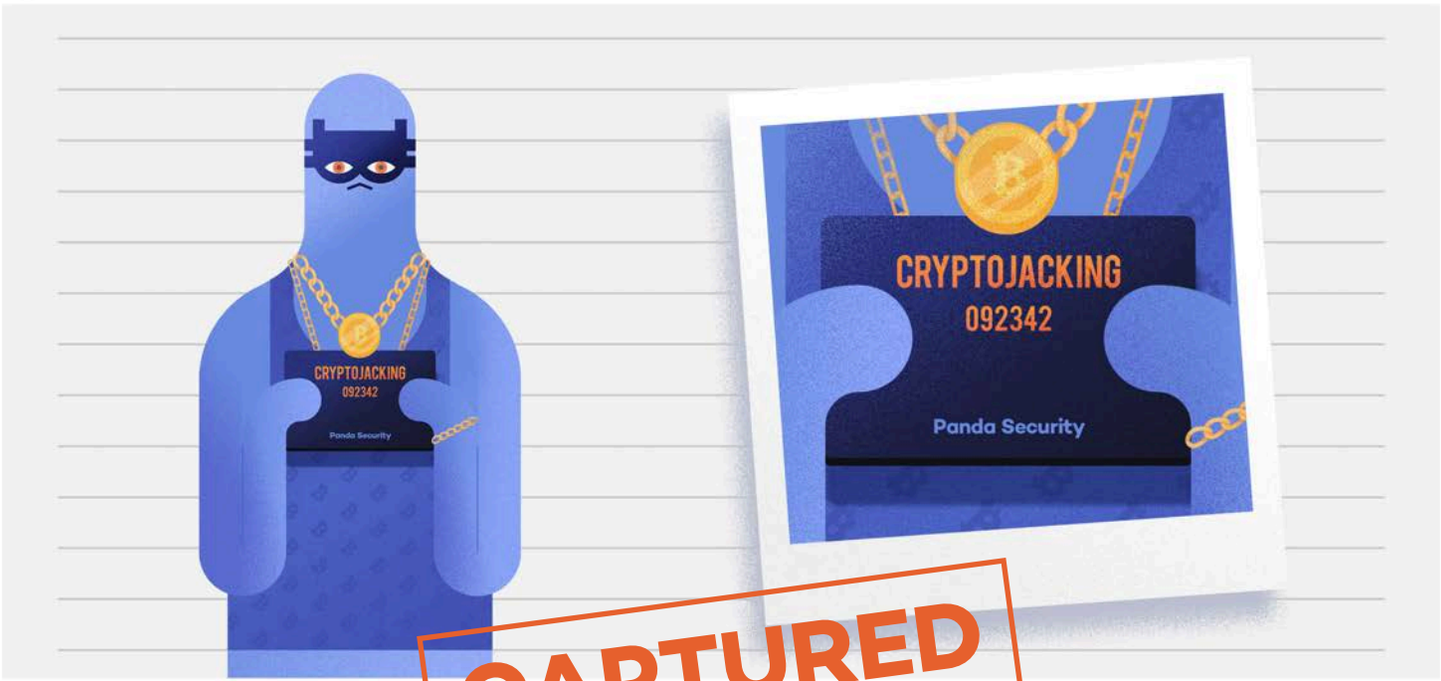

Name

Cryptojacking

Date of Birth

2011

Origin

Clues point to Russia.

Modus Operandi

Cryptojacking uses other people's devices without permission to mine cryptocurrencies illegally.

Attackers make use of malware to take over computers, tablets, or smartphones and take advantage of their processing power to mine cryptocurrencies in secret, using the devices' energy resources.

Most cryptojacking attacks use CoinHive code to mine cryptocurrencies

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

900 90 70 80

info@pandasecurity.com

Criminal Record

Smominru

At the start of 2018, Smominru was discovered. It is a piece of malware used to mine Monero, and which had infected over half a million machines since May 2017, mainly in Russia, India and Taiwan. It is estimated that the cybercriminals had already made up to $3.6 million.

Adylkuzz y Wannamine

One of the most problematic vulnerabilities in 2018 has been EternalBlue, which was also used by WannaCry. This vulnerability was how Adylkuzz got onto systems. This malware was used to generate Monero, and infected thousands of computers all around the world. In fact, it is believed to have affected even more computers than WannaCry.

Attack on DoubleClick

Towards the end of January 2018, YouTube was found to be affected when it was discovered that, hidden within its ads was malicious code, putting numerous users at risk. In this case, the advertising platform DoubleClick was the victim of an attack that hid the CoinHive cryptojacking code in YouTube adverts..

WinstarNssmMiner

In May 2018, another particularly dangerous piece of malware called WinstarNssmMiner infected half a million computers in three days. This malware got in using phishing emails and infected websites. Once on a system, it used all of the computer's power to mine cryptocurrency

HiddenMiner

Discovered in March 2018, HiddenMiner managed to make its way onto mobile devices via applications downloaded from third party (i.e., non-official) app stores.

One of the reasons it was so dangerous is that, in older versions of Android, it was almost impossible to get rid of. Once inside, it used all the device's resources, making it overheat and crash.