Hive Pro

Threat Level

Red

CISA: AA24-242A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

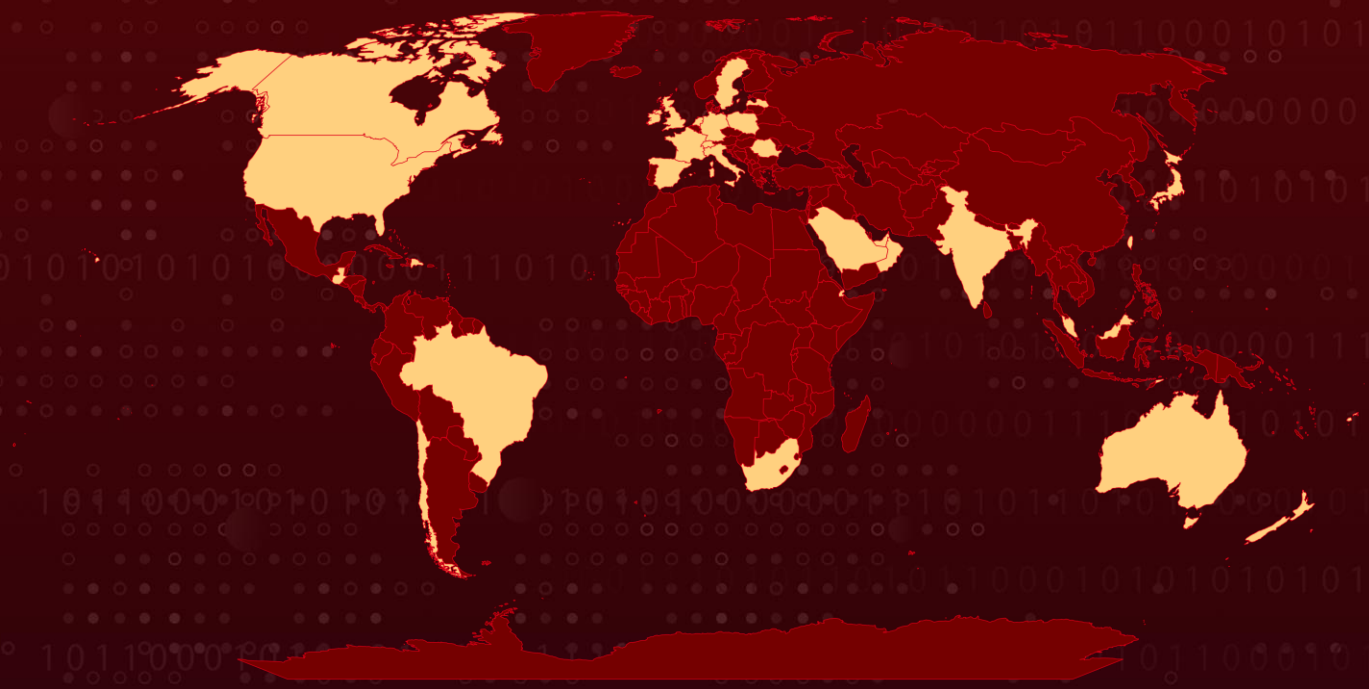
RansomHub: The RaaS Powerhouse Exploiting 200+ Victims

Date of Publication	Admiralty Code	TA Number
September 6, 2024	A1	TA2024343

Summary

First Seen: February 2024
Malware: RansomHub Ransomware
Targeted Countries: Australia, Bahrain, Brazil, Canada, Chile, Djibouti, Dominican Republic, Fiji, France, Germany, Guatemala, India, Ireland, Italy, Japan, Latvia, Malaysia, Netherlands, New Zealand, Northern Ireland, Oman, Poland, Romania, Saudi Arabia, South Africa, Spain, Sweden, Switzerland, Taiwan, Timor-Leste, United Arab Emirates, United Kingdom, United States
Targeted Industries: Agriculture, Business Services & Consulting, Non-Profit, Commercial Facilities, Critical Infrastructure, Education, Emergency Services, Energy, Financial Services, Food and Beverages, Government, Healthcare, Hospitality, IT, Legal, Manufacturing, Real Estate, Retail, Technology, Telecommunications, Transportation, Utility
Attack: RansomHub, a ransomware-as-a-service (RaaS) platform, has rapidly gained prominence in the cybercriminal landscape since February 2024. Responsible for targeting over 200 victims across various industries, RansomHub's affiliates employ a 'double extortion' tactic, encrypting and exfiltrating sensitive data to pressure victims into paying a ransom.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN	✓	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	✗	✓	✓
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Atlassian Confluence Data Center and Server	✓	✓	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✗	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS	✗	✓	✓
CVE-2017-0144	EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	Microsoft SMBv1	✓	✓	✓
CVE-2020-1472	Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability	Microsoft Windows	✗	✓	✓

