Hive Pro

Threat Level

Red

CISA: AA24-207A

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

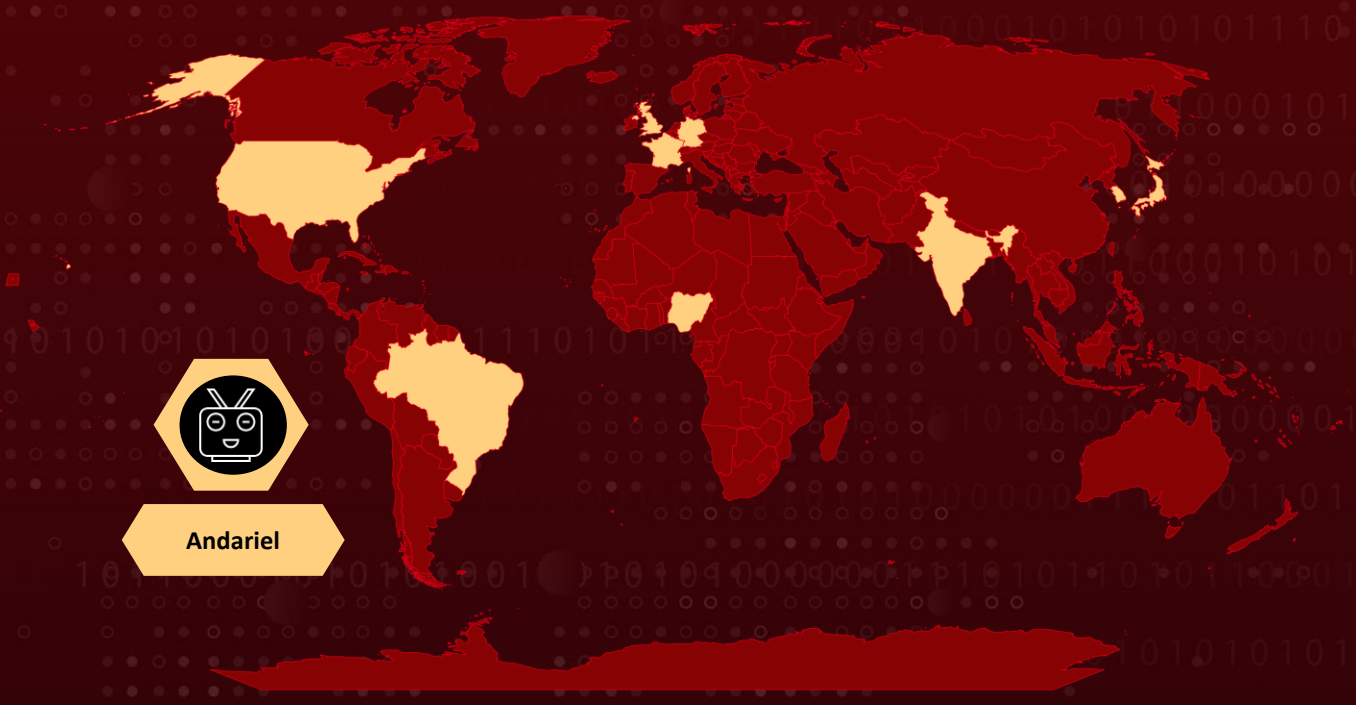
Andariel: North Korea's Evolving Cyber Threat Landscape

Date of Publication	Admiralty code	TA Number
July 30, 2024	A2	TA2024288

Summary

First Appearance: 2009
Actor Name: Andariel (aka APT45, Onyx Sleet, formerly PLUTONIUM, DarkSeoul, Silent Chollima, and Stonefly)
Targeted Countries: United States, Brazil, India, Japan, South Korea, United Kingdom, Germany, France, Nigeria
Malware: Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware
Targeted Industries: Critical Infrastructure, Defense, Aerospace, Government, Financial, Healthcare, Pharmaceutical, Engineering, Telecommunications, Transportation, Technology, Biotech, Chemicals, Education, Energy, Insurance, Legal, Medical Equipment, Nuclear Power, Retail, Utilities, and Agricultural

Actor Map



Attack Details

#1

Andariel, a North Korean cyber espionage group active since 2009, is known for its evolution from destructive attacks to specialized cyber espionage and ransomware operations. This group poses a significant and ongoing threat to various industry sectors worldwide. Initially focused on espionage campaigns targeting government agencies and defense industries, Andariel has expanded into financially motivated operations, setting it apart from other North Korean cyber operators like TEMP.Hermit and APT43. The group frequently targets critical infrastructure, reflecting the strategic priorities of the DPRK.

