ETDA สพธอ
www.etda.or.th

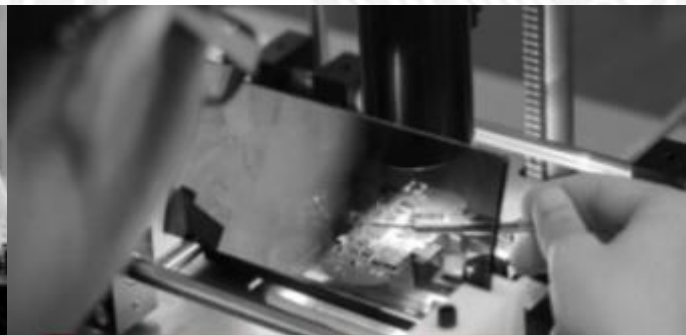
MINISTRY OF ICT
Smart Thailand

วิเคราะห์ ความเสี่ยงจากภัยคุกคามไซเบอร์ และเทคโนโลยีจำเป็นต่อบริการออนไลน์

ETDA MISSION

Trusted e-Document Authority (TeDA)

ภัยคุกคามไซเบอร์ และ กรณีศึกษาจาก ThaiCERT



ETDA MISSION

SECURITY | STANDARD | LAW

e-COMMERCE

QUALITY OF LIFE & ECONOMIC GROWTH

QUALITY OF LIFE

- SECURE ONLINE
- e-PAYMENT STANDARD
- e-DOC FOR TRADE FACILITATION
- GUIDELINES FOR AUTHENTICATION

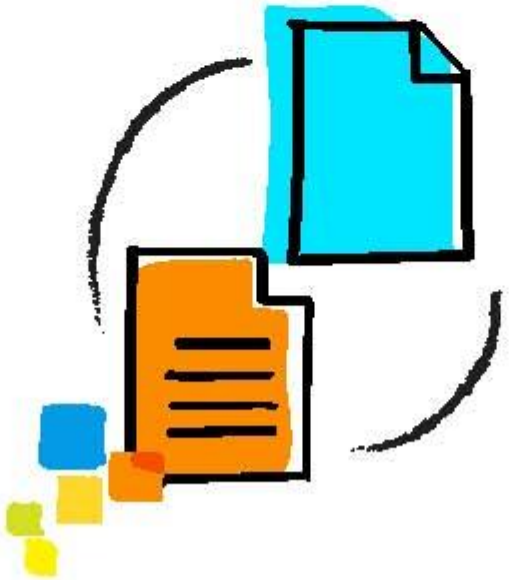
ECONOMIC GROWTH

- PROMOTE SMES & OTOP FOR e-MARKET
- TRUSTMARK ON WEBSITE FOR SECURITY AND PRIVACY PROTECTION
- IT STANDARD FOR BUSINESS PROCESS MANAGEMENT
- e-TRANSACTIONS STATISTICS

TRUSTED E-DOCUMENT AUTHORITY

PKI-BASED TECHNOLOGY

การสร้างเอกสารอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลทางกฎหมายเทียบเท่าเอกสารกระดาษ



ELECTRONIC DOCUMENT

ELECTRONIC BASED TRANSACTION

TRANSITION PERIOD

e-Document

- ม. ๘ การทำเป็นหนังสือ/มีหลักฐานเป็นหนังสือ/มีเอกสารมาแสดง
- ม. ๑๐ ต้นฉบับเอกสาร
- ม. ๑๒ การเก็บรักษา
- ม. ๘ วรรค ๒ การปิดอากรแสตมป์

e-Signature

- ม. ๙ การลงลายมือชื่อด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น username/password
- ม. ๒๖ ลายมือชื่ออิเล็กทรอนิกส์
- ม. ๙ วรรค๒ ตราประทับนิติบุคคลอิเล็กทรอนิกส์

Paper ⇄ e-Doc

- ม. ๑๒ การแปลงเอกสารกระดาษเป็นเอกสารอิเล็กทรอนิกส์
- ม. ๑๐ วรรค ๔ สิ่งพิมพ์ออก (printout)

ม. ๑๑ พยานหลักฐานอิเล็กทรอนิกส์

e-EVIDENCE

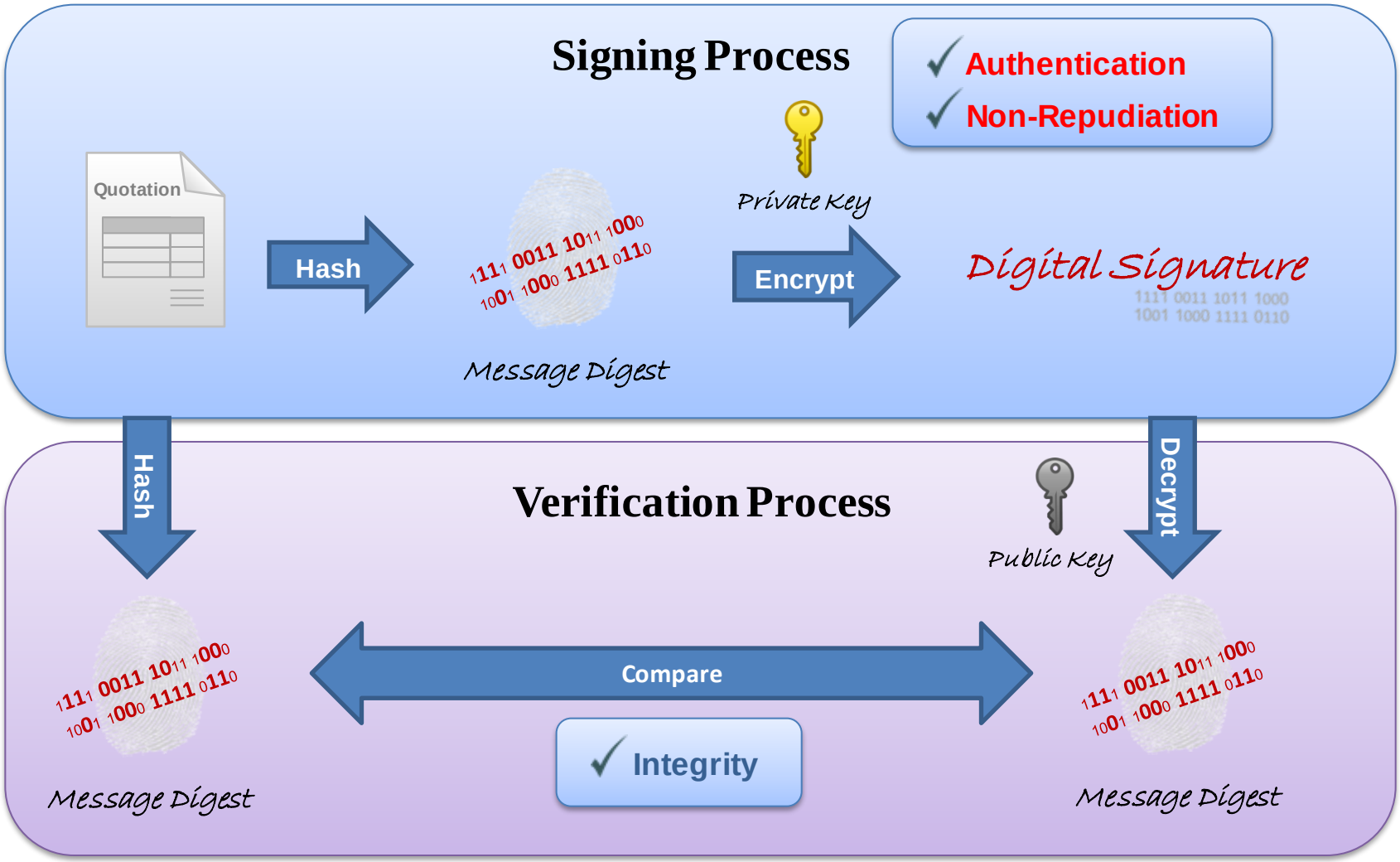
ม. ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล

ความน่าเชื่อถือของพยานหลักฐานดูจาก

- ลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์
- ลักษณะหรือวิธีการเก็บรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลง
- ลักษณะ วิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล
- รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา 25
วิธีการแบบปลอดภัย
(การปฏิบัติตามมาตรา 25 จะได้ประโยชน์จากข้อสันนิษฐานทางกฎหมาย)

ลายมือชื่ออิเล็กทรอนิกส์ กับ PKI (Public Key Infrastructure)



TRUSTED ELECTRONIC DOCUMENT AUTHORITY TEDA

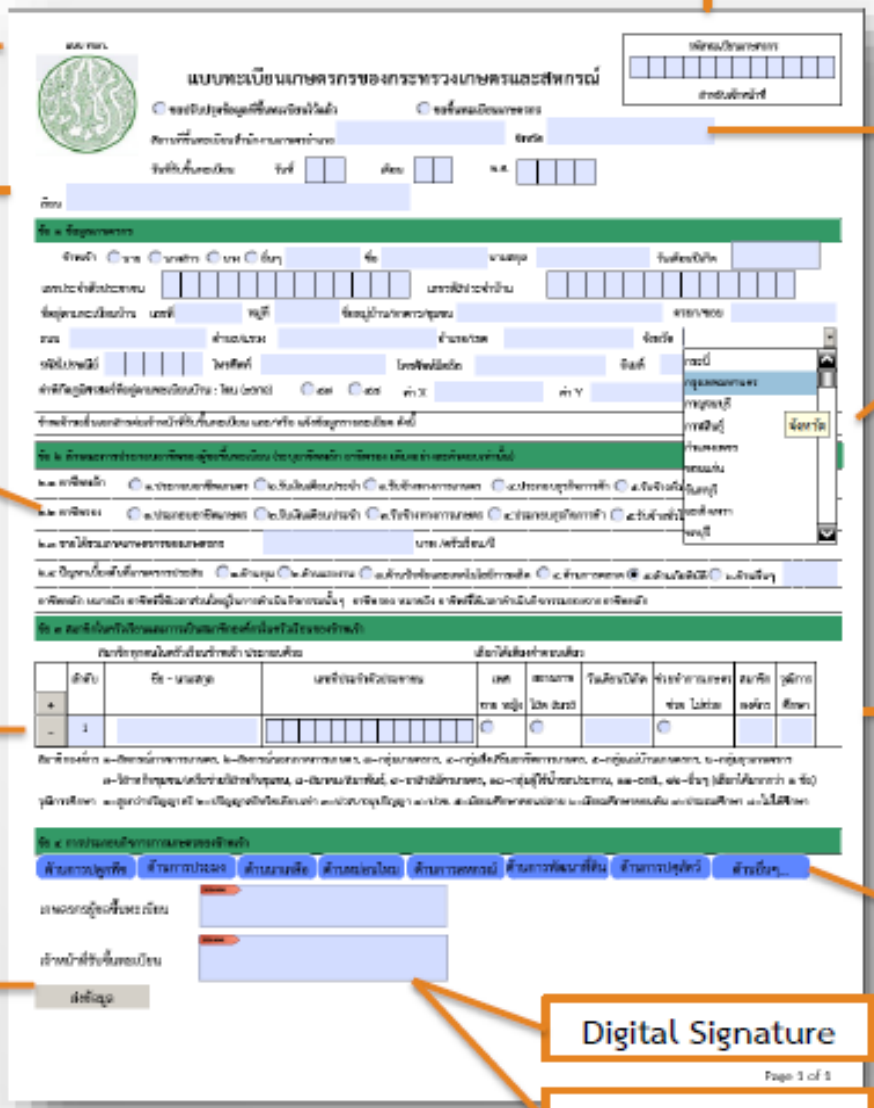
บริการที่สร้างความน่าเชื่อถือให้กับเอกสารอิเล็กทรอนิกส์ เพื่อสนับสนุนระบบงานอิเล็กทรอนิกส์ที่สำคัญของประเทศ

- **TeDA Time** — การรับรองความมีอยู่/ความถูกต้องของเอกสารด้วยการประทับรับรองเวลา
- **TeDA Safe** — การเก็บเอกสารอิเล็กทรอนิกส์ระยะยาว (Long-term Archive)
- **TeDA Sign** — การลงลายมือชื่ออิเล็กทรอนิกส์ ตาม ม.26 พ.ร.บ.ว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์
- **TeDA Form** — แบบฟอร์มอิเล็กทรอนิกส์
- **TeDA Rights** — การระบุว่าบุคคลที่ลงนามลงนามในบทบาท/หน้าที่อะไร เช่น ผู้อำนวยการ, ผู้จัดการ, แพทย์, วิศวกร

