Medusa Ransomware: Evolving Tactics in Modern Cyber Extortion

loginsoft.com/post/medusa-ransomware-evolving-tactics-in-modern-cyber-extortion

September 18, 2024

Jason Franscisco

+

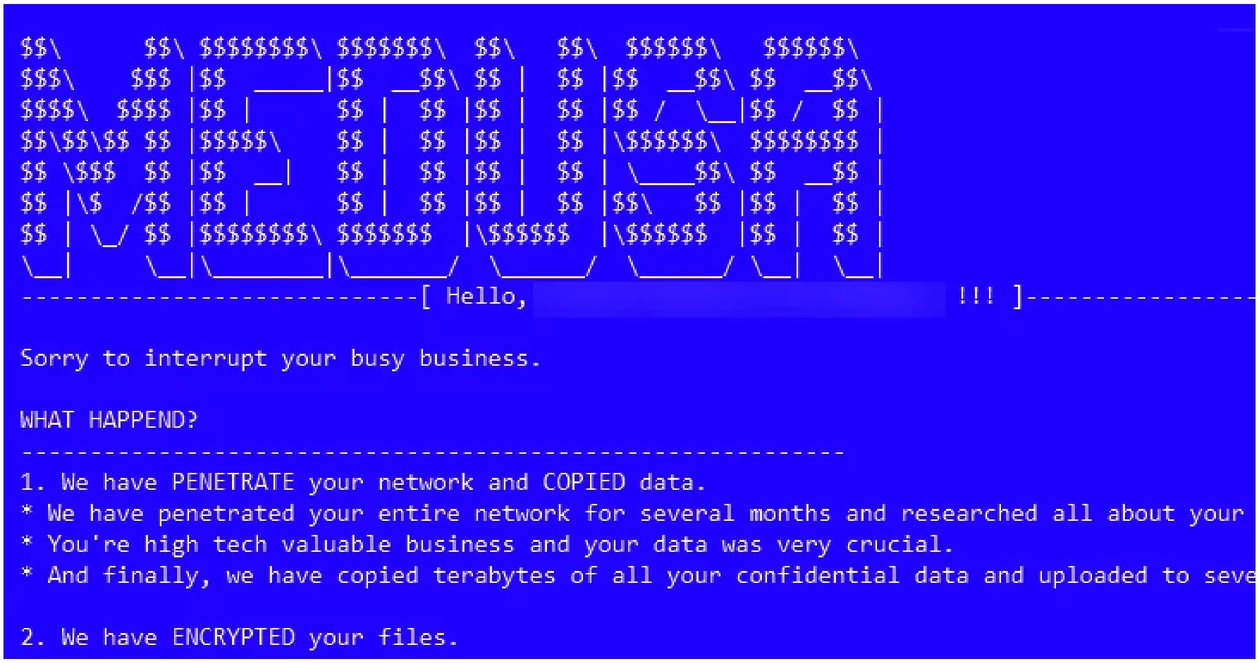
Introduction

Medusa, a prominent ransomware-as-a-service (RaaS) platform, emerged in June 2021 and has rapidly gained popularity among cybercriminals. In contrast to many ransomware groups that operate exclusively on the dark web, Medusa has taken an unconventional approach by establishing a visible presence on the surface web. This dual-platform strategy allows the group to reach a wider audience and potentially attract more affiliates.

Since 2023, the Medusa ransomware group has steadily increased its number of victims. Bitdefender projects that in 2024, Medusa could target over 200 organizations, a significant jump from the 145 victims reported in 2023. Medusa should not be confused with MedusaLocker, a similar ransomware-as-a-service (RaaS) that has been active since 2019.

This ransomware has demonstrated a global reach, targeting broad spectrum of industries such as healthcare, education, manufacturing, and retail with a particular focus on organizations in the United States, Europe, and Africa.

Recent investigations have uncovered that Medusa has been leveraging **CVE-2023-48788**, a critical SQL injection vulnerability in Fortinet's FortiClient EMS software, to gain initial access to targeted systems.



```
$$\      $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\
$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |
$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |
$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |
\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|
-----------------------------[ Hello, [redacted] !!! ]----------------

Sorry to interrupt your busy business.

WHAT HAPPEND?
-------------------------------------------------------------
1. We have PENETRATE your network and COPIED data.
* We have penetrated your entire network for several months and researched all about your
* You're high tech valuable business and your data was very crucial.
* And finally, we have copied terabytes of all your confidential data and uploaded to seve

2. We have ENCRYPTED your files.
```

Medusa Ransomware

Technical Analysis

Initial access

Medusa ransomware primarily gains access to networks through unsecured Remote Desktop Protocol (RDP) and phishing, while also exploiting vulnerable services and public-facing assets with known unpatched vulnerabilities.

