Cyber Security Awareness Seminar

Dr. Yin Minn Pa Pa
2017/12/29
YCDC, Myanmar

Introduction

Dr. Yin Minn Pa Pa

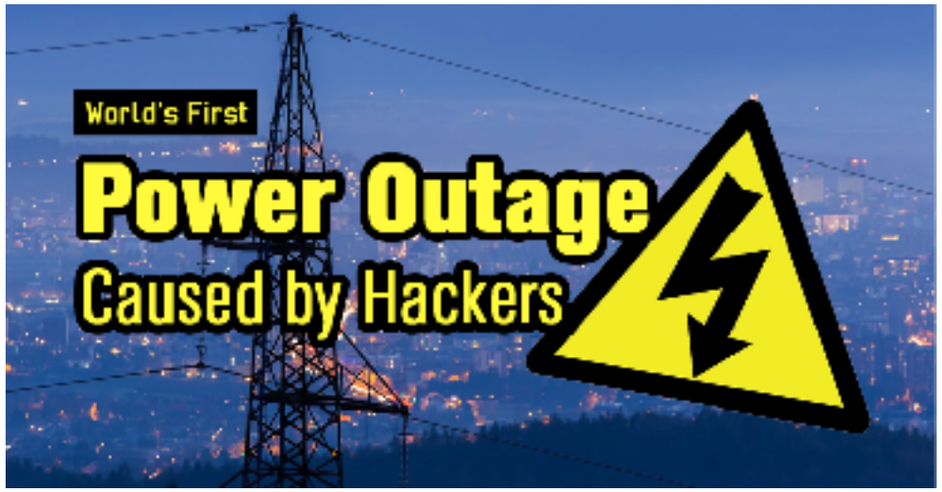
Security Researcher, PwC Cyber Services

PwC, Japan

Website: www.yinminnpapa.com

Why do they HACK?

