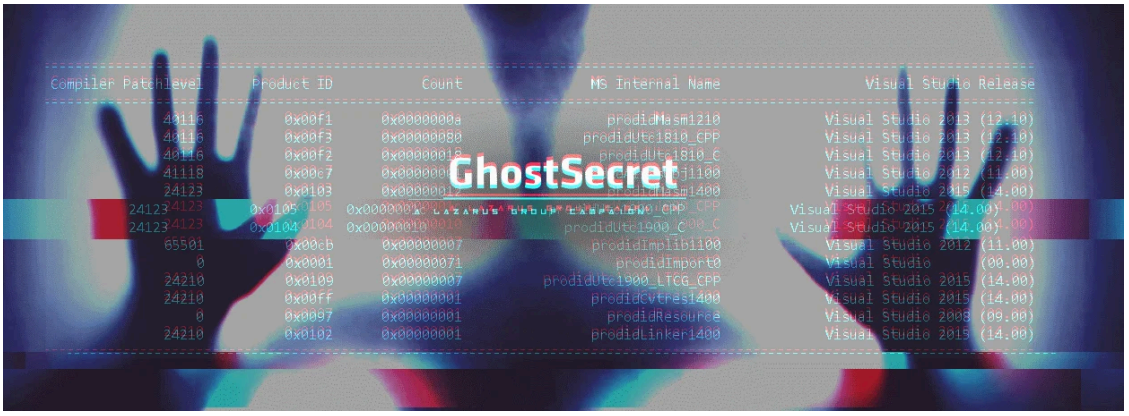
North Korean Hackers Are up to No Good Again

By Catalin Cimpanu

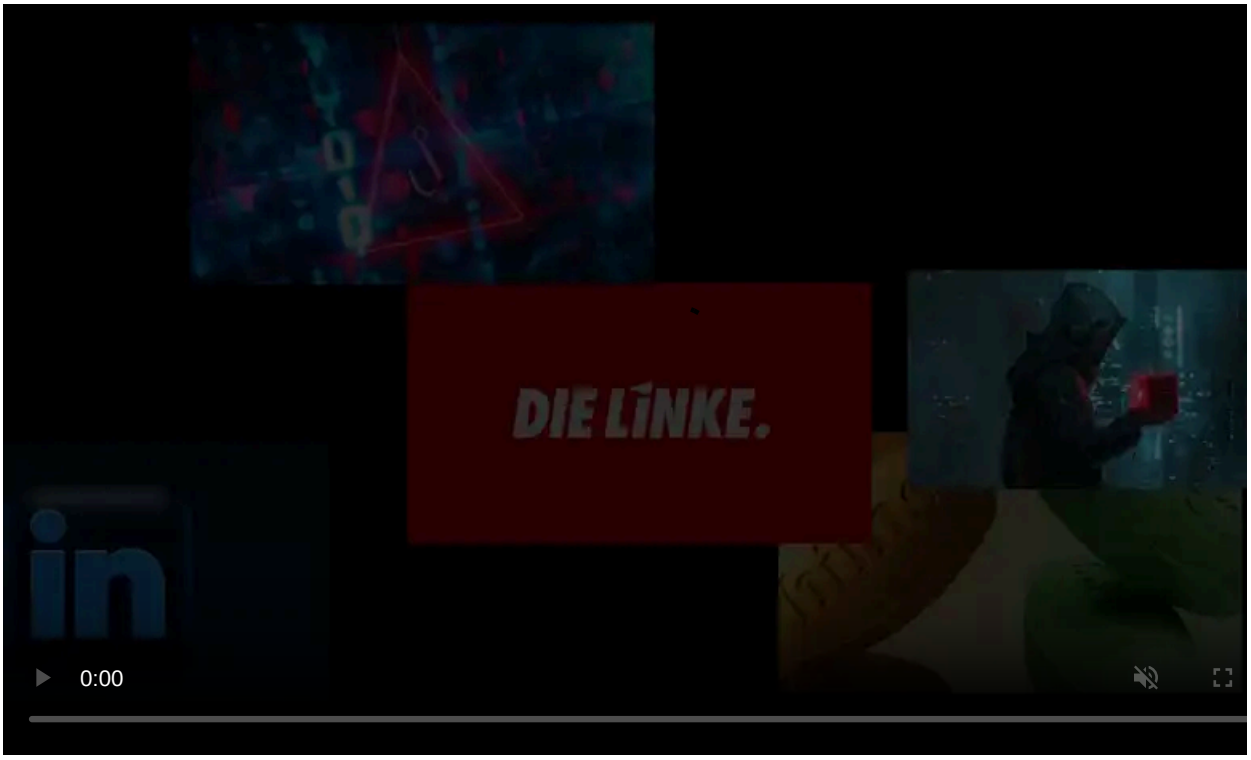
Published: 2018-04-27 · Archived: 2026-04-05 12:46:47 UTC



For a month leading up to today's historic meet between North and South Korea's presidents, a North Korean hacking group has amplified operations and has targeted a wide variety of business sectors in at least 17 countries.

The purpose of this campaign was to infect organizations, perform reconnaissance, and steal sensitive data. Targeted industries included critical infrastructure, entertainment, finance, healthcare, and telecommunications.

This overly aggressive campaign appears to be a new operation carried out by a group of hackers primarily known as Lazarus Group, the ones responsible for the infamous Sony Studios hack in 2014. Other names for this group are Hidden Cobra, the name US authorities are using to describe it, but also the Hastati Group, Group 77, or Labyrinth Chollima.


DIE LINKE.
0:00

The group operates in bursts of hacking activity aimed at specific targets. Past operations include Operation Troy, Blockbuster, or Dark Seoul.

Operation GhostSecret started last month

The most recent Lazarus Group operation is codenamed Operation GhostSecret and appears to have started in mid-March 2018 with attacks targeting the Turkish financial sector.

Cybersecurity firm McAfee describes this particular campaign as sophisticated due to the "significant capabilities, demonstrated by their tools development and the pace at which [the attackers] operate."

Researchers identified malware with shared capabilities to hacking tools used in the 2014 Sony hack, but they also found newer tools such as Bankshot (implant), Proxysvc (downloader), and Escad (backdoor).

Attacks amplify in scale following public disclosure

Experts noted that despite exposing the first attacks on the Turkish financial sector, the group continued its attacks unphased by the attention their tools and hacking infrastructure were getting.

Furthermore, attacks seem to have ramped up, most likely in an attempt to use hacking tools while they were still effective and before security software would be able to detect them.

McAfee said it alerted the Thai government that some of the command and control servers used for Operation GhostSecret were hosted on the compromised servers of Thammasat University in Bangkok. ThaiCERT seized and shut down the servers two days ago.

A full and detailed report on Operation GhostSecret, including IoCs, is available here.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