#2

Andariel employs a range of sophisticated techniques and custom tools across various stages of the cyber kill chain. The group gains initial access through exploiting web server vulnerabilities, like Log4j, or phishing for initial compromise. They establish footholds using tools like PowerShell and Visual Basic. They maintain presence and escalate privileges through methods such as scheduled tasks and process injection, utilizing tools like ARTSHOW and IRONSTORM.

#3

Andariel's reconnaissance activities include utilizing publicly available internet scanning tools to identify vulnerable hosts. The group has been observed conducting scans for over 40 CVEs and targeting them for infiltration and other nefarious activities. They employ a mix of publicly available tools and custom malware, characterized by unique code reuse and encoding techniques for execution, credential access, lateral movement, and data exfiltration. The group's malware library is distinct from other North Korean operators. Their command and control operations use sophisticated tunneling techniques to maintain communication with compromised systems, disguising malware traffic to evade detection.

#4

The operations of Andariel have evolved with North Korea's shifting geopolitical interests. While the group's early activities were predominantly espionage-focused, targeting government and defense entities, it began targeting the financial sector by 2016 and nuclear facilities by 2019. This shift underscores Andariel's role in supporting North Korean state objectives. The group's suspected development of ransomware indicates a dual focus on funding its operations and supporting broader state goals.

#5

Even during the COVID-19 pandemic, Andariel, like other North Korean operators, targeted the healthcare and pharmaceutical sectors. However, Andariel has continued to focus on these sectors longer than its peers, suggesting an ongoing mandate to collect related information. They have been observed launching ransomware attacks and conducting cyber espionage operations simultaneously against targeted entities.

#6

Andariel is linked to North Korea's Reconnaissance General Bureau (RGB), and the U.S. government has offered a $10 million reward for information leading to the capture of Rim Jong Hyok, who is connected to Andariel's cyber activities. The group's advanced espionage campaigns highlight the severe threat they pose, emphasizing the need for organizations to implement robust cybersecurity measures to defend against such threats.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Andariel	North Korea **MOTIVE** Espionage and Information theft, Financial gain	United States, Brazil, India, Japan, South Korea, United Kingdom, Germany, France, Nigeria	Critical Infrastructure, Defense, Aerospace, Government, Financial, Healthcare, Pharmaceutical, Engineering, Telecommunications, Transportation, Technology, Biotech, Chemicals, Education, Energy, Insurance, Legal, Medical Equipment, Nuclear Power, Retail, Utilities, and Agricultural

Recommendations

Implement Email Security Solutions: Deploy email filtering and security solutions to detect and block phishing emails containing malicious attachments or links. Educate employees on recognizing phishing attempts.

Threat Exposure Management: Implement a robust threat exposure management framework to continuously assess, prioritize, and mitigate cybersecurity risks across the organization's digital footprint.

Zero-Trust Architecture: Adopt a Zero-Trust approach by verifying every request as though it originates from an open network, regardless of whether it originates from inside or outside the network perimeter. Implement strict access controls based on identity, device health, and other contextual factors.

Security-by-Design Principles: Incorporate security considerations into the design and development phases of systems and applications. Follow secure coding practices, conduct architecture reviews, and integrate automated security testing tools into the CI/CD pipeline.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation	TA0042 Resource Development
TA0003 Persistence	TA0007 Discovery	TA0008 Lateral Movement	TA0043 Reconnaissance
TA0009 Collection	TA0011 Command and Control	TA0006 Credential Access	TA0010 Exfiltration
TA0005 Defense Evasion	T1566 Phishing	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1059.001 PowerShell	T1059.006 Python	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1059.003 Windows Command Shell	T1055.012 Process Hollowing	T1055 Process Injection
T1055.003 Thread Execution Hijacking	T1134 Access Token Manipulation	T1098 Account Manipulation	T1543.003 Windows Service
T1543 Create or Modify System Process	T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1021.002 SMB/Windows Admin Shares
T1007 System Service Discovery	T1087 Account Discovery	T1591 Gather Victim Org Information	T1592 Gather Victim Host Information

T1595 Active Scanning	T1596 Search Open Technical Databases	T1003 OS Credential Dumping	T1048 Exfiltration Over Alternative Protocol
T1090 Proxy	T1560 Archive Collected Data	T1572 Protocol Tunneling	T1587.001 Malware
T1587.004 Exploits	T1190 Exploit Public-Facing Application	T1027 Obfuscated Files or Information	T1071 Application Layer Protocol
T1039 Data from Network Shared Drive	T1567 Exfiltration Over Web Service		