Financial Value



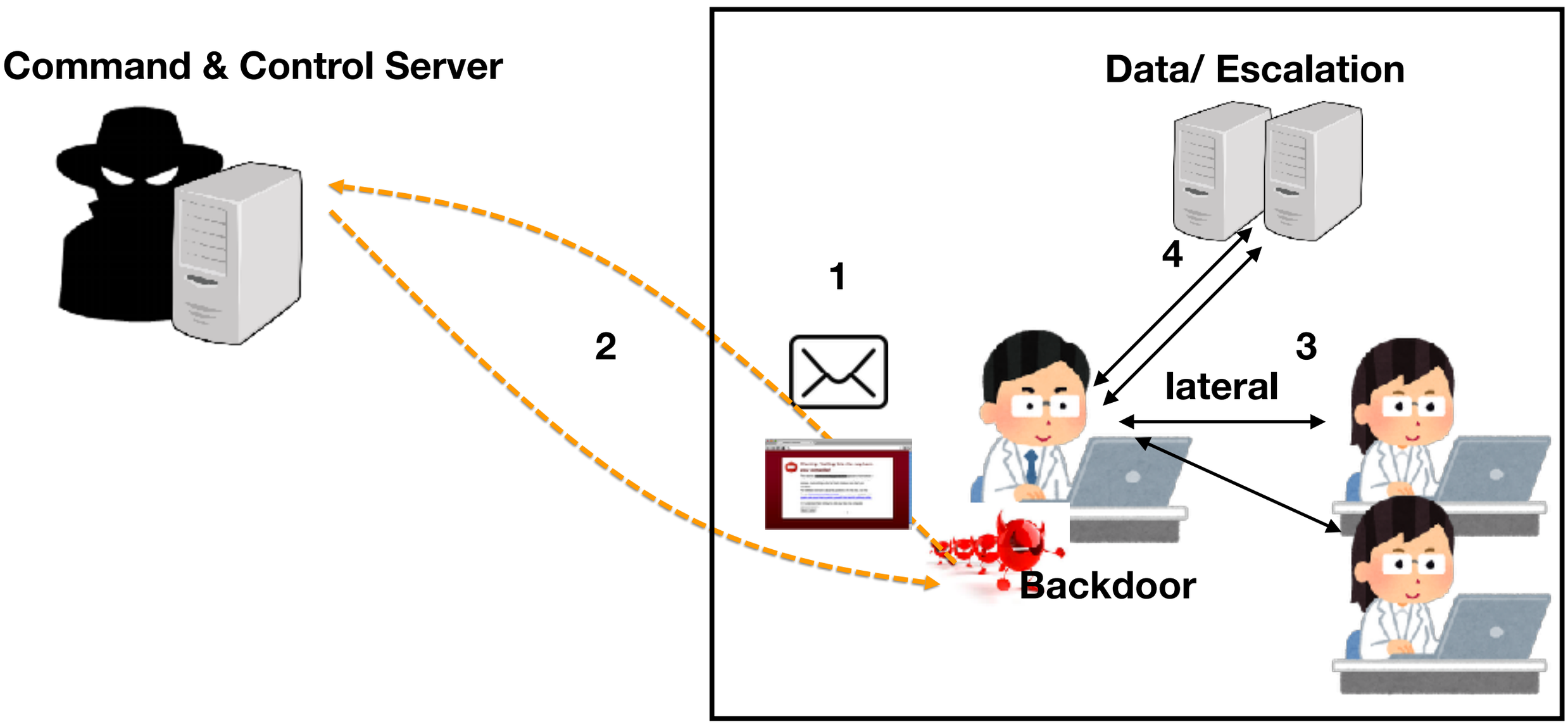
Political Value

Contents

- Attacks
  - Targeted Attacks
  - IoT Attacks
  - Ransomware
  - Wireless Attacks
  - Web Attacks
- Defenses
  - Minimum Defense Mechanism
  - CIS controls

Targeted Attacks

Targeted Attacks



Notable targeted attack groups

Sandworm

est. 2014

Possible region of origin: Russia

Aliases / *Quedagh, BE2 APT*

Tools, tactics, & procedures (TTP)
Spearphishing, vulnerabilities, zero-days, custom backdoor programs, destructive payloads

Motives
Espionage, sabotage

Target categories & regions
Governments, international organizations, energy, Europe, US

Recent activities
Linked to destructive attacks against Ukrainian media and energy targets

Housefly

est. 2001

Possible region of origin: US

Aliases / *Equation*

Tools, tactics, & procedures (TTP)
Watering holes, infected CD-ROMs, infected USB keys, vulnerabilities, zero-days, custom back door and information-stealing programs, worm programs

Motives
Espionage

Target categories & regions
Targets of interest to nation-state attackers

Recent activities
Breached in 2016, with tools and exploits leaked

Fritillary

est. 2010

Possible region of origin: Russia

Aliases / *Cozy Bear, Office Monkeys, EuroAPT, Cozyduke, APT29*

Tools, tactics, & procedures (TTP)
Spearphishing, custom back door programs

Motives
Espionage, subversion

Target categories & regions
Governments, think tanks, media, Europe, US

Recent activities
Associated with Democratic National Committee (DNC) attacks

Strider

est. 2011

Possible region of origin: Western

Aliases / *Remsec*

Tools, tactics, & procedures (TTP)
Advanced surveillance tool

Motives
Espionage

Target categories & regions
Embassies, airlines, Russia, China, Sweden, Belgium

Recent activities
Uncovered by Symantec in 2016

Swallowtail

est. 2007

Possible region of origin: Russia

Aliases / *Fancy Bear, APT28, Tsar Team, Sednit*

Tools, tactics, & procedures (TTP)
Spearphishing, watering holes, infected storage devices, vulnerabilities, zero-days, custom back door and information-stealing programs

Motives
Espionage, subversion

Target categories & regions
Governments, Europe, US

Recent activities
Associated with WADA and DNC hacks

Suckfly

est. 2014

Possible region of origin: China

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs signed using stolen certificates

Motives
Espionage

Target categories & regions
E-commerce, governments, technology, healthcare, financial, shipping

Recent activities
Targeted attacks using multipe stolen code-signing certificates

Cadelle

est. 2012

Possible region of origin: Iran

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs

Motives
Espionage

Target categories & regions
Airlines, telecommunications, Iranian citizens, governments, NGOs

Recent activities
Surveillance on domestic targets in Iran and orgs in the Middle East

Buckeye

est. 2009

Possible region of origin: China

Aliases / *APT3, UPS, Gothic Panda, TG-0110*

Tools, tactics, & procedures (TTP)
Spear phishing, zero-days, custom back door programs

Motives
Espionage

Target categories & regions
Military, defense industry, media, education, US, UK, Hong Kong

