How your smart fridge might be mining bitcoin for criminals

June 29 2018, by Robert Stevens

In this Feb. 7, 2018 file photo, a neon sign hanging in the window of Healthy Harvest Indoor Gardening in Hillsboro, Ore., shows that the business accepts bitcoin as payment. A raft of recent cyber-security firms and governments now cite the rising trend of 'crypto-jacking'—in which devices are infected with invisible malicious cryptocurrency mining software that uses the computing power of victims' devices to mine virtual currency—as the main cyber security threat to businesses and consumers worldwide. (AP Photo/Gillian Flaccus, File)

Is the web browser on your phone slower than usual? It could be mining bitcoin for criminals.

As the popularity of virtual currencies has grown, hackers are focusing on a new type of heist: putting malicious software on peoples' handsets, TVs and smart fridges that makes them mine for digital money.

So-called "crypto-jacking" attacks have become a growing problem in the cybersecurity industry, affecting both consumers and organizations. Depending on the severity of the attack, victims may notice only a slight drop in processing power, often not enough for them to think it's a hacking attack. But that can add up to a lot of processing power over a period of months or if, say, a business's entire network of computers is affected.

"We saw organizations whose monthly electricity bill was increased by hundreds of thousands of dollars," said Maya Horowitz, Threat Intelligence Group Manager for Checkpoint, a cybersecurity company.

Hackers try to use victims' processing power because that is what's needed to create—or "mine"—virtual currencies. In virtual currency mining, computers are used to make the complex calculations that verify a running ledger of all the transactions in virtual currencies around the world.

Crypto-jacking is not done only by installing malicious software. It can also be done through a web browser. The victim visits a site, which latches onto the victim's computer processing power to mine digital currencies as long as they are on the site. When the victim switches, the mining ends. Some websites, including Salon.com, have tried to do it legitimately and been transparent about it. For three months this year, Salon.com removed ads from its sites in exchange for users allowing them to mine virtual currencies.

Industry experts first noted crypto-jacking as a threat in 2017, when virtual currency prices were skyrocketing to record highs.

The price of bitcoin, the most widely known virtual currency, jumped six-fold from September to almost $20,000 in December before falling back down to under $10,000.

The number of crypto-jacking cases soared from 146,704 worldwide in September to 22.4 million in December, according to anti-virus developer Avast. It has only continued to increase, to 93 million in May, it says.

The first big case emerged in September and centered on Coinhive, a legitimate business that let website owners make money by allowing customers to mine virtual currency instead of relying on advertising revenue. Hackers quickly began to use the service to infect vulnerable sites with miners, most notably YouTube and nearly 50,000 Wordpress websites, according to research conducted by Troy Mursch, a researcher on crypto-jacking.

Mursch says Monero is the most popular virtual currency among cyber-criminals. A report by cybersecurity company Palo Alto Networks estimates that over 5 percent of Monero was mined through crypto-jacking. That is worth almost $150 million dollars and doesn't count mining that occurs through browsers.

In the majority of attacks, hackers infect as many devices as possible, a method experts calls "spray and pray."

"Basically, everyone with a (computer processing unit) can be targeted by crypto-jacking," said Ismail Belkacim, a developer of an application that prevents websites from mining virtual currencies.

As a result, some hackers target organizations with large computing power. In what they believe might be the biggest crypto-jacking attack so far, Checkpoint discovered in February that a hacker had been exploiting a vulnerability in a server that over several months generated over $3 million in Monero.

Crypto-jackers have also recently targeted organizations that use cloud-based services, in which a network of servers is used to process and store data, providing more computing power to companies who haven't invested in extra hardware.

Abusing this service, crypto-jackers use as much power as the cloud will allow them to, maximizing their gains. For businesses, this results in slower performance and higher energy bills.

Martin Hron, a security researcher at Avast, says that besides the rise in interest in virtual currencies, there are two main reasons for the rise in attacks.

First, crypto-jacking scripts require little skill to implement. Ready-made computer code that automates crypto-mining is easy to find with a Google search, along with tips on the vulnerabilities of devices.

Second, crypto-jacking is harder to detect and is more anonymous than other hacks. Unlike ransomware, in which victims have to transfer money to regain access to their computers blocked by hackers, a victim of crypto-jacking might never know their computer is being used to mine currency. And as currency generated by crypto-jacking goes straight into a hacker's encrypted wallet, the cyber-criminal leaves less of a trail.

Both Apple and Google have started to ban applications that mine virtual currencies on their devices. But Hron, the Avast researcher, warns that

the risk is growing as more everyday devices are connected to the internet—from ovens to home lighting systems—and that these are often the least secure. Hron said that cheaply made Chinese devices were particularly easy to hack.

Some experts say new techniques like artificial intelligence can help get a faster response to suspicious software.

That's what Texthelp, an education technology company, used when it was infected with a crypto-jacker, said Martin McKay, the company's chief technology officer. "The risk was mitigated for all customers within a period of four hours."

But security researcher Mursch says that these precautions won't be enough.

"They might reduce the impact," he says, "But I don't think we're going to stop it."