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	befba41ba023bb72f70b5ef904517d8f, f8f7eced1411d76e2a0319151ecf80b7, 4d30612a928faf7643b14bd85d8433cc, 0f9b876031ffc16c7eedfeaf2ca9dc5b, 0d696d27bae69a62def82e308d28857a, 152b264288bcf5dc02222cee49587b8e, dd9625be4a1201c6dfb205c12cf3a381, 17335705966160a4c5da10b596d83f72, 4bb54e135302bf3c21bff89177f70759, 3e9ee5982e3054dc76d3ba5cc88ae3de, 3a3bad366916aa3198fd1f76f3c29f24, cf236bf5b41d26967b1ce04ebbdb4041, 640e70b0230dc026eff922fb1e44c2ea, 2e18350194e59bc6a2a3f6d59da11bd8, cdeae978f3293f4e783761bc61b34810, 2cc302d80050dd10e8d8c489e5873a1c, 31b6d895da1fbe17d45b3905b71bdb94, 41882402c8937f2ba2c4791c081f54c3, 7c30ed6a612a1fd252565300c03c7523, 11ec5eb513e5a4d9d35be0b8c3335099, 6c2b947921e7c77d9af62ce9a3ed7621, 0ed084c48634e8497c7eda51570793c1, b48a887f303c6e01ce054353f8318523, 769617b07d0a455fd666418bafbdae1b, 43e756d80225bdf1200bc34eef5adca8, 9767aa592ec2d6ae3c7d40b6049d0466,

TYPE	VALUE
MD5	0055a266aa536b2fdadb3336ef8d4fba, eb4c52b2c9564583f244570528f3f6a1, 0a5a3d31346f91bffcfc69950bac18c3, 028693c655be9ced65a5fdd419f870c1, 88f9824b5a76591d62d391e6b1ef1d31, 6dad4ad013a1991695302bdd34fbb566, f49c34718ad43d37624d4bddf70fe79b, c027d641c4c1e9d9ad048cda2af85db6, 9b9d4cb1f681f19417e541178d8c75d7, 079b4588eaa99a1e802adf5e0b26d8aa, 59ec24539c786e6ac9467dad3183c280, 88a7c84ac7f7ed310b5ee791ec8bd6c5, 6ab4eb4c23c9e419fbba85884ea141f4, 97ce00c7ef1f7d98b48291d73d900181, 0873b5744d8ab6e3fe7c9754cf7761a3, 0ecf4bac2b070cf40f0b17e18ce312e6, 17c46ed7b80c2e4dbea6d0e88ea0827c, 1f2410c3c25dadf9e0943cd634558800, 2968c20a07cfc97a167aa3dd54124cda, 33e85d0f3ef2020cdb0fc3c8d80e8e69, 4118d9adce7350c3eedeb056a3335346, 4aa57e1c66c2e01f2da3f106ed2303fa, 58ad3103295afcc22bde8d81e77c282f, 5c41cbf8a7620e10f158f6b70963d1cb, 61a949553d35f31957db6442f36730c5, 72a22afde3f820422cfdbba7a4cbabde, 84bd45e223b018e67e4662c057f2c47e, 86465d92f0d690b62866f52f5283b9fc, 8b395cc6ecdec0900facf6e93ec48fbb, 97f352e2808c78eef9b31c758ca13032, a50f3b7aa11b977ae89285b60968aa67, afd25ce56b9808c5ed7eade75d2e12a7, afdeb24975a318fc5f20d9e61422a308, b697b81b341692a0b137b2c748310ea7, bcac28919fa33704a01d7a9e5e3ddf3f, c892c60817e6399f939987bd2bf5dee0, d0f310c99476f1712ac082f78dd29fdc, d8da33fae924b991b776797ba8cde24c, e230c5728f9ea5a94e390e7da7bf1ffa, f4d46629ca15313b94992f3798718df7, fb84a392601fc19aeb7f8ce11b3a4907, ff3194d3d5810a42858f3e22c91500b1, 13b4ce1fc26d400d34ede460a8530d93, 41895c5416fdc82f7e0babc6bb6c7216, c2f8c9bb7df688d0a7030a96314bb493, 33a3da2de78418b89a603e28a1e8852c, 4896da30a745079cd6265b6332886d45, 73eb2f4f101aab6158c615094f7a632a, 7f33d2d2a2ce9c195202acb59de31eee, e1afd01400ef405e46091e8ef10c721c,

