Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

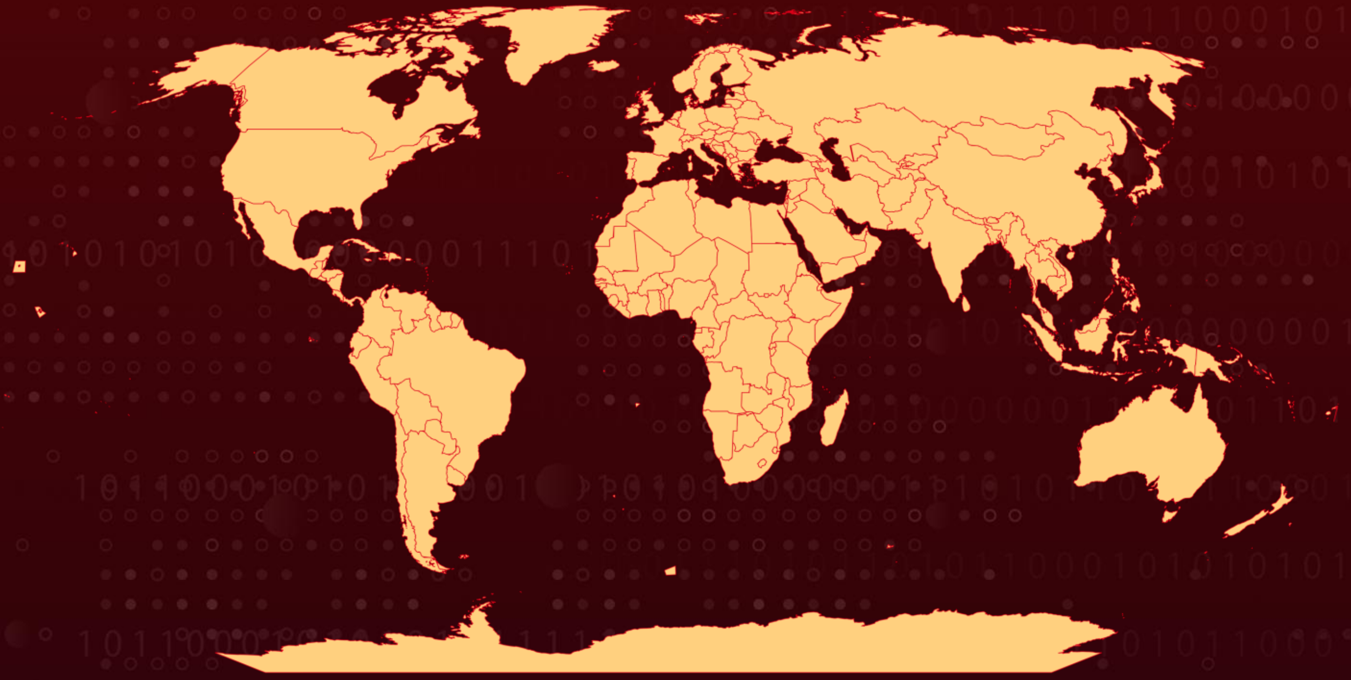
Medusa Ransomware Unleashed A Growing Cybersecurity Menace

Date of Publication	Admiralty Code	TA Number
January 12, 2024	A1	TA2024014

Summary

Attack Began: 2022
Attack Region: Worldwide
Malware: Medusa Ransomware
Affected Platform: Windows
Targeted Industries: Technology, Education, Manufacturing, Healthcare, Wholesale and Retail, Professional and Legal Services, Construction, Hospitality, Media & Entertainment, Nonprofit, Agriculture, Transportation and Logistics, Insurance, Mining, State and Local Government, Financial Services, Telecommunications, Pharma and Life Sciences, Federal Government, Real Estate
Attack: Medusa ransomware, a potent threat since late 2022, employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non-compliant organizations. Operating as a ransomware-as-a-service, Medusa's global impact underscores the need for proactive cybersecurity measures to counter its evolving tactics.

Attack Regions



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

Attack Details

#1 Medusa ransomware, emerging as a significant threat in late 2022, gained notoriety in 2023 for its multifaceted extortion tactics. Operating as a ransomware-as-a-service (RaaS) platform, Medusa primarily targets Windows environments.

#2 The group utilizes a dedicated leak site called the Medusa Blog to publicly disclose sensitive data from organizations unwilling to comply with ransom demands. Their approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.

