RSA APJ SUMMIT
ENABLING BUSINESS DRIVEN SECURITY

THREAT DETECTION & RESPONSE

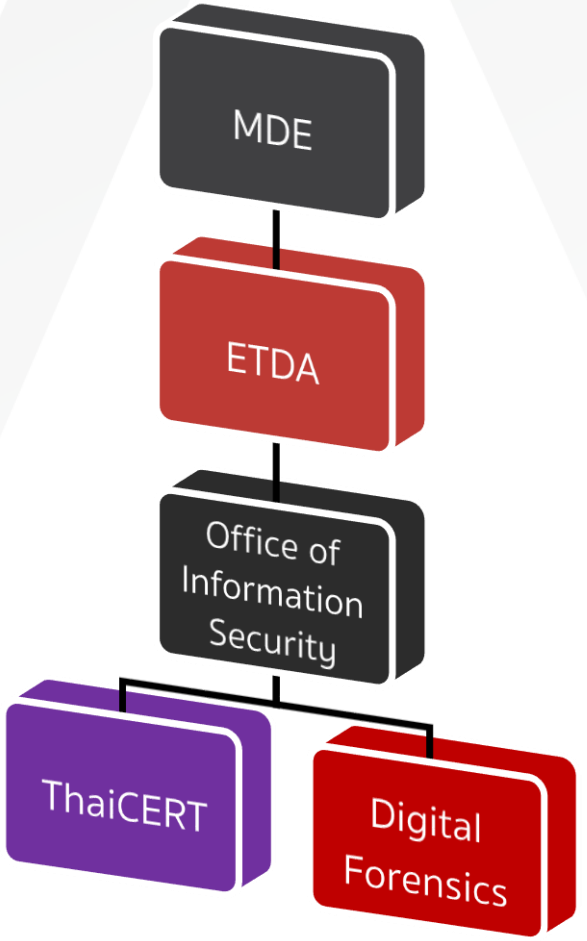
PROTECTING THE THAI GOVERNMENT

Martijn van der Heide, ThaiCERT

ELECTRONIC TRANSACTIONS DEVELOPMENT AGENCY

ETDA is a public organization, established in 2011

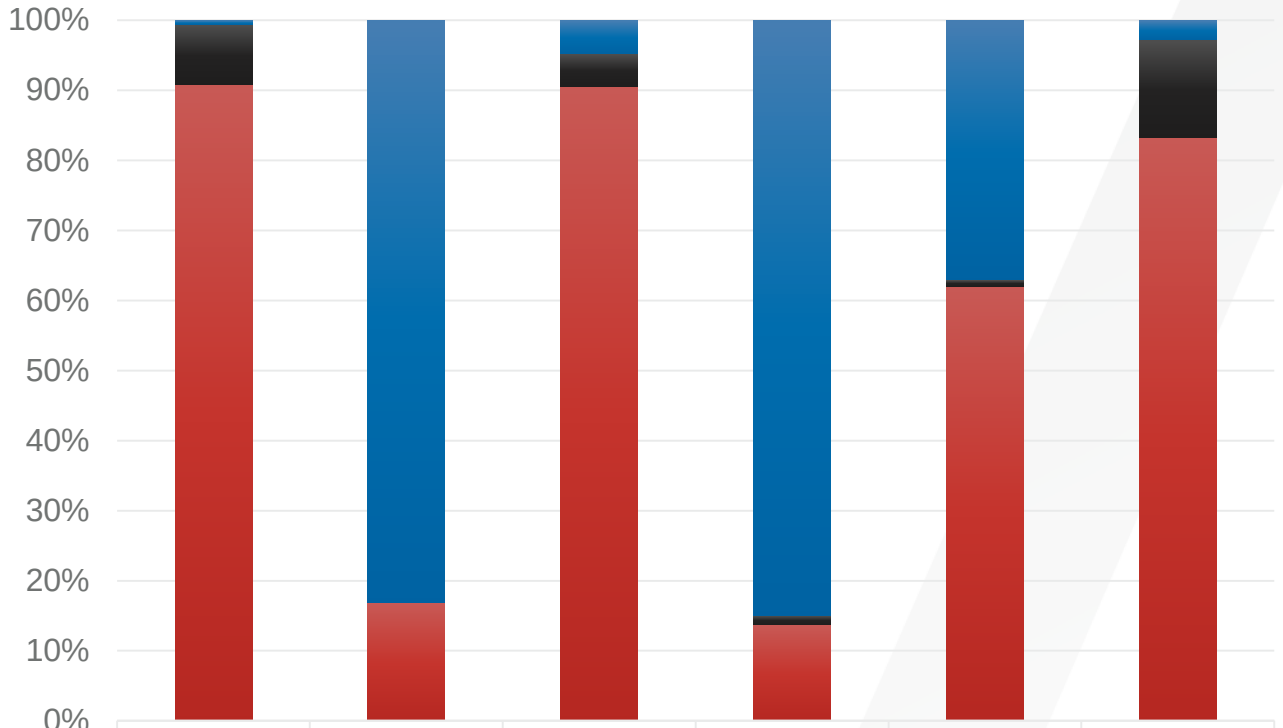
- Promote and support Thailand's electronic transactions
- Provide an IT infrastructure which facilitates electronic transactions
- Help businesses regarding electronic transactions and create secure, safe and reliable IT standards and communication



