Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

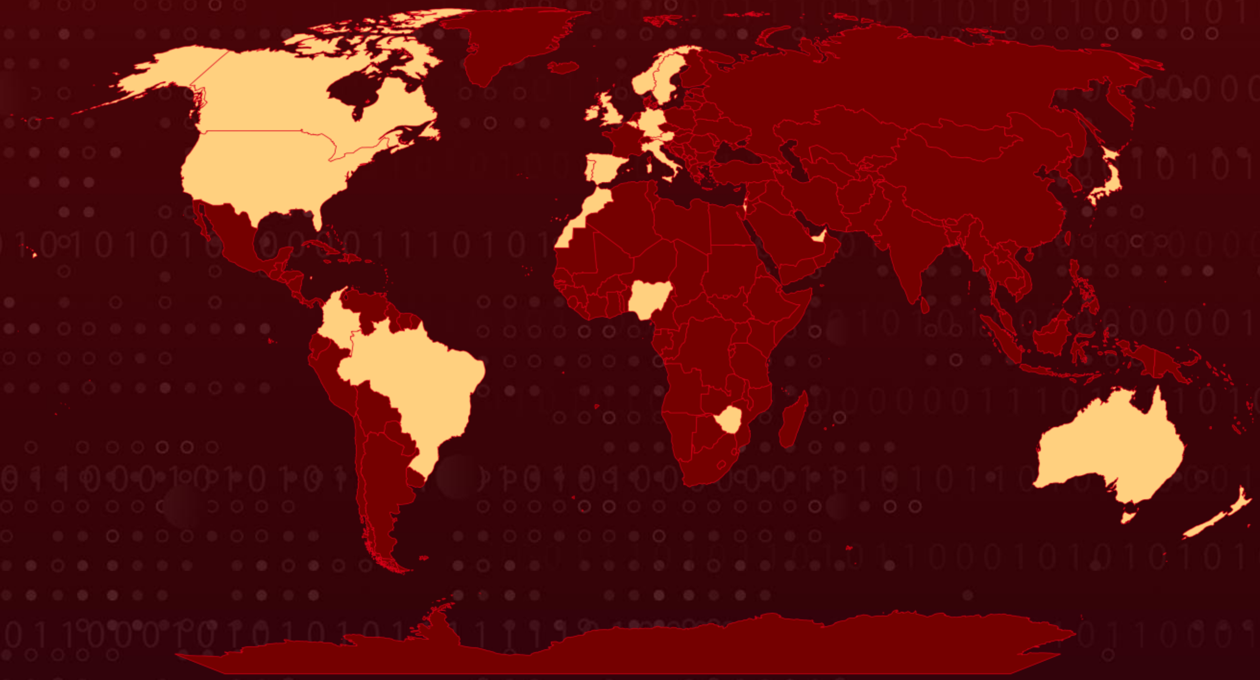
Meow Ransomware Resurfaces with an Extortion-Centric Model

Date of Publication	Admiralty Code	TA Number
September 4, 2024	A1	TA2024339

Summary

First Seen: August 2022
Malware: Meow Ransomware (alias MeowCorp, MeowLeaks)
Targeted Countries: Australia, Austria, Belgium, Brazil, Canada, Colombia, Germany, Ireland, Israel, Italy, Japan, Morocco, New Zealand, Nigeria, Norway, Portugal, Singapore, South America, Spain, Sweden, United Arab Emirates, United Kingdom, United States, Zimbabwe
Ransom Demand: $199 - $500,000
Targeted Industries: Aerospace, Aviation, Banking, Business Services & Consulting, Dairy Industry, Defense, Education, Energy, Financial Services, Food & Beverage, Government, Healthcare, Hospitality, Information Technology, Insurance, Legal, Manufacturing, Oil & Gas, Pharmaceutical, Professional Services, Retail, Technology, Transportation
Attack: In late 2022, the Meow ransomware variant emerged, originating from the leak of Conti's ransomware strain. Despite a temporary halt following the release of a free decryptor in March 2023, Meow resurfaced in 2024, swiftly claiming new victims. It is suspected that the latest version may now operate primarily as an extortion group.

