



**APJ SUMMIT**

ENABLING BUSINESS DRIVEN SECURITY

# THREAT DETECTION & RESPONSE

# PROTECTING THE THAI GOVERNMENT

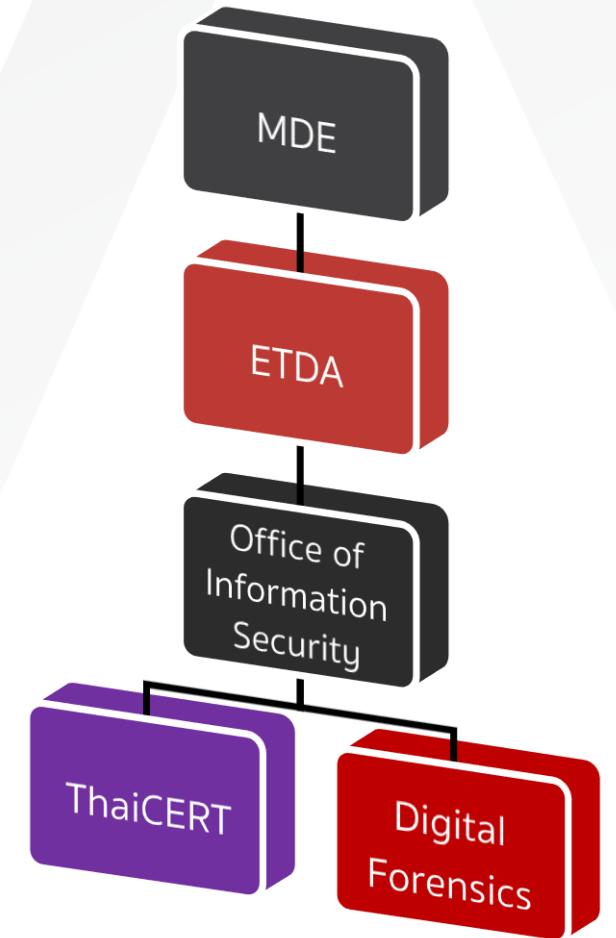
Martijn van der Heide, ThaiCERT



# ELECTRONIC TRANSACTIONS DEVELOPMENT AGENCY

ETDA is a public organization, established in 2011

- Promote and support Thailand's electronic transactions
- Provide an IT infrastructure which facilitates electronic transactions
- Help businesses regarding electronic transactions and create secure, safe and reliable IT standards and communication

