Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

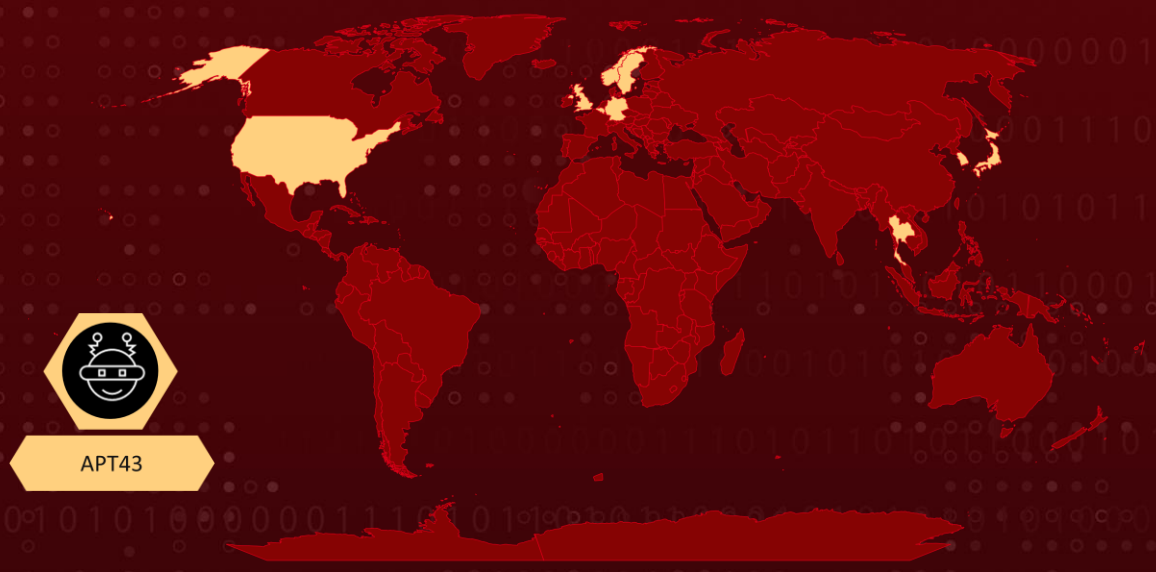
Unraveling North Korea's Cyber Espionage Group APT43 Targeting Geopolitical Interests

Date of Publication	Admiralty code	TA Number
April 4, 2023	A1	TA2023169

Summary

First Appearance: June 2018
Actor Name: APT43
Target Countries: United States, Germany, Belgium, United Kingdom, Sweden, Norway, Thailand, South Korea, Japan
Target Sectors: NGOs, Education, Governments, Media and entertainment, Construction, Materials, Defense, Aerospace, Telecoms, High-tech , Pharmaceuticals, Consulting and Professional services

Actor Map



Actor Details

#1 APT43 is a cyber espionage group that serves North Korean regime interests by targeting government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues, mainly in South Korea and the US. The group uses social engineering tactics and moderately advanced technical capabilities, funding its primary mission of collecting strategic intelligence through cybercrime operations. To purchase operational tooling and infrastructure, the group creates numerous fake personas and cover identities.

#2 The group collects strategic intelligence that aligns with North Korea's geopolitical interests and engages in financially motivated cybercrime. APT43's intelligence collection priorities align with North Korea's foreign intelligence service, the Reconnaissance General Bureau, and focus on foreign policy and nuclear security issues that support North Korea's strategic and nuclear ambitions. In 2021, the group also targeted health-related verticals to support pandemic response efforts.

