MedusaLocker Ransomware and Medusa Threat Actor: An ATT&CK Threat Intelligence Report

Group Name: Medusa

Associated Groups: None documented

Description: Medusa is a cyber threat group known for deploying the MedusaLocker ransomware, which targets various sectors to extort ransom payments by encrypting critical data and demanding cryptocurrency payments for decryption.

Techniques:

1. Phishing: Spearphishing Attachment (T1566.001)
   - Description: Medusa uses spearphishing emails with malicious attachments to gain initial access to target systems.
   - Reference: [FireEye](https://www.fireeye.com/blog/threat-research/2020/05/ransomware-attackers-use-spear-phishing-emails.html)

2. Command and Scripting Interpreter: PowerShell (T1059.001)
   - Description: MedusaLocker employs PowerShell scripts to execute malicious commands and facilitate lateral movement within a network.
   - Reference: [Microsoft](https://www.microsoft.com/security/blog/2020/04/15/attackers-leveraging-powershell-to-gain-foothold-in-networks/)

3. Valid Accounts: Local Accounts (T1078.003)

- Description: MedusaLocker uses stolen or compromised local accounts to maintain persistence and escalate privileges.
- Reference: [CISA](https://us-cert.cisa.gov/ncas/alerts/aa20-205a)

4. File and Directory Discovery (T1083)
   - Description: Medusa conducts file and directory discovery to identify critical files and directories to encrypt.
   - Reference: [Sophos](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-whitepaper-latest-ransomware-techniques.pdf)

5. Data Encrypted for Impact (T1486)
   - Description: MedusaLocker encrypts data on target systems to disrupt operations and coerce ransom payments.
   - Reference: [Kaspersky](https://securelist.com/ransomware-attacks-2020/97222/)

Software Name: MedusaLocker

Group Association: Medusa

Description: MedusaLocker is ransomware used by the Medusa group to encrypt data and demand ransom payments for decryption keys.

Platform: Windows

Techniques:

- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

  - Description: MedusaLocker adds registry run keys to ensure the ransomware starts upon system boot.
  - Reference: [MITRE](https://attack.mitre.org/techniques/T1547/001/)

- File and Directory Discovery (T1083)
  - Description: MedusaLocker performs file and directory discovery to locate files for encryption.
  - Reference: [Sophos](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-whitepaper-latest-ransomware-techniques.pdf)

Rationale for Technique Choices

Phishing: Spearphishing Attachment (T1566.001)

- Effective initial access method, widely used.

Command and Scripting Interpreter: PowerShell (T1059.001)

- Versatile tool for executing commands and scripts.

Valid Accounts: Local Accounts (T1078.003)

- Allows persistent access and privilege escalation.

File and Directory Discovery (T1083)

- Essential for locating valuable data to encrypt.

Data Encrypted for Impact (T1486)

- Directly impacts operations, increases likelihood of ransom payment.

Vulnerability Analysis

CVE-2021-34527 (PrintNightmare)

- CWE: CWE-269, CWE-306, CWE-287
- CAPEC: CAPEC-111 (Abuse Elevation Control Mechanism), CAPEC-93 (Command and Scripting Interpreter), CAPEC-272 (Valid Accounts)
- ATT&CK:
  - T1548.002: Abuse Elevation Control Mechanism (Used by Medusa)
  - T1059.001: Command and Scripting Interpreter: PowerShell (Used by Medusa)
  - T1078: Valid Accounts (Used by Medusa)
- Action: Take action
- Rationale: PrintNightmare allows remote code execution and privilege escalation, both critical vulnerabilities. Medusa uses related techniques, making it likely they would exploit this CVE.
- Reference: [Microsoft](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)

CVE-2020-1472 (ZeroLogon)

- CWE: CWE-287, CWE-345, CWE-362
- CAPEC: CAPEC-272 (Valid Accounts), CAPEC-220 (Exploitation of Remote Services), CAPEC-212 (Impair Defenses)
- ATT&CK:
  - T1078: Valid Accounts (Used by Medusa)
  - T1210: Exploitation of Remote Services (Not used by Medusa)
  - T1562.001: Impair Defenses: Disable or Modify Tools (Not used by Medusa)
- Action: Take action
- Rationale: ZeroLogon can bypass authentication to gain admin access. Medusa's usage of valid

accounts techniques suggests they might exploit this CVE.

- Reference: [CISA](https://us-cert.cisa.gov/ncas/alerts/aa20-205a)

CVE-2019-0708 (BlueKeep)

- CWE: CWE-787, CWE-400, CWE-415
- CAPEC: CAPEC-76 (Remote Service Exploitation), CAPEC-111 (Command Execution via PowerShell), CAPEC-192 (Indicator Removal)
- ATT&CK:
  - T1210: Exploitation of Remote Services (Not used by Medusa)
  - T1059.001: Command and Scripting Interpreter: PowerShell (Used by Medusa)
  - T1070.004: Indicator Removal on Host: File Deletion (Not used by Medusa)
- Action: Ignore
- Rationale: While BlueKeep is serious, it primarily targets remote services, which Medusa does not exploit extensively. Only one relevant ATT&CK code aligns with their methods.
- Reference: [Microsoft](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708)

References

1. FireEye: https://www.fireeye.com/blog/threat-research/2020/05/ransomware-attackers-use-spear-phishing-emails.html

2. Microsoft: https://www.microsoft.com/security/blog/2020/04/15/attackers-leveraging-powershell-to-gain-foothold-in-networks/

3. CISA: https://us-cert.cisa.gov/ncas/alerts/aa20-205a

4. Sophos: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-whitepaper-latest-ransomware-techniques.pdf

5. Kaspersky: https://securelist.com/ransomware-attacks-2020/97222/

6. MITRE: https://attack.mitre.org/techniques/T1547/001/

7. Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

8. CISA: https://us-cert.cisa.gov/ncas/alerts/aa20-205a

9. Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708