Bitcoins & Cryptojacking

Introduction to Cryptocurrencies

To some degree or another, most of us have heard of the term "Virtual Currency". This is essentially the cloud-based version of the traditional paper money. For example, with Ransomware a Cyber attacker wants to be paid with this new type of currency, usually in the form of Bitcoin. There are other types of virtual currencies that are out there, and collectively, these are also known as "Cryptocurrencies".

There was a time earlier this year, when Cryptocurrencies were all the rage, especially in the financial markets. Futures contracts and even indexes were created and tracked for them, and were traded heavily. For a period of time, the value of them went sky high, and people thought that this would be the real thing again, just like the .com craze back in the early 90's.

Cryptomining & Cryptojacking Defined

But, as that came to a crashing end, so did the volatility of the Cryptocurrencies. They are still being traded, but not with the volume and the market capitalization that it once had. Now, here is another twist to the story. The Cyber attacker is entering into this realm, with a new threat called "Cryptojacking", which is essentially mining the various Cryptocurrencies for monetary value.

But first, it is important to define what Cryptomining is all about, and it is as follows:

"Bitcoin mining is done by specialized computers. The role of miners is to secure the network and to process every Bitcoin transaction. Miners achieve this by solving a computational problem which allows them to chain together blocks of transactions (hence Bitcoin's famous "blockchain"). For this service, miners are rewarded with newly-created Bitcoins and transaction fees."

(SOURCE: https://www.buybitcoinworldwide.com/mining/).

Technically, Cryptojacking can be defined as follows:

"Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser." (SOURCE: https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html).

The Blockchain Explained

Ok, so now we have two long definitions, let us put these in simpler terms. We all have an idea of what a virtual currency is. Because there is no way to actually track down this digital currency, it needs to be made secure on the Internet.

So, this is where the mining aspect of it comes into play. It is the job of the miners to protect all of these currencies and transactions, by having the ability to solve very complex math problems.

Once this has been done a successive fashion, all of these transactions then form a "block" (aka the "Blockchain") which creates the line of defense to protect these virtual currencies and their associated transactions. In return for their services, these miners (which are legal entities by the way), are paid a certain fee percentage.

How a Cryptojacking Attack is Launched

Because of the return that is associated, the Cyber attacker now wants to gain their foot into this game, and become cryptominers themselves, but of course illegally. But keep in mind, there are very complex mathematical problems to solve in order the miner to be rewarded. This of course takes a lot of computing and processing power.

The Cyber attacker does not want to spend the money in terms of procuring the extra hardware to do this, so as the above definition states, he or she will hijack your computer, and from there, steal the processing power as well as the electricity in order to mine the Cryptocurrencies. You may be asking at this point; how can they do this to your computer?

It's quite easy. All they have to do is send you a Phishing like Email, which contains a malicious link or attachment. Once you have fallen victim to this, a specialized Cryptomining code is then installed onto your computer or even mobile device.

But what is even stealthier is that even if you visit a website, there could be infected pieces of Java source code running behind the site you are viewing, and from there, the Cryptomining code can then be covertly loaded onto your computer. At this point in the game, the Cryptomining code is now technically malware.

But the problem with this new malware is that it is very difficult to spot on your computer, and can installed and deployed in a very sneaky manner. In these instances, the Cyber attacker is not just exclusively targeting computers and wireless devices, they will go after anything that will give them free electricity. This includes servers, routers, cable modems, firewalls, network intrusion devices, etc.

It is also important to keep in mind that there is no specialized package that the Cyber attacker has to deploy onto a device – the malware is just a few lines of infected source code, and as a result, this makes it all the more difficult to detect. Because of the extremely low overhead that is required, and its sneaky nature, the rise in Cryptojacking has increased significantly.

For example, McAfee has just discovered almost 3 million new cases of it, which ***is a staggering 629% increase from 2017***. So, what are some of the telltale signs if your computer has been hijacked for the purposes of Cryptojacking? Here are some clues:

*Slowdown in the speed of your computer;
*Very slow load times when trying to connect to the Internet;
*A slow increase in your electricity bill.

Cryptojacking & The Cloud

It is important to keep in mind that the Cryptojacker of today is not just out to steal the processing and electrical resources of your individual computer and/or wireless device. They are also out to attack the

overall Cloud Infrastructure, as there are many more resources that can be used to launch even stealthier and more covert Cryptojacking attacks. A prime example of this is Tesla.
They are an auto manufacturing company, and have used the Amazon Web Services (AWS) for their Cloud Infrastructure needs. In this particular instance, they made use of an open source platform available from Google called the "Kubernetes System". This is an application which allows for businesses and corporations to completely automate the deployment, scaling, and the management of containerized Cloud based applications.