#3 APT43 is highly active in phishing and credential collection campaigns and coordinates with other North Korean cyber espionage groups. The group targets regions including South Korea, the US, Japan, and Europe, with campaigns aimed at enabling North Korea's weapons program. The group's activities strongly correlate with geopolitical developments that affect North Korean leader Kim Jong-un and the ruling elite and closely align with state interests.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
APT43	North Korea **MOTIVE** Information theft & Espionage; State-sponserd	United States, Germany, Belgium, United Kingdom, Sweden, Norway, Thailand, South Korea, Japan	NGOs, Education, Governments, Media and entertainment, Construction, Materials, Defense, Aerospace, Telecoms, High-tech , Pharmaceuticals, Consulting and Professional services

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 actor 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	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1583 Acquire Infrastructure	T1583.003 Virtual Private Server
T1584 Compromise Infrastructure	T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1588.004 Digital Certificates
T1608 Stage Capabilities	T1608.003 Install Digital Certificate	T1608.005 Link Target	T1047 Windows Management Instrumentation

T1053 Scheduled Task/Job	**T1053.005** Scheduled Task	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.003 Windows Command Shell	**T1059.005** Visual Basic	**T1059.007** JavaScript	**T1129** Shared Modules
T1203 Exploitation for Client Execution	**T1204** User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File
T1569 System Services	**T1569.002** Service Execution	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1071.004 DNS	**T1090** Proxy	**T1090.003** Multi-hop Proxy	**T1095** Non-Application Layer Protocol
T1102 Web Service	**T1102.002** Bidirectional Communication	**T1105** Ingress Tool Transfer	**T1132** Data Encoding
T1132.001 Standard Encoding	**T1573** Encrypted Channel	**T1573.002** Asymmetric Cryptography	**T1007** System Service Discovery
T1010 Application Window Discovery	**T1012** Query Registry	**T1016** System Network Configuration Discovery	**T1033** System Owner/User Discovery
T1057 Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery	**T1087** Account Discovery
T1518 Software Discovery	**T1614** System Location Discovery	**T1614.001** System Language Discovery	**T1056** Input Capture
T1056.001 Keylogging	**T1113** Screen Capture	**T1115** Clipboard Data	**T1213** Data from Information Repositories
T1560 Archive Collected Data	**T1560.001** Archive via Utility	**T1137** Office Application Startup	**T1505** Server Software Component
T1505.003 Web Shell	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1547.004** Winlogon Helper DLL	**T1547.009** Shortcut Modification	**T1027** Obfuscated Files or Information

T1027.001 Binary Padding	T1027.002 Software Packing	T1027.005 Indicator Removal from Tools	T1027.009 Embedded Payloads
T1036 Masquerading	T1036.001 Invalid Code Signature	T1036.007 Double File Extension	T1055 Process Injection
T1055.001 Dynamic-link Library Injection	T1055.003 Thread Execution Hijacking	T1070 Indicator Removal	T1070.004 File Deletion
T1070.006 Timestomp	T1112 Modify Registry	T1134 Access Token Manipulation	T1140 Deobfuscate/Decode Files or Information
T1218 System Binary Proxy Execution	T1218.005 Mshta	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks
T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control	T1553 Subvert Trust Controls	T1553.002 Code Signing
T1564 Hide Artifacts	T1564.003 Hidden Window	T1564.007 VBA Stomping	T1620 Reflective Code Loading
T1622 Debugger Evasion	T1489 Service Stop	T1529 System Shutdown/Reboot	T1020 Automated Exfiltration
T1110 Brute Force	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	982fc9ded34c85469269eacb1cb4ef26 de9a8c26049699dbbd5d334a8566d38d 144bd7fd423edc3965cb0161a8b82ab2 cd83a51bec0396f4a0fd563ca9c929d7 33df74cbb60920d63fe677c6f90b63f9 ebaf83302dc78d96d5993830430bd169 b846fa8bc3a55fa0490a807186a8ece9 f92a75b98249fa61cf62e8b63cb68fae 1dcd5afeccfe2040895686eefa0a9629 5fe4da6a1d82561a19711e564adc7589

