HC3: Analyst Note
February 24, 2023 TLP:CLEAR Report: 202302241700

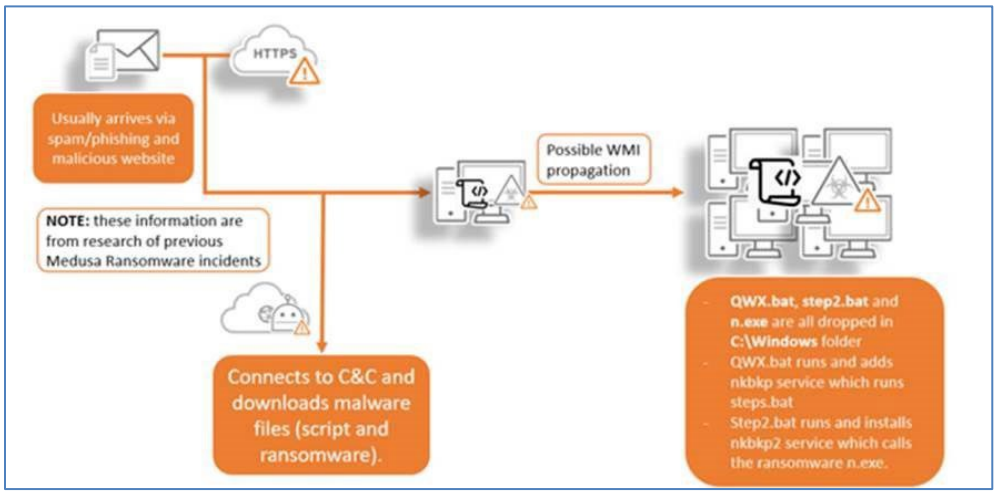
MedusaLocker Ransomware

Executive Summary
Ransomware variants used to target the healthcare sector, from relatively well-known cyber threat groups, continue to be a source of concern and attention. (See HC3 reports on Royal Ransomware and Clop Ransomware). Likewise, the threat from lesser known but potent ransomware variants, such as the MedusaLocker, should also be a source of concern and attention by healthcare security decision makers and defenders.

Report
The MedusaLocker ransomware was first detected back in September of 2019. Since then, MedusaLocker has infected and encrypted systems across multiple sectors, with primary targeting of the healthcare sector. During 2019, Medusa Locker leveraged the disorder and confusion surrounding the COVID-19 pandemic to launch attacks. MedusaLocker appears to operate as Ransomware-as-a-Service (RaaS) model, in which the developer of the MedusaLocker shares the ransomware with other threat actors in return for a share of the ransom payment. Based on the observed split noted in a June 2022 Advisory on the MedusaLocker by United States federal law enforcement agencies, including the Federal Bureau of Investigation (FBI), MedusaLocker ransomware payments appear to be consistently split between the affiliates who receive a share of the ransom. The affiliates receive approximately 55-60 percent per the time of the Advisory, and the developer receives the remainder.

Initially, threat actors behind the ransomware relied on phishing and spam email campaigns to compromise targets. As of 2022, Remote Desktop Protocol (RDP) vulnerabilities are the preferred Tactics, Techniques, and Procedures (TTP) to gain access to targeted networks by cyber criminals behind the ransomware. Moreover, MedusaLocker threat actors may still gain entry into networks via phishing campaigns in which the malware is attached to emails.

Figure 1. MedusaLocker attack vector and infection chain via spam or phishing.



Attribution
In June of 2022, security researchers examined millions of Russian hosts visible to internet scans,

specifically for penetration tools on Russian servers. The scans unveiled a network of hosts potentially used to launch ransomware attacks by criminal groups. MedusLocker infrastructure was identified as some of those hosts. Also discovered via identification of these Russian hosts was that ransomware cybercriminals were leveraging United States infrastructure, potentially in preparation of future attacks. This is not uncommon due to ransomware groups difficulties launching attacks from Russian infrastructure because most security tools preemptively block incoming traffic from Russia. To get around this, cybercriminals typically compromise hosts in the United States, or less conspicuous countries. To further obfuscate attacks, cybercriminals leverage infrastructure from universities or data centers, etc. Those compromised hosts are then used as redirects.

MedusaLocker Life Cycle

After initial access the MedusaLocker will propagate throughout a network from a batch file that executes a PowerShell script. MedusaLocker will next disable security and forensic software, restart the machine in safe mode to prevent detection or ransomware, and then encrypt files with AES-256 encryption algorithm. MedusaLocker will further establish persistence by deleting local backups, disabling start-up recovery to ultimately place a ransom note into every folder containing a file with compromised host's encrypted data.

Additional MedusaLocker Ransomware TTPs:

Tactic: Initial Access

- *MITRE ATT&CK T1078 Valid Accounts*

  Threat actors use brute-force password guessing for RDP services. The revealed password allows the attacker to gain initial access to the victim's network.
- *MITRE ATT&CK T1566 Phishing*

  In some cases, the ransomware is delivered via a phishing email as an attachment.
- *MITRE ATT&CK T1133 External Remote Services*

  Threat actors exploit vulnerable RDP services in the victim network to gain initial access.

Tactic: Execution

- *MITRE ATT&CK T1059.001 Command and Scripting Interpreter: PowerShell*

  MedusaLocker ransomware typically consists of a batch file named "qzy.bat" and a PowerShell script saved as a text file named "qzy.txt". When the batch file is executed, it calls the text file and runs the PowerShell script in the text file.
- *MITRE ATT&CK T1047 Windows Management Instrumentation*

  MedusaLocker uses Windows Management Instrumentation command-line utility (wmic) to delete volume shadow copies to prevent victims from recovering their encrypted data.