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 Asia Pacific Computer Emergency Response Team and FIRST
  - Cooperate with Thai organizations and overseas
- Incident Monitoring 24x7

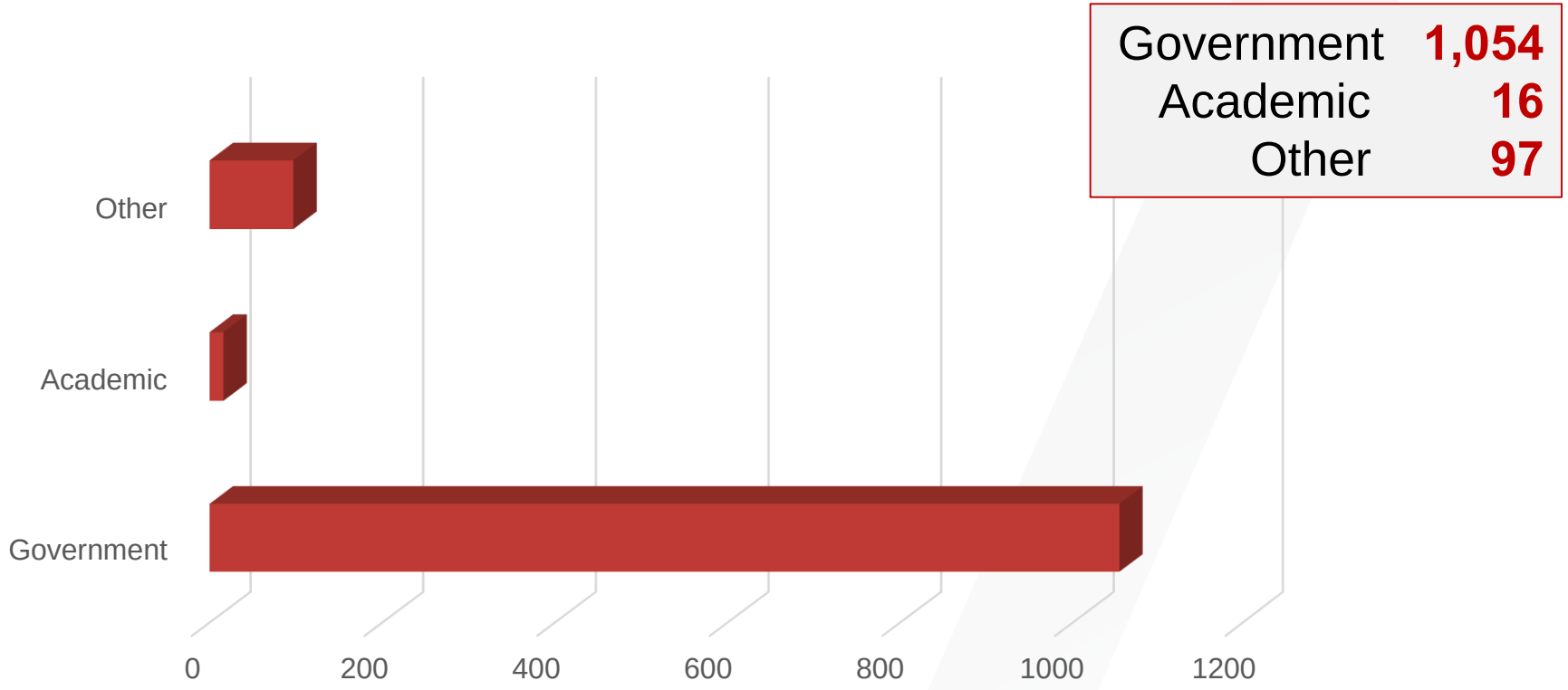
STATISTICS ON .TH WEB ATTACKS IN 2016



	co.th	mi.th	ac.th	go.th	in.th	or.th
Web Defacement	2	54	16	1054	40	1
Phishing	29	0	16	16	1	5
Malware URL	305	11	306	171	67	30

THAI WEB DEFACEMENT STATISTICS IN 2016

Government websites were by far the largest target of defacements



OBSERVED TRENDS

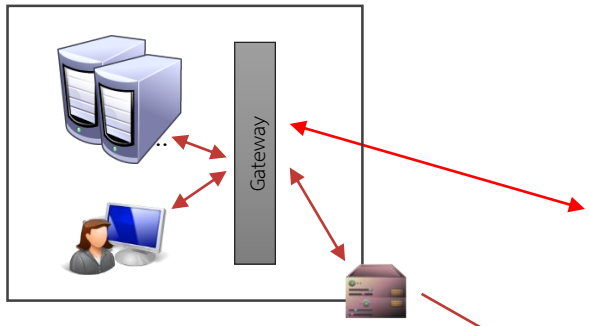
- Many repeated incidents
  - Back-ups are restored rather than underlying vulnerabilities patched
  - Similar vulnerabilities throughout government IT
- Lack of capacity and capabilities
  - Difficulties to find enough qualified staff (more than 250 agencies)
  - Security often not recognized as crucial