TYPE	VALUE
MD5	fe25c192875ec1914b8880ea3896cda2, 232586f8cfe82b80fd0dfa6ed8795c56, c1f266f7ec886278f030e7d7cd4e9131, 49bb2ad67a8c5dfbfe8db2169e6fa46e, beb199b15bd075996fa8d6a0ed554ca8, 4053ca3e37ed1f8d37b29eed61c2e729, 3a0c8ae783116c1840740417c4fbe678, 0414a2ab718d44bf6f7103cff287b312, ca564428a29faf1a613f35d9fa36313f, ad6d4eb34d29e350f96dc8df6d8a092e, dc70dc9845aa747001ebf2a02467c203, 3d2ec58f37c8176e0dbcc47ff93e5a76, 0a09b7f2317b3d5f057180be6b6d0755, 1ffccc23fef2964e9b1747098c19d956, 9112efb49cae021abebd3e9a564e6ca4, ac0ada011f1544aa3a1cf27a26f2e288, 0211a3160cc5871cbcd4e5514449162b, 7416ea48102e2715c87edd49ddbd1526, a2aefb7ab6c644aa8eeb482e27b2dbc4, e7fd7f48fbf5635a04e302af50dfb651, 33b2b5b7c830c34c688cf6ced287e5be, e5410abaaac69c88db84ab3d0e9485ac, eb35b75369805e7a6371577b1d2c4531, 5a3f3f75048b9cec177838fb8b40b945, 9d7bd0caed10cc002670faff7ca130f5, 8434cdd34425916be234b19f933ad7ea, bbaee4fe73ccff1097d635422fdc0483, 79e474e056b4798e0a3e7c60dd67fd28, 95c276215dcc1bd7606c0cb2be06bf70, 426bb55531e8e3055c942a1a035e46b9, cfae52529468034dbbb40c9a985fa504, deae4be61c90ad6d499f5bdac5dad242, bda0686d02a8b7685adf937cbcd35f46, 6de6c27ca8f4e00f0b3e8ff5185a59d1, c61a8c4f6f6870c7ca0013e084b893d2, 5291aed100cc48415636c4875592f70c, f4795f7aec4389c8323f7f40b50ae46f, cf1a90e458966bcba8286d46d6ab052c, 792370eb01e16ac3dc511143932d0e1d, 612538328e0c4f3e445fb58ef811336a, b22fd0604c4f189f2b7a59c8f48882dd, e53ca714787a86c13f07942a56d64efa, c7b09f1dd0a5694de677f3ecceda41b7, c8346b39418f92725719f364068a218d, 730bff14e80ffd7737a97cdf11362ab5, 9a481bc83fea1dea3e3bdfff5e154d44, ddb1f970371fa32faae61fc5b8423d4b, 977d30b261f64cc582b48960909d0a89, 7ce51b56a6b0f8f78056ddfc5b5de67c, ecb4a09618e2aba77ea37bd011d7d7f7,

TYPE	VALUE
MD5	0fd8c6f56c52c21c061a94e5765b27b4, c90d094a8fbeaa8a0083c7372bfc1897, 55bb271bbbf19108fec73d224c9b4218, 0c046a2f5304ed8d768795a49b99d6e4, f34664e0d9a10974da117c1ca859dba8, a2c2099d503fcc29478205f5aef0283b, e439f850aa8ead560c99a8d93e472225, 81738405a7783c09906da5c7212e606b, eb7ba9f7424dffdb7d695b00007a3c6d, 073e3170a8e7537ff985ec8316319351, 9b0e7c460a80f740d455a7521f0eada1, 2d02f5499d35a8dffb4c8bc0b7fec5c2, 0984954526232f7d05910aa5b07c5893, 4156a7283284ece739e1bae05f99e17c, 3026d419ee140f3c6acd5bff54132795, 7aa132c0cc63a38fb4d1789553266fc7, 1a0811472fad0ff507a92c957542fffd, f8aef59d0c5afe8df31e11a1984fbc0a, 82491b42b9a2d34b13137e36784a67d7, 0a199944f757d5615164e8808a3c712a, 9c97ea18da290a6833a1d36e2d419efc, 16f768eac33f79775a9672018e0d64f5
SHA256	0c5e0a81efc0ccc406e5e6eaa222a79b491f4aa2938cf7cc72d0d027b53a9d99, 0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f, 1177105e51fa02f9977bd435f9066123ace32b991ed54912ece8f3d4fbeeade4, 152743ffa9df246e5f8c5687381121d8a66dfc05ca2ec2e58000caf964abafc2, 16db0063e4aa666d94752414549fa09fb33142481d894b01a0fae45b339a09fb, 2e500b2f160f927b1140fb105b83300ca21762c21bb6195c44e8dc613f7d7b12, 2eb16dbc1097a590f07787ab285a013f5fe235287cb4fb948d4f9cce9efa5dbc, 3cf63d516c580d8f988aa4f9b7d482bbdf3901dce435356dbca83eb311c32382, 42daf0f3080b50a0a1f14291f5ae3fa8fa400d838a915618f68a8f059777bcd4, 4e5e42b1acb0c683963caf321167f6985e553af2c70f5b87ec07cc4a8c09b4d8, 0c5e0a81efc0ccc406e5e6eaa222a79b491f4aa2938cf7cc72d0d027b53a9d99, 58fef66f346fe3ed320e22640ab997055e54c8704fc272392d71e367e2d1c2bb, 60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145,

