

HiveForce Labs

THREAT ADVISORY

**ATTACK REPORT**

Medusa Ransomware: A High-Stakes Game of Digital Hostage

Date of Publication

March 14, 2025

Admiralty Code

A1

TA Number

TA2025078

Summary

First Seen: June 2021

Malware: Medusa Ransomware

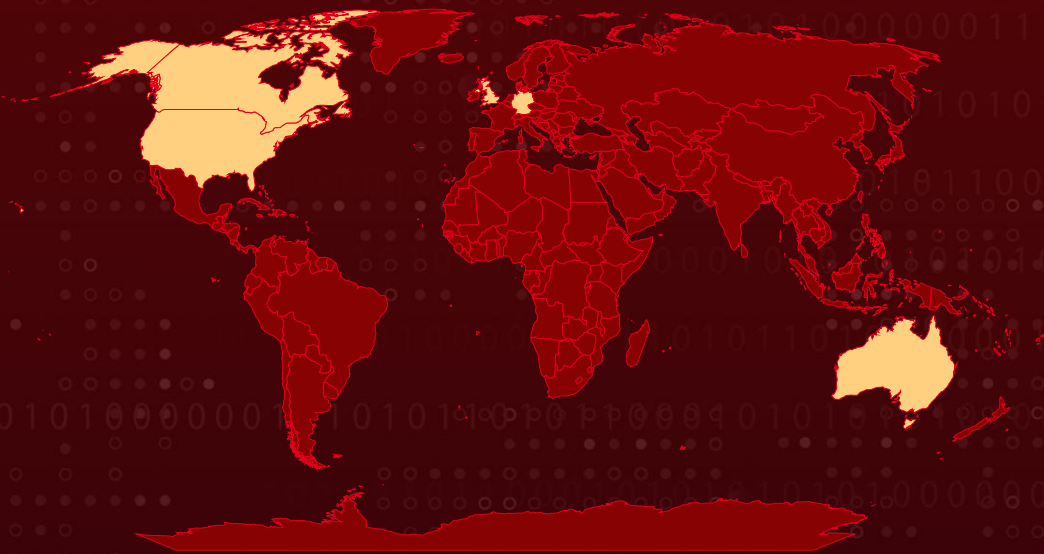
Targeted Industries: Critical Infrastructure, Medical, Education, Legal, Insurance, Technology, Manufacturing, Media, Retail, Business Services & Consulting, Healthcare, Transportation, Government, Energy, Food Service, Charitable Organizations, Aviation, Financial Services

Targeted Countries: United Kingdom, United States, Australia, Canada, Germany

Ransom: \$100,000 - \$15 million

Attack: Medusa ransomware has rapidly evolved into a relentless cyber threat, striking with increasing intensity and leaving hundreds of victims in its wake. Operating as a ransomware-as-a-service (RaaS), it lures cybercriminals with lucrative payouts and employs stealthy infiltration tactics to breach organizations worldwide. With ransom demands, dark web auctions, and aggressive follow-ups, Medusa is more than just malware; it's a high-stakes digital predator tightening its grip on the cyber underworld.




🗡️ Attack Regions



⚙️ CVEs

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	❌	✅	✅

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClientEMS			

Attack Details

#1

First surfacing in June 2021, [Medusa ransomware](#) has evolved into a formidable ransomware-as-a-service (RaaS) operation, striking with increasing intensity. Between 2023 and 2024, Medusa attacks surged by 42%, and by early 2025, the onslaught had nearly doubled compared to the same period the previous year. By February 2025, Medusa's operators and affiliates had claimed over 300 victims across diverse industries, leaving a trail of disruption in their wake.

#2

Fueling this rapid expansion is Medusa's calculated recruitment of initial access brokers (IABs) from cybercriminal forums and underground marketplaces. These affiliates, enticed by **payouts ranging from \$100 to \$1 million**, are offered the opportunity to work exclusively for Medusa. Leveraging well-worn attack vectors, they infiltrate victims' networks primarily through phishing campaigns and by exploiting unpatched vulnerabilities—most notably, the **ScreenConnect flaw (CVE-2024-1709)** and the **Fortinet EMS SQL injection vulnerability (CVE-2023-48788)**.

#3

Medusa actors deploy a mix of legitimate tools to navigate compromised environments unnoticed. Advanced IP Scanner and SoftPerfect Network Scanner aid them in mapping users, systems, and networks, allowing them to deepen their foothold before unleashing the ransomware.

#4

Medusa's business model hinges on a ruthless double extortion strategy. Victims are forced to pay not only for decryption but also to prevent their stolen data from being publicly leaked. The ransom note grants them 48 hours to respond via a Tor-based live chat or Tox, an encrypted messaging platform.

#5

If they remain silent, Medusa actors escalate, contacting them directly via phone or email. Meanwhile, Medusa's dark web leak site publicly lists victims sets countdowns to data exposure and simultaneously offers the stolen information for sale. Those desperate to delay disclosure can pay an additional \$10,000 in cryptocurrency to extend the countdown by a single day a costly reprieve in an already dire situation.

Recommendations



Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.



Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.



Patch and Update Software Regularly: Apply security patches immediately, particularly for known vulnerabilities such as CVE-2024-1709 (ScreenConnect) and CVE-2023-48788 (Fortinet EMS SQL injection). Automate patch management to ensure no critical updates are missed.



Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.



Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0005</u> Defense Evasion
<u>TA0006</u> Credential Access	<u>TA0007</u> Discovery	<u>TA0008</u> Lateral Movement	<u>TA0010</u> Exfiltration
<u>TA0011</u> Command and Control	<u>TA0040</u> Impact	<u>T1190</u> Exploit Public-Facing Application	<u>T1566</u> Phishing

<u>T1070.003</u> Clear Command History	<u>T1027.013</u> Encrypted/Encoded File	<u>T1027</u> Obfuscated Files or Information	<u>T1070</u> Indicator Removal
<u>T1562.001</u> Disable or Modify Tools	<u>T1046</u> Network Service Discovery	<u>T1083</u> File and Directory Discovery	<u>T1135</u> Network Share Discovery
<u>T1016</u> System Network Configuration Discovery	<u>T1082</u> System Information Discovery	<u>T1069.002</u> Domain Groups	<u>T1003.001</u> LSASS Memory
<u>T1059.001</u> PowerShell	<u>T1059.003</u> Windows Command Shell	<u>T1072</u> Software Deployment Tools	<u>T1021.001</u> Remote Desktop Protocol
<u>T1569.002</u> Service Execution	<u>T1047</u> Windows Management Instrumentation	<u>T1567.002</u> Exfiltration to Cloud Storage	<u>T1105</u> Ingress Tool Transfer
<u>T1071.001</u> Web Protocols	<u>T1219</u> Remote Access Software	<u>T1136.002</u> Domain Account	<u>T1486</u> Data Encrypted for Impact
<u>T1490</u> Inhibit System Recovery	<u>T1657</u> Financial Theft	<u>T1529</u> System Shutdown/Reboot	<u>T1489</u> Service Stop

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
Email	key[.]medusa[.]serviceteam[.]protonmail[.]com, medusa[.]support[.]onionmail[.]org, mds[.]svt[.]breach[.]protonmail[.]com, mds[.]svt[.]mir2[.]protonmail[.]com, MedusaSupport[.]cock[.]li
File Name	!!!READ_ME_MEDUSA!!!.txt, openrdp.bat, pu.exe
MD5	44370f5c977e415981febf7dbb87a85c, 80d852cd199ac923205b61658a9ec5bc

TYPE	VALUE
<p>SHA256</p>	<p>c28fa95a5d151d9e1d7642915ec5a727a2438477cae0f26f0557b468800111f9, 622b9c7a39c3f0bf4712506dc53330cdde37e842b97f1d12c97101cfe54bebd4, ae312393ef8e7c4a813a0ed8d4dd9e6a85b00303eb070eb15133797f41e99d90, dbe480495be5abc23437b5e916fa0368c617e4dbd58d9ed7ea303b102a6dc3b1, 16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eedb777a3ffefa99c97f0, b1553dfce1da93fd2dedb0755230ce4e21d4cb78cfc369de29d29d04db1fe013, 5f9d864d11c79b34c4502edba7d0e007197d0df086a6fb9d6bfda84a1771ff0f, b7703a59c39a0d2f7ef6422945aaeaf061431af0533557246397551b8eed505, df6cb5199c272c491b3a7ac44df6c4c279d23f7c09daed758c831b26732a4851, 9632d7e4a87ec12fdd05ed3532f7564526016b78972b2cd49a610354d672523c, 55e4ce3fe726043070ecd7de5a74b2459ea8bed19ef2a36ce7884b2ab0863047, 7f2f3e90863de8f753169fdc107df72c0ba95826de848a2d5f753f9f58a35fb4, f5acae25462bee1c2120fa53c33126792d0747cb93105b475f1dc15ae95d86f8, 16c7497fc7b31936c1ecb845d2e61ef30935c1bba3074ac66a7329d7d134cbb1, bf3b4762b518c4682cb06fe5848e7cf3cc515fca1c367f82c8d69a847ac1a0a1, e61b3377065034c79f2ac9c5593f117182a5a7a0d572f8ea8b7e6b10e10bb431, ae8553ec071675f372e0666fb73655e15119ebe705a518293373acc4589fa2da, c005dda544098874b1f923c835c9183d1ad4f601b2e9a29b1afa02ae3061e5d4, c9e05b08731892295a0842f7d17be0747c16226fcb75fa4a23b43b61a833c8cf, 583940ab94608408294e344af4503c8caed96966a08165c58cdc4faa03ab52a9, dfdb6d5ef505a0d4cabbcd97e142106ecab9604d0086d77c9431e2fb09088eb6, c6ac5a83942a8aa3954650dfaa343a4bc4d3cff81c771ec0bb60bf1d2208c4e1,</p>

TYPE	VALUE
SHA256	3a7f64223a51e35a8253804c42d0ba92b663e06da8c21d398a6507 4b8e50beec, 9d5616672189557f171cae0f122853f3498bc9160ee92f3844404d4 6ec45210a, dd0e796f52fc1fcad488df122db8f5fcc9423ffdd3b5edbccc66d6055ab 8a2247, 6106d1ce671b92d522144fcd3bc01276a975fe5d5b0fde09ca1cca16 d09b7143, 3770c122f3f289cea730a5d1d16978e7f354686d3d2d4f667cfd9e37 d5e9d368, 038fb5e0ba6c35e3ee2f56b5bd926109e8b321bd0c9e3b75948931 2518efea65, 1b7add5adbb9ba5b85437c11825e47663bd59729442f6f44fb2576b 25945f0eb, e0b562b70b9fed98a05680a613f786bd482f71456976c7290ca2059 004cb64a5, e7cad51c71403c229364147d66ef1858065b10645d1d09774cd9a9 1dd8e54717, ad3ec38f79b4964fc9ba0d8f2d9d28c7cd3bd20dee0e3acf427eabb5 dc819275, 7c340e4d69ac5221bbebcad320814929c1bc376c4d9a64e5daf70c1 91137fd4a, 01b91c60866b22b22d82284cbaac35565818eba353ac834018971d 180a790a77, f365ca957e733714691f4ac19f136b33442269816e71cab84c3ce0b 319084cc2, 7880968b0020947d5d13fac826e49c70b5a9421e3d6546a3466380 3a411b97ff, 77a96b9bcc2bdcbc5c5cd39d606b8b14112e04390c04e4c9a7570a8 bbca32ed2, 0b3b9076591240a9639929a1a5a78922b5db0af3dba2e782d595ec c139ffb7e1, 53e5c44c1f47895004d61d18cbc74e83d7118dfcb2eb073c1e9c6a3 7abf38bd9, 3be651fe6619e62e483ff8d46e49c3578e7ce9d60b6d2b31d8d3e32 beeeabec, 08f05c597ac7c8e35515a63a9e139ef75b44d92093ed8c5b1b3c064 f9c7f6cb8, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f049 1e3161eb, d5a1f90dc5c9717b3f900c91a6cdccc20e56e6f1d20f24170189260e 8dde7608, 8dff18f10c857dd3eeb5511f5724da0ab1d9e411044aea27f6de23ee 33f798c8, 276024580b5bc903656a1c12a7ec02daccb10e6e6bdf6872765c9a6 7f1cd6da5

Recent Breaches

<https://www.cpi-print.co.uk/>
<https://www.srpcompanies.com/>
<https://cmsonline.com/>
<https://bellsambulace.com/>
<https://www.kablefulfillment.com/>
<https://www.auroragov.org/>
<https://www.friendshipousede.org/>
<https://www.laurens56.k12.sc.us/>
<https://www.mundeleinparks.org/>
<https://auroraboardworks.com/>
<https://www.heartlandhealthcenter.org/>
<https://martinenergygroup.com/>
<https://www.gateshead.gov.uk/>
<https://bentonil.com/>
<https://www.hcrgcaregroup.com/>
<https://www.robinson-dentistry.com/>
<https://www.cragercpa.com/>
<https://jpex.com.bd/>
<https://cdh.idaho.gov/>
<https://cachevalleyent.com/>
<https://www.braums.com/>
<https://www.paightonzoo.org.uk/>
<https://naturesorganics.com.au/>
<https://medescollege.ca/en/>
<https://www.greenwichmedicalspa.com/>
<https://www.brockwayhairdesign.com/>
<https://serenityplano.com/>
<https://trueworldfoods.com/>
<https://michaelshairbodymind.com/>
<https://aviation-technics.com/>
<https://www.hayter.co.uk/>
<https://www.simonmed.com/>
<https://rhsctn.com/>
<https://glowspaseattle.com/>
<https://www.grailsprings.com/>

Patch Details

Upgrade to **ConnectWise ScreenConnect version 23.9.8 or later**, as license restrictions have been removed, allowing all partners to proceed with the update.

Download here:

<https://screenconnect.connectwise.com/download>

For Fortinet FortiClientEMS, apply the following patches:

- Upgrade to version **7.2.3 or higher** for FortiClientEMS 7.2
- Upgrade to version **7.0.11 or higher** for FortiClientEMS 7.0

More details are available at:

<https://fortiguard.fortinet.com/psirt/FG-IR-24-007>

References

<https://www.cisa.gov/sites/default/files/2025-03/aa25-071a-stopransomware-medusa-ransomware.pdf>

<https://www.security.com/threat-intelligence/medusa-ransomware-attacks>

<https://hivepro.com/threat-advisory/medusa-ransomware-unleashed-a-growing-cybersecurity-menace/>

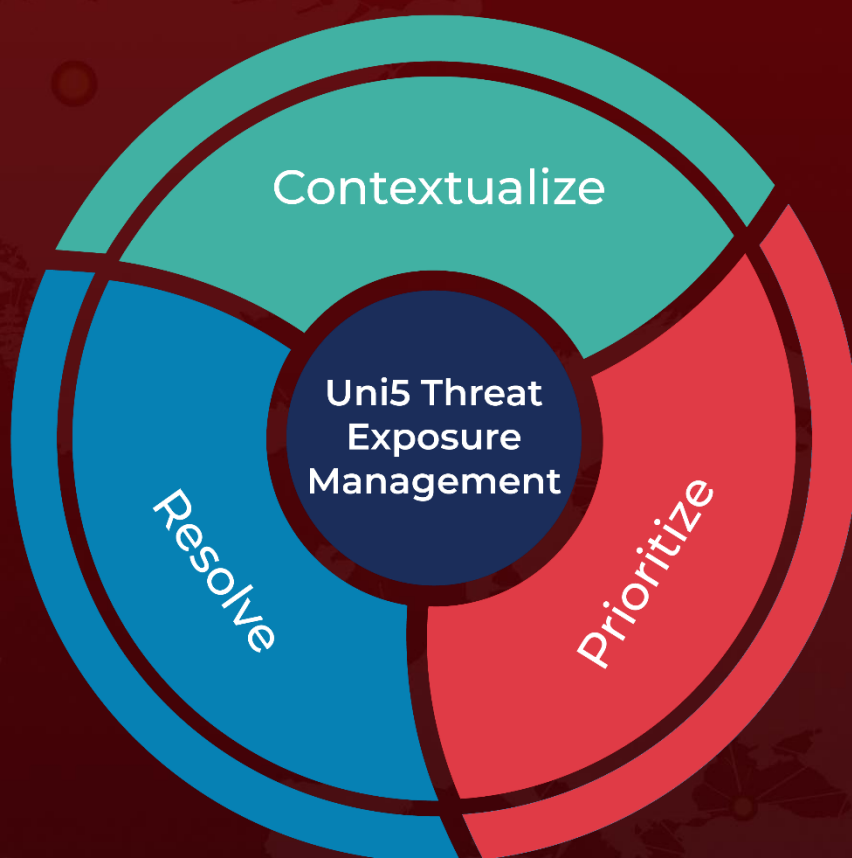
<https://hivepro.com/threat-advisory/critical-vulnerabilities-in-screenconnect-under-active-exploitation/>

<https://hivepro.com/threat-advisory/fortinet-releases-patches-for-critical-vulnerabilities-in-various-products/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

March 14, 2025 • 1:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com