Medusa Group, Group G1051 | MITRE ATT&CK®

Archived: 2026-04-05 13:33:16 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Medusa Group has attempted to bypass UAC using Component Object Model (COM) interface.[4]

Enterprise T1087 .001 Account Discovery: Local Account

Medusa Group has leveraged `net user` for account discovery.[2]

Enterprise T1650 Acquire Access

Medusa Group has purchased user credentials and other sensitive data from Initial Access Brokers (IABs).[5][6][1][4]

Enterprise T1583 .006 Acquire Infrastructure: Web Services

Medusa Group has utilized a file hosting service named filemail[.]com to host a zip file that contained malicious payloads that facilitated follow-on actions.[5]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Medusa Group has communicated through reverse or bind shells over port 443 (HTTPS).[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Medusa Group has leveraged PowerShell for execution and defense evasion.[6][1][4] Medusa Group has also utilized PowerShell to execute a bitsadmin transfer from file hosting site.[5]

.003 Command and Scripting Interpreter: Windows Command Shell

Medusa Group has used Windows Command Prompt to control and execute commands on the system to include ingress, network, and filesystem enumeration activities.[1]

Enterprise T1136 .002 Create Account: Domain Account

Medusa Group has created a domain account within the victim environment.[1]

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

Medusa Group has used vulnerable or signed drivers to modify security solutions on victim devices.[1]

Enterprise T1486 Data Encrypted for Impact

Medusa Group 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."[5][1][2][3]

Enterprise T1652 Device Driver Discovery

Medusa Group has queried drivers on the victim device through the command `driverquery`.[1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Medusa Group has used HTTPS for command and control.[1]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

Medusa Group has created social media accounts including Telegram and X to publicize their activities.[5][6]

.002 Establish Accounts: Email Accounts

Medusa Group has created email accounts used in ransomware negotiations.[1]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Medusa Group has utilized Rclone to exfiltrate data from victim environments to cloud storage.[1][2]

Enterprise T1190 Exploit Public-Facing Application

Medusa Group has leveraged public facing vulnerabilities in their campaigns against victim organizations to gain initial access.[5][2] Medusa Group has also utilized CVE-2024-1709 in ScreenConnect, and CVE-2023-48788 in Fortinet EMS for initial access to victim environments.[1]

Enterprise T1083 File and Directory Discovery

Medusa Group has searched for files within the victim environment for encryption and exfiltration.[5][1][3] Medusa Group has also identified files associated with remote management services.[5][1]

Enterprise T1657 Financial Theft

Medusa Group has stolen and encrypted victims' data in order to extort victims into paying a ransom.[5][6][1][4][2][3]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Medusa Group has utilized the `ShowWindow` API function to hide the current window.[3]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Medusa Group has terminated antivirus services utilizing the gaze.exe executable and utilizing `psexec.exe`.[5][1][2] Medusa Group has also leveraged I/O control codes (IOCTLs) for terminating and deleting processes of identified security tools.[5]

.003 Impair Defenses: Impair Command History Logging

Medusa Group has removed PowerShell command history through the use of the PSReadLine module by running the PowerShell command `Remove-Item (Get-PSReadlineOption).HistorySavePath`.[1]

.004 Impair Defenses: Disable or Modify System Firewall

Medusa Group has utilized PsExec to execute batch scripts that modify firewall settings.[1] Medusa Group has also enabled and modified firewall rules to allow for RDP connections for lateral movement and device interactions.[1]

Enterprise T1070 .003 Indicator Removal: Clear Command History

Medusa Group has cleared command history by running the PowerShell command `Remove-Item (Get-PSReadlineOption).HistorySavePath`.[1]

.004 Indicator Removal: File Deletion

Medusa Group has deleted previously installed tools.[1]

Enterprise T1105 Ingress Tool Transfer

Medusa Group has leveraged certutil, PowerShell, and Windows Command to download additional tools to include RMM services.[1] Medusa Group has also engaged in "Bring Your Own Vulnerable Driver" (BYOVD) and downloaded vulnerable or signed drivers to the victim environment to disable security tools.[1][2]

Enterprise T1490 Inhibit System Recovery

Medusa Group has deleted recovery files such as shadow copies using `vssadmin.exe`.[5][1][2][3]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

Medusa Group has leveraged Component Object Model (COM) to bypass UAC.[4]

Enterprise T1570 Lateral Tool Transfer

Medusa Group has utilized legitimate software services such as PDQ Deploy to transfer malicious binaries and tools to other victimized hosts within the target environment.[2]

Enterprise T1112 Modify Registry

Medusa Group has modified Registry keys to elevate privileges, maintain persistence and allow remote access.[1]

Enterprise T1106 Native API

Medusa Group has leveraged Windows Native API functions to execute payloads.[3]

