Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

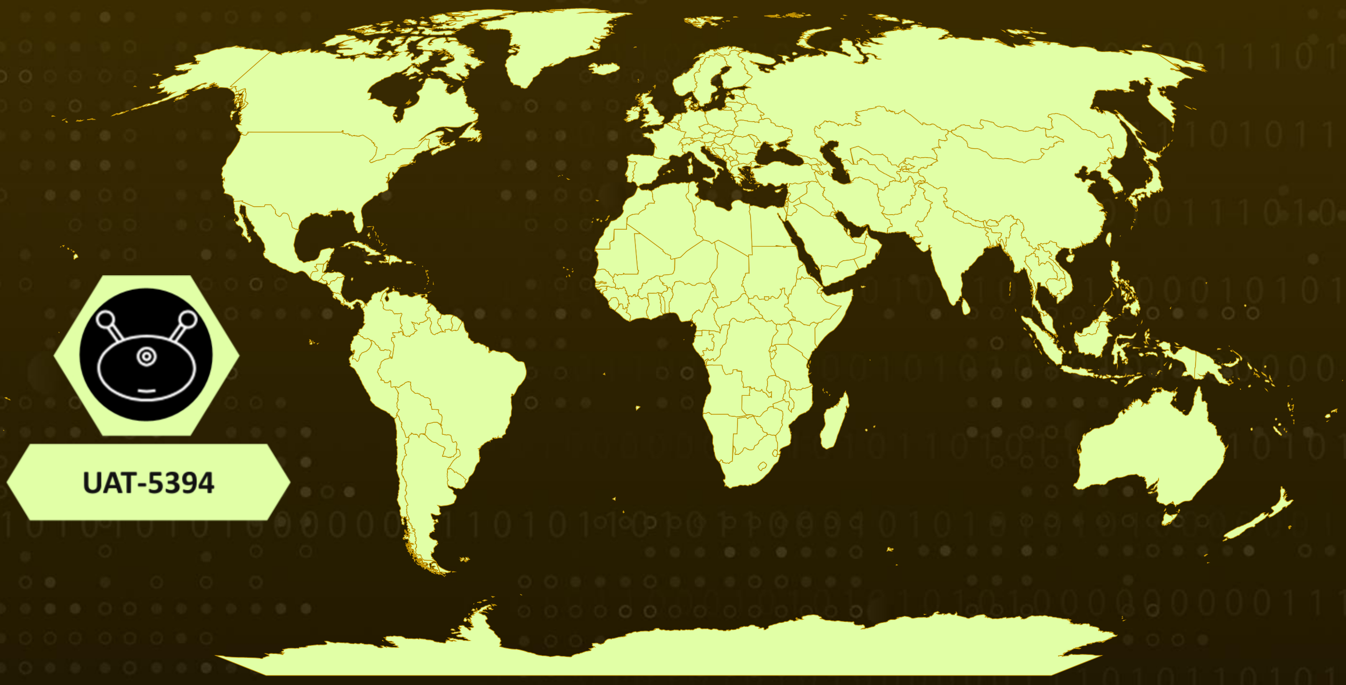
North Korean Hackers Roll Out Their New MoonPeak RAT

Date of Publication	Admiralty Code	TA Number
August 23, 2024	A2	TA2024326

Summary

First Seen: June 2024
Malware: MoonPeak
Threat Actor: UAT-5394
Targeted Region: Worldwide
Attack: UAT-5394, a state-sponsored North Korean cyber threat actor, is potentially a distinct group or a sub-division of the infamous Kimsuky APT group. Renowned for its tactical alignment with Kimsuky, UAT-5394 is actively engaged in the development and deployment of a new XenoRAT malware variant, known as MoonPeak.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 UAT-5394 is a state-sponsored North Korean threat actor group, believed to be a distinct entity or possibly a sub-group within the infamous North Korean APT group, **Kimsuky**. UAT-5394 exhibits tactical overlaps with Kimsuky, suggesting a connection between the two.

#2 The group has been actively engaged in developing and deploying a new variant of the open-source **XenoRAT** malware, known as MoonPeak. This Remote Access Trojan (RAT) continuously evolves, reflecting UAT-5394's strategy of adapting its tools to outpace detection mechanisms.