TeDA Form

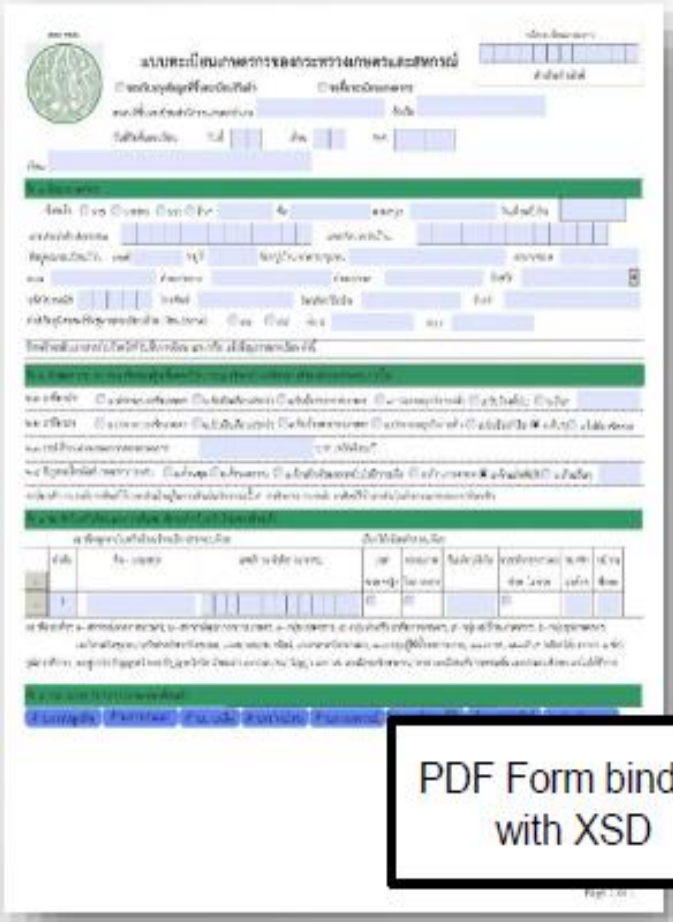
PDF Form: Features

- Data format using Schema
- XML based form
- Fillable form
- Import/export data
- CMR – Code list
- Form validation
- Digital Right Management
- Dynamic Form
- Programmatically
- Submit Form/Data
- Digital Signature
- Time Stamping



TeDA Form

PDF Form: Import/Export data

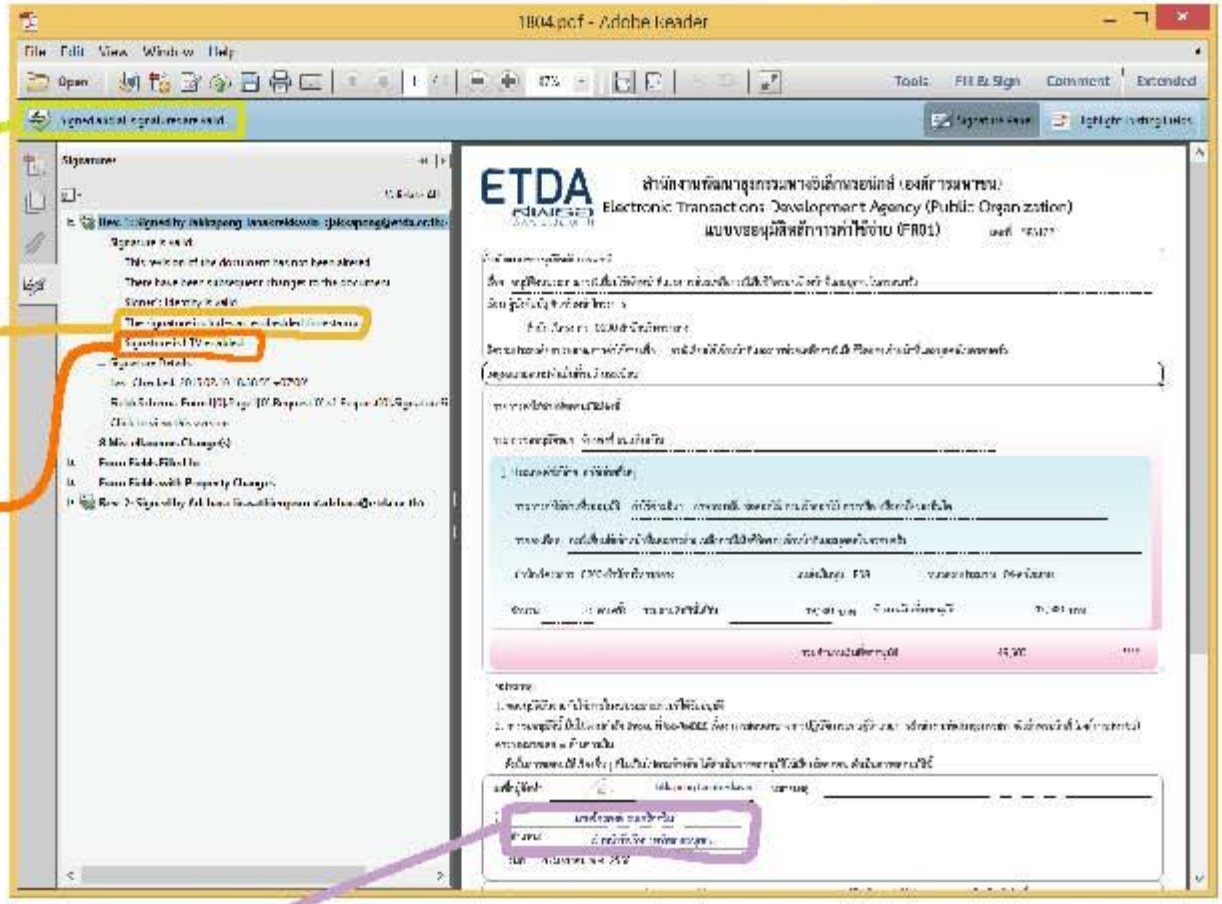


PDF Form binding with XSD

Import/Export

XML

ระบบประทับรับรองเวลา



แสดงผลการตรวจสอบเอกสาร/ลายมือชื่อ

ประทับเวลาเพื่อรับรองการมีอยู่/ความถูกต้องของเอกสาร

สามารถตรวจสอบเอกสาร/ลายมือชื่อได้ภายหลัง แม้จัดเก็บเป็นระยะเวลานาน (LONG-TERM VALIDATION)

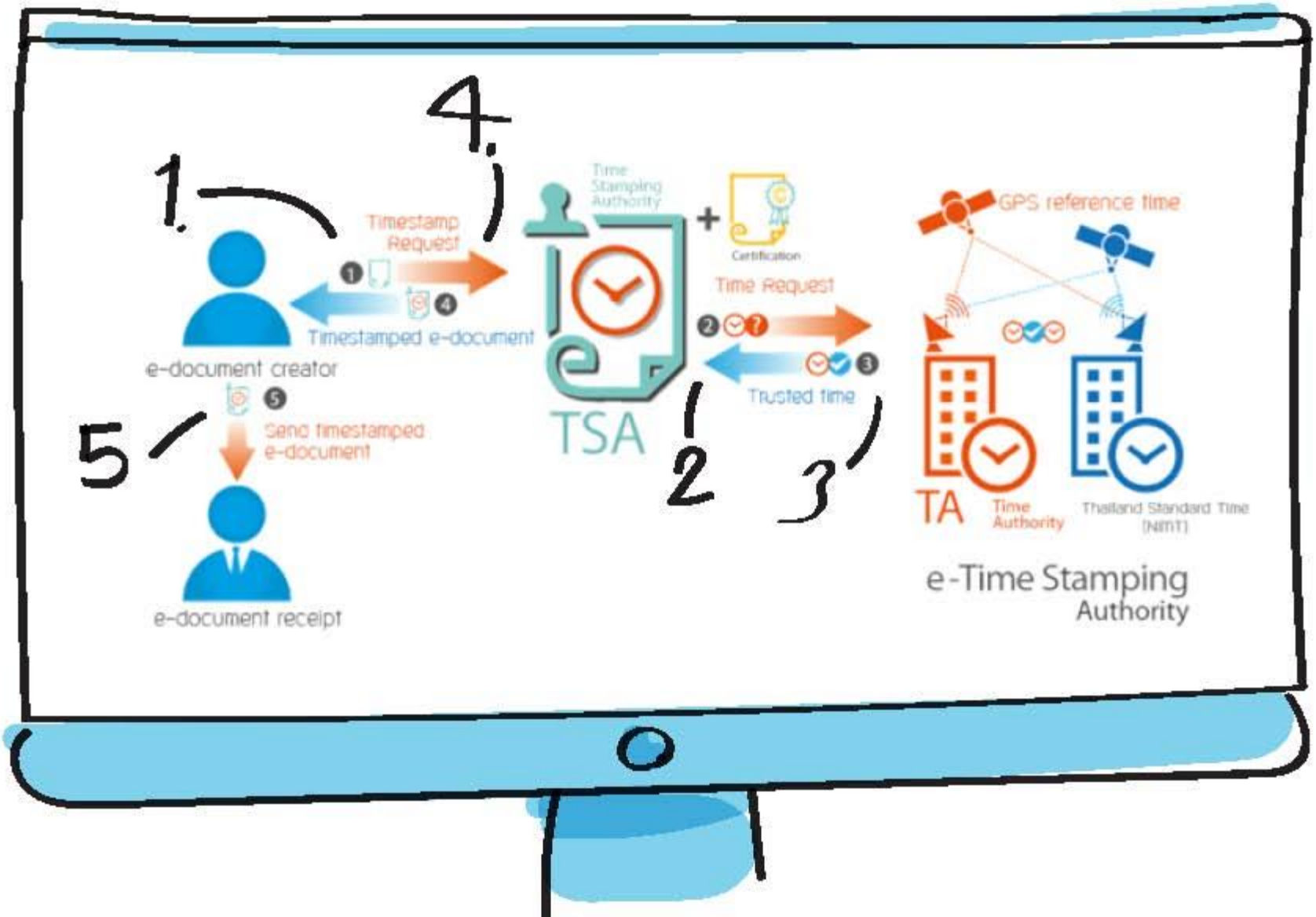
การลงลายมือชื่อในรูปแบบภาษาไทย พร้อมการระบุตำแหน่งหน้าที่ในขณะลงนาม

TeDA Sign

TeDA Rights

TeDA Time

ตัวอย่างการลงลายมือชื่อดิจิทัล/ประทับรับรองเวลา

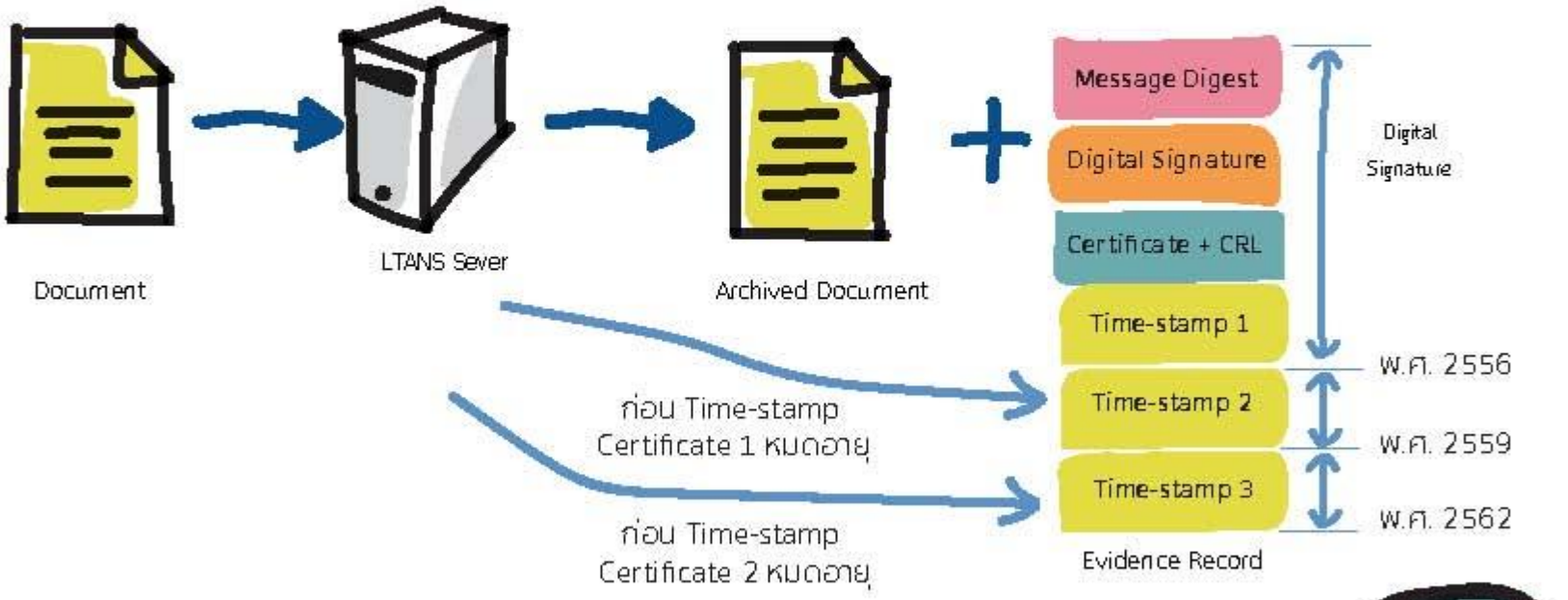


การเก็บเอกสารอิเล็กทรอนิกส์ระยะยาว (LONG-TERM ARCHIVE)