Recent activities
Shifted focus from Western targets to Hong Kong

Appleworm

est. 2012

Possible region of origin: North Korea

Aliases / *Lazarus*

Tools, tactics, & procedures (TTP)
Spear phishing, DDoS attacks, disk wiping, zero-days, custom back door and information-stealing programs, destructive payloads

Motives
Espionage, sabotage, subversion

Target categories & regions
Financial, military, governments, entertainment, electronics

Recent activities
Subject to disruption operations in early 2016. Links with Bangladesh Bank attackers

Tick

est. 2006

Possible region of origin: China

Aliases / *None*

Tools, tactics, & procedures (TTP)
Spear phishing, watering holes, custom back door programs

Motives
Espionage

Target categories & regions
Technology, broadcasting, aquatic engineering, Japan

Recent activities
Long-standing campaigns against targets in Japan

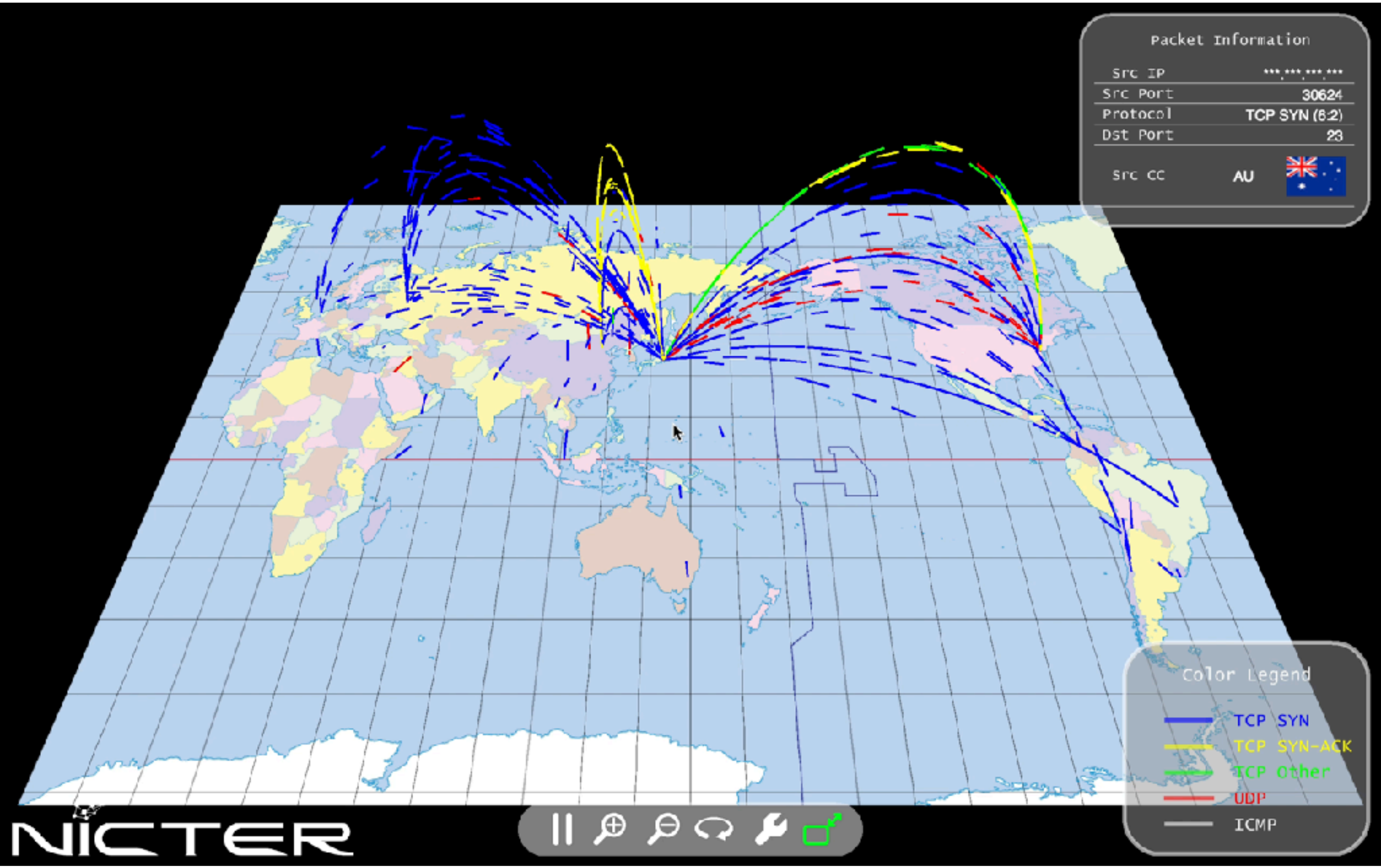
Ref: symantec ISTR

Best Practices

- People
  - Never click attachments of unknown mail
  - Never access unknown website
  - Never use usb (or) check before use
  - Use strong passwords / regularly update passwords
  - Never Share what is unknown
    Never believe what is not sure
  - Training
- Technology
  - Network
    - Firewall and gateway antivirus
    - IPS/ IDS
    - End point security
- Process
  - Incident response manual

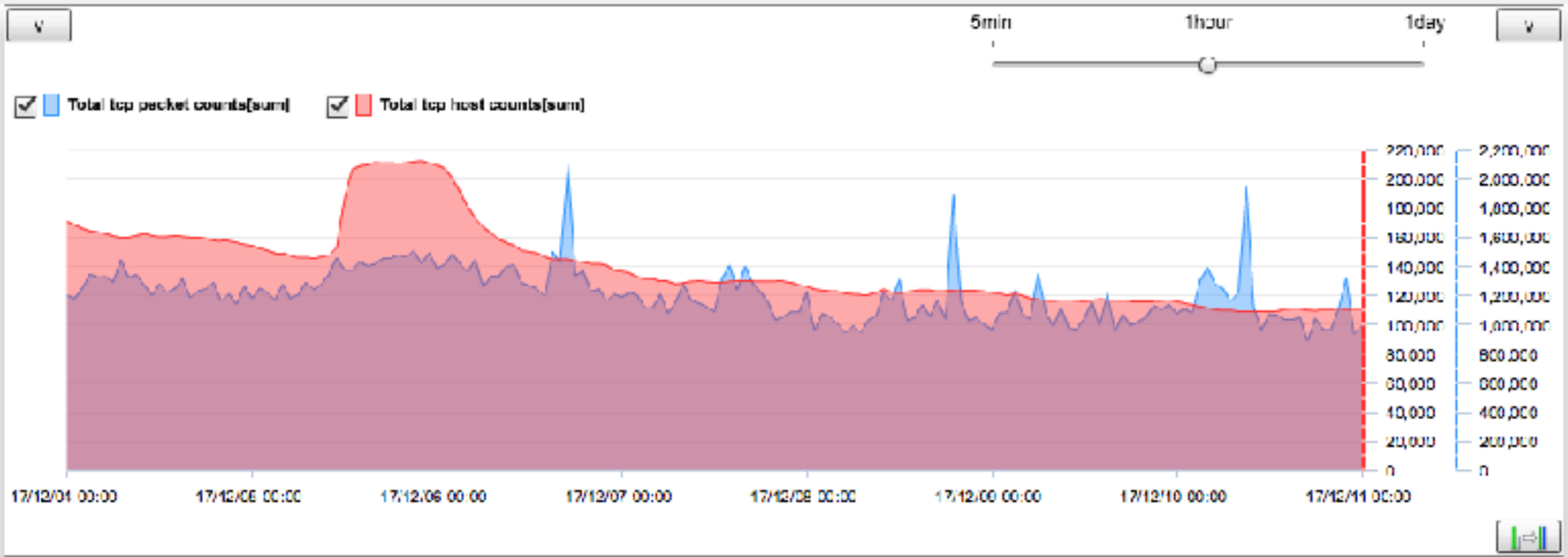
IoT Attacks

Monitoring Attacks - By NICT



Attacks

Stats



Top 10 List

2017/12/11のデータを表示中

国別ユニークホスト数 Top 10

国名（国コード）	ホスト数	割合
ブラジル（BR）	194,202	36%
中国（CN）	61,590	11%
エクアドル（EC）	22,422	4%
ロシア連邦（RU）	22,367	4%
コロンビア（CO）	22,322	4%
インド（IN）	20,559	4%
日本（JP）	20,442	4%
インドネシア（ID）	19,163	4%
アメリカ合衆国（US）	15,281	3%
ベトナム（VN）	13,559	3%

