

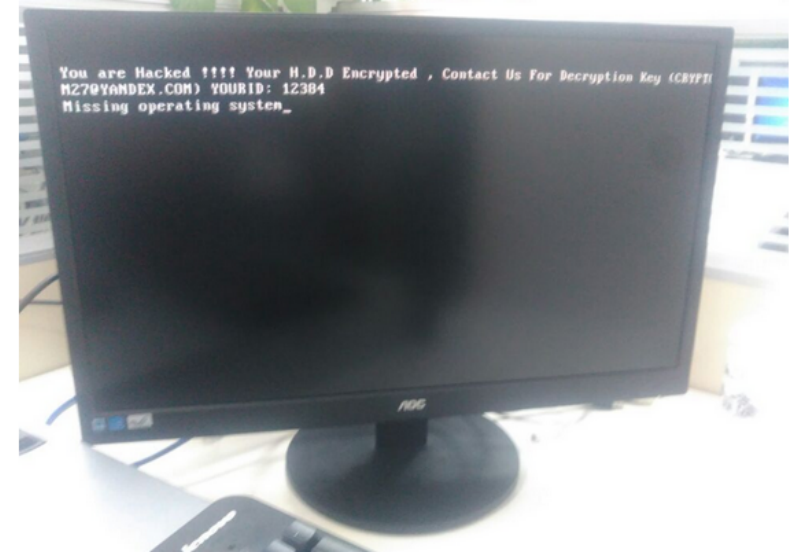
CSIRT / CERT Intro

Adli Wahid

adli@apnic.net

This Week

- Firefox 0-day Exploit
 - <http://thehackernews.com/2016/11/firefox-tor-exploit.html>
 - Exploit code published (HTML / JavaScript)
 - Affected version ?
- 900k Deutsche Telekom's broadband routers knocked offline
 - <http://thehackernews.com/2016/11/mirai-router-offline.html>
 - DDoS - services affected
 - Remote code Execution flaw in routers made by Zyxel and Speedport
 - Port, 7547. TR-069 and related TR-064 protocols
 - Shodan.io – 41Million has port 7547 open
- SF Metro hit by Ransomware
 - <https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/>
 - 100 btc (73k USD)
 - Hacker was “hacked”
 - Previous extortions discovered (140k USD)



KPN Cyber Security Policy

- KPN – One of the largest ISPs in NL
- These documents are shared on Github
 - <https://github.com/KPN-CISO/kpn-security-policy>
- Good for reference and understand scope of security
- Good Example of Leadership in Security
- Download from our internal portal
 - CSIRT/references Folder
 - kpn.zip

Policy Framework

- Framework identifies security requirements
- Top Level Policy (High Level Overview) [Mandatory]
 - Standards (What & Why) - aimed at managers [Mandatory]
 - Rules (How) – technical / practical measures [Mandatory]
 - Guidelines – Supporting
 - Tools – Supporting
- Top Level
 - Overall of Framework
 - Roles and Responsibilities
 - Assurance & Compliance

Quick Walkthrough

- Time to do some READING 😊

Other References

- NIST Cyber Security Framework
- CIS 20 Critical Security Controls
- ISO 27000 series (Information Security Management Systems)
- CERT Societe General IRP

CIS CSC Introduction

- Initially developed by SANS.org and now managed by Centre of Internet Security (CIS.org)
- To secure against Cyber Attack, organizations must defend against internal & external threats
- Two guiding principles:
 - Prevention is ideal but detection is a must
 - Offense informs defense

Goals of CSC

- What
 - Protect critical assets, infrastructure, and information
- How
 - strengthening your organization's defensive posture
 - Focusing on continuous, automated protection and monitoring of your infrastructure
- Ultimately
 - reduce compromises
 - minimize the need for recovery efforts
 - and lower associated costs
- Making fundamental computer security defenses a well-understood, replicable, measurable, scalable, reliable, automatable, and continuous process

CSC Version 6.0

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability

CSC Version 6.0 (2)

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

CSC 12: Boundary Defense

CSC 13: Data Protection

CSC 14: Controlled Access Based on the Need to Know

CSC 15: Wireless Access Control

CSC 16: Account Monitoring and Control

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

CSC 18: Application Software Security

CSC 19: Incident Response and Management

CSC 20: Penetration Tests and Red Team Exercises

CERT-Societe Generale IR Methodologies

<https://cert.societegenerale.com/en/publications.html>

Pause for a Moment

- What do we want to protect ?
- How are we protecting them ?
- Are we prepared if we have an incident today?
- Has your security philosophy changed yet?