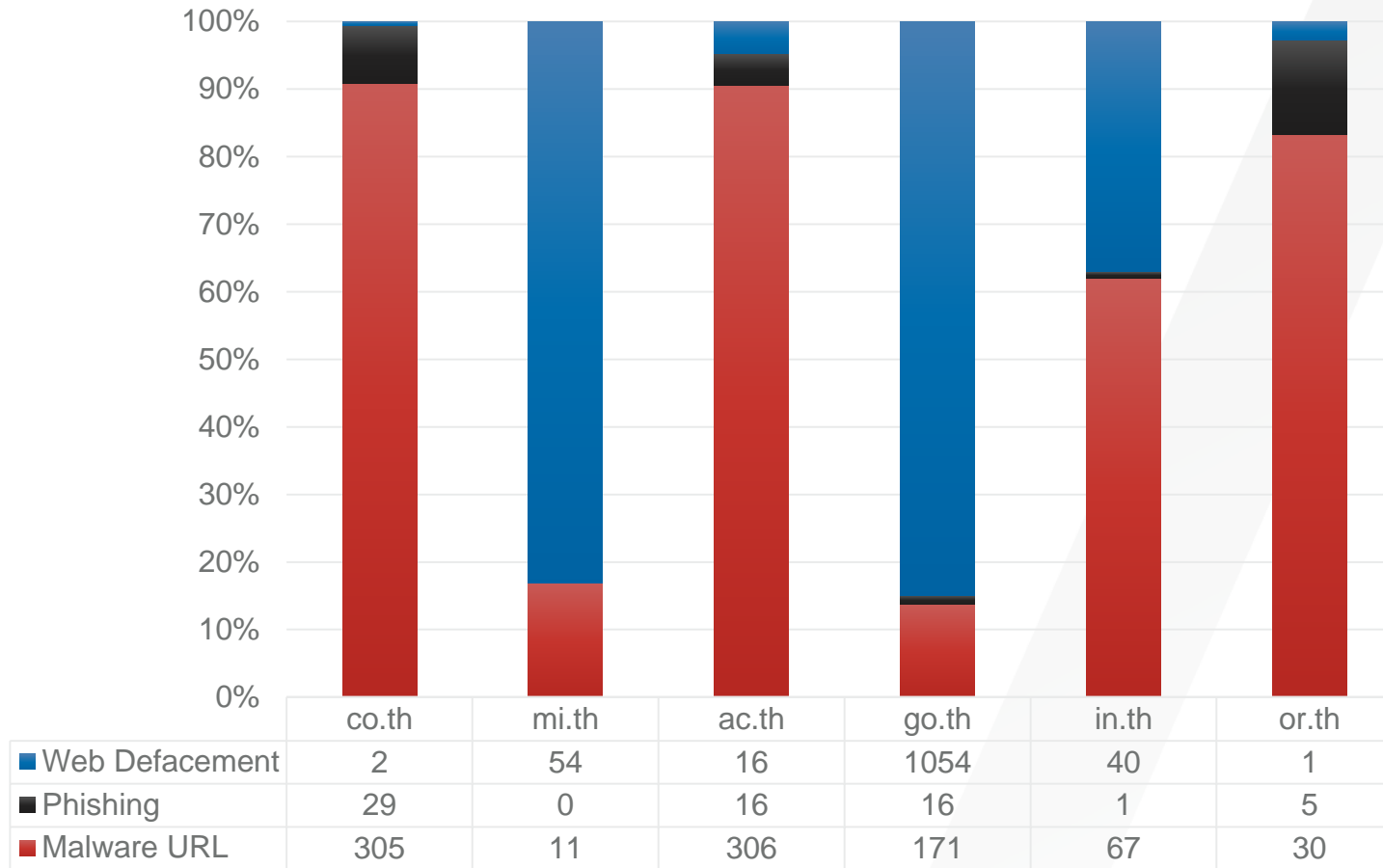


# THAICERT MISSION SINCE 2000

- **Incident Response**
  - Monitor and alert computer security incidents
  - Provide essential support and technical details
  - Research and develop tools and security guidelines
  - First team outside Europe to be TI Accredited
- **Threat monitoring**
- **Member of  APCERT and  FIRST**
  - Cooperate with Thai organizations and overseas
- **Incident Monitoring 24x7**