Attack Details

#1 RansomHub, formerly known as Cyclops and Knight, is a prominent ransomware-as-a-service (RaaS) variant that has gained traction in the cybercrime ecosystem. Since February 2024, it has impacted over 200 victims across diverse industries, employing both data encryption and exfiltration.

#2 Affiliates of RansomHub, cybercrime groups using this specific RaaS platform, also employ this "double extortion". It involves encrypting a victim's data on one side and its theft on the other. The data theft enables the attacker to threaten the victim with publishing the stolen data unless the ransom is paid.

#3 Victims typically get from three to 90 days to respond with payment before data gets published on the RansomHub data leak site. Initial access to the network is gained by various tactics: phishing campaigns, abusing known vulnerabilities, and password spraying. Once in the targeted environment, affiliates perform reconnaissance via Nmap and PowerShell-based network scanning.

#4 To evade detection, they have been known to rename ransomware executables with benign-sounding names such as "Windows.exe" and disable antivirus solutions. They often leverage Mimikatz for privilege escalation and use RDP in combination with PsExec and AnyDesk for lateral movement.

#5 As for exfiltration, it will be through several means, but the most common would be via tools like WinSCP, PuTTY, and Cobalt Strike. Affiliates often delete volume shadow copies via vssadmin.exe to complicate recovery. RansomHub is also known to use legitimate software for malicious ends: using Cobalt Strike for lateral movement and Rclone for theft of data, thus mixing the malicious activity with the operation of a normal system.

Recommendations

Patch Exploited Vulnerabilities Promptly: Focus on Known Vulnerabilities. RansomHub commonly exploits unpatched, known vulnerabilities. Ensure rapid patching of critical internet-facing systems to minimize this risk.

Disable Unnecessary Services and Ports: Disable unused ports, such as RDP (Remote Desktop Protocol), which RansomHub affiliates exploit for lateral movement.

Regularly Review Domain Controllers and Active Directory: Regularly review domain controllers, servers, and Active Directory for newly created or unrecognized accounts that RansomHub affiliates may use to maintain persistence.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0008 Lateral Movement	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.005** Exploits	**T1566** Phishing	**T1190** Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1047** Windows Management Instrumentation	**T1136** Create Account

T1219 Remote Access Software	**T1098** Account Manipulation	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol
T1036 Masquerading	**T1070** Indicator Removal	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1003 OS Credential Dumping	**T1110** Brute Force	**T1110.003** Password Spraying	**T1018** Remote System Discovery
T1046 Network Service Discovery	**T1210** Exploitation of Remote Services	**T1048** Exfiltration Over Alternative Protocol	**T1048.002** Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
T1537 Transfer Data to Cloud Account	**T1048.003** Exfiltration Over Unencrypted Non-C2 Protocol	**T1486** Data Encrypted for Impact	**T1490** Inhibit System Recovery

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\crackmapexec.exe, C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\kerbrute.exe, C:\Users\%USERNAME%\Downloads\Anydesk.exe, C:\Users\%USERNAME%\Desktop\IamBatMan.exe, C:\Users\backupexec\Desktop\stealer_cli_v2.exe, C:\Users\%USERNAME%\Downloads\nmap-7.94-setup.exe, C:\Program Files (x86)\Nmap\nmap.exe, C:\Users\%USERNAME%\Downloads\mimikatz_trunk\x64\mimikatz.exe, C:\Users\backupexec\Downloads\x64\mimikatz.exe
IPv4	8[.]211[.]2[.]97, 45[.]95[.]67[.]41, 45[.]134[.]140[.]69, 45[.]135[.]232[.]2, 89[.]23[.]96[.]203, 188[.]34[.]188[.]7, 193[.]106[.]175[.]107, 193[.]124[.]125[.]78, 193[.]233[.]254[.]21

