How much do you know about **crypto mining malware**?

Get up to speed on the new generation of malware, and learn **how to protect yourself from crypto malware attacks**

Source: Pixabay

You've probably heard about malware being used to steal peoples' crypto or other digital assets, but what about **crypto *mining* malware**? Many people often claim that the world of crypto is like the Wild West. While that's definitely exciting, there is also a fair amount of danger.

If you take the proper precautions, you can avoid falling victim to a scam or hack. But part of preparing is knowing what to look out for. **Crypto mining malware** is a unique cause of **crypto malware attacks** because it doesn't steal your data, money, or digital assets.

So if **crypto mining malware** doesn't steal these things, what does it do? And is it possible to learn **how to protect yourself from crypto malware attacks**?

Crypto malware terms to know

Crypto mining

To understand **crypto mining malware**, you first have to know what crypto mining is. Crypto mining is the process of creating new cryptocurrency coins. Mining involves a network of computers around the world competing to be the first to solve a complex cryptographic puzzle. These puzzles are mathematical equations that verify transactions and add security to the blockchain network when solved. In return for doing this work, the miners operating the computers receive some cryptocurrency as a reward.

Malware

A combination of the words "malicious software." Malware is developed by hackers to steal someone's data, sensitive information, money, and other valuable files stored on their computer.

Ransomware

Ransomware is a type of malware that takes over the victim's computer. The hacker then demands the victim pay a ransom to regain access to their computer and data. In some cases, the victim is completely locked out of their computer controls, keyboard, and mouse functionality.

Crypto malware

Crypto malware is another way to refer to **crypto mining malware**. It is the actual malware program used in the process of criminal crypto mining. It is a type of malware that allows the hacker to use the CPU power of the victim's computer to conduct crypto mining without the victim's knowledge.

Source: Pixabay

Crypto ransomware

Crypto ransomware is one of two main types of ransomware. It takes over a user's computer files, encrypts them, and then demands a ransom payment to decrypt the files and let the user regain access.

Cryptojacking

Cryptojacking is the name for the process of criminal crypto mining. Hackers use crypto malware to harness the CPU power of the victim's computer. Unlike other forms of malware or ransomware, these programs aim to work undetected by the victim.

Encryption Trojans

Encryption Trojans are the vehicles that deliver various ransomware onto a victim's computer. They can come from links in a suspicious email, an infected website, app, or browser plug-in, or any downloadable content from an untrustworthy website.

How **crypto mining malware** differs from other malware, ransomware, or cryptojacking

With so many terms related to **crypto mining malware**, things can definitely get confusing. Especially if you're new to crypto, it can be hard to know **how to protect yourself from crypto malware attacks**. After all, do these terms refer to the same thing? Is each one a different type of attack?

Overall, these terms are pretty similar, but they have some slight differences in meaning that are important to understand. Let's break it down further:

Crypto ransomware vs. **crypto mining malware**

These are two distinct types of malware that attack someone in different ways. The goals of the hackers using these attacks are also different.

Crypto ransomware is used to steal crypto or money from the victim; the hackers' primary goal is to get money. Ransomware is somewhat riskier for the hacker than other malware methods because the hacker has no guarantee the victim will pay the requested amount.

On the other hand, the goal of **crypto mining malware** is to only use the processing power of the victim's computer to mine cryptocurrency. Unlike ransomware, this type of malware seeks to remain undetected, making it much harder to learn **how to protect yourself from crypto mining attacks**.

Crypto mining malware works in the background of your computer, and you wouldn't know it unless you notice your computer performance getting slower.

Source: Pixabay

Crypto malware vs. **crypto mining malware**

These two terms actually refer to the same thing: a form of malware that is specifically designed to use the victim's computer to mine cryptocurrency.

Malware more broadly, including ransomware, has been used throughout both the crypto and non-crypto worlds. It is used to steal items of value like private data, logins and passwords, financial information, and money, including Bitcoin and other cryptocurrencies.

According to SonicWall's 2020 Cyber Threat Report, 2020 saw 5.6 billion malware attacks globally. This is actually down 43% from 2019. In addition, while different malware variants are on the decline, certain types are gaining more use, including ransomware, IoT attacks, and cryptojacking. And new ones are popping up all the time as hackers figure out new ways to get around existing defense systems.

But **crypto mining malware** is a newer form of malware that has only gained popularity among cybercriminals in the past couple of years. In the same report, SonicWall claimed a 28% increase in **crypto malware attacks** from 2019 to 2020.

Crypto malware is unique from other kinds of malware because its only goal is to steal the processing power of the victim's computer– not their data or money. While this might sound

relatively harmless compared to other malware attacks, it still comes with some serious consequences for the victim that we'll get into below.

