CyberGuard Technologies

Proactive Cyber Defence Report

July 2018

Ransomware is not an unfamiliar threat. For the last few years it has been affecting the world of cyber security, infecting and blocking access to various devices or files and requiring users to pay a ransom (usually in Bitcoins or another widely used e-currency), if they want to regain access to their files and devices.

As security vendors and new technology have entered the market place this has helped drive down the effectiveness of ransomware and we have seen a significant decrease in the number of cases we are attending where ransomware is involved. In fact, the only ransomware cases our incident response team has attended this year all relate to poorly configured terminal servers (more on this later).

It's not only CyberGuard that is seeing the decrease in ransomware, Kaspersky Lab is reporting a fall off about 30%.

Good news we would think? But cyber-criminals have not just disappeared they still need to make money and like any good business they look for new and more efficient ways to make money… crypto-miners!

The architecture of crypto-currencies assumes that, in addition to purchasing crypto-currency, a user can create a new currency unit (or coin) by harnessing the computational power of machines that have specialised 'mining' software installed on them.

Crypto-currency mining is the process of creating these coins – it happens when various crypto-currency transactions are verified and added to the digital blockchain ledger. The blockchain, in its turn, is a chain of successive blocks holding recorded transactions such as who has transferred bitcoins, how many, and to whom. All participants in the crypto-currency network store the entire chain of blocks with details of all of the transactions that have ever been made, and participants continuously add new blocks to the end of the chain.

Recent reports have suggested a substantial increase in 'crypto-jacking', where cyber-criminals install malware onto a victim's devices and use them to mine crypto-currency.

Crypto-jacking malware is reportedly becoming harder to detect and sometimes operates to coincide with times where the device is not normally used, and thus remains undetected.

This type of malware is increasingly being found on devices across multiple sectors and is evolving to use the processing power of internet-connected devices, such as TVs. Some aggressive mining malware has also been found to damage devices.

In response to the increase in crypto-mining, Apple has recently introduced App Store guidelines prohibiting it. It is uncertain whether other providers will follow.

Crypto-mining malware is a low-cost method of earning money and cyber-criminals will almost certainly continue to develop and adapt it, as long as crypto-currencies are of value.

In other news, CyberGuard's Threat Intelligence Team, Unit 12, has highlighted a sharp increase in reports of scam WannaCry emails.

Users are told that their devices are infected with WannaCry ransomware and that all files will be deleted if they do not pay a fine in Bitcoin.

In doing so, the cyber-criminals behind the scam are exploiting the chaos and destruction of the WannaCry attack to trick users into paying. It is highly unlikely that any such threat exists - these are simply attempts to extort money from alarmed individuals.

Over the last couple of weeks, we have seen a number of large scale breaches for some high-profile UK companies including Ticketmaster, Whitbread as well as US company Adidas. Details of these breaches are limited at the moment, but the initial diagnosis is that all of these involved third-party companies who supplied applications or had IT access into the company. Supply chain attacks are becoming more and more common and it is strongly recommended that if you work with, or allow access to your systems to, third party companies that you review and evaluate the risk of this relationship.

With the introduction of GDPR we are likely to see more breaches being reported over the coming months.

We frequently get asked about what companies should do to secure themselves and while every company is different, and we don't have enough time to go into all the details, we do recommend you start by focusing on 3 main areas:

- Configuration - make sure you have a secure configuration, get tested to verify this
- Users - control user access, introduce 2FA where possible, and limit access to privileged accounts
- Vulnerability - make sure you are up-to-date with patching and remove unused software

On a lighter note I am pleased to confirm that we recently won Kaspersky Labs "Most Innovative Partner" for our work with incident response and threat intelligence.

Thank you to our partners this month; Kaspersky Lab, Carbon Black, Anomali and the National Cyber Security Centre.

Stay safe.

Paul Colwell