MCMC Network Security Centre

Advisory: September 2016 Edition

Table of Contents

Advisory 1: Data Breach (User)

Systems Affected:

- Users involved in a data breach incident.

Risk

- High.

Overview

- A data breach occurs when an unauthorized user illegally steals an organization's confidential data such as the username and password of customers.
- Malaysia's Personal Data and Protection Act 2010 (PDPA) compel organizations in Malaysia to take steps in protecting customers' personal data from any unauthorized, accidental access or disclosure.

Description

- An attacker gaining access to the vulnerable organization's system and stole its customer login credentials and confidential information.
- The compromised account would then be sold on the dark web or released to the public.
- Unless the victim have been notified by the organization or media, there are limited way for the victim to know his account has been breached until its already been compromised.

Impact

- An email account involved in a data breach can be taken over by the attacker or targeted with phishing emails.
- An attacker may be able to use the information to impersonate the victim and send a personalized email attack.

Organization	Breached Date	Stolen Data
Yahoo!	Late 2014	Names, Email Addresses, Tel. Numbers, Birthdays, Passwords, Security Questions
Dropbox	Mid 2012	Email Address, Password
LinkedIn	2012	Email Address, Password
Tumblr	Early 2013	Email Address, Password
Last.Fm	March 2012	Email Addresses, Passwords, Usernames, Website activity

Recommendation

- Visit data breach email checker site to check whether an email account has been compromised.
- Change all email accounts, passwords and security questions that have similar details as the breached account.
- Please be vigilant when browsing online and frequently clear your browser's cache, cookies and history.

Reference:

1. https://haveibeenpwned.com/
2. http://privacypolicies.com/blog/personal-data-breach/
3. https://united-kingdom.taylorwessing.com/globaldatahub/article_malaysia_dp.html

Advisory 2: Shadow Broker Exploits

Systems Affected:

- Network Infrastructure Devices.

Risk

- High.

Overview

- An unknown group calling themselves Shadow Broker has partially released few exploits it claims was stolen from the National Security Agency (NSA), USA.
- The group are auctioning off the full exploit to the highest bidder. However, they have yet to release any new information after releasing the exploit.

Description

- The Shadow Broker group's exploits are currently targeting vulnerabilities in routers and firewalls.
- Even after network administrator recovers control of their network; an attacker with persistent access on the network devices can re-attack the host.
- Since the full exploits haven't been released, the vulnerability is likely to still exist.

Impact

- The attacker will be able to obtain full control of the network's infrastructure, allowing them to further compromise an organization's system.

Shadow Broker Exploits			
Vendor	**CVE**	**Exploit Name**	**Vulnerability**
Fortinet	CVE-2016-6909	EGREGIOUSBLUNDER	Authentication cookie overflow
WatchGuard	CVE-2016-7089	ESCALATEPLOWMAN	Command line injection via ipconfig
Cisco	CVE-2016-6366	EXTRABACON	SNMP remote code execution
Cisco	CVE-2016-6367	EPICBANANA	Command line injection remote code execution
Cisco	CVE-2016-6415	BENIGNCERTAIN / PIXPOCKET	Information/memory leak
TOPSEC	N/A	ELIGIBLEBACHELOR	Attack vector unknown, but has an XML-like payload beginning with <?tos length="001e.%8.8x"?
TOPSEC	N/A	ELIGIBLEBOMBSHELL	HTTP cookie command injection
TOPSEC	N/A	ELIGIBLECANDIDATE	HTTP cookie command injection
TOPSEC	N/A	ELIGIBLECONTESTANT	HTTP POST parameter injection

Recommendations

- Network administrators are strongly advised to properly segregate networks and functions, limit unnecessary lateral communications, hardening your network devices, implement secure access to infrastructure devices, perform Out-of-Band management and validate integrity of hardware and software in the organization.
- Please make sure all your systems are up to date and properly patched. Kindly liaise with your vendors on any workaround on known vulnerabilities.

Reference:

1. https://www.us-cert.gov/ncas/alerts/TA16-250A
2. https://www.mycert.org.my/en/services/advisories/mycert/2016/main/detail/1234/index.html
3. https://medium.com/@msuiche/shadow-brokers-nsa-exploits-of-the-week-3f7e17bdc216 - .o38iyf90j
4. https://www.riskbasedsecurity.com/2016/08/the-shadow-brokers-lifting-the-shadows-of-the-nsas-equation-group/

Security News Headline

Zero-day vulnerability found within MySQL database application – ZDNet

Cisco issues security advisory for newly discovered Shadow Brokers vulnerability – Ciodive

Clinton, Trump Tackle Cybersecurity in Debate – Bank Info Security

A fake 'Pokémon Go' app tricked half a million players into downloading malware – Digital Trends

Global Smartphone Malware Jumps 98% Over Six Months – Infosecurity

Hackers sell tool to spread malware through torrent files – CSO

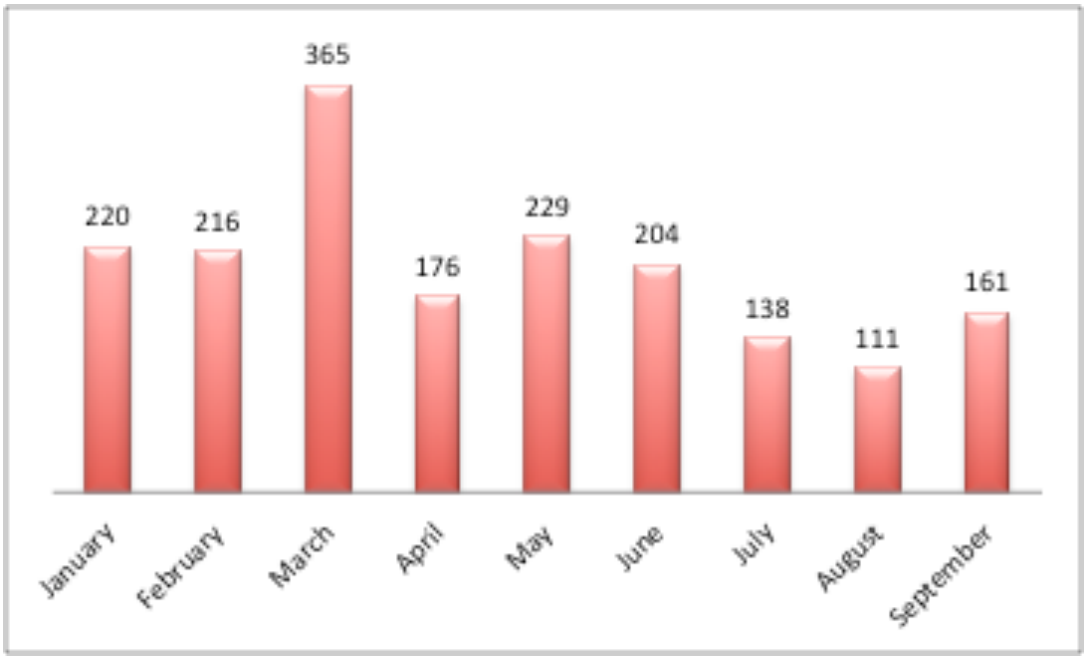
Internet's most dangerous celebrity of 2016 revealed – Mirror

Largest DDoS attack ever delivered by botnet of hijacked IoT devices – Networkworld

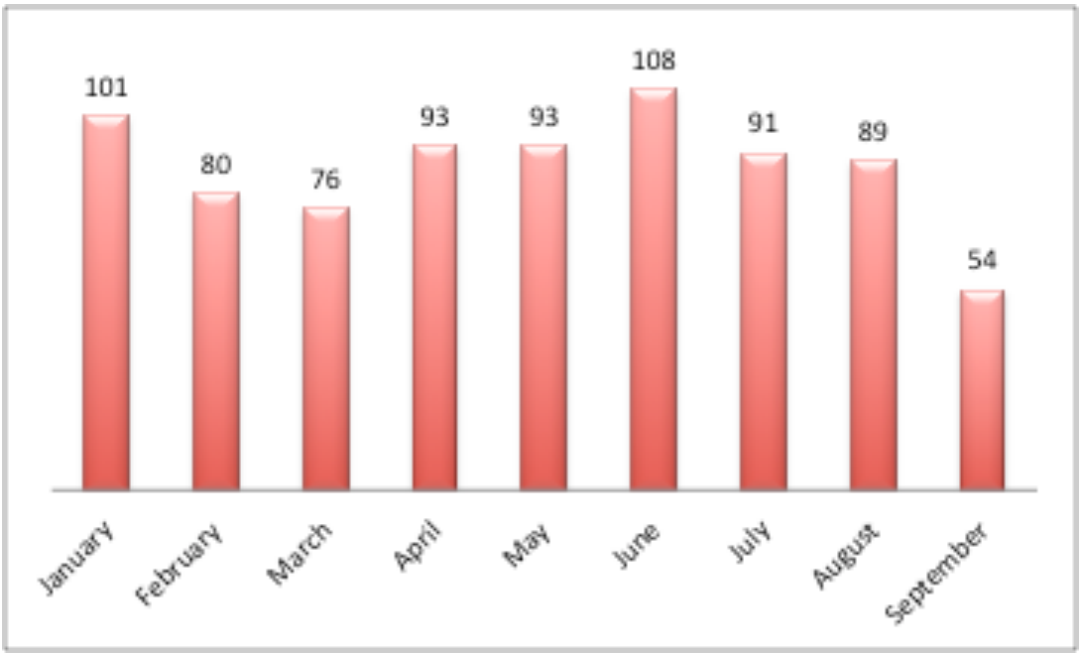
Yahoo says 500 million accounts stolen – CNN

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