BAMBOO
CYBER EYES

Please see an update of the last few weeks news. Please continue to send useful information on what you are seeing too to cyber@bamboo.tech.

WHAT WE'VE SEEN

Scam calls and texts continue...

Ofcom have received reports of scam calls and texts relating to the coronavirus, or Covid-19.

Scammers are calling home phones and sending text messages to mobile phones, which contain misinformation or could leave you out of pocket if you fall victim.

Some calls and texts claim to be from the Government, your GP's surgery, the NHS, or even the World Health Organisation (WHO).

In the calls, a recorded message or caller will claim to be contacting you about the coronavirus. They might offer a test for the virus, a treatment or cure, or might offer to discuss your medical needs.

However, these calls are designed to encourage you to either speak to an operator, or press a button on your phone for more information.

- If you speak to an operator, you could be at risk of giving them your personal information or your financial details, which could result in identity theft or financial loss.
- If you press a button on your phone you could be connected to a high-cost premium number, leaving you liable for a significant call cost.

WHAT WE'VE HEARD ABOUT

Not all attacks are categorised as cyber-attacks. However, they still have the potential to be financially crippling, reputation damaging and non-compliant with basic security standards.

Telephone system (PBX) fraud is one of these. This is where the telephone system is hacked into allowing calls to be routed through the system to high rate international/premium rate numbers.

Whilst we all focus on ensuring our homeworkers VPNs are secure, our software is patched to the hilt and our staff know what and how to report SMS, email and website issues we often forget the vulnerabilities that are laid bare through our phone systems. Telephony fraud is most likely to occur when your organisation is most vulnerable. Now is the time to be extra vigilant.

Features such as remote-access voicemail, message forwarding, and call diversion can all be exploited to enable this illegal call dialling.

Recent incoming reports would indicate that you should be wise to attacks of this nature.

You can:

- Educate staff about how to minimise the risk and report into the business
- Place international bars if you are not operating international business
- Ensure you have full bill analysis capability
- Change system passwords
- Review call logging

For further information or indicators of compromise please email **cyber@bamboo.tech**

BAMBOO
CYBER EYES

WHAT WE'VE BEEN MADE AWARE OF

Surface Web

Latest Apple Text-Bomb Crashes iPhones

Apple devices are vulnerable to a "text bomb" attack where simply looking at messages or posts containing characters in the Sindhi language can crash devices. The bug affects iPhone, iPad, Macs and Apple Watches, and arises from macOS and iOS failing to properly render a Unicode symbol used when writing in the language.

Dark Web

Formbook stealer

FormBook is an inexpensive stealer available on the dark web as malware-as-a-service (MaaS). Capabilities include recording keystrokes, stealing passwords (stored locally and in web forms),and taking screenshots.

The latest FormBook activity involves an email spam campaign impersonating the World Health Organization (WHO). The emails use the subject line "Latest on corona-virus", which
the incorrect hyphen quickly acts as a red flag. The body of the email, which also contains smaller grammatical errors, displays the WHO logo and text outlining updates relating to COVID-19 (aka Coronavirus). The text also points to an attached ZIP file that claims to be a e-book about research on the pandemic and guidelines for protection. The ZIP file houses a copy of GuLoader, a downloader that ultimately delivers the final FormBook payload.

This payload downloads from a Google Drive location. This marks yet another example of threat actors exploiting the global fear surrounding COVID-19. This trend is highly likely to continue with countless malware families and threat actors for the foreseeable future.

Chinese COVID-19 Detection Firm Source Code

Unidentified attackers compromised the Chinese company Huiying Medical and stole a trove of data. Available for 4 Bitcoin (USD 30,000), the data allegedly includes usernames, names, mobile numbers, genders, passwords, occupations, titles, provinces, city, creator IDs, creator names, operator names, and operator IDs.

Casino + Marketing Databases

A dark web listing for an extensive list of multiple databases from 2018 – 2020 relating to casinos and marketing. Totalling millions of lines of data, most of which relates to countries in Europe and the United States.

In UK news

Cyber-spies hunt Covid-19 research UK and US warn

'organisations that might not have considered themselves to be top targets for hackers from foreign states are now in their sights.'

https://www.bbc.com/news/technology-52551023

For further information or indicators of compromise please email cyber@bamboo.tech