INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

INCIDENT HANDLER JOURNAL

Information Security CS-375

Ms. Umara Zahid

Hajira Gul 4454-FOC/BSSE-F22-A

Section-A

12-30-2024

Incident handler's journal

Cyber Security Incident Analysis 1:

Mustang Panda Feeds Worm-Driven USB Attack Strategy

Date: September 9, 2024	Entry: #1
Description	Documenting a cyber-security incident involving a Chinese state-sponsored threat actor using self-propagating malware and spear-phishing.
Tool(s) used	Self-propagating malware (HIUPAN worm, PUBLOAD, FDMTP, PTSOCKET), spear-phishing campaign.
The 5 W's	• **Who**: Mustang Panda (Chinese state-sponsored threat actor). • **What**: Cyber-espionage attack involving self-propagating malware via USB drives and spear-phishing to deliver multistage malware. • **Where**: Government entities in the Asia-Pacific (APAC) region. • **When**: The incident was observed in a blog post by Trend Micro on September 9, 2024. • **Why**: To achieve system control and persistent data exfiltration, targeting government organizations for cyber espionage.
Additional notes	• **Impact:** Mustang Panda's cyber espionage campaign enables system control and sensitive data theft from APAC government entities through various malware delivery methods. 1. How could the APAC government entities prevent an incident like this from occurring again? 2. Should the targeted entities take specific actions to safeguard their data?

Cyber Security Incident Analysis 2:

Ransom ware attack forces high school in London to close and send students home

Date: September 9, 2024	Entry: #2
Description	The attack was likely initiated through phishing, exploiting vulnerabilities, or compromised credentials, the attack involved lateral movement to encrypt files across the network. This was followed by data exfiltration and a ransom demand, threatening a public data release, ultimately leading to system lock-out and school closure.
Tool(s) used	Ransomware (unspecified type), potentially exfiltration tools for data theft.
The 5 W's	• **Who**: Unknown cybercriminal group (likely ransomware group); Possibly Vice Society. • **What**: Ransomware attack causing system lockdown, data breach, threat of information release. • **Where**: Charles Darwin School, South London, UK • **When**: Discovered on or before Thursday of the week of September 9th, 2024. • **Why**: Financial gain through ransom payment, possibly data exfiltration.
Additional notes	• **Impact:** School closure, 1,300 students sent home, disruption to teaching, potential data breach for staff and students, systems cleansing. 1. What specific security measures could the school implement to prevent similar ransomware attacks in the future? 2. How can the school ensure more secure storage and backup of sensitive data, and how should it improve its recovery strategies?

Cyber Security Incident Analysis 3:

Hospitals cyber-attack impacts 800 operations

Date: Not specified in the article, but the article is dated in June 2024	Entry: #3
Description	A ransomware attack on pathology provider Synnovis severely disrupted London hospitals, leading to the rescheduling of 800+ operations and 700+ appointments, along with blood testing delays and a potential patient data breach.
Tool(s) used	Ransomware (unspecified type)
The 5 W's	• **Who**: Unknown cybercriminal group (likely ransomware group) • **What**: Ransomware attack on Synnovis, a pathology service provider, causing major disruption to NHS hospitals' ability to process tests, schedule appointments, and conduct operations. • **Where**: London, UK – specifically affecting King's College Hospital NHS Foundation Trust and Guy's and St Thomas' NHS Foundation Trust • **When**: The attack occurred sometime before June 2024 (the article does not give the date of the attack). Disruption and rearrangements happened in the first week after the attack. • **Why**: Financial gain through extortion of ransom payment, and potential for data theft.
Additional notes	• **Impact:** The cyberattack caused widespread disruption, with over 1500 operations and appointments rescheduled, including critical C-sections, and organ diversions. 1. What specific IT weaknesses enabled the ransomware attack? 2. How can the NHS strengthen cybersecurity for third-party providers like Synnovis?

Cyber Security Incident Analysis 4:

Marriott & Starwood Face $52M Settlement after Security Breaches

Date: Not specified for the breaches, but the settlement was in 2024	**Entry: #4**
Description	A series of data breaches (2014-2020) at Marriott/Starwood exposed 344 million customer's data, leading to a $52M settlement and demands for better security.
Tool(s) used	Unspecified tools for network intrusion and data exfiltration
The 5 W's	• **Who**: Malicious actors (unspecified groups or individuals) • **What**: Data breaches at Starwood Hotels, leading to the exposure of vast amounts of customer data. • **Where**: Primarily impacting customers of Marriott and Starwood Hotels worldwide, with a focus on US-based customers in the settlement. • **When**: Breaches occurred between June 2014 and 2020, with the settlement taking place in 2024. The first breach went undetected for 14 months. The second went undetected for years before being exposed in 2018. The third went undetected until 2020. • **Why**: Likely for financial gain, identity theft, or other malicious purposes.
Additional notes	• **Impact:** The breaches compromised the data of 344 million customers, resulting in a $52 million settlement and highlighting major security failings. Sensitive data, including payment and passport details, were exposed, leading to significant potential for harm. 1. What specific security flaws were exploited? 2. How did attackers maintain long-term system access?

