Moonstone Sleet - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:16:13 UTC

APT group: Moonstone Sleet

Names	Moonstone Sleet *(Microsoft)* Storm-1789 *(Microsoft)* Stressed Pungsan *(Datadog Security Research)*	
Country	North Korea	
Motivation	Information theft and espionage, Financial gain	
First seen	2023	
Description	(Microsoft) Moonstone Sleet is a threat actor behind a cluster of malicious activity that Microsoft assesses is North Korean state-aligned and uses both a combination of many tried-and-true techniques used by other North Korean threat actors and unique attack methodologies. When Microsoft first detected Moonstone Sleet activity, the actor demonstrated strong overlaps with Diamond Sleet (Lazarus Group, Hidden Cobra, Labyrinth Chollima), extensively reusing code from known Diamond Sleet malware like Comebacker and using well-established Diamond Sleet techniques to gain access to organizations, such as using social media to deliver trojanized software. However, Moonstone Sleet quickly shifted to its own bespoke infrastructure and attacks. Subsequently, Microsoft has observed Moonstone Sleet and Diamond Sleet conducting concurrent operations, with Diamond Sleet still utilizing much of its known, established tradecraft. Moonstone Sleet has an expansive set of operations supporting its financial and cyberespionage objectives. These range from deploying custom ransomware to creating a malicious game, setting up fake companies, and using IT workers.	
Observed		
Tools used		
Operations performed	Jul 2024	Stressed Pungsan: DPRK-aligned threat actor leverages npm for initial access

		<https://securitylabs.datadoghq.com/articles/stressed-pungsan-dprk-aligned-threat-actor-leverages-npm-for-initial-access/>
	Aug 2024	North Korea Still Attacking Developers via npm <https://blog.phylum.io/north-korea-still-attacking-developers-via-npm/>
	Feb 2025	Microsoft: North Korean hackers join Qilin ransomware gang <https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/>
Information	<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://checkmarx.com/blog/a-new-north-korean-group-emerges-disrupting-the-open-source-ecosystem/>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
