CyberGuard Technologies

Proactive Cyber Defence Report

May 2019

Hopefully you will have seen the exciting news this month that CyberGuard has signed the first UK commercial agreement with Kaspersky Lab to provide advanced threat intelligence. If not you can read all about it here: https://www.ogl.co.uk/cyberguard-uk-first-threat-intelligence-service

Kaspersky Lab's research team track some of the world's most active and advanced cyber criminals and this intelligence is added to the services you are receiving giving you and our Security Operations Team un-paralleled visibility against cyber-attacks.

Why is threat intelligence important? Different businesses face different challenges; a UK building society will face very different challenges to a small, regional law firm, so understanding the attacker, their motivation, tactics and techniques is vital in preparing your defences. Threat intelligence gives our security analysts a global view, enabling us to track emerging threats so we can understand which vulnerabilities are being used to launch these attacks. This, in turn, helps us prioritise what to focus on when undertaking patch management to plug any potential gaps in customers' networks.

Passwords, Passwords, Passwords! They continue to be a huge problem for IT and security teams. The NCSC, in collaboration with international web security expert Troy Hunt, have put together a list of the top 100,000 passwords (the full list can be found here: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt). If your password is on this list you might want to change it, but it you are the IT Manager maybe you can use this list to stop any of your users using them by uploading this list to Active Directory.

I spent a couple of minutes going through the list, it's always time well spent, and I was intrigued to see some of the following on the list.

Quite a few football teams appear on the list; Arsenal, Liverpool and Juventus to name a few. Blues123 is on there and I'm claiming that as Birmingham City.

A few pop stars such as Eminem, Nirvana and the mighty Slipknot (Whoooo!) along with all the superheroes; Spiderman, Superman, Superwoman and my personal favourite Batman.

Even after all the breaches and user training, Password1, 12345 and abc123 still appear high on the list. It is vital that we continue the education of users but also look at how technology can help.

Talking of superheroes, last month I saw the launch of 'Avengers: Endgame' which quickly smashed all box office records. As is normal with high profile events, the cyber-criminals were quick to try and exploit this.

According to Kaspersky Lab researchers, scam sites have cropped up across the internet, promising the ability to "download the Avengers: Endgame full movie".

The "free" account captures a username and password – potentially useful to cyber-criminals, given the rampant practice of password re-use (see above). But a second screen then asks for billing information and full credit card details, including the CVC code. The site purports to need the information simply to verify geography and to make sure the service is "licensed to distribute" the movie in the region of the user. But of course, it's merely a smokescreen in order to lift the information for nefarious purposes.

We saw similar activity around the final series of Game of Thrones as well.

Nobody is too big or too technical when battling cyber-criminals and Microsoft has confirmed that a hacker - or group of hackers - has broken into a customer support account for the company before gaining access to information related to the customers' email accounts.

Hackers were reportedly able to access email content from a large number of Outlook, MSN, and Hotmail email accounts.

The compromise has not affected Office 365.

Victims have been told that details accessed could include email folder names, subject lines and contacts. Microsoft has also said content in the body of messages was also vulnerable.

Thank you to NCSC, Kaspersky Labs, Carbon Black and Anomali Labs for content.

Stay safe
Paul