MCMC Network Security Centre

Advisory: October 2016 Edition

Table of Contents

Advisory 1: IoT Botnet Denial of Service Attack

Systems Affected:

- Insecure Internet of Things (IoT) devices

Risk

- High.

Overview

- McKinsey Global Institute defined Internet of Things as the use of sensors, actuators, and data communications technology built into physical objects—from roadways to pacemakers—that enable those objects to be tracked, coordinated, or controlled across a data network or the Internet.
- The nature of IoT that is always/constantly online makes it a target of self-propagating malware (botnet). Infected IoT devices might be used to locate and compromise other IoT devices in order to further grow the botnet or launch a distributed denial of service attack.

Description

- The botnet scans the Internet for devices running telnet and SSH with default credentials. It will then use a brute force technique to crack the password.
- Upon successful login, the botnet will attempt to kill and block anything running on port 22, 23 and 80. This helps maximize the attack potential of the botnet devices.
- The IoT devices targeted by these botnets are usually home routers, network-enabled cameras, printers and digital video recorders.

Impact

- The availability of the botnet source code has increased the risk of more IoT devices being affected and more distributed denial of service attack launched.
- These botnet attacks can cause potential operational failures and interruptions to organization services.

Recommendation

- Since most of IoT botnet devices exist in dynamic memory., disconnecting the devices from the Internet and rebooting will remove them.
- Before reconnecting, change the default password to a stronger password to avoid reinfection. Update IoT devices as soon as security patches becomes available.
- Network administrator should harden network against the possibility of distributed denial of service attack.

Reference:

1. https://www.us-cert.gov/ncas/alerts/TA16-288A
2. https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html
3. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Advisory 2: New Phishing Method Targeting Malaysian Banks

Systems Affected:

- Unsuspected users

Risk

- High.

Overview

- Phishing or Fraud is defined by any act using computers, the Internet, Internet devices, and Internet services to defraud people, companies, or government agencies of money, revenue, or Internet access.
- A new variant of phishing email attack involves impersonation of government agencies to obtain the unsuspecting victim's financial account information.

Description

- The phishing URLs are usually hidden in a pdf attachment file. This makes it easier for the email to bypass an organization's spam filter.
- Unsuspecting victims are required to select their preferred bank to correct or update information as per request by the phishing email.
- Below is an example screenshot of a phishing site. Selecting any of the banks listed will redirect visitor to the bank phishing website.

Impact

- Loss of money.
- Possible identity theft and potential target in/for malicious activities.

Recommendations

- Kindly visit the MCMC website to learn more about phishing.
- Please report any phishing activity to MCMC NSC Anti-Phishing Initiative at antiphishing@cmc.gov.my.

Reference:

1. http://www.skmm.gov.my/FAQs/Phishing-Attack.aspx/
2. http://snsc.skmm.gov.my/ini-anti-phishing.php

Advisory 3: Dirty Cow Linux Vulnerability

Systems Affected:

- All version of Linux operating system

Risk

- High.

Overview

- Vulnerability in Linux, which allows the attacker to gain administrative privilege, have been discovered by the security company, Red Hat Inc.
- According to Red Hat Inc.; the vulnerability can be described as a race condition that exists in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings.

Description

- An unprivileged local attacker could use this flaw to gain highly privileged write-access rights to memory mappings that would normally be read-only.
- However, the attacker without local or shell access can use this exploit by combining it with another vulnerability such as SQL Injection to elevate administrative privilege and gaining a root status.
- The vulnerability have been found exploited in the wild, suggesting attackers had used the exploit for some time, since the vulnerability have existed since the past nine years.

Impact

- The attacker can gain control of the vulnerable system.
- An attacker will then be able to perform administrative tasks such as deleting files, viewing private information, or installing unwanted and malicious programs.

CVE-2016-5195

Recommendation

- All Linux administrators are advised to install the patch to avoid from this exploitation. Please ensure all your systems are up to date and properly patched.
- Kindly liaise with your vendors on any workaround on the known vulnerabilities.

Reference:

1. http://dirtycow.ninja/
2. http://www.csoonline.com/article/3133965/security/easy-to-exploit-rooting-flaw-puts-linux-computers-at-risk.html
3. http://arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/

Security News Headline

Dyn DDoS attack highlights vulnerability of global internet infrastructure – Computer Weekly

Rowhammer: Memory chip flaw enables hackers to root Android devices – The Inquirer

Fake Microsoft Security Essentials Antivirus Out in the Wild– Softpedia News

Ransomware Is Booming and Companies Are Paying Up – Wall Street Journal

Millions of Indian debit cards 'compromised' in security breach – BBC News

Weebly confirms hack affecting over 40 million users, Foursquare accounts also exposed– IB Times