TCP 宛先ポート別ユニークホスト数 Top 10

宛先ポート	ホスト数	割合
23	313,347	41%
445	97,714	13%
2323	68,047	9%
22	21,092	3%
37215	16,607	2%
21	11,305	1%
2222	10,925	1%
3389	9,343	1%
81	8,212	1%
9000	6,499	1%

UDP 宛先ポート別ユニークホスト数 Top 10

宛先ポート	ホスト数	割合
18183	1,503	5%
3544	1,441	5%
18439	754	2%
1900	675	2%
50295	400	1%
25232	352	1%
3889	308	1%
53806	240	1%
53	233	1%
19726	221	1%

These are IoT devices

LED display control system

Solid Stage Recorder

Data Acquisition Server

Wireless Router

TV Receiver

GSM Router

IP Phone

Parking Management System

VoIP Telephony System

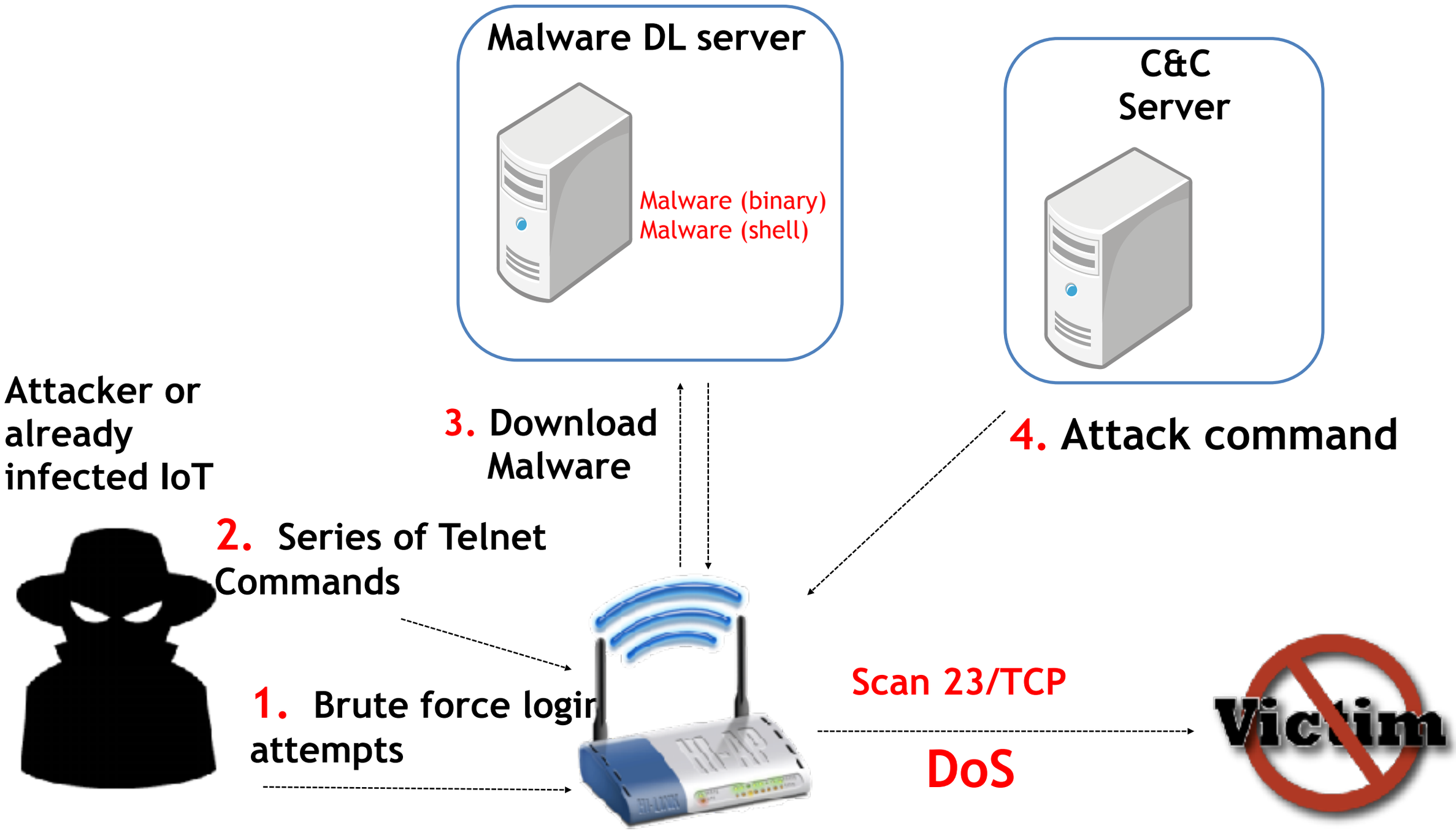
Fire Alarm

Security Appliance

Internet Communication Module

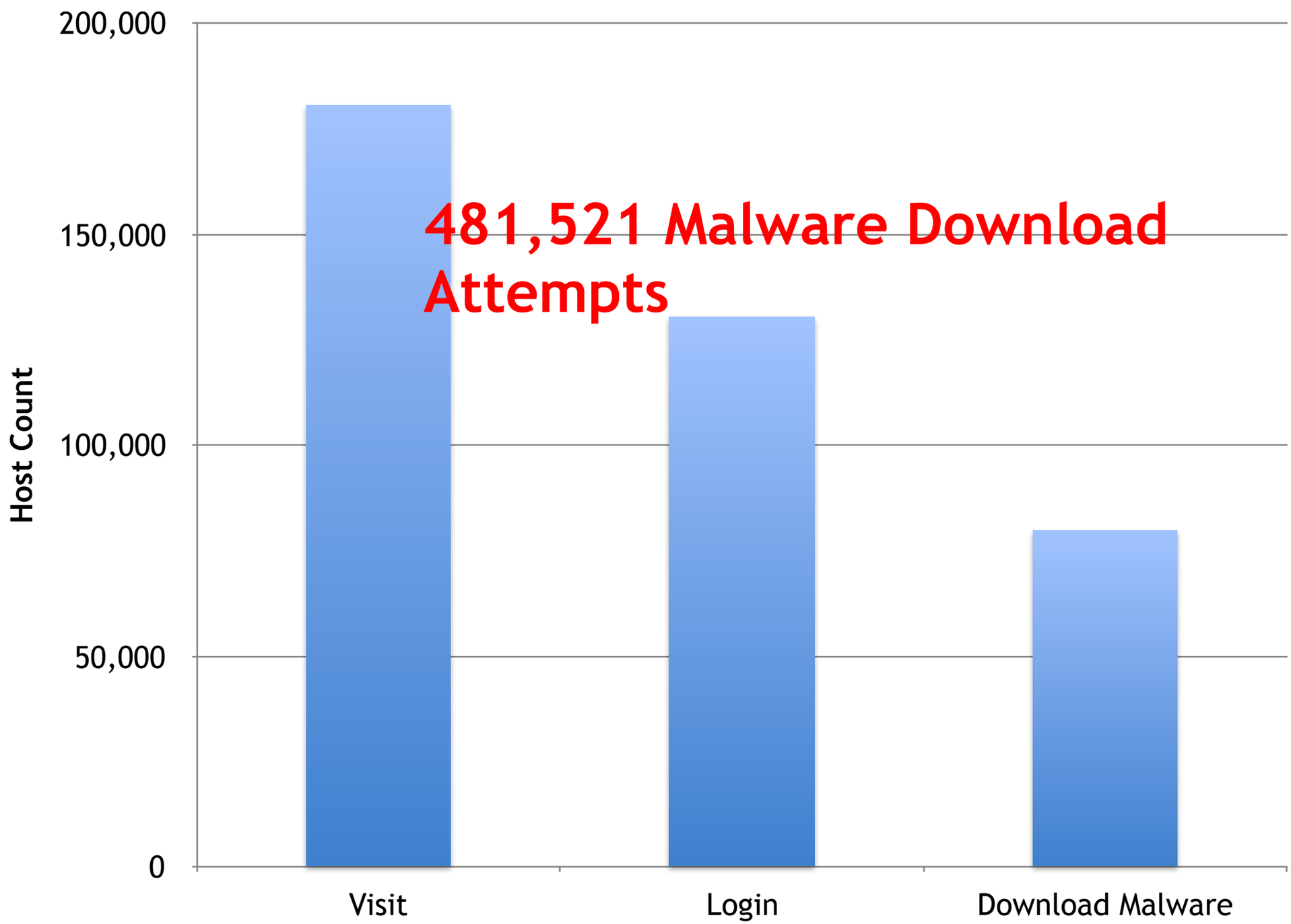