TYPE	VALUE
MD5	e8da7fcdf0ca67b76f9a7967e240d223 2bf26702c6ecbd46f68138cdcd45c034 2d330c354c14b39368876392d56fb18c 15ec5c7125e6c74f740d6fc3376c130d 2a5562de1d3e734d9328a1c78b43c2e5 0cc0aa5877cec9109b7a5a0e3a250c72 2c530adb841114366ce6177ce964a5e6 c066b81c4b8b0703f81f8bc6fb432992 1d30dfa5d8f21d1465409b207115ded6 21cffaa7f9bf224ce75e264bfb16dd0d 20bc53deb7b1214580e9d9efeaa5e9d7 9cdda333432f403b408b9fe717163861 ddae18c65d583b41a2157d496a4bde61 1ffccf6cb3b74d68df2b899fd33127a5 60efecf4e1b5b2c580329e9afa05db15 0f77143ce98d0b9f69c802789e3b1713 0b558ee89a7bb32968ef78104f6b9a28 139d2561f5c72fabb099a12c16b8960c 14a00f517012279af53118a491253e5c 37e7d679cd4aa788ec63f27cb02962ea b077ba5af1dfbd4ac523923eab56bcd4 04d0856afb1aa9168377d6aa579c5403 4626ed60dfc8deaf75477bc06bd39be7 18df13900f118158c33df904c662e875 107f917a5ddb4d3947233fbc9d47ddc8 768c84100d6e3181a26fa50261129287 946f787c129bf469298aa881fb0843f4 c9d70bf370172609da848fa785989939 0085bc8ce16ef17643909c4799ead02b 68ce092f1a3d19852ea32db8388de5c7 7e609404cc258bbe283bea6ddd7af293 0821884168a644f3c27176a52763acc9 8ca84c206fe8436dcc92bf6c1f7cf168
SHA1	636f2c20183b45691b742949d49b3d6c218c9cce 1f6c7c9219f6b6ea30cd481968ae1a038789be67 6618e25dd49b68f7b2b266eb2d787e6f05c964bc 700acc4e48eae84f80f4dbaf74bf60b79efd49bd 25d94c9ab7635ff330dabe96780f330f7f2ba775 851ba2182b37bc7380420a986840e16f73947413 d3b233d6d8b11235929e4a0cbdb12eefdd47d927 e5b312155289cdc6a80a041821fc82d2cca80bcd 40826e2064b59b8b7b3e514b9ef2c1479ac3b038

TYPE	VALUE
SHA1	6f4b6938ac8fd9591fc399219dbaf4347d8b444b 75c516dde8415494c288e349d440ce778dede8e3 11f646095495d625e7d71038578cc838a6d5e111 a9ff1ebb548f5bba600d38e709ff331749fa9971 f3b774e921eaad9335b9c057dd49b918c5dae4a6 4e93797dd3b383050cf0ee585aa5b5525efb2380 7d66c1f36b4b48d990461ec44d626793ade6a8d1 98040f42103ce3b840dd54bf3490587f141a0bc3 2dd269608dd7f4da171d1a220fe97347162008c7 b7fdb5e5b31adfc5ada0de1e05b0c069968e5bce 7da4e8b743478370fa41fe39a45e3ff2ca2194b3 12c508ace6e8aa42be02750d759e720b800bf796 a61f009e73ae81a18751e9aee39f8121a3902280 63e113f0a906af82903dbfac3e78bdd2d146e738 d80be054a569df5f201191dcc4fea0dde9622da5 e74b816f1c6d6347cb40121e0b50dadd0d8f1f97 862abce03f7f5de0c466fdbd24ad796578eaa110 942fd7b4ef1ccf7032a40acad975c7b5905c3c77 2508f5ff0c28356c0c3f8e6cae7b750d53495bca 5b69e3e5f4f49cf8b635a57a8c92e17a4f130d50 1d49d462a11a00d8ac9608e49f055961bf79980d 4b0d0ebb0c676efe855bed796221dd475a39ba40 47a32bc992e5d4613b3658b025ab913b0679232c e205ed81ccb99641dcc6c2799d32ef0584fa2175 1087efbd004f65d226bf20a52f1dc0b3e756ff9e f3b047e6eb3964deb047767fad52851c5601483f 539acd9145befd7e670fe826c248766f46f0d041 bc6cb78e20cb20285149d55563f6fdcf4aaafa58 c0c6b99796d732fa53402ff49fd241612a340229 e79527f7307c1dda62c42487163616b3e58d5028 1b9a4c0a5615a4f96a041d771646c1a407b17577 b0c2312852d750c4bceb552def6985b8b800d3f3 a1f72c890d0b920f4f4cb2d59df6fa40734de90d fb09b89803da071b7b7eb23244771c54d979a873
SHA256	25c2f4703cbaa1ff4dbcfcc16a10b29ef35ccc174b71b21de360d898 540889f8 502136707a70b768800640224e48c634057dc651892113b62522f0 dd2fcf1e87 e7fae41c0bd8d3d95253bd75dce99015599ecc404bd8d737cec305f c3e4dd018 7943bf9cc7b2adf50f7f92dd37347381e6d0aef23b34a3cd0a3afcda 1d72e16d 2d41b04f5d86047dc2353a10595418b0d5239c22112f36eb9d253b 2e8b6eb0d0 98d4471fe549bb3067ac2f2d9afd50ed1baaddab41ec4270834989e 7f1ade14d

