Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

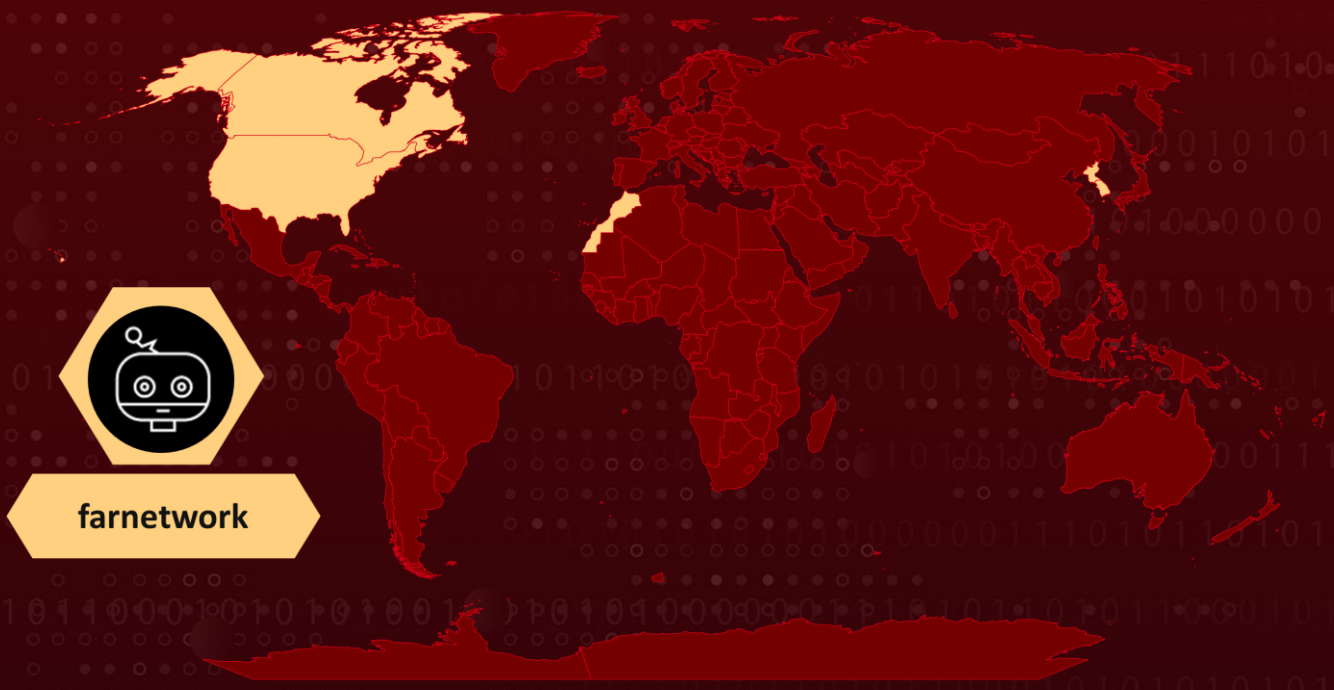
Farnetwork the Mastermind of Five Ransomware Strains

Date of Publication	Admiralty Code	TA Number
November 9, 2023	A1	TA2023455

Summary

Active Since: 2019
Threat Actor: farnetwork (aka farnetworkl, jingo, jsworm, razvrat, piparkuka, and farnetworkit)
Malware: Nokoyawa, JSWORM, Nefilim, Karma, and Nemty
Attack Region: United States, Korea, Canada, Morocco, Saint Kitts and Nevis
Targeted Industries: Utilities, Construction, Engineering, Trading Companies, Healthcare, Hotels, Restaurants & leisure, Distributors, Road & rail, Media, Education Services, and Automotive.
Attack: Farnetwork, a highly skilled threat actor fluent in Russian, has played a key role in five distinct ransomware-as-a-service (RaaS) programs, assuming diverse roles such as orchestrator and contributor to malware development.

Attack Regions



Attack Details

#1 A highly proficient threat actor, widely recognized as farnetwork and fluent in Russian, has intricately associated itself with five distinct ransomware-as-a-service (RaaS) programs, assuming diverse roles within each. As the orchestrator of the **Nokoyawa** ransomware-as-a-service, farnetwork cultivated expertise in the digital realm of underground forums.

#2 Operating under various pseudonyms, their engagements spanned from 2019 to 2023, during which they actively contributed to the JSWORM, Nefilim, Karma, and Nemty affiliate programs by overseeing malware development and operational management.

#3 Farnetwork subjected potential affiliates to rigorous assessments, providing them with corporate account credentials sourced from the Underground Cloud of Logs service, which trades in logs pilfered by info-stealers like RedLine, Vidar, and Raccoon. Affiliates were expected to escalate their privileges within target networks, exfiltrate files, execute the encryptor, and subsequently demand ransom payments.

