North Korean Hackers Linked to New FakePenny Ransomware

Date: 30th May 2024 | Severity: High

Summary

Microsoft has revealed the deployment of a new “FakePenny” ransomware variant by a North Korean threat actor, targeting organizations across the software, information technology, education, and defense industrial base sectors for espionage and monetary gains.

Microsoft researchers have discovered a new North Korean threat actor, now known as Moonstone Sleet (formerly Storm-1789). This actor targets companies for financial and cyberespionage purposes by utilizing a variety of well-established tactics also employed by other North Korean threat actors as well as original attack methodologies. In order to interact with possible targets, Moonstone Sleet is known to build fake companies and job opportunities, use trojanized copies of legitimate tools, create malicious games, and distribute brand-new customized ransomware.

The ransomware comprises a straightforward loader and encryptor module. While North Korean threat groups have previously created custom ransomware, “this is the first time we have observed this threat actor deploying ransomware,” according to Microsoft.

Attack Vectors

- Moonstone Sleet employs a variety of methods to achieve its financial and espionage goals. The group has been seen creating fake companies, using trojanized versions of legitimate tools, and even developing malicious games to infiltrate targets. Their rapid evolution and adaptation of techniques are notable.
- Moonstone Sleet distributed a compromised version of PuTTY, an open-source terminal emulator, through platforms like LinkedIn, Telegram, and freelancing websites.
- The trojanized software decrypted and executed embedded malware when users provided an IP and password found in a text document within the malicious Zip file sent by the threat actor. A similar technique was used by another North Korean actor, Diamond Sleet.
- Moonstone Sleet has also targeted victims using malicious “npm” packages distributed via freelancing sites and social media, often masquerading as technical assessments that lead to additional malware downloads when executed.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58 • cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb • 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5 • 70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260 • cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24 • 9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1 • f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be • 09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38 • 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c • ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146
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

Recommendation

- Detect human-operated ransomware attacks with Microsoft Defender XDR.
- Enable controlled folder access.
- Ensure that tamper protection is enabled in Microsoft Dender for Endpoint.
- Enable network protection in Microsoft Defender for Endpoint.
- Follow the credential hardening recommendations in our on-premises credential theft overview to defend against common credential theft techniques like LSASS access.
- Run endpoint detection and response (EDR) in block mode.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- 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/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-links-moonstone-sleet-north-korean-hackers-to-new-fakepenny-ransomware/