TYPE	VALUE
URLs	hxxp[:]//188[.]34[.]188[.]7/555, hxxp[:]//188[.]34[.]188[.]7/555/, hxxp[:]//188[.]34[.]188[.]7/555/amba16[.]ico, hxxp[:]//188[.]34[.]188[.]7/555/bcrypt[.]dll, hxxp[:]//188[.]34[.]188[.]7/555/CRYPTSP[.]dll, hxxp[:]//188[.]34[.]188[.]7/555/en, hxxp[:]//188[.]34[.]188[.]7/555/en-US, hxxp[:]//188[.]34[.]188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE[.]exe, hxxp[:]//188[.]34[.]188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE[.]exe[.]Config, hxxp[:]//188[.]34[.]188[][.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE[.]INI, hxxp[:]//89[.]23[.]96[.]203/, hxxp[:]//89[.]23[.]96[.]203/333, hxxp[:]//89[.]23[.]96[.]203/333/, hxxp[:]//89[.]23[.]96[.]203/333/1[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/1[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/10[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/12[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/12[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/2[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/2[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/3[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/3[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/4[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/4[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/5[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/5[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/6[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/7[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/8[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/9[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/92[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/AmbaPDF[.]ico, hxxp[:]//89[.]23[.]96[.]203/333/ambapdf[.]ico[.]DLL, hxxp[:]//89[.]23[.]96[.]203/333/bcrypt[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/Cabinet[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/CRYPTBASE[.]DLL, hxxp[:]//89[.]23[.]96[.]203/333/cryptnet[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/CRYPTSP[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/cv4TCGxUjvS[.]exe,

TYPE	VALUE
URLs	hxxp[:]//89[.]23[.]96[.]203/333/DPAPI[.]DLL, hxxp[:]//89[.]23[.]96[.]203/333/en, hxxp[:]//89[.]23[.]96[.]203/333/en/d%E5%AD%97%E5%AD%97[.]resources[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/en/d%E5%AD%97%E5%AD%97[.]resources[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/en/d%E5%AD%97%E5%AD%97[.]resources/d%E5%AD%97%E5%AD%97[.]resources[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/en/d%E5%AD%97%E5%AD%97[.]resources/d%E5%AD%97%E5%AD%97[.]resources[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/en-US, hxxp[:]//89[.]23[.]96[.]203/333/en-US/d%E5%AD%97%E5%AD%97[.]resources[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/en-US/d%E5%AD%97%E5%AD%97[.]resources[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/enUS/d%E5%AD%97%E5%AD%97[.]resources/d%E5%AD%97%E5%AD%97[.]resources[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/enUS/d%E5%AD%97%E5%AD%97[.]resources/d%E5%AD%97%E5%AD%97[.]resources[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/iertutil[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/information[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/information[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/information[.]INI, hxxp[:]//89[.]23[.]96[.]203/333/IPHLPAPI[.]DLL, hxxp[:]//89[.]23[.]96[.]203/333/mshtml[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/msi[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/SspiCli[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR[.]exe[.]Config, hxxp[:]//89[.]23[.]96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/xwenxub285p83ecrzvft[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/cv4TCGxUjvS[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/urlmon[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/USERENV[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/webio[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/winhxxp[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/WININET[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/WINMM[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/WINMMBASE[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/winnlsres[.]dll, hxxp[:]//89[.]23[.]96[.]203/333/xwenxub285p83ecrzvft[.]exe, hxxp[:]//89[.]23[.]96[.]203/333/xwenxub285p83ecrzvft[.]exe[.]Config,