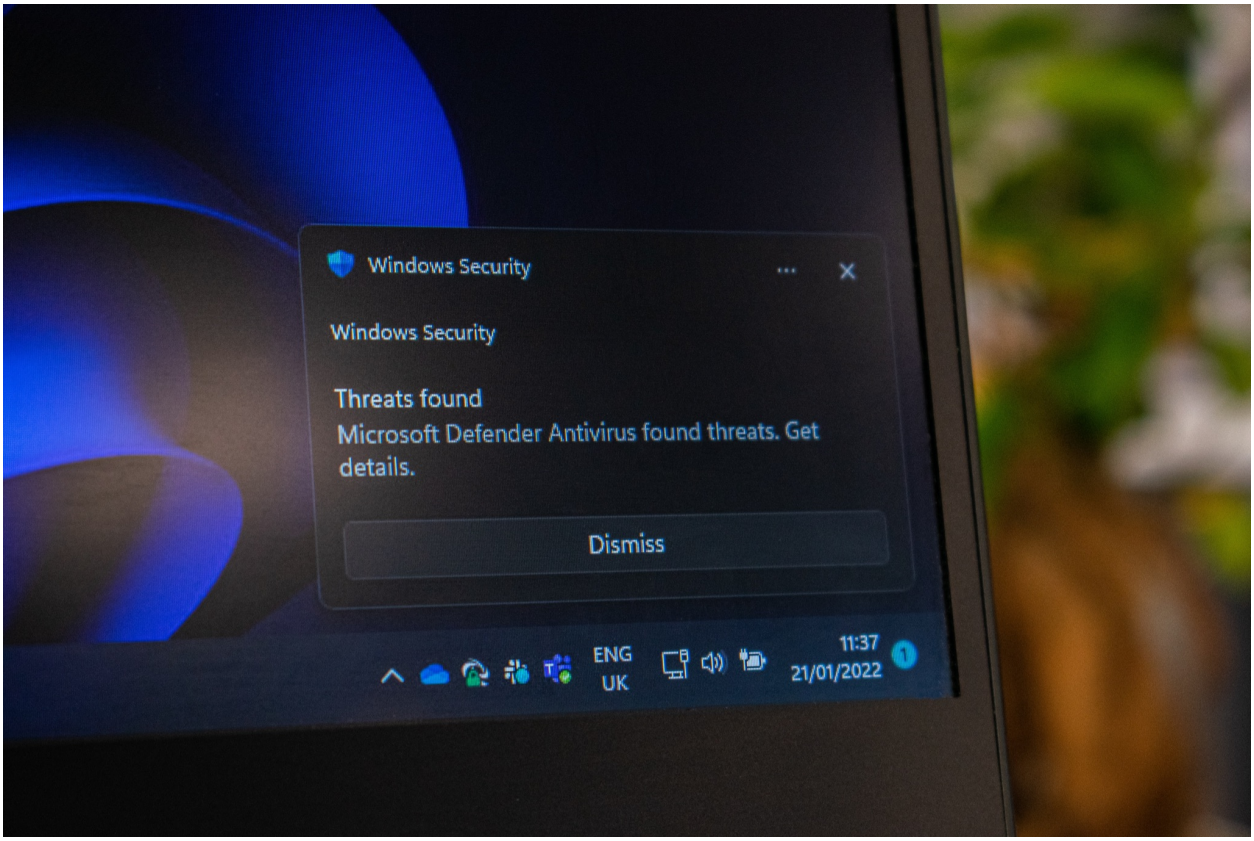
Cryptojacking vs. **crypto mining malware**

These two terms are closely related but have different meanings: **crypto mining malware** is the malware used to initiate the process of cryptojacking.

Crypto malware attacks can come in different forms. In some cases, the hacker doesn't need to gain direct access to the victim's computer. Instead, they can create JavaScript code that runs on a single website. When someone visits the website, the code lets the hacker use that person's CPU power for the duration they're on the site.

Crypto malware can also infect servers. In this case, individuals who access the websites hosted on the server won't be affected; only the server power itself will be used by the hackers.

Cryptojacking is the criminal activity of harvesting CPU power without the individual's consent. Why would hackers even want to steal CPU power? Mining cryptocurrency is expensive and requires a lot of energy and equipment. If someone can't afford to purchase a mining rig or pay for 24/7 electricity to run it, then they might turn to stealing that energy from someone else's computer, leaving the victim to pay the energy bills.



Source: Photo by Ed Hardie on Unsplash

Recent **crypto malware attacks** and effects of cryptojacking

So, what's so bad about cryptojacking if your data and money aren't stolen? Well, **crypto malware attacks** slow down your computer significantly.

If left to run, **crypto mining malware** can result in your graphics card or processor chip burning out, your computer's performance becoming extremely slow, your computer overheating, and even its memory declining.