→ Leverage scale: much more efficient to combine efforts into 1 solution


GOVERNMENT
MONITORING SYSTEM

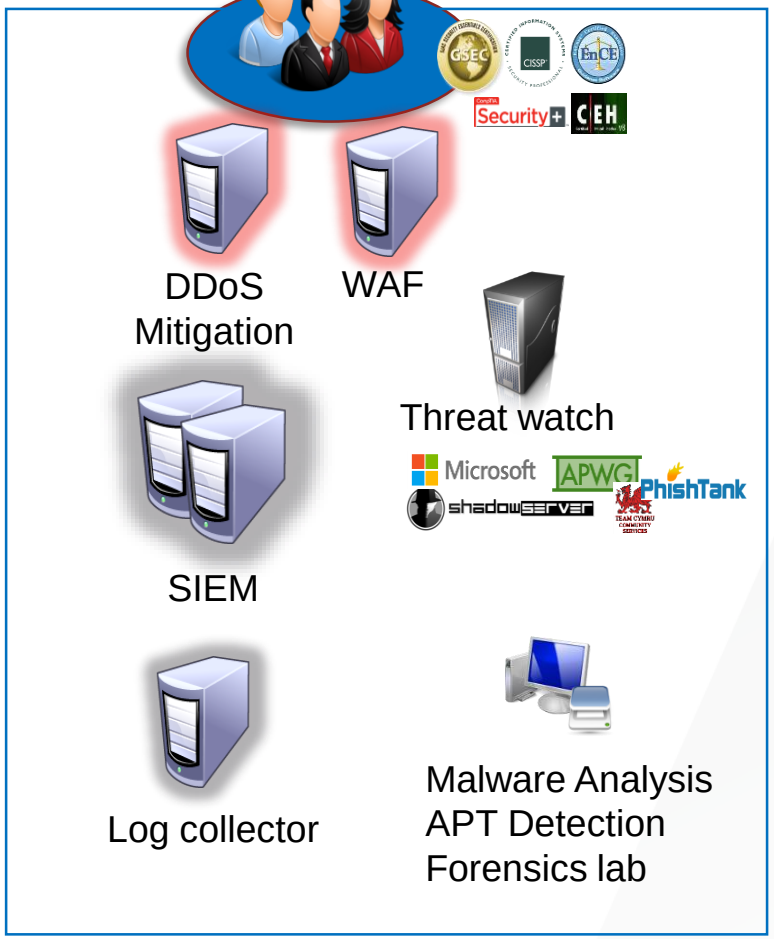
GOVERNMENT MONITORING SYSTEM

Agencies

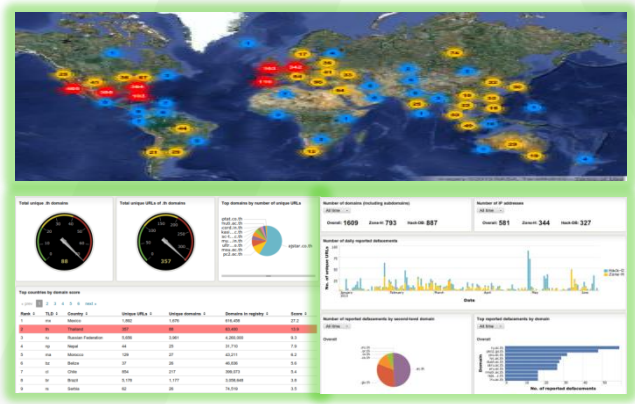


ETDA/ThaiCERT

CyberSecurity Operations Center (CSOC)



Monitoring



Post Incident Services

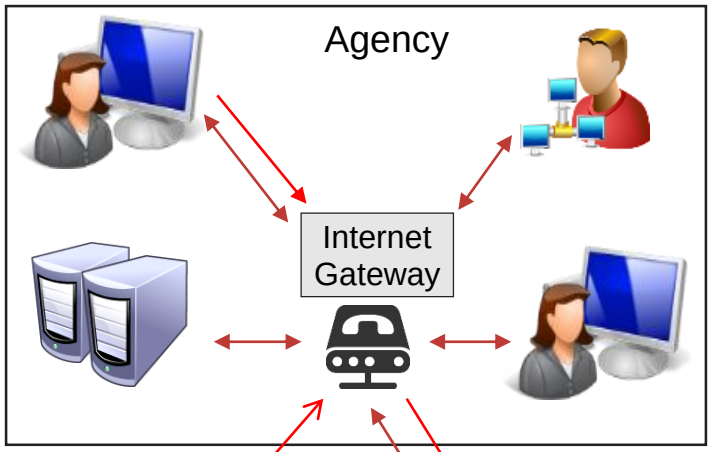
Incident Handling	Malware Analysis
Digital Forensics	Penetration Testing
Network Forensics	Awareness Training

Government Monitoring System (GMS)

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

GOVERNMENT THREAT MONITORING

1 Collect log from agency's perimeter

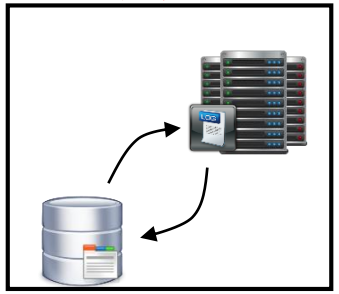


2 Find suspicious traffic pattern

3 Send alert to agency including threat details and advisory

CyberSecurity Operations Center

C&C



SIEM

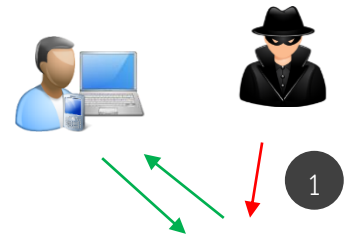
Intelligence Engine

Bookworm (Nov '15)

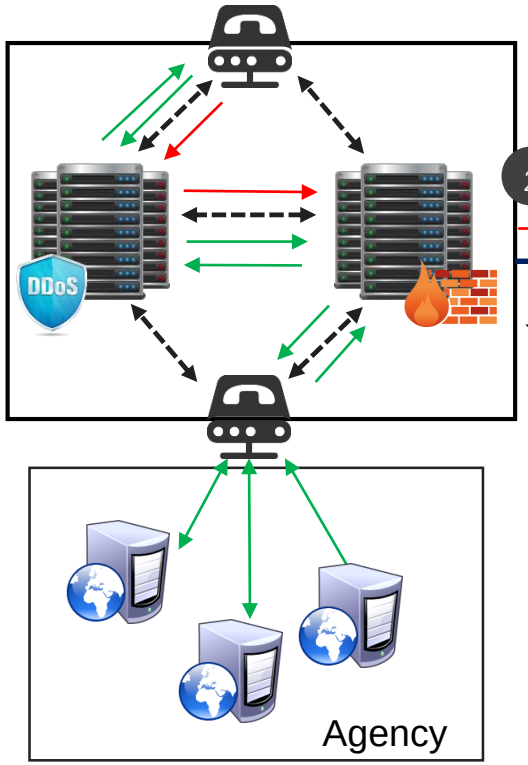
- Analyze suspect email
- Malicious code was attached to email
- Correlate information and found infections in more than 10 agencies

Alert	Advise
☑	☑

GOVERNMENT WEBSITE PROTECTION



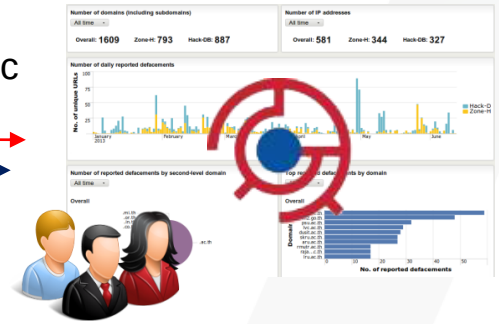
1 Hackers/Users access website under our supervision



2 DDoS and WAF work by dropping and alerting malicious traffic

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

- More than 43 percent use vulnerable Joomla!



