Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

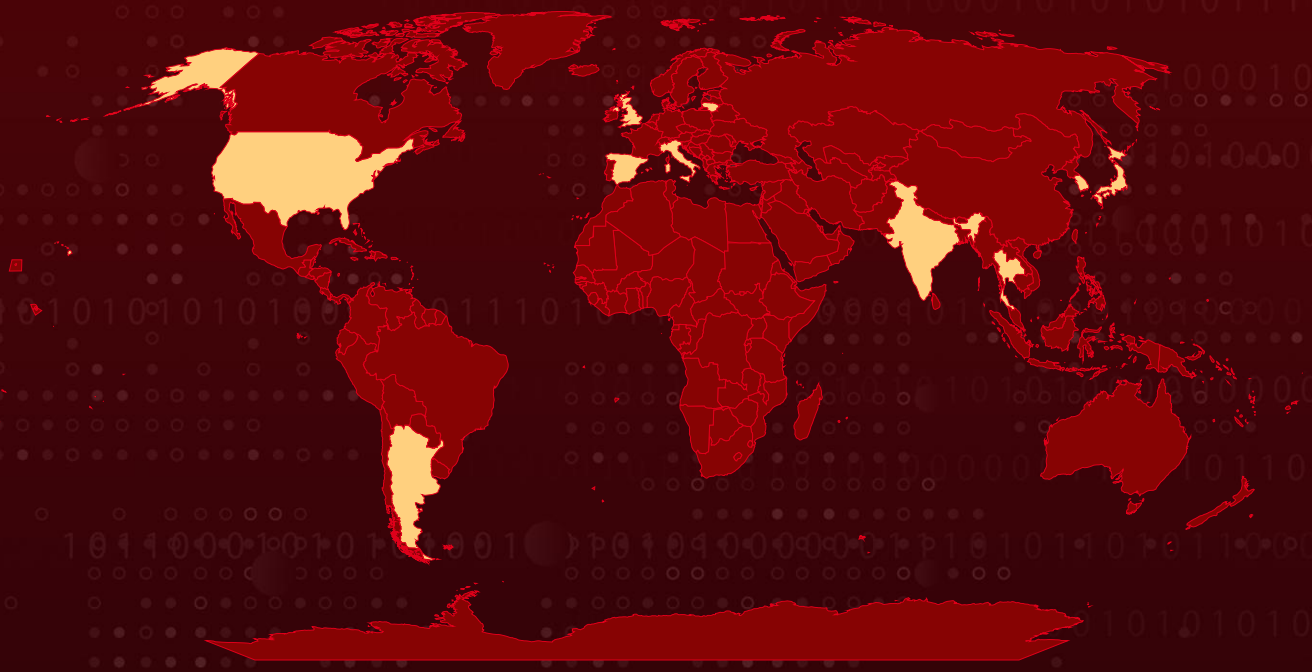
BlackNevas Ransomware: A Rising Global Cyber Threat

Date of Publication	Admiralty Code	TA Number
September 18, 2025	A1	TA2025286

Summary

First Seen: November 2024
Targeted Countries: Spain, Argentina, Singapore, Japan, Thailand, South Korea, Lithuania, United Kingdom, United States, Italy, India
Targeted Industries: Healthcare, Finance, Manufacturing, Legal, Telecommunications
Targeted Platforms: Windows, Linux, NAS devices, VMware ESXi
Malware: BlackNevas ransomware (aka Trial Recovery)
Attack: BlackNevas ransomware, first identified in November 2024, has rapidly spread across Asia, Europe, and North America, targeting industries such as healthcare, finance, manufacturing, and legal services. Operating independently outside the RaaS model, it combines AES-RSA dual encryption with data theft, appending ".-encrypted" to files and demanding ransom via email or Telegram under threat of leaks. The malware supports Windows, Linux, NAS, and ESXi systems, delivered through phishing or vulnerability exploits, with modular options for selective or destructive actions while sparing critical system files. High-profile attacks underscore its aggressive double-extortion tactics and growing global impact.

Attack Regions



Attack Details

#1

BlackNevas ransomware, also known as Trial Recovery, is a sophisticated variant derived from the Trigona ransomware family and was first identified in November 2024. Since its emergence, it has rapidly expanded its operations across Asia, Europe, and North America. The group targets both enterprises and mid-sized organizations in critical sectors including healthcare, finance, manufacturing, and legal services. Nearly half of its campaigns have been concentrated in the Asia-Pacific region, with notable incidents in Japan, Thailand, and South Korea, while attacks have also been reported in the UK, Italy, Lithuania, and the U.S.

