# IT SECURITY NEWSLETTER

Issue No.1290/IT - January 2016

## Security Tips!

1. Never reuse the same username and password combinations, so oftentimes a hacker will gather in that information and use it successfully on other sites.
2. While installing a wireless router, always choose WPA, or its newer variant, WPA2, as they're considered more secure than the older WEP encryption.
3. Use and maintain anti-virus software and anti-spyware tools up to date.

### Cognizance

### Healthcare IT at risk from security-agnostic GenMobile workforce

Due to lack of requisite security procedures in place to protect a new and more collaborative digital generation entering the workforce, employees tend to follow risk-prone sharing behaviors.

In the healthcare industry where more than a third (35%) of medical professionals report their organization uses mobile apps to interact with patients, only three quarters of work mobile devices are password protected, according to a new study by Aruba which leads to a high security lapse.

### Hacking groups targeting ME region

Symantec reports that two hacking groups have been spying on targets in UAE,Bahrain and Saudi. Reports says that the Cadelle and Chafer groups have been using back door threats to conduct targeted surveillance of domestic and international targets in ME region, especially airlines and telecoms companies.

The Cadelle group uses Backdoor, Cadelspy, while Chafer, uses Backdoor. Remexi and Backdoor. Remexi.B, all of which are capable of opening a back door and stealing information from victims' computers.

## Hacker group takes Down Top Saudi Arabian Government Websites

The online hackivist group Anonymous hacked the Saudi government websites. The latest cyber-attack was responsible for shutting down the official website of Ministry of Defense, the Royal Air Force, Saudi Ministry of Education and the Saudi Press Association, the Saudi Customs Service, the Saudi Mistry of Finances, the Saudi Ombudsman's Office and the General Passports Service.

## Spear-phishing campaign impersonates Dubai Police official

Cyber-criminals discovered spoofing a Dubai Police email address in a spear-phishing campaign designed to trick recipients into executing malicious attachments.

According to Symantec security, the campaign was aimed at various large companies in the Middle East and Canada. The campaign does not target a specific industry, and it found that such emails being sent to the energy, defense contractor, finance, government, marketing and IT sectors.

## Cybercrime one of the biggest Middle East security threats

Experts are warning that the Middle East has become a hotbed for cybercrime. According to Cisco's 2014 Annual Security Report, total global threats have reached their highest recorded level, increasing 14% from 2012 to last year, mainly with a sharp rise in malware attacks on the Middle East's oil and gas sector.

There are currently cyber-crime laws at varying levels in several Middle East jurisdictions. Elsewhere in the GCC, Bahrain and Qatar have draft laws on computer crimes under consideration while Saudi Arabia and Oman have cyber-crimes legislation in place.

## The Biggest Security Threats We'll Face in 2016

Hackers are nothing if not persistent. They brute-force their way through barriers or find ways to game or bypass them and they'll patiently invest weeks and months devising new methods to do so. Cybersecurity techniques are getting bolder and more sophisticated each year. Some of the most expected threats in 2016 are below:

- Extortion Hacks
- Attacks That Change or Manipulate Data
- Chip-and-PIN Innovations
- IoT Zombie Botnet
- Backdoor attacks

## Largest DDoS Attack in the History

The largest DDoS attack in the history was reported and carried out against the BBC website: Over 600 Gbps. The group calling itself New World Hacking claimed responsibility for taking down both the BBC's global website and Donald Trump's website last week. The group targeted all BBC sites, including its iPlayer on-demand service, and took them down for at least three hours on New Year's Eve.

The group claimed that they allegedly used their own tool called BangStresser to launch a DDoS attack of up to 602 Gbps on the BBC's website.

## Social media sharing leaves users easy target for cybercriminals: study

A quiz from Kaspersky Lab has found that almost a third (30%) of social network users share their posts, check-ins and other personal info with everybody who is online – not just their friends. This leaves the door wide open for cybercriminals to attack, as users remain unaware of just how public their private information can be on these channels.

Despite over three quarters (78%) of Internet users having a social media account, the quiz showed a distinct lack of awareness amongst social media users. One in ten (9%) quiz respondents didn't think people outside of their friends list could be seeing their pages and posts, making it easy for their personal information to fall into the wrong hands, or even be used by criminals for identity theft and financial fraud.

To ensure social network sharing doesn't leave you exposed to danger, Internet users to be cautious about whom they befriend and trust on these sites, as all might not be as it seems. If in doubt, they should not accept a friend request or click on a link that they are not expecting. It is also essential that privacy settings within social network accounts are at their highest, to ensure it is only real friends users are sharing status updates with.

Along with vigilance, security software makes it possible to protect users' digital life against Internet threats and safeguard your privacy and identity.

For more information, enquiries and events please do not hesitate to contact us:

***Ranjith Kumar***, Director, *ranjith.kumar@keypoint.me*, +973 17206 827

***Chahira Ashcroft***, Senior Manager, *chahira.ashcroft@keypoint.me*, +973 17206 870