Long-term Archiving and Notary Service (LTANS)

เป็นระบบที่ช่วยในการเก็บรักษาเอกสารและช่วยในการตรวจสอบความถูกต้องครบถ้วน (Integrity)
สำหรับเอกสารที่จำเป็นต้องเก็บรักษาเป็นระยะเวลานาน เช่น พินัยกรรม เวชระเบียน สัญญา สารบบคดี เป็นต้น

กลไกในการรักษาความถูกต้องครบถ้วนของเอกสาร



TeDA Safe

การบริหารจัดการเอกสารภายใน สพธอ. ในปัจจุบัน (AS-IS)

ACTIVE DOCUMENTS

INACTIVE DOCUMENTS

เอกสารอิเล็กทรอนิกส์ +ลงลายมือตาม ม.26

งานการเงิน/พัสดุ:
- แบบคำขออนุมัติจัดหาพัสดุ (PR)
- แบบคำขออนุมัติเหตุการค่าใช้จ่าย (FR01)
- แบบขออนุมัติเบิกค่าใช้จ่าย (FR02)
- แบบขออนุมัติยืมเงิน (AD)
- แบบขออนุมัติคืนเงินทดรองจ่าย (CV)

จัดเก็บเอกสาร
พร้อม Metadata

Enterprise Content Management

Archive

LTANS System

TeDA Safe

เอกสารอิเล็กทรอนิกส์ +ลงลายมือชื่อตาม ม.9

งานสารบรรณ:
- หนังสือจากหน่วยงานภายนอก(สแกน)
- บันทึกข้อความ
- เอกสารแนบ

จัดเก็บเอกสาร
พร้อม Metadata

เอกสารกระดาษ

งานจัดซื้อ/พัสดุ
- เอกสารจัดซื้อ เช่น TOR, PROPOSAL,
- หนังสือมอบอำนาจ
- เอกสารตรวจรับงาน เช่น เอกสารตรวจรับ,
- ส่งส่งมอบ, ใบเสร็จรับเงิน, หลักฐานการจ่ายเงิน

งานสารบรรณ:
- หนังสือจากหน่วยงานภายนอก

Archive

โกดังเก็บเอกสาร

การบริหารจัดการเอกสารภายใน สพธอ. ในอนาคต (TO-BE)

ACTIVE DOCUMENTS

INACTIVE DOCUMENTS

เอกสารอิเล็กทรอนิกส์ +ลงลายมือตาม ม.26

งานการเงิน/พัสดุ:
- แบบคำขออนุมัติจัดหาพัสดุ (PR)
- แบบคำขออนุมัติเหลักการค่าใช้จ่าย (FR01)
- แบบขออนุมัติเบิกค่าใช้จ่าย (FR02)
- แบบขออนุมัติยืมเงิน (AD)
- แบบขออนุมัติคืนเงินทดรองจ่าย (CV)

จัดเก็บเอกสาร
พร้อม Metadata

Enterprise Content Management

Archive

LTAHS System

TeDA Safe

เอกสารอิเล็กทรอนิกส์ +ลงลายมือชื่อตาม ม.9

งานสารบรรณ:
- หนังสือจากหน่วยงานภายนอก(สแกน)
- บันทึกข้อความ
- เอกสารแนบ

จัดเก็บเอกสาร
พร้อม Metadata

ลงลายมือชื่อ
ตาม ม. 26

เอกสารกระดาษ

งานจัดซื้อ/พัสดุ
- เอกสารจัดซื้อ เช่น TOR, PROPOSAL,
- หนังสือมอบอำนาจ
- เอกสารตรวจรับงาน เช่น เอกสารตรวจรับ,
- ส่งส่งมอบ, ใบเสร็จรับเงิน, หลักฐานการจ่ายเงิน

งานสารบรรณ:
- หนังสือจากหน่วยงานภายนอก

ลงลายมือชื่อ
ตาม ม. 26

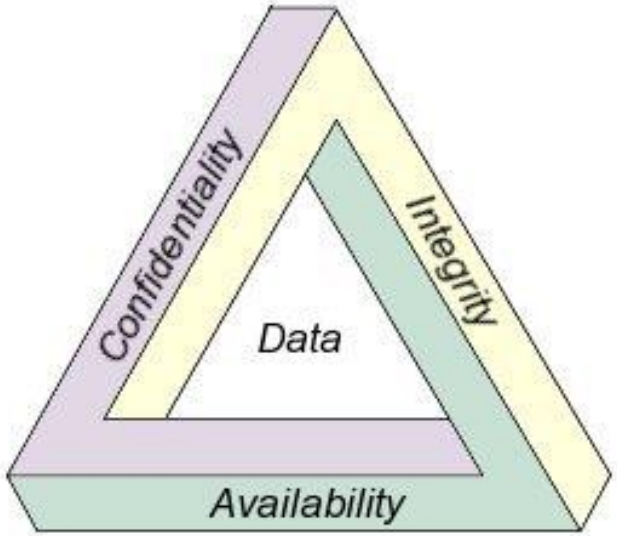
สแกนเอกสาร

ขั้นตอนการสแกนเอกสาร สอดคล้องตามประกาศ สธอ. เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

วิเคราะห์ภัยคุกคามไซเบอร์
และ กรณีศึกษาจากไทยเซิร์ต

การกระทำผิดทางคอมพิวเตอร์ - ต่อระบบ/ต่อข้อมูล

กำหนดมาตรการในการป้องกัน
และปราบปรามการกระทำ
ความผิดเกี่ยวกับคอมพิวเตอร์



การรักษาความลับ
(confidentiality)

การรักษา
ความครบถ้วน
(integrity)

การรักษาสภาพพร้อม
ใช้งาน (availability)

หลัก C.I.A.

รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

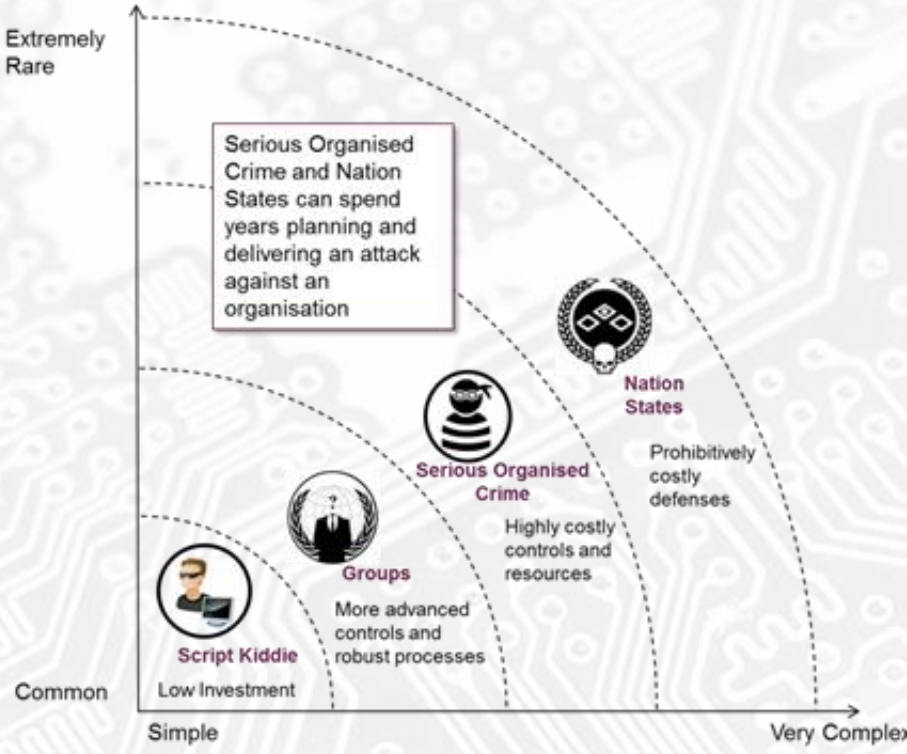
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)

C.I.A. = หลักการพื้นฐานของ Information Security และ Cybersecurity

19

รูปแบบภัยคุกคามและการกระทำผิดทางคอมพิวเตอร์

- ผู้กระทำความผิดอยู่ตรงไหนก็ได้ในโลก
- ความเสียหายกระทบถึงคนจำนวนมาก & รวดเร็ว
- ใช้เทคโนโลยีที่ซับซ้อนในการกระทำความผิด
- ยากต่อการตรวจพบร่องรอยการกระทำผิด
- ยากต่อการจับกุมและนำผู้กระทำผิดมาลงโทษ
- สามารถริเริ่มการกระทำความผิดครั้งใหม่ได้โดยรวดเร็ว



หลักการทำงานการสื่อสารบนเครือข่ายคอมพิวเตอร์

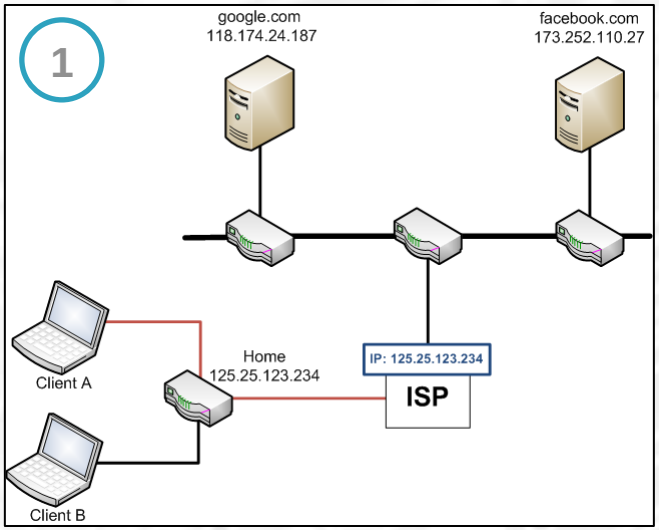
ผู้ให้บริการออนไลน์

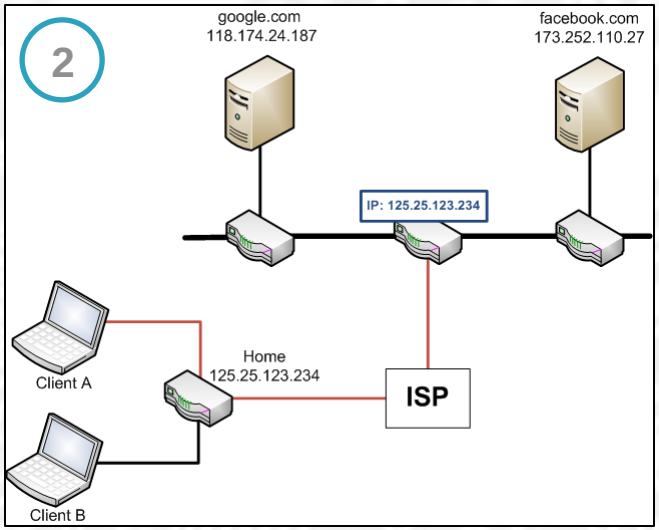
ผู้ให้บริการเครือข่าย

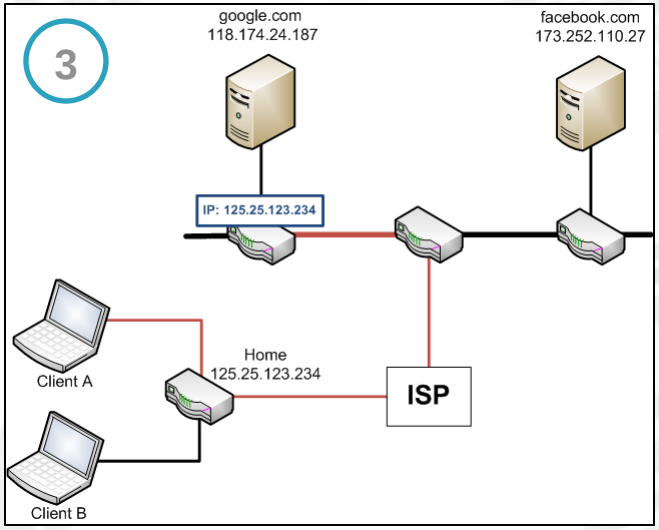
ผู้ใช้บริการ

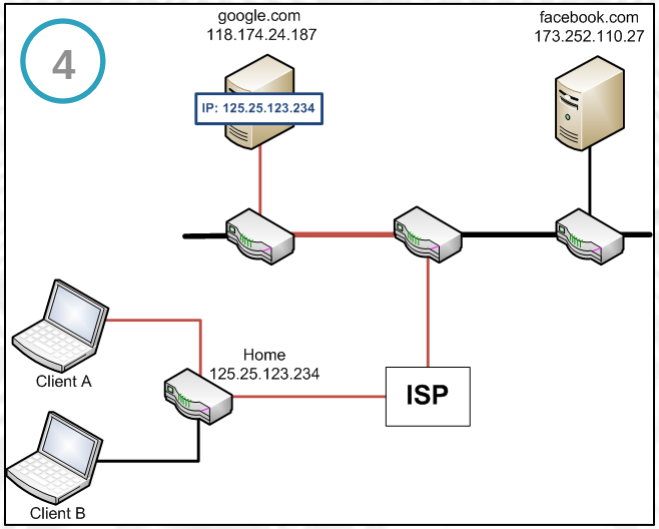
21

การสื่อสารในเครือข่ายอินเทอร์เน็ต ผ่าน ISP

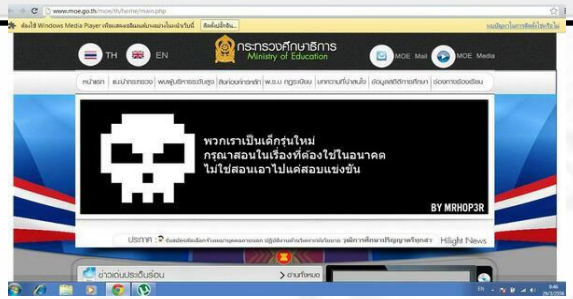








จะเกิดอะไรขึ้นถ้าสิ่งใดสิ่งหนึ่งทำงานผิดปกติ?



