Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Malicious DPRK Actors Target the Healthcare Industry in the US & South Korea

Date of Publication

February 28, 2023

Admiralty Code

A1

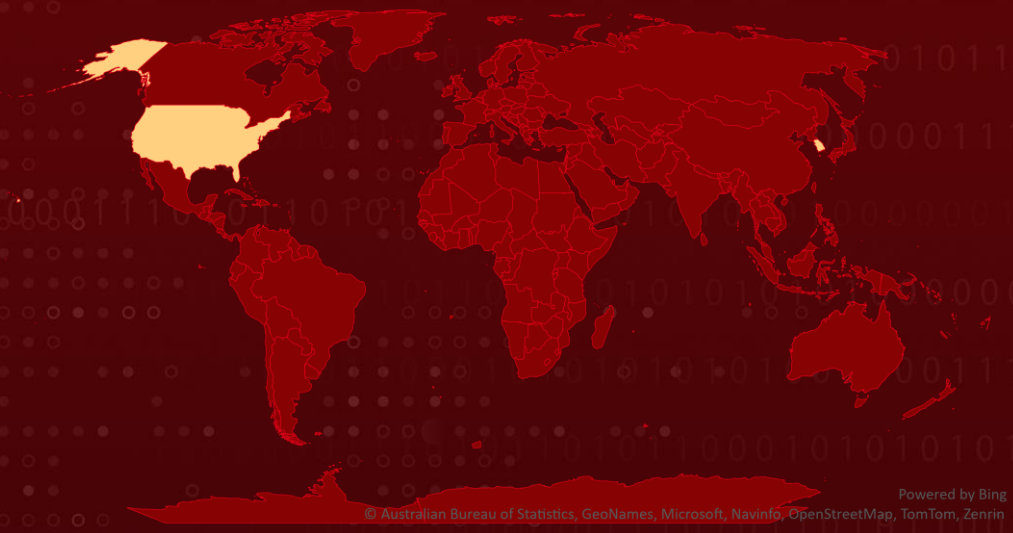
TA Number

TA2023108

Summary

Attack Begin: May 2021
Affected Industry: Healthcare
Attack Regions: United States & South Korea
Attack: State-sponsored actors from the Democratic People's Republic of Korea (DPRK) have carried out a ransomware attack against the healthcare systems of South Korea and the United States.

Attack Regions



CVEs

CVE	NAME	PATCH
CVE-2021-44228	Apache Log4j2 Remote Code Execution	✓
CVE-2021-20038	SonicWall Appliances Stack-Based Buffer Overflow	✓
CVE-2022-24990	TerraMaster OS Remote Command Execution	✓

Attack Details

#1

The Democratic People's Republic of Korea (DPRK) state-sponsored actors have a well-planned attack path for their ransomware operations. First, they create domains, personas, and accounts and identify cryptocurrency services to conduct their operations. They use cryptocurrency generated through illicit cybercrime activities, like ransomware and cryptocurrency theft, to purchase infrastructure, IP addresses, and domains. To obfuscate their involvement, the DPRK actors operate with or under third-party foreign affiliate identities and use third-party foreign intermediaries to receive ransom payments. They also purchase VPNs, VPSs, or use third-country IP addresses to appear to be from innocuous locations instead of from DPRK.

#2

Once they gain access to the target's network, DPRK actors use various exploits of common vulnerabilities and exposures (CVE) to escalate privileges and gain access. They use staged payloads with customized malware to perform reconnaissance activities, upload and download additional files and executables, and execute shell commands. They also employ various ransomware tools, including publicly available tools for encryption, and demand ransom in cryptocurrency, mainly bitcoin. DPRK cyber actors communicate with victims via Proton Mail email accounts and may threaten to expose the company's proprietary data to competitors if ransoms are not paid.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0007 Discovery	TA0008 Lateral Movement
TA0010 Exfiltration	TA0040 Impact	T1486 Data Encrypted for Impact	T1083 File and Directory Discovery
T1021 Remote Services	T1195 Supply Chain Compromise	T1190 Exploit Public-Facing Application	T1133 External Remote Services
T1583 Acquire Infrastructure	T1583.003 Virtual Private Server		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	xpopup.pe[.]kr xpopup.com
IPV4	115.68.95[.]128 119.205.197[.]111
MD5	b6f91a965b8404d1a276e43e61319931 bdece9758bf34fcad9cba1394519019b c3850f4cc12717c2b54753f8ca5d5e0e c50b839f2fc3ce5a385b9ae1c05def3a cf236bf5b41d26967b1ce04ebbdb4041 d0e203e8845bf282475a8f816340f2e8 ddb1f970371fa32faae61fc5b8423d4b f2f787868a3064407d79173ac5fc0864 fda3a19afa85912f6dc8452675245d6b a2c2099d503fcc29478205f5aef0283b 9c516e5b95a7e4169ecbd133ed4d205f d6a7b5db62bf7815a10a17cdf7ddbd4b c6949a99c60ef29d20ac8a9a3fb58ce5 4b20641c759ed563757cdd95c651ee53 25ee4001eb4e91f7ea0bc5d07f2a9744 29b6b54e10a96e6c40e1f0236b01b2e8 18126be163eb7df2194bb902c359ba8e eaf6896b361121b2c315a35be837576d

TYPE	VALUE
MD5	079b4588eaa99a1e802adf5e0b26d8aa 0e9e256d8173854a7bc26982b1dde783 12c15a477e1a96120c09a860c9d479b3 131fc4375971af391b459de33f81c253 17c46ed7b80c2e4dbea6d0e88ea0827c 1875f6a68f70bee316c8a6eda9ebf8de 1a74c8d8b74ca2411c1d3d22373a6769 1f6d9f8fbdbbd4e6ed8cd73b9e95a928 2d02f5499d35a8dffb4c8bc0b7fec5c2 2e18350194e59bc6a2a3f6d59da11bd8 3bd22e0ac965ebb6a18bb71ba39e96dc 40f21743f9cb927b2c84ecdb7dfb14a6 4118d9adce7350c3eedeb056a3335346 43e756d80225bdf1200bc34eef5adca8 47791bf9e017e3001ddc68a7351ca2d6 505262547f8879249794fc31eea41fc6 5130888a0ad3d64ad33c65de696d3fa2 58ad3103295afcc22bde8d81e77c282f 5be1e382cd9730fbe386b69bd8045ee7 5c6f9c83426c6d33ff2d4e72c039b747 640e70b0230dc026eff922fb1e44c2ea 67f4dad1a94ed8a47283c2c0c05a7594 70652edadedbacfd30d33a826853467d 739812e2ae1327a94e441719b885bd19 76c3d2092737d964dfd627f1ced0af80 802e7d6e80d7a60e17f9ffbd62fcbbeb 827103a6b6185191fd5618b7e82da292 830bc975a04ab0f62bfedf27f7aca673 85995257ac07ae5a6b4a86758a2283d7 85f6e3e3f0bdd0c1b3084fc86ee59d19 87a6bda486554ab16c82bdfb12452e8b 891db50188a90ddacfaf7567d2d0355d 894de380a249e677be2acb8fbdfba2ef 8b395cc6ecdec0900facf6e93ec48fbb 92a6c017830cda80133bf97eb77d3292 9b0e7c460a80f740d455a7521f0eada1 9b9d4cb1f681f19417e541178d8c75d7 a1f9e9f5061313325a275d448d4ddd59 a452a5f693036320b580d28ee55ae2a3 a6e1efd70a077be032f052bb75544358 ad4eababfe125110299e5a24be84472e b1c1d28dc7da1d58abab73fa98f60a83

TYPE	VALUE
MD5	e4ee611533a28648a350f2dab85bb72a e268cb7ab778564e88d757db4152b9fa 1f239db751ce9a374eb9f908c74a31c9 6fb13b1b4b42bac05a2ba629f04e3d03 cf8ba073db7f4023af2b13dd75565f3d 4e71d52fc39f89204a734b19db1330d3 43d4994635f72852f719abb604c4a8a1 5ae71e8440bf33b46554ce7a7f3de666
File Names	x-PopUp.exe xpopup.exe xpopup.rar
SHA256	99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd F8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86 Bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af 6e20b73a6057f8ff75c49e1b7aef08abfcfe4e418e2c1307791036f081335c2d f4d10b08d7dacd8fe33a6b54a0416eecdaed92c69c933c4a5d3700b8f5100fad 541825cb652606c2ea12fd25a842a8b3456d025841c3a7f563655ef77bb67219 2d978df8df0cf33830aba16c6322198e5889c67d49b40b1cb1eb236bd366826d 414ed95d14964477bebf86dced0306714c497cde14dede67b0c1425ce451d3d7 99b448e91669b92c2cc3417a4d9711209509274dab5d7582baacfab5028a818c 60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145 f6375c5276d1178a2a0fe1a16c5668ce523e2f846c073bf75bb2558fdec06531 dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469 92adc5ea29491d9245876ba0b2957393633c9998eb47b3ae1344c13a44cd59ae 151ab3e05a23e9ccd03a6c49830dabb9e9281faf279c31ae40b13e6971dd2fb8 1c926fb3bd99f4a586ed476e4683163892f3958581bf8c24235cd2a415513b7f 1f8dcfaebbcd7e71c2872e0ba2fc6db81d651cf654a21d33c78eae6662e62392 38491f48d0cbaab7305b5ddca64ba41a2beb89d81d5fb920e67d0c7334c89131

TYPE	VALUE
SHA256	Df0c7bb88e3c67d849d78d13cee30671b39b300e0cda5550280350775d5762d8 5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e 45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78 56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19 830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570 458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456 99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f 3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878 87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6 0054147db54544d77a9efd9baf5ec96a80b430e170d6e7c22fcf75261e9a3a71 f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7 6263e421e397db821669420489d2d3084f408671524fd4e1e23165a16dda2225 b9af4660da00c7fa975910d0a19fda072031c15fad1eef935a609842c51b7f7d 672ec8899b8ee513dbfc4590440a61023846ddc2ca94c88ae637144305c497e7 ba8f9e7afe5f78494c111971c39a89111ef9262bf23e8a764c6f65c818837a44 4f089afa51fd0c1b2a39cc11cedb3a4a326111837a5408379384be6fe846e016 655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae 6b7f566889b80d1dba4f92d5e2fb2f5ef24f57fcfd56bb594978dffe9edbb9eb 5081f54761947bc9ce4aa2a259a0bd60b4ec03d32605f8e3635c4d4edaf48894 afb2d4d88f59e528f0e388705113ae54b7b97db4f03a35ae43cc386a48f263a0 863b707873f7d653911e46885e261380b410bb3bf6b158daefb47562e93cb657 f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c c92c1f3e77a1876086ce530e87aa9c1f9cbc5e93c5e755b29cad10a2f3991435

TYPE	VALUE
SHA256	18b75949e03f8dcad513426f1f9f3ca209d779c24cd4e941d935633b1bec00cb 5ad106e333de056eac78403b033b89c58b4c4bdda12e2f774625d47ccfd3d3ae a3b7e88d998078cfd8cdf37fa5454c45f6cbd65f4595fb94b2e9c85fe767ad47 6319102bac226dfc117c3c9e620cd99c7eafbf3874832f2ce085850aa042f19c 3fe624c33790b409421f4fa2bb8abfd701df2231a959493c33187ed34bec0ae7 196fb1b6eff4e7a049cea323459cfd6c0e3900d8d69e1d80bffbaabd24c06eba 6122c94cbfa11311bea7129ecd5aea6fae6c51d23228f7378b5f6b2398728f67 bffe910904efd1f69544daa9b72f2a70fb29f73c51070bde4ea563de862ce4b1 f1576627e8130e6d5fde0dbe3dffcc8bc9eef1203d15fcf09cd877ced1ccc72a 980bb08ef3e8afcb8c0c1a879ec11c41b29fd30ac65436495e69de79c555b2be 0837dd54268c373069fc5c1628c6e3d75eb99c3b3efc94c45b73e2cf9a6f3207 d1aba3f95f11fc6e5fec7694d188919555b7ff097500e811ff4a5319f8f230be f5f6e538001803b0aa008422caf2c3c2a79b2eeee9ddc7feda710e4aba96fea4 dfdd72c9ce1212f9d9455e2bca5a327c88d2d424ea5c086725897c83afc3d42d A557a0c67b5baa7cf64bd4d42103d3b2852f67acf96b4c5f14992c1289b55eaa 9d6de05f9a3e62044ad9ae66111308ccb9ed2ee46a3ea37d85afa92e314e7127

Patch Links

https://logging.apache.org/log4j/2.x/security.html

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

https://forum.terra-master.com/en/viewtopic.php?t=3030

References

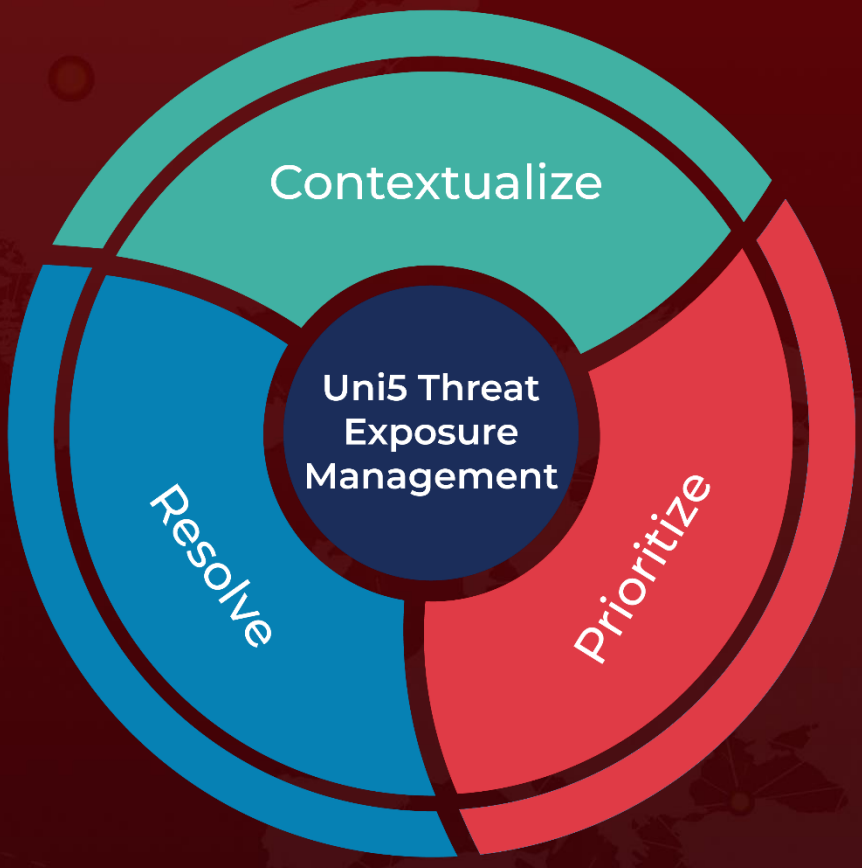
https://www.cisa.gov/news-events/alerts/2023/02/09/stopransomware-ransomware-attacks-critical-infrastructure-fund-dprk-espionage-activities

https://www.hivepro.com/north-korean-state-sponsored-actors-employ-maui-ransomware-to-target-the-health-care-industry/

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

February 28, 2023 . 6:30 AM

More at www.hivepro.com