Create signature
☑
Alert with newsbite
☑

CyberSecurity Operations Center

Intelligence Engine

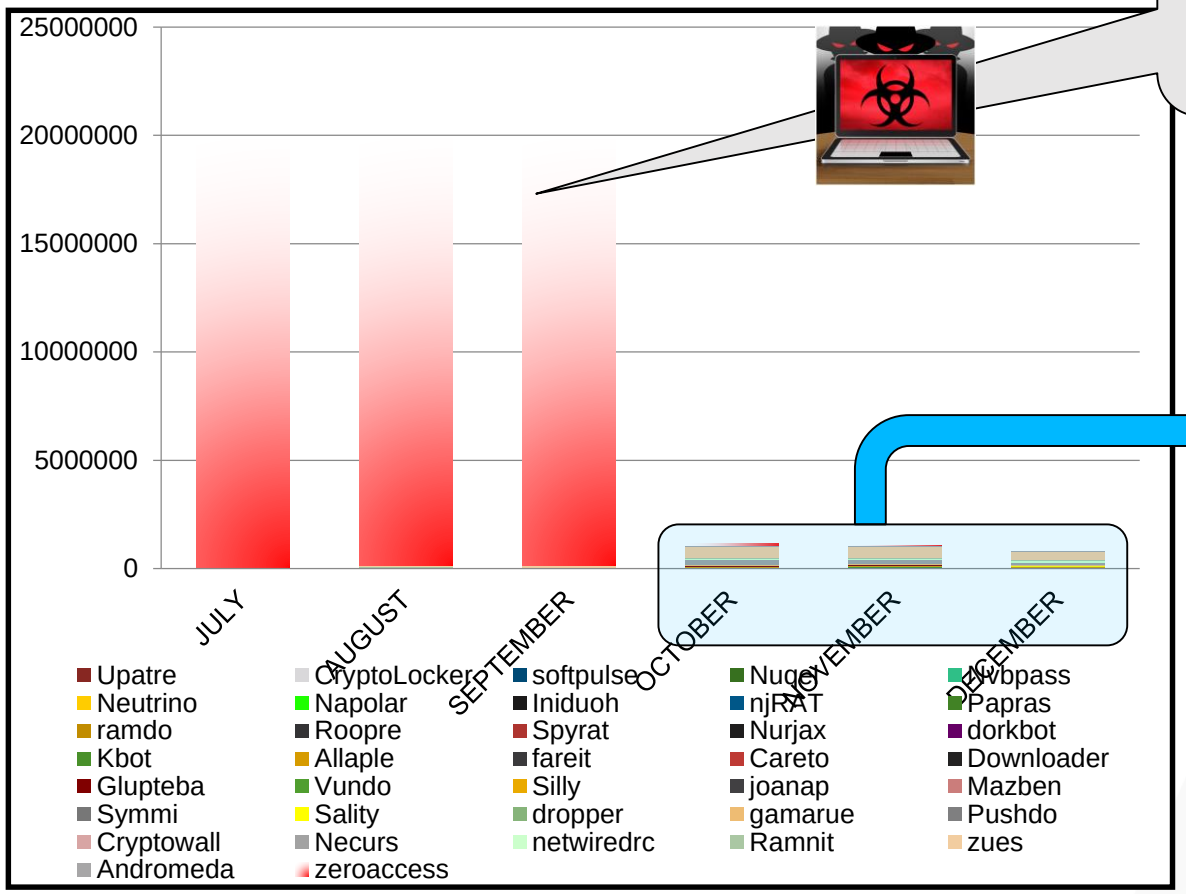
ROLES IN THE GMS

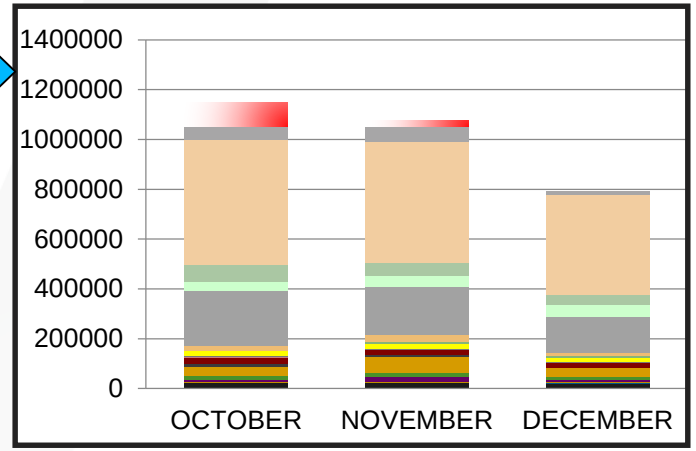
Process name	ThaiCERT	Agencies
Monitor and identify incident	**X**	**X (Optional)**
