Microsoft: North Korean hackers join Qilin ransomware gang

By Sergiu Gatlan

Published: 2025-03-07 · Archived: 2026-04-05 13:45:15 UTC

Microsoft says a North Korean hacking group tracked as Moonstone Sleet has deployed Qilin ransomware payloads in a limited number of recent attacks.

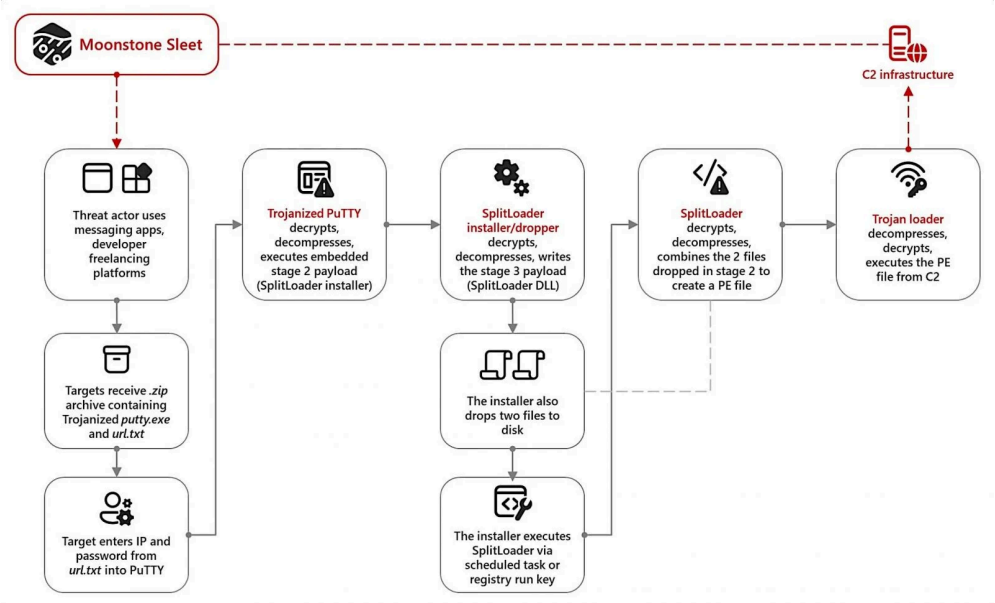
"Since late February 2025, Microsoft has observed Moonstone Sleet, a North Korean state actor, deploying Qilin ransomware at a limited number of orgs," the company's threat intelligence experts said this week

"Moonstone Sleet has previously exclusively deployed their own custom ransomware in their attacks, and this represents the first instance they are deploying ransomware developed by a RaaS operator."


DIE LINKE.
0:00

Previously tracked as Storm-1789, this threat group's activity initially overlapped with other North Korean attackers like Diamond Sleet and Onyx Sleet. However, it has since switched to its own tactics and custom tooling and attack infrastructure.

Microsoft says Moonstone Sleet hackers are targeting both financial and cyberespionage targets using trojanized software (e.g., PuTTY), custom malware loaders, malicious games and npm packages, and fake software development companies (e.g., C.C. Waterfall, StarGlow Ventures) set up to interact with potential victims on LinkedIn, various freelancing networks, Telegram, or via email.



Moonstone Sleet PuTTY attack flow (Microsoft)

Since it surfaced in August 2022 under the "Agenda" name, the Qilin ransomware gang has claimed over 300 victims on its dark web leak site. However, the Ransomware-as-a-Service (RaaS) operation was barely active until attacks peaked towards the end of 2023. In December 2023, Qilin affiliates began deploying one of the most advanced Linux encryptors to target VMware ESXi virtual machines.

So far, BleepingComputer has seen Qilin ransom demands ranging from $25,000 to millions, depending on the victims' size. Qilin has claimed over 310 victims since it emerged, including automotive giant Yangfeng, American newspaper publisher Lee Enterprises, Australia's Court Services Victoria, and pathology services provider Synnovis.

The latter led to an outage that impacted several major NHS hospitals in London, which forced them to cancel hundreds of operations and appointments.

In May 2024, Microsoft also linked Moonstone Sleet to a custom FakePenny ransomware variant. After a successful FakePenny ransomware attack, the North Korean hackers were observed asking for a ransom demand of $6.6 million in BTC.

Moonstone Sleet is not the first North Korean-backed threat group linked to ransomware attacks in recent years. In May 2017, the U.S. and U.K. governments blamed the Lazarus Group for the WannaCry ransomware outbreak, which brought down hundreds of thousands of computers worldwide.

Years later, in July 2022, Microsoft and the FBI linked North Korean hackers to the Holy Ghost ransomware operation and Maui ransomware attacks targeting healthcare orgs.

Source: https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/