Enterprise T1046 Network Service Discovery

Medusa Group has the capability to use living off the land (LOTL) binaries to perform network enumeration.[1] Medusa Group has also utilized the publicly available scanning tool SoftPerfect Network Scanner (`netscan.exe`) to discover device hostnames and network services.[2]

Enterprise T1135 Network Share Discovery

Medusa Group has identified network shares using `cmd.exe /c net share` .[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Medusa Group has packed the code of dropped kernel drivers using the packer ASM Guard.[5]

.010 Obfuscated Files or Information: Command Obfuscation

Medusa Group has obfuscated PowerShell scripts with Base64 encoding.[1] Medusa Group has also obfuscated the code of dropped kernel drivers using a software known as Safengine Shielden which randomized the code through code mutations and then leveraged an embedded virtual machine interpreter to execute the code.[5]

Enterprise T1588 .002 Obtain Capabilities: Tool

Medusa Group has obtained and leveraged numerous RMM services, along with publicly available tools used for scanning.[5][1][2] Medusa Group has utilized tools such as Advanced IP Scanner and SoftPerfect Network scanner for user, system and network discovery.[1] Medusa Group has also acquired tools for command and control and defense evasion which include tunneling tools Ligolo and Cloudflared.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Medusa Group has leveraged Mimikatz to dump LSASS to harvest credentials.[1]

.003 OS Credential Dumping: NTDS

Medusa Group has accessed the ntds.dit file to engage in credential dumping.[2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

Medusa Group has utilized the `net group` command to query domain groups within the victim environment.[1]

Enterprise T1057 Process Discovery

Medusa Group has utilized a hard-coded security tool process list that identifies and terminates using an undocumented IOCTL code 0x222094.[5]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Medusa Group has used TOR nodes for communications.[5][6][2]

Enterprise T1219 Remote Access Tools

Medusa Group has leveraged Remote Access Software for lateral movement and data exfiltration.[5][1][2][3] Medusa Group has also been known to utilize Remote Access Software such as AnyDesk, Atera, ConnectWise, eHorus, N-Able, PDQ Deploy, PDQ Inventory, SimpleHelp and Splashtop.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Medusa Group has used RDP to conduct lateral movement and exfiltrate data.[1] Medusa Group has also utilized the Windows executable `mstsc.exe` for RDP activities through the command `mstsc.exe /v:{hostname/ip}`.[1]

Enterprise T1018 Remote System Discovery

Medusa Group has used PDQ Inventory to get an inventory of the endpoints on the network.[2]

Enterprise T1505 .003 Server Software Component: Web Shell

Medusa Group has utilized webshells to an exploited Microsoft Exchange Server.[5]

Enterprise T1489 Service Stop

Medusa Group has terminated services related to backups, security, databases, communication, filesharing and websites.[1][2][3]

Enterprise T1072 Software Deployment Tools

Medusa Group has utilized software deployment and management solutions to deploy their encryption payload to include BigFix and PDQ Deploy.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Medusa Group has detected security solutions for termination or deletion within the victim device using hard-coded lists of strings containing security product executables.[5]

Enterprise T1608 .002 Stage Capabilities: Upload Tool

Medusa Group has utilized a file hosting service called filemail[.]com to host a zip file that contained a RMM service such as ConnectWise.[5]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Medusa Group has utilized vulnerable or signed drivers to kill or delete services associated with endpoint detection and response (EDR) tools.[1]

Enterprise T1218 .014 System Binary Proxy Execution: MMC

Medusa Group has leveraged Microsoft Management Console (MMC) to facilitate lateral movement and to interact locally or remotely with victim devices using the command `mmc.exe compmgmt.msc /computer:{hostname/ip}`.[1]

Enterprise T1082 System Information Discovery

Medusa Group has leveraged `cmd.exe` to identify system info `cmd.exe /c systeminfo`.[1]

Enterprise T1016 System Network Configuration Discovery

Medusa Group has obtained host network details utilizing the command `cmd.exe /c ipconfig /all`.[1]

Enterprise T1033 System Owner/User Discovery

Medusa Group has utilized PsExec to execute `quser` to discover the user session information.[2]

Enterprise T1569 .002 System Services: Service Execution

Medusa Group has utilized PsExec to execute scripts and commands within victim environments.[5][1][2] Medusa Group has also used the Windows service RoboCopy to search and copy data for exfiltration.[2]

Enterprise T1529 System Shutdown/Reboot

Medusa Group has manually turned off and encrypted virtual machines.[1]

Enterprise T1078 Valid Accounts

Medusa Group has utilized compromised legitimate local and domain accounts within the victim environment to facilitate remote access and lateral movement sometimes in combination with PsExec.[1]

Enterprise T1047 Windows Management Instrumentation

Medusa Group has utilized Windows Management Instrumentation to query system information.[5][1][4]
