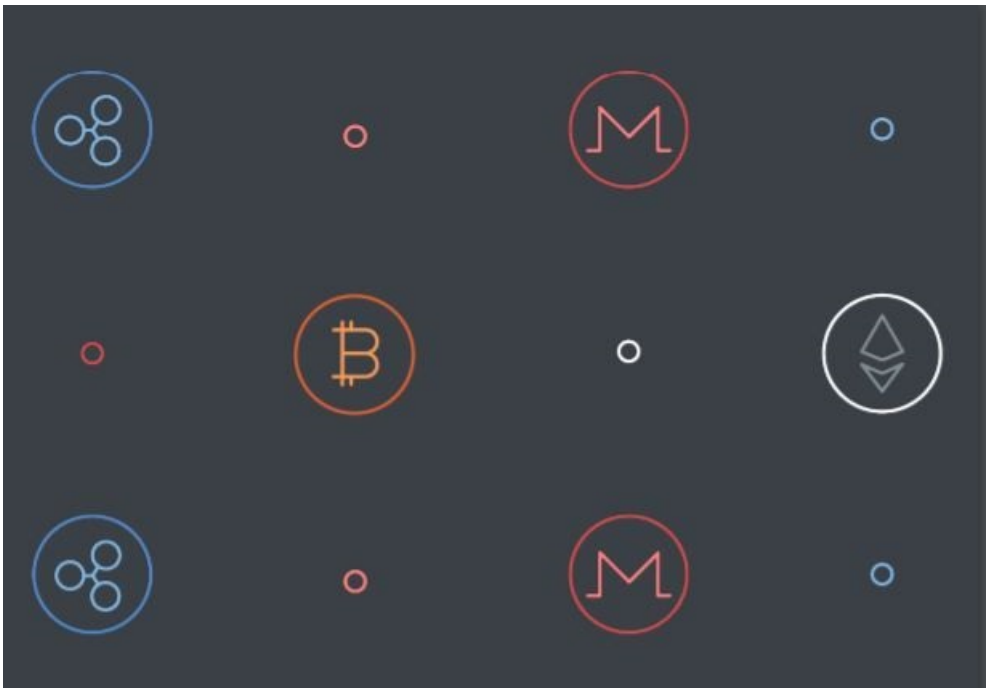
Cryptojacking: A hidden cost for your company

After gaining momentum in mid-2017, we have seen a worldwide boom of digital cryptocurrencies like Bitcoin. Cryptocurrencies have become synonymous with ransomware attacks, but now cybercriminals have discovered another way to make money - mining cryptocurrencies.



Cryptomining is no easy feat, requiring immense computing power to be successful. This is due in part to blockchain technology that is the cornerstone of cryptocurrencies' impenetrable defence and anonymity, using complex algorithms to create and authenticate the currency.

The kind of computing power hackers need to solve these algorithms and successfully mine cryptocurrencies is the equivalent of that of large technology companies. To gather that much power cybercriminals are using malware to hack into devices and use them to trawl the web, consuming their resources to mine cryptocurrencies.

To shed more light on this new threat Panda Security compiled the report, 'Cryptojacking: A Hidden Cost'.

Cryptojacking - a silent threat

11 Sep 2018

"Cryptojacking is an easy way to make money, and doing it is really cheap. Cryptojacking kits can be bought on the dark web for around $30. The attacker can install it on 100 machines, for example, and all of them will constantly contribute money by generating cryptocurrency with little risk" says Josu Franco, Technology and Strategy Consultant at Panda Security.
"What's more, we're seeing a significant increase in legitimate websites infected with CoinHive, a JavaScript that means that it isn't even necessary to install mining software; it simply runs as long as the user is active on that page" continues Franco.

Cybercriminal's can use a number of attacks methods to get into your device virtually unnoticed, including infected

websites, unpatched vulnerabilities, Phishing and unsecured IoT devices.

How will you know if your device has been compromised?

One of the first indications of cryptojacking malware infection is unusually high electricity consumption. Users should also take note of a serious slowdown of the device.

How can you protect against Cryptojacking?

“The kinds of advanced cyber threats we face today have the potential to cripple organisations. To combat these threats business leaders need to develop a comprehensive cybersecurity strategy that includes next-generation EDR (Endpoint Detection and Response) technology to provide visibility and control of the network, as well as developing policies and procedures that govern user behaviour” says Jeremy Matthews, regional manager at Panda Security Africa

Recognising and preventing modern cyber scams

Doros Hadjizenonos 22 Oct 2018

PandaLabs, Panda Security’s malware research facility shared the following tips for protecting against Cryptojacking:

- Carry out periodical risk evaluations to identify vulnerabilities.
- Analyse resources to make sure there is no unusual activity.
- Thoroughly investigating any spikes in IT problems related to unusual CPU performance
- Careful with your browser. If you suspect that cryptojacking is getting in via websites, install plugins to block these sites on your browser.
- Regularly update all the company’s devices and systems.