Cryptocurrency Miners Hacking Servers

Posted At : September 29, 2017 4:54 PM | Posted By : Wil Genovese
Related Categories: ColdFusion, Coldfusion Security, Security

Are your free CPU cycles making others rich? There's a chance they are and it's at your expense. A recent article at **Vice.com** states that "At Least 1.65 Million Computers Are Mining Cryptocurrency for Hackers So Far This Year". If this is to be believed then it's possible a server you are running has been compromised and is actually mining cyrptocurrency for the hackers.

Cyrptocurrency is an anonymous, digital currency that is supposed to be untraceable. It's used on the internet to purchase more and more products and services. One of the most common forms of cryptocurrency is Bitcoin. This is from the **Wikipedia entry on Bitcoin**.

> Bitcoin is a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, since the system works without a central repository or single administrator. It was invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto and released as open-source software in 2009. The system is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a blockchain. Besides being created as a reward for mining, bitcoin can be exchanged for other currencies, products, and services. As of February 2015, over 100,000 merchants and vendors accepted bitcoin as payment. Bitcoin can also be held as an investment. According to research produced by Cambridge University in 2017, there are 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin. ...

Bitcoin Mining is a record-keeping service that runs on peoples computers, servers, or specialized Mining Devices, that are setup by individuals to help process Bitcoin transactions. As a reward for doing this you are given newly created bitcoins and transaction fees. ie. You can make money by mining for Bitcoin.

This reward is enough that hackers have taken it to the next level and started hacking servers around the world so they can install mining software and use YOUR computers and servers to make money for themselves. Just this week it was discovered that some of **Showtime's web servers** were mining cryptocurrency. This isn't a new thing either. Back in 2014 **Iowa State University servers** were also hacked for the purpose on mining Bitcoins. These are not isolated occurrences. They are happening regularly. This practice is free to the hackers an costly to the owners of the servers. Here's why.

Case Study

CF Webtools has seen this type of hack in the real world. We recently had a company come to us seeking our services for both **Server Administration and ColdFusion programming**. Part of taking this new company on as a client we performed a security review on all of their servers. They also had existing issues that we needed to look at in particular. One of their web servers was rebooting multiple times per day at what seemed like "random" intervals.

Upon review we found the web server was always running at 100% CPU usage with no services claiming to be using that much CPU power. Certainly not ColdFusion or IIS. After completing additional research we decided to install a malware removal tool and scanned for malware. It didn't take long to find that indeed there was malware running on the server. What we found surprised us only because we had not seen this in action before. It was a cryptocurrency miner and it was so intensive that it would crash the server. All attempts to remove the malware failed. It would end up back on the server in a short period of time. The fact is this server was compromised. To resolve the issue we sent one of our decommissioned, but powerful servers, preinstalled with a clean OS to their data center. Then our Operations Manager went on the road to install the new server as well as a physical firewall. We essentially rearchitected their entire server setup. Meanwhile the malware removal tool did it's best to keep the malware at bay while I recreated their web server on the new server. It was a busy week (or more), but we were able to clean the code on the clients server and put that on the new server. We also had to research and rebuild all the dependancies from scratch. When it was all said and done we replaced the compromised server with the new one and put all their servers behind a Cisco ASA.

This case of Hacking for Bitcoins proved costly in the end to the company who's systems were compromised all while providing a free profit to the hacker(s).

This is one more friendly reminder to make sure your ColdFusion servers are patched! Either patch them yourself, have your hosting provider patch them. If you need help upgrading your VM or patching your server (or anything else) our operations group is standing by 24/7 - give us a call at 402-408-3733, or send a note to operations at cfwebtools.com.