Case Study

- The following case study is based on a real incident that took place in January 2015.
- The information shared here is based on what is available in the public domain
- No confidential information is disclosed.

404 - Plane Not Found



Hacked by LIZARD SQUAD - OFFICIAL CYBER CALIPHATE

F O L L O W C Y B E R C A L I P H A T E O N T W I T T E R :

@ L I Z A R D M A F I A

@ U M G R O B E R T

@ U M G _ C H R I S

Greetz 2:
Lizard Squad
UGNazi
NATHAN NYE
HENRY BLAIR STRATER

So What Happened?

- Hacked? Hijacked? Defaced?
 - What do these terminologies mean.
- What is the impact?
 - Business operation
 - Business reputation
 - Customers or Stakeholders
- What is affected?
 - Website
- Risk of exposure

More Questions!

- Who should be notified?
- Can you be reached if there is an security incident?
- Do you have a plan?
- Have you exercise the plan?
- How do we communicate with the media?
- Who do we need to escalate the event to?

Whois – Who is the Registrar?

Domain Name: MALYSIAAIRLINES.COM

Registrar: WEB COMMERCE COMMUNICATIONS LIMITED DBA WEBNIC.CC

Sponsoring Registrar IANA ID: 460

Whois Server: whois.webnic.cc

Referral URL: <http://www.webnic.cc>

Name Server: ASIA1.AKAM.NET

Name Server: EUR2.AKAM.NET

Name Server: EUR5.AKAM.NET

Name Server: EUR6.AKAM.NET

Name Server: NS1-104.AKAM.NET

Name Server: NS1-194.AKAM.NET

Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>

Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>

Updated Date: **26-jan-2015**

Creation Date: 01-oct-1996

Expiration Date: 30-sep-2020

Legitimate

;; ANSWER SECTION:

malaysiaairlines.com.	19	IN	A	92.122.49.249
malaysiaairlines.com.	19	IN	A	92.122.49.224
malaysiaairlines.com.	59	IN	NS	eur2.akam.net.
malaysiaairlines.com.	59	IN	NS	ns1-104.akam.net.
malaysiaairlines.com.	59	IN	NS	use3.akam.net.
malaysiaairlines.com.	59	IN	NS	eur5.akam.net.
malaysiaairlines.com.	59	IN	NS	use2.akam.net.
malaysiaairlines.com.	59	IN	NS	ns1-194.akam.net.
malaysiaairlines.com.	59	IN	NS	asia1.akam.net.
malaysiaairlines.com.	59	IN	NS	eur6.akam.net.
malaysiaairlines.com.	21599	IN	SOA	rusa.skali.com.my. domreg.skali.net. 2015011201 3600 900 604800 3600
malaysiaairlines.com.	599	IN	MX	5 mx4.malaysiaairlines.com.
malaysiaairlines.com.	599	IN	MX	5 mx3.malaysiaairlines.com.
malaysiaairlines.com.	599	IN	TXT	"v=spf1 ip4:202.75.63.206 ip4:185.15.197.10 ip4:103.6.237.252 ip4:202.75.63.207 ip4:202.75.63.194 ip4:103.6.237.183 ip4:103.6.237.184 ip4:103.6.237.186 ip4:103.6.237.190 ip4:103.6.237.203 ip4:103.6.237.210 ip4:103.6.237.240 ip4:103.6.237.248" " ip4:89.106.26.72 ip4:89.106.26.73 ip4:89.106.26.74 ip4:89.106.26.75 ip4:89.106.26.76 ip4:89.106.26.77 ip4:54.251.41.17 ip4:46.137.219.120 ip4:122.248.246.218 ip4:46.137.240.237 ~all"

\$dig again

;; ANSWER SECTION:

malaysiaairlines.com.	299	IN	A	104.28.20.11
malaysiaairlines.com.	299	IN	A	104.28.21.11

;; Query time: 73 msec

;; SERVER: 8.8.8.8#53(8.8.8.8)

;; WHEN: Mon Jan 26 04:37:23 2015

;; MSG SIZE rcvd: 70

; <<>> DiG 9.8.3-P1 <<>> malaysiaairlines.com MX

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15431

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;malaysiaairlines.com.	IN	MX
------------------------	----	----

;; ANSWER SECTION:

malaysiaairlines.com.	299	IN	MX	20 quick.nigger.cooking.
malaysiaairlines.com.	299	IN	MX	10 quick.nigger.cooking.

