Security researcher identified Sharpshooter spy attacks related to the Korean hacker group

The finding comes through new evidence collected by researchers after analyzing a command and control server (command-and-control server - C2).

After working with countless in-depth studies and analyzes, a group of security researchers have uncovered a link between a previously discovered large-scale global cyber-espionage campaign. It targets critical infrastructure around the world with a Korean APT hacker group.

The finding was made possible through new evidence collected by researchers after analyzing a command and control server (command-and-control server - C2) related to espionage campaigns and Arrested by law enforcement forces.

More specifically, this cyber espionage campaign is named Sharpshooter, with the aim of targeting many different large and small organizations around the world, originally discovered in December 2018 by security researchers. at McAfee.

At that time, even after finding many technical links between the Sharpshooter campaign and the Korean Lazarus hacker group, the researchers still could not immediately attribute this campaign to a flag attack. False flag.

1. There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

The Sharpshooter command server has been operated on

According to a recently shared press release with The Hacker News, the in-depth analysis was conducted on confiscated code and command and control servers (C2) from the Sharpshooter campaign allowed. Researchers understand the inner workings of this global cyber espionage campaign, and the final conclusion is that it comes from a group of sponsored hackers in Korea.

More specifically, as originally expected, the Lazarus Group, also known as Hidden Cobra or Guardians of Peace, was identified as the organization behind the Sharpshooter campaign. Lazarus Group, which is no stranger to other security researchers, has previously been involved in a number of major attacks, including the release of the 2017 WannaCry global ransomware malware, the hack. SWift Banking 2016, as well as Sony Pictures hack in 2014.

Besides, the analysis report also revealed that the Sharpshooter global spy campaign began to be deployed in September 2017, which is one year earlier than previously stated and is still ongoing.

While previous attacks under the Sharpshooter campaign are primarily targeted at areas such as telecommunications and finance in countries such as the United States, Switzerland, Israel and other English-speaking countries, new evidence is available. Recent findings suggest that the Sharpshooter has expanded its focus to critical infrastructure, with the most recent attacks targeting Germany, Turkey, the United Kingdom and the United States.

1. McAfee expert explained how deepfake and AI are drilling through the cyber security wall

Sharpshooter: Cross-border spy campaign

The global Sharpshooter campaign spreads by sending malicious documents containing macros that are 'weaponized' to the specified targets via Dropbox. After downloading and opening this document, the macro takes advantage of the embedded shellcode to bring the Sharpshooter downloader into the memory of Microsoft Word.

To further exploit, the macro will be implanted in memory and silently download stage 2 Rising Sun malware, using the source code from Lazarus' own Duuzer backlink Trojan. This is the first malicious software released in 2015 in Korea.

"Access to command server code and control of the opponent is a rare opportunity. These systems provide greater insight for security professionals on the inner workings of the infrastructure. This attack is often carried out by law enforcement agencies and is rarely provided to private researchers (not working for state organizations). updating this code is indispensable in the effort to understand and fight against the threats existing on the cyberspace, as well as the most sophisticated and prominent offensive campaigns, "Christiaan Beek, One of the leading network security researchers and senior engineers of McAfee shared.

1. DDoS is ranked as the top threat for businesses in 2018

Furthermore, the server analysis and the log file of the command and control server also showed a link to Africa, when researchers discovered a network of IP addresses originating from a city located in Namibia - a country in Africa.

This prompted many McAfee Advanced Threat Research analysts to suspect that the agents behind the Sharpshooter campaign may have tested their transplants and other techniques in the African region before conducting the campaign. Broader attack on a global scale.

Command and control server infrastructure used by attackers with core backends written in Hypertext Pre (PHP) and Active Server Pages (ASP), "seems to be customized and reserved For this group, "is also part of the chain of activities Lazarus has been running since 2017.