TYPE	VALUE
SHA256	6319102bac226dfc117c3c9e620cd99c7eafbf3874832f2ce085850aa042f19c, 655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae, 6ca3c2a6001f1149ff75ab46402dee40d97602bab0b43ac144ca70fbd2101404, 782791c9ec3550cd522fd27b992e75381d5c5bc4d95b2f3934f9af6b6d5a57f4, 789c3aeb31700b078f6449cb310b4a2b7d8c03aefeed46a69b1dcb40a18001a7, 846c2a02505dc1463019cabc021969f7f6095215efb63ec374da1d055e778390, 8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b, 8bc74559c3678d299826755f29d5ba75b1148b0f8d1fa71a120b2f879f85f08b, 90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4, a0a0b0dd33b5b685317f6abe7b4caf0610938f548f6d178919bf43c24e1a3a4b, a1990d863e0b5c7661358dab72ce9223e2d54570915105707374ea8cf68828bd, ac5e0ec03658a281bb57e8b1b17f1fa1da2c819a373524577459c63b0b9d9a75, afb2d4d88f59e528f0e388705113ae54b7b97db4f03a35ae43cc386a48f263a0, b7435d23769e79fcbe69b28df4aef062685d1a631892c2354f96d833eae467be, c28bb61de4a6ad1c5e225ad9ec2eaf4a6c8ccfff40cf45a640499c0adb0d8740, c8fb5988ad3f71412cb5b4f1248df7ddf82c8c5f3dce60c73c4787b6e443b7b0, c9724eecab6cfb1c312d4538630fdac0d30434c0cffa131f9190e5a76bef6304, cb4d45338798b97177d8d96eea82dae22481dada40174dda0386026d11136209, d30abdf9db88da8a23dccb8188cd4caff48bc437bb3eb3ad576a013ff675161a, e263aa0e7e6a6a1d59677eaf2d4ccb848fe65a84035ab4f24c4e26a1ab089c79, e8e61112e8b896ad00ddefb42feb33e5d0fc38d2fb462b9f980606fe79d42571, ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6, f5f6e538001803b0aa008422caf2c3c2a79b2eeee9ddc7feda710e4aba96fea4, f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7,

TYPE	VALUE
SHA256	f93ddb2377e02b0673aac6d540a558f9e47e611ab6e345a39fd9b1ba9f37cd22, db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984, 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df, 05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d, e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe, 1962ebb7bf8d2b306c6f3b55c3dcd69a755eeff1a17577b7606894b781841c3a, f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb, 6db57bbc2d07343dd6ceba0f53c73756af78f09fe1cb5ce8e8008e5e7242eae1, 66415464a0795d0569efa5cb5664785f74ed0b92a593280d689f3a2ac68dca66, def2f01fbd4be85f48101e5ab7ddd82efb720e67daa6838f30fd8dcda1977563, 323cbe7a3d050230cfaa822c2a22160b4f8c5fe65481dd329841ee2754b522d9, 74529dd15d1953a47f0d7ecc2916b2b92865274a106e453a24943ca9ee434643, 1e4de822695570421eb2f12fdfe1d32ab8639655e12180a7ab3cf429e7811b8f, 8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5, c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f, dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469, 452ca47230afd4bb85c45af54fcacbfa544208ef8b4604c3c5caefe3a64dcc19, 199ba618efc6af9280c5abd86c09cdf2d475c09c8c7ffc393a35c3d70277aed1, ce779e30502ecee991260fd342cc0d7d5f73d1a070395b4120b8d300ad11d694, 34d5a5d8bec893519f204b573c33d54537b093c52df01b3d8c518af08ee94947, 664f8d19af3400a325998b332343a9304f03bab9738ddab1530869eff13dae54, 772b06f34facf6a2ce351b8679ff957cf601ef3ad29645935cb050b4184c8d51, aa29bf4292b68d197f4d8ca026b97ec7785796edcb644db625a8f8b66733ab54, 9a5504dcfb7e664259bfa58c46cfd33e554225daf1cedea2ec2a9d83bbbfe238, c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c, 38f0f2d658e09c57fc78698482f2f638843eb53412d860fb3a99bb6f51025b07

TYPE	VALUE
SHA1	3c5f4caf1a9d08d939a7d31f5ddb232806746b56, f632336918ab18ba397a5dd2f956d58c58a5f6ab, d35ee806e383e2aac359d8c29174505ac123fceb, fec0156d8cc2e4bca6ed943b361b99a978c8409a, 9076b865017a06a5f1ce918896f592c237ccaf44, 596977d016edc850f3dfccc91296724c68bc22f2, a058be590bdbe6f6e1781bbaf555da0aa32902f1, 630e8bcade0d273eb6499aa681dfe8377eb51655, a4e5925b566684b6530613fe1ab0df49ce9b6e2b, 6799f1fbf3ebb1cbf9962aedeec58d2fd551ee42, 3c5f4caf1a9d08d939a7d31f5ddb232806746b56, f632336918ab18ba397a5dd2f956d58c58a5f6ab, d35ee806e383e2aac359d8c29174505ac123fceb, fec0156d8cc2e4bca6ed943b361b99a978c8409a, 9076b865017a06a5f1ce918896f592c237ccaf44, 596977d016edc850f3dfccc91296724c68bc22f2, a058be590bdbe6f6e1781bbaf555da0aa32902f1, 630e8bcade0d273eb6499aa681dfe8377eb51655, a4e5925b566684b6530613fe1ab0df49ce9b6e2b, bad180a18e0ffd789eafcff14be48c8a67c8dc4f, feb79a5a2bdf0bcf0777ee51782dc50d2901bb91, 5d83eb9efbf6e9dfdb704f7e14b968e767403abf, 2a7433dc09218ba98c0e530bb8a76f5f2a05005b, 0768165c77d91993ca64f3ad9c756c0483cbc763, 5a1878d0eea07c514da9256e0c378eb0f79ca325, 55e1b54424fde8f2ab93d75e97ced908757072d5, e5ea8cb6dc3c090530fc88424ee6f26ccc3875c4, 67f9a8047d21b8e8261dce1d699e3377b7abeb5d, 7bd97c0c277f4b3e73784a6a38d18e83bce8002f, a6d63439404b38f28606566f8b95298c624bc1e1, 29a7cd7ac2bb8c6d0fc02ddec05d7867607e293f, 0c998e4a5ba1d2d7d39532380d3d55a76ddf9e7d, d9b1e15bbfdb0ded59de8d7bb6a387ef641bffd1, 01a5e1c618fced0173e666ce8debd6027725806e, 8caff714b0a10d9bf36297a1fc0b4aaf71063a1d, 9b0156f0fa11a9ecd0f676727040763f157cbae0, 9e123e022f97f7b0d35c0dd148c45a8d27ead334, 6624fa0b0a3fb9a83ce1f98705964bc1b7e77a89, f0f33f02b3fe363b629f4bea14651b1f6684cb1d, 793d959e047486be9738521908a3383364a009a2, 71be418950af763c50595fb3cc0bed0309c16cb0, 09f61bf55f552246c98bdba61b8e83015e9b2548, f141f9dfc7e082521c9d26980bfc8bf100bb2f61, 3b665481a57096c026c5dcb62be17eb1714dc4c0, e1ff89f8b2830778ee9bdae64ab94fc64d16af5a, 8bab70bdfb7f8df0356727d9cb3c6024acb383a2

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	✓	✓	✓
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	JetBrains TeamCity	✗	✓	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-35078	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✓	✓	✓
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	Apache RocketMQ	✗	✓	✓
CVE-2023-32784	KeePass Password Dump Vulnerability	KeePass	✗	✗	✓
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Ignite Realtime Openfire	✗	✓	✓
CVE-2023-3079	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	✓	✓	✓
CVE-2023-28771	Zyxel Multiple Firewalls OS Command Injection Vulnerability	Zyxel Multiple Firewalls	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-33010	Zyxel Multiple Firewalls Buffer Overflow Vulnerability	Zyxel Multiple Firewalls	✗	✓	✓
CVE-2023-2868	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	Barracuda Networks Email Security Gateway (ESG) Appliance	✓	✓	✓
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN	✓	✓	✓
CVE-2023-25690	Apache HTTP Smuggling Vulnerability	Apache	✗	✗	✓
CVE-2023-21932	Oracle Unauthorized Access Vulnerability	Oracle Hospitality OPERA 5 Property Services	✗	✗	✓
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine	✗	✓	✓
CVE-2022-41352	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	Zimbra Collaboration (ZCS)	✓	✓	✓
CVE-2022-27925	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	Zimbra Collaboration (ZCS)	✗	✓	✓
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2022-25064	TP-LINK Remote Code Execution Vulnerability	TP-LINK	✗	✗	✗
CVE-2022-24990	TerraMaster OS Remote Command Execution Vulnerability	TerraMaster	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-45837	TerraMaster Remote Code Execution Vulnerability	TerraMaster	✗	✗	✗
CVE-2022-24785	Moment.js Path Traversal Vulnerability	Moment.js	✗	✗	✓
CVE-2022-24665	PHP Everywhere Code Injection Vulnerability	PHP	✗	✗	✓
CVE-2022-22965	Spring Framework JDK 9+ Remote Code Execution Vulnerability	VMware Spring Framework	✓	✓	✓
CVE-2022-22947	VMware Spring Cloud Gateway Code Injection Vulnerability	VMware Spring Cloud Gateway	✓	✓	✓
CVE-2022-22005	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2022-21882	Microsoft Win32k Privilege Escalation Vulnerability	Microsoft Win32k	✓	✓	✓
CVE-2021-44142	Samba Code Execution vulnerability	Samba	✗	✗	✓
CVE-2021-43226	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows	✗	✗	✓
CVE-2021-41773	Apache HTTP Server Path Traversal Vulnerability	Apache HTTP Server	✓	✓	✓
CVE-2021-40684	Talend ESB Remote Code Execution Vulnerability	Talend ESB	✗	✗	✓
CVE-2021-3018	IPeakCMS SQL Injection Vulnerability	IPeakCMS	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	SonicWall SMA 100 Appliances	✗	✓	✓
CVE-2021-20028	SonicWall Secure Remote Access (SRA) SQL Injection Vulnerability	SonicWall Secure Remote Access (SRA)	✗	✓	✓
CVE-2019-15637	Tableau XXE Vulnerability	Tableau	✗	✗	✓
CVE-2019-7609	Kibana Arbitrary Code Execution	Elastic Kibana	✗	✓	✓
CVE-2019-0708	Microsoft Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Remote Desktop Services	✗	✓	✓
CVE-2017-4946	VMware V4H and V4PA Privilege Escalation Vulnerability	VMware V4H and V4PA	✗	✗	✓

Patch Links

https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.15.0/

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

https://blog.jetbrains.com/teamcity/2023/09/cve-2023-42793-vulnerability-post-mortem/

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

https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

https://github.com/vdohney/keepass-password-dumper?tab=readme-ov-file

https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm

https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop.html

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-307

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/U4OXTNIZY4JYHJT7CVLPAJQILI6BISVM/

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/DYTXO5E3FI3I2ETDP3HF4SHYYTFMKMIC/

https://www.debian.org/security/2023/dsa-5420

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls

https://status.barracuda.com/incidents/34kx82j5n4q9

https://www.helpnetsecurity.com/2023/06/11/cve-2023-27997/

https://httpd.apache.org/security/vulnerabilities_24.html

https://lists.debian.org/debian-lts-announce/2023/04/msg00028.html

https://www.ibm.com/support/pages/security-bulletin-ibm-http-server-vulnerable-http-request-splitting-due-included-apache-http-server-cve-2023-25690

https://www.ibm.com/support/pages/security-bulletin-vulnerability-apache-http-server-cve-2023-25690-affects-power-hmc

https://www.oracle.com/security-alerts/cpuapr2023.html

https://duo.com/decipher/fortra-patches-actively-exploited-zero-day-in-goanywhere-mft

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

https://forum.terra-master.com/en/viewforum.php?f=28

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24990

https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4

https://lists.debian.org/debian-lts-announce/2023/01/msg00035.html

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6QIO6YNLTK2T7SPKDS4JEL45FANLNC2Q/

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ORJX2LF6KMPIHP6B2P6KZIVKMLE3LVJ5/

https://www.rapid7.com/db/vulnerabilities/ubuntu-cve-2022-24785/

https://www.ibm.com/support/pages/security-bulletin-vulnerability-nodejs-momentjs-affect-cloud-pak-system-cve-2022-24785

https://access.redhat.com/security/cve/CVE-2022-24785

https://spring.io/security/cve-2022-22947

https://www.microsoft.com/downloads/details.aspx?familyid=e66ce694-33fb-41c6-ac72-535d3d6c579d

https://www.microsoft.com/downloads/details.aspx?familyid=9062c391-efc6-40d0-b679-e7a31d2bb294

https://www.microsoft.com/downloads/details.aspx?familyid=931bc018-8f42-4e39-ae81-ebdb7e4180f3

https://www.microsoft.com/downloads/details.aspx?familyid=977f2baf-941b-423a-bc79-8383a844310a