TYPE	VALUE
SHA256	43c2d5122af50363c29879501776d907eaa568fa142d935f6c80e823d18223f5 557ff6c87c81a2d2348bd8d667ea8412a1a0a055f5e1ae91701c2954ca8a3fdb 2b78d5228737a38fa940e9ab19601747c68ed28e488696694648e3d70e53eb5a fb7fb6dbaf568b568cd5e60ab537a42d5982949a5e577db53cc707012c7f20e3 94aa827a514d7aa70c404ec326edaaad4b2b738ffaea5a66c0c9f246738df579 5cbc07895d099ce39a3142025c557b7fac41d79914535ab7ffc2094809f12a4b 855656bfecc359a1816437223c4a133359e73ecf45acda667610fbe7875ab3c8 d0971d098b0f8cf2187feeed3ce049930f19ec3379b141ec6a2f2871b1e90ff7 07aed9fa864556753de0a664d22854167a3d898820bc92be46b1977c68b12b34 8d0bafca8a8e8f3e4544f1822bc4bb08ceaa3c7192c9a92006b1eb500771ab53 9dac6553b89645ac8d9e0a3dc877d12641e6d05fb52e8de6ae5533b2bdf0abc9 38d1d8c3c4ec5ea17c3719af285247cb1d8879c7cf967e1be1197e60d42c01c5 f86d05c1d7853c06fc5561f8df19b53506b724a83bb29c69b39f004a0f7f82d8 4a1c43258fe0e3b75afc4e020b904910c94d9ba08fc1e3f3a99d188b56675211 203ea478fa4d2d5ef513cad8b51617e0c9f7571bf3a3becf9c267a0d590c6d72 1324acd1f720055e7941b39949116dfe72ce2e7792e70128f69e228eb48b0821 873b8fb97b4b0c6d7992f6af15653295788526def41f337c651dc64e8e4aeebd 63b4bd01f80d43576c279adf69a5582129e81cc4adbd03675909581643765ea8 ed0161f2a3337af5e27a84bea85fb4abe35654f5de22bcb8a503d537952b1e8a a605570555620cea6d6be211520525fc95a30961661780da4cc4bafe9864f394 908777e581616156576636568 61c212ac25696741ef69411021474158fa2b4cf d2f4bf0caed5a442198fcdc43c83c7b27ae04f341a72b270c9ed40778aa77afe a4ba1e6ab678a1bdf8bc05bea8310d743928a4e2c05bad104e61afdd9cccf9a1