#3 Medusa's impact is widespread, affecting 74 organizations globally across diverse sectors, with a focus on high technology, education, and manufacturing. The ransomware group demonstrates an international footprint, with the United States being a major target, followed by Europe and isolated incidents in other regions.

#4 Medusa’s gains initial access through exploiting vulnerable services, defense evasion with kernel drivers, and reconnaissance using tools like Netscan. Medusa's unique approach involves the use of a leak site, videos showcasing compromised organizations, and a Telegram channel for publicizing and releasing exfiltrated data. The group's ransom demands are accompanied by a countdown, visitor count, and victim details.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Conduct Regular Data Backups and Test Restoration: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups.

Enhance Endpoint Security: Employ reputable antivirus and anti-malware solutions to detect and block known malware signatures. Regularly update and patch operating systems and software to address vulnerabilities that threat actors may exploit.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0008 Lateral Movement
TA0010 Exfiltration	TA0042 Resource Development	TA0043 Reconnaissance	TA0007 Discovery
TA0040 Impact	T1007 System Service Discovery	T1106 Native API	T1059 Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	T1059.007 JavaScript	T1588.006 Vulnerabilities	T1659 Content Injection
T1059.001 PowerShell	T1027 Obfuscated Files or Information	T1485 Data Destruction	T1588.005 Exploits
T1070.004 File Deletion	T1070 Indicator Removal	T1047 Windows Management Instrumentation	T1021.004 SSH
T1021 Remote Services	T1059.005 Visual Basic	T1588 Obtain Capabilities	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270

Recent Breaches

https://www.limburg
https://www.waterforpeople.org
https://www.biomatrix.com
https://www.atcoproducts.com
https://www.gusd.net
https://www.hinsdale.k12.il.us
https://www.sagent.com
https://www.campbell.kyschools.us
https://www.acculab.com

References

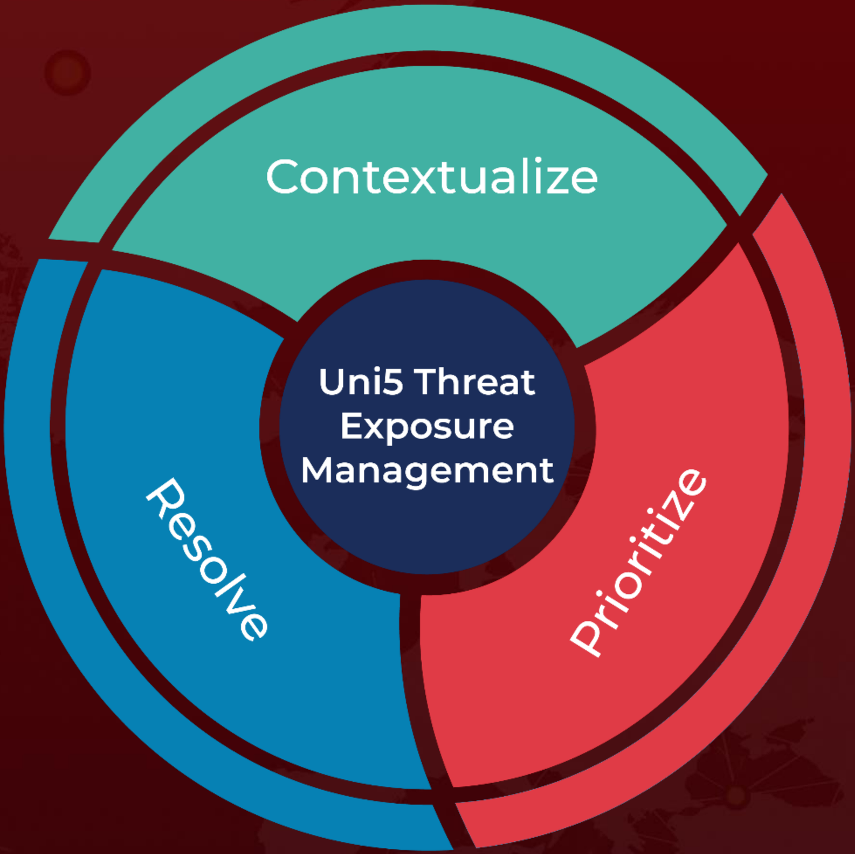
https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/

https://twitter.com/FalconFeedsio/status/1745460559292866589

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

January 12, 2024 • 6:30 AM

More at www.hivepro.com