Analyze incident	**X**	**X (Optional)**
Coordination	**X**	**X**
Advisory	**X**	**X**
Follow up and close incident	**X**	**X**
Monthly report	**X**	**-**

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

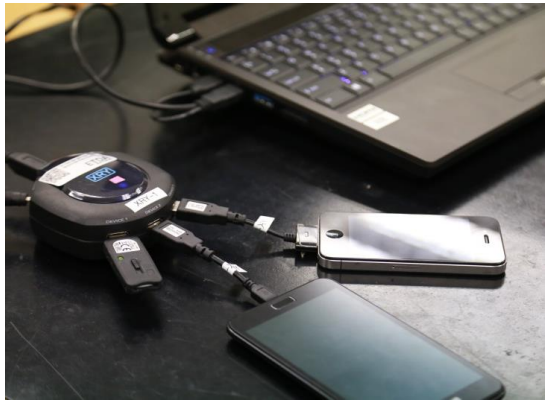
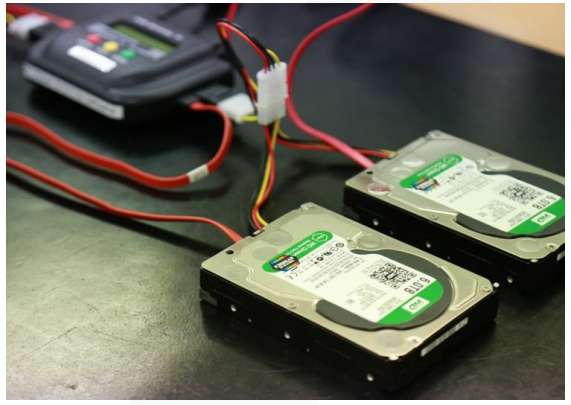
Alert	Advisory
☑	☑