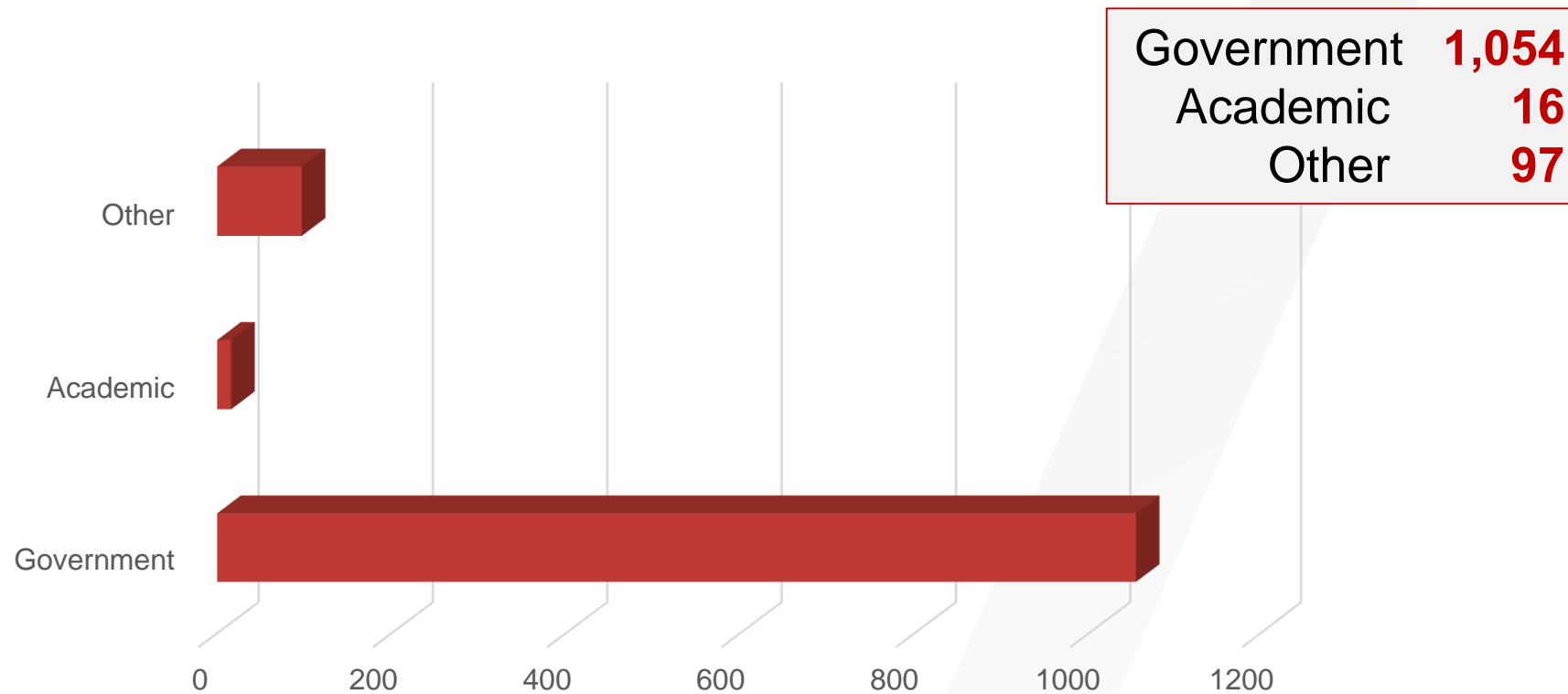


# STATISTICS ON .TH WEB ATTACKS IN 2016



# THAI WEB DEFAACEMENT STATISTICS IN 2016

Government websites were by far the largest target of defacements



# OBSERVED TRENDS

- **Many repeated incidents**
    - Back-ups are restored rather than underlying vulnerabilities patched
    - Similar vulnerabilities throughout government IT
  - **Lack of capacity and capabilities**
    - Difficulties to find enough qualified staff (more than 250 agencies)
    - Security often not recognized as crucial
- **Leverage scale:** much more efficient to combine efforts into 1 solution



