

MoonPeak and the Growing Sophistication of DPRK Intrusions

 cybersecsentinel.com/moonpeak-and-the-growing-sophistication-of-dprk-intrusions

Cybersec Sentinel

January 28, 2026



Threat Group UAT-5394 with strong tactical overlap to Kimsuky

Threat Type Remote Access Trojan derived from XenoRAT delivered via weaponised LNK files and PowerShell droppers

Exploited Vulnerabilities Windows LNK execution trust abuse, PowerShell execution policy bypass, LOTS and LOLBins abuse, trusted cloud and code hosting platforms

Malware Used MoonPeak RAT based on modified XenoRAT with custom C2 handlers and obfuscation

Threat Score  8.7/10 High risk

Last Threat Observation 24 January 2026

Overview

MoonPeak is an advanced remote access trojan attributed to the North Korean aligned threat cluster UAT-5394. The malware represents a mature evolution of DPRK cyber espionage capabilities, combining the modular foundation of the open source XenoRAT framework with custom command and control protocols, layered obfuscation, and resilient attacker controlled

infrastructure. MoonPeak is designed for long term intelligence collection rather than short term financial gain and is actively used against diplomatic, government, academic, and financial organisations worldwide.

Background and Discovery

MoonPeak was publicly documented in January 2026 following analysis by Cisco Talos and corroborated by independent threat intelligence reporting. Researchers identified MoonPeak while tracking UAT-5394 activity after the group transitioned away from earlier tooling such as QuasarRAT. The malware drew particular attention due to the actor's rapid pivot from public cloud infrastructure to attacker owned servers, a move that significantly reduces takedown risk and supports long term operational persistence.

Technical Analysis

Delivery Method

MoonPeak is delivered primarily through targeted spear phishing emails containing weaponised Windows LNK files. These shortcuts are visually disguised as legitimate PDF or document files and commonly reference diplomatic meetings, investment briefings, or policy related events. When executed, the LNK file launches a hidden and heavily obfuscated PowerShell command while simultaneously opening a decoy document to distract the victim.

In select campaigns, the delivery chain abuses Google advertising redirection infrastructure, leveraging legitimate click tracking domains to bypass email security controls and redirect victims to malicious staging servers.

Payload and Behaviour

Once executed, MoonPeak performs detailed environment profiling, harvesting system metadata such as hostname, operating system version, hardware configuration, logged in users, and installed security tooling. This data is transmitted to command and control servers to enable operator prioritisation of high value targets.

MoonPeak provides full remote access capabilities including command execution, file transfer, screen capture, keylogging, and process manipulation. The malware also functions as a modular loader capable of retrieving additional payloads such as credential stealers, network discovery tools, and secondary backdoors.

A distinctive evasion technique observed in MoonPeak campaigns involves file header manipulation during payload delivery. PowerShell scripts download files masquerading as Rich Text Format documents and then replace the initial bytes with GZIP headers, transforming the file

into a compressed archive that contains the MoonPeak binary. This technique bypasses security controls that rely on superficial file type inspection.

Indicators of Compromise IoCs

File hash indicators

MD5

640f54bb6d29d98d92344136fee49d07
ea5d9be286f7af423c070128af170085

SHA1

665a1cdb7f050816dcb7b90a5516f2a38613e281
d8e96e777de3234e0771e6c53b7c09a659542f12
ebec41675fff24858ad558429ce4e4e32c30da55

SHA256

1553bfac012b20a39822c5f2ef3a7bd97f52bb94ae631ac1178003b7d42e7b7f
8de36cb635eb87c1aa0e8219f1d8bf2bb44cad75b58ef421de77dd1aae669bf4
aaac6eadac6c325bfc69b561d75f7cfd979ac289de1cc4430c5cc9a9a655b279

These hashes correspond to MoonPeak payload samples and staging components. Frequent recompilation and packing changes should be expected.

Endpoint indicators

Malicious LNK shortcut files disguised as PDF or document files
Obfuscated PowerShell scripts staged in C:\ProgramData\ or %TEMP% directories
Text based configuration files retrieved from public code repositories for C2 redirection
Persistence via registry run keys or service installation

Registry keys

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\System\CurrentControlSet\Services

Process behaviour

PowerShell execution with encoded commands and hidden window styles
Creation of scheduled tasks mimicking legitimate services
Unexpected Defender exclusions added for ProgramData directories

Network indicators

IPv4 addresses

95[.]164[.]86[.]148
167[.]88[.]173[.]173
104[.]194[.]152[.]251
91[.]194[.]161[.]109
27[.]102[.]137[.]88

Observed ports

9999
9966
9936
8936

These indicators are associated with MoonPeak command and control, payload staging, script hosting, and administrative hop points. Infrastructure roles and port usage change frequently.