เซิร์ฟเวอร์ถูกแฮ็ก

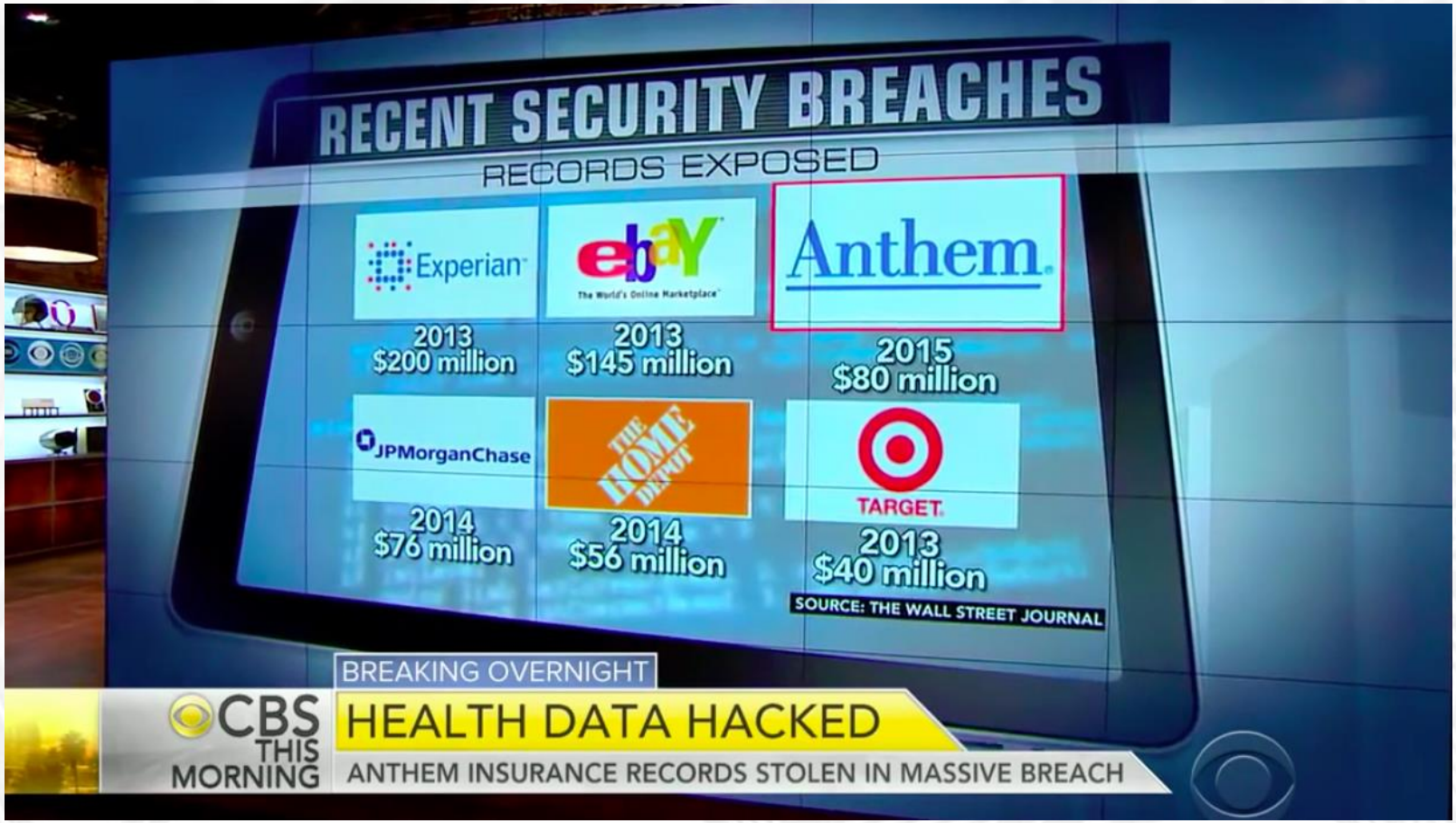
Defacement/Phishing

ถูกดักรับข้อมูลจากเครื่องข่าย

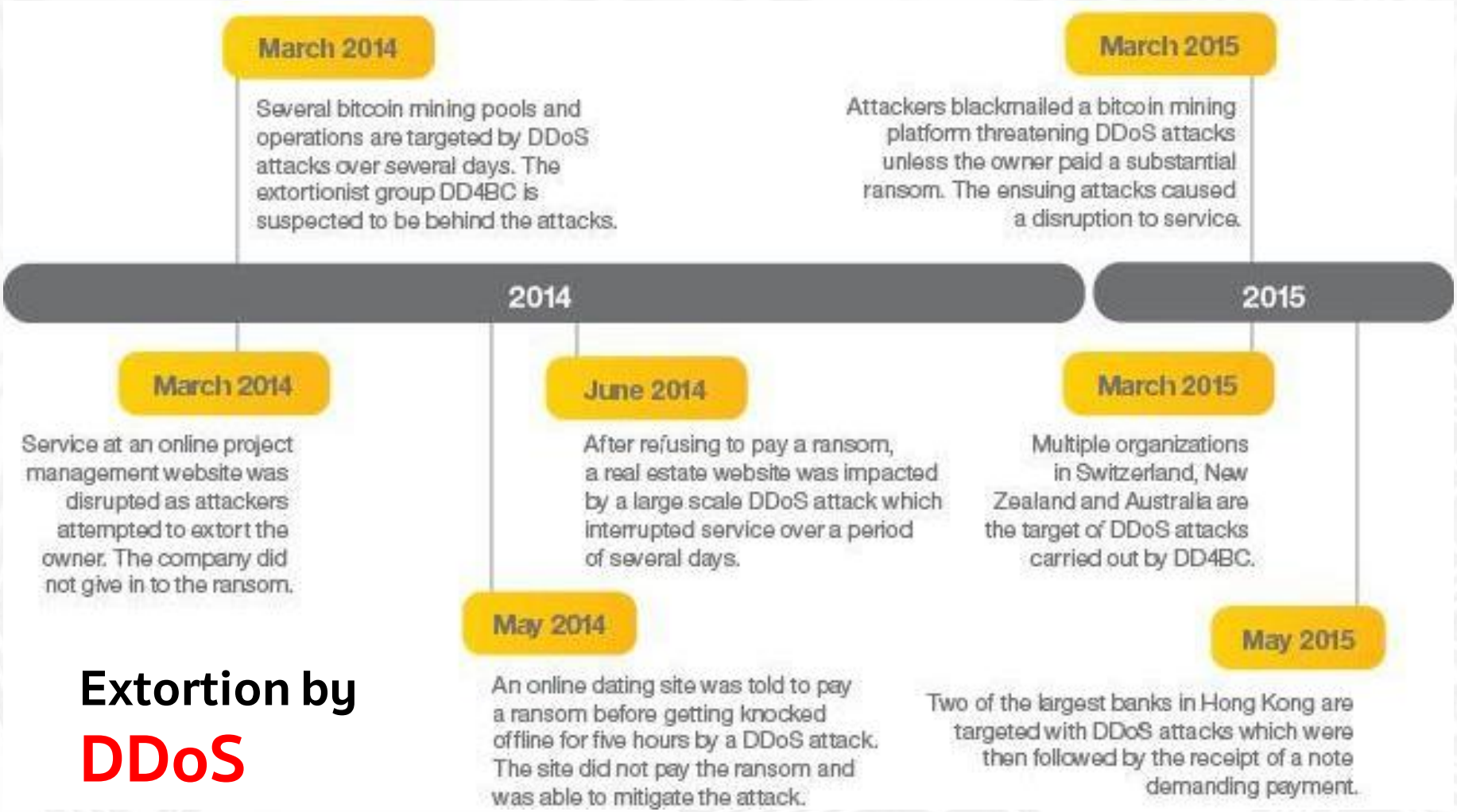
เครื่องถูกผู้ประสงค์ร้ายใช้เป็นเครื่องมือในการกระทำผิด

เครื่องติดมัลแวร์ขโมยข้อมูล

ความเสี่ยงของข้อมูลที่มาพร้อมกับเทคโนโลยี



ความเสี่ยงของบริการที่มาพร้อมกับเทคโนโลยี



Extortion by

DDoS

กรณีศึกษาจาก THAICERT – INTERNET FRAUD

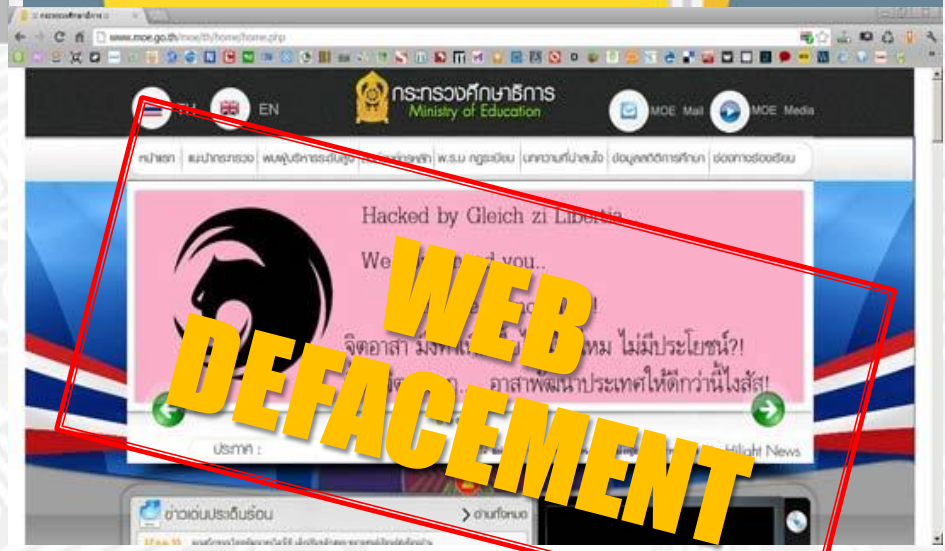
Phishing / Web defacement

From: "Kasikorn Bank Plc" <e-alert@kasinkornbank.com>
To: <[redacted].com>
Sent: 4 กุมภาพันธ์ 2553 1:25
Subject: New Security Message From Kasikorn Bank Plc

In the last fews weeks, our Online Banking Security
team has observed multiple logon attempts on your
internet banking account from different blacklisted IP's.
For your safety we have decided to suspend your access.
You will need to verify your identity by.

CLICK HERE TO VERIFY → กรุณาอย่าคลิกลิงค์ใด ๆที่อยู่ในอีเมล์หลอกลวงนี้

Customer Service
KASIKORNBANK Plc.