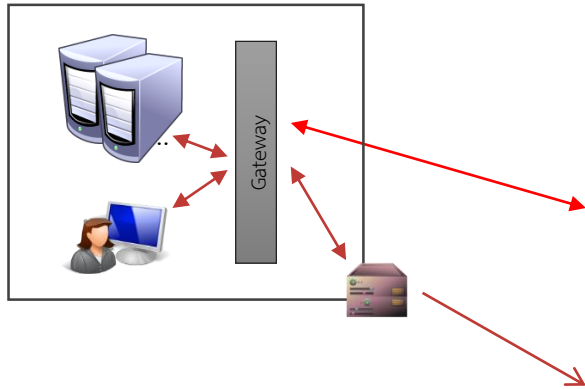
# GOVERNMENT MONITORING SYSTEM



@RSAAPJ #RSAAPJ **RSA**

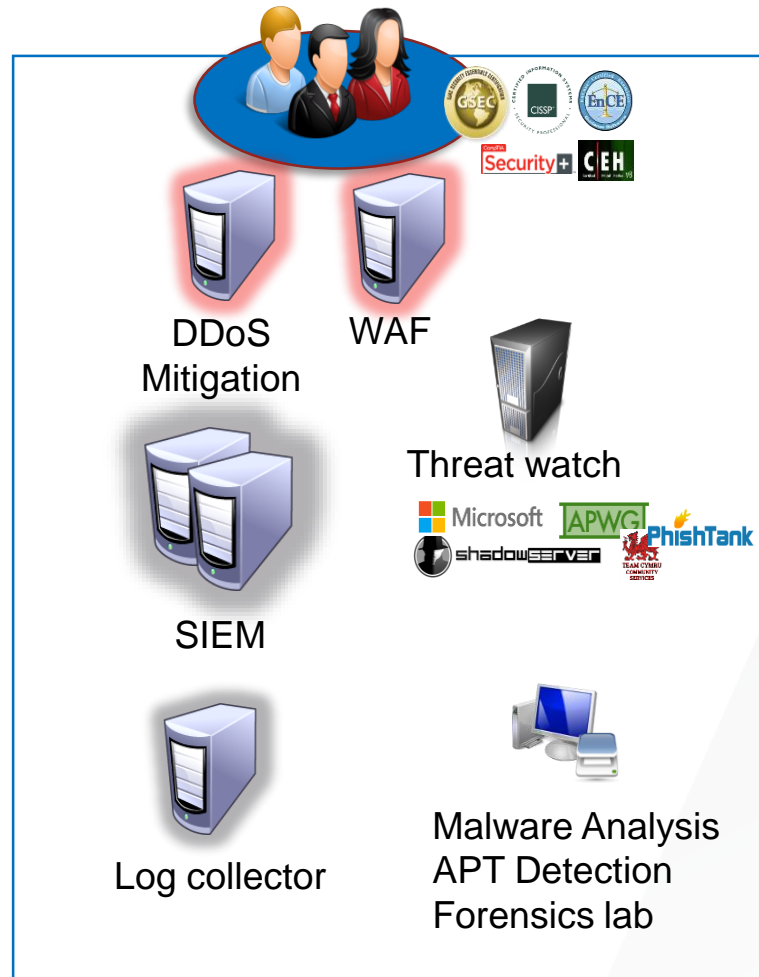
# GOVERNMENT MONITORING SYSTEM

## Agencies

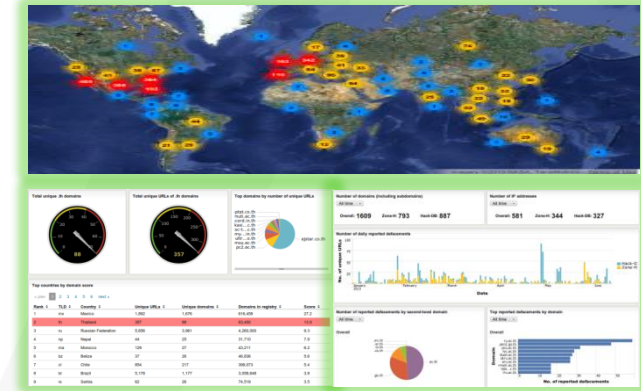


## ETDA/ThaiCERT

### CyberSecurity Operations Center (CSOC)



## Monitoring



Post Incident Services

Government Monitoring System (GMS)