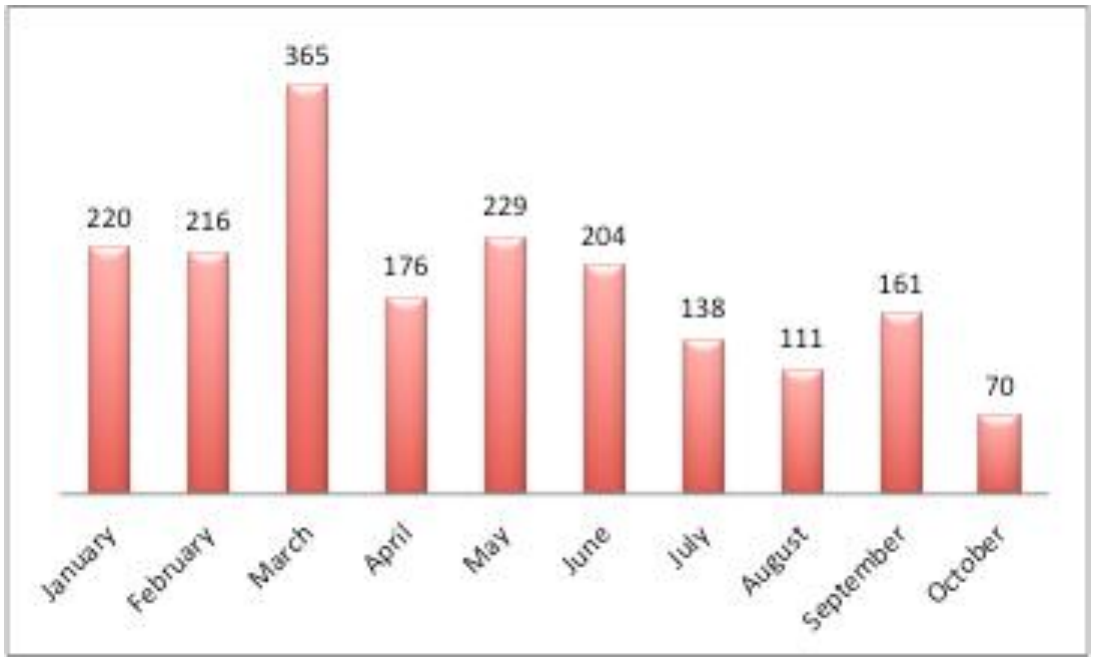
How hackers broke into John Podesta and Colin Powells Gmail accounts – Motherboard

Hacker who stole nude photos of celebrities gets 18 months in prison – The Guardian

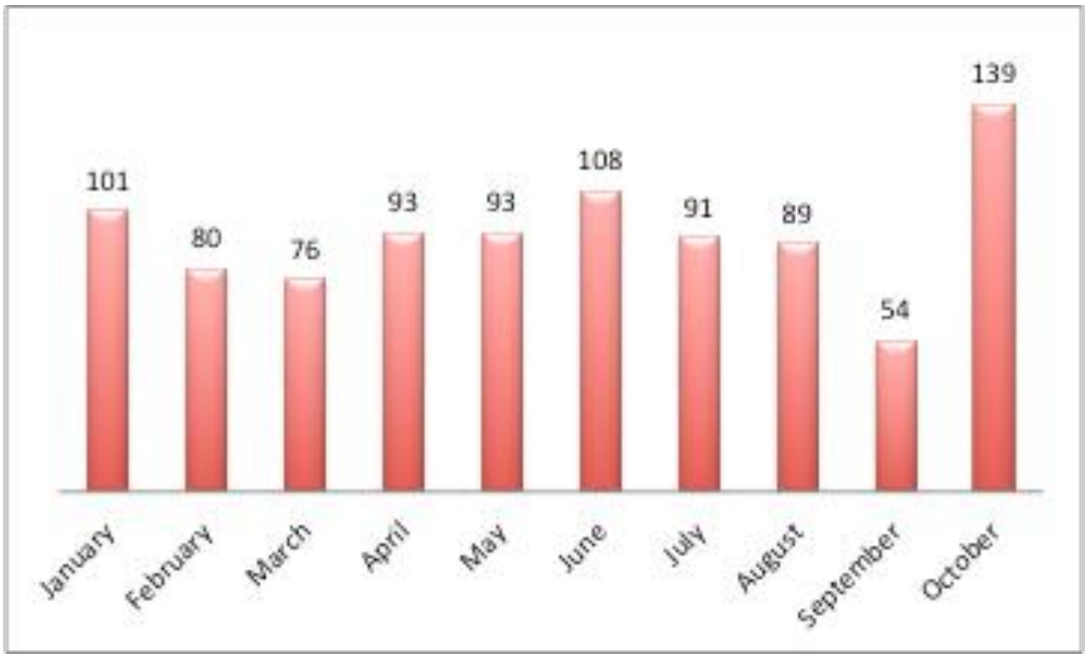
Singapore launches National Cybersecurity Strategy – Enterprise Innovation

Defacement .My and Phishing Statistic for 2016

Defacement .My:



Phishing:



Please note that defacement and phishing statistics are only based on incidents handled by MCMC NSC team. It is not a total indication of defacement and phishing occurring on that given month.

Contact Us:

MCMC Network Security Centre,
Network Surveillance Department,
Malaysian Communications and Multimedia Commission,
MCMC Tower 1,
Jalan Impact, Cyber 6,
63000, Cyberjaya,
Selangor Darul Ehsan
Tel: 03 8688 8303
Fax: 03 8688 1018
Email: nsc@cmc.gov.my
Incident Report: incident@nsc.org.my
Phishing Report: antiphishing@cmc.gov.my
Website: www.nsc.org.my