TYPE	VALUE
URLs	hxxp[:]//temp[.]sh/KnCqD/superloop[.]exe, hxxps[:]//grabify[.]link/Y33YXP, hxxps[:]//i[.]ibb[.]co/2KBydfw/112882618[.]png, hxxps[:]//i[.]ibb[.]co/4g6jH2J/2773036704[.]png, hxxps[:]//i[.]ibb[.]co/b1bZBpg/2615174623[.]png, hxxps[:]//i[.]ibb[.]co/Fxhyq6t/2077411869[.]png, hxxps[:]//i[.]ibb[.]co/HK0jV1G/534475006[.]png, hxxps[:]//i[.]ibb[.]co/nbMNnW4/2501108160[.]png, hxxps[:]//i[.]ibb[.]co/p1RCtpy/2681232755[.]png, hxxps[:]//i[.]ibb[.]co/SxQLwYm/1038436121[.]png, hxxps[:]//i[.]ibb[.]co/v1bn9ZK/369210627[.]png, hxxps[:]//i[.]ibb[.]co/V3Kj1c2/1154761258[.]png, hxxps[:]//i[.]ibb[.]co/X2FR8Kz/2113791011[.]png, hxxps[:]//i[.]ibb[.]com:443/V3Kj1c2/1154761258[.]png, hxxps[:]//12301230[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]css, hxxps[:]//12301230[.]co/npm/module[.]external/jquery[.]min[.]js, hxxps[:]//12301230[.]co/npm/module[.]external/moment[.]min[.]js, hxxps[:]//12301230[.]co/npm/module[.]external/client[.]min[.]js, hxxps[:]//12301230[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]external/jquery[.]min[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]external/moment[.]min[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]external/client[.]min[.]js, hxxps[:]//samuelelena[.]co/, hxxp[:]//samuelelena[.]co/, hxxps[:]//samuelelena[.]co/npm, hxxps[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js, hxxp[:]//samuelelena[.]co/npm/, hxxp[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js, hxxp[:]//samuelelena[.]co/npm/module[.]external/client[.]min[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.], hxxps[:]//samuelelena[.]co/npm/module[.]external/jquery[.]min[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]external, hxxps[:]//samuelelena[.]co/np, hxxps[:]/samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js, hxxps[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js hxxps[:]//samuelelena[.]co/npm/module[.]external/client[.]min[.]js,

TYPE	VALUE
URLs	hxxps[:]//samuelelena[.]co/npm/module[.]external/jquery[.]min[.]js , hxxp[:]//samuelelena[.]co:443/, hxxp[:]//samuelelena[.]co/npm/module[.]external/jquery[.]min[.]js, hxxps[:]//40031[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]css, hxxps[:]//40031[.]co/npm/module[.]external/jquery[.]min[.]js, hxxps[:]//40031[.]co/npm/module[.]external/moment[.]min[.]js, hxxps[:]//40031[.]co/npm/module[.]external/client[.]min[.]js, hxxps[:]//40031[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js
Email	brahma2023[@]onionmail[.]org
TOR Address	ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
ToxID	5596A55062A4232F5AA55C2F7C4DF0AC1EAD10B78D4055A3328AD142A42B555E
SHA256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fabc14801a, 342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b, 56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763

Patch Links

https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

https://www.fortiguard.com/psirt/FG-IR-23-097

https://activemq.apache.org/security-advisories.data/CVE-2023-46604

https://www.atlassian.com/software/confluence/download-archives

https://my.f5.com/manage/s/article/K000137353

https://www.fortiguard.com/psirt/FG-IR-24-007

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0787

Recent Breaches

https://cbt-gmbh.de
https://inorde.com
https://parknfly.ca
https://towellengineering.net
https://phdservices.net
https://cps-k12.org
https://plannedparenthood.org
https://bennettcurrie.co.nz
https://galgorm.com
https://pcipa.com
https://gardenhomesmanagement.com
https://www.sanyo-av.com
https://www.amberbev.com
https://removal.ai
https://schneider.ch
https://nissan-dubai.com
https://timortelecom.tl
https://fenceauthority.com
https://iph-bet.fr
https://www.ramoncorripio.com
https://gruyeria.ch
https://iiitd.ac.in
https://grant-associates.uk.com
https://www.johnkellys.com
https://ciot.com
https://wilmingtoncc.org
https://polycohealthline.com
https://electriforce.com
https://rainierarms.com
https://www.spie-tec.de
https://smarterp.com
https://www.banhampoultry.co.uk
https://blowerdempsay.com
https://capitalfund1.com
https://inlighten.net
https://ccsdschools.com
https://gmchc.org
https://lennartsfors.com
https://www.regentcaravans.com.au
https://martinswood.herts.sch.uk
https://glasstile.com
https://allanmcneill.co.nz
https://netconfig.co.za
https://albynhousing.org.uk