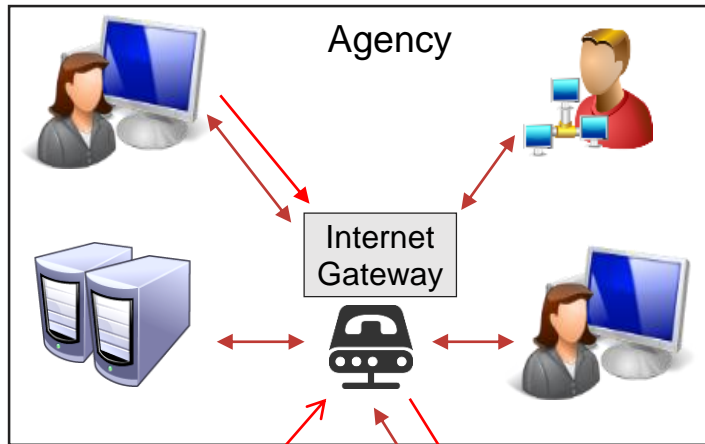
1. Government Threat Monitoring System (GTM)
2. Government Website Protection (GWP)

|                   |                     |
|-------------------|---------------------|
| Incident Handling | Malware Analysis    |
| Digital Forensics | Penetration Testing |
| Network Forensics | Awareness Training  |



# GOVERNMENT THREAT MONITORING

1 Collect log from agency's perimeter

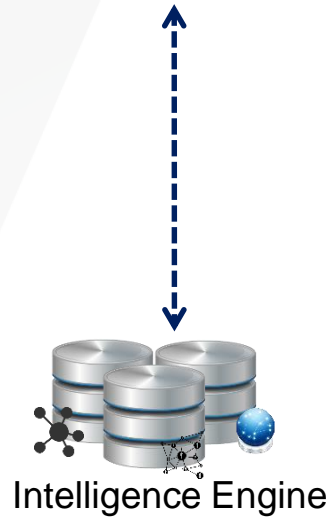
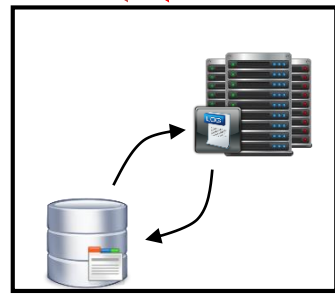


3 Send alert to agency including threat details and advisory



CyberSecurity Operations Center

2 Find suspicious traffic pattern



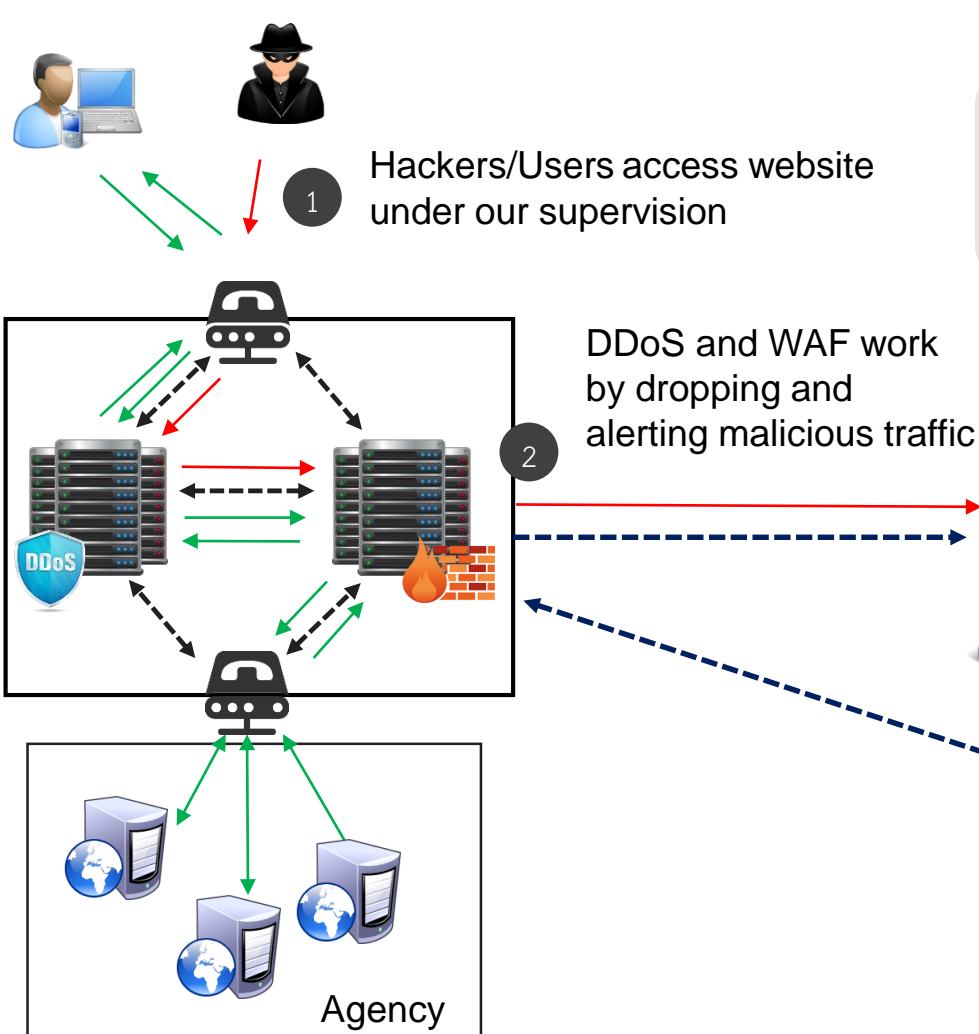
## Bookworm (Nov '15)

