STARDUST CHOLLIMA | Threat Actor Profile | CrowdStrike

By AdamM

Archived: 2026-04-05 18:39:11 UTC

STARDUST CHOLLIMA is a targeted intrusion adversary with a likely nexus to the Democratic People's Republic of Korea (DPRK). This adversary is typically involved in operations against financial institutions with the intention of generating liquid assets for the DPRK. Previous activity tied to this adversary includes campaigns focused on abusing Society for Worldwide Interbank Financial Telecommunication (SWIFT) systems, as well as intrusions against global banking networks via strategic web compromise operations.

Methods & Techniques

STARDUST CHOLLIMA uses several implants that share a code framework tracked by CrowdStrike® as "TwoPence." This actor also uses techniques such as code protection tools like Enigma protector, password protected executables and secure deletion functions to remain hidden on target system for long periods of time by avoiding legacy security products. Recent Falcon Intelligence™ reporting has been published to customers assessing that STARDUST CHOLLIMA is suspected of targeting Latin America-based organizations since mid-2017.

Targets

STARDUST CHOLLIMA primarily targets its victims with the aim of acquiring funds. CrowdStrike has not directly observed STARDUST CHOLLIMA conducting intelligence-gathering or destructive operations. It is not known at this time whether the TwoPence framework is used exclusively by STARDUST CHOLLIMA or if elements of it are shared between other related DPRK adversaries such as LABYRINTH CHOLLIMA, RICOCHET CHOLLIMA or SILENT CHOLLIMA. Currency generation represents an additional mission of DPRK actors beyond destructive attacks and espionage; this may reflect the impact of sanctions levied against the DPRK by the international community and the 2017 banning of the DPRK from SWIFT.

CrowdStrike identified earlier attempts at revenue generation by SILENT CHOLLIMA prior to tracking STARDUST CHOLLIMA, which leveraged unique tools and infrastructure; however, no overlap between the two actors was identified. In addition to financial sector targeting, there is some technical overlap between the Wannacry ransomware, which began self propagating in May 2017, and both STARDUST CHOLLIMA and LABYRINTH CHOLLIMA. The earliest observed version of WannaCry, created in February 2017, generates a custom TLS handshake message as part of its C2 protocol that is sent before actual payload data is transmitted. This handshake message selects a random number of cipher suite constants from a hard-coded array, resulting in changing patterns of network traffic. Some variants of Hawup also generate a fake TLS header with a random selection of cipher suite identifiers that is prepended to actual C2 traffic. While the code is not the same, the concept and structure are similar enough to assume a relation. All WannaCry samples, many Hawup variants, and many tools based on the TwoPence library were compiled using Microsoft Visual Studio 6, which is rarely

observed almost 19 years after its release. A hypothesis explaining these similarities is that the different actor groups have access to the same development resources, perhaps even a shared code library, but they engage in different types of attacks according to their respective missions. Community or industry names Lazarus Group, and Bluenoroff have been associated with this actor.

Learn More

- ***Curious about other nation-state adversaries?*** Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.
- To learn more about how to incorporate intelligence on threat actors like STARDUST CHOLLIMA into your security strategy, please visit the Falcon Intelligence product page.
- **Want the insights on the latest adversary tactics, techniques, and procedures (TTPs)?** Download the *CrowdStrike 2020 Global Threat Report*
