MINING FOR GOLD

Ben Williams *explains how to protect yourself from the spiralling threat of malicious cryptojacking adverts.*

Picture credit: Getty

Most of you have probably heard about the soaring value of cryptocurrencies. The price of one Bitcoin, the most popular digital currency, has rocketed from just $0.003 seven years ago to $7,604 today. It was inevitable that the surging demand, price, and popularity of the crypto market would lead to greater interest from opportunistic scammers and online criminals. Already this year we have seen Japanese crypto exchange Coincheck fall victim to a $500m hack that affected up to 260,000 of its customers. Meanwhile in the UK, reports came out of a crypto trader being held at gunpoint in his own home, with intruders demanding that he transfer large quantities of Bitcoin to them.

Those that have not yet made the leap into the crypto gold rush may deem themselves safe, however, there lies a more subtle and widespread security risk to be considered: cryptojacking. Cryptojacking is the act of secretly using another's computing device to mine digital currencies. To legitimately create new digital currencies, miners must solve computational problems, which require large volumes of computing power, energy and capital. By hacking another's computer however, cryptojackers can bypass these barriers and mine new currencies at a far lower cost. This activity has become so lucrative that in November 2017 it was reported as the sixth most common type of malware worldwide.

> ATTACKS HAVE BECOME INCREASINGLY FREQUENT, ATTACHING THEMSELVES TO A RANGE OF WEBSITES

You may remember a story not long ago about PirateBay, the popular torrent website that covertly placed code on some of its pages that used visitors' machines to mine virtual currency. Highly visited websites are well placed to cash in on this as cryptocurrencies rely on large networks of machines to verify transactions and create new coins. The more machines that they can manipulate to mine on their behalf, the better.

Unknowingly to the user however, these codes drain their central processing unit (CPU) as a means of running the mining software, leading to wider consequences. Not only is consumer choice completely sidelined and disrespected in this situation, but users can face a reduction in the performance and lifespan of their machines. This is because corrupted computers are forced to work significantly harder for the cryptojacker, consuming vast amounts of energy and often increasing their temperature to dangerous levels. Once a device is overheated, component failure can occur, requiring users to buy new parts or replace the hardware all together. In the case of PirateBay, it is unsurprising that many users were appalled to hear that the code had been forced on them without any consent or notification.

A FAIR EXCHANGE

This type of technology was first popularised by code developer Coinhive as a means of replacing traditional methods of monetising internet traffic, such as adverts and pay walls. In these cases, companies opt in for the JavaScript to be run on their website, and often inform their users that they will be 'borrowing' some of their CPU in order to maintain a free service.

To some users, this is a fair exchange for using a website's services and offers an opportunity to give back to their favourite content creators. To most it was a surprise. But the technology has been hijacked by cyber attackers and used to create advert-based cryptojackers that reside on popular websites without knowledge of the host or user. These malicious adverts dupe users into sacrificing their processing power for nothing in return and take up to 80 percent of their computing capacity. This can be particularly damaging to businesses with high reliance on computing technologies to carry out their operations. To make matters worse, the mining programmes are often accompanied by adverts that display fake antivirus software that installs even more dangerous malware on to users' computers.

YouTube most recently fell victim to this, after a group of attackers successfully bypassed its defence system and placed coinjacking malware on its adverts. Users immediately reported a noticeable slowdown in their devices, and Google later confirmed that the site had been breached. These types of attacks have become increasingly frequent, attaching themselves to a range of popular websites including CBS Showtime, UFC live-streams and even governmental pages for the UK and US.

THE NEW THREAT

Many have looked to platform owners such as Google and Facebook to address this, accusing them of negligence and putting consumers at risk. The response has been swift, with teams and systems being put together to spot and respond to abusers as soon as possible. In its most recent crypto-breach, YouTube was able to remove the malicious adverts within two hours, and reassured users that they operate a 'multi-layered' detection system to fend off attacks. But not every organisation has the resources to put these types of systems into place, and therefore only a minority of website owners are working to protect their consumers from this new security threat.

Once more, those website owners that are working to protect their consumers can only offer solutions that work on their platform, failing to address the threats that come with wider internet use. This is because these malicious 'cryptojacking' adverts appear on all parts of the internet, and so solutions must be provided that aid consumers across their entire browsing experience. Solely relying on websites to deal with this issue is a step in the wrong direction, and risks distracting from more effective solutions that are already accessible to the average user.

Adblocking and anti-cryptomining extensions are very effective at detecting and blocking these types of scripts, protecting consumers and offering peace of mind while surfing the internet. As we know, cryptojacking works via running of a JavaScript that is either attached to a website or covertly placed into an advertisement. For website-based cryptojackers, such as that used by PirateBay, users can utilise filters that detect and stop mining software in its tracks. And for the latter, those scripts that are embedded into an online advert and inserted into an unknowing website host, users can utilise a regular advert blocker that removes the malicious content all together.

The good thing is that these solutions are free to consumers and are extremely accessible, requiring a mere extension download that works across all mainstream web browsers. Once more, they are advantageous as they work across the entire internet, eliminating the need for consumers to depend on the security practices of website owners.

Those users' that would prefer not to use an

▶

adblocker, however, can also take steps to protect themselves. One technique is to manually monitor the Operating System's Task Manager. This method enables users to review their CPU and memory usage for all tabs and extensions in use and spot irregular activity.

WARNING SIGNS

It is hard to say what a 'normal' CPU looks like, seeing as the processing power and applications that people run can vary so much. However, a drastic increase in CPU use when visiting a regular website can indicate the presence of this type of malware. Users can then simply choose not to visit those websites that are unjustifiably draining their computing power. Other and perhaps more simple warning signs to look out for include a slow and unresponsive computer or an overheating device.

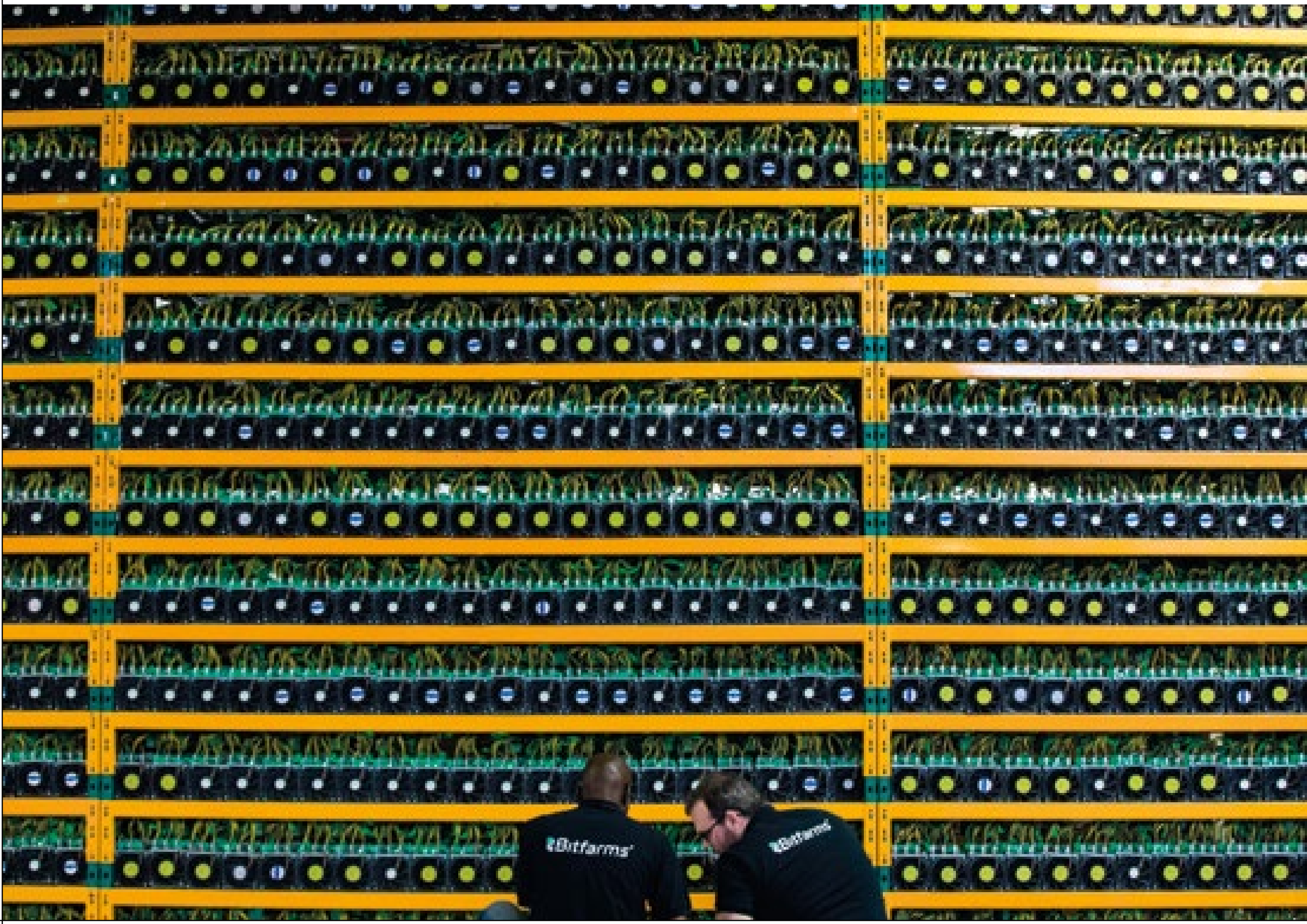
If you are suspicious that cryptojacking is taking place, you can take three simple steps to protect yourself; close your browser, restart your computer and run an antivirus scan for good measure. To safeguard your future internet use, consider blocking that website or use your browser's privacy controls to only allow the running of JavaScripts from certain websites that you trust.

It is also worth noting that some antivirus and security vendors have updated their services to block these types of scripts. Those users who have access to these services should make the most out of them, but keep in mind that they cannot provide 100 percent protection. As cryptojacking is a relatively new and adapting phenomena, the anti-virus world is partly playing catch up. Vendors can only respond and update to new threats as they emerge, giving attackers the opportunity to develop new ways of bypassing their systems to pose a constant threat to consumers. Furthermore, cryptojacking requires no installation from the host computer, making it even more difficult for these types of systems to spot and respond to threats with a 100 percent success rate.

These strategies have their own advantages, offering different types of solutions with varying efficacy levels and drawbacks. The most effective means of tackling the issue of cryptojacking is for consumers to be educated on the threats and to adopt these techniques in conjunction with each other. Consumers can pick and choose which solution works best for them and adopt new strategies as threats emerge. By users remaining vigilant and informed on this evolving threat, attackers have a greatly reduced pool of computers that they can exploit, which will affect the profitability of the act – the cryptojacker's Achilles' heel ●

THE POPULARITY OF THE CRYPTO MARKET HAS LEAD TO GREATER INTEREST FROM ONLINE CRIMINALS

Ben Williams has worked at Cologne-based eyeo since July 2013. Since then, he has been instrumental in turning eyeo's most popular product, Adblock Plus, into the world's most popular browser extension, with over 1 billion downloads to date. He has previous experience working for government and non-profit organisations across the US and Germany.



Two technicians inspect Bitcon mining at Bitfarms in Saint Hyacinthe, Quebeco

Picture credit: Getty