CyberGuard Technologies

Proactive Cyber Defence Report

February 2019

One of our main security vendors, Carbon Black, has issued a threat report for the UK. The report from the survey of 250 UK businesses highlights some frightening statistics that should make us sit up and take notice.

The full report can be found here https://www.carbonblack.com/uk-threat-report-2018/ but below are some of the main highlights:

- 88% of UK companies have suffered a breach
- 100% of Government and Local Authority organisations have been breached
- 3.67 is the average number of breaches suffered by a UK company
- 89% of respondents said the attacks were becoming more sophisticated
- Phishing attacks were still the primary cause of an attack
- 93% of organisations have plans to increase their cyber security budget

As depressing as some of these statistics are, it is important that we continue to focus on the basics of cyber security by protecting users against phishing, setting unique complex passwords, adding two-factor on cloud or remote logins, and making sure your software is as up-to-date as possible.

A cyber-crime group calling themselves 'The Dark Overlord' continue to threaten to release stolen files from US law firms as well as a London-based plastic surgery clinic, if ransom demands are not met.

The FBI is investigating the theft of 18,000 insurance and legal documents relating to the September 11 attacks on the World Trade Centre. The group reportedly obtained access to the documents after compromising a specialist law firm in the US that provided advice to global insurance firm, Hiscox. The insurance firm has confirmed that their own systems were unaffected by this incident.

In October 2017, the Met Police confirmed that it was investigating the group for stealing data from a London cosmetic surgery clinic, popular with celebrity clients. The group continue to threaten the release of this historic, personal data for money.

After distributing a small preview set of files, the group has publicly released a decryption key for more files, in a bid to bolster their extortion efforts.

The news gives insight into how hacking groups may be evolving in their extortion efforts; opting to drip out stolen material bit by bit, while generating public interest through the media and their own announcements, all to exert pressure on the ransom victim.

This story really does highlight the need to protect personal and confidential information and we expect these kinds of extortion attacks to accelerate throughout 2019.

Two hackers – HackerGiraffe and j3ws3r – claimed to have taken control of 70,000 Google Chromecast smart TV devices around the world, in a stunt to raise awareness of cyber security and to promote YouTuber PewDiePie.

The hackers exploited a vulnerability which tricks Google's media streamer into playing any YouTube video they want. In this instance, the affected Chromecasts displayed a pop-up notice, warning the user that their misconfigured router is exposing their Chromecast and smart TV to hackers.

Businesses that are looking at connecting more and more smart devices to the internet, need to make sure these are secure and are not offering an easy way for a hacker to gain access to your network.

Last month we wrote about a zero-day flaw in Mac OS that could sell on the dark web for over $2 million. A researcher discovered a flaw letting him steal passwords in Mac OS but is not sharing his findings with Apple without a Mac OS bug bounty program.

A researcher claims to have found a new Apple zero-day impacting Mac OS that could allow an attacker to extract passwords from a targeted Mac's keychain password management system. However, the researcher refuses to disclose the alleged vulnerability citing Apple's lack of Mac OS bug bounty program.

Keychain Access is the password management system app in Mac OS, which holds various encrypted passwords for services such as Facebook and Twitter.

The researcher behind the attack, Linus Henze, said that the vulnerability exists in the application's access control and enables him to extract local keychain passwords without root or administrator privileges, and without password prompts.

When you could potentially sell this flaw for $2 million to cyber criminals why would you disclose it to Apple for free?

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

Stay safe.

Paul