Medusa leverages the **CVE-2023-48788** vulnerability in Fortinet's FortiClient EMS to gain initial access to target systems. By exploiting an SQL injection flaw, attackers can manipulate the FCTUID parameter in web requests, executing arbitrary commands on the affected server via **xp_cmdshell.**   This allows Medusa to establish a webshell, facilitating further data exfiltration and ransomware deployment.

Execution

Medusa utilizes PowerShell scripts to execute commands on host systems, facilitating data exfiltration and referencing the executable and binary components required to deploy the ransomware and perform encryption. During the execution phase, the **gaze.exe** component is run to terminate various services using the net command and to load files that include TOR links for data exfiltration.

Persistence

To maintain persistence, Medusa employs several strategies. The group uses compromised Remote Monitoring and Management (RMM) tools such as ConnectWise, PDQDeploy, and

AnyDesk, which are often whitelisted and less likely to raise suspicion. They conduct discovery processes to identify applications within the victim's environment, allowing them to replace legitimate programs with their own compromised versions.

Additionally, Medusa establishes persistence by executing PowerShell commands that modify registry key values, such as run in HKLM and HKCU, to ensure that their payloads execute on system startup.

Privilege Escalation

Once inside a network, Medusa leverages tools like **PsExec** to escalate privileges and secure a deeper foothold within the compromised system.

Defense Evasion

Medusa employs a sophisticated anti-malware evasion technique involving the installation of a malicious RMM agent and the loading of vulnerable drivers. These drivers actively identify and terminate processes associated with anti-malware solutions. By cross-referencing active processes with a predefined list, Medusa can disable over two hundred security-related processes. The group disables security tools using PowerShell scripts and adjusts registry settings to evade detection. They also employ string encryption techniques to obfuscate their malicious code.

Discovery

Medusa conducts thorough network reconnaissance with tools such as **Netscan** to identify valuable targets and map out the network topology.

Lateral Movement

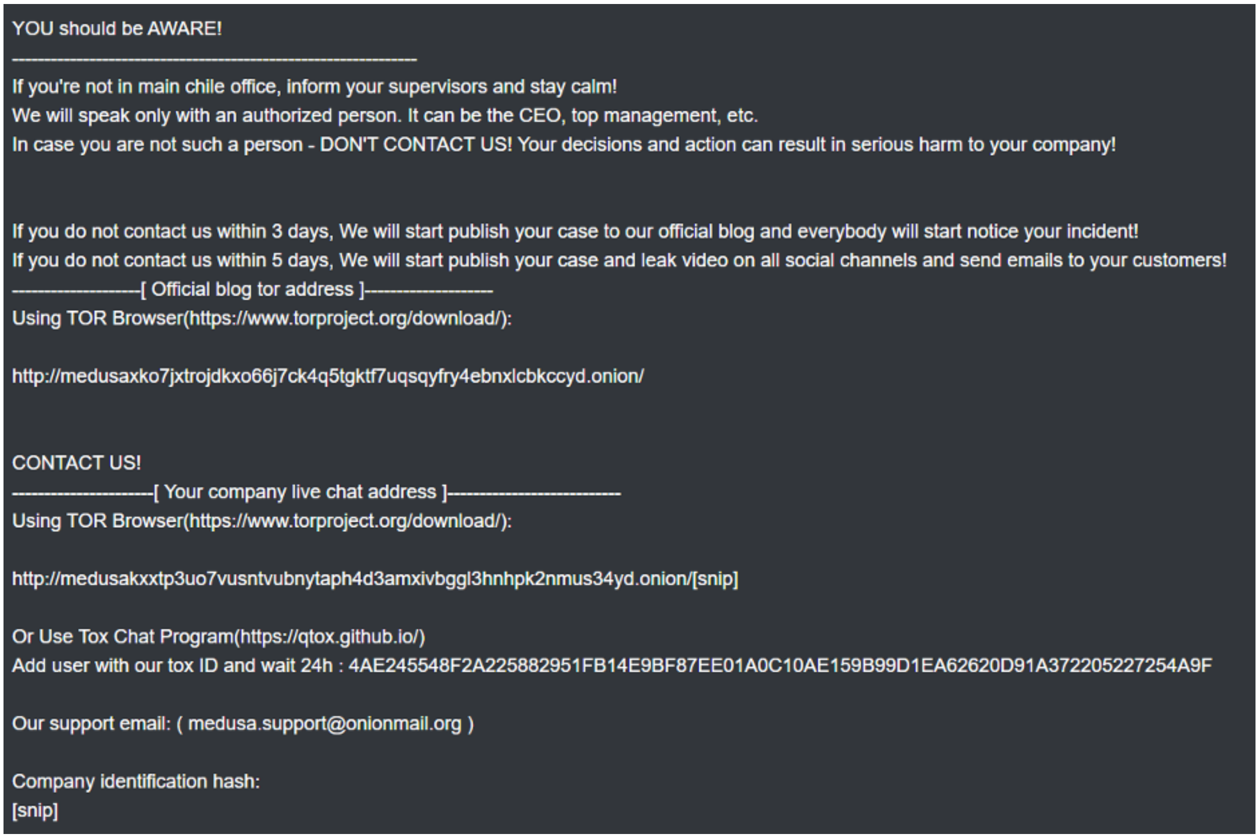
Medusa often acquires credentials by exploiting the compromised server and extracting them from the LSASS process. To achieve lateral movement, the ransomware group utilizes tools like **bitsadmin** to transfer malicious files from their webshell to target hosts. It also uses protocols such as RDP and SMB to move laterally within the network.