- Analyze suspect email
- Malicious code was attached to email
- Correlate information and found infections in more than 10 agencies



| Alert                               | Advise                              |
|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

# GOVERNMENT WEBSITE PROTECTION



Joomla!

New Joomla! 0-Day announced to public (Dec 15)

- More than 43 percent use vulnerable Joomla!

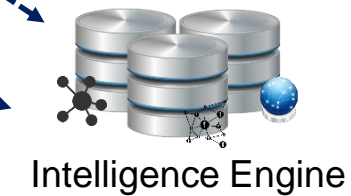
Create signature



Alert with newsbite



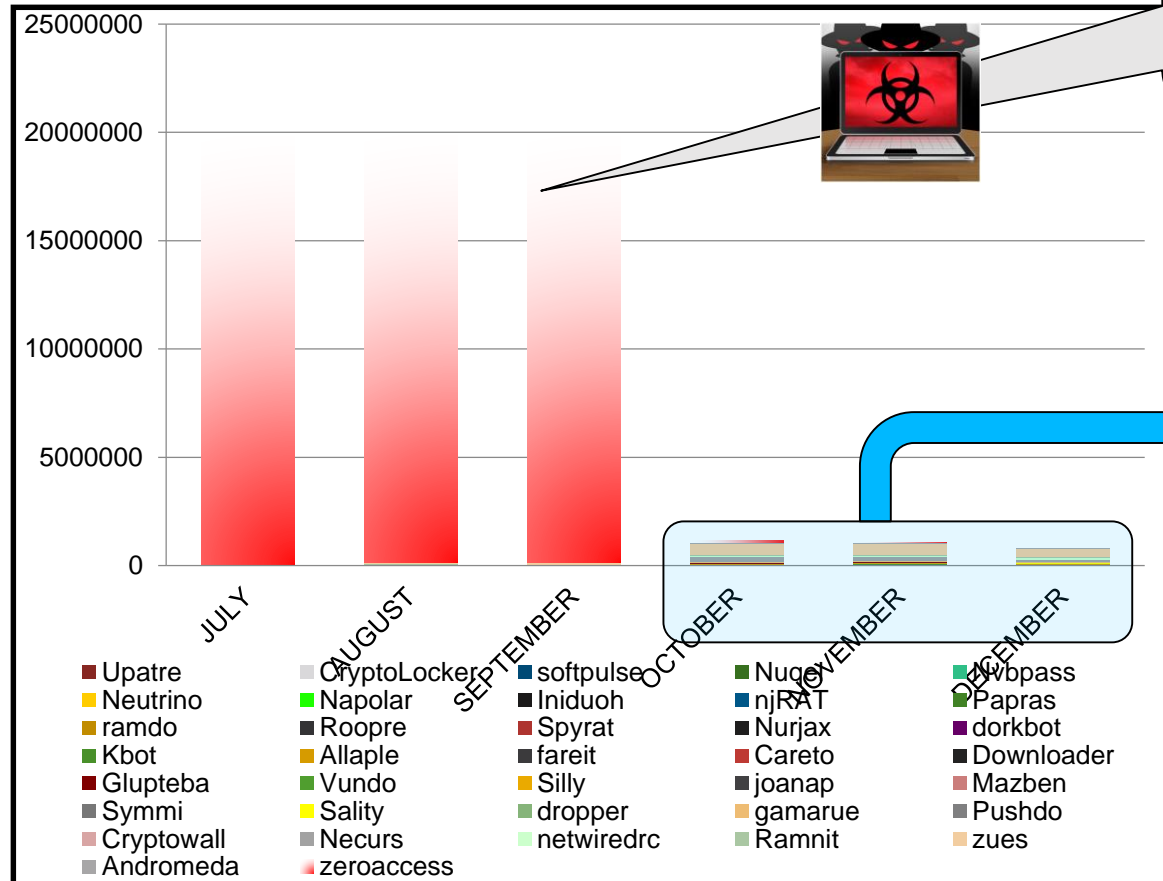
CyberSecurity Operations Center



# ROLES IN THE GMS

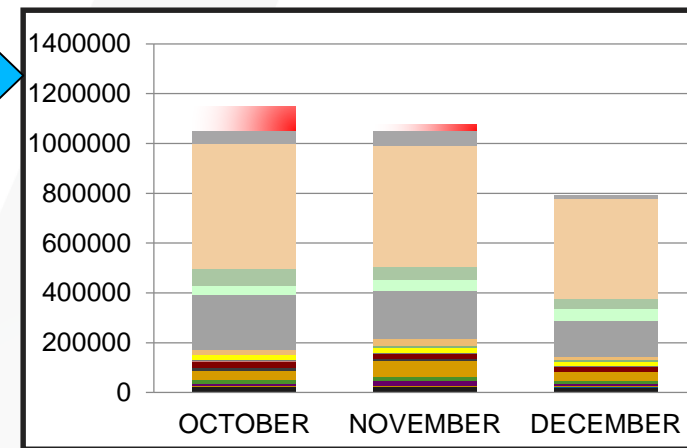
| Process name                  | ThaiCERT | Agencies     |
|-------------------------------|----------|--------------|
| Monitor and identify incident | X        | X (Optional) |
| Analyze incident              | X        | X (Optional) |
| Coordination                  | X        | X            |
| Advisory                      | X        | X            |
| Follow up and close incident  | X        | X            |
| Monthly report                | X        | -            |

# FIRST SUCCESS



Zeroaccess was the most seen infection family in 2015, after September 2016, the number of infection went down to 0.8 M records

|                                     |                                     |
|-------------------------------------|-------------------------------------|
| Alert                               | Advisory                            |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |



# DIGITAL FORENSICS CENTER

- Receives evidences from government and law enforcement agencies
- Operates under ISO/IEC 17025:2005 and ISO/IEC 27001:2013
- Can analyze any digital medium, with a clean room for hard disks
- Also skilled in malware analysis and reverse engineering





# TRAINING AND ACTIVITIES



Malware Analysis Training



PHP/Java/Android Secure Coding



Sector-based CERT



Thailand CTF Competition



# PUBLICATION AND SECURITY AWARENESS

Available at  
[www.etcha.or.th](http://www.etcha.or.th) and [www.thaicert.or.th](http://www.thaicert.or.th)

**ETDA ThaiCERT**  
 Thailand Computer Emergency Response Team  
 a member of ETDA

แจ้งเหตุภัยคุกคาม กิจกรรม แจ้งเตือนและขอแนะนำ เอกสารเผยแพร่ บริการ เว็บไซต์ที่เกี่ยวข้อง เกี่ยวกับไทยเซิร์ต

