The rise of cryptojacking

Malware has been around nearly as long as computers.
In its earliest forms,
it was used by troublemakers
as a form of digital vandalism.
In today's digital world, alware has become a profitable crime that attackers use for their own financial gain.
As a security professional, it's important that you remain aware of the latest evolutions.
Let's take a closer look at one way malware has evolved.
We'll then use this example to consider how malware can be spotted and how you can proactively protect against malware.
Ransomware is one of the types of malware attackers use to steal money.
Another more recent type of malware is cryptojacking.
Cryptojacking is a form of malware that installs software to illegally mine cryptocurrencies.
You may be familiar with cryptocurrency from the news.
If you're new to the topic, cryptocurrencies are a form of digital money that have real-world value.
Like physical forms of currency, there are many different types.
For the most part, they're referred to as coins or tokens.
In simple terms, crypto mining is a process used to obtain new coins.
Crypto mining is similar to the process for mining for other resources, like gold.
Mining for something like gold involves machinery, such as trucks and bulldozers, that can dig through the Earth.
Crypto coins, on the other hand, use computers instead. Rather than digging through the Earth, the computers run software that dig through billions of lines of encrypted code.
When enough code is processed, a crypto coin can be found.
Generally, more computers mining for coins mean more cryptocurrency can be discovered.
Criminals unfortunately figured this out.
Beginning in 2017, cryptojacking malware started being used to gain unauthorized control of personal computers to mine cryptocurrency.
Since that time, cryptojacking techniques have become more sophisticated.
Criminals now regularly target vulnerable servers to spread their mining software.
Devices that communicate with the infected server become infected themselves.
The malicious code then runs in the background, mining for coins unknown to anyone.
Cryptojacking software is hard to detect.
Luckily, security professionals have sophisticated tools that can help.
An intrusion detection system, or IDS, is an application that monitors system activity and alerts some possible intrusions.
When abnormal activity is detected like, malware mining for coins, the IDS alerts security personnel.
Despite their usefulness, detection systems have a major drawback.
New forms of malware can remain undetected.
Fortunately, there are subtle signs that indicate a device is infected with cryptojacking software or other forms of malware.

By far the most telling sign of a cryptojacking infection is slowdown.
Other signs include increased CPU usage, sudden system crashes, and fast draining batteries.
Another sign is unusually high electricity costs related to the resource- intensive process of crypto mining.
It's also good to know that there are certain measures you can take to reduce the likelihood of experiencing a malware attack like cryptojacking.
These defenses include things like using browser extensions designed to block malware, using ad blockers, disabling
JavaScript, and staying alert on the latest trends.
Security analysts can also educate others in their organizations on malware attacks.
While cryptojacking is still relatively new, attacks are becoming more common.
The type of malicious code cybercriminals spread is continually evolving.
It takes many years of experience to analyze new forms of malware.
Nevertheless, you're well on your way towards helping defend against these threats.

Revision #1
Created 2023-08-27 13:56:00 UTC by naruzkurai
Updated 2023-08-27 13:58:47 UTC by naruzkurai