Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

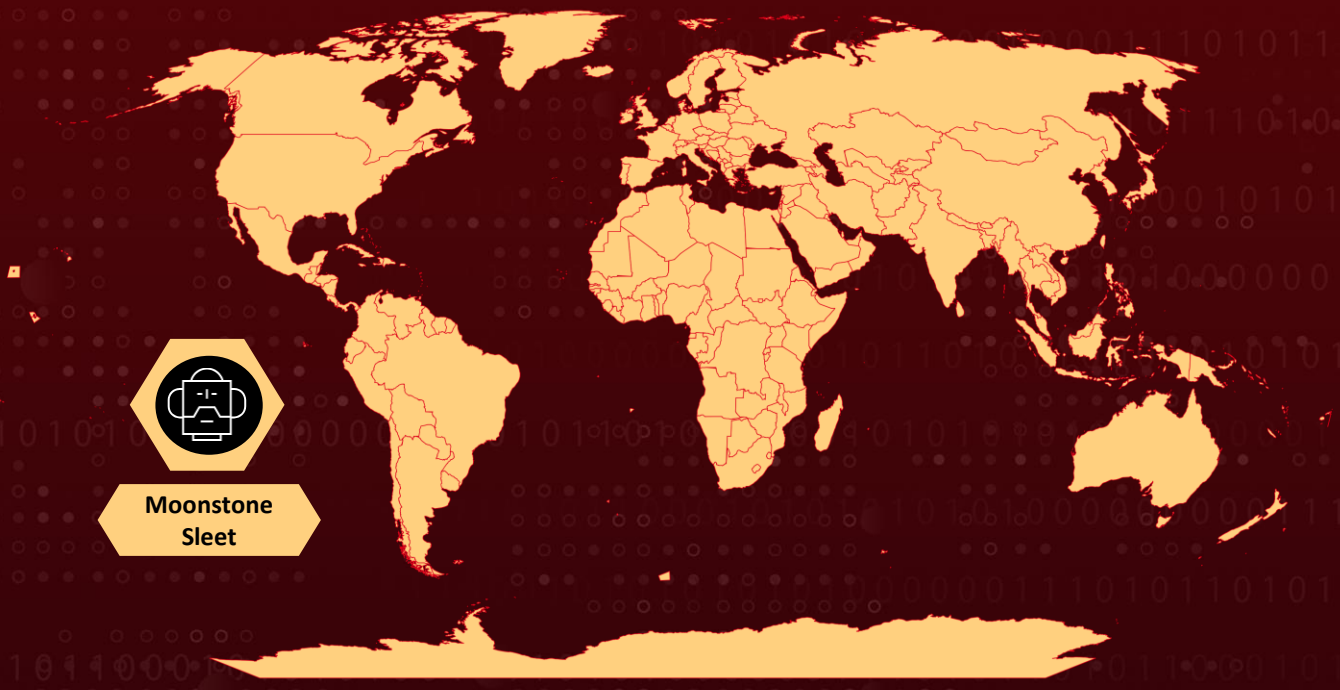
Moonstone Sleet: A New North Korean Cyber Threat

Date of Publication	Admiralty Code	TA Number
May 29, 2024	A1	TA2024211

Summary

First Seen: January 2024
Targeted Regions: Worldwide
Malware: FakePenny Ransomware
Threat Actor: Moonstone Sleet (aka Storm-1789)
Targeted Industries: Information technology, Education, and Defense
Attack: Moonstone Sleet, a newly discovered North Korean hacking group, targets companies for financial gain and stealing information. They use a mix of common tactics like fake companies and trojanized software, alongside unique methods like creating malicious games, custom ransomware. This well-resourced group is likely to become even more sophisticated in the future.

Attack Regions



Attack Details

#1 A new North Korean threat actor named Moonstone Sleet, previously known as Storm-1789, which utilizes a blend of traditional techniques used by other North Korean groups along with unique attack methods to target companies for financial gain and cyberespionage.

#2 Moonstone Sleet has been observed setting up fake companies and job opportunities to engage potential victims, deploying trojanized versions of legitimate tools such as PuTTY, creating a malicious game, and delivering a new custom ransomware called FakePenny.

#3 Initially, Moonstone Sleet's operations overlapped with those of another North Korean threat actor, Diamond Sleet, but it has since established its own infrastructure and attack strategies, distinguishing itself as a separate and formidable entity.

#4 The group's tactics include distributing trojanized software through social media and freelancing platforms, creating fake companies like StarGlow Ventures and C.C. Waterfall to approach targets with collaboration offers, and pursuing legitimate software development jobs to infiltrate organizations.

