**Threat Analysis of MediSecure / Health Company**

**Introduction:**

The following report outlines the potential threat actors for the MediSecure which is a health company with people sensitive personal data, this report will mainly focus on the 1st critical threat found in the Nessus scan of IP-192.168.56.50 and its vulnerabilities.

1. **202039 - KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024)**

KB5040437 is a windows NTLM (NT LAN Manager) spoofing vulnerability. Where due to the lack in security features like MFA’s and identity validation, hackers can gain entre to unauthorized sections and access sensitive information or possibly install ransomware which might be used for extortion purpose.

Below you will find a report done on a possible threat actor that might attack and exploit this vulnerability for financial gain.

**Threat Report:**

|  |  |
| --- | --- |
| Group Name: | * Gold SouthField Group   *https://attack.mitre.org/groups/G0115/* |
| Associated Groups: | * G0115 – Pinchy spider   *https://attack.mitre.org/groups/G0115/* |
| Description: | * Gold SouthField is a financially motivated hacker group discovered in 2018, uses ransomware and back door tactics to gain access to private and confidential information. They have been has been seen to use innovative tactics while running targeted attacks to extort monetary gain.   [*https://attack.mitre.org/groups/G0115/*](https://attack.mitre.org/groups/G0115/)  *https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack* |
| Techniques: | * Phishing email , with malicious links, downloaded as “Legitimate zip” file that had ransomware ready to install   *https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack* |
| Software Name: | * REvil (ID-S0496)   *https://www.secureworks.com/research/revil-sodinokibi-ransomware* |
| Group Association: | * Sodinokibi   *https://attack.mitre.org/software/S0496/* |
| Description: | * Sodinokibi or otherwise known as REvil is a ransomware attack, that is believed to be based out of Russia but activity has been seen in Asia. REvil   [*https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack*](https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack)   * REvil was first detected and identified to be used by Gold SouthField in 2019   *https://www.secureworks.com/research/revil-sodinokibi-ransomware* |
| Platform: | * Windows * Network Environments |
| Techniques: | * Remote Access Software (T1219) * [External Remote Services](https://attack.mitre.org/techniques/T1133) (T1133) * [Phishing](https://attack.mitre.org/techniques/T1566) (T1566) * [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195): [Compromise Software Supply Chain](https://attack.mitre.org/techniques/T1195/002) (T1195.002) * Command and Scripting Interpreter: PowerShell (T1059.001)   <https://www.secureworks.com/research/revil-sodinokibi-ransomware>  <https://attack.mitre.org/groups/G0115/>  *https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack* |

**Life Cycle of REvil/ Sodinokibi:**

* **Stage 1 / Infection Stage** – Usually spread through infected software downloads attached to phishing emails
* **Stage 2/ Malware Execution** – Begins searching the system to encrypt files
* **Stage 3/ Data Encryption** – Uses asymmetric and symmetric encryption to encrypt files
* **Stage 4/ Ransom Demand** – Once the sensitive data has been encrypted, REvil displays a ransom message asking for payment for the decryption key
* **Stage 5/ Payment and Decryption** – If paid, Decryption key is given to recover data
* **Stage 6/ Data Exfiltration** – Could possible exfiltrate sensitive data from the corrupted system for later extortion
* **Stage 7/ System Compromise** – Could possible corrupted further parts of the system leading to further attacks from other attackers
* **Stage 8/ Eradication** – If REvil has been detected, removal of it must be done immediately to prevent further damage
* **Stage 9/ Recovery** – After REvil has been removed, the systems should be restored to a secure state with implementing new security measures
* **Stage 10/ Post-Incident Activities** – Conduct reviews to identify the weakness that the attacker was able to exploit and implement new procedures

**Rationale choices why to fix the 202039 - KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024) Vulnerability:**

* Remote Access Software (T1219)
  + Can be installed and executed later on after the initial attack
  + Control the infected system
* [External Remote Services](https://attack.mitre.org/techniques/T1133) (T1133)
  + RDP Attacks
  + Can use remote management and monitoring (RMM) to gain access to systems
* [Phishing](https://attack.mitre.org/techniques/T1566) (T1566)
  + Phishing Campaigns
  + If convincing enough it is an easy way to gain access to sensitive systems
  + Relies on people complacency
* [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195): [Compromise Software Supply Chain](https://attack.mitre.org/techniques/T1195/002) (T1195.002)
  + Ransomware-as-a-service (RaaS)
  + Backdoor access
* Command and Scripting Interpreter: PowerShell (T1059.001)
  + Can use PowerShell to run scripts on infected systems

**Conclusion:**

It is imperative to address the vulnerabilities associated with 202039 - KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024) as to keep confidentiality and integrity of customer’s medical information and to maintain a secure IT environment for the customers as well.

By addressing this vulnerability you are also addressing the following exploits that might be used in the future malicious activity.

* Remote Access Software (T1219)
* [External Remote Services](https://attack.mitre.org/techniques/T1133) (T1133)
* [Phishing](https://attack.mitre.org/techniques/T1566) (T1566)
* [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195): [Compromise Software Supply Chain](https://attack.mitre.org/techniques/T1195/002) (T1195.002)
* Command and Scripting Interpreter: PowerShell (T1059.001)

Hacker groups like the one outlined in this report Gold SouthField could possibly be a great threat to the organisation by exploiting this vulnerability by using REvil/ Sodinokibi and exploiting the weaknesses found associated with KB5040437 while executing REvil/ Sodinokibi to encrypt data and use it for extortion and financial gain.

**References:**

<https://attack.mitre.org/groups/G0115/>

<https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack>

<https://www.secureworks.com/research/revil-sodinokibi-ransomware>

<https://attack.mitre.org/software/S0496/>

<https://attack.mitre.org/techniques/T1219/>

<https://attack.mitre.org/techniques/T1059/>

<https://attack.mitre.org/techniques/T1566/>

<https://attack.mitre.org/techniques/T1195/>

<https://attack.mitre.org/techniques/T1133/>