Internet Fraud – Phishing 2.0

Feb - Jun 2015

1

ผู้ร้ายเจาะระบบผู้อื่น
และสร้างหน้า
Phishing

2

ผู้ร้ายจดทะเบียนโดเมน
เนม ใกล้เคียงกับชื่อของ
สถาบันการเงิน

3

ผู้ร้ายลงโฆษณาหน้า
Phishing ผู้ให้บริการ
Search Engine

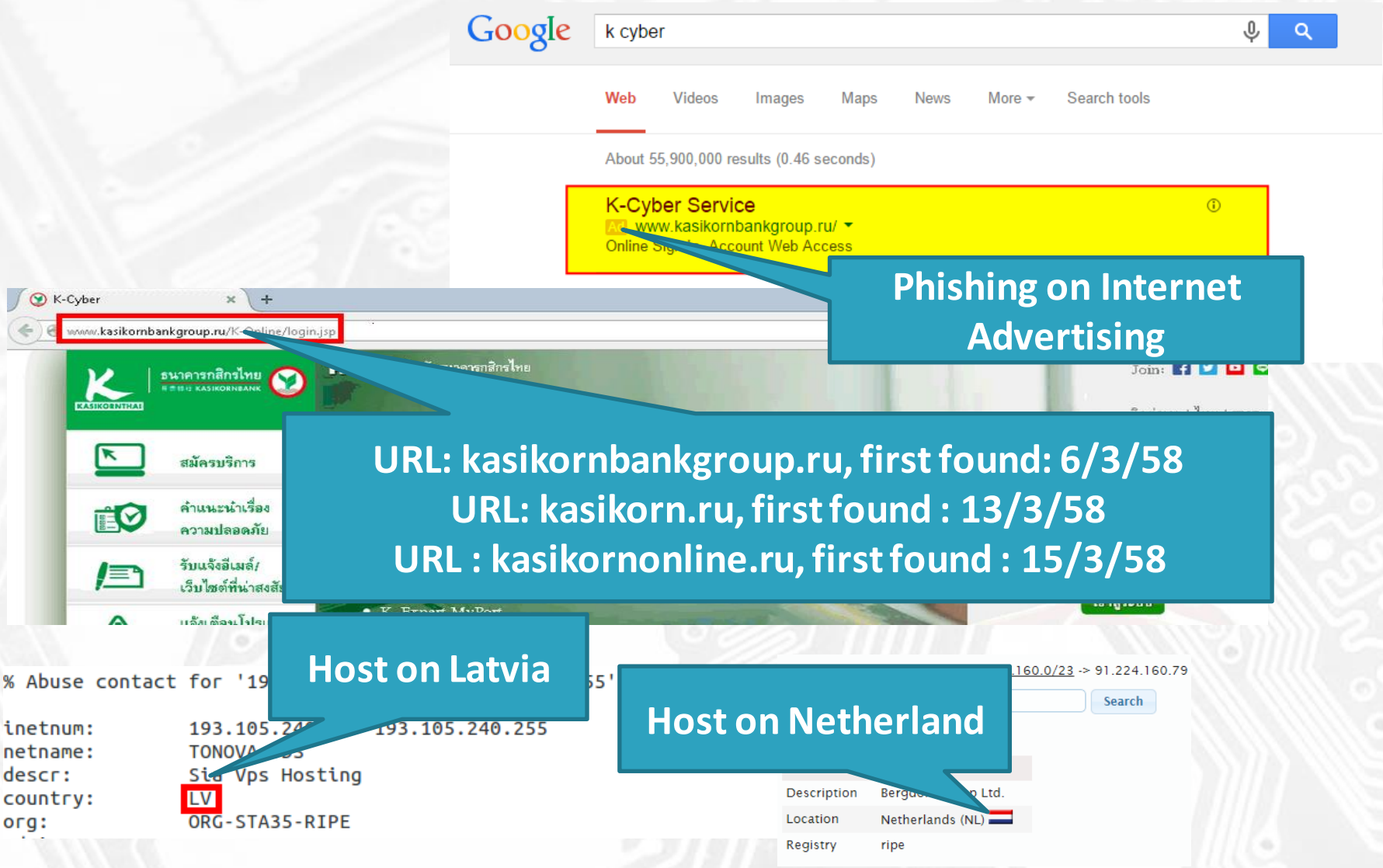
3

v.1 ผู้ร้ายส่งอีเมล Phishing
หลอกลวงลูกค้าของสถาบัน
การเงิน

4

ลูกค้าสถาบันการเงินหลงเชื่อ
และใส่ข้อมูล Username
และ รหัสผ่านในหน้า
Phishing

Phishing Case Study

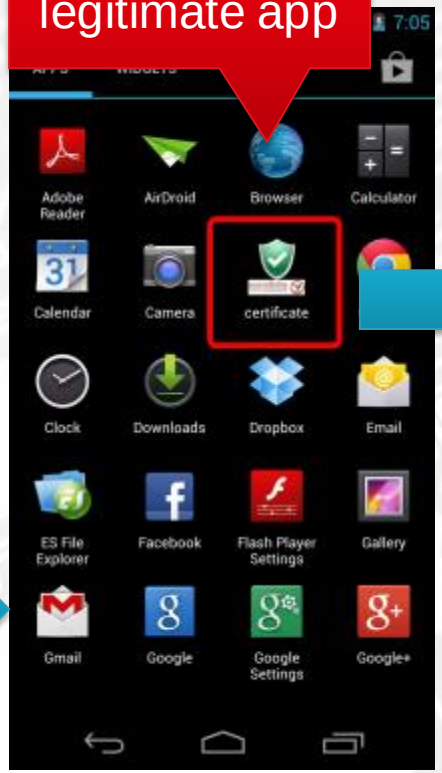


Malware stealing Bank OTP

Feb 2013

Downloaded outside Google Play

Shown as a legitimate app



Requires a password

Sends user's info via SMS to the attacker

```
Pass: xxx
OTP: yyy
```

A remote control Trojan for OTP Interception

เครื่องของเหยื่อตอบรับการควบคุม

เครื่องของเหยื่อส่งต่อ SMS ที่ได้รับไปให้กับผู้โจมตี

ผู้โจมตี ส่งคำสั่งเข้ามาควบคุมเครื่องของเหยื่อ

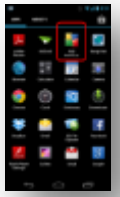
Watering Hole/Multi Stage & e-banking Trojan

May 2013

1 เหยื่อเปิดเว็บไซต์หนังสือพิมพ์ที่มีมัลแวร์

2 มัลแวร์ถูกติดตั้งบนเครื่องคอมพิวเตอร์เหยื่อโดยอัตโนมัติ

3 มัลแวร์ทำงานเมื่อเหยื่อเข้าใช้งาน e-banking โดยแฝงโฆษณาเรื่องการแจกโปรแกรม antivirus บนโทรศัพท์มือถือ



4 เหยื่อหลงเชื่อและติดตั้ง Antivirus ปลอมทำให้ถูกขโมย SMS ที่ใช้ในระบบ e-banking

3 ผู้ไม่หวังดีเข้าถึงระบบ e-banking เพื่อขโมยเงินออกจากบัญชีเหยื่อ

eBanking Fraud : eBanking Trojan

Jan 2014

เหยื่อถูกหลอกให้รันไฟล์มัลแวร์

1

2

มัลแวร์เชื่อมต่อและส่งข้อมูลกลับมายัง C&C (เครื่องของแฮกเกอร์) เช่น ข้อมูล Keylogger เป็นต้น

https://online.kasikorn[Enter] myUsername[Tab]myPassword [Enter]..

3

ผู้ไม่หวังดีแจ้งขอทำซิมเบอร์โทรศัพท์มือถือของเหยื่อใหม่

4

ผู้ไม่หวังดีเข้าสู่ระบบ e-Banking ด้วยบัญชีผู้ใชงานของเหยื่อโดย SMS ยืนยันการโอนเงินถูกส่งไปยังโทรศัพท์มือถือของแฮกเกอร์แทน

Android SMS Trojan แจ้ง.apk

Aug 2014

26 Aug - http://goo.gl/pbS3Tj
25 Aug - http://goo.gl/lNFLXN
23 Aug - http://goo.gl/AjT773
22 Aug - http://goo.gl/YzeUVx
21 Aug - http://goo.gl/q87XnM
13 Aug - http://goo.gl/WhVvXT
12 Aug - http://goo.gl/NPD8sd

Malware โจมตีผู้ใช้งาน Android แพร่กระจายทาง SMS ตัวอย่างข้อความ “ข้อความ “(ชื่อผู้ติดต่อในโทรศัพท์), แจ้งให้ทราบการจัดส่งของคุณ http://goo.gl/NPD8sd” และมีความสามารถในการขโมย OTP ของธนาคาร