#5 Moonstone Sleet employs multi-stage malware delivery processes and leverages malicious npm packages through freelancing websites and social media platforms to target individuals and organizations in the software, IT, education, and defense sectors. As Moonstone Sleet evolves, it underscores the persistent and sophisticated nature of cyber threats emanating from state-aligned actors.

Recommendations

Enhance Email Security: Deploy advanced email filtering solutions to detect and block phishing attempts and malware attachments before they reach users' inboxes. Additionally, enable multi-factor authentication (MFA) for email accounts to add an extra layer of security.

Implement Endpoint Protection: Deploy comprehensive endpoint protection platforms (EPP) that include behavior analysis and real-time threat detection capabilities. Ensure all systems and software are kept up-to-date with the latest security patches.

Application Whitelisting: Use application whitelisting to ensure that only approved applications and software can execute on systems. This helps prevent trojanized versions of legitimate tools from running.

Network Segmentation and Access Control: Segment networks to limit the lateral movement of attackers. Implement robust access control policies to restrict user access to only necessary resources, based on the principle of least privilege.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0003 Persistence	TA0011 Command and Control
TA0007 Discovery	TA0040 Impact	TA0001 Initial Access	TA0009 Collection
T1566 Phishing	T1204 User Execution	T1204.002 Malicious File	T1036 Masquerading
T1140 Deobfuscate/Decode Files or Information	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1055.001 Dynamic-link Library Injection
T1055 Process Injection	T1033 System Owner/User Discovery	T1016 System Network Configuration Discovery	T1584 Compromise Infrastructure
T1657 Financial Theft	T1486 Data Encrypted for Impact	T1656 Impersonation	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58, cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb, 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5, 70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260, cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24, 9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1, f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be, 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c, ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146, 09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38
Domains	bestonlinefilmstudio[.]org, blockchain-newtech[.]com, ccwaterfall[.]com, chaingrown[.]com, defitankzone[.]com, detankwar[.]com, freenet-zhilly[.]org, matrixane[.]com, pointdnt[.]com, starglowventures[.]com, mingeloem[.]com

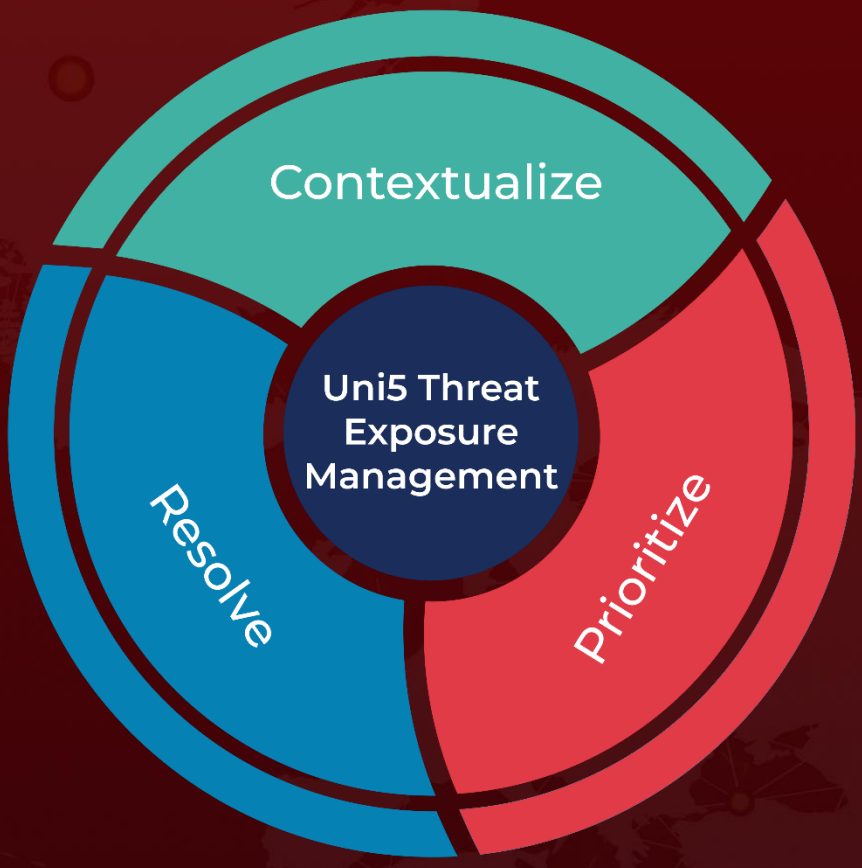
References

https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

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

May 29, 2024 • 6:30 AM

More at www.hivepro.com