TYPE	VALUE
SHA256	da22d327124a0ee6a93cd07e85f9804fbc98eda87824ddcf7c8a63d349e87034 034d29fb89a8f68ba714f1868b2181c4cd59d4a2604630ef1554a6ccf3fe6d75 54a8b8c933633c089f03d07cfbd5cafbf76a6d7095f2706d6604e739bb9c950f 79c0fe1467dada33e0b097dd772c36229618b7091baa5f10da083f894192a237 2c338055e8245057169f1733846e0490bc4ae117d1dadefe0a3f07a63dc87520 26a98b752fd8e700776f11bad4169a0670824d5b5b9337f3c8f46fac33bc03e8 b55e9d65a3130f543360a9c488d35475d4789ee7a32a4e94d02f33c21a172bcb 4a08b78d410bc3d9b78dd63b146767f293dc3f3f6f8092352d2aa2f589e9c772 e637c86ae20a7f36a0ad43618b00c48f47b5591a03af3fb689a16c45afa43733 2365a48f7d6cf6dcc83195f06ea11b93c955c3a491c60b50ba42788917ba22e2 780e7edbfad5f68051c2039036b00b304d3f828fdbee85d2d09edbcc6d07ea34 32beeda8cffc2ecc689ea2529194cf806955879a334ec68176864d1e6c09800c ba3c79dbeca0234fa838ae4c956409115556f437372aeeb0737206d71caf4a38 a9c404e100bfd2716a8f6bfafc07b0bd6175bedb047d10b94390c79249258272

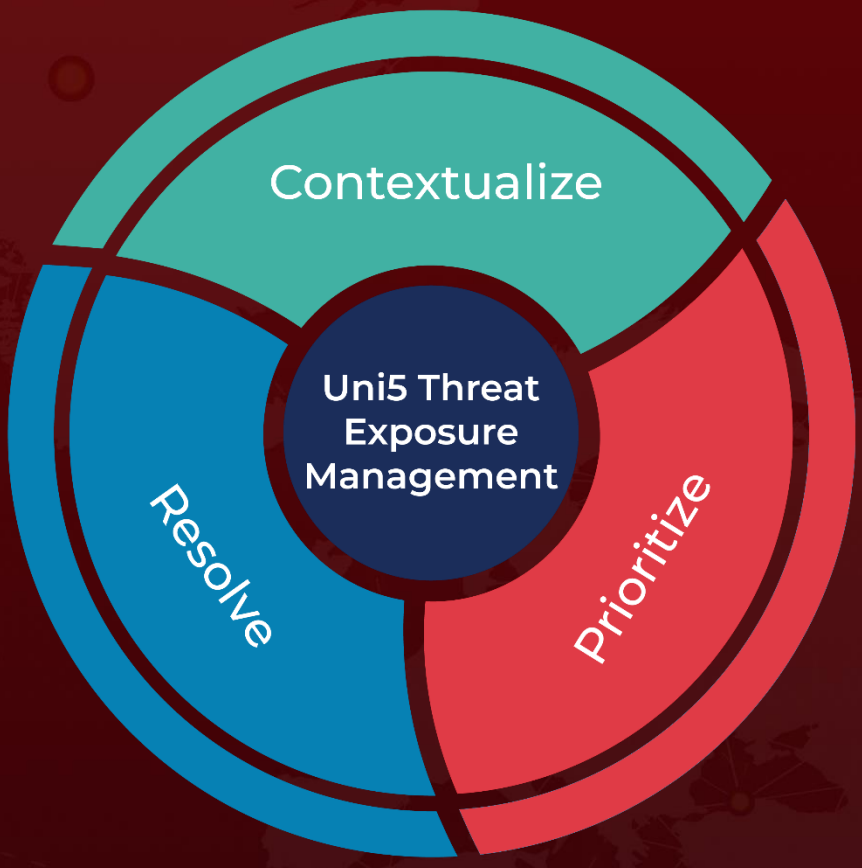
References

https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

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

April 4, 2023 • 6:00 AM

More at www.hivepro.com