#3 The attack chain orchestrated by UAT-5394 unfolds in several stages, beginning with the deployment of MoonPeak via command and control (C2) servers. Initially, the group hosted its malicious payloads on legitimate cloud services but later transitioned to attacker-controlled infrastructure, likely to avoid potential shutdowns by cloud service providers.

#4 UAT-5394's infrastructure is extensive, comprising multiple C2 servers, payload-hosting sites, and test machines used to refine their implants before widespread deployment. Throughout the operation, UAT-5394 has employed sophisticated techniques, such as modifying server and client configurations to ensure that only specific versions of MoonPeak can communicate with corresponding C2 servers.

#5 This tactic not only bolsters their operational security but also complicates the detection and analysis of their activities. Additionally, UAT-5394's infrastructure is highly dynamic, with servers frequently changing operating systems and configurations to evade detection and maintain control over compromised networks.

Recommendations

Implement Endpoint Detection and Response (EDR): Deploy EDR solutions to monitor, detect, and respond to suspicious activities on endpoints. Ensure EDR tools are configured to identify and analyze RAT behaviors, such as those used by MoonPeak.

Adopt Zero Trust Architecture: Implement a Zero Trust approach to network security, ensuring that all access requests are thoroughly verified regardless of their origin. This can help mitigate risks associated with RATs and other threats.

Implement Network Segmentation: Divide your network into isolated segments to contain potential infections and limit lateral movement of malware. Use firewalls, VLANs, and access control lists (ACLs) to enforce segmentation policies.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0007** Discovery	**TA0011** Command and Control
TA0010 Exfiltration	**T1082** System Information Discovery	**T1071** Application Layer Protocol	**T1008** Fallback Channels
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1204.002** Malicious File	**T1027** Obfuscated Files or Information
T1046 Network Service Discovery	**T1082** System Information Discovery	**T1041** Exfiltration Over C2 Channel	**T1574** Hijack Execution Flow
T1010 Application Window Discovery	**T1033** System Owner/User Discovery	**T1057** Process Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0b8897103135d92b89a83093f00d1da845a1eae63da7b57f638bab48a779808e, 2b35ef3080dcc13e2d907f681443f3fc3eda832ae66b0458ca5c97050f849306,

TYPE	VALUE
SHA256	4108c5096a62c0a6664eed781c39bb042eb0adf166fcc5d64d7c89139d525d4f, 44e492d5b9c48c1df7ef5e0fe9a732f271234219d8377cf909a431a386759555, 4599a9421e83fb0e2c005e5d9ac171305192beabe965f3385accaf2647be3e8e, 58fdc1b6ce4744d6331f8e2efc4652d754e803cae4cc16101fc78438184995e6, 97ba8d30cf8393c39f61f7e63266914ecafd07bd49911370afb866399446f37d, a80a35649f638049244a06dd4fb6eca4de0757ef566bfbe1affe1c8bf1d96b04, b8233fe9e903ca08b9b1836fe6197e7d3e98e36b13815d8662de09832367a98a, f4aa4c6942a87087530494cba770a1dcbc263514d874f12ba93a64b1edbae21c, facf3b40a2b99cc15eee7b7aee3b36a57f0951cda45931fcde311c0cc21cdc71, 0ed643a30a82daacecfec946031143b962f693104bcb7087ec6bda09ade0f3cb, 41d4f7734fbf14ebcdf63f51093718fd5a22ec38a297c0dc3d7704a3fb48b3f9, 6a3839788c0dafe591718a3fb6316d12ccd8e82dbcb41ce40e66b743f2dd344d, 148c69a7a1e06dc06e52db5c3f5895de6adc3d79498bc3ccc2cbd8fdf28b2070, 1ad43ddfce147c1ec71b37011d522c11999a974811fead11fee6761ceb920b10, 458641936e2b41c425161a9b892d2aa08d1de2bc0db446f214b5f87a6a506432, 8a4fbcdec5c08e6324e3142f8b8c41da5b8e714b9398c425c47189f17a51d07b, 293b1a7e923be0f554ec44c87c0981c9b5cf0f20c3ad89d767f366afb0c1f24a, 6bf8a19deb443bde013678f3ff83ab9db4ddc47838cd9d00935888e00b30cee6, 72a25d959d12e3efe9604aee4b1e7e4db1ef590848d207007419838ddbad5e3f, 15eee641978ac318dabc397d9c39fb4cb8e1a854883d8c2401f6f04845a79b4b, 3e39fc595db9db1706828b0791161440dc1571eaa07b523df9b721ad65e2369b, f928a0887cf3319a74c90c0bdf63b5f79710e9f9e2f769038ec9969fcc8ee329, 27202534cc03a398308475146f6710b790aa31361931d4fe1b495c31c3ed54f7