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5009543

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5009545

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5009566

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5009555

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5009557

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-43226

https://www.talend.com/security/incident-response/#cve-2021-40684

https://www.fortiguard.com/psirt/FG-IR-22-377

https://github.com/M4DM0e/m4dm0e.github.io/blob/gh-pages/_posts/2020-12-07-ipeak-cms-sqli.md

https://community.tableau.com/s/news/a0A4T000001v3QsUAI/important-adv2019030-xxe-vulnerability-in-tableau-products

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23532

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-008

https://customerconnect.vmware.com/patch

https://www.tableau.com/support/releases

https://jira.talendforge.org/browse/SF-141

https://www.fortiguard.com/psirt/FG-IR-22-377

https://ipeak.ch/en/

https://github.com/moment/moment/blob/develop/CHANGELOG.md

https://security-tracker.debian.org/tracker/CVE-2022-24785

https://bodhi.fedoraproject.org/updates/FEDORA-2022-85aa8e5706

https://bodhi.fedoraproject.org/updates/FEDORA-2022-35b698150c

https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-August/006723.html

https://www.ibm.com/support/pages/security-bulletin-vulnerability-nodejs-momentjs-affect-cloud-pak-system-cve-2022-24785

https://access.redhat.com/security/cve/CVE-2022-24785

https://keepass.info/news/n230603_2.54.html

https://httpd.apache.org/security/vulnerabilities_24.html

https://security-tracker.debian.org/tracker/CVE-2023-25690

https://exchange.xforce.ibmcloud.com/vulnerabilities/249287?_ga=2.53797423.626329635.1722332376

https://support.oracle.com/rs?type=doc&id=2935379.1

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

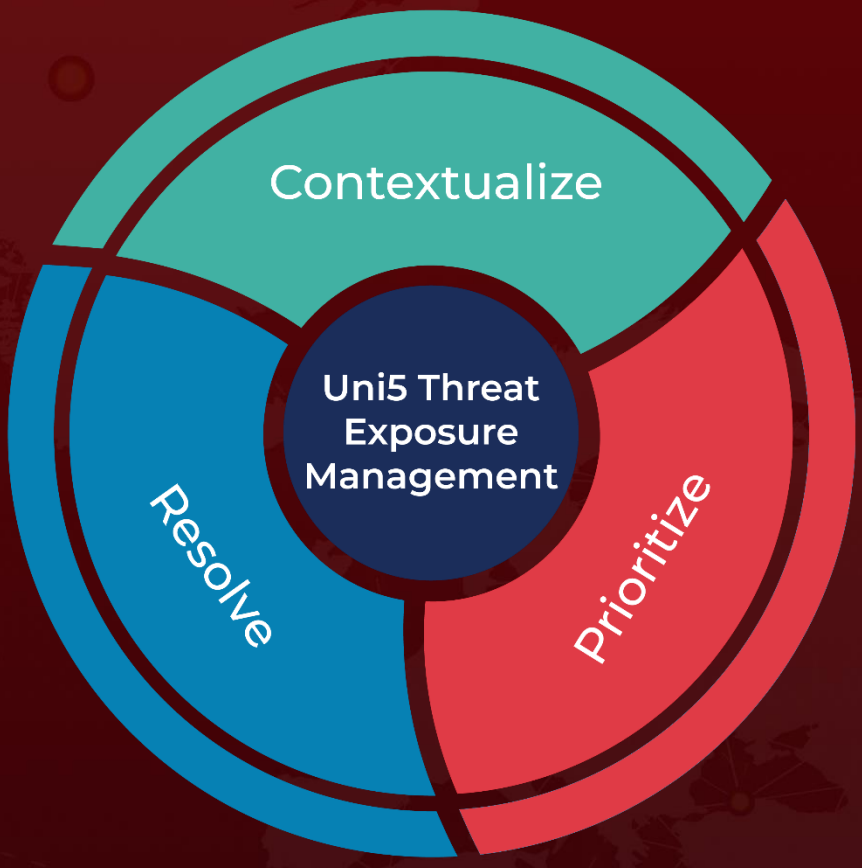
https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

https://www.fbi.gov/wanted/cyber/rim-jong-hyok

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

July 30, 2024 • 9:30 PM

More at www.hivepro.com