Moonstone Sleet

Date: 31st May 2024 | Severity: High

Summary

The Moonstone Sleet threat group (AKA Storm-1789) was first reported by Microsoft in May 2024. The North Korean state-sponsored group targets both individuals and organizations in the software and information technology, education, and defense industrial base sectors. Moonstone Sleet had operational overlaps with the North Korean APT group, Lazarus (AKA Zinc); however, Microsoft assessed that it operates independently.

Attack Vectors

- Moonstone Sleet distributes its malware by approaching victims through LinkedIn, Telegram, freelancing networks, or email, tricking them into downloading Trojanized utility software (such as PuTTY), games, or npm packages.
- To increase their authenticity, the threat actors often impersonate software development and IT service providers (for example, StarGlow Ventures and C.C. Waterfall).
- The malicious files either lead to credential theft from the Windows Local Security Authority Subsystem Service (LSASS) process or drop malware loaders (SplitLoader or YouieLoad) that write the next-stage payload to disk. This next-stage payload then retrieves a Trojan loader from the attackers' command and control (C2) server.

Indicator of compromise

INDICATOR TYPE	INDICATORS	
Domains	• Defitankzone[.]com • Pointdnt[.]com • Detankwar[.]com • Ccwaterfall[.]com • Mingeloem[.]com • blockchain-newtech[.]com	• freenet-zhilly[.]org • matrixane[.]com • bestonlinefilmstudio[.]org • starglowventures[.]com • chaingrown[.]com

File Hash	• a09d152aa2b6261e3b0a1d1c19fa8032f215932186829cfcca954cc5e84a6cc38 • be6909ba6e0b4d228da5b9daccc83f7082c06cf2 • 9863173e0a45318f776e36b1a8529380362af8f3e73a2b4875e30d31ad7bd3c1 • 14af3f039f2398b454bbb64c7fdf4a22 • cb97ec024c04150ad419d1af2d1eb66b5c48ab5f345409d9d791db574981a3fb • ecce739b556f26de07adbfc660a958ba2dca432f70a8c4dd01466141a6551146 • 550bdf367fba63a81276465a65dcb64280240dda • cafaa7bc3277711509dc0800ed53b82f645e86c195e85fbf34430bbc75c39c24 • c0bb453d00bf3d8acde09b691ca9b5f2 • 2ebfcbf2deb09e9af046ae765797a654b49645c2 • f1f75da17e8c125b87fdafd76386f90213362bcf • 70c5b64589277ace59db86d19d846a9236214b48aacabbaf880f2b6355ab5260 • b0479c5d4de5541a60923b5627ed62e6391efe2f • dd8b8c4de92d9b6d1d04f0e995f4cc7e746d0a64 • 66c45a736e165cf78cee7970bbc74ead • bda08d55f14827abf21abb79384039660f2fa198 • 39d7407e76080ec5d838c8ebca5182f3ac4a5f416ff7bda9cbc4efffd78b4ff5 • 1d5ad4a60ec9be32c11ad99f234bfe8f • e99d44e93069001129c8f88f7a5259fb21bb6b68 • 330fff5b3c54a03fd59a64981e96814d • 6c76f795c4b3ff2e478766dee7c738d6 • f66122a3e1eaa7dcb7c13838037573dace4e5a1c474a23006417274c0c8608be • 56554117d96d12bd3504ebef2a8f28e790dd1fe583c33ad58ccbf614313ead8c • b8e1fe2955282a58fa3042b25f2ce19d • 608fb305734364e63513ef36da787f2b • dd91678f1d023607430d53b5ff5f1d6533a98469 • f59035192098e44b86c4648a0de4078edbe80352260276f4755d15d354f5fc58 • 39898007146d7b436d013924db58ebc6

Recommendation

- Stay Informed: Continuously monitor security news and updates related to Moonstone Sleet. Being aware of their tactics and techniques is crucial.
- Patch and Update: Regularly update and patch your software and systems. Vulnerabilities in outdated software can be exploited by threat actors.
- Employee Education: Educate your employees about social engineering risks. Encourage them to be cautious when interacting with emails, attachments, and links.
- Network Monitoring: Implement network monitoring tools to detect suspicious activity. Look for signs of unauthorized access or lateral movement.
- Access Controls and Segmentation: Restrict access to critical systems. Implement strong access controls and network segmentation to limit lateral movement within your network.

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://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/66586edfc926e0050e8ec444
- https://thehackernews.com/2024/05/microsoft-uncovers-moonstone-sleet-new.html

Copyright © Mphasis Corporation. All rights reserved