The attack occurred recently (exact date not specified in the article)- around June 14,2024. • **Why:** Likely financially motivated ransomware attack aimed to disrupt services, cause chaos, and potentially access patient data.
Additional notes	1. How was patients care being prioritized during this disruption? 2. How does this attack compare to other recent cyberattacks on healthcare providers? Was a pattern observed?

➢ Entry: #4 Marriott & Starwood Face $52M Settlement

Date: Oct 12,2024 (Settlement)	Entry# 4
Description	Multiple data breaches affecting Marriott International, Inc. and its subsidiary, Starwood Hotels, resulting in the exposure of sensitive customer data,
Tool(s) used	None.
The 5 W's	• **Who:** Unknown attackers breached Marriott/Starwood, affecting 344 million customers • **What:** Three data breaches exposed customer data, resulting in a $52 million settlement and mandated security improvements.. • **Where:** Marriott/Starwood systems and customers worldwide. • **When:** The breaches occurred between 2014 and 2020, with varying detection times. • **Why:** Likely for financial gain, exploiting security weaknesses in Marriott/Starwood's systems.
Additional notes	1. What steps were taken to eradicate the threat actors from the network? 2. Was any of the stolen data found to be used in subsequent attacks or sold on the dark web?

➢ <u>Entry: #5</u> American Water Reconnects Its Network Taps

Date: Oct 12,2024 (Blog Posted)	Entry# 5
Description	American Water, the largest regulated water and wastewater utility company in the US, experienced a cybersecurity incident that necessitated the temporary disconnection of its IT systems.
Tool(s) used	None.
The 5 W's	● **Who:** American Water was affected by an unknown attacker. ● **What:** A cybersecurity incident caused a temporary shutdown of IT systems but not water treatment operations. ● **Where:** The incident impacted American Water's corporate IT network across the US. ● **When:** The incident was initially reported on October 7, 2023. ● **Why:** The motive behind the attack is currently unknown but could be financial gain, espionage, or disruption.
Additional notes	1. Was a root cause analysis been initiated to determine how the attackers gained initial access? 2. Were any security tools bypassed or disabled during the attack?

➢ Entry: #6: Snowflake Account Attacks

Date: July 17,2024 (Blog Posted)	Entry# 6
Description	A financially motivated threat actor, UNC5537, targeted Snowflake customer accounts using stolen credentials obtained from infostealers and the dark web
Tool(s) used	Infostealers and Dark Web Marketplaces.
The 5 W's	• **Who:** The threat actor UNC5537, a financially motivated group, was behind the attacks. • **What:** Stolen credentials were used to access Snowflake customer accounts, resulting in data exfiltration and extortion attempts. • **Where:** The attacks targeted Snowflake's cloud data warehousing platform, specifically customer accounts hosted on it. • **When:** The incident was initially reported on Mid-April 2024. • **Why:** The primary motivation was financial gain through data theft and extortion.
Additional notes	1. Did the attackers use any specific techniques to bypass existing security measures within the Snowflake platform, or was it purely credential-based access? 2. How quickly were the affected companies able to detect and respond to the breaches?

➢ Entry: #7: Ransomware Attack On London Hospitals

Date: Sep 16,2024 (Blog Posted)	Entry#7
Description	A ransomware attack targeting Synnovis, a pathology service provider for NHS hospitals in London, resulted in the theft and subsequent online publication of sensitive patient data.
Tool(s) used	None.
The 5 W's	● **Who:** Attackers were the Qilin ransomware gang. ● **What:** A ransomware attack on Synnovis that led to the theft and online publication of sensitive NHS patient data. ● **Where:** The attacks targeted NHS hospitals. ● **When:** The attack occurred "earlier this year(2024)" it should be kept in mind that the data was published in June. ● **Why:** The likely motivation was financial extortion, a common goal for ransomware groups.
Additional notes	1. What was the potential impact on affected patients? 2. Are there any lessons learned from this incident that can be applied to improve cybersecurity within the healthcare sector?

➢ Entry: #8: Ethereum Classic Hit

Date: Aug 29,2020 (Blog Posted)	Entry#8
Description	Ethereum Classic (ETC) blockchain experienced its third 51% attack within August, reorganizing over 7,000 blocks and impacting roughly two days of mining activity.
Tool(s) used	None.
The 5 W's	● **Who:** Unknown attackers targeted the Ethereum Classic network ● **What:** A 51% attack, which is the third such attack on the Ethereum Classic blockchain in august. ● **Where:** The attack occurred on the Ethereum Classic blockchain ● **When:** The attack took place on a Saturday evening in August, following two similar attacks earlier in the same month. ● **Why:** The motive is likely financial gain through double-spending but the exact reason remains unknown.
Additional notes	1. What are the long-term implications for ETC if these attacks continue? 2. What are the specific technical vulnerabilities that allowed these 51% attacks to succeed?

➢ <u>Entry: #9:</u> 51% Attack: Definitaion, Who Is At Risk, Cost, Example

Date: May 08,2024 (Blog Posted)	Entry#9
Description	A 51% attack is a malicious act targeting a blockchain network where a single entity or group gains control of the majority (over 50%) of the network's mining hash rate (for Proof-of-Work blockchains) or staked value (for Proof-of-Stake blockchains).
Tool(s) used	ASICs (Application-Specific Integrated Circuits) or GPUs,
The 5 W's	• **Who:** Malicious actors seeking control of a blockchain's hash rate or staked value.. • **What:** Gaining over 50% network control to manipulate transactions, double-spend coins, and disrupt the blockchain. • **Where:** On the targeted cryptocurrency's blockchain network, with the attack originating from the attacker's mining or staking location. • **When:** Precisely timed to introduce an altered blockchain, with duration lasting as long as attackers maintain majority control. • **Why:** Typically for financial gain through double-spending, market manipulation, or to sabotage the targeted cryptocurrency.
Additional notes	1. How can the community be better prepared to respond to similar attacks in the future? 2. In most cases, does the attackers leave any traces or make any mistakes that could be used for future prevention?

➢ Entry: #10: DES Encryption Cracked via Brute Force Attack

Date: Jan 28, 2010 (Blog Posted)	Entry#10
Description	The Data Encryption Standard (DES), the U.S. government's standard symmetric encryption algorithm at the time, was successfully cracked using a distributed brute force attack performed by the DESCHALL team
Tool(s) used	DESCHALL Software.
The 5 W's	• **Who:** DESCHALL team (led by Rocke Verser, Matt Curtin, and Justin Dolske), with participation from numerous individuals and organizations contributing computing resources. • **What:** Cracked a DES-encrypted message by performing a distributed brute force attack, proving the weakness of the 56-bit key size, using idle computer resources. • **Where:** The attack was distributed globally, utilizing the internet to connect computers in various locations. • **When:** The attack took place during the summer of 1997, with the successful crack occurring in June 1997. • **Why:** To demonstrate the vulnerability of DES to brute force attacks, win the RSA Secret Key Challenge, and ultimately advocate for stronger encryption standards.
Additional notes	1. What are the key takeaways from the DES cracking story for security professionals and incident handlers? 2. What specific weaknesses in DES made it vulnerable to a brute-force attack, even though it was considered strong at the time?