PING quick.nigger.cooking (128.199.57.70): 56 data bytes

64 bytes from 128.199.57.70: icmp_seq=0 ttl=53 time=78.743 ms

64 bytes from 128.199.57.70: icmp_seq=1 ttl=53 time=152.181 ms

64 bytes from 128.199.57.70: icmp_seq=2 ttl=53 time=74.585 ms

nscan report for quick.nigger.cooking (128.199.57.70)

- Host is up (0.079s latency).
- PORT STATE SERVICE VERSION
- 25/tcp open smtp Postfix smtpd

★	Subject	From
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: X9GMC	Malaysia Airlines
🔍	Re: BBAM/Alafco/MAS: MSN 39333 - DLA Opinion	Chang, Terry
☆	Malaysia Airlines Travel Itinerary Receipt: W9LDY	Malaysia Airlines
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: X78PE	Malaysia Airlines
☆	✳️ myIDTravel Leisure Booking/Listing Confirmation	noreply@myidtravel.com
☆	✳️ myIDTravel Leisure Booking/Listing Confirmation	noreply@myidtravel.com
☆	✳️ myIDTravel Leisure Booking/Listing Confirmation	noreply@myidtravel.com
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: KMJ65	Malaysia Airlines
☆	✳️ LBU to BKT; MH3076; Wed, Jan 28, 15:20 - Booking	Malaysia Airlines
☆	✳️ myIDTravel Leisure Booking/Listing Confirmation	noreply@myidtravel.com
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: X9GKE	Malaysia Airlines
☆	✳️ [#E5J-MM43VZ]: Fw: BOOKING AIR TKT SZB-KBR GOM DATO SRI MUSTAPA MOHAMED DEPT26JAN15.URGENT	Reservations
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: KMJ4S	Malaysia Airlines
☆	✳️ Malaysia Airlines Travel Itinerary Receipt: KMHT7	Malaysia Airlines
☆	✳️ Don't miss out on your booking....	Fireflyz
☆	✳️ myIDTravel Leisure Booking/Listing Confirmation	noreply@myidtravel.com





From Malaysia Airlines <noreply@malaysiaairlines.com.my>☆
 Subject **Malaysia Airlines Travel Itinerary Receipt: W9LDY**
 To BOO CHUANG WEI <amykeh@pacificvet.com.my>☆

🔒 To protect your privacy, Thunderbird has blocked remote content in this message.

