GLOBAL CYBER SECURITY INCIDENCE REPORT

NEW MEDIA & INFORMATION SECURITY DEPARTMENT

April 2015

1. THE SONY PICTURES STUDIO HACKING INCIDENT

Description:

Hackers gained access to Sony's corporate (but private) emails and released several embarrassing messages to the public. Many believed that was the extent of the hack, but there was more to it: the cybercriminals also stole critical data from the company's business affairs division that included copies of unreleased films, executive salaries, and personally identifiable information about Sony's employees.

A Hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment or to evaluate those weaknesses to assist in removing them. Hacking is a diverse term that can be described in many ways.

Basis of Attack:

In an act of what some are calling cyberterrorism and in opposition to the release of the upcoming Sony Picture's movie- *The Interview*, the hackers attempted to blackmail Sony. With access to Sony's confidential data, they threatened Sony and warned them not to release the movie in any form. Sony did not comply. Although *The Interview* was released to the public, the breach, according to experts, could cost Sony more than $100 million dollars.

Defense against hacking:

- You're best off with a long password phrase that includes numbers and at least one capital letter. Something like "Iwant99pizzasand12beersfordinnertonight" is actually more secure than "Gx1U2y," because the algorithms that are used to crack passwords have to process many more computations for longer passwords.
- Don't download unnecessary attachments from emails, chat messengers, websites etc.
- Install and update recommended Antivirus software on your phones and devices.
- Another good rule is to turn off your peripherals when they're not in use

http://www.businessinsider.com/how-to-defend-yourself-against-hacking-on-any-device-2013-11#ixzz3YDVOaxvm

http://cyber-defense.sans.org/blog/2015/01/02/the-top-5-cybersecurity-breaches-of-2014

2. THERE ARE 10M COMPROMISED MOBILE APPS SAYS KASPERSKY

Description:

Mobile phone malware which can hijack a user's handset is becoming a bigger problem than ever before, Kaspersky security firm has warned.

Basis of attack:

Kaspersky labs say it has spotted over 10 million rogue android and mobile apps which can do everything from sending spam to snooping passwords. It said apps that steal user's financial information were the most common. In most cases malicious programs target the user's financial information.

The firm said the reason hackers targeted Android more was because of its open app store, unlike Apple's iTunes store which checks and controls every app made available. Android is still target number one, attracting a whopping 98.05% of known malware, no other OS gets anywhere close.

The reason for this are android's leading market position, the prevalence of third party app stores and the fact that android has a rather open architecture, making it easy to use for both app developers and malware authors alike.

Mode of Attack:

Malware are mostly installed unknowingly on target devices with the intention of stealing sensitive information or spy on users' computer for an extended period. It can take the form of executable code, scripts, active content, and other software. Malware is often disguised as, or embedded in, non-malicious files. The majority of active malware threats were worms or Trojans rather than viruses.

How to handle such incidence:

- Install anti-malware software on your android devices.
- Be very cautious of the source and what software you install on your android devices.

http://dailytrust.info/index.php/it-world/16388-there-are-10m-compromised-android-apps

3. DARWIN NUKE VULNERABILITY ALLOWS DOS IN OS X 10.10 AND IOS DEVICES

Description:

Vulnerability, dubbed "Darwin Nuke," can expose operating systems (X 10.10 and iOS 8) devices to remotely activated denial of service attacks (DoS), research from Kaspersky Lab has revealed.

According to a Securelist blog post, Discovered in 2014 in the kernel of the operating systems' Darwin open source component, the vulnerability had the potential to damage devices and corporate networks.

Mode of attack:

The vulnerability, which Apple has since patched, is connected with the processing of an IP packet that has a specific size and invalid IP options. A single incorrect network packet sent to the victim will crash the system.

While routers and firewalls usually drop incorrect packets with invalid option sizes, Kaspersky researchers discovered several combinations of incorrect IP options that are able to pass through the Internet routers.

How to handle such incidence:

- Always download latest updates via apple store: Apple iPhone, iPad, and Mac users have one more reason to upgrade to the latest versions of iOS and OS X besides the new Photos app, the 300 additional emoji characters, and several other features that Apple has packed into the operating systems.
- Updates also address any serious security vulnerabilities of previous version.
- Be very cautious of the source and what software you install on your devices.

http://www.darkreading.com/endpoint/apple-patches-darwin-nuke-other-security-flaws-with-new-os-releases/d/d-id/1319881

http://www.scmagazine.com/darwin-nuke-vulnerability-allows-dos-in-os-x-1010-and-ios-devices/article/408511/

4. PHONE SCAMMERS BACK IN BUSINESS, MICROSOFT WARNS S/AFRICANS

Description:

Microsoft South Africa is once again warning local consumers to be cautious of a reoccurring phone scam, which has left the wallets of unsuspecting consumers hundreds and (in some instances) thousands of dollars lighter.

Style of Attack:

The scam typically unfolds in the following manner: A cold caller, claiming to be a representative of Microsoft, one of its brands or a third party contracted by Microsoft, tells the victim they are checking into a computer problem, infection or virus that has been detected by Microsoft.

Cybercriminals and scammers make use of public phone directories as info gathering sources on consumers, in an effort to convince clients that they can be trusted. In addition, these callers also claim to be from Windows Helpdesk, Windows Service Centre, Microsoft Tech Support, Microsoft Support, Windows Technical Department Support Group or even Microsoft's Research and Development Team, the Microsoft warns.

Basis of attack:

In reality, the scammer only tricked unsuspecting consumers into believing that there is a problem and that paying a fee would be the best way to sort the issues out. Often they will also push clients to purchase a one year computer maintenance subscription, says Ashleigh Fenwick, Microsoft South Africa's PR and communications manager. Beyond this tactic, cybercriminals also aim to trick consumers into installing malware onto their PCs, with the aim of gathering sensitive data the likes of online banking logins.

How to tackle such incidence:

- Do not purchase software or services over the telephone, if there is a fee associated with the service, then hang up.
- Consumers should never authorise remote control over a PC to a third party, unless they can confirm that the party concerned is a legitimate representatives of a computer support team with whom they are already a customer.
- If you feel that a caller is acting suspicious, take down their information and report them to the relevant authorities.
- Never provide credit card or financial information to someone claiming to be from Microsoft tech support.

http://dailytrust.info/index.php/it-world/16386-phone-scammers-back-in-business-microsoft-warns-s-africans