CyberGuard Technologies

Proactive Cyber Defence Report

October 2017

September, again, saw two major cyber breaches for global companies, Deloitte and Equifax. Deloitte provides auditing, tax consultancy and cyber security advice to some of the world's biggest banks, multi-national companies, media enterprises, pharmaceutical firms and US Government agencies. According to the Guardian newspaper, Deloitte clients across these sectors had material in the company email system that was breached. The breach was believed to be US-focused, affecting well-known companies as well as US Government departments. The compromise was discovered in March this year, but it was reported that the attackers may have had access to Deloitte systems since October or November 2016.

According to the newspaper, the hacker compromised the firm's Microsoft Azure Cloud global email server through an administrator's account that, in theory, provided them with privileged, unrestricted access. The account required only a single password and did not have "two-step" verification. Emails to and from Deloitte's 244,000 staff were stored in the Azure Cloud Service, which is Microsoft's equivalent to Amazon Web Services and Google's Cloud Platform.

Equifax has confirmed it was the victim of a data breach between May and July 2017. Equifax, based in the US, is one of three large credit scoring agencies used by companies to check the credit worthiness of customers. It has stated that the records of up to 143 million Americans may have been accessed during the breach. These records reportedly include names, social security numbers, dates of birth and other personally identifiable information (PII). The extent of the impact on UK individuals is not yet clear; however, Equifax has confirmed that limited personally identifying information (PII) of UK citizens has been exposed. It is reported that hackers were able to exploit a known vulnerability in Equifax's web servers, allowing them access to this data.

Equifax has confirmed that around 400,000 UK citizens have been affected by the recent Equifax data breach.

At this moment in time, password-related data does not appear to have been involved in this breach.

The main risk to UK citizens affected by this data breach is that they could be on the receiving end of more targeted and realistic phishing messages. Fraudsters can use the data to make their phishing messages look much more credible, including using real names and statements such as:

"To show this is not a phishing email, we have included the month of your birth and the last 3 digits of your phone number".

These phishing messages may be unrelated to Equifax and may use more well-known brands. It is unlikely that any organisations will ask their customers to reset security information or passwords as a result of the Equifax breach, but this may be a tactic employed by criminals. The NCSC guidance on protecting yourself from phishing still applies.

Usually, if you are the target of a phishing message, your real name will not be used. However, in this case, if cyber criminals have your name, people will need to be extra vigilant around any message that purports to be from an organisation they deal with, especially when there are attachments or links which take people to sites asking for more personal information.

Cyber criminals may also call. If you do receive a phone call that is suspicious, for example by asking you for security information, do not divulge any information, and hang up. You should then contact the organisation the caller claimed to be from, never using the details they provided during the call.

Unit 12, CyberGuard's Threat Intelligence Team, has seen an increase in a number of banking trojans mainly based on Emotet Trojan. Samples of the banking Emotet Trojan have begun to surface with the ability to internally propagate, using credential brute-force techniques. Cyber criminals have seen the success of WannaCry and Petya and are adapting traditional based malware to spread in the same way.

Emotet is generally delivered via email and evades a number of traditional virus checkers by changing file names and file locations. Emotet is designed to steal your personal information, including your banking user names and passwords.