การทำงานของมัลแวร์ แจ้ง.apk และ รับทราบ.apk

Dropbox

- i3d

- Global Layer

SMS &
Phone Book

1

ผู้ไม่หวังดีอัปโหลดแอป
พลิเคชันอันตรายไว้บน
บริการฝากไฟล์

3

ผู้ใช้หลงเชื่อและดาวน์โหลด
แอปพลิเคชันมาติดตั้งบน
โทรศัพท์มือถือ

Internet

4

แอปพลิเคชันจะแอบดัก SMS
และส่งข้อมูลไปยังเซิร์ฟเวอร์
ของผู้ไม่หวังดี

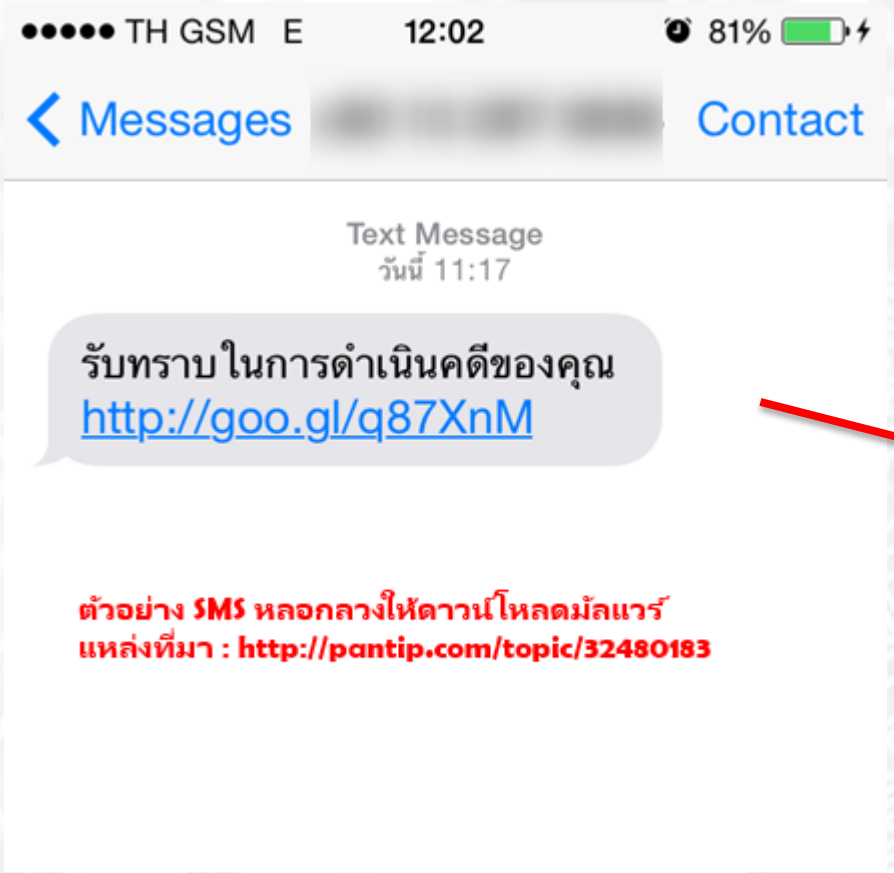
http://goo.gl/xyz

SMS

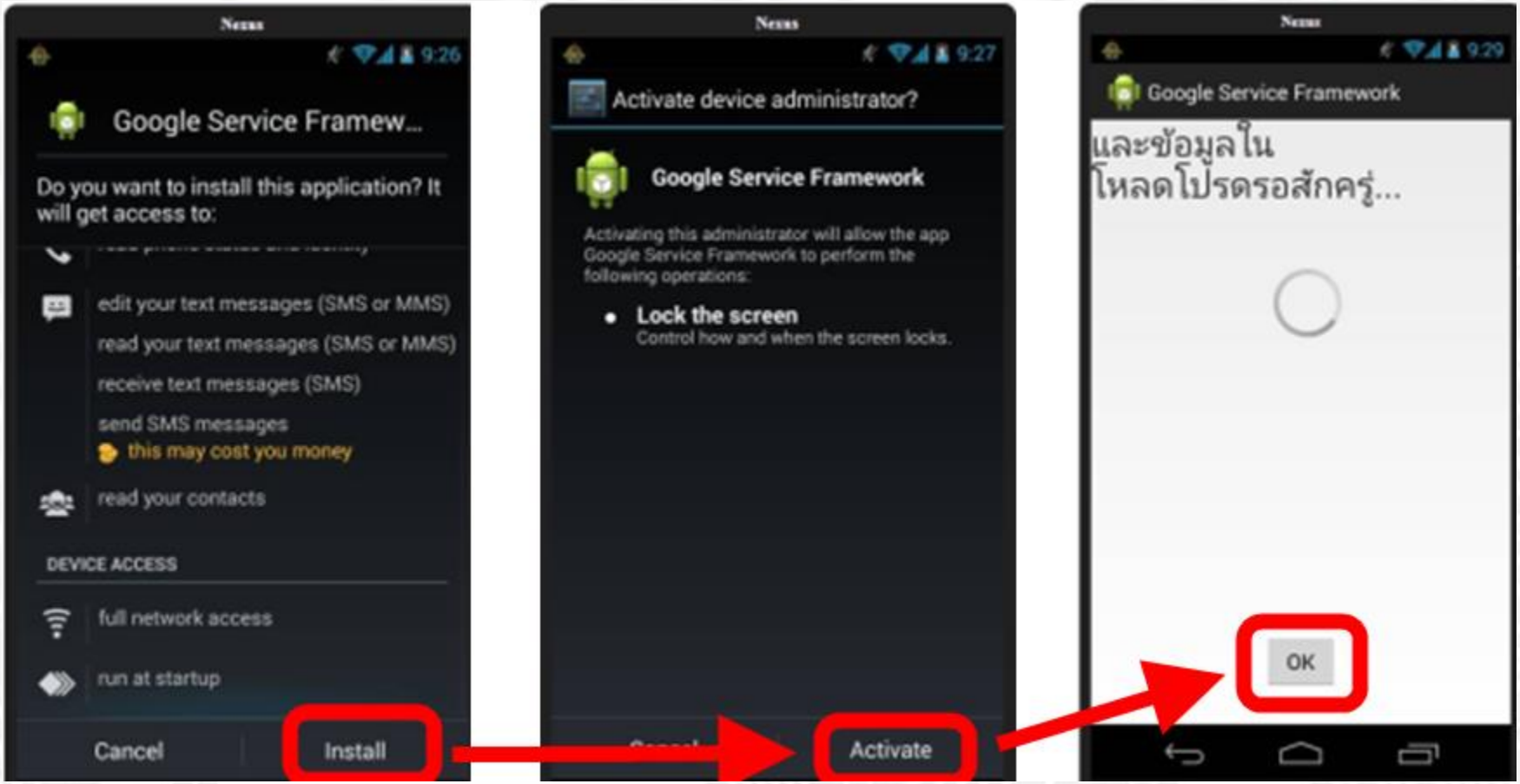
2

ผู้ไม่หวังดีส่ง SMS พร้อมกับแนบ
URL ที่ให้ดาวน์โหลดแอปพลิเคชัน
ดังกล่าวไปยังผู้ใช้

ตัวอย่าง SMS หลอกลวงที่ผู้ใช้ได้รับ



ตัวอย่างจำลองการติดตั้งมัลแวร์ของผู้ใช้



แฮกเร้าเตอร์ เพื่อขโมยข้อมูลและฝังมัลแวร์

1

เหยื่อใช้งานอินเทอร์เน็ตที่บ้าน และมีการเปิดเว็บไซต์ธนาคารออนไลน์

เว็บไซต์ธนาคารออนไลน์จริง

Legitimate DNS

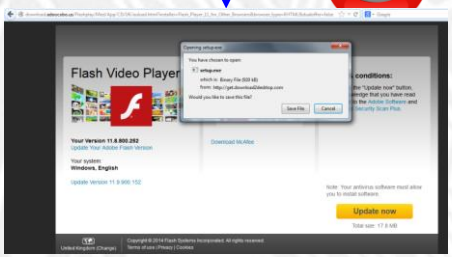
3

เหยื่อเชื่อมต่อไปยัง DNS server ของแฮกเกอร์

Illegitimate DNS

เหยื่อถูก Redirect ไปยังเว็บไซต์ปลอม ซึ่งมีการหลอกให้ติดตั้งโปรแกรมปลอม (มัลแวร์)

4

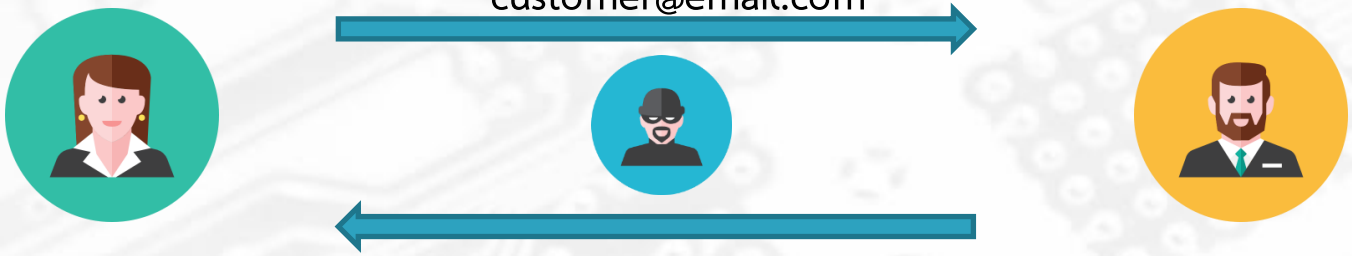


2

ผู้ไม่หวังดีโจมตีช่องโหว่ของเร้าเตอร์ เพื่อเข้าควบคุมการทำงานของอุปกรณ์ โดยมีการเปลี่ยนการตั้งค่า DNS server ให้ชี้ไปยังเครือข่ายของแฮกเกอร์แทน

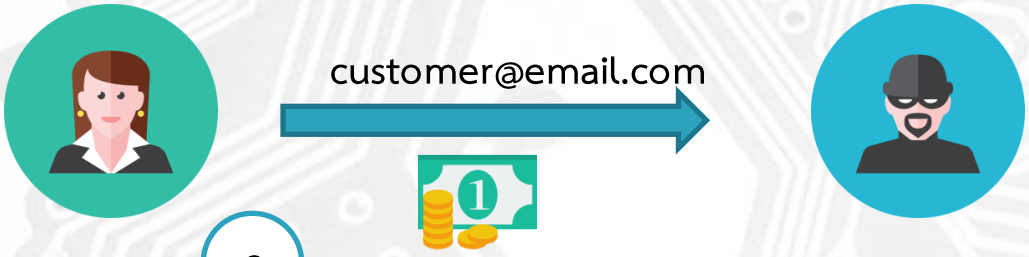
Jan 2015

กรณี อีเมลปลอมหลอกให้โอนเงินกับ SME ไทย



1 ผู้ซื้อกับผู้ขายพูดคุยซื้อขายสินค้ากันในอีเมล โจรสามารถดักอ่านการสนทนาของทั้งสองฝ่ายได้

2 ในขณะที่กำลังจะตกลงซื้อขาย โจรปลอมอีเมลหลอกทั้งสองฝ่าย แล้วบอกผู้ซื้อให้โอนเงินมาที่บัญชีธนาคารของโจร



3 ผู้ซื้อหลงเชื่อและโอนเงินเข้าบัญชีธนาคารของโจร

2014 - 2015

การโจมตีผู้ใช้งานด้วยมัลแวร์เรียกค่าไถ่ (Ransomware)

1

ผู้ไม่หวังดีแฮกเว็บไซต์แล้วฝังมัลแวร์ที่จะใช้เผยแพร่ หรือใช้วิธีส่งอีเมลที่มีไฟล์แนบเป็นมัลแวร์ไปยังผู้ใช้

6

ผู้ใช้ยอมชำระเงินให้กับผู้ไม่หวังดี โดยอาจจ่ายเป็นสกุลเงินจริงหรือเงินเสมือน เช่น Bitcoin ขึ้นอยู่กับเงื่อนไขของมัลแวร์แต่ละตัว

2

ผู้ใช้เข้าชมเว็บไซต์ที่มีมัลแวร์ฝังอยู่ หรือเปิดไฟล์แนบในอีเมลที่เป็นมัลแวร์

5

มัลแวร์แสดงข้อความบนหน้าจอ ข่มขู่หรือหลอกลวงให้ผู้ใช้ชำระเงินเพื่อให้มาซึ่งวิธีการในการถอดรหัสลับไฟล์เอกสาร

3

มัลแวร์ถูกดาวน์โหลดและติดตั้งลงในคอมพิวเตอร์ของผู้ใช้

4

มัลแวร์เข้าควบคุมคอมพิวเตอร์ และเข้ารหัสลับไฟล์เอกสาร เช่น .doc .xls .jpg ฯลฯ ทำให้ผู้ใช้ไม่สามารถใช้งานไฟล์เหล่านั้นได้

2014-2015

การข่มขู่จะโจมตีธนาคารด้วยวิธีการ DDoS

ต.ค.58 ธนาคารพาณิชย์ 5 แห่ง ได้รับเมลข่มขู่จากกลุ่มแฮกเกอร์ Armada Collective ว่าจะโจมตีบริการของธนาคารด้วยวิธีการแบบ DDoS ในวันที่ 25 ต.ค. 58 หากไม่จ่ายเงินจำนวน 50 Bitcoin หรือประมาณ 16,519.50 เหรียญสหรัฐ

ต.ค.58 ไทยเซิร์ต สพธอ. แจ้งมาตรการรับมือการโจมตีแบบ DDoS และได้เริ่มประสานงานให้เครื่องที่เป็นต้นกำเนิดการโจมตียุติการโจมตี (Take Down)

ต.ค.58 ไทยเซิร์ต สพธอ. ประสานผู้ให้บริการ email ในประเทศสหพันธ์สาธารณรัฐเยอรมัน พร้อมกับประสานงานกับหน่วยงานในเครือข่ายความร่วมมือ CERT ในการขอข้อมูลเกี่ยวกับผู้ใช้ชื่ออีเมล armadacollective@?.de เพื่อสืบหาผู้กระทำความผิด

พ.ย. 58 ไทยเซิร์ต สพธอ. ประสานกับผู้ให้บริการอินเทอร์เน็ตในประเทศไทยเพื่อขอความร่วมมือในการแจ้งเหตุสถานการณ์ DDoS ที่อาจเกิดขึ้นมายังไทยเซิร์ต สพธอ. เพื่อใช้ในข้อมูลในการประสานแก้ไขปัญหา

คำอธิบายศัพท์

DDoS (Distributed Denial of Service) การโจมตีระบบไอทีรูปแบบหนึ่งที่มุ่งหวังให้เกิดผลกระทบต่อสภาพความพร้อมใช้งานของระบบ โดยอาศัยการโจมตีจากหลายแหล่ง

Bitcoin เป็นข้อมูลอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือบริการทางอินเทอร์เน็ต โดยมูลค่าขึ้นอยู่กับอุปสงค์และอุปทาน และมีช่องทางแลกเปลี่ยนเป็นเงินสดได้ ออกแบบมาเพื่อสนับสนุนการทำธุรกรรมแบบนิรนาม ณ วันที่ 2 พ.ย. 58 1 Bitcoin = USD 330.39 http://www.coindesk.com/price/

การบริหารจัดการภัยคุกคามไซเบอร์

New Landscape - New Challenges

Last 10 years, see the growth of encrypted traffics (by service providers and malware) More malwares are using PDF as a container

- Internet of Things is coming to your organization
  - Things are about you as a consumer and sensors
  - Compute Power (Cloud)
  - Network Connectivity (Internet, LTE, WIFI)
  - Proximity Communication (NFC, Bluetooth)
- Implication
  - Hard to define your enterprise network perimeter
  - Patch management is impossible (things use too many Oses and Apps)
  - Goal of Security shifts from damage containment to minimize adverse impact
  - Require timely detection and response

The Inconvenient Truth

Protection is Ideal

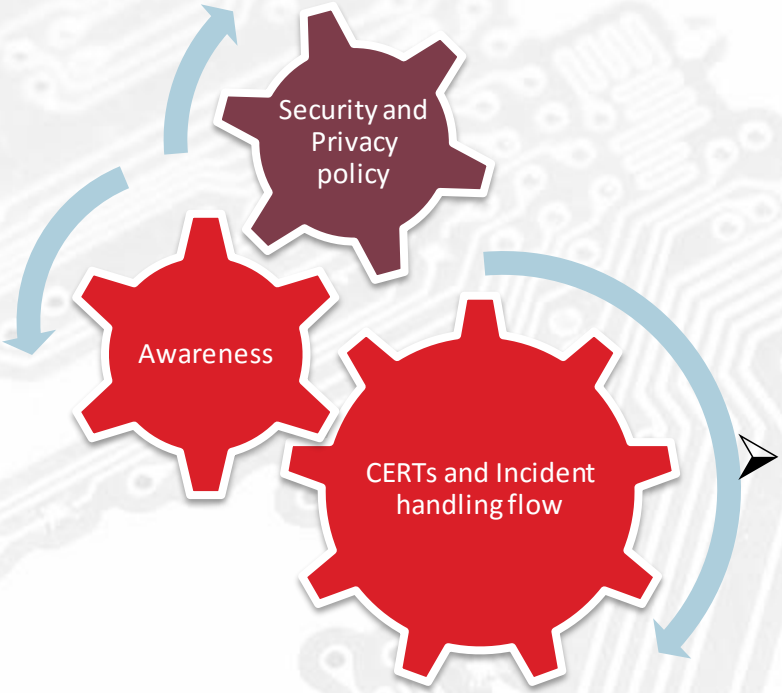
But

Detection is a Must

If you have **not detected an attack**/compromise in the last 6 month, it is not because it is not happening – it is because you are **not looking in the right areas**

Approaches to cope with Cyber Threats

- Encourage public and private organizations to have security and privacy policies that are in line with international standards and best practices



- Raise awareness to ensure that individuals are equipped with sufficient knowledge and skills to protect themselves against cyber attacks.

