OCTOBER 2018

Cyber Security Awareness Month

INFOSEC NEWSBYTES OF THE WEEK | ISSUE 4

BDO
WE SUPPORT CYBER SECURITY AWARENESS MONTH 2018

Tracking Tick Through Recent Campaigns Targeting East Asia

The Advanced Persistent Threat (APT) group, "Tick" (also known as "Bronze Butler" and "Redbaldknight"), has been active since 2016 targeting countries such as Japan and South Korea, as observed by researchers at Cisco Talos. While initial attack vectors are unclear, it is assumed the APT group is likely to deliver their malware via drive-by downloads or watering hole attacks on South Korean and Japanese sites. An insecure South Korean laundry service website was observed to be a host to one of the Command and Control (C2) servers controlled by the APT group.

The group is observed to utilise malware known as "Datper" that can execute shell code onto a victim's computer to obtain hostnames and drive information, as well as the "xxmm" and "Emdivi" backdoors. It was discovered that several IP addresses that Tick uses to host their C2 servers actually resolve to hijacked, but legitimate South Korean and Japanese websites, and it is possible that the APT group purchased them to make them less suspicious and detectable.

BDO TRA Recommendation:

It is critical that the latest security patches be applied as soon as possible to the web browser used by your company. Vulnerabilities are discovered relatively frequently, and it is paramount to install the security patches because the vulnerabilities are often posted to open sources where any malicious actor could attempt to mimic the techniques that are described.

Oracle Patches 301 Vulnerabilities in October Update

Oracle's final Critical Patch Update (CPU) for 2018 is now available, patching 301 vulnerabilities spread across Oracle's product portfolio.

Of the 301 vulnerabilities, 49 are rated with a CVSS (Common Vulnerabilities Security Scoring) score of 9.0 or higher, with only a single issue garnering the top severity rating of 10.0 The October CPU became generally available on 16th October and included patches for both first-party and third-party components that Oracle develops and ships in its products.

"As with previous Critical Patch Update releases, a significant proportion of the patches is for third-party components (non-Oracle CVEs, including open source components)," Eric Maurice, director of security assurance at Oracle, wrote in a blog post.

While 331 flaws is a large number, it is actually fewer than the 334 that Oracle patched in the last CPU that it released on 18th July. Looking at the most severe flaw across the 331, the single CVSS 10.0 was given to the CVE-2018-2913 flaw in Oracle's GoldenGate software.

Hacked, scammed and on your own: navigating cryptocurrency 'wild west'

When Peggy and Marco Lachmann-Anke learned in January that hackers cracked a 40-character password and cleaned out

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

their cryptocurrency wallet, they did not go to the police or alert the tokens' issuer, the Berlin-based technology group IOTA.

They bought more coins.

The Cyprus-based German couple, who describe themselves as financial educators, figured they had no chance of recovering the coins and it was not even clear who might take up their case. Yet they took the roughly $14,000 loss in stride - something that comes with the territory when one bet on a new, exciting technology in a yet unregulated market.

"We really believe in cryptocurrencies. We have studied this for about a year before investing, so we are aware of the risks," Peggy Lachmann-Anke said. "There was nothing we could do."

Far from unusual, the episode is emblematic for a market where few rules apply and where investors' faith in the blockchain technology goes hand in hand with the belief that it also helps criminals cover their tracks so well that trying to catch them is a fool's errand.

Patrick Wyman, FBI supervisory special agent at the financial crimes section of the agency's anti-money laundering unit acknowledges cryptocurrencies pose some unique challenges.

iPhone A Growing Target Of Crypto-Mining Attacks

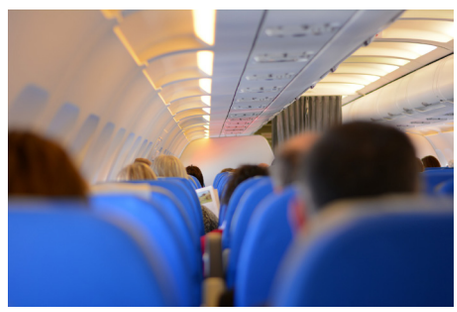
iPhone's have seen a substantial increase of almost 400% in the last two weeks of September 2018 for cryptomining attacks targeting the Safari browser. Attackers were observed by Check Point researchers to have used Coinhive mining malware to specifically target iPhones.

Since September 2018, there has been a sharp increase in cryptomining and other malware attacks targeting the Safari browser, and subsequently, iPhone users.

BDO TRA Recommendation:

iPhones and other Apple products have historically been better protected against malware threat compared to Windows and Microsoft products. However, that is changing as threat actors are developing more advanced methods to attack a greater variety of targets. Always keep your mobile phone fully patched with the latest security updates to ensure your device is protected against known threats and vulnerabilities. Use the Google Play Store/Apple App Store to obtain your software, and avoid downloads, even if they appear legitimate, from third-party stores and sites.

Cathay Pacific Data Breach Exposes 9.4 Million Passengers



Cathay Pacific, the Hong Kong-based international airline, acknowledged on, 24th October that its computer system had been compromised at least seven months ago, exposing the personal data and travel histories of as many as 9.4 million people.

The breach involved private user information, including phone numbers, dates of birth, frequent flier membership numbers and passport and government ID numbers, as well as information on passengers' past travels. The airline said that 27 credit card numbers — but not their corresponding security codes — had been obtained, as had 403 expired credit card numbers.

The company said that no passwords were compromised and that the breach would not affect flight operations or safety. It said it learned in May that passenger data had been exposed after first discovering suspicious activity on its network in March. It did not immediately respond when asked whether it had any indication of who was responsible, and why it did not announce the breach earlier.

Airlines are juicy targets for hackers, with their vast stores of information not only on people's identities and credit cards but also on where they have been.

Still, the types of information in Cathay's systems that were compromised could be particularly useful to malicious agents. Names, birthdays, travel itineraries and passport details could be used to reset passwords or obtain private financial information.

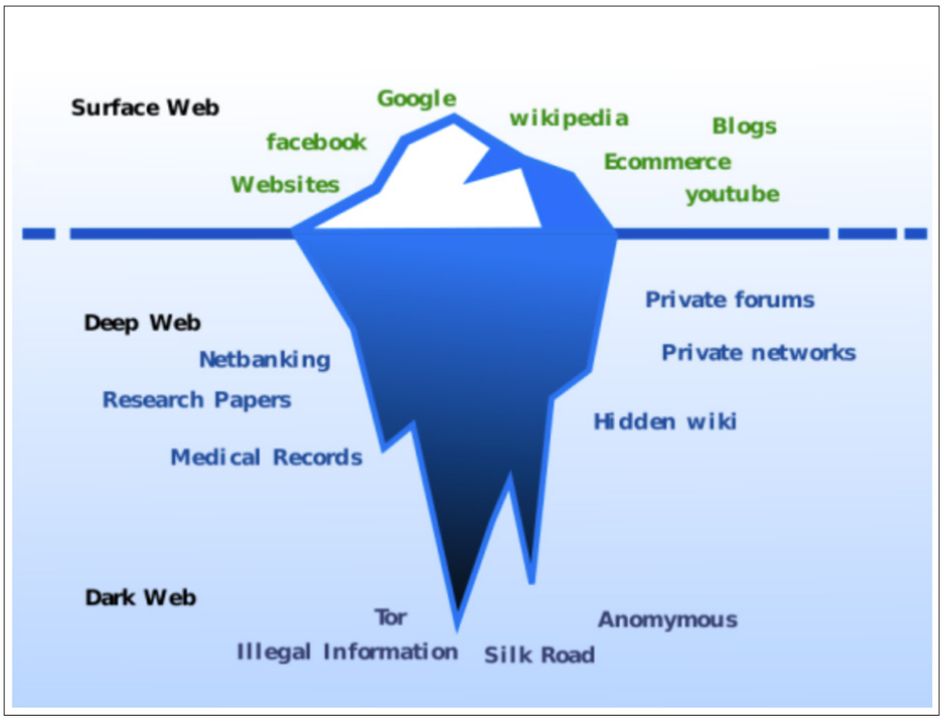
What is the difference between Deep and Dark Web?

There is a corner of the deep web which is intentionally hidden from casual perusers of the world wide web. It is only discoverable through the use of certain internet browsers (mainly Tor) and is home to a host of illegal and vile, and not so illegal and vile sites.

For now, to the difference between the dark web and the deep web. To make the distinction, it helps to start firstly with the section of the internet we are all most familiar with, 'the surface web'. This is the first layer of the ecosystem - where the sun still penetrates, where flowers grow, where bands of merry woodland creatures prance and preen.

This is the area of the internet which is discoverable by search engines - the millions of results that jump up when you type in queries about that humiliating medical issue (for example). These sites are indexed by search engines such as Google and therefore can be stumbled across by someone on a breezy internet stroll.

Now, beneath this first layer, there are the many submerged layers of the deep web, and the only difference between these and the surface web is that search engines do not index them.



Source: http://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

There are many reasons why information is not discoverable by search engines. Just think, would you want someone to be able to pull up your online banking information with a Google search? Thought not. This is only one example of deep web information, with others being specific databases, workplace intranets and archived information which you have to search for on a particular site rather than a search engine. So there you have it, the deep web is nothing to fear, but is rather a necessary part of how the internet works.