Threat Bulletin

Cryptojacking

May 2018

Cryptojacking: Real-time Report

Cryptocurrency mining, (or cryptomining) is the process whereby computer programmers, or "miners", run special mining programs on their computers for profit. Using this software, miners solve complex calculations, or algorithms to verify cryptocurrency transactions in order to prevent fraud. The more miners working on the algorithms, the faster the transactions are confirmed, and the less chance there is of fraud occurring. For each algorithm solved, a miner receives a fraction of a bitcoin in payment and the verification of that transaction is added to a distributed digital payment record called the blockchain.

Cryptomining has become increasingly popular and rewarding since the exponential increase in the value of bitcoin and other cryptocurrencies towards the end of 2017. This popularity waned after the collapse in the bitcoin value following the introduction of cryptocurrency futures by the Cboe and CME. However, since that price collapse, cryptocurrency pricing has stabilized and is starting to bring miners back into the field.

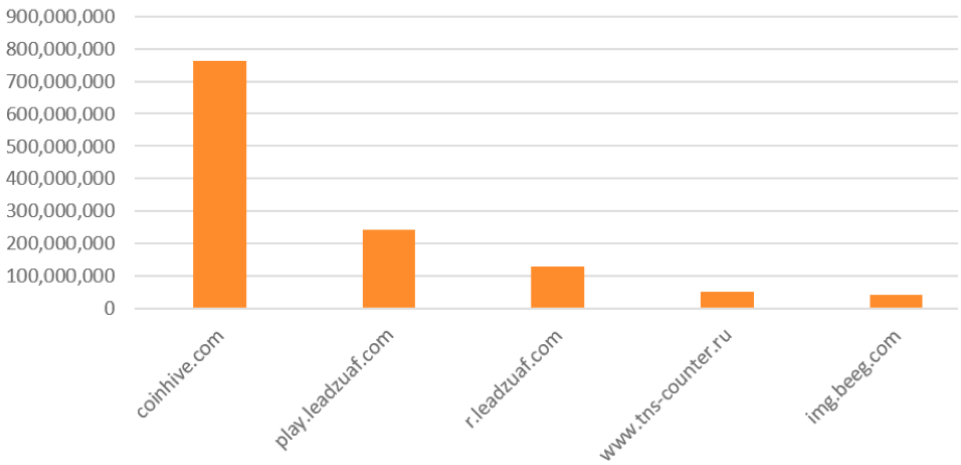
Cryptojacking is the illegal practice of accessing and using the resources of a target computer, mobile device, or server to mine cryptocurrencies. Hackers achieve this goal by using social engineering and other practices to lure targets to click on malicious email links, or by clicking on ads in infected websites that run JavaScript code, which infects the website visitor. Clicking on those email links, or running the website scripts, exploits vulnerabilities in the target devices that hackers can freely manipulate to illegally access target computer resources.

Origins

Cryptojacking made its first appearance in September of 2017, when a website called Coinhive published code that enabled cryptominers to mine the cryptocurrency Monero by donating a small amount of the processing capacity of third party CPUs. The peer-to-peer file-sharing site Pirate Bay then incorporated this code into their website, inviting their clients to use this method to generate funds for Pirate Bay in lieu of viewing on-site ads. Following the Coinhive debut, malicious copycat websites came online providing similar scripts that enabled miners to illegally hijack the computing resources of mobile devices, personal computers, and servers.

A recent report performed by Allot described the number of times that links to questionable Internet sites were blocked in three European countries from Nov. 2017 until Feb. 2018.

Top 5 Total Pre-blocks EU Counties Nov. 2017-Feb 2018



This graph shows the actual number of blocks, the majority of which were Trojan-Bitcoin related. This indicates the high prevalence of malware infections related to bitcoin transactions.

Furthermore, the study also determined that the most blocked webpage, with an astounding 750,000,000 blocks, was coinhive.com

How Does It Work?

Cryptojacking employs JavaScript programs to run on a web page in order to mine cryptocurrencies. Due to JavaScript's widespread use by most Internet users, there is no requirement to install it before mining begins. In fact, due to the small amount of processing power that is "stolen", the user is unlikely to notice any significant fall in computer performance. It is only when multiple events of the script are running, for example when many browser windows are open at once, that the user may experience some downgraded computer response. Additionally, the temperature of the processor will generate a great deal of heat, which is another indication that a device may have been compromised.

In a similar way to a symbiotic relationship in nature, the cryptojacker will feed off his target, but will want to keep him alive so that he can continue to feed.

Cryptojacking not only involves the theft of computer resources, it also results in a drain on battery power and electricity, both paid for by the oblivious target. Finally, the extensive overuse and overclocking of computer hardware will inevitably reduce its lifespan.

Running JavaScript without the consent of a targeted user is unethical at least, and ultimately illegal. Unauthorized entry into computer systems and the illegal use of computer resources is undoubtedly stealing, and such practice is outlawed. "Cryptojacking lite", which takes the form of consensual sharing of computer resources to replace advertising costs, is an accepted practice in the industry. However, this recognized and inventive practice is easily distorted and manipulated to pave the way towards illegal cryptojacking.

Targets

The targets used for cryptojacking are both home and corporate customers, both on-premise and in the cloud. Cryptojackers deploy extended botnets to accumulate CPU cycles to mine digital currencies at low cost.