- Bring together CERTs to create the incident handling flow, allows cybersecurity incident to be handle effectively.

ไทยเซิร์ต : Thailand Computer Emergency Response Team

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

"to improve the nation's cybersecurity"

1) 24x7 operations center

2) Worldwide Collaboration & Coordination

3) ยกระดับการปกป้อง Critical Information Infrastructure

ตัวอย่างงานบริการ ไทยเซิร์ต

- การเฝ้าระวังภัยคุกคามไซเบอร์กับระบบสารสนเทศภาครัฐ
- การวิเคราะห์ภัยคุกคามของไทยเซิร์ต
- ระบบ Cyberthreat Information Sharing
- จัดอบรมและสอบ, เตรียมความพร้อม บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
- การสร้าง awareness ทั้ง online-offline

TF-CSIRT Trusted Introducer

Accredited CSIRT

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

ThaiCERT
Thailand Computer Emergency Response Team

Accredited
since 01 Oct 2015

Fields describing the team

Team Details

Official Name	Short Name	Country
Thailand Computer Emergency Response Team	ThaiCERT	Thailand

Established	Host Organisation
01 Oct 2000	ETDA (Electronic Transactions Development Agency), a public organization under supervision by the Ministry of Information and Communication Technology

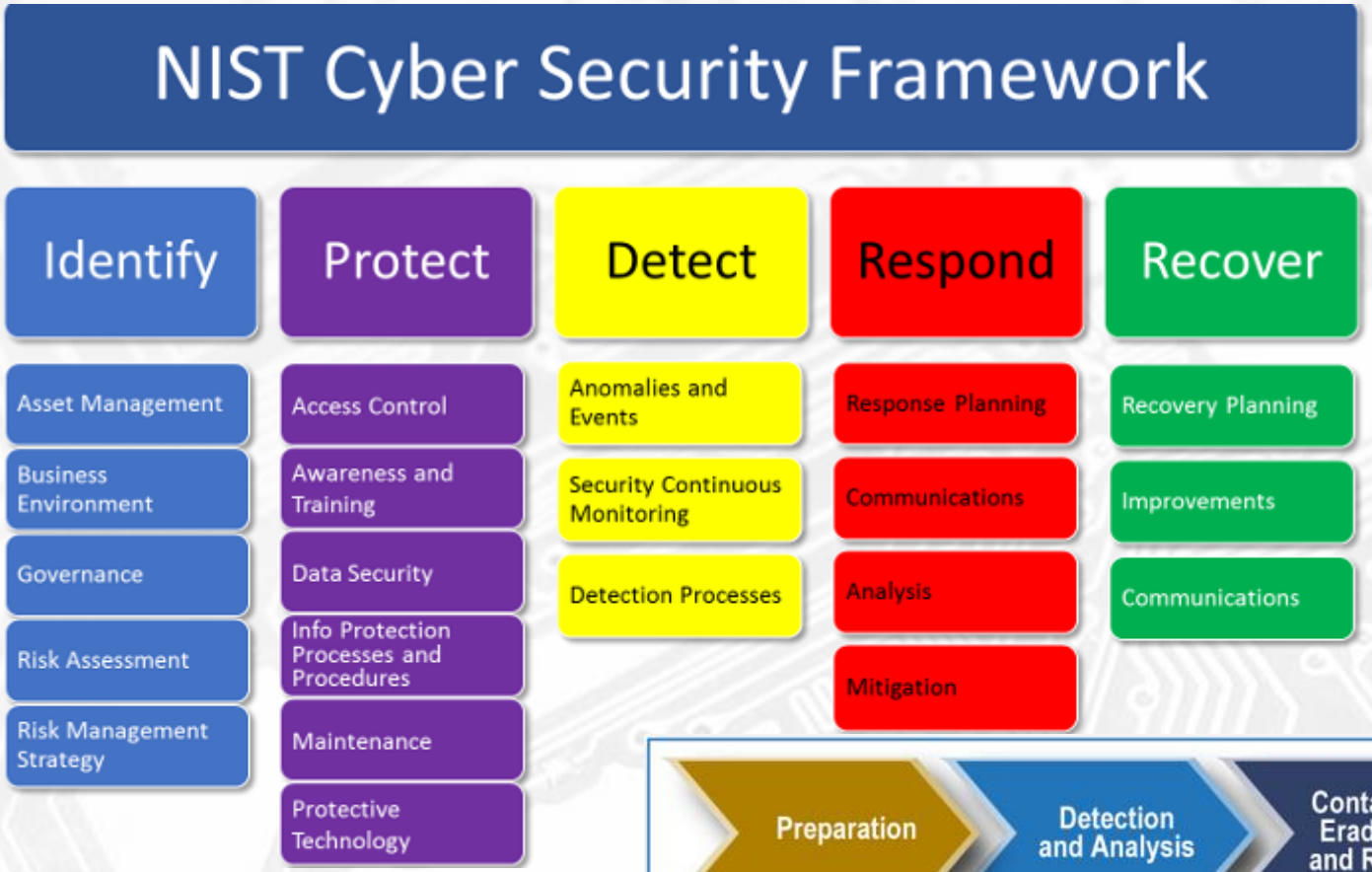
Constituency

Constituency Type	Country of Constituency
Government, National	Thailand

ASNs, Domains, IP ranges	Description
- *.th -	All of Thailand (.th)

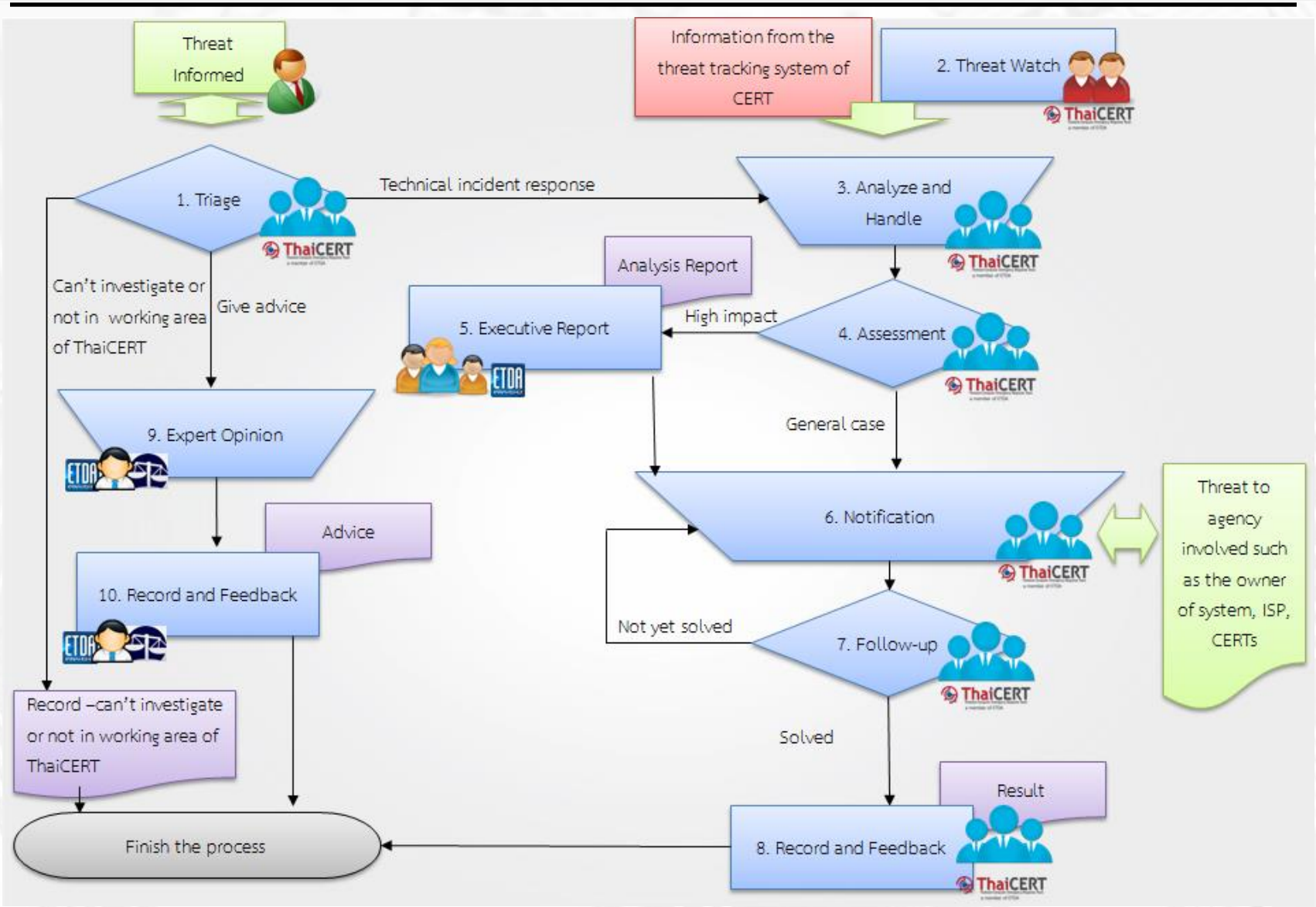
Coordinate with >370 CERTs

กรอบการบริหารจัดการ Cybersecurity และขั้นตอนการรับมือภัยคุกคาม

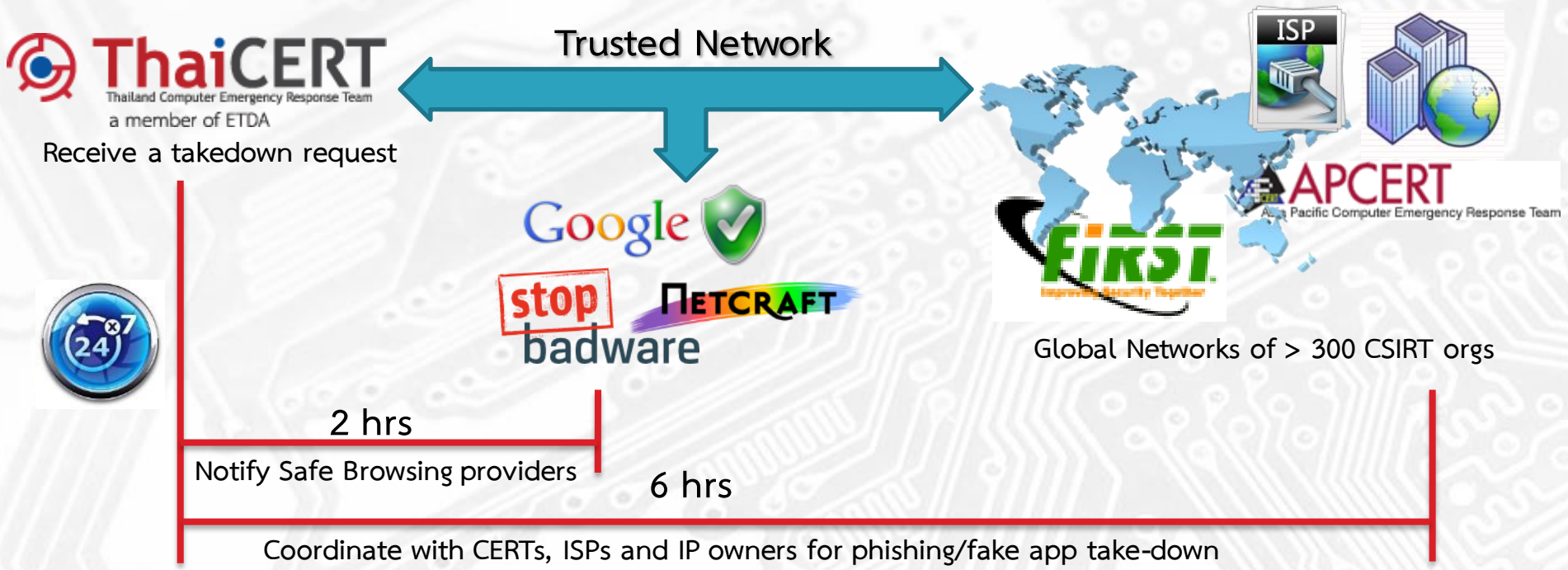


*Similar framework can be found in ISO/IEC 27000s, ISACA IT Governance, SANS Critical Controls and other international standards

ขั้นตอนปฏิบัติในการรับมือภัยคุกคาม Incident Response



Incident Handling: Phishing website/ Fake App takedown



In 2013, ThaiCERT took down 694 phishing websites
with the takedown time (average 31:23 hours, median 9:48 hours)*

*Global Phishing Survey: Trends and Domain Name Use 2H2013

Artifact Handling: Digital Forensics & Malware Analysis

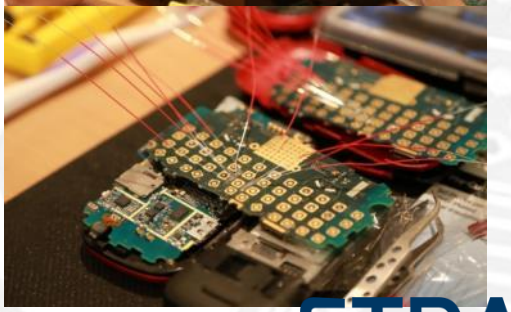
- Analyzes digital evidences to uncover fraud and data-stealing malware activities.
- Provides assistance on case filing to LEA to prepare the court admissible digital evidences.

