LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 21:04:31 UTC

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

- 41 Subscribers

US-CERT: North Korean Malicious Cyber Activity [HIDDEN COBRA]

On February 14, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released six (6) new Malware Analysis Reports (MARs) and one (1) updated MAR related to

malicious cyber activity from North Korea. Each MAR is designed to enable network defenders to identify and reduce exposure to North Korean government malicious cyber activity.

- 82 Subscribers

- 1,344 Subscribers

DPRK Hidden Cobra Update: North Korean Malicious Cyber Activity

FileHash-SHA256: 29

"The US-CERT recently released a new set of MARs (Malware Analysis Reports) covering newly uncovered/updated malware/implants attributed to North Korea. More specifically, these are tools attributed to the Lazarus Group / Hidden Cobra. These updates provide a sizeable glimpse into the ever expanding DPRK toolset. As we have seen in the past, the complexity and sophistication of these tools varies widely. Most of the families

covered in this update are meant to function as RATs or Cobalt-Strike-like (beacon) tools meant to enable persistence and manipulation of infected hosts."

- 374,006 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:SLICKSHOES