#2

Unlike many ransomware gangs that operate under a Ransomware-as-a-Service model, BlackNevas functions independently. Its attacks combine strong file encryption with aggressive data theft, making it a classic double-extortion operation. The malware uses AES to encrypt files and RSA to secure the AES keys, preventing decryption without the attacker's private key. Files are renamed with a distinctive ".-encrypted" extension, while ransom notes labeled how_to_decrypt.txt appear in every encrypted folder. Victims are instructed to negotiate through email or Telegram, under the threat that stolen data will be leaked, auctioned, or published on partner sites if ransom demands are not met within seven days.

#3

BlackNevas is highly versatile, it supports Windows, Linux, NAS, and VMware ESXi environments, often delivered through phishing attacks or exploitation of unpatched vulnerabilities. Its modular design allows attackers to tailor campaigns, using command-line options such as /full, /path, or /fast to control the scope of encryption, and /erase or /shdwn to damage files or shut down systems. To ensure victims remain reliant on them for recovery, the malware carefully avoids encrypting critical operating system files, leaving infected machines bootable but unusable without a decryption key.

#4

The group's extortion tactics have been highlighted in recent cases such as the attack on Spanish firms, where stolen file inventories were publicized to pressure payment. By combining stealthy deployment, strong cryptography, and data leak threats, BlackNevas has positioned itself as a serious and expanding global threat.

Recommendations

Keep Systems Updated: Regularly patch operating systems, applications, NAS devices, and virtualization platforms like VMware ESXi. Attackers often exploit known vulnerabilities, so timely updates significantly reduce exposure. Ensure all endpoints are covered and critical security patches are applied promptly.

Implement Strong Access Controls: Enforce the principle of least privilege for users and services. Limit administrative rights and restrict access to sensitive data to only necessary personnel. This reduces the potential for ransomware to spread laterally across networks.

Monitor and Detect Suspicious Activity: Deploy endpoint detection tools to track unusual processes, file modifications, and abnormal network traffic. Look for signs such as .-encrypted file extensions or rapid file encryption. Early detection can prevent widespread damage.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an BlackNevas ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0040 Impact
T1566 Phishing	T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1078 Valid Accounts
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation

T1497 Virtualization/Sandbox Evasion	T1070 Indicator Removal	T1562 Impair Defenses	T1083 File and Directory Discovery
T1012 Query Registry	T1135 Network Share Discovery	T1561.001 Disk Content Wipe	T1561 Disk Wipe
T1486 Data Encrypted for Impact	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2374998cffb71f3714da2075461a884b, 4a1864a95643b0211fa7ad81b676fe2e, 9f877949b8cbbb3adfe07fd4411b9f26, f2547a80dd64dcd5cba164fe4558c2b6
SHA1	203f81cbe35c64071f52f34afbbbfc7d61b3e702, 2a79c999e20c5d8102e0b728733cc8eba2b4d8ac, 3226ebfc23dbe1a6cc44c3255d1a0e12f0dd153c, 3ff7aedacf36f96fef42391aaadb2c63820bef7f, 49551cb0bbc2da3f6d36523a005af5ee1f5ad1a8, 499cd23b37a00b9a8ad212f879501705baad1781, 4d5605008bd0619a5980c4633889d7c253093360, 4db3b2876ef5c8e5ea977d8ffedef428b93408a4, 61c56c25f5ca4bee336aa30e89123eb2daf5166a, 646533556a16a9d17bd7ad2265873bc8f1ccb4f4, 67750b2b0b90572ade6ef760bcded1ef5fc09982, 781a8e52c2399c07ca4853def924d79be5182b32, 7b3cbd60020c1d155b12271881d69c968fcde04f, 7bf79cc58fb8f3d0ec774cb8b9e8ce311cbc27d2, 7c4f10d85607e65386fb504446b45419901c5276, 812d65b67ce28905f5e07ac1f82b827ebd36470a, 88aee839de69ce1602ef2bb401a6cabb6b376e19, 8cbbcbe187ff66c44908a205236d4230931f7d73, 923be026c79e7b5b5d29461420887fe2e8875b01,

