Medusa Ransomware, Software S1244 | MITRE ATT&CK®

Archived: 2026-04-02 11:57:59 UTC

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Medusa Ransomware has launched PowerShell scripts for execution and defense evasion.[3][2]

.003 Command and Scripting Interpreter: Windows Command Shell

Medusa Ransomware has used `cmd.exe` to execute command on an infected host.[3][2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Medusa Ransomware has created a new PowerShell process using the `CreateProcessA` API.[2]

Enterprise T1486 Data Encrypted for Impact

Medusa Ransomware has encrypted files using AES-256 encryption, which then appends the file extension ".medusa" to encrypted files and leaves a ransomware note named "!READ_ME_MEDUSA!!!.txt."[3][1][4][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Medusa Ransomware has decoded XOR encrypted strings prior to execution in memory.[3][2]

Enterprise T1083 File and Directory Discovery

Medusa Ransomware has searched for files within the victim environment for encryption and exfiltration.[3][1][2] Medusa Ransomware has also identified files associated with remote management services.[3][1]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Medusa Ransomware has utilized the `ShowWindow` function to hide current window.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Medusa Ransomware has terminated antivirus services utilizing the gaze.exe executable.[3] Medusa Ransomware has also terminated antivirus services utilizing PowerShell scripts.[3][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Medusa Ransomware has the ability to delete itself after execution.[4] Medusa Ransomware also has the ability to delete itself after execution through the command `cmd /c ping localhost -n 3 > nul & del` .[3][2]

Enterprise T1490 Inhibit System Recovery

Medusa Ransomware has deleted recovery files such as shadow copies using `vssadmin.exe` .[3][1][4][2]

Enterprise T1559 Inter-Process Communication

Medusa Ransomware has leveraged the `CreatePipe` API to enable inter-process communication.[2]

Enterprise T1680 Local Storage Discovery

Medusa Ransomware has enumerated logical drives on infected hosts.[2]

Enterprise T1106 Native API

Medusa Ransomware has leveraged Windows Native API functions to execute payloads.[2]

Enterprise T1135 Network Share Discovery

Medusa Ransomware has identified networked drives.[3][4][2]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Medusa Ransomware has utilized XOR encrypted strings.[3][2]

Enterprise T1057 Process Discovery

Medusa Ransomware has utilized an encoded list of the processes that it detects and terminates.[3][4][2]

Enterprise T1679 Selective Exclusion

Medusa Ransomware has avoided specified files, file extensions and folders to ensure successful execution of the payload and continued operations of the impacted device.[3][4][2]

Enterprise T1489 Service Stop

Medusa Ransomware has the capability to terminate services related to backups, security, databases, communication, filesharing and websites.[1][4][2] Medusa Ransomware has also utilized the `taskkill /F /IM <process> /T` command to stop targeted processes and `net stop <process>` command to stop designated services.[4][2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Medusa Ransomware has the capability to detect security solutions for termination or deletion within the victim device using hard-coded lists of strings containing security product executables.[3]

Enterprise T1082 System Information Discovery

Medusa Ransomware has collected data from the SMBIOS firmware table using `GetSystemFirmwareTable` .[2]

Enterprise T1007 System Service Discovery

Medusa Ransomware has leveraged an encoded list of services that it designates for termination.[3][4][2]

Enterprise T1124 System Time Discovery

Medusa Ransomware has discovered device uptime through `GetTickCount()`.[2]

Source: https://attack.mitre.org/software/S1244