ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about a new North Korean advanced persistent threat group known as Moonstone Sleet.

Summary

Moonstone Sleet is the latest North Korean threat actor group identified by security researchers, demonstrating a high level of sophistication and adaptability in their cyber-espionage operations. This group, which has previously been active under different aliases, leverages advanced techniques to infiltrate and compromise various targets globally. Their operations are meticulously planned and executed, primarily focusing on sectors such as government, finance, and critical infrastructure, highlighting their strategic intent to gather sensitive and valuable information.

One of the primary methods Moonstone Sleet uses to gain initial access to target networks is through spear-phishing campaigns. These campaigns are often highly personalized and sophisticated, designed to exploit zero-day vulnerabilities, making them particularly effective. The group's ability to craft convincing phishing emails that can bypass traditional security measures underscores their expertise in social engineering. This initial access is crucial for establishing a foothold within the target network, from where they can deploy further stages of their attack.

Moonstone Sleet's operations do not stop at gaining entry; they are also adept at maintaining persistence within the compromised networks. This is achieved through a combination of custom-developed malware and the use of publicly available tools. Their toolkit allows them to escalate privileges, move laterally across the network, and exfiltrate sensitive data without raising immediate suspicion. The group's operational security practices are robust, making it challenging for defenders to detect and attribute their activities accurately. This level of sophistication indicates significant resources and expertise, positioning Moonstone Sleet as a formidable threat in the realm of cyber-espionage.

Recommendations

Recommendation #1: Stay up to date

Monitor official channels to stay informed and updated on the situation involving security vulnerabilities.

Recommendation #2:

References

1. 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/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team