Video Broadcaster

Attak Flow

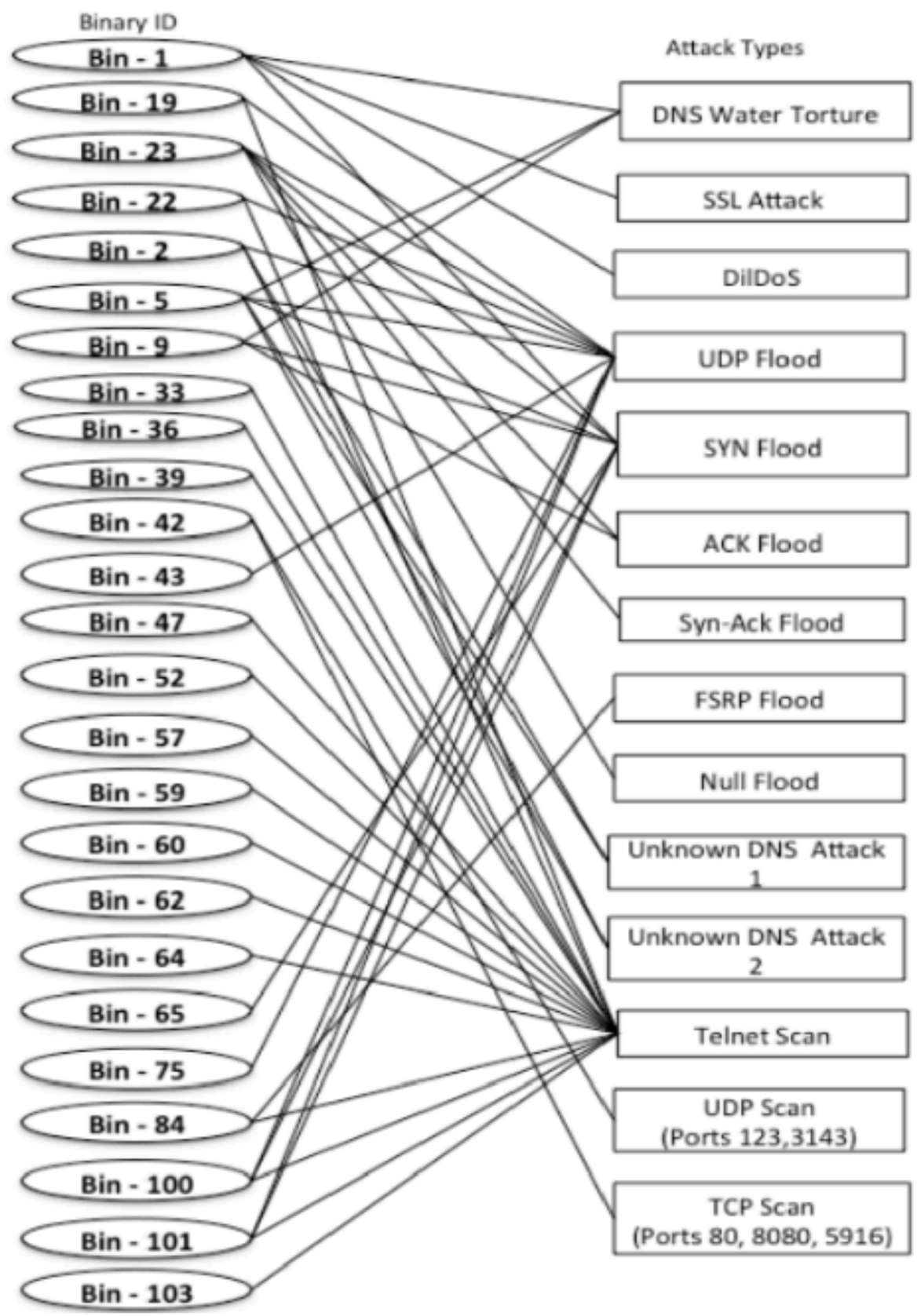

Malware DL server
Malware (binary)
Malware (shell)
C&C
Server
Attacker or
already
infected IoT
3. Download
Malware
4. Attack command
2. Series of Telnet
Commands
1. Brute force login
attempts
Scan 23/TCP
DoS
Victim

IoTPOT Results

- During 81 days of