Encryption

Medusa ransomware employs asymmetric RSA encryption to encode targeted files and directories, which also contain a copy of Medusa's ransom note. Encrypted files typically have extensions such as **.medusa** or **.mylock**. Extensions associated with executable programs, dependencies, or shortcuts such as **.exe**, **.dll**, or **.lnk** are generally excluded from encryption to ensure that essential utilities remain operational.

Data Exfiltration

Data is exfiltrated to remote servers controlled by the attackers and used to pressurize victims into paying the ransom.



```
YOU should be AWARE!
------------------------------------------------------------
If you're not in main chile office, inform your supervisors and stay calm!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!


If you do not contact us within 3 days, We will start publish your case to our official blog and everybody will start notice your incident!
If you do not contact us within 5 days, We will start publish your case and leak video on all social channels and send emails to your customers!
-------------------[ Official blog tor address ]-------------------
Using TOR Browser(https://www.torproject.org/download/):

http://medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion/


CONTACT US!
---------------------[ Your company live chat address ]--------------------------
Using TOR Browser(https://www.torproject.org/download/):

http://medusakxxtp3uo7vusntvubnytaph4d3amxivbggl3hnhpk2nmus34yd.onion/[snip]

Or Use Tox Chat Program(https://qtox.github.io/)
Add user with our tox ID and wait 24h : 4AE245548F2A225882951FB14E9BF87EE01A0C10AE159B99D1EA62620D91A372205227254A9F

Our support email: ( medusa.support@onionmail.org )

Company identification hash:
[snip]
```

Image representing ransomware note of Medusa

Impact

In the final phase of the attack, Medusa leaves a ransom note on the desktop typically named "**!!read_me_medusa!!.txt**," To prevent system recovery, the ransomware also deletes shadow copies and other backups, making it difficult for victims to restore their data. The group employs a combination of RSA and AES encryption to secure the ransom transactions.

Significant attacks carried out by Medusa ransomware

1. ***Exploitation of Fortinet vulnerability***
   Recent investigations revealed that Medusa ransomware has been actively exploiting **CVE-2023-48788**, a critical SQL injection vulnerability in Fortinet's FortiClient EMS software, as a primary attack vector. This vulnerability allows attackers to gain unauthorized access to vulnerable systems, serving as an entry point for launching complex ransomware attacks. Medusa leverages this flaw to infiltrate networks, execute malicious payloads, and encrypt critical data, significantly escalating the threat posed to organizations relying on unpatched versions of FortiClient EMS.
   Apart of this, Medusa ransomware was observed exploiting:
   CVE-2022-2294: Heap Buffer Overflow vulnerability in WebRTC
   CVE-2022-2295: Type Confusion vulnerability in Google Chrome V8
   CVE-2022-21999: Elevation of Privilege vulnerability in Windows
   CVE-2018-13379: Path Traversal vulnerability in Fortinet FortiOS