Attack Regions



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

Attack Details

#1 In late 2022, following the leak of Conti's ransomware strain, a variant known as Meow ransomware emerged. This crypto-ransomware was first detected in late August, continued its activities through mid-September 2022, and persisted until February 2023. By March 2023, a free decryptor for Meow ransomware became available, effectively ending its operations.

#2 However, Meow resurfaced in 2024, demonstrating a swift return with 62 victims reported this year. The latest version of Meow ransomware may now be functioning solely as an extortion group, assuming it is the same entity. Meow utilizes the ChaCha20 encryption algorithm to compromise data on targeted servers.

#3 Although their list of targeted countries is limited, the majority of their victims are based in the United States. They likely focus on organizations holding sensitive information, as encryption alone may no longer suffice to coerce ransom payments. Frequently targeted sectors include healthcare, oilfield services, and medical.

#4 Meow ransomware spreads via multiple attack vectors, including unsecured Remote Desktop Protocol (RDP) configurations, email spam containing malicious attachments, deceptive downloads, botnets, exploits, malvertising, web injections, fake updates, and infected software installers.

#5 Once deployed, the ransomware encrypts various file types, appending ".MEOW" as the file extension. The attackers prefer victims to communicate through email or Telegram, with contact information provided in the ransom note titled "readme.txt."

#6 Notably, Meow's evolution suggests a potential shift toward an extortion-centric model, where attackers threaten to publicly release stolen sensitive data to pressure victims into paying ransoms. This change reflects a strategic pivot from traditional encryption-based ransomware attacks to more complex cyber extortion schemes.

Recommendations

Secure RDP and Email Protocols: Disable or tightly secure Remote Desktop Protocol (RDP) configurations and implement anti-spam measures to block email attachments containing malicious payloads.

Vendor and Third-Party Risk Management: Regularly assess the security posture of third-party vendors, especially those with access to your sensitive data, to ensure they comply with stringent security standards. Require vendors to undergo regular security audits and maintain adherence to best security practices, mitigating risks associated with supply chain attacks.

Honeyfiles and Honeypots: Deploy deception technology employing honeyfiles (fake sensitive documents) and honeypots to detect ransomware activity early. These files can lure attackers and trigger alarms when accessed, helping to identify and respond to Meow ransomware attempts before they escalate.

Utilize Open-Source Exploit Tools: Incorporate tools like RansomLord, which automate the creation of PE files to exploit vulnerabilities in ransomware. This tool helps identify and exploit weaknesses in ransomware code, potentially neutralizing threats like Meow ransomware.

Track Outbound Traffic: Monitor outbound network traffic for unusual spikes that may indicate data exfiltration. Configure IDS/IPS systems to send alerts when unusual outbound traffic occurs, especially to external IP addresses or suspicious domains. Establish thresholds for normal outbound data flows, and trigger alerts when traffic exceeds these thresholds, particularly during non-business hours.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1071 Application Layer Protocol	T1573 Encrypted Channel
T1190 Exploit Public-Facing Application	T1133 External Remote Services	T1566 Phishing	T1129 Shared Modules
T1027 Obfuscated Files or Information	T1027.005 Indicator Removal from Tools	T1036 Masquerading	T1041 Exfiltration Over C2 Channel

T1056 Input Capture	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1497 Virtualization/Sandbox Evasion	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1080** Taint Shared Content
T1486 Data Encrypted for Impact	**T1021.001** Remote Desktop Protocol	**T1189** Drive-by Compromise	**T1204.002** Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9, 7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f, 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099, 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f, 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec
SHA1	59e756e0da6a82a0f9046a3538d507c75eb95252, 987ad5aa6aee86f474fb9313334e6c9718d68daf, 94a9da09da3151f306ab8a5b00f60a38b077d594, 5949c404aee552fc8ce29e3bf77bd08e54d37c59, 578b1b0f46491b9d39d21f2103cb437bc2d71cac, 4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b
MD5	8f154ca4a8ee50dc448181afbc95cfd7, 4dd2b61e0ccf633e008359ad989de2ed, 3eff7826b6eea73b0206f11d08073a68, 1d70020ddf6f29638b22887947dd5b9c, 033acf3b0f699a39becdc71d3e2dddcc, 0bbb9b0d573a9c6027ca7e0b1f5478bf
TOR Address	meow6xanhzfci2gbkn3lmbqq7xjjufskkdfocqdngt3ltvzgqpsg5mid[.]onion, totos7fquprkecvcsl2jwy72v32glgkp2ejeqlnx5ynnxvbebgnletqd[.]onion

Recent Breaches

https://iccesar.com
https://nobi.as
https://doncoandsons.com
https://grupomodestocerqueira.com
https://caseificioaltavalsesia.com
https://specialoilfieldservices.com
https://successmicrofinancebank.com
https://yshilat.com
https://diamcad.com
https://modulkit.com
https://finlogic.it
https://woden.com
https://wt-gruber.de
https://artesaniachopo.com
https://barkalfood.com
https://vanslumberandcustombuilders.com
https://completepayrollsolutions.com
https://allparksinsurance.com
https://optimizeegs.com
https://southamericantours.com
https://burnsindustrialequipment.com
https://certifiedtransmission.com
https://lennartsfors.com
https://rostanceedwards.com
https://zyduspharmaceuticals.com
https://ezup.com
https://americancontractsystems.com
https://aerotechsolutions.com
https://safefood.com
https://gastonfence.com
https://elementfoodsolutions.com
https://huduser.gov
https://kla.com
https://fatboycellular.com
https://banxsystems.com

References

https://socradar.io/dark-web-profile-meow-ransomware/

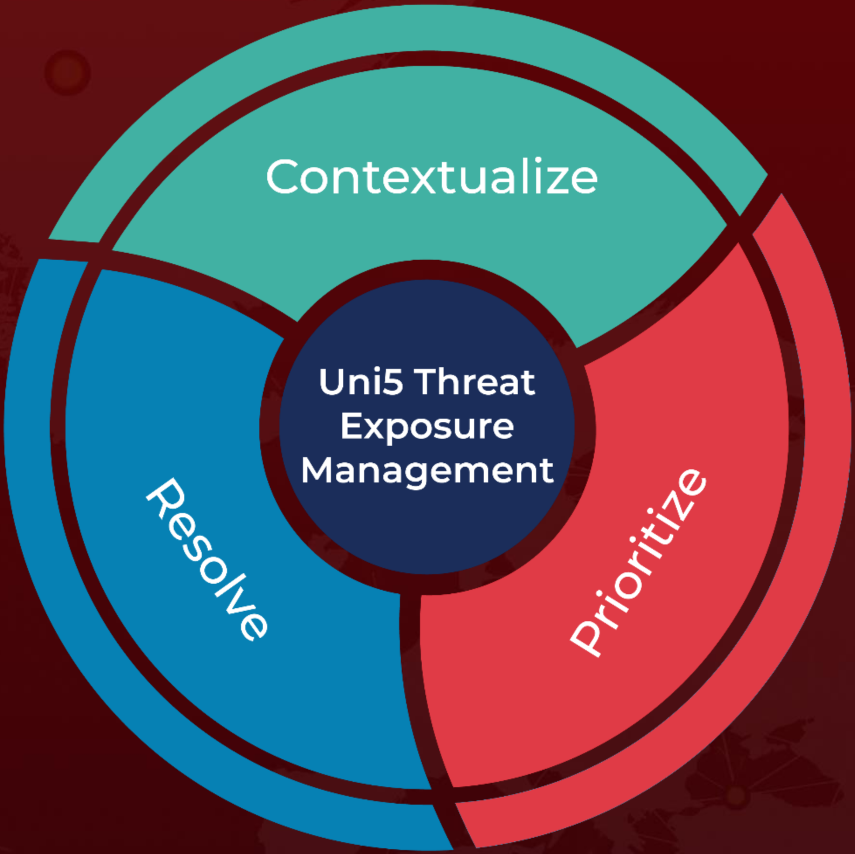
https://hivepro.com/threat-advisory/new-ransomware-variants-created-using-leaked-conti-source-code/

https://github.com/malvuln/RansomLord

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

September 4, 2024 • 11:30 PM

More at www.hivepro.com