Computer & media Forensic

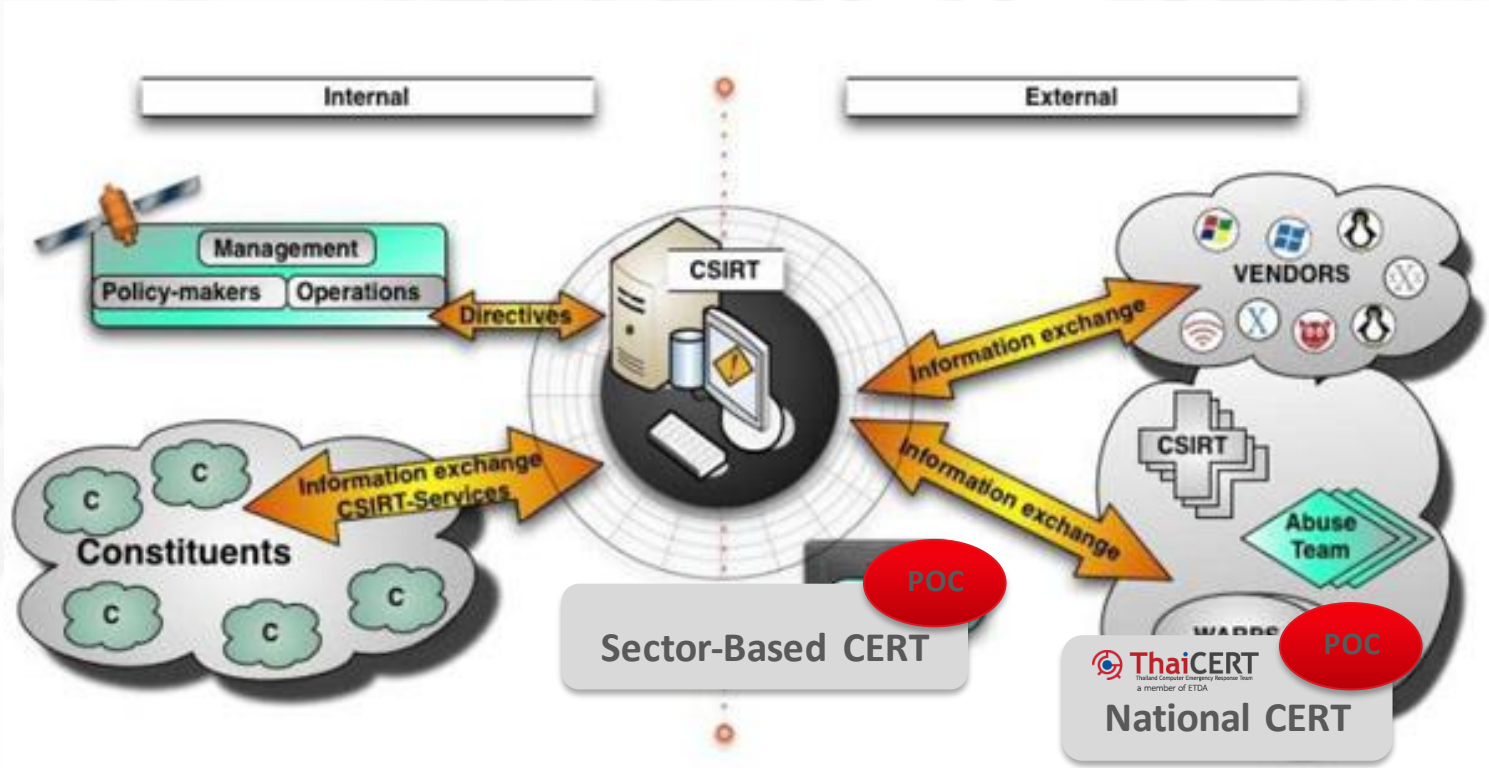
Clean Room

Mobile Forensic

Malware Analysis



SECTOR-BASED CERT เพื่อพร้อมรับมือภัยคุกคามไซเบอร์



ความสัมพันธ์กับหน่วยงานภายใน

- หน่วยงาน CERT ดำเนินการภายใต้ขอบเขตและนโยบายจากฝ่ายบริหารของหน่วยงาน
- ให้บริการและแลกเปลี่ยนข้อมูลภัยคุกคามกับหน่วยงานภายใต้ขอบเขตดำเนินการ (Constituents)

ความสัมพันธ์กับหน่วยงานภายนอก

- มอบหมาย POC ในการประสานงาน
- เป็นศูนย์กลางของการแลกเปลี่ยนข้อมูลภัยคุกคามกับผู้ค้าและหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ (National CERT)

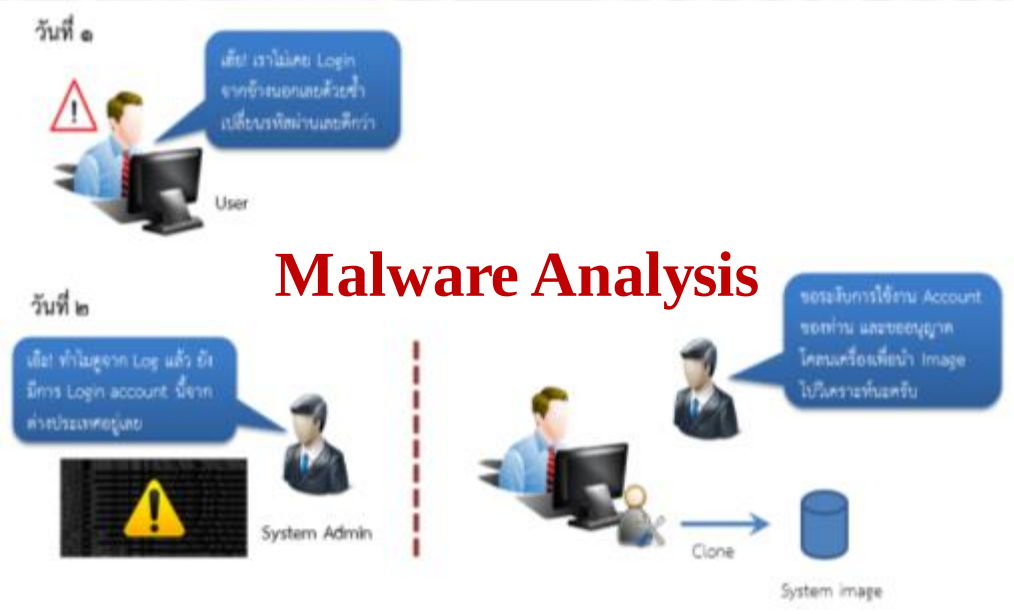
Ref: Basic set of good practice on how to successfully run a Computer Security and Incident Response team (CSIRT), ENISA

52

ซ้อมรับมือภัยคุกคามไซเบอร์

Objectives:

- Create cybersecurity awareness within the banking sector in Thailand
- Practice incident handling coordination between the banks and CERTs
- Assess advanced technical skills such as malware analysis



"To enhance the communication and participating teams' incident response capabilities and cooperation between teams"

จัดอบรมและสอบบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

หลักสูตร "การฝึกอบรมและสอบวัดสมรรถนะเพื่อพัฒนามาตรฐานการรับรองบุคลากรด้านความมั่นคงปลอดภัยระบบสารสนเทศของประเทศไทย" ครั้งที่ 3 จัดขึ้นระหว่างวันที่ 20-23 มกราคม พ.ศ. 2558 ณ ห้อง Open Forum ของ ETDA ชั้น 21 อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (หลังเซ็นทรัลพระราม 9) โดยผู้เข้าอบรมนั้นมาจากหน่วยงานราชการ ทหาร รัฐวิสาหกิจ สถาบันการศึกษา สถานพยาบาล บริษัทเอกชน และธนาคาร รวมทั้งสิ้น 58 คน ซึ่งการสอบวัดสมรรถนะและการรับรองคุณวุฒิผู้เชี่ยวชาญแบ่งเป็น 2 กลุ่ม คือ

- iSEC-M (Information Security Expert Certification–Management) : ผู้เชี่ยวชาญความมั่นคงปลอดภัยระบบสารสนเทศ (ด้านบริหารจัดการ) จำนวน 28 คน
- iSEC-T (Information Security Expert Certification-Technical) : ผู้เชี่ยวชาญความมั่นคงปลอดภัยระบบสารสนเทศ (ด้านเทคนิค) จำนวน 30 คน

USER is the weakest link

หยุด!! คิด!! ก่อนคลิกลิงก์ หรือเปิดไฟล์แนบในอีเมล
ถ้าไม่อยากตกเป็นเหยื่อภัยทางไซเบอร์

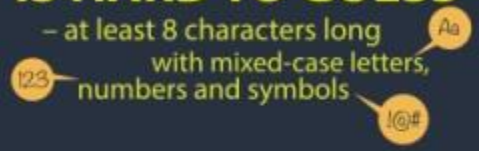
SECURITY AWARENESS

DON'T

Make sure that your

PASSWORD IS HARD TO GUESS

– at least 8 characters long with mixed-case letters, numbers and symbols



PASSWORD MUST BE CHANGED

at least **every 3 months** for important systems, and **every 6 months** for others

DO NOT REVEAL YOUR PASSWORD

with anyone.

DO NOT WRITE YOUR PASSWORDS DOWN

and leave them lying around.

DO NOT ENABLE

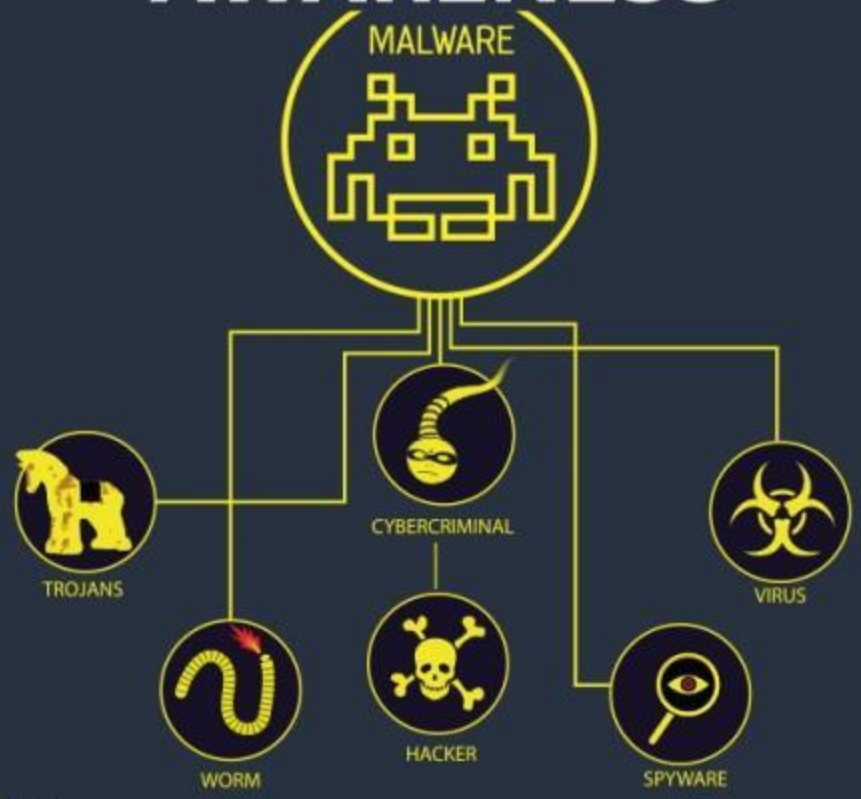
THE 'REMEMBER PASSWORD' option if prompted

DO NOT USE THE SAME PASSWORD FOR WORK AND PERSONAL ACTIVITIES

www.thaicert.or.th
twitter.com/thaicert

ThaiCERT ETDA ICT

MOBILE MALWARE AWARENESS



Ensure that all of your
SOFTWARE IS UP TO DATE

Do use
ANTI-VIRUS SOFTWARE
and update
them all regularly.

DO NOT INSTALL
ANY UNKNOWN APPS
or apps from untrusted sources.

www.thaicert.or.th
twitter.com/thaicert

ThaiCERT ETDA ICT

THANK YOU

www.etda.or.th

www.thaicert.or.th