CyberGuard Technologies

Proactive Cyber Defence Report

December 2017

Just another average month in the info security world! Uber has a breach that exposes 57 million customers' and drivers' personal information, and the National Cyber Security Centre (NCSC) warn of Russian State sponsored cyber-attacks.

Apple has not had the best of months either. Not only was the new facial recognition security in the new iPhone X successfully compromised, but a new critical flaw was discovered in its flagship Mac Operating system, High Sierra.

The security flaw could allow anyone to access locked settings on a Mac, using the user name "root" and no password, subsequently unlocking the computer. The security flaw, discovered a couple of weeks ago and disclosed in an Apple developer support forum, has been shown to work within the software's user preferences screen, among other locations. Once triggered the same combination will also bypass the lock screen of Macs, running Apple's latest operating system.

Apple quickly released a patch to fix this issue and we urge all Mac users to patch this immediately.

Again, this shows the importance of making sure that you have a robust patching strategy in place that not only patches Microsoft products but covers other operating systems and software.

Uber's Chief Security Officer has revealed that the Company experienced a data breach in October 2016, but did not report it to regulators or victims. It is reported that Uber paid $100,000 ransom demand in exchange for the deletion of the stolen data.

It is reported that the personal information of an estimated 50 million customers and 7 million drivers, including names, email addresses and telephone numbers were stolen, along with the driving licence details of 600,000 US-based drivers. Uber has stated that no trip history information, credit card numbers, bank account numbers, social security numbers or dates of birth were taken in the breach. The attackers are reported to have obtained login credentials for an Uber Amazon Web Services account that contained the data.

UK citizens are believed to be among the 57 million customers and drivers whose personal information was stolen. Based on current information, the NCSC has not seen evidence that financial details have been compromised.

Even though there is no financial compromise we expect to see a rise in phishing emails around this breach as cyber-criminals look to exploit the information moving forward.

It does raise the question of paying the ransom and while we understand that in some cases businesses may not have an alternative, it is important to understand that you are making a deal with criminals and there is a risk of them not releasing the data, or as in Uber's case, not deleting the data.

It is critical that you have a robust, tested backup of all of your data. You also need to make sure that this backup is offline and protected, as we have seen a number of cases where by the backup has also been compromised or encrypted.

It is also important that you have a cyber incident response tried and tested plan in place, so that if the worst happens you have access to the right support quickly, and that your business

has a clear understanding of the situation to control the breach. Keep the business updated and pull together all third party businesses and regulators.

The NCSC, via GCHQ, are writing to all Government Agencies warning them against using Russian security products for protecting systems relating to national security, of which Kaspersky is one.

At this point the NCSC are not recommending members of the public or companies stop using Kaspersky products, which are used by about 400 million people globally. Officials say the NCSC's decision is based on risk analysis, rather than evidence that such espionage has already taken place.

And while there was some mild hysteria in the media, there is very little to worry about. OGL Computer and CyberGuard have a long working history with Kaspersky and we share threat intelligence with the global malware team.

Whilst we understand that the British Government departments that protect critical UK assets look to fortify their position, and talking about Russian spies is fun as you will have read in this threat report as well as previous ones, 99% of risks and incidents within UK businesses relate to one of the following:

- Patching software
- Weak passwords
- Poor configuration of firewalls and other network devices

Businesses should really be focusing on these before worrying about super Russian spies!

Merry Christmas
The CyberGuard Team