Tactic: Persistence

- *MITRE ATT&CK T1547 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder*
  MedusaLocker establishes persistence and executes the ransomware at system startup by adding the following registry entry.
- *MITRE ATT&CK T1168 Local Job Scheduling*
  MedusaLocker creates a scheduled task called "svhost" that runs the ransomware automatically every 15 minutes.

Tactic: Privilege Escalation

- *MITRE ATT&CK T1548.002 Abuse Elevation Control Mechanism Bypass UAC*
  MedusaLocker ransomware uses the built-in Windows tool called Microsoft Connection Manager Profile Installer (cmstp.exe) to bypass User Account Control (UAC) and runs arbitrary commands with elevated privileges.
- *MITRE ATT&CK T1078 Valid Accounts*
  Threat actors use brute-force password guessing for RDP services. If the guessed password belongs to the domain administrator, they can execute commands with elevated privileges.

Tactic: Defense Evasion

- *MITRE ATT&CK T1562.001 Impair Defenses: Disable or Modify Tools*
  MedusaLocker disables security products such as antivirus to avoid being detected.
- *MITRE ATT&CK T1562.009 Impair Defenses: Safe Mode Boot*
  In safe mode, Windows OS starts up with limited defenses. MedusaLocker abuses this aspect of the safe mode to evade endpoint defenses.

Tactic: Credential Access

- *MITRE ATT&CK T1110 Brute Force*
  Threat actors use brute-force password guessing for RDP services.

Tactic: Discovery

- *MITRE ATT&CK T1083 File and Directory Discovery*
  MedusaLocker searches for files and directories in the victim's computer. After discovery, the ransomware starts to encrypt all files and directories with the exception of the following folders.

- *MITRE ATT&CK T1135 Network Share Discovery*
  MedusaLocker searches for shared files in the network. The shared files also indicate that there might be other hosts in the network that can be moved to laterally.

- *MITRE ATT&CK T1012 Query Registry*
  MedusaLocker searches the registry hive to learn about security products deployed in the victim's network.

Tactic: Lateral Movement

- *MITRE ATT&CK T1021 Remote Services*
  MedusaLocker ransomware uses remote services to infect other hosts in the victim's network. Threat actors use RDP, PsExec, and SMB to spread the ransomware payload.

Tactic: Command and Control

- *MITRE ATT&CK T1105 Ingress Tool Transfer*
  MedusaLocker uses certutil.exe to transfer files from its command-and-control server to the victim's network.

Tactic: Impact

- *MITRE ATT&CK T1486 Data Encrypted for Impact*
  MedusaLocker uses a hybrid encryption approach. The victim's files are encrypted with an AES-256 symmetric encryption algorithm, and the secret key is encrypted with RSA-2048 public-key encryption.
- *MITRE ATT&CK T1490 Inhibit System Recovery*
  MedusaLocker deletes backup copies of the encrypted files to prevent its victims from recovering them with the following commands.

Mitigation

MedusaLocker is currently targeting unsecured RDP servers, desktops and vulnerabilities in the software. To defend against RDP attacks, healthcare organizations should holistically require all RDP instances to have multiple levels of access and authentication controls, including some of the following:

- Monitor RDP utilization, and flag first-time-seen and anomalous behavior -- particularly failed login attempts.
- Implementing account lockout policies to defend against brute force attacks.
- Prioritize patching RDP vulnerabilities that have known public exploits.
- Make strong passwords and two-factor authentication mandatory when using RDP.
- RDP should never be open to the Internet.

- Utilize a VPN to enable remote users to securely access the corporate network without exposing their computer to the Internet.
- Change the default port used by RDP from 3389 to another.
- Restrict access to the Remote Desktop port to an individual or group of trusted IP addresses and allow-list connections to specific trusted hosts.

Additional Mitigation Steps

Other mitigation techniques should include:

- Implementing a recovery plan that maintains and retains multiple copies of sensitive or proprietary data and servers in physically separate, segmented, and secure locations.
- Adding an email banner to emails received from outside your organization.
- Disabling hyperlinks in received emails.

Additional Partner and Industry Resources:

- Tips and Tactics: Preparing Your Organization for Ransomware Attacks (nist.gov)
- Stop Ransomware | CISA
- Ransomware Playbook - Cyber Readiness Institute
- Prepare, React, and Recover from Ransomware (405d-website-8459en001cm127.s3.amazonaws.com)
- #StopRansomware: MedusaLocker | CISA

References

"Solutions and Protections against the Medusa Ransomware." Trend Micro. 17 December 2020. Solutions and Protections against Medusa Ransomware (trendmicro.com)

"StopRansomware: MedusaLocker." CISA. 11 August 2022. #StopRansomware: MedusaLocker | CISA

"Russian Ransomware C2 Network Discovered in Censys Data." Censys. 21 July 2022. Russian Ransomware C2 Network Discovered in Censys Data - Censys

Yuceel, Huseyin Can. "MedusaLocker Ransomware Analysis, Simulation, and Mitigation." Picus Security. 01 July 2022. MedusaLocker Ransomware Analysis, Simulation, and Mitigation (picussecurity.com)

Cobb, Michael. "10 RDP Security Best Practices to Prevent Cyberattacks." TechTarget. August 2020. 10 RDP security best practices to prevent cyberattacks | TechTarget

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback