VNCERT issued an emergency alert warning malicious code exploiting Coinhive virtual money

The malicious code will automatically run on the user's computer as an extension or directly in the browser to 'dig' Bitcoin virtual money, Monero ..., illegally use CPU, hard drive, memory ... and send it about hackers' electronic wallets.

According to the warning information released on November 16, through the monitoring of incidents on cyberspace in Vietnam, Vietnam Computer Emergency Response Center (VNCERT) said that many incidents have been recorded. Secure information about malicious code exploiting Coinhive virtual money hidden on websites.

When users visit the site, the Coinhive code library will automatically run on the user's computer as an extension or directly in the browser to 'dig' Bitcoin virtual money, Monero . by using Unauthorized user resources such as CPU, hard drive, memory . and sent to hackers' e-wallets.

Facing this fact, VNCERT Center requires leaders of units to direct the units under management to urgently perform necessary tasks to ensure safety and security.

For website administrators, it is necessary to check and review the source code to detect the inserted code. Identifiers include keywords in the website source code 'coinhive.com', 'coinhive', 'coin-hive', 'coinhive.min.js', 'authedmine.com', authedmine.min.js.

If it detects that the website has been inserted with exploitation codes as mentioned above, it is necessary to check and check the vulnerabilities on the server, the vulnerability on the website, check the leaked accounts have the right to change the source code to overcome The vulnerability is exploited.

For network administrators, implement measures to prevent the unauthorized running of "Coinhive" code on the computer as follows: perform monitoring and disassembly on the computers in the network that appear connect to the following domain names: **afminer.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine .com** .

Use a firewall to block connections to the following addresses: **ifminer.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com , ppoi.org, authedmine.com** .

Scan, examine the system to find and remove code snippets included in the web browser's "Add-on" extension software.

VNCERT recommends that users install extensions: 'No Coin Chrome' or 'minerBlock' for Chrome; Install 'NoScripts' for Firefox.

Along with that, guide users to check the CPU usage of the computer with applications such as Windows Task Manager and Resource Monitor.

If the computer shows signs of slowdown and checks that the performance of the browser or extension CPU is high, it may be that the computer has been infected with Coinhive, urgently need to notify the network administrator for processing.

Regularly check and scan existing vulnerabilities to detect the appearance of malicious code in time. In case of detection of vulnerabilities, immediately implement corrective measures, update additional patches and remove malicious programs that have been inserted by hackers.

After implementation, request the units to report on the situation of infection and the results of processing if available to the National Coordinating Agency (VNCERT Center) before November 30, 2017. VNCERT requires leaders of units to seriously implement the coordination order.

According to ictnews