The most sophisticated cryptojacking programs will "attack" target devices during periods when devices are less active—normally after office hours. In this way, cryptominers will maintain low visibility, which will reduce their chance of discovery by their unwitting hosts. In a similar way to a symbiotic relationship in nature, the cryptojacker will feed off his target, but will want to keep him alive so that he can continue to feed.

No target is out of range of the cryptojackers. The critical Supervisory Control and Data Acquisition (SCADA) facility of a European water company has been hit, as has a Russian facility used in the production of nuclear weapons. Likewise, the International Commissioner's Office (ICO) in the United Kingdom was also targeted. The threats are significant, and growing.

Trends and Evolution

Although cryptocurrencies have been around for the best part of a decade, it is only since mid-2017 that they have attracted mainstream investment, and also criminal, interest. Should the cryptocurrency highs of December 2017 prove to be the bubble that burst, then in all likelihood, cybercriminals will move onto other projects. However, if blockchain technology and the cryptocurrencies that fund its development are here to stay, then malware and criminal activity associated with cryptojacking will continue to expand.

Protection

Cryptojacking has surpassed many other cybercrimes such as ransomware, and as such is of primary concern to all home and corporate computer users. "Sharing" CPU power can be dressed up in many ways, but increasingly it is now being used for criminal purposes.

So, can anything be done to protect against cryptojacking? Fortunately, the answer to this question is "yes". The following sections explain the steps that can be taken by specific groups of targets.

For Corporate Users

Any IT manager or system administrator worth their salt will have their on-premise server array protected with hardened credentials. In fact, it is doubtful whether any cybercriminal would attempt to access corporate servers through such an avenue. However, this is unfortunately less true when those credentials apply to cloud resources. This is the favored target of attack for cryptojackers, and it is in that direction that IT professionals should place greater emphasis.

Access control protection is another area that cryptojackers can exploit to gain access to corporate computer resources. In February of 2018, electric car manufacturer Tesla left its Kubernetes cloud containers open and cybercriminals accessed their systems installing cryptocurrency miners on those Kubernetes containers.

To protect corporates from covert cryptomining, the most efficient and detectable solution is to approach this issue through network visibility and monitoring. This practice has proved itself as an effective defense against cryptojacking and is not complicated to implement. In October 2017, Vodafone Spain, using its Secure Net cybersecurity service that protects devices connected to its mobile network, blocked cryptohijacking attacks on 750,000, or 17% of the 4.3 million Spanish customers who subscribed to this service. In 98% of the cases, Vodafone Secure Net blocked access to the websites that contained a cryptomining program, and 2% of the blocks were made as the software was in the process of installation (Read the complete article).

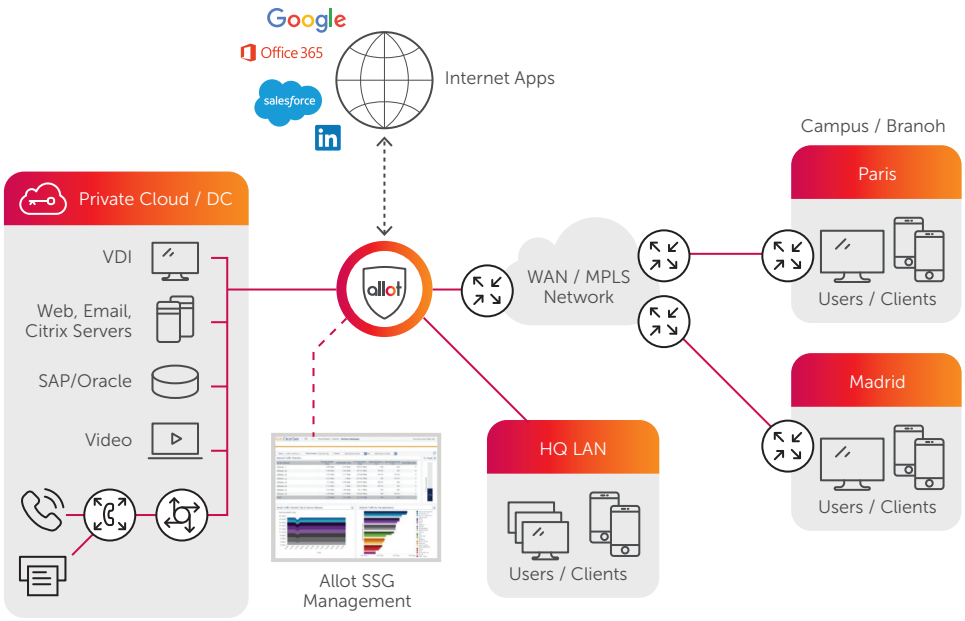
Correct scanning and visibility into what is running on servers and across a network is of vital importance when detecting and defending against potential cryptojacking attacks. Cryptocurrency mining software is resource intensive, so any CPU processes that are not recognized that are also consuming inordinate amounts of resources should also be investigated.

For Consumers

There is a clearly-defined and well-publicized list of measures that consumers can take to protect their computer systems and mobile devices. These include:

- Employ strong passwords for computers, IoT devices, and Wi-Fi networks.
- Never use common or easily guessable passwords such as “123456” or “password”.
- Purchase online security protection from your Internet or Communications Service Provider.
- Patch your operating system and software on a regular basis.
- Never click on an email link unless you know who sent it to you. Email is the number one vector for infecting computer systems with malware.
- Perform regular back ups of your files. This also removes the chance of any ransomware attack in the future.

Network Monitoring Layout



Need a defense strategy against cryptojacking? We can help.

Contact Allot »