https://www.manotherm.ie
https://www.patelco.org
https://nrcollecties.nl
https://atwoodcherny.com
https://osg.com
https://isnart.it
https://imobesidade.com.br
https://police.praca.gov.pl
https://ljglaw.com
https://welevelup.com
https://bedford.k12.oh.us
https://naturalcuriosities.com
https://wmwmeyer.com
https://dhcgrp.com
https://alliuminteriors.co.nz
https://rationalenterprise.com

References

https://www.cisa.gov/sites/default/files/2024-08/aa24-242a-stopransomware-ransomhub-ransomware_0.pdf

https://hivepro.com/threat-advisory/andariel-north-koreas-evolving-cyber-threat-landscape/

https://hivepro.com/threat-advisory/fortinet-releases-patch-for-pre-announced-critical-vulnerability/

https://hivepro.com/threat-advisory/atlassian-confluence-zero-day-actively-exploited-in-the-wild/

https://hivepro.com/threat-advisory/unc5174-functions-as-an-initial-access-broker-exploiting-vulnerabilities/

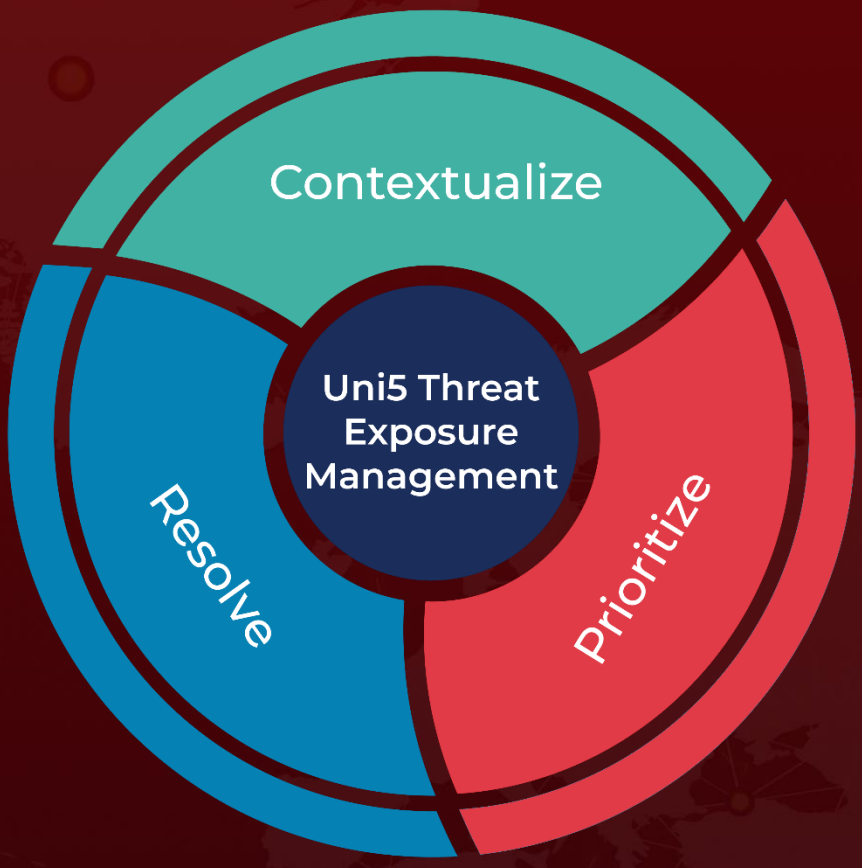
https://hivepro.com/threat-advisory/fortinet-releases-patches-for-critical-vulnerabilities-in-various-products/

https://hivepro.com/threat-advisory/ransomhub-a-rebranded-menace-exploiting-the-zerologon-vulnerability/

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 6, 2024 • 7:15 AM

More at www.hivepro.com