North Korean Hackers Are up to No Good Again

bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Catalin Cimpanu

By
Catalin Cimpanu

- April 27, 2018
- 06:05 AM
- 2

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.

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.

Related Articles:

Lazarus hackers target VMware servers with Log4Shell exploits

US sanctions Bitcoin laundering service used by North Korean hackers

Cyberspies use IP cameras to deploy backdoors, steal Exchange emails

FBI links largest crypto hack ever to North Korean hackers

US warns of Lazarus hackers using malicious cryptocurrency apps

- APT
- Cyber-espionage
- Lazarus Group
- North Korea

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

- 
  Occasional - 4 years ago
  -
  -

  War by other means? Perhaps, NK figures it can accomplish its goals more effectively via cyber. If they have effective assets in place now (with the constraints and sanctions), how much more effective would they be with more money and access? Maybe Kim thinks the Democrats are right about the Russians using cyber to sway the U.S. 2016 elections; and he can do even better with next elections in SK, Japan.... Don't think he has to worry about the next election in NK.
  With their nuclear program, it will take time even to establish the framework of an agreement; then more time to implement - and if they eventually close all their facilities; will all their nukes go to China and Russia, as Syria's chemical weapons did to Russia?
  Suppose they do shed their nukes; they still have enough conventional artillery to flatten the SK capital; it would just take minutes, rather than seconds. A treaty, would void the UN use-of-force resolution from 1950 - and good luck getting another one past Russia and China.
  Still, today's breakthrough is a reason for optimism; just as long as it's tempered with skepticism - and for heaven's sake: don't send John (let's make a deal), Kerry to negotiate!

- 

  rhasce - 4 years ago

  -
  -

  Indeed since it is know that only 30 computes exist on NK and they are in control of the government, so obviously it is the government, why are we playing stupid? :)

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: