The US warned about DealtaCharlie - DDoS botnet malware from Korea

The US government recently issued a warning about the possibility of a malware backed by the Korean government, which is 8 years old.

The FBI and US Department of Homeland Security (DHS) report provides details about DeltaCharlie, a malware variant used by a hacker group called Hidden Cobra that can infect hundreds of thousands of computers worldwide, and become part of the DDoS botnet system.

According to this report, Hidden Cobra hacker group is said to be backed by the North Korean government as well as the group behind the cyber attack on many global organizations, including the press and financial sectors, universe and essential infrastructure.

While the US government calls the Korean hacker group Hidden Cobra, they are also known as the Lazarus Group and Guardians of Peace, the group is believed to be involved in the attack of the WannaCry ransow to knock down many hospital systems. and businesses around the world.

DeltaCharlie - Malware botnet DDoS

"Highly reliable" IP addresses have been discovered that are linked to DeltaCharlie - a DDoS tool that DHS and FBI believe North Korea has used to launch a distributed denial-of-service attack (DDoS) makes the computer system overload. DeltaCharlie can launch many types of DDoS attacks on victims, including Domain Name System (DNS), Network Time Protocol (NTP) and Character Generation Protocol (CGP).

Picture 1 of The US warned about DealtaCharlie - DDoS botnet malware from Korea

Botnet takes user machines into an infected computer network

Malware botnet has the ability to download executable files on the infected system, update the compiled library, change the configuration in real time, stop processing and activation processes, and stop DDoS attacks.

DeltaCharlie DDoS is also not a new malware. It was first reported by Novetta in the Operation Blockbuster Malware Report 2016 report, which described it as the third malware from the Korean hacker group, following DeltaAlpha and DeltaBravo.

Other malware used by Hidden Cobra also includes Destover, Wild Position or Duuzer, Hangman with complex capabilities such as DDoS botnet, keystroke tracking, remote access tool RAT and data deletion.

Favorite vulnerability of Hidden Cobra

Operating since 2009, Hidden Cobra often targets systems running old OS, not supported by Microsoft and often exploits vulnerabilities in Adobe Flash Player to gain access to victim machines.
Here are some of the hidden problems that Hidden Cobra uses:

1. Hangul Word Processor bug (CVE-2015-6585)
2. Microsoft Silverlight flaw (CVE-2015-8651)
3. Adobe Flash Player 18.0.0.324 and 19.x vulnerability (CVE-2016-0034)
4. Adobe Flash Player 21.0.0.197 Vulnerability (CVE-2016-1019)
5. Adobe Flash Player 21.0.0.226 Vulnerability (CVE-2016-4117)

The simplest way to avoid these types of attacks is to always update the operating system and installation software, protect network assets with a firewall. Since Adobe Flash Player received many attacks, Adobe has patched 9 Player holes today, users are encouraged to update or remove them completely from the computer.

FBI and DHS provide many indicators of hacked device capabilities (IOCs), malware descriptions, network signatures, and Yara rules (basic search strings) to help detect hacker attacks from Chosen.

"If users or administrators see Hidden Cobra indicator tools, quickly flag, report to DHS NCCIC or FBI Cyber ??Watch (CyWatch) and prioritize ways to reduce network attacks."

Details information see at this address.