Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

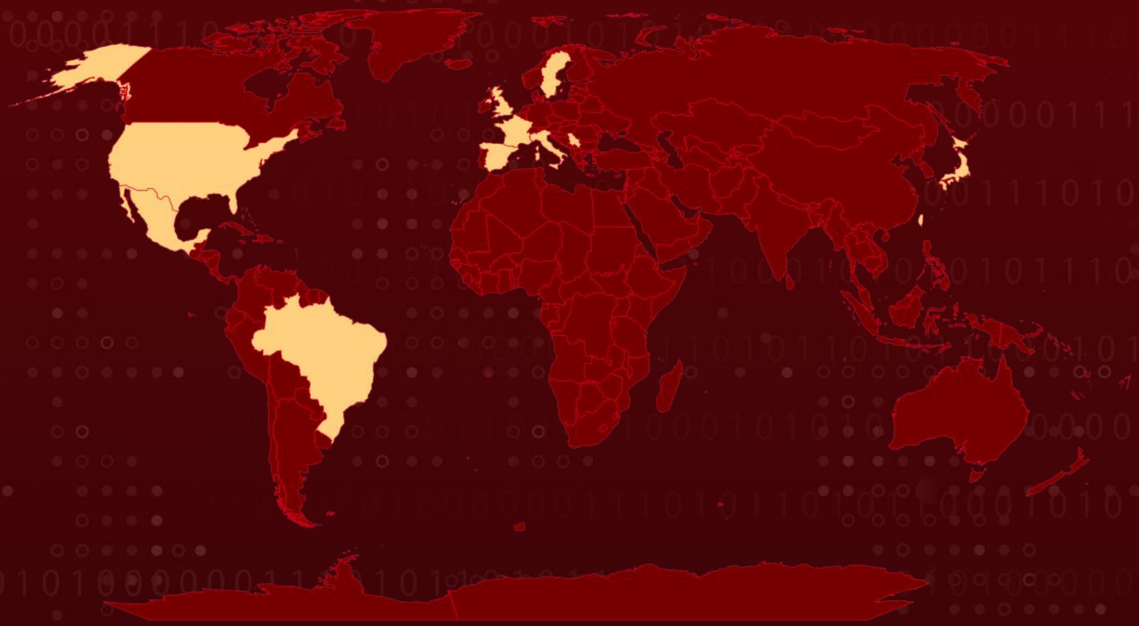
RansomHub A Rebranded Menace Exploiting the ZeroLogon Vulnerability

Date of Publication	Admiralty Code	TA Number
June 7, 2024	A1	TA2024220

Summary

First Seen: February 2024
Malware: RansomHub, Knight ransomware
Attack Region: United States, Taiwan, Serbia, Sweden, Italy, United Kingdom, France, Spain, Mexico, Japan, Brazil
Targeted Industries: Financial Services, Technology, Telecommunications, Construction, Engineering, Energy, Government, Education, Fashion, Medical, Agriculture, Food, Healthcare, Transportation, Non-profit, Real Estate, Utilities, Aviation
Attack: RansomHub, a newly emerged Ransomware-as-a-Service (RaaS) entity, is believed to be an updated and rebranded iteration of the Knight ransomware. Driven by financial gain, RansomHub explicitly forbids attacks on specific countries.

Attack Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-1472	Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓

Attack Details

#1 RansomHub, a newly emerged Ransomware-as-a-Service (RaaS) entity, has swiftly ascended to become one of the most prominent ransomware groups in operation. It is suspected to be an updated and rebranded iteration of the Knight ransomware.

#2 The source code for Knight, originally known as Cyclops, was put up for sale on underground forums in February 2024 following the developers' decision to cease their activities. Both RansomHub and Knight have payloads written in Go, with most variants obfuscated using Gobfuscate.

#3 There is a substantial degree of code overlap between the two families, evidenced by their nearly identical command line help menus. The primary difference is the inclusion of a sleep command in RansomHub.

#4 A distinctive feature of both Knight and RansomHub is their ability to restart an endpoint in safe mode before commencing encryption, a technique previously utilized by the Go-based Snatch ransomware.

#5 Recent RansomHub attacks have seen attackers gain initial access by exploiting the Zerologon vulnerability (CVE-2020-1472), which allows an attacker to obtain domain administrator privileges and seize control of the entire domain.

#6 The attackers employed several dual-use tools before deploying the ransomware. Atera and Splashtop facilitated remote access, while NetScan was likely used to discover and gather information about network devices.

#7 RansomHub comprises hackers from various global locations, united by a common objective of financial gain. The group explicitly prohibits attacks on specific countries and non-profit organizations. Their website states they refrain from targeting the CIS, Cuba, North Korea, and China. Despite suggesting a global hacker community, their operations closely mirror the characteristics of a traditional Russian ransomware setup.

Recommendations

Patch Management: Prioritize timely patching of known vulnerabilities, especially those like CVE-2020-1472 in Microsoft, which are exploited by RansomHub threat actors for initial access.

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.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
TA0040 Impact	**T1190** Exploit Public-Facing Application	**T1133** External Remote Services	**T1016** System Network Configuration Discovery
T1082 System Information Discovery	**T1588.006** Vulnerabilities	**T1057** Process Discovery	**T1562.009** Safe Mode Boot
T1562 Impair Defenses	**T1018** Remote System Discovery	**T1105** Ingress Tool Transfer	**T1562.001** Disable or Modify Tools
T1219 Remote Access Software	**T1090** Proxy	**T1560.001** Archive via Utility	**T1041** Exfiltration Over C2 Channel
T1587 Develop Capabilities	**T1587.001** Malware	**T1486** Data Encrypted for Impact	**T1657** Financial Theft

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292, 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087, 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a, 8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7, ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00, 104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2, 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad, 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e, 595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb, 7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2, e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23, fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e, f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3, A96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2
Tor Address	ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion, ransomgxjnwmu5ceqwo2jrjssxpoicolmgismfpnslaixg3pgpe5qcad[.]onion

Patch Link

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

Recent Breaches

http://crezit.com/
https://clevo.com.tw/
https://frontier.com/
http://psgbdvor.rs/
https://www.bjurholm.se/
https://www.christies.com/
https://siaed.it/
https://iseta.fr/
http://brittanyhorne.com/
https://www.throttleup.io/
https://acslabtest.com/
http://www.mataderodegijon.es/
https://oriux.com/
http://mataderodegijon.es/
http://houstonwastesolutions.com/
http://neodesha.org/
https://www.okuant.com/en/home/
http://chuoss.co.jp/
https://eastshoresound.com/
https://chuoss.co.jp/
https://www.eucatex.com.br/
https://www.rockymountainsales.com/
https://confins.com.br/
https://portosaofrancisco.com.br/
https://apsfs.com.br/

References

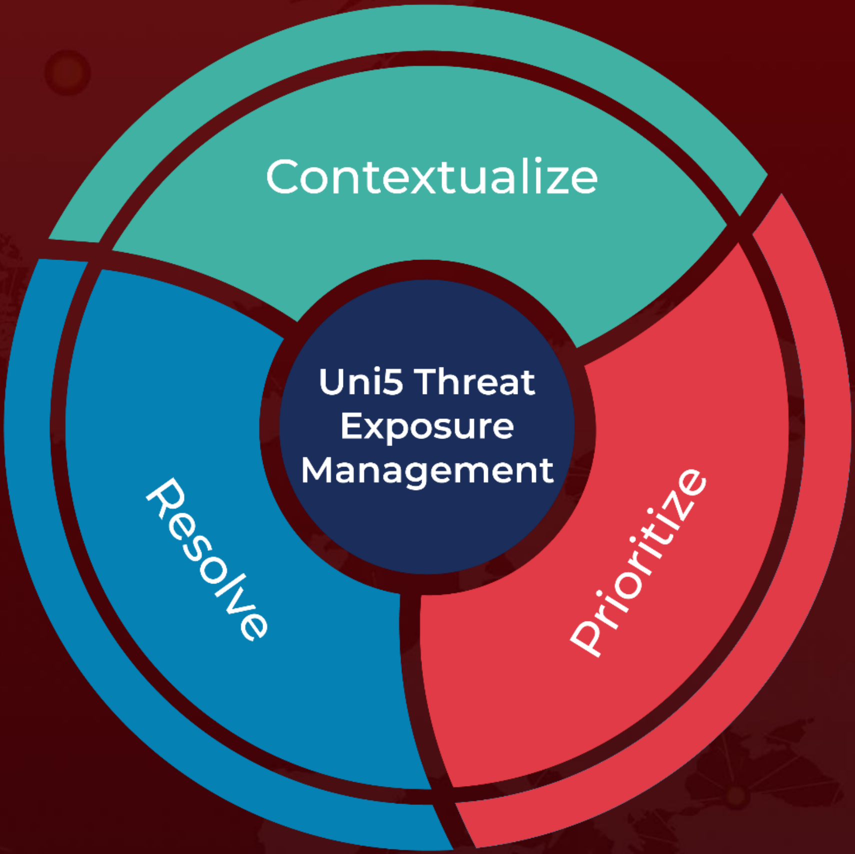
https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

https://socradar.io/dark-web-profile-ransomhub/

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

June 7, 2024 • 2:30 PM

© 2024 All Rights are Reserved by HivePro

More at www.hivepro.com