## Botnet of Things

ภัยคุกคามจาก Internet of Things  
 และแนวทางการรับมือ

**เอกสารเผยแพร่ล่าสุด**

**2016-11-16**  
 Botnet of Things - ภัยคุกคามจาก Internet of Things และแนวทางการรับมือ

**2015-07-17**  
 ข้อเสนอแนะในการเปิดการใช้งาน Flash Player บนอินเทอร์เน็ตเพื่อป้องกันไม่ให้อุปกรณ์ถูกแฮกเมื่อเกิดช่องโหว่

**2015-06-09**  
 Locker Unlocker : โปรแกรมถอดรหัสไฟล์ Ransomware

**ThaiCERT Annual Report**

|  |  |   |  |   |
|--|--|---|--|---|
| ThaiCERT Annual report 2015 Thai version | ThaiCERT Annual report 2013 Thai version | ThaiCERT Annual report 2013 English version | ThaiCERT Annual report 2012 Thai version | ThaiCERT Annual report 2012 English version |
|--|--|---|--|---|

**Cyber Security Articles & Alerts**

|                                     |                                     |                                     |                              |                          |
|-------------------------------------|-------------------------------------|-------------------------------------|------------------------------|--------------------------|
| Cyber Threat Alerts & Articles 2015 | Cyber Threat Alerts & Articles 2014 | Cyber Threat Alerts & Articles 2013 | Cyber Security Articles 2012 | Cyber Threat Alerts 2012 |
|-------------------------------------|-------------------------------------|-------------------------------------|------------------------------|--------------------------|

**SECURITY AWARENESS**

Make sure that your **PASSWORD IS HARD TO GUESS**  
 - at least 8 characters long  
 with mixed-case letters  
 numbers and symbols

**3 Months 6 Months**  
**PASSWORD MUST BE CHANGE**  
 at least every 3 months for important systems, and every 6 months for others

**จะเกิดอะไรขึ้น? ...**  
 ถ้า รหัสผ่านอีเมลส่วนตัว

**พฤติกรรมเสี่ยงใช้งาน LINE**  
 ที่ช่วยต่อการสวมรอยบัญชี

การสวมรอยบัญชี LINE ไม่ได้อาศัยแค่การไม่  
 ปลอดภัยในการใช้งาน LINE อย่างกรณีดังนี้

1. แชร์ลิงก์ไปยังบัญชี LINE
2. แชร์ลิงก์ไปยังบัญชี LINE
3. แชร์ลิงก์ไปยังบัญชี LINE
4. แชร์ลิงก์ไปยังบัญชี LINE
5. แชร์ลิงก์ไปยังบัญชี LINE
6. แชร์ลิงก์ไปยังบัญชี LINE

**THE SA WOR**  
 BANK • E-MAIL • SOCIAL MEDIA TRAINING A/C

**รหัสผ่านอีเมลปลอดภัย**

หมั่นเปลี่ยนรหัสผ่าน ทุก ๆ 3 เดือน

**สัญญาณเตือนว่า กำลังมีใครใช้งานบัญชีคุณอยู่**

สิ่งที่ไม่ได้  
 ตรวจสอบตามปกติ

พบข้อความแจ้งเตือน  
 ว่ามีการล็อกอิน

ตรวจดูรายชื่อ  
 ที่ไม่ใช่ตัว

ใช้งานอยู่  
 ลองดูว่า  
 ใช้งานได้จริง

ETDA ThaiCERT ICT

# GMS DRILL TWICE PER YEAR

- Network forensics, DDoS attack response
- System forensics, finding point of entry, lateral movement, backdoors and other artifacts on hacked systems
- Log file analysis, correlating event alerts, reconstructing time-line





**APJ SUMMIT**

ENABLING BUSINESS DRIVEN SECURITY

**THANK YOU**

**@RSAAPJ #RSAAPJ**