CyberGuard Technologies

Proactive Cyber Defence Report

December 2018

Welcome to the final threat report of 2018.

It has been quite a year for Cyber Security and although we haven't witnessed the large-scale ransomware attacks of 2017, we have seen the number of companies affected by cyber-attacks grow. We will see lots of predictions for 2019, but most of the companies that I speak to are still not getting the basics right. Companies need to focus on passwords, patching and protecting their users against phishing attacks. Once these are complete they should then look to threat detection and log management, along with Cyber Essentials.

We have talked about how more and more devices are getting connected to the internet for convenience and management, which leads to a security headache. A story emerged last week of a hacker targeting printers connected to the internet. The hacker, under the Twitter handle @HackerGiraffe, hacked over 50,000 printers to promote Felix Kjellberg - also known as PewDiePie - a Swedish YouTuber, comedian and video game commentator (ask your kids ☺). According to the hacker, he found three different vulnerable printing protocols on Shodan (IPP, LPD, and JetDirect), with up to 800,000 vulnerable printers in total. Although this hacker only used this vulnerability to print an advert for YouTube, many of these printers are connected back into an internal network which could potentially give a cybercriminal access to much more. CyberGuard ran the same query just for the UK and found that there are over 6500 printers vulnerable to LPD alone.

If there is ever a story that highlights the need for active monitoring, it is the recently discovered breach at the Marriott Hotel Group. Although details about the breach are still to be released, it has been claimed that the cybercriminals have been active in the network since 2014! A cybercriminal can gather a lot of information in four years and it is reported that they stole over 500 million personal customer records, including email and home addresses as well as passport numbers.

According to recent reports, smishing, a technique similar to phishing but using an SMS message rather than an email, is on the rise. The SMS message, which can be disguised to appear as being sent from an official source, will have a link which can download malware or redirect the victim to a malicious website to steal credentials or other personal data.

As smartphones become more popular and the use of email declines, criminals are turning to smishing to spread malware. A UK bank recently suffered IT issues, which resulted in cybercriminals taking advantage of the situation by sending SMS messages purporting to be the bank, but containing malicious links to malware.

Security reports suggest that the use of smishing poses greater security concerns as phones can hold more information about individuals than a PC. Furthermore, the reports state that as people believe smartphones are less susceptible to malware than PCs, they may not have the relevant security systems installed including antivirus which is standard in all PCs.

In December 2017, the NCSC wrote about criminals using SSL certificates to try to legitimise phishing websites. Recent reports have indicated that 49% of phishing sites were using the padlock, up from 25% a year ago and 35% in the second quarter of 2018.

HTTPS sites are verified by TLS (previously known as SSL) Certificate Authorities, and the padlock links to the certificate provider's website. The padlock symbol indicates that the data being communicated has been encrypted.

Although individuals were historically advised to look for the padlock, the December 2017 report highlighted that the padlock could no longer be trusted, as this does not guarantee that the webpage is legitimate or authentic.

The recent reports have shown that this threat has developed significantly and that criminals are increasingly using legitimate means to obtain information.

The NCSC has previously blogged about the importance of using HTTPS to protect data.

We are seeing a dramatic increase in phishing and spam as we approach Christmas, so make sure you warn users to be extra careful as cybercriminals will look to target the large brands in the run up.

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

Have a Merry Christmas and a Happy New Year!

Stay safe

Paul Colwell
Chief Technical Officer