Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

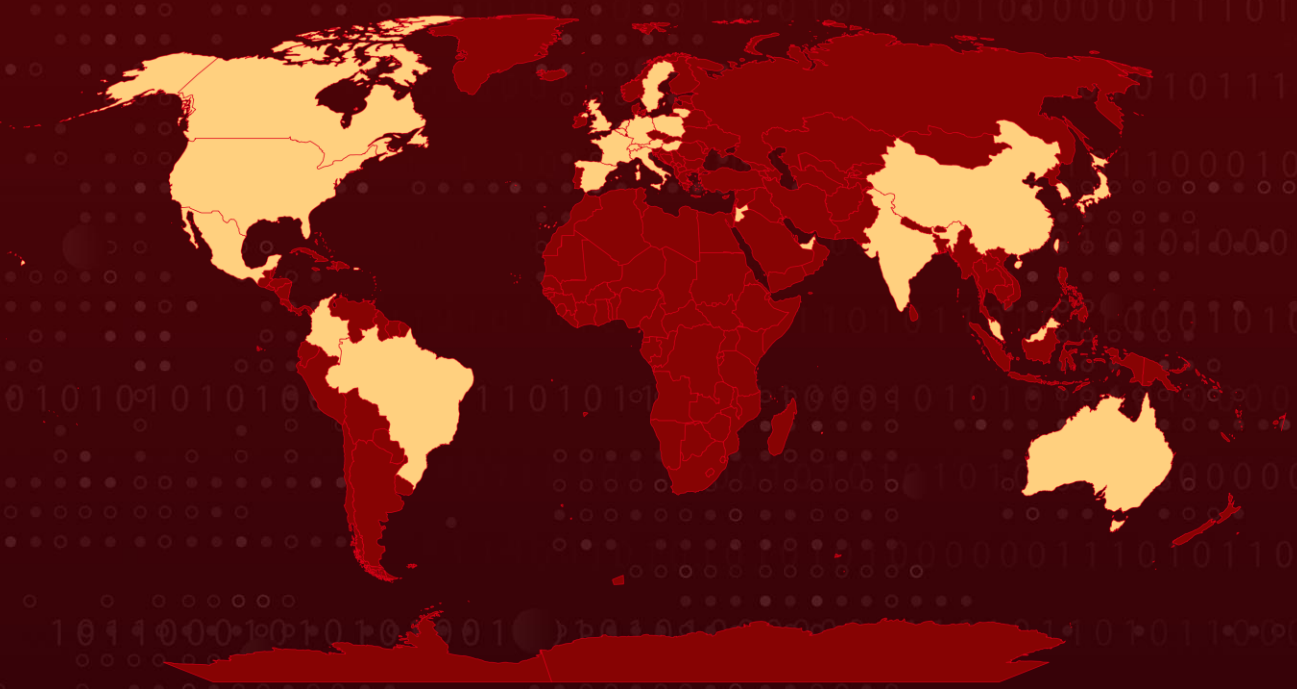
In-Depth Analysis of NoEscape Ransomware

Date of Publication	Admiralty Code	TA Number
November 16, 2023	A1	TA2023463

Summary

First Appearance: March 2023
Attack Region: United States, Sweden, Australia, France, Canada, United Kingdom, Switzerland, Poland, Puerto Rico, Italy, Netherlands, South Korea, United Arab Emirates, Mexico, Belgium, Germany, Spain, Hungary, Japan, Austria, China, Malaysia, India, Brazil, Republic of Korea , Taiwan, Lithuania, Jordan, Mauritius, Colombia
Affected Platform: Windows, Linux, and ESXi
Malware: NoEscape Ransomware
Targeted Industries: Business Services, Manufacturing, Retail, Education, Construction, Healthcare, Government, Law Firms & Legal Services, Financial services, Hospitality
Attack: The NoEscape ransomware, suspected to be a rebrand of Avaddon, targets enterprises globally through multi-extortion attacks. Operating as Ransomware-as-a-Service, it encrypts files, changes wallpapers, and demands ransom, emphasizing financial motives via a TOR negotiation site.

Attack Regions



Attack Details

#1 The NoEscape ransomware, which emerged in May 2023 and is suspected to be a rebrand of Avaddon, operates as Ransomware-as-a-Service and targets enterprises through multi-extortion attacks. It steals data and encrypts files on Windows, Linux, and VMware ESXi servers, affecting various industries globally, with the United States as a primary target.

#2 The infection mechanism involves executing commands to delete Windows Shadow Volume Copies, local backup catalogs, and disabling Windows automatic repair. The ransomware terminates various processes, including those related to security software, backup applications, web, and database servers.

#3 It also stops relevant Windows services to unlock files for encryption. NoEscape and Avaddon encryptors are nearly identical, with the former using the Salsa20 algorithm instead of AES. Encrypted files have a unique 10-character extension, and the ransomware changes the Windows wallpaper to display recovery instructions.

#4 The NoEscape ransomware encrypts and exfiltrates victims' files, demanding a ransom for decryption. It appends a unique extension to encrypted files and avoids certain file types and directories. Victims receive a ransom note guiding them to a TOR site for negotiations, emphasizing the group's financial motives.

Recommendations

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Regularly Update and Patch Systems: Ensure that all operating systems, software, and applications are up to date with the latest security patches. Regularly update and patch Windows, Linux, and VMware ESXi servers to address vulnerabilities that ransomware may exploit.

Enhance Endpoint Security: Utilize advanced endpoint protection solutions, such as antivirus and endpoint detection and response (EDR) tools, to detect and prevent ransomware infections. Ensure that security software is regularly updated and configured to provide optimal protection.

Network Segmentation: Implement network segmentation to contain and isolate potential infections. Restrict communication between network segments to prevent the lateral movement of the ransomware within the organization's network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0040 Impact	TA0043 Reconnaissance
TA0010 Exfiltration	TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0007 Discovery	T1547.009 Shortcut Modification
T1133 External Remote Services	T1078 Valid Accounts	T1204.002 Malicious File	T1204 User Execution
T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1027.002 Software Packing	T1027 Obfuscated Files or Information
T1055 Process Injection	T1070.004 File Deletion	T1070 Indicator Removal	T1112 Modify Registry
T1140 Deobfuscate/Decode Files or Information	T1497.001 System Checks	T1003 OS Credential Dumping	T1497 Virtualization/Sandbox Evasion

T1087 Account Discovery	T1482 Domain Trust Discovery	T1069 Permission Groups Discovery	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1560.001 Archive via Utility	T1071.001 Web Protocols	T1567.002 Exfiltration to Cloud Storage
T1567 Exfiltration Over Web Service	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1486 Data Encrypted for Impact
T1485 Data Destruction	T1543.003 Windows Service	T1543 Create or Modify System Process	T1490 Inhibit System Recovery
T1119 Automated Collection			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	204f028c983f654be32b97e849edeaab, 47ae17d89c2d9b6acdc7458f5df1c6f7, 5779cec690b5bbc61687381ae8a8d518, 58b4a4eed74fbfbf104d0ffd92207018, a106c1236357c315722ddbd985c5613c, c850f6816459e3364b2a54239642101b
SHA1	ea1f7940271fc80d06b2f222506020b650ad41bc, 30f71a24c15dd81965b12996a79d914acf4f169e, 12dc0a2de3ad30201107bfcb679de5acacf31e5c, 30c60f18279ed5fd36e3ac2d3ba5ddbdc5d1f624, 9cbc7417fa5ce2f6d87026337fc7892e4f485819, d38c613020cb4616783c8535380e28404f7eaebf, b17403e7dcb992ba8d2b56dd843406264d3910e5, 317f296131b37a73c9a5d253015821dfdc8b1190, 8770132656d4f3d9b973848b89e96fc95d736179, 994edc8d183a1a7243790539044d12b80b1d5d84, aa8ebc0b00d116cfe46245e0bb4a0b5108aadc0f, e128b01745ae1cb0de41c1b1c2e7271a172cf696