#4 In the RaaS framework, affiliates stand to gain 65% of the ransom proceeds, while the botnet owner retains 20%. The ransomware developer, in this model, claims 15% of the overall share, with the possibility of a reduction to 10%. Farnetwork recently declared its retirement from the cyber scene, culminating in the October shutdown of the Nokoyawa RaaS program, accompanied by the exposure of data from 35 victims.

Recommendations

Adoption of Advanced Threat Detection Technologies: Investing in advanced threat detection technologies, such as artificial intelligence-based solutions, can bolster the capability to identify and neutralize evolving cyber threats. These technologies can analyze patterns, detect anomalies, and respond in real time to potential security breaches.

Credential Security and Training: Recognizing farnetwork's use of stolen corporate account credentials, organizations should prioritize the security of their authentication systems. Employee training programs on recognizing phishing attempts and maintaining secure password practices can significantly reduce the risk of unauthorized access.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0040 Impact	T1190 Exploit Public-Facing Application
T1059.001 PowerShell	T1027 Obfuscated Files or Information	T1083 File and Directory Discovery	T1113 Screen Capture
T1114 Email Collection	T1005 Data from Local System	T1490 Inhibit System Recovery	T1048 Exfiltration Over Alternative Protocol
T1486 Data Encrypted for Impact	T1491 Defacement	T1555 Credentials from Password Stores	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	8800e6f1501f69a0a04ce709e9fa251c, 1e4dd35b16ddc59c1ecf240c22b8a4c4, f23be19024fcc7c8f885dfa16634e6e7, a2313d7fdb2f8f5e5c1962e22b504a17, 46168ed7dbe33ffc4179974f8bf401aa, 2e936942613b9ef1a90b5216ef830fbf, feb7b1e0161df136c3d385bfd2d4b247, c159afb7d2111690326cad610776db34
SHA256	46761b8b727f3002d1c73fa6c8568ebcf2ec0066666251f66dcda9d4268e03e8, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee620276, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599,

TYPE	VALUE
SHA256	eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f, ee9ea85d37aa3a6bdc49a6edf39403d041f2155d724bd0659e6884746ea3a250, f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5, fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 24ada19b269279612370bdf16f2becc1d5b7e0f69821050e2d9b48cfc874dca0, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 24f1b3b9562ffa9b87b1497397c3da9dffa9f872f96b77d2643b18f9846aafaa, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, 0125e74c95d3e2762f7e29dc833592f33d5ded892ba4708e2b519eb5f400c2ee, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, 3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, ea6ced3730495e2231c1a755fcc1aefac7622ac4bd5e269b2a5996572acb42f9, 2e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 5104b8abb22cca1b078dd5b86e61f515a73404b0269fe7e6765ec818fbdf830b, 2b4b2a707662973236ae9b2fc732533b5d7236b279a2fccb2874da07e09af4b3, 7d7c44f9c577c0af913d905b51797f17399d650de0331885abc8828c2696d37f,

TYPE	VALUE
SHA256	8b35aa930dd7260060f12ff92f1447850fc1a6bd79a28ba05a2d4e54a3aad504, fd3c8be2d1ead92101e8909a85695a0a40c2576c87eefeef6d32376a7fe22f1c, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5, a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3, 4dec9a9044631caef283c7f39a576e4e5c1cc1e6a97ce5c60936a3a3d0097818, 124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59, ad841882052c3f9d856ad9a393232e0a59d28e17c240d23258f1dac62f903ab8, 19417c0a38a1206007a0cc82c0fc2e19db897214d27d0998bc4dbac53cc2788d, a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 34629751d8202be456dcf149b516afefc980a9128dd6096fd6286fee530a0d20, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90, 267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e, 064debda941fb6b1ac7de62e4990f658ded67870f55f48757ab72a772c640995, 17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae, c41f14cf5a0c8d407b70cf07f552a5ba26db3b23bfdbfae7b24e7ff8de7ec1a7, dd228f63f0ef02749759ef6d75f9f84d5ba8b0787dadef0d41b390176ea5d6a1,