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

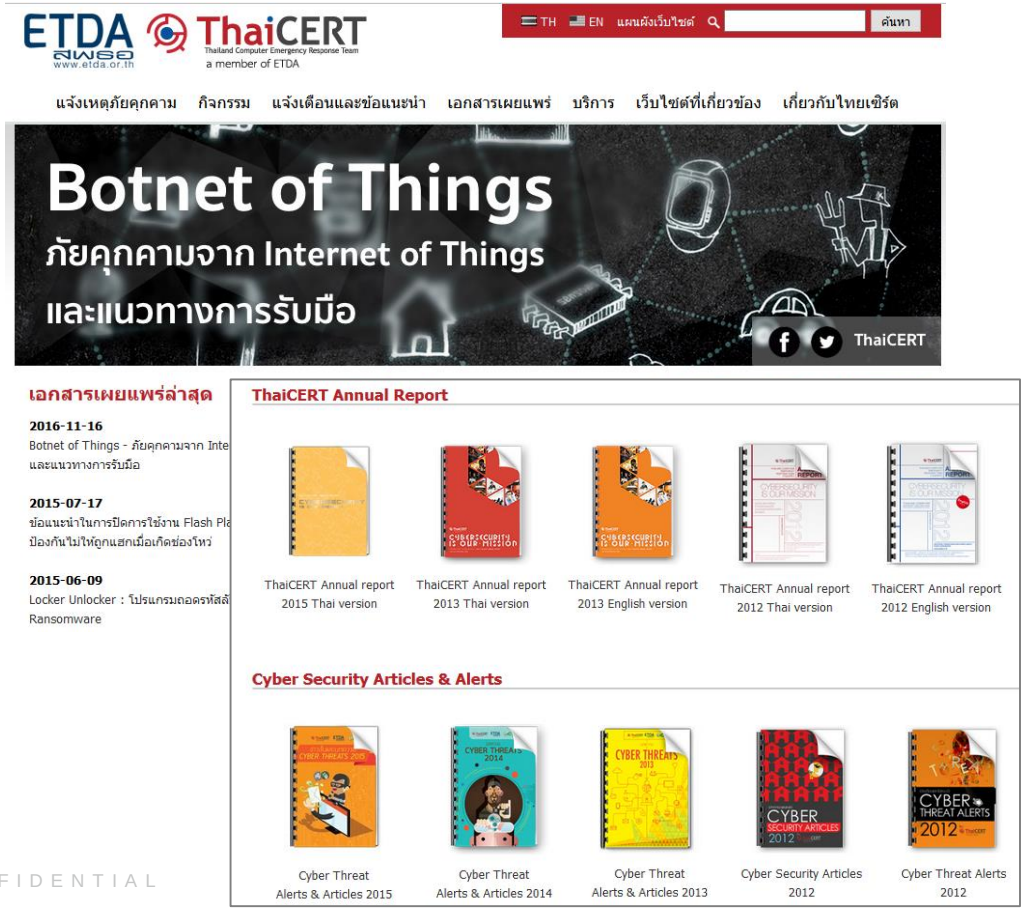
PHP/Java/Android Secure Coding

Sector-based CERT

Thailand CTF Competition

PUBLICATION AND SECURITY AWARENESS

Available at
www.etda.or.th and www.thaicert.or.th



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

RSA

APJ SUMMIT

ENABLING BUSINESS DRIVEN SECURITY

THANK YOU