TYPE	VALUE
IPv4	167[.]88[.]173[.]173, 95[.]164[.]86[.]148, 80[.]71[.]157[.]55, 84[.]247[.]179[.]77, 45[.]87[.]153[.]79, 45[.]95[.]11[.]52, 104[.]194[.]152[.]251, 27[.]255[.]81[.]118, 212[.]224[.]107[.]244, 27[.]255[.]80[.]162, 210[.]92[.]18[.]169, 91[.]194[.]161[.]109
Domain	nmailhostserver[.]store, yoiroyse[.]store, pumaria[.]store,nsonlines[.]store

References

https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/

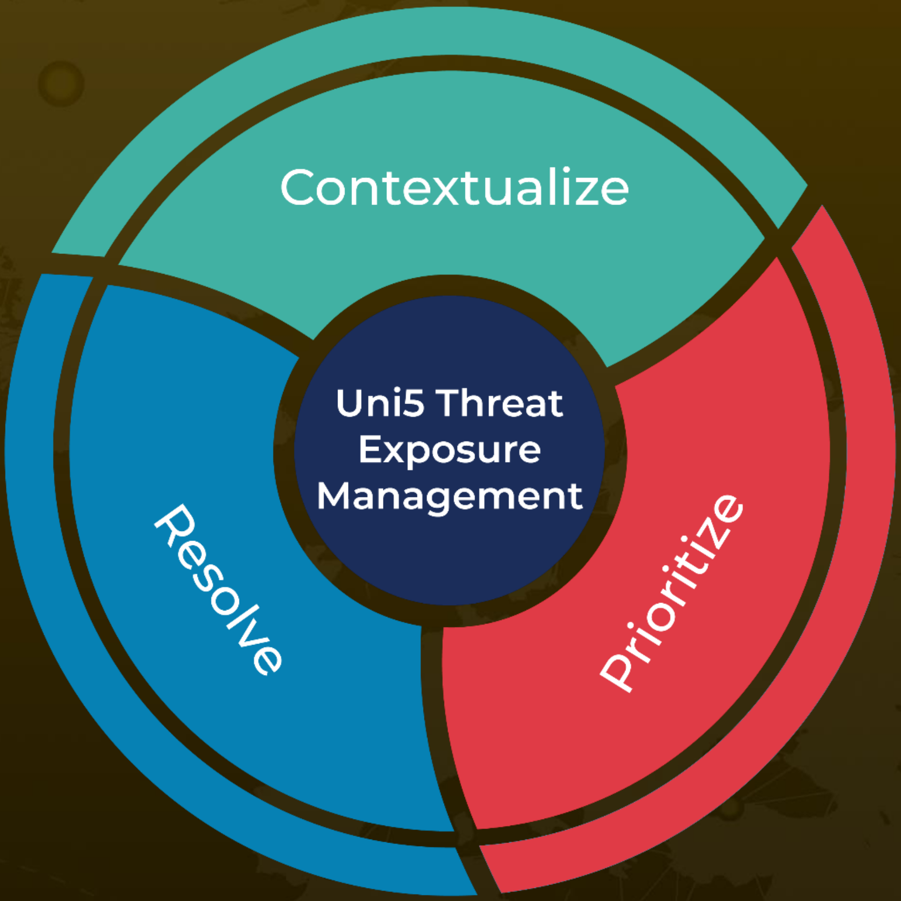
https://hivepro.com/threat-advisory/kimsuky-expands-its-arsenal-with-new-backdoor/

https://hivepro.com/threat-advisory/xeno-rat-open-source-trojan-sparks-alarm/

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

August 23, 2024 • 7:00 AM

More at www.hivepro.com