Cryptomining & Cryptojacking Malware

Report by Jeffrey Farnan

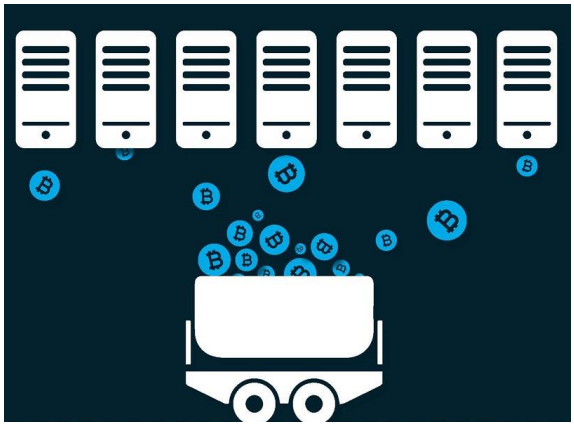
TABLE OF CONTENTS

INTRODUCTION

This report will look at Cryptomining, explain the different types of Cryptomining, how bitcoins are created and mined. Take a look at Cryptomining Malware and how it is deployed. Explain what Cryptojacking is and how it infects browsers, the top Cryptojacking malware out today and current trends.

WHAT IS CRYPTOMIING

Cryptomining is a process in which a machine performs certain tasks to obtain a little bit of cryptocurrency. You can start of small by downloading the software, using your own machine to start mining,or you can become a legitimate cryptominer, investing in the setup and resourses which is very costly.



Bitcoin miners receive Bitcoin as a reward for completing "blocks" of verified transactions which are added to the blockchain. Mining rewards are paid to the miner who discovers a solution to a complex hashing puzzle first, and the probability that a participant will be the one to discover the solution is related the portion of the total mining power on the network.

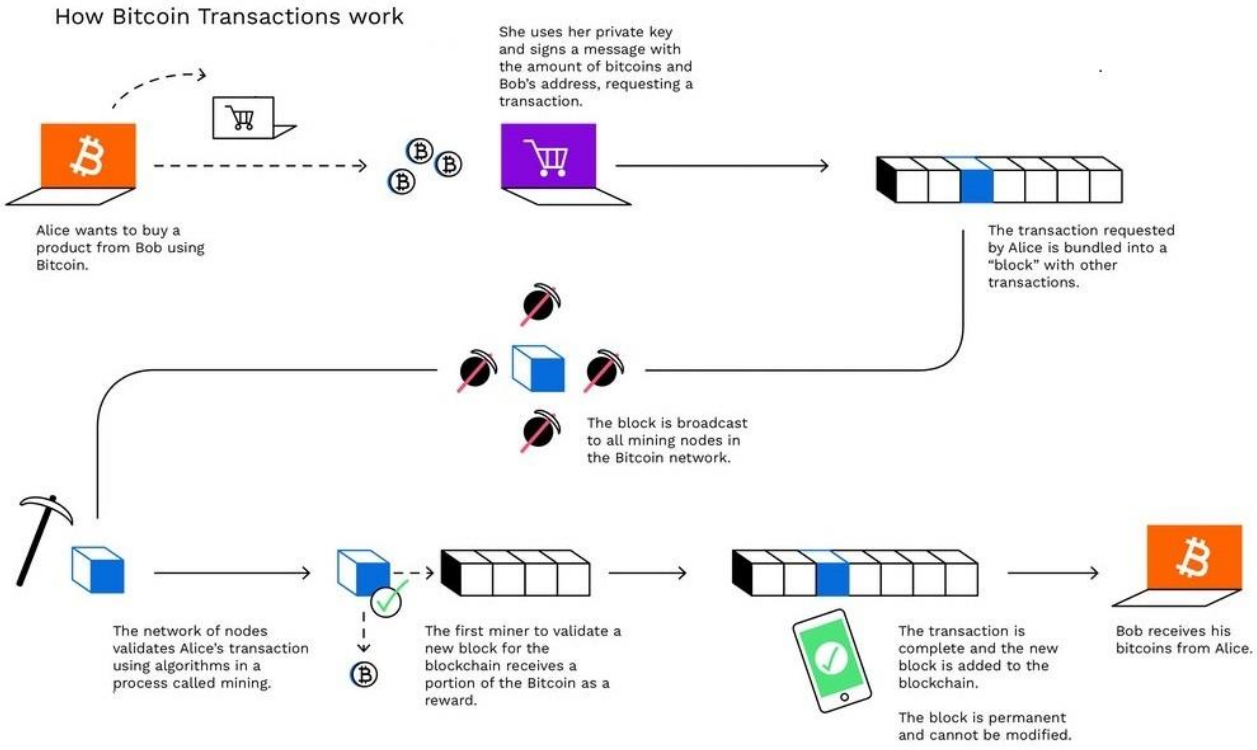
What is Bitcoin

- There are more than 1,300 cryptocurrencies the best known is Bitcoin, which was created in January 2009.
- It is a digital currently offers the promise of lower transaction fees than traditional online payment mechanisms.
- It is under no authority unlike government-issued currencies, it is not backed by any banks or governments, it is not legal tender.
- Bitcoin mining has a two-fold purpose: it allows for the creation of new coins and facilitates the processing of transactions in the network.

HOW IS BITCOIN MINED

In order to become a Bitcoin miner, a person first needs a computer and mining software like Coinhive. This program uses the computer's resources to perform complex mathematical calculations.

Bitcoin mining is the process of adding records of a new transaction to the Blockchain, the public ledger of all transactions that have ever taken place in the Bitcoin network.
New transactions are added in batches called "blocks" hence the name Blockchain. Then ledger is needed for the nodes of the Bitcoin network to always be able to confirm valid transactions.



Roughly every 10 minutes the Bitcoin code creates a 'target' number that the mining machines try to guess, call this finding the next block. Whichever machine guesses the target number first earns the mining reward, while also earning the transaction fees that people spent sending bitcoin to each other.

DIFFERENT TYPES OF CRYPTOMINING

There are different methods to mine crypto currency:

- **CPU Mining**: A CPU miner uses the computer's central processor to do the mining and so a powerful processor will give you more mining power.

CPU Mining

- **GPU Mining:** Graphics Processing Unit, is responsible for the digital rendering in a computer system. Due to a GPU's power potential vs. a CPU, or central processing unit, they have become more useful in mining due to their speed and efficiency.

GPU Mining

- **Cloud Mining:** A host company owns Bitcoin mining hardware and runs it at a professional mining facility. You pay the company and rent out some of the hardware.

Cloud Mining

- **FPGA Mining:** makes use of the new generation of FPGA chips capable of delivering high hash rate power at low power consumption.

FPGA Mining

- **ASIC Mining:** Application-Specific Integrated Circuit, a device especially designed to mine a specific digital currency.

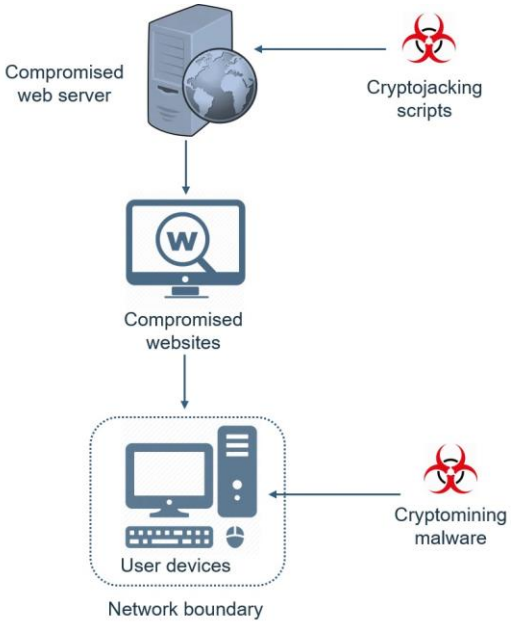
ASIC Mining

CRYPTOMINING MALWARE

How Cryptomining is deployed

Cryptomining malware arrives on users systems using various ways:

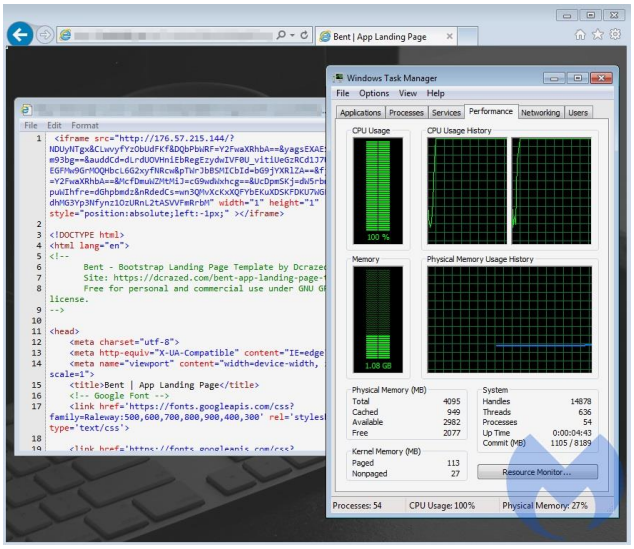
- These may be dropped or downloaded by other malware or users surfing malicious sites may also unknowingly download these onto their system.
- Crybercriminals may exploit a certain network vulnerability in order to infect users system with these malware.
- Once the malware is installed in a users system, if forces the infected system to generate bitcoins or join a mining pool without the users knowledge.
- Bitcoins generated by the malware land in the cybercriminals eagerly waiting hands.



WHAT IS CRYPTOJACKING

Up until recently malicious cryptominers would try to download and execute on targeted devices, with high levels of security catching these executables were being caught. A new method called “cryptojacking” allows the same activity to run in a browser without any software being downloaded.

- The victim clicks on a malicious link in an email that loads Cryptomining code onto the victims device. Another method is by infecting a website with JavaScript code which auto-executes once loaded in the victims browser.
- The unsuspecting victims use their machines as normal, while the Cryptomining code works in the background. The only sign a victim may notice a slower performance or a lag in execution.



Why Cybercriminals use Monero

- The best known Cryptocurrency is bitcoin but cybercriminals are known to use Monero.
- Monero which differs from Bitcoin in that its transactions are virtually untraceable, and there is no way for an outsider to track Monero transactions between two parties.
- Naturally, this quality makes Monero an especially appealing choice for cybercriminals.

TOP CRYPTOJACKING MALWARE

At its height in 2018 Cryptojackers is reported to have affected 55% of worldwide businesses using as much as 65% of their CPU power. Here are some of the most popular Cryptomining software:

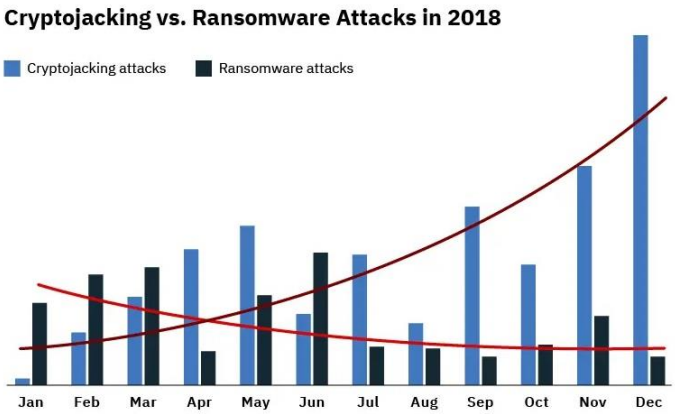
- **Jsecoin:** a JavaScript miner that can be embedded into websites and runs directly in the browser.
- **XMRig**: is a Trojan Horse posing as Adobe Flash Player which can mine different types of digital currency.
- **Cryptoloot:** started off as a legal software letting users who want to mine use their code, was taken advantage of by hackers for their own purposes.
- **Coinhive:** Coinhive's code frequently locks up a user's browser and drains the device's battery as it continues to mine Monero for as long a visitor is browsing the site.
- **WannaMine:** is designed to mine Monero. It cripples computer resources to maximum use of the processor and RAM, causing the computer to fail and eventually die.
- **RubyMiner:** goes after Windows and Linux webservers using outdated software.

Cryptojacking vs Ransomware Attacks

From 2017 – 2018 saw a big increase in Cryptojacking compared to Ransomware over the same period.

Some of the reasons are:

- Victims are unaware.
- Can remain undetected.
- Can infect corporate workstations as well as servers.
- The more machines which are infected the greater the profits for the attacker.



PREVENT BROWSER CRYPTOJACKING

People usually think their “secure” browser can prevent Cryptojacking, unfortunately this is not true here are some ways to spot and prevent browser Cryptojacking:

- Use antivirus software with added miner detection built in.
- Have web filtering tools kept up to date, which should detect Cryptojacking scripts.
- Check for legitimate browser extensions, delete non-legitimate extensions.
- Use a cloud Browser which provide a higher level of protection.
- Include Cryptojacking in company security awareness training, with including warning signs of a Cryptojacking attack.

Current Trends

- Although Cryptojacking attacks dropped significantly in previous years mainly due to the sharp fall in the value of cryptocurrencies, this trend remains a threat.
- As cryptocurrency prices continue to rise through 2020, Cryptojacking malware attacks will continue to be lucrative for cybercriminals.