TYPE	VALUE
SHA1	92b0ce569d838cd9b773cc13b6b6ea5609e85fd7, B00897AE5B116680CCDD2E43A3A9599D8C3E166E, b8c85fa5a81b3d70a21835fbea394e0611461bf8, c1c9008b4be855583df0f04204443262a3fbc8ab, cd2f25a8ab74bdc17d7c8170f2c4135537ece3c4, cdb07718787743ceb488b5bd184d9a4939c12dbf, d026954e6f646b84943f8514be606650be8c18bb, dc6d4f0a88ea0458926ff8f57dbd8239ed140824, ebf63e7a27c91f96d84b66d7ba435ddc3a153b71, 2d8e9ea39b9853d5676957a51f09f14d3703d1bd, d6e1a47a0cf9bc94a816149f6e1f1a04c53f99d1, 1b14a60d50622a7c846f9e81d9668b4962fc356b, 70e9b61e0a8e708e8512c54f96b90b32bac38984, a35b2be3167b72c73b2f8f9ac058576cf080f752, 1c0620a81f8cfb3c2a8b073b7e5a5c2329b511a5, f7d2d8fd75a62a9ce4533196b13f9ba55e985b62, 3b8185e491bbfe4ba0583f3a5810674aeaff26ad, 1ad51a365293269da14fd6914c3014fb3556f69f, a61aaf88253bfb4bd80e0ca7bbaf4a78e6bb2591, 67a078a7d703308e3c0eb2af7ea0c288453cd705, 80ad69638820c264552e5f73ed696f88614fa3bd, cbe2b0cfa599fe7477ebbe92feaadb54b5b25deb, ad63f0652ce21b0dac5284158cf301410f57d0f9, f7ac2604e6e186a647318544c36ba5758cdcb85a, 97fa0c24f75164940717672f22643ba31161c638, f18b501eca2a7390705967a24f67b808b43d2212, 8dfd14d230d93ff6eea3dd09934ebf9c9e860a0f, 93ba61e1b7d12277e0bcee27ec7f37a74d8f1c97, 119388459d68d2781b843e1db71be8f5e01e965a, 0a33ed85842cf189f96ae9ea804a2e0789200430, 3bcf26bb616c57330da226f5db4e89bb609147e8, 827c01503a92b1e202939ae5a0e3e4d5ff02f4ae, 2e2046d5e8fb4ccc18f7fdf1a4dd076bf2333417, 18af0b641e456ed5df3908f2e2fc16ea01fef0f2, 1881f7bd1867e7d625e2ef2f0dc856437a376112, 1b87e342d2fdd5cf5db3a8280bac92f90f099516, 6b22150c7eeafd74dca41b749bf33f391401d094, a7da9e83c69a9deb6aa4de1fb0ec7d0badb4a426, 67c0338c0a58493befc6c77c9f7fb16d753eb155, 0b02e7c36714e9af519fd24bca893172afd2562d, aa10da9d601482262b87cb1e0748acca7a91c2a5

TYPE	VALUE
Email	amsomar[@]consultant[.]com, avalonsupp[@]consultant[.]com, biosannetsuabvg[@]mail[.]com, black4over[@]newlookst[.]com, compsupp[@]techie[.]com, corubete[@]dr[.]com, milford[@]usa[.]com, murrock[@]consultant[.]com, ovtaitonine[@]usa[.]com, suppcarter[@]uymail[.]com, toxicavalon[@]toke[.]com, varentsujikyuke[@]mail[.]com, widemoucerpco[@]mail[.]com, paymeuk[@]consultant[.]com , Serina5Murrock[@]email[.]com
TOR Address	Hxxp[://]ctyfftrjgtwdjzlgqh4avbd35sqrs6tde4oyam2ufbjch6oqpqtkdtid[.]onion
SHA256	23642a78addcffd124db133a2dd2fcd2d1bdb060dd1e41da33cb18eec7a88867, 2b9fe8a2629727470be1c928f7c9be7e2ea6cc22fb12f971902bf9cea8b16afb, 360758c296310ba428d0d52c90e31c05fc43d5889282fa840283cf468f2378e8, 3d09e930305cb3aa4ca54a39b0e3749f083d432f202606c8adac8455014b47fc, 43f145fccec00f1e100ec3377eaf0ab60df3b9c5291b8011e05141cc04704be1, 49fcbd606ff10d4661e222b8910ab7829d1668e3c97f1bab7eb51e8ec7d799a5, 501821a19ccf59830789849beff94238736adb4b213870a511890c5c8efab2a6, 623f3e98908962669e48edd414dbb67e9d4e204f677998fdcc9c2d790816a67f, 713392f009bc133f24b3271379a4ac147e1a7782b6a1ac957c1fda69d676b550, 840b1c580bfd15ca3eb1cc94cf479f63b93285d2599bc2e3cd361e3f5a340f19, 8a2d6d27ffcc66400a640d3c9c9e6becb90c04c5bab452cac56f999c48a04d63, 910cc03d64bf09f53cdf3b83068cc46368c23a061c2e1ed5df0e3a35d6c9e084,