Cyber Security Incident Analysis 5:

American Water Reconnects Its Network Taps after Cyber Incident

Date: October 12, 2024 (Report Date)	**Entry: #5**
Description	American Water, a major US water and wastewater utility, took its systems offline after a cyber-security incident on Oct. 7th. The company is now reconnecting its infrastructure, stating no evidence of impact to water/wastewater facilities.
Tool(s) used	Unspecified cyberattack method.
The 5 W's	• **Who**: Unspecified cyber attacker(s). • **What**: Cyber incident forcing American Water to take systems offline. • **Where**: United States, impacting American Water's services across 14 states and 18 military installations. • **When**: Incident reported on Oct. 7, 2024, systems being reconnected by Oct 10th, 2024 • **Why**: Unspecified motivation.
Additional notes	• **Impact:** The incident led to the temporary shutdown of American Water's systems, impacting customer portal access and billing processes, though water/wastewater services were not affected. The incident highlights vulnerabilities in critical infrastructure and prompts discussions of enhanced cyber security measures. 1. What was the initial method of entry for the cyber attack on American Water's systems? 2. How long were the system offline, and how were services managed during the disruption?

Cyber Security Incident Analysis 6:

Snowflake Account Attacks Driven by Exposed Legitimate Credentials

Date: May 2024 (Start of Campaign), Article Date in June 2024	Entry: #6
Description	A campaign exploited exposed credentials to breach Snowflake customer accounts, allowing data theft and extortion. The attacks leveraged a lack of MFA, weak credential management, and absence of network allow lists.
Tool(s) used	Infostealer malware (to obtain credentials), compromised/stolen credentials.
The 5 W's	• **Who**: UNC5537 (financially motivated threat actor) and potentially other actors. • **What**: Account breaches via stolen credentials and data theft from Snowflake customer accounts. • **Where**: Impacting various companies using the Snowflake platform. • **When**: Campaign began in late May 2024, advertised in June 2024. • **Why**: Financial gain through extortion and data sales.
Additional notes	• **Impact:** The attacks compromised 165+ Snowflake customer accounts leading to data theft and extortion, highlighting major vulnerabilities from exposed credentials and a lack of MFA. 1. What measures should vendors take to monitor and respond to cyber attacks targeting their service providers? 2. How were the customer credentials exposed, and what is being done to prevent similar exposures?

Cyber Security Incident Analysis 7:

51% Attack: Definition, Who Is At Risk, Example, and Cost

Date: May 8, 2024 **(Article Update Date)**	**Entry: #7**
Description	A 51% attack occurs when an entity controls over 50% of a cryptocurrency network's hashing power, potentially allowing them to manipulate transactions, double-spend coins, and disrupt the network.
Tool(s) used	Control of over 50% of the network's hashing power (computing resources), specialized mining hardware (ASICs).
The 5 W's	• **Who**: A malicious entity or group controlling over 50% of a cryptocurrency network's hashing power. • **What**: A 51% attack aimed at manipulating blockchain transactions, double-spending, and disrupting network operations. • **Where**: Applicable to any cryptocurrency network using PoW or PoS with high concentration of staked coins. • **When**: Potential attack is continuous. However, the analysis was done in May, 2024. • **Why**: Primarily financial gain through double-spending and disrupting competing entities.
Additional notes	• **Impact:** Though costly and unlikely, a 51% attack could enable double-spending and disrupt crypto network operations. 1. How can crypto networks strengthen consensus to prevent 51% attacks? 2. How can users protect against losses from 51% attacks on smaller networks?

Cyber Security Incident Analysis 8:

Ethereum Classic Hit by Third 51% Attack in a Month

Date: August 29, 2020 (Date of Attack)	**Entry: #8**
Description	The Ethereum Classic blockchain suffered its third 51% attack in August 2020, allowing attackers to potentially manipulate transactions and double-spend coins.
Tool(s) used	Control of over 50% of the Ethereum Classic network's hashing power.
The 5 W's	• **Who**: Unidentified malicious entity or group. • **What**: 51% attack on the Ethereum Classic blockchain. • **Where**: Ethereum Classic network. • **When**: August 29, 2020, third attack in the month of August 2020 • **Why**: Likely financial gain through double-spending.
Additional notes	• **Impact:** This third 51% attack in a single month further compromised the Ethereum Classic network's integrity, enabling double-spending and raising concerns about its security. 1. What factors made the Ethereum Classic network particularly susceptible to these repeated attacks? 2. How can the Ethereum Classic community enhance its blockchain security and prevent future 51% attacks?

Cyber Security Incident Analysis 9:

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

Date: Data published in June 2024; analysis done in September 2024; article date not specified.	**Entry: #9**
Description	A Qilin ransomware attack on Synnovis exposed over 900,000 NHS patients' sensitive medical data, including symptoms and personal details.
Tool(s) used	Ransomware (Qilin), data exfiltration techniques
The 5 W's	• **Who**: Qilin ransomware group, Synnovis (impacted organization). • **What**: Ransomware attack leading to the theft and publication of sensitive NHS patient data. • **Where**: London, UK, impacting NHS patients using services through Synnovis. • **When**: Initial attack occurred before June 2024, stolen data published in June 2024. • **Why**: Financial gain, extortion, and potentially reputational damage.
Additional notes	• **Impact:** A ransomware attack on Synnovis leaked sensitive medical data of 900,000+ NHS patients, raising concerns about data protection. 1. How can NHS organizations ensure prompt, transparent communication after a cyberattack? 2. How can Synnovis improve security to prevent future breaches?