Incident Report

Contents

1. EXECUTIVE SUMMARY

An advanced and coordinated cyber-attack, indicative of state-sponsored capability, targeted our network infrastructure, compromising multiple hosts. The attack manifested through the execution of stealth commands across critical systems, escalation of privileges, harvesting of credentials, and strategic malware deployment. Notably, the incident involved the extraction of sensitive patient data and NATO-related information, signaling a blend of political espionage and financial gain motives.

The operational sophistication, alongside the tactical footprint left by the adversaries, closely corresponds with the behavioral patterns of known Advanced Persistent Threat (APT) groups. The primary suspects include APT29, APT40, and APT41, each with distinct geopolitical ties and operational histories. APT29, linked to Russian intelligence, is known for infiltrating government and political institutions. APT40's activities typically reflect China's strategic interests in maritime and healthcare sectors. However, the multi-faceted nature of the attack, including healthcare data exfiltration and association with a Hong Kong IP address, aligns significantly with APT41—referred to as Wicked Panda. APT41's dual espionage and cybercrime pursuits, coupled with their documented use of similar malware and attack methodologies, place them as the most likely orchestrators of this breach.

This event underscores the necessity for heightened cybersecurity vigilance, prompt legal compliance actions under GDPR, and an informed public relations strategy to mitigate patient concerns and broader stakeholder implications. The incident's ramifications necessitate a multifaceted response strategy, emphasizing legal adherence, patient communication, and long-term security enhancements to bolster trust and resilience against future cyber threats.

2. INCIDENT SUMMARY

A coordinated cyber-attack was detected and analyzed, affecting multiple hosts within our network. Initial compromise occurred through stealthy execution of scripts via cmd.exe on hosts sql01, epj01, ad01, and ad02. Following the breach, the attackers escalated privileges and conducted credential harvesting on confluence01 and exchange01. Defensive evasion was observed with the clearing of logs to mask activities.

Malware deployment was identified on ad02, with the installation of a remote access trojan and the use of mimikatz.exe for extracting credentials. This facilitated lateral movement within the network, as the attackers established persistence through account manipulation and privilege escalation on ad01 and ad02. The culmination of the attack is observed in the form of PowerShell downloads on epj01 and sql01, which likely preface the packaging of data for extraction. These actions, paired with more privilege escalation, indicate the attackers are setting the stage for a potential data exfiltration event.

Our analysis revealed a pattern consistent with advanced persistent threats, including the use of known malware, tactics for maintaining long-term access, and methods to avoid detection. Indications of command and control behavior were detected, primarily through PowerShell activity, which we assess was likely used for staging data extraction.

3. TIMELINE

Please refer to the attached file Incident_Evidence_Timeline.pdf.

The attack progresses through critical network assets, initiating with stealthy command executions on `sql01`, `epj01`, `ad01`, and `ad02`. `confluence01` and `exchange01` show signs of privilege escalation and log clearances for defense evasion. The attackers then use `ad02` for malware deployment and credential dumping, moving laterally to `ad01` to entrench their presence. The final act involves `epj01` and `sql01`, with indications of preparation for data exfiltration, culminating a sophisticated cyber assault.

4. ADVERSARY ACTIONS

Please refer to the MITRE_ATT&CK.pdf to see the full overview.

Execution:

Technique: T1059: Command and Scripting Interpreter

Correlating Incident details: The adversary used cmd.exe spawned by svchost.exe to execute commands across multiple systems (sql01, epj01, ad01, ad02), indicating an attempt to execute commands or scripts in a stealthy manner.

Persistence:

Technique: T1136: Create Account

Correlating Incident details: New user accounts were created to ensure continued access to systems, as seen on ad02.

Technique: T1098: Account Manipulation

Correlating Incident details: Users were added to privileged groups within Active Directory on ad02 and ad01, adjusting account properties to maintain access.

Privilege Escalation:

Technique: T1548: Abuse Elevation Control Mechanism

Correlating Incident details: There were attempts to exploit system mechanisms for privilege escalation, as indicated by the detection of privilege escalation using a first-time driver on ad01.

Defense Evasion:

Technique: T1070: Indicator Removal on Host

Correlating Incident details: Repeated clearing of windows and event log data was observed on exchange01 and ad02 to conceal the attackers' presence and actions.

Technique: T1036: Masquerading

Correlating Incident details: Processes were executed from unusual directories on ad02, suggesting attempts to masquerade the execution as benign activity.