TYPE	VALUE
SHA256	4cf87dd16d57582719a8fe6a144360f3dfa5d21196711dc140ce1a738ab9816e, abf148370f7cc9c16e20c30590a08f85208f4e594062c8a9e59c0c89cd8ff43f, ddadfcc43e4576de65f5844396a08fec47410663a6b6921991206b7a0df32ada, 57e25a37d8279fe563415d636b1983d447b5521ec6c024e18fd4d578840d2e20, 9913afe01dc4094bd3c5ff90ca27cc9e9ef7d77b6a7bdbf5f3042a8251b96325, 1d828a6c85bd5896ea27eeb17483dfe3bef81e0bf31521c91bcdf2559a03da1f, 31ee05823a66851cf6965f32d02e767206785d0bf0c9fa65e7dcf1ffed32c18e, 12da8dee83df90880d7d9cb4b0a7b608950bb57e9bc59c8b96f68c364350447c, d809ab5906fe6dba964cb30a21753213f5b077e28abb67680b2f28d65cbfc83b, a7558decb9516122781243e791c982977660152813817fb7ed00359365fcb0d3, e410854d9c8afe6e691c0ae638dfd04d792c3745dbb9e335f6f949e7a6b298d8, 5439452012a052851fdd0625abc4559302b9d4f4580e2ec98680e9947841d75d, a9f6d5ad40d5b073be92fc46666ce1f96e30c50494a018d472cfee56ff2b8c65, a5590a987d125a8ca6629e33e3ff1f3eb7d5f41f62133025d3476e1a6e4c6130, 3a061909a2631041b16d1d57212c1f44baca897efce50d095a141f8b7563db0b, 17864c4e21c0ebaf30cca1f35d67f46d3c3c33a5b8ea87d4c331e9d86d805965, a127323192abed93aed53648d03ca84de3b5b006b641033eb46a520b7a3c16fc, 2c41b93add9ac5080a12bf93966470f8ab3bde003001492a10f63758867f2a88, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b,

TYPE	VALUE
SHA256	3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5, 52e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377

Recent Breaches

https://studiodomaine.com
https://rcda.org
https://peariver.com
https://muncyhomes.com
https://at.or.kr
https://onehealth.co
https://visionsource-moderneyez.com
https://vcbweb.org
https://tgh.org
https://canaropa.com
https://roadieslogistics.com
https://liveaction.org
https://miamioh.edu
https://mua.edu
https://chattanoogastate.edu
https://hyundai.ma

References

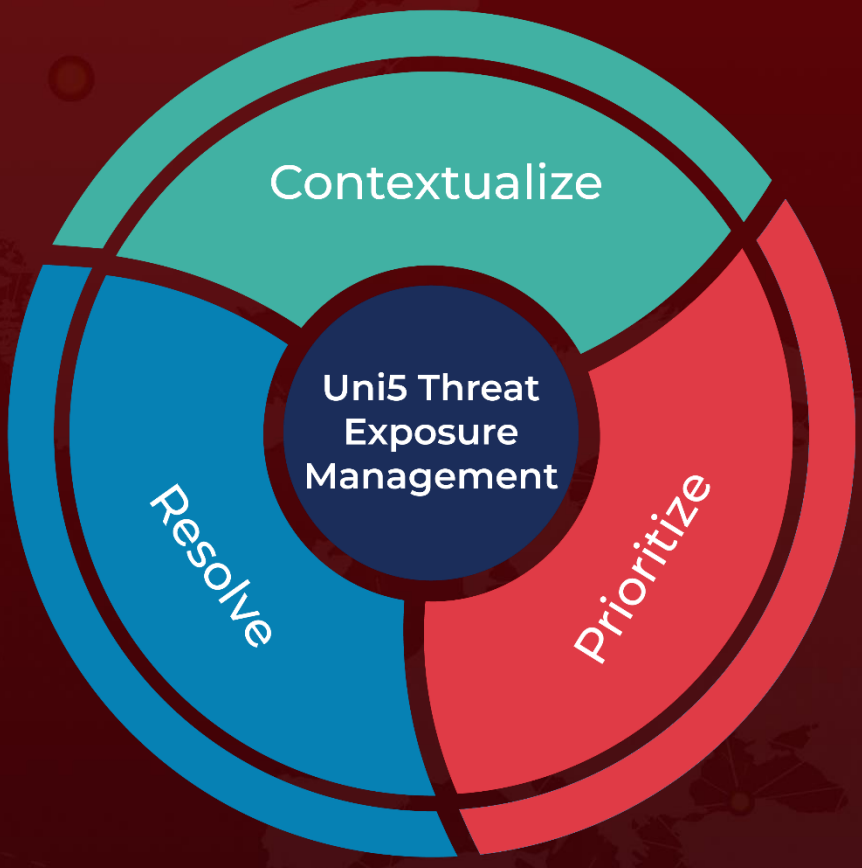
https://www.group-ib.com/blog/farnetwork/

https://www.hivepro.com/threat-advisory/nokoyawa-2-0-a-reworked-rust-based-ransomware/

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 9, 2023 • 5:30 AM

More at www.hivepro.com