OCTOBER 2018

Cyber Security Awareness Month

INFOSEC NEWSBYTES OF THE WEEK | ISSUE 1

BDO
WE SUPPORT CYBER SECURITY AWARENESS MONTH 2018

The Facebook breach: A design flaw and a wake-up call

The recent Facebook breach which attacked 50 million accounts should be a wake-up call for the industry, according to security experts commenting on the security issue which Facebook discovered on 25th September.

Facebook has temporarily taken down the feature that had the security vulnerability. The feature is called "View As", and it's a privacy tool to let you see how your own profile would look to other people.

In a post on Facebook, Mark Zuckerberg shared that "an attacker exploited a technical vulnerability to steal access tokens that would allow them to log into about 50 million people's accounts on Facebook. We do not yet know whether these accounts were misused, but we are continuing to look into this and will update when we learn more."

When a feature like "View As" can be turned on its head into an exploit, it indicates a design problem that led to an unanticipated security vulnerability. Design flaws like this lurk in the mind-boggling complexity of today's commercial systems, and must be systematically uncovered and corrected when software is being designed and built.

Facebook said it had fixed the vulnerabilities and notified law enforcement officials.

BDO TRA Recommendation:
Reset your Facebook password and any password where you have used Facebook authentication to log in.

Singapore has the worst cyber hygiene in the region, survey finds

Singapore consumers may seem heavily wired up, but may have the worst habits when it comes to cyber hygiene when compared to their peers in ASEAN, a survey on Wednesday (03 Oct) showed.

A study by enterprise software provider VMware Inc. showed that 45 per cent of those surveyed in Singapore does not take proper measures to secure their financial data, by using the same passwords across services and apps that contain personal payment data. This is the highest percentage in South-east Asia.

To add, a majority of the Singapore consumers surveyed store their bank account details on at least one to six mobile applications, yet just about 14 per cent of them are using different passwords for all their accounts. This gives Singapore the country the dubious honour of having the least cyber hygiene of those surveyed in the region, with the regional average at 24 per cent.

Their lax attitude aside, Singapore consumers are simultaneously more sceptical towards the level of security afforded by new payment methods than their counterparts in the region and find more comfort in traditional payment methods such as cash and ATMs. Specifically, 53 per cent of Singapore consumers polled found e-payment wallets and apps safe - again, the least in South-East Asia.

VMware Inc. said that to meet the needs for mobile-first consumers, "forward-thinking" banks are already gaining traction by offering biometric payment, with at

At BDO, we have the expertise and experience in a range of cybersecurity services and solutions. Please feel free to contact us and let us know how we can assist you.

FOR MORE INFORMATION

CECIL SU
+65 6829 9628
cecilsu@bdo.com.sg

www.bdo.com.sg

BDO

least three-quarters of consumers in the region placing high trust in the technology, alongside cash payment.

VMware conducted the study in September this year with 6,000 consumers in Indonesia, Malaysia, Singapore, the Philippines, Thailand and South Korea.

Source: The Straits Times

Security researcher fined for hacking hotel Wi-Fi and putting passwords on the internet

Tencent security researcher hacks hotel without authorisation and publishes a blog post about it containing unredacted information.

Singapore authorities have fined a Chinese security researcher with SGD$5,000 (USD$3,600) for hacking into a local hotel's Wi-Fi system without authorisation and then publishing a blog post about it, revealing passwords for the hotel's internal network. The incident took place at the end of August, this year, when Zheng Dutao, 23, of China, visited Singapore to attend the Hack In The Box conference that took place in the city.

Zheng took it upon himself, without asking for permission first, to hack into the Wi-Fi network of a Fragrance Hotel branch, where he checked in for the conference's duration. The researcher, who works for Chinese internet giant Tencent, hacked into the hotel's internet gateway system, an AntLabs IG3100 device that controls access to the Wi-Fi network for staff and guests alike.

He discovered that the device was using a factory default Telnet password, which he used to gain access to a limited shell on the device. From here, he used various scripts and exploits to elevate his access and eventually discovered the password for a MySQL database that contained information on the hotel's internal Wi-Fi network.

The researcher didn't report the security issues to the hotel but instead wrote a blog post about his findings, which he later shared online. Zheng did not do any damage to the hotel's Wi-Fi systems, but he also did not take any precautions to censor sensitive information from his blog, revealing the hotel's Telnet and MySQL passwords and other details that hackers could have exploited against a more serious attack on the hotel's network.

The Cyber Security Agency of Singapore (CSA) discovered Zheng's blog days later, warned the hotel, and took the researcher into custody.

Cobalt threat group serves up SpicyOmelette in fresh bank attacks

The Cobalt Gang has been connected to the theft of millions of dollars from financial institutions worldwide.

Advanced persistent threat group (APT) the Cobalt Gang, also known as Gold Kingswood, is spreading SpicyOmelette malware in campaigns targeting financial institutions worldwide.

In a world where cyber attacks against businesses and consumers alike are spreading and evolving in nature and sophistication, it is often financial institutions which bear the brunt.

Banking customers hoodwinked by fraudulent schemes or those that become the victims of theft through the loss of their financial credentials will often try to claim back lost funds -- of which, banks appear to vary when it comes to compensation.

Some banks attempt to lay the responsibility of fraud at their customers' feet to reduce the expense. However, it is not just customers that can become victims, but the institutions themselves.

Cobalt is a sophisticated hacking group known to pursue high-value financial targets rather than immerse themselves into mass spam campaigns or individual credential thefts. Active since at least 2016, the APT specialises in targeted, network intrusion to gain access to systems which can be compromised for the purposes of theft.

The hacking group's latest campaigns are no different.

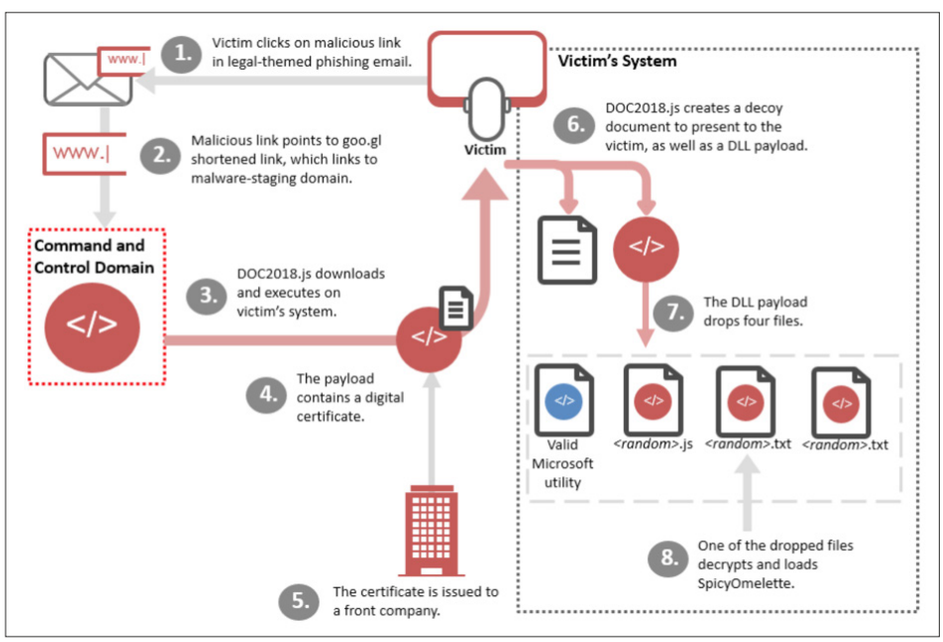

Figure: SpicyOmelette infection chain (Source: SecureWorks)