2. ***Toyota Financial Services breach***
   In November 2023, TFS, a subsidiary of Toyota Motor Corporation, confirmed unauthorized access to its systems in Europe and Africa, following a ransomware claim by Medusa. Security analysts pointed to a potential vulnerability in TFS's German office, linked to an unpatched Citrix Gateway endpoint, suggesting a possible exploitation. Medusa demanded an $8 million ransom, threatening to leak allegedly stolen data. The ransom note provided Toyota with a 10-day deadline, with an option to extend it for $10,000 per day.
   To validate their breach, the attackers released sample data, including financial documents, spreadsheets, hashed account passwords, and internal organization charts.
3. ***Minneapolis Public School (MPS) District Attack***
   In February 2023, Medusa ransomware not only encrypted data but also exfiltrated approximately 100 GB of sensitive information from the Minneapolis Public School (MPS) District. This included highly confidential details about students and staff, which the group later leaked online. Despite a $1 million ransom demand, MPS refused to pay, claiming they had successfully restored their systems using backups. Instead of using a traditional dark web leak site, Medusa published the stolen data on a public website, and social media further amplified the exposure of this information.
4. ***Philippine Health Insurance Corporation (PhilHealth***)
   In September 2023, Medusa exfiltrated nearly 750 GB of sensitive data from PhilHealth, a Philippine government health insurance agency. The stolen data included information on millions of members. The ransomware group demanded a $300,000 ransom and made the stolen data available on the dark web. PhilHealth revealed that it was unprotected by antivirus software at the time of the attack due to an expired license. The renewal process had been delayed due to government procurement procedures. Despite the breach, PhilHealth was able to recover its systems and restore public-facing applications within a month.

MITRE ATT&CK TACTICS AND TECHNIQUES

Table representing technique and tactics employed by Medusa ransomware:

ID	Technique	Comments
T1078	Valid accounts	Medusa ransomware utilizes stolen credentials, typically acquired through vulnerabilities or credential dumping, to gain unauthorized access.
T1190	Exploit Public-facing application	Medusa ransomware targets vulnerabilities in unpatched servers or gateways to gain initial access.

T1566	Phishing	Medusa ransomware often uses Phishing to deliver malicious payloads to its victims.
T1047	Windows management instrumentation	Medusa ransomware uses Windows Management Instrumentation (WMI) to execute malicious commands and payloads.
T1059.001	PowerShell	Medusa ransomware often uses PowerShell to execute malicious commands on compromised systems.
T1059.003	Windows Command Shell	Medusa ransomware also uses the Windows Command Shell (cmd.exe) to run malicious scripts and commands on compromised systems.
T1036.007	Double File extension	Medusa ransomware disguises malicious files with deceptive file extensions.
T1070.004	File deletion	Medusa ransomware deletes or modifies those files that could leave evidence of its presence on a compromised system.
T1083	File and directory discovery	Medusa ransomware scans the victim's system for valuable files and directories, identifying key data to encrypt or exfiltrate.
T1210	Exploitation of Remote Services	Medusa ransomware spreads laterally within a network by exploiting vulnerabilities in remote services like RDP or web applications.
T1489	Service Stop	Medusa ransomware terminates critical services, such as security tools and backup processes, to disable defenses and hinder recovery efforts.
T1486	Data encrypted for impact	Medusa ransomware encrypts data on targets systems to disrupt access to system and network resources.
T1485	Data destruction	Medusa ransomware deletes or corrupts the files to prevent victims from restoring their data without paying the ransom.
T1490	Inhibit system recovery	Medusa ransomware removes volume shadow copies from Windows systems.

Defense mechanisms

1. **Implementing Multi-Factor Authentication**
   Using strong passwords and enabling multi-factor authentication (MFA) protects against Medusa ransomware by minimizing the risk of unauthorized access via compromised or weak credentials. Strong passwords reduce the likelihood of successful brute-force attacks, while MFA adds an extra layer of security, ensuring that even if credentials are stolen, attackers cannot easily access the system without the additional authentication factor.
2. **Audit User Accounts**
   Eliminating inactive and unused user accounts, combined with auditing administrative privileges, mitigates Medusa ransomware risks by reducing the attack surface and potential entry points. This approach minimizes credential theft risks and ensures that only necessary access is granted, limiting opportunities for privilege escalation.
3. **Use of updated software**
   Keeping software updated is crucial to avoid vulnerabilities that ransomware like Medusa can exploit. Regular updates apply the latest security patches, protecting against evolving threats and reducing the risk of exploitation.
4. **Scheduling regular backups**
   Scheduling regular backups helps to mitigate the risk of Medusa ransomware by ensuring that critical data is consistently saved and can be restored in case of an attack. Frequent backups minimize the impact of data encryption, allowing recovery without paying ransom.
5. **Anti-Ransomware Solutions**
   The data encryption and exfiltration activities associated with ransomware attacks are distinctive and serve as clear indicators of such threats. Anti-ransomware solutions can leverage these behavioral patterns, among other factors, to detect, block, and remediate infections caused by Medusa ransomware.

Sources Cited: