Newsletter – Issue No.1240/IT – MAY 2014

IT Security Newsletter

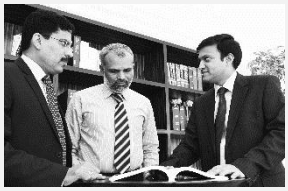
Welcome to the monthly newsletter on IT Security by Keypoint. This issue of the newsletter contains the following topics:

- iBanking Android Malware targeting Facebook Users with Web Injection techniques.
- Gulf Information Security Expo and Conference 2014 provides impetus to combating increase in global cybercrimes
- First Heart bleed attack reported; taxpayer data stolen

Security Tip for the Month

Don't click the "unsubscribe" link at the bottom of unsolicited emails

Spam filters are catching most unwanted e-mail, but some might still reach you. Most spam is designed to get you to respond with your own email or to click a link to "unsubscribe." When you respond or click the "unsubscribe" link, the sender takes your email address and adds it to a SPAM database of active email addresses. You might then start to receive a large amount of SPAM in your inbox. Do not respond or click the "unsubscribe" links.



iBanking Android Malware targeting Facebook Users with Web Injection techniques

iBanking is nothing but a mobile banking Trojan app which impersonates itself as a security app for Android devices and distributed through HTML injection attacks on banking sites, in order to deceive its victims. Recently, its source code has been leaked online through an underground forum that gave the opportunities to a larger number of cyber criminals to launch attacks using this kind of ready-made mobile malware.

The malicious iBanking app installed on victims' phone has capabilities to spy on user's communications. The bot allows an attacker to spoof SMS, redirect calls to any pre-defined phone number, capture audio using the device's microphone and steal other confidential data like call history log and the phone book contacts. According to new report from ESET security researchers,

now this iBanking Trojan (Android/Spy.Agent.AF) is targeting Facebook users by tricking them to download a malware application.

The malware uses JavaScript web injection method to create a fake Facebook verification page for Facebook users. Injected fake verification page prompts users to enter their mobile number in order to verify the Facebook account authenticity, and then shows the following page if he indicates that his mobile is running Android. Next fake page asks victim to download an Android app from the shown URL or using QR code method, if SMS somehow fails to reach the user's phone. Once downloaded and installed, the malware connects to its command-and-control server that allows attackers to issue commands to each infected device.

Facebook also has two-factor authentication features for quite a long time, but this is the very first time when Facebook users are targeted by iBanking Trojan. The reason may be an increasing number of people using it. Since many banking sites use two-factor authentication and transaction authorization systems in order to deal with the various threats, but in order to bypass two factor authentication, cyber criminals have started to create various mobile malware like iBanking to solve their purpose.

Gulf Information Security Expo and Conference 2014 provides impetus to combating increase in global cybercrimes

In the wake of increasing global cybercrimes and cyber-attacks, the importance of information security as the top priority of governments, businesses and security services in the Middle East has prompted significant investments to detect, protect and react to the ever-changing cyber landscape. Addressing issues on global cyber security vulnerabilities and threats against systems, applications, and personal networks, the second edition of Gulf Information Security Expo & Conference (GISEC) will be held from 9-11 June 2014 at Dubai World Trade Centre.

The must-attend event is set to draw 3,000 trade visitors from 51 countries and more than 100 exhibitors from the world's leading information security companies and brands. GISEC 2014, the region's only large-scale information security platform, will gather industry, government and thought leaders as well as international and regional cyber security experts in various business sectors such as I.T., oil & gas, banking & finance, government, legal, healthcare and telecoms to meet the growing requirements for information security and countermeasures in the region. 91% of last year's attendees were purchasing decision makers from a wide range of industries.

The two-day I.T. security-focused conference segment of GISEC hosts delegates from over 18 countries. In addition, free-to-attend security sessions on vendor-run educational presentations, workshops, demonstrations,

informative speeches and case-studies will be held to give I.T. professionals useful insights to help defend their businesses from cyber-attacks.

First Heart bleed attack reported; taxpayer data stolen

The Heart bleed bug has caused widespread anxiety, sent engineers scrambling into patch-mode, and likely prompted millions of users to re-invent their passwords, but so far there have been no accounts of attacks leveraging the bug... until now.

In the first known report of an attack using the security flaw, Canadian police have arrested a man who allegedly used Heart bleed to steal user data from the government's tax Web site, according to Reuters.

Authorities discovered earlier this week that the Canada Revenue Agency (CRA) site was hacked into over a six-hour period and the Heart bleed vulnerability was exploited to nab roughly 900 social insurance numbers and possibly other information from Canadian taxpayers.

"The CRA worked around the clock to implement a 'patch' for the bug, vigorously test all systems to ensure they were safe and secure, and re-launch our online services," said CRA commissioner Andrew Treusch in a statement. "The CRA is one of many organizations that was vulnerable to Heart bleed, despite our robust controls."

Police arrested Stephen Solis-Reyes, 19, in London, Ontario, on Wednesday and seized his computer equipment. He is allegedly associated with the attack, according to Reuters, and faces criminal charges of unauthorized use of computer and mischief in relation to data.

"It is believed that Solis-Reyes was able to extract private information held by CRA by exploiting the vulnerability known as the Heart bleed bug," the Royal Canadian Mounted Police said, according to Reuters.

News of the massive Heart bleed bug reverberated across the Internet last week showing how easily people's online data could be accessed. This particularly nasty vulnerability -- which has the capability to potentially extract people's usernames, passwords, and credit card information -- is said to have affected up to 500,000 Web sites, including Google, Facebook, Yahoo, and many more.

While the hack into the CRA appears to be the first reported attack with Heart bleed, it likely won't be the last.

Featured Technology Products

Mobile banking technologies are rapidly growing and Financial institutions in the region showing a strong desire to be differentiated by its mobile application offering to customers to make their life easy. Our team recently introduced mPassbook for retail banks, a mobile application e-passbook for retail banking customers which will allow account holders to track transaction of multiple accounts conveniently using their mobile phone. The application provides real-time updates and multiple account management options to retail banking customers in a secure way with ease of use.

Do you wish to benchmark yourselves on the mobile space with your competitors? Contact us to avail our free expert consulting for limited hours.

To download the full summary of the newsletter please click here

To unsubscribe from the mailing list, please click here

For more information, enquiries and events please do not hesitate to contact: *Ranjith Kumar* on ranjith.kumar@keypoint.me or *Chahira Ashcroft* on chahira.ashcroft@keypoint.me