Threat Context

MoonPeak reflects a broader DPRK strategy of adapting open source malware to reduce development cost while increasing stealth and resilience. The actor's shift away from cloud hosted infrastructure toward attacker owned servers mirrors similar transitions observed across North Korean campaigns following public disclosure. Strong overlap in infrastructure management, social engineering themes, and targeting aligns MoonPeak activity closely with historical Kimsuky operations.

Risk Assessment

The likelihood of compromise is high for organisations involved in diplomacy, government policy, academic research, and financial investment analysis. Successful compromise enables long term surveillance, credential theft, internal reconnaissance, and lateral movement. MoonPeak's use of LOTS techniques, living off the land tooling, and frequent iteration significantly reduces the effectiveness of signature based detection and increases dwell time.

Detection and Mitigation

Detection Guidance

Monitor for PowerShell execution using encoded commands and execution policy bypass flags. Alert on outbound connections from endpoints communicating over uncommon TCP ports. Hunt for LNK execution spawning PowerShell followed by scheduled task or service creation.

Mitigation Strategies

Restrict script execution initiated via LNK files using group policy controls.

Enforce PowerShell constrained language mode and mandatory script signing.

Deploy and tune EDR solutions with behavioural detection and lateral movement visibility.

Sources

Cisco Talos Intelligence – MoonPeak malware from North Korean actors unveils new details on attacker infrastructure – <https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/>

The Hacker News – North Korean hackers deploy new MoonPeak Trojan in cyber campaign – <https://thehackernews.com/2024/08/north-korean-hackers-deploy-new.html>

Fraunhofer FKIE Malpedia – UAT-5394 threat actor profile – <https://malpedia.caad.fkie.fraunhofer.de/actor/uat-5394>

Broadcom Security – North Korean based threat actor develops MoonPeak RAT – <https://www.broadcom.com/support/security-center/protection-bulletin/north-korean-based-threat-actor-develops-moonpeak-rat>

Dark Reading – Constantly evolving MoonPeak RAT linked to North Korean spying – <https://www.darkreading.com/cyberattacks-data-breaches/constantly-evolving-moonpeak-rat-linked-to-north-korean-spying>



[Threat Group China aligned APT operators tracked as SHADOW VOID 044 and SHADOW EARTH 045](#) [Threat Type JScript based command and control framework abusing trusted Windows utilities](#) [Exploited Vulnerabilities Abuse of Windows Script Host trust model, mshta.exe execution, ScriptControl ActiveX usage, browser watering hole injection, legacy Chrome V8 flaws](#)



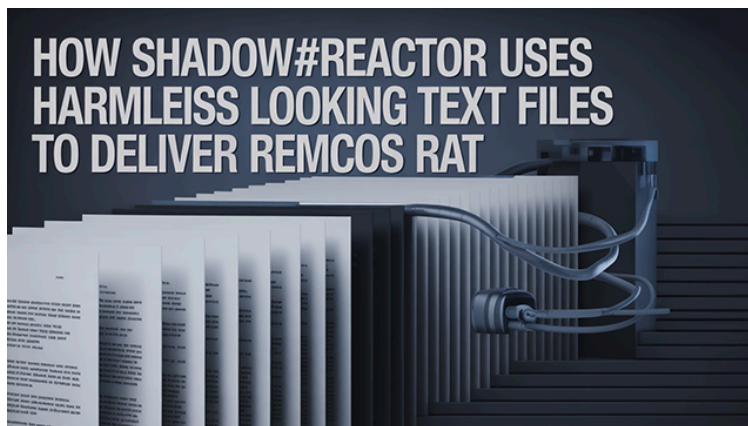
Threat Group: Unknown cybercriminal operators leveraging developer tooling supply chains

Threat Type: Information stealer malware delivered via malicious development extensions

Exploited Vulnerabilities: Abuse of the Visual Studio Code extension trust model, DLL side

loading, PowerShell execution policy misuse, Windows process hollowing

Malware Used: Evelyn Stealer, Lightshot.dll downloader, iknowyou.model



Threat Group – Unattributed, activity consistent with an initial access broker model

Threat Type – Multi stage loader chain delivering remote access capability

Exploited Vulnerabilities – None publicly confirmed, primary access relies on user execution and script based lures

Malware Used – Remcos RAT delivered via SHADOW#REACTOR staging and loader framework

Threat Score

Cybersec Sentinel © 2026