And because **crypto mining malware** runs 24/7, it will consume a large amount of electricity, which you will end up paying the bill for. So while the hackers don't steal your money directly, you still lose it in the end. This is why it's important to learn **how to protect yourself from crypto malware attacks**.

Some recent **crypto malware attacks** include crypto mining companies Coinhive and Crypto-Loot. Both services let website owners install crypto miners on their websites through Javascript code. Coinhive was a legitimate service that worked as an alternative to having ads on the site.

This software worked through an individual's browser to use their excess CPU power while they visited the website.

However, hackers quickly exploited the code by adding it to thousands of websites – without the owners' knowledge. It even affected major sites like YouTube and the LA Times. This rise in cryptojacking prompted CoinHive to officially shut down in 2019.

Crypto-Loot follows the same idea and was similarly intended not to harm website users. It even gives website owners the ability to inform the website visitors and have them opt-in to the process.

However, this feature is optional, which means hackers can still exploit Crypto-Loot the same way as Coinhive. However, Crypto-Loot can only mine coins for one blockchain called uPlexa, so it isn't as widely used as CoinHive was.

Source: Pixabay

What's the best way to prevent cryptojacking?

So what can you do to prevent cryptojacking from happening to you? The problem with **crypto mining malware** is that it is very good at staying undetected – making it difficult to remove them once your computer is infected.

In fact, crypto malware can hide within useful programs and disguise itself so it isn't immediately noticeable. Some viruses don't even live in files, meaning they can't be removed by just deleting a contaminated file. But this doesn't mean that **crypto mining malware** is impossible to remove!

The best way to protect yourself is through prevention. On the simple end, top-of-the-line antivirus software is a must. Avoiding any suspicious websites, emails, ads, and links is also crucial. You should also make sure all your software is updated to the most current version.

In addition, using an ad-blocker or VPN can help protect you. If you're really concerned about encountering crypto malware, you can disable JavaScript when you visit a website (keep in mind this will affect other features on the site).

There are also browser extensions that guard against **crypto mining malware** while you're online: minerBlock, No Coin, and Anti Miner. Even Google added a crypto mining prevention device in early 2022 in response to an increase of mining attacks on users' Google Cloud accounts.

How to protect yourself from crypto malware attacks

If you suspect your computer could be infected with this malware, monitor the CPU usage and the computer's overall performance. If any apps are maintaining unusually long connections to the internet, it could be a sign of mining activity.

In this case, run an antivirus software capable of removing file-less viruses. If you're having difficulties, consider consulting a professional to remove the virus. If the cryptojacking is happening on a website, closing your browser should be enough to stop it.

About the author:

Jennifer Jones is a content writer who just recently started exploring the world of crypto. She loves learning about new things and breaking down complex ideas. Whenever she's not writing, she enjoys playing guitar and obsessing over her cats.

About Decentral Publishing:

Decentral Publishing is dedicated to producing content through our blog, eBooks, and docuseries to help our readers deepen their knowledge of cryptocurrency and related topics. Do you have a fresh perspective or any other topics worth discussing? Keep the conversation going with us online at: Facebook, Twitter, Instagram, and LinkedIn.

Legal disclaimer:

The views and opinions expressed in this website, its publications, and video content are the Company's opinion. Investing involves the risk of loss as well as the possibility of profit. All investments involve risk, and all investment decisions of an individual remain the responsibility of the individual. Option investing involves risk and is not suitable for investors. Past performance and recommendations are not a guarantee of future results. No statement in this website, its publications, and video content should be construed as a recommendation to buy or sell a particular option and/or security. Decentral Publishing ("Company") has not made any guarantees that the strategies outlined in this website, its publications, and video content will be profitable for the individual investor and are not liable for any potential trading losses related to these strategies. For more information about the terms of service for this website, its publications, and video content, please refer to Decentral Publishing Terms & Conditions.

Focus keyword:

Crypto mining malware

Secondary keyword(s:

Crypto malware attacks

How to protect yourself from crypto malware attacks

Social description + hashtags:

Twitter: What is crypto mining malware, and how is it unique from other malware? Learn more about this relatively new type of cyberattack and how to prevent it! #cybersecurity #malware #cryptomining #bitcoin

Facebook: You've probably heard of malware stealing peoples' digital assets, but what about a malware attack that steals someone's computing power? Learn more about crypto mining malware in this post!

LinkedIn: Crypto mining malware is a type of malware attack that steals someone's CPU power to mine crypto. Learn more about how it works and how you can prevent it.

Short description:

Crypto mining malware is a virus that steals CPU power. Learn how it works and how to prevent it.

Long description:

You've probably heard about malware designed to steal peoples' crypto coins and other digital assets, but what about crypto mining malware? This type of virus is used in crypto malware attacks that steal someone's CPU power – not their money or data. The hackers then use this power to mine cryptocurrency. Learn how crypto mining malware works and how to protect yourself from crypto malware attacks in this post.