Credential Access:

Technique: T1003: OS Credential Dumping

Correlating Incident details: Mimikatz.exe was detected on ad01, which is commonly used for dumping credentials from the memory of the LSASS process.

Discovery:

Technique: T1087: Account Discovery

Correlating Incident details: Discovery operations such as WhoAmI were executed to gather information about users and accounts on ad02.

Lateral Movement:

Technique: T1021: Remote Services

Correlating Incident details: The adversary used remote services, such as initiating remote file creation and tool transfer via SMB share on ad02 and ad01, and remote execution via file shares was observed.

Command and Control:

Technique: T1105: Ingress Tool Transfer

Correlating Incident details: Downloading of Roshal Archive (RAR) files or PowerShell scripts from the internet was observed on epj01, which is indicative of pulling tools or scripts into a compromised environment for further actions like data extraction.

5. THREAT ACTOR ATTRIBUTION

The complexity and sophistication of the cyber-attack on our systems indicate that it was state-operated. The use of advanced persistent threats, the capability for stealthy execution of scripts, lateral movement, and the deployment of specialized malware like Mimikatz for credential harvesting all point to the involvement of an adversary with resources and capabilities that extend beyond those of independent hackers or small groups. Furthermore, the targeted collection of sensitive patient data and NATO-related information align with state-sponsored interests in intelligence, surveillance, and potential influence operations.

Three state-sponsored groups emerge as primary suspects based on the attack's characteristics: APT29 (Cozy Bear), APT40, and APT41 (Wicked Panda). APT29 is known for targeting governmental networks in Europe and NATO countries and is linked to Russia's intelligence services. APT40 has been associated with operations that align with China's maritime and healthcare interests. APT41, also attributed to China, is known for its dual espionage and financial objectives, targeting a range of industries including healthcare and technology.

The modus operandi of the attack aligns most closely with APT41. This group has demonstrated the ability to conduct operations that serve both state-sponsored espionage and financial gain, which corresponds with the mixed motives observed in this breach. The deployment of malware for persistent access and data collection within the breached networks fits APT41's known capabilities. The political and financial implications of extracting patient information and NATO-related data also align with APT41's history of broad targeting and financial profiteering. The technical indicators, such as the malware used and the tactics of remaining undetected, are consistent with APT41's documented methods.

6. RECOMMENDATIONS

The timeline event list indicates that the attackers may have executed malicious activities on the hospital's network, potentially gaining unauthorized access to sensitive data stored within the hospital's systems. The presence of Mimikatz and other malware poses serious risks to patient data security and confidentiality. The attackers may have gained access to patient records, medical histories, treatment plans, and other sensitive health-related information stored within the hospitals systems. In this section we will highlight the need for immediate legal assessment under GDPR, as well as a legal liability that relies upon an analysis of the legal ramifications of past medical data breaches. Thus, through this section we will provide a prioritization of the activities under legal compliance. For the scope of this report the different recommendations have been assigned priority levels, these levels indicate how quickly the hospital should implement the recommendation after the attack, and what their plan of action should be.

6.1 Legal Compliance

6.1.1 Immediate Legal Assessment Under GDPR

Priority: ***HIGH***

Being an organization that handles the personal data of EU residents Nymindegab Private hospital must adhere to General Data Protection Regulation (GDPR). Nymindegab Private hospital processes sensitive personal data, specifically health data, this includes information related to patients' medical conditions, treatments, and histories, which are considered highly sensitive under GDPR (Art. 9).

A cybersecurity attack impacting sensitive health data triggers specific legal obligations under GDPR. It's crucial to understand these obligations to mitigate potential legal consequences and uphold compliance. Thus, the first step is the notification to the relevant supervisory authority, without undue delay, but no later than 72 hours of becoming aware of the breach (Art. 33 GDPR). Additionally, since the breach poses a high risk to individuals' rights and freedoms, affected data subjects must also be notified without undue delay (Art. 34 GDPR). Failure to comply will result in a maximum fine of up to €10 million or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83).

GDPR emphasizes the importance of implementing appropriate technical and organizational measures to ensure the security of personal data (Art. 32 GDPR). Following a cybersecurity attack, it's crucial to review and enhance these measures to prevent future breaches and safeguard sensitive data effectively.

GDPR encourages conducting regular risk assessments to identify vulnerabilities and mitigate potential risks to personal data. A thorough assessment following the cybersecurity attack is necessary to understand the extent of the breach and take corrective actions accordingly.

The cybersecurity attack may necessitate a Data Protection Impact Assessment (DPIA) to assess the impact on the security and privacy of health data and implement appropriate safeguards.