Travel Itinerary Receipt

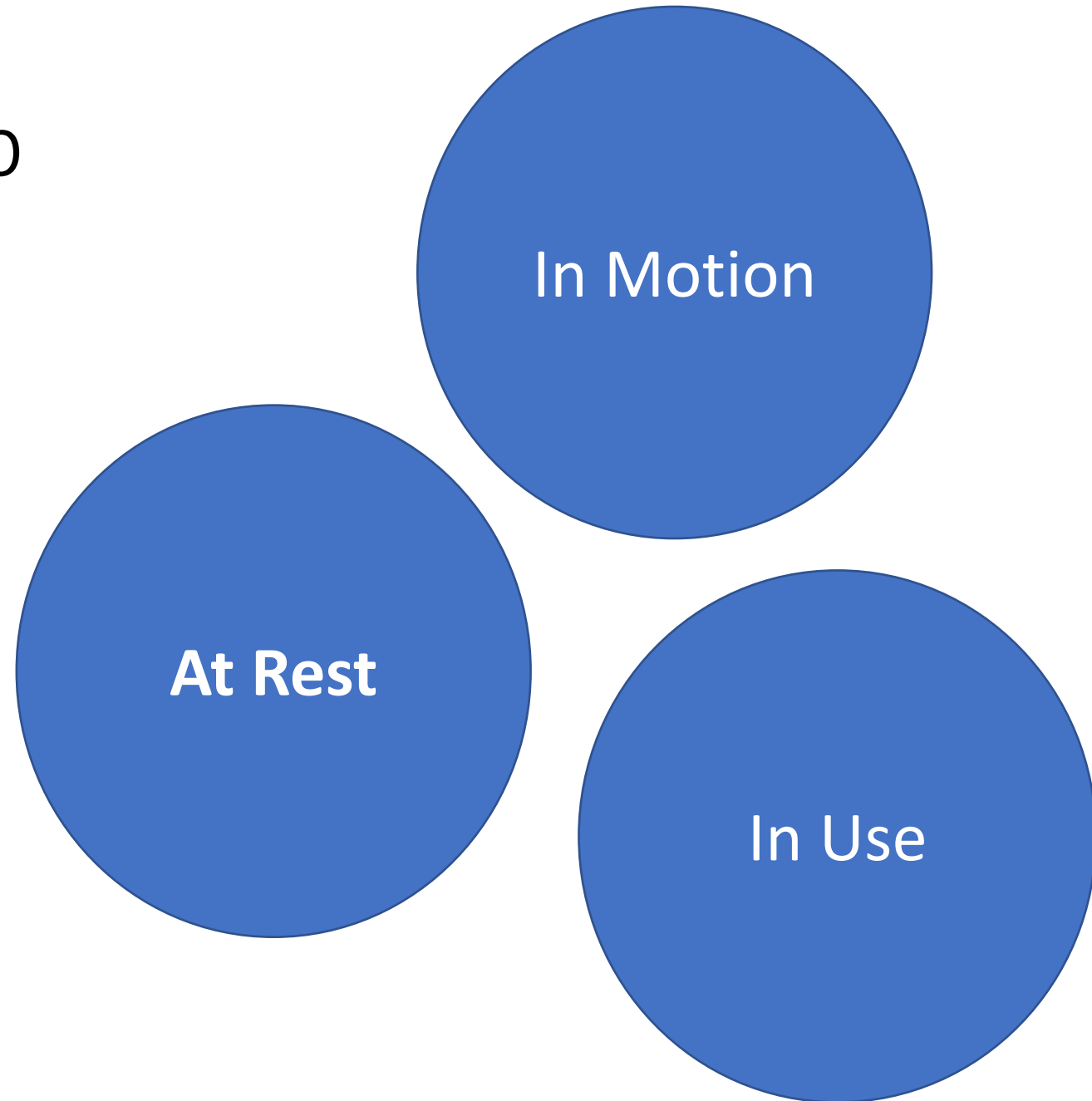
Reference: **W9LDY**
 Main contact: Ms SZE KIN
 Email: keven_1123@hotmail.com
 Mobile: 019-3331776

Passengers

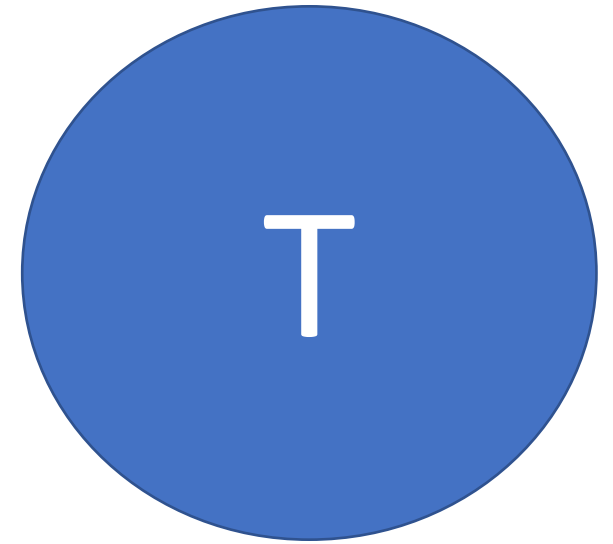
Ms KOH KIM ENG	Insurance	Travel Insurance
Ms SZE KIN	Flight	KUL-TPE, TPE-KUL
	Special Request	[Passenger Provided Contact]
	Ticket Number	2322431017933
	Seat	<div>  KUL-TPE  TPE-KUL </div>
		Seat not selected Seat not selected
Ms SZE BOOT	Insurance	Policy Number: 78672500
	Flight	KUL-TPE, TPE-KUL
	Special Request	[Passenger Provided Contact]
	Ticket Number	2322431017930
		<div>  KUL-TPE  TPE-KUL </div>

Lessons-Learned Recap

- Secure your DNS
- Authoritative & Secondary
 - Configuration
 - Application (latest?)
 - Operating system (latest?)
 - Access Control
 - Monitor Changes
- Registry / Registrar
 - 2FA
 - Monitor Changes
- Preparation / Active Defense
 - Response Time
 - Encryption (Mail)



Cyber Security



End of Case Study