GLOBAL CYBER SECURITY INCIDENCE REPORT

NEW MEDIA AND INFORMATION SECURITY DEPARTMENT

July, 2015

1. HACKER BREAKS INTO WEBCAM, SENDS VICTIM PHOTOS

Definition:

This is a technique that offers attackers the capability of logging onto systems using victims' keystrokes, stealing their documents, capturing images from their screens and staring creepily at them through their webcams.

Mode of incident

Hackers mostly uses different techniques to convince you download a piece of software that, when downloaded onto the computer, let hacker control the machine remotely. Anything you could do sitting at your desk, they could do thousands of miles away, from creating documents to playing MP3s to popping open the disk drive.

Combating such attacks:

- Use Antivirus, anti-malware etc. from renowned vendors.
- Do not open, install attachments and free software from unknown sources.
- Do not open, run or save file attachments from unknown sender.

http://www.today.ng/tech/08023001-hacker-breaks-webcam-sends-victim-photos/

2. HACKERS ARE USING MICROSOFT POWERPOINT TO ATTACK COMPUTERS

Definition:

Microsoft is scrambling to issue a Windows update after security researchers discovered a flaw in PowerPoint that hackers are using to seize control of computers.

Source of incidence:

Computer World reports that the security problem affects all of the currently supported releases of Windows. The vulnerability was discovered by three Google employees and two staff of McAfee Security.

Mode of incidence:

Hackers can use the flaw to send a target an infected PowerPoint presentation. When opened, the file will ask for certain permissions to display it. Most users, unaware of the security risks from files downloaded over the internet, will simply click to grant

permissions. Once they've done that, hackers have control over the computer and can quietly intercept its web traffic.

Preventive measures:

In an advisory notice on Microsoft site, it warned that it was aware of limited, targeted attacks taking place using the PowerPoint vulnerability. The company says it is currently investigating the problem, and it may issue a security update to protect users. In the meantime, Microsoft has released a security workaround to block infected PowerPoint files.

- Microsoft users should be very cautious when downloading PowerPoint documents on the internet.

http://www.businessinsider.com/hackers-are-using-microsoft-powerpoint-to-attack-computers-2014-10#ixzz3HL5IJJSG

3. GSMEM MALWARE DESIGNED TO INFILTRATE AIR-GAPPED COMPUTERS, STEAL DATA

Description

Newly designed malware could, if properly replicated, allow an attacker to pick up the data of air-gapped computers, which are typically thought of as relatively secure.

An **Air Gap** or air wall is a network security measure, also known as air gapping, employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

Source of incident

The malware runs in conjunction with a mobile rootkit embedded in the baseband firmware of a cell phone. It can be installed through social engineering, physical access or a malicious app. Baseband chips manage the low-level Radio Frequency (RF) connection with the cell phone network.

The malware, on the target computer, is slightly more difficult to install as it can only be put on through physical access or interdiction methods, such as poisoning the supply chain.

Mode of incident

GSMem, exploits electromagnetic radiation (EMR) emissions and forces a computer's memory bus to function similarly to an antenna in order to wirelessly transmit data to a phone over cellular frequencies.

Once both the rootkit and the malware are successfully implemented, data transmissions can be received from 3 to 18 feet away. With a hardware receiver, the data can be sent from a distance of more than 98 feet.

The components exploited by the proposed attack model are present on virtually all computers and cellular devices and even lower-end cell phones have this capability.

Basis of the attack

Modern computers are electronic devices and are bound to emit some electromagnetic radiation (EMR) at various wavelengths and strengths. Furthermore, cellular phones are agile receivers of EMR signals. Combined, these two factors create an invitation for attackers seeking to exfiltrate data over a covert channel.

How to handle such incidence

Researchers acknowledge that many organizations air-gap their computers and sometimes go as far as preventing USB insertion. Other companies, such as Intel Security, also prevent smartphones with Wi-Fi capability, cameras and Bluetooth, to enter classified areas.

Furthermore, technically the researchers recommend multiple countermeasures, including meticulous forensic analysis of a device and behavioural dynamic analysis and anomaly detection, or trying to detect GSMem activities at runtime on the process level.

1. Never open, run or save attachments from unknown sender.
2. Keep your devices physically safe.
3. Get your devices from renowned vendors.

http://www.scmagazine.com/israeli-researchers-create-new-malware-and-rootkit/article/428789/

4. APPLE APP STORE AND ITUNES BUYERS HIT BY ZERO-DAY

Description

A zero-day flaw in Apple's online AppStore and iTunes store reportedly allows attackers to hijack users' purchasing sessions, buy and download any app or movie they want, then charge it to the original user

Source of incident

German security researcher and Vulnerability Lab founder, Benjamin Kunz Meyri found that the filter bypass flaw in Apple's online invoicing system.

He published his findings on Full Disclosure on 27th July 2015, after first alerting Apple to the bug on 9 June. It is not clear from the reported timeline when Apple fixed the bug.

Mode of incident

Vulnerability Lab says the zero-day demonstrates a significant risk to buyer, sellers or Apple website managers/developers. And it warns that attackers only need a low-privilege Apple AppStore/iCloud account and low or medium user interaction to carry out the attack.

Vulnerability Lab describes the problem as an application-side input validation bug which allows remote hackers to inject their own malicious code into the Apple online service, and change the buyer's name to make their purchase.

How to handle such incidence

1. Do not click on links in unsolicited emails or pop-up adverts asking for personal information.
2. Do not send confidential information such as apps store account details and passwords over the Internet or in an email.
3. Avoid downloading unnecessary applications even from apple store and other renowned apps stores.

http://www.scmagazine.com/apple-app-store-and-itunes-buyers-hit-by-zero-day/article/428890/