6.1.2 Legal Liability Analysis

Priority: ***MEDIUM***

With the help of a legal counsel conduct a thorough analysis of potential legal liabilities stemming from the breach, including any fines or penalties imposed by regulatory authorities and potential civil litigation from affected individuals. Once again, the sensitive nature of the data that was breached could result in a more severe reaction from the public and the consequent legal actions. It therefore is imperative that the hospital engages with professionals to display transparency through legal cooperation.

6.2 Public Relations and Business Recommendations

6.2.1 Emergency support

Priority: ***MEDIUM***

In the immediate aftermath of the cyberattack, many questions will arise from the patients about the best way forward, possible attacks / extortion using the data, what can be done to further mitigate any risks, etc.. To help the patients navigate this tumultuous time and show that Nymindegab Private Hospital is sympathetic to the consequences they are facing they should provide emergency support to the victims. This emergency support will be given in the form of: (1) legal advice, and (2) bridging contact to organizations that provide mental health guidance. The sooner these resources are provided to the victims the better they will be at mitigating the long-term adverse effects of such an attack for the mental health, and legal health of the affected patients.

6.2.2 Long-term Strategic Planning

Priority: ***LOW***

Following the cyberattack, the relationship between Nymindegab Private Hospital and its patients may become increasingly strained. This was quite notably seen in the aftermath of the data breach at the Finnish psychotherapy service provider, Vastaamo. The attackers initially demanded a ransom sum of €450,000 from Vastaamo, when Vastaamo refused to pay they contacted the compromised data subjects and demand a sum of €200-300 (“Finland Shocked by Therapy Center Hacking, Client Blackmail | AP News,” 2021).

To mitigate the negative consequences of the shaken trust Nymindgab Private Hospital must remain pro-active in showing that they are taking every reasonable step to mitigate the fallout, as well as ensuring that such an event does not happen again.

Due to the ripple effects of this cyberattack, there could be further reaching implications of the trust levels, not just for private hospitals but for any entity that holds our sensitive data. This could result in an increase in distrust for public hospitals too. Therefore, a collaboration with the Danish public hospitals which would display an increase in security measures and show a united front in all hospitals about how they are dedicated to ensuring this situation does not arise again.

Furthermore, by bringing in an external cybersecurity consultant to review their systems and publish that the cybersecurity attack was: (1) not the fault of the hospital, or if their security measures of the hospital are found insufficient (2) that the hospital has now implemented sufficient cybersecurity measures and are adhering to the newest advancements within the field. This should be coupled with a long-term plan of revisions of the cybersecurity methods, as well as continuous simulations that allow the hospital to familiarize themselves with the best approach during an attack, ensuring that the appropriate precautions have been taken. Indicating to the victims and relevant stakeholders that the likelihood of another attack is low, and if does happen they are equipped with the best tools to keep sensitive data from being breached.

6.3 System & Organization Recommendations

We would advise a dual-pronged strategy focused on system robustness and organizational agility. For systems, implementing continuous monitoring protocols is imperative for early threat detection. Strengthening identified system vulnerabilities is a non-negotiable step towards fortifying your defense against cyber intrusions, while routine control checks are essential to identify emergent weaknesses.

Organizationally, the creation of a detailed emergency response plan is paramount. This plan should outline clear procedures and designate responsibilities to key personnel, ensuring that all team members understand their roles in crisis scenarios. Effective communication channels must be established to ensure smooth coordination during an incident. Regular drills simulating extreme cyber threat scenarios will test the plan's efficacy and the staff's readiness, ensuring that both systems and personnel are prepared to respond to various cyber threats effectively.

7. REFERENCES

Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®. (o. D.). https://attack.mitre.org/techniques/T1595/

APT41, Wicked Panda, Group G0096 | MITRE ATT&CK®. (o. D.). https://attack.mitre.org/groups/G0096/

Chocolatecoat. (o. D.). *presentations/Analysis Without Paralaysis - MiSecCon.pptx at main · chocolatecoat/presentations*. GitHub. https://github.com/chocolatecoat/presentations/blob/main/Analysis%20Without%20%20Paralaysis%20-%20MiSecCon.pptx

Finland shocked by therapy center hacking, client blackmail | AP News. (2021, April 20). *AP News*. https://apnews.com/article/psychotherapy-cabinets-finland-6b27c895df0abd532a4fb000c9d5d517

IP Address LookUp | Geolocation. (o. D.). https://www.iplocation.net/ip-lookup