TYPE	VALUE
SHA256	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a, 2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5, 21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da, 4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e, 53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128, 68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0, 73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e, 8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31, 9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c, c34c5dd4a58048d7fd164e500c014d16befa956c0bce7cae559081d57f63a243

Recent Breaches

www.sosbonedocs.com
www.landercountynv.org
carespring.com
www.mprlift.se
www.putzelelectric.com
www.pargroup.com
www.ezifloor.com.au
www.actionsantetravail.fr
jeffcoat.us
www.avianor.com
oefederal.org
www.orionlibrary.org
www.laborforce.com
www.agiledisplaysolutions.com
www.rnwooler.co.uk
schwob.swiss
www.vinovalie.com
www.prclinical.com

twosaints.org.uk
www.mckeagandco.com
www.strumet.pl
www.spolzino.com
straphaels.org.uk
www.dynametal.com
www.floristssupply.com
victorvilleca.gov
www.opl.it
www.koreapetroleum.com
instantaccess-co.com
www.gasmart.mx
www.bmw-ducati.com
misterminit.eu
icschool-uae.com
www.kbs-accountants.nl
ucb.edu.pr
penfieldfire.org
kbs-accountants.nl

References

https://www.fortinet.com/blog/threat-research/ransomware-roundup-noescape

https://www.sentinelone.com/anthology/noescape/

https://www.csk.gov.in/alerts/NoEscape_ransomware.html

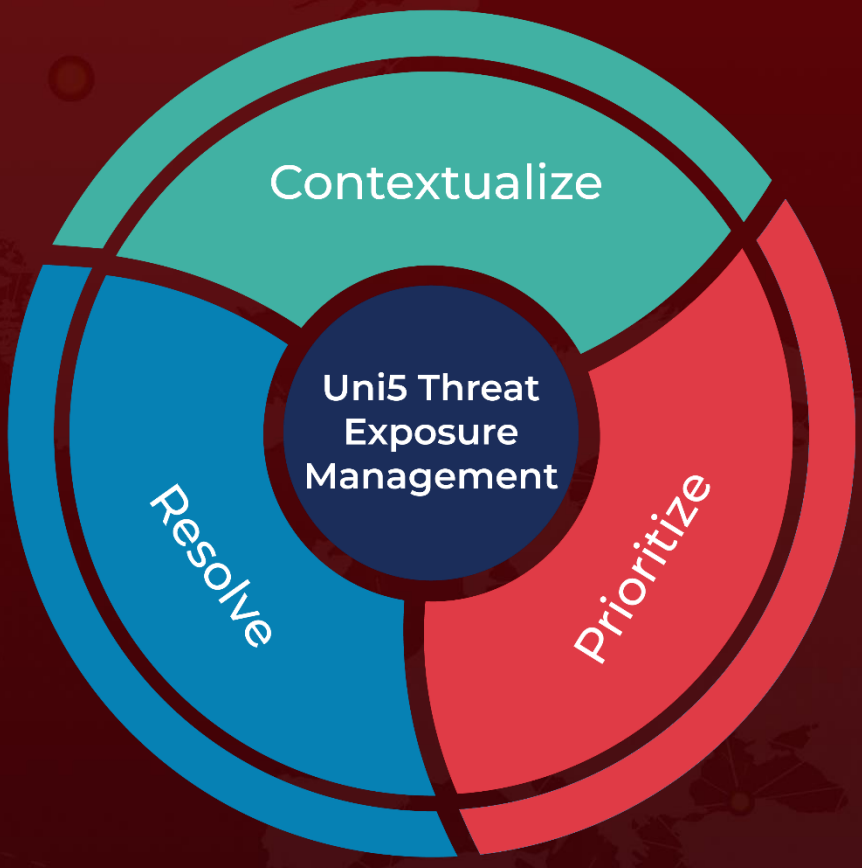
https://socradar.io/dark-web-profile-noescape-ransomware/

https://healthitsecurity.com/news/noescape-ransomware-emerges-targeting-healthcare

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

November 16, 2023 . 5:00 AM

More at www.hivepro.com