TYPE	VALUE
SHA256	95e744ddcc2e8f89f6c6e25503eff2eb5e70e98f6989bb4a4e93f17b09448e78, 9d9c146910f294b3e2a755f76e8066cd2edfac057ff54f00f405e2f9e8b9e51a, a0630e2a81775e8334ea9f8cac73cebf1b9a70507ea3347c0c2eba82c80219a6, a331504acf589be5d11202232a7a93eeb4fe6b053beea231d9a0a661bcaf3fd6, b0dfaf509de38749c49afcb3cd34d27126044bb77cc16896b02ebced6f95db02, b2353fce403b079735a606294c4ffc20a71f1c6b16ec15e94f554beafcddd1ea, bad3c2f72ef2be522a554a9615dc93027416a3d4048f77519fca5104fabba1f9, bf4adad2eb1163369c133ae61c181a3f91ef8640a457e9c4e72d77a60fbfa7ab, c08a752138a6f0b332dfec981f20ec414ad367b7384389e0c59466b8e10655ec, c0fc61631a20c373ce17e939e09cfb4f5179c9e0788e80079b4ee8986afe89bd, d953bce4d87f5837ce318481e3a1b6617cf64af976043d3b4b4866475bb31972, def75a41435dc28430097a7e116b2d17526ce2b0172995618f2749b0d732f7ea, e7706a633f24679c7550a31b96088dda8f772c98f64daee7cfbf0dc17a4a8338, eb8cbc4a0eae33bfdc4ecb99d033c81224b005e55588ceb86346f2b2d3fd790f, f25f76a85ded0d4d285d9ae5482d8fe07dade3e241853d00b17642d7873733e8

Recent Breaches

https://www.cartonajesbernabeu.com
https://oftaltech.com
https://www.sistran.com
https://toyota-asia.com
https://www.taniabe.co.jp
https://www.ckpower.co.th
https://www.chabaabangkok.com
https://dragonflygame.com
https://www.cili.lt
https://kinas.co.uk
https://www.cosaen.es
https://www.payme.co.uk
https://www.qds.biz
https://learn.k12.ct.us
https://promosfera.com
https://www.clearsynth.com

References

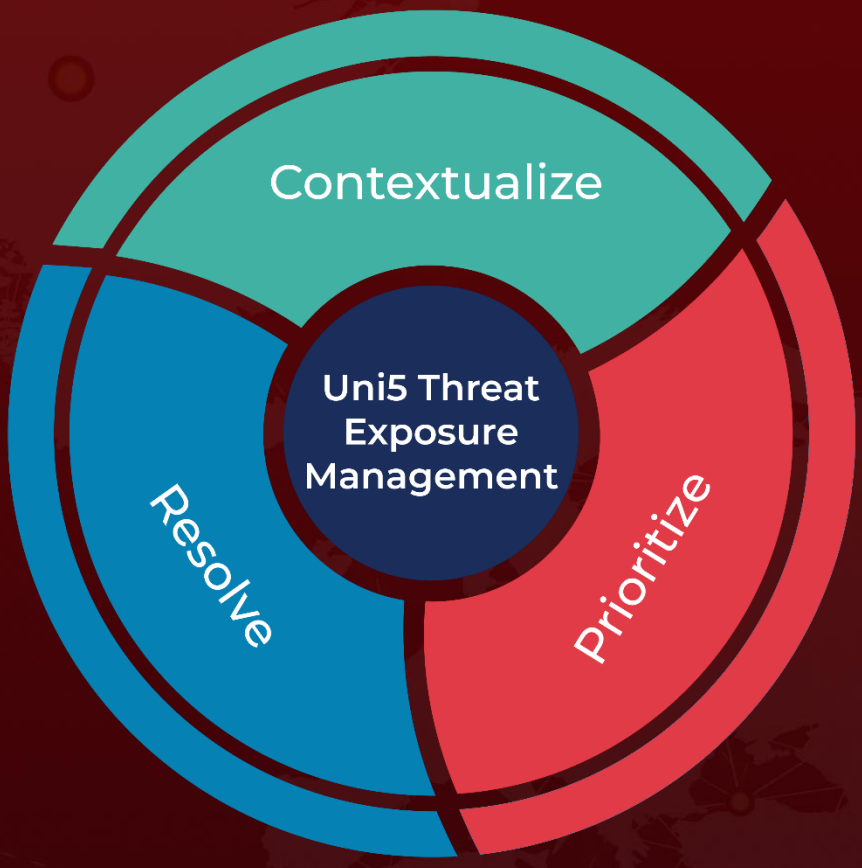
https://asec.ahnlab.com/en/90080/

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

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 18, 2025 . 5:30 AM

More at www.hivepro.com