BIZCOMMUNITY

Cryptojacking - a silent threat

An alarming number of online users are falling prey to a new wave of cyber attacks called cryptopjacking.

According to global cybersecurity leader Bitdefender, the number of reported cryptojacking attacks have overtaken ransomware placing amongst the top treats to date.

But what is this sinister sounding, cyber threat? Cryptojacking is basically the unauthorised use of a computer to mine cryptocurrency. Hackers either get victims to click on a malicious link through a phishing-type e-mail that loads crypto mining code, or they infect a website or online ad with JavaScript code that auto-executes once loaded in the browser.

Either way, the crypto mining code then works in the background as unsuspecting victims continue with their daily tasks. The only sign is the CPU usage is higher which leads to slower performance or lags in execution.

“Hackers see cryptojacking as a cheaper, more profitable alternative to ransomware. It involves less risk and the profits could be higher, depending on the number of victims. For example, with ransomware a hacker might get two to three organisations to pay (the ransom) out of 100 targeted businesses whereas cryptojackers can infect hundreds of machines that will deliver a steady stream of cryptocurrency for a potentially long time,” says Tudor Florescu, sales engineer at Bitdefender.

Tudor Florescu, sales engineer at Bitdefender

“The risk of being detected is also lower than ransomware, as the crypto mining code runs quietly in the background without throttling computing resources up to 100%, remaining undetected for a long time. Also, when detected it can be quite difficult to trace it back to the original point of infection, thus leaving the company with a potential security vulnerability that they are oblivious of.”

Not so innocent

Whilst cryptojacking won’t cause mega data breaches or regulatory compliance headaches per se, it is usually indicative of a potential vulnerability that may have been exploited to deliver the cryptocurrency mining software. Businesses can’t afford to ignore it, as the presence of cryptocurrency miner may just be the aftermath of a data breach that had already occurred, with attackers continuing to exploit the infrastructure for added profit. As cryptojacking targets CPUs, it can lead to a high load and degraded performance and in extreme cases operating system (OS) failure.

In some instances, infected machines may also attempt to infect neighbouring machines and therefore generate large amounts of traffic that can overload business networks.

Unfortunately, laptops, desktops and mobile devices are just the tip of the iceberg. Many criminals are finding that the high-powered servers and datacentre rigs that make up the backbone of enterprise infrastructure can also be made into extremely powerful crypto mining machines when they can be subverted.

According to Forrester Research, corporate servers have become the number one device in the enterprise-targeted for cryptocurrency mining by external attackers.

“Internal attackers are also setting up their own illegal crypto mining operations on company servers. Some engineers even tried mining for cryptocurrency harvesting the computing power of the nuclear research facility they were working in,” says Florescu.

And crytojackers aren't limiting their attacks to just on-premises datacentres. Dark Reading says approximately 25% of businesses today are now being targeted by cryptojacking in the cloud. Worrying is that this figure has increased significantly from last year’s 8% statistic.

“The Tesla incident is an example where attackers managed to use the company’s AWS (Amazon Web Services) account

to mine for cryptocurrency in the cloud, by first breaking into a Kubernetes instance that was poorly configured. Misconfigured containerisation technology is now enabling cryptojackers to easily start draining computing cycles," he explains.

Unfortunately, it's not just computing capabilities that attackers are stealing in these cryptojacking attacks, they are also drawing electricity. Researchers at FireEye found that a machine which ran Coinhive over a 24-hour period used 1.212kWh of electricity. And in South Africa where electricity bills continue to rise, this is worrying indeed.

Protection

Awareness is critical particularly when it comes to e-mail phishing-type attempts – users should always be very careful what links they click on and should rather delete an e-mail when unsure.

In the case of auto-executing cryptojacking from legitimate websites, it is obviously more difficult to detect potential foul play. Here the following technology can be used to good effect:

End-point protection – Security software vendors like Bitdefender have added crypto miner detection to their products and it will help protect against it. Also, as cryptojackers constantly change their technique similarly security software will be updated with the newest detection technology;

Ad-blocking or anti-cryptomining extensions on web browsers; since cryptojacking scripts are often delivered through web ads, installing an ad blocker can be an effective means of stopping it;

- Browser extension maintenance - some attackers are using malicious browser extensions or poisoning legitimate extensions to execute crypto mining scripts; and

- Up-to-date web filtering tools - once a website that delivers cryptojacking scripts is identified, filtering tools will make sure users are blocked from accessing it again.

- Infrastructure baselining – having a baseline of the average infrastructure operation and its performance under normal stress, can help identify anomalous performance spikes that are usually indicative of a cryptojacking infection.