Tesla had deployed the Kubernetes System onto their AWS Platform, but it was not made secure enough (there was no administrative password that was created and implemented), because various Cryptojackers were able to gain access to their overall AWS Environment. After this was accessed, numerous Cryptojacking mining scripts were then covertly installed onto the particular Kubernetes System instances.

As a result of this, the Cryptojacker was then able to gain 100% control of Tesla's AWS processing and electrical resources, and use that to launch multiple Cryptojacking attacks. They were also able to gain access to sensitive information and data, which were located in Tesla's AWS Simple Storage Service (S3) buckets.

The Cryptojackers also used other tactics to avoid detection. For example, they made use of private Mining Pool Software packages, which was then utilized to instruct the mining scripts to connect to an unlisted endpoint. By making use of this approach, existing Domain and IPI based threat detection systems could not pick up on the Cryptojacking activities that were taking place.

Also, the Cryptojackers were able to mask the true IP address of the mining pool by hiding them behind a Content Delivery Network known as "CloudFlare." They were even able to make use of nonstandard Network Port Numbers to secretly communicate with the hidden IP addresses. This is was all done in an effort to keep CPU usage low. This strategy allowed for any type of suspicious network-based traffic to go undetected for long periods of time.

Typically, Cryptojackers have made use of JavaScripts from which to leverage their attacks. But now, they are using more advanced techniques such as the exploitation of Zero Day Vulnerabilities and compromising Network Endpoints in order to create Cryptojacking Botnets. In fact, 80% of organizations that rely upon the AWS or Microsoft Azure to house their IT Infrastructures are at risk of falling victim to a Cryptojacking attack.

Although not using a password (or even a weak one for that matter) can be a major cause for these kinds of attacks, the implementation of very poor-quality API Access Rules also exposes root accounts to be further manipulated in order to launch Crpytojacking attacks.

Conclusions

So, what can a business or a corporation do protect their Cloud Infrastructures from being used by a Cryptojacker? Here are some recommended strategies:

1) Take ownership of your Security responsibilities. Although it is up to your Cloud Provider to provide all of the Security features that they can, it is still your primary responsibility to work with your Cloud Provider to make sure that everything is properly configured. If you are offered

default Security settings, don't use them and create your own that specifically tailored to your Security requirements. Also make use of advanced Encryption techniques if they are offered by your Cloud Provider.

2) Many cloud based Crpytojacking attacks can be traced back to poor login credentials (once again, using very weak passwords). Make use of a Password Manager to create long and complex passwords.

3) Set up your Virtual Machines as you absolutely need them. Do not create extra ones that you are not going to use, as this will simply increase the attack surface for the Cryptojacker.

4) Make sure that you educate anybody in your organization that is tasked to manage your Cloud Infrastructure in its proper design and secure deployment.

But just like how a Cloud Infrastructure is prone to a Cryptojacking attack, so are mobile apps. In fact, a recent study (conducted by a Cyber security firm known as Sophos) detected 25 rogue mobile applications which had the infected Cryptojacking source code in them. These mobile apps were downloaded at least 120,000 times by different end users. This can be illustrated in the diagram below:

SOURCE: https://www.nbcnews.com/tech/tech-news/your-computer-could-be-quietly-mining-bitcoin-someone-else-n922101)

The details of the Sophos study can be seen here:
https://news.sophos.com/en-us/2018/09/24/cryptojacking-apps-return-to-google-play-market/

So, in response to the recent to this, tech giants like Google and Apple whom have mobile app stores are taking proactive actions to protect their customers. For example, with the former, they no longer allow for browser extensions in its Web Store that mine cryptocurrencies. The Google Play Store allows for customers to pick extensions and apps that personalize their Chrome web browser, but this will now become highly restricted.

Sources

https://searchcloudsecurity.techtarget.com/tip/How-to-prevent-cloud-cryptojacking-attacks-on-your-enterprise

https://www.globalknowledge.com/blog/2018/03/20/cloudjacking-and-cryptojacking-are-leaving-cloud-owners-in-the-dark/

https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/

https://searchsecurity.techtarget.com/news/252435506/Cryptojacking-attacks-hit-enterprises-cloud-servers