March 25, 2025

EMERGING THREATS

MEDUSA RANSOMWARE

UPDATE 03/25/2025: Since June 2021, Medusa ransomware, operating as a ransomware-as-a-service (RaaS), has been confirmed to have compromised over 300 organizations across critical infrastructure sectors, including healthcare, education, legal, insurance, technology, and manufacturing. In March of 2025, CISA released a Cybersecurity Advisory as a part of their @StopRansomware effort, offering technical details that were identified through recent FBI investigations. The actors exploit unpatched vulnerabilities in public-facing applications and often collaborate with initial access brokers to infiltrate networks. They have been observed to employ living-off-the-land techniques, leveraging legitimate system tools like PowerShell and Windows Management Instrumentation (WMI) for reconnaissance and lateral movement. Medusa affiliates deploy tools such as Mimikatz for credential harvesting and use software deployment utilities like PDQ Deploy and PsExec to distribute the ransomware payload. As mentioned in the earlier release of this collection, the ransomware encrypts data using AES-256 encryption, appends the ".medusa" extension to affected files, and deletes volume shadow copies to inhibit system recovery. In conjunction with the advisory released by CISA, threat hunters at Intel 471 have updated the collection with additional Hunt Packages.

THREAT SUMMARY

UPDATE 03/25/2025: Since June 2021, Medusa ransomware, operating as a ransomware-as-a-service (RaaS), has been confirmed to have compromised over 300 organizations across critical infrastructure sectors, including healthcare, education, legal, insurance, technology, and manufacturing. In March of 2025, CISA released a Cybersecurity Advisory as a part of their @StopRansomware effort, offering technical details that were identified through recent FBI investigations. The actors exploit unpatched vulnerabilities in public-facing applications and often collaborate with initial access brokers to infiltrate networks. They have been observed to employ living-off-the-land techniques, leveraging legitimate system tools like PowerShell and Windows Management Instrumentation (WMI) for reconnaissance and lateral movement. Medusa affiliates deploy tools such as Mimikatz for credential harvesting and use software deployment utilities like PDQ Deploy and PsExec to distribute the ransomware payload. As mentioned in the earlier release of this collection, the ransomware encrypts data using AES-256 encryption, appends the ".medusa" extension to affected files, and deletes volume shadow copies to inhibit system recovery.

In conjunction with the advisory released by CISA, threat hunters at Intel471 have updated the collection with additional Hunt Packages related to the following:

- Installation(and usage) of malicious tooling
- Privilege escalation via user addition(s) to security groupings
- Manipulation of RDP related settings to forcing a system to be more susceptible

Prior Information: Medusa Ransomware is a variant that was believed to have emerged in June 2021 and has been becoming increasingly prolific as of late. While \u201cMedusa\u201d has been commonly used in the name of other ransomware, malware, and botnets, it is distinct from its similarly named competitors (such as MedusaLocker). The ransomware claims to exfiltrate data from compromised organizations to perform a "double-extortion attack", this is a type of attack in which the threat actor will not only encrypt compromised systems, but also sell or release the exfiltrated data publicly if a ransom is not met. Medusa Ransomware uses a .MEDUSA file extension for files it encrypts. Medusa Ransomware is considered to be an active threat, and thus poses a significant and present risk that should be ascertained and prepared for.

Hunt Package Collection:

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('BFF39DDE-2798-48D0-BC23-3517498A95E7'),touched:!t)

SYNOPSIS

Medusa Ransomware is a human-operated ransomware that was first observed in June 2021, and has recently come into the spotlight after a series of successful and high-profile attacks on corporate victims, including the Minneapolis Public School district. The group has demanded a $1 million ransom in exchange for the decryption key. Medusa Ransomware is distinct from other actors, malware, and ransomware that go by the same name, such as MedusaLocker or Medusa Botnet.

The ransomware shuts down over 280 Windows services and processes, including those for mail servers, backup servers, database servers, and security software, that may prevent files from being encrypted. Medusa then deletes Windows Shadow Volume Copies to prevent them from being used to recover files. The ransomware encrypts files with the AES-256 + RSA-2048 encryption using the BCrypt library, appends the .MEDUSA extension to encrypted file names, and creates a ransom note named !!!READ_ME_MEDUSA!!!.txt in each folder containing information about what happened to the victim's files. Medusa is different from the older MedusaLocker Ransomware in several ways, including the type of ransom notes they leave ("!!!READ_ME_MEDUSA!!!.txt") and the file extensions they use for encrypted files (".MEDUSA").

The ransomware claims to exfiltrate data from compromised organizations to perform a "double-extortion attack", this is a type of attack in which the threat actor will not only encrypt compromised systems, but also sell or release the exfiltrated data publicly on their leak site "Medusa Blog" if a ransom is not met. Due to Medusa Ransomware being a relatively new variant, and with additional information about its campaign, targets, and any additional capabilities being discovered, Intel 471 will be updating the Threat Hunt Packages as more information about it is released.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('BFF39DDE-2798-48D0-BC23-3517498A95E7'),touched:!t)

RELATED HUNT PACKAGES

Rclone Activity - Potential Data Exfiltration

https://hunter.cyborgsecurity.io/details/use-case/7b8b354f-8f5b-41ba-bc26-786dcaae6439

Excessive Process and Service Stop Attempts - Potential Malware Infection

https://hunter.cyborgsecurity.io/details/use-case/f7c8103d-8366-45f0-b49b-50a121c43907

Enabling RDP Connections through Registry Modification

https://hunter.cyborgsecurity.io/details/use-case/c44db69a-314e-46cc-b14a-7e5bd6a6e551

Suspicious BITS Activity - ScriptBlock

https://hunter.cyborgsecurity.io/details/use-case/a829ece6-c94c-4dae-b34c-e2b80309d2a1

Suspicious BITS Activity

https://hunter.cyborgsecurity.io/details/use-case/a96fd1ad-53c7-4125-9dfd-1dffa2f68f2d

Possible Delayed Execution in CommandLine Argument Using Ping.exe and Loopback Address

https://hunter.cyborgsecurity.io/details/use-case/a2e40a77-69b7-4cdc-bf89-e04288bbe2c5

SoftPerfect Network Scanner Write File Validation

https://hunter.cyborgsecurity.io/details/use-case/9c24237b-b737-43d1-8615-997bc690579d

Taskkill.exe executed multiple times in a short period

https://hunter.cyborgsecurity.io/details/use-case/219d9dd8-0ffb-4052-909e-8ba86a6db08c

Potential Exfiltration - Common Rclone Arguments

https://hunter.cyborgsecurity.io/details/use-case/f075c217-783e-459a-aeb4-42ea91e07af7

UAC Bypass Attempt via Elevated COM Abuse

https://hunter.cyborgsecurity.io/details/use-case/03036b01-dc04-4cd1-9388-bd62e1b0ff2d

UAC Bypass Method - Cmstplua COM (Process Execution)

https://hunter.cyborgsecurity.io/details/use-case/6a26c900-3e20-4796-b4db-c66276f086ee

Disabling Windows Security Services via Registry Edit Methods

https://hunter.cyborgsecurity.io/details/use-case/bdb6f049-914c-4fae-a2fa-74443e9fd1a2

CertUtil file download

https://hunter.cyborgsecurity.io/details/use-case/f7b279bf-f1f9-4506-b636-e66f1834a278

Excessive Windows Discovery and Execution Processes - Potential Malware Installation

https://hunter.cyborgsecurity.io/details/use-case/6d1c9f13-e43e-4b52-a443-5799465d573b

Attempted Backup Deletion - Potential Ransomware Activity

https://hunter.cyborgsecurity.io/details/use-case/70cecfdc-dfb0-49de-a2ad-1a07344cf776

Volume Shadow Copy Service Disabled

https://hunter.cyborgsecurity.io/details/use-case/2edc918b-5d28-4e4d-8003-2cf980329f67

Advanced IP Scanner Tool Utilization

https://hunter.cyborgsecurity.io/details/use-case/181b11a6-3391-4d98-aaab-a2544f03c2ef

RDP Enabled Via NETSH

https://hunter.cyborgsecurity.io/details/use-case/6322023c-8874-41f2-aa0b-c6600d47398c

Resize Shadow Storage with 'vssadmin'

https://hunter.cyborgsecurity.io/details/use-case/4e88afda-0ae4-4acf-ac55-b7e01d48de68

User Added to Default Privileged Windows Security Groups

https://hunter.cyborgsecurity.io/details/use-case/b6365ad5-0ccd-4426-97bc-b9484eb9579f

Suspicious bcdedit Activity - Potential Ransomware

https://hunter.cyborgsecurity.io/details/use-case/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

Shadow Copies Deletion Using Operating Systems Utilities

https://hunter.cyborgsecurity.io/details/use-case/2e3e9910-70c1-4822-804a-ee9919b0c419

Common Ransomware Encrypted File Extensions

https://hunter.cyborgsecurity.io/details/use-case/970ae439-d6f5-497d-9086-ac7307327efc

Powershell Encoded Command Execution

https://hunter.cyborgsecurity.io/details/use-case/d2d3bbc2-6e57-4043-ab24-988a6a6c88db

Windows Defender Tampering - Possible Malware Activity

https://hunter.cyborgsecurity.io/details/use-case/aa6e2535-e1e3-4f0f-80e4-68cc47fc2684

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2024-1709
  - CVE-2024-1708
  - CVE-2023-4966

- MITRE Tactic Names:
  - Persistence
  - Command and Control
  - Impact
  - Discovery
  - Initial Access
  - Execution
  - Privilege Escalation
  - Exfiltration
  - Defense Evasion

- MITRE Technique Names:
  - PowerShell
  - Local Accounts
  - External Remote Services
  - Exfiltration Over Alternative Protocol
  - Network Share Discovery
  - Time Based Evasion
  - Domain Account
  - Service Stop
  - Bypass User Account Control
  - Exfiltration to Cloud Storage
  - Inhibit System Recovery
  - Modify Registry
  - Remote System Discovery

    - Disable or Modify System Firewall
    - System Network Configuration Discovery
    - Data Encrypted for Impact
    - Ingress Tool Transfer
    - Disable or Modify Tools
    - BITS Jobs
    - Obfuscated Files or Information

- MITRE Technique IDs:
    - T1486
    - T1567.002
    - T1197
    - T1562.004
    - T1562.001
    - T1548.002
    - T1105
    - T1016
    - T1497.003
    - T1490
    - T1135
    - T1048
    - T1133
    - T1489
    - T1018
    - T1078.003
    - T1027
    - T1112
    - T1059.001
    - T1136.002

- Threat Names:
    - Medusa Ransomware

REFERENCES

1. https://www.techradar.com/pro/security/us-government-warns-medusa-ransomware-has-hit-hundreds-of-critical-infrastructure-targets
2. https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/
3. https://www.techradar.com/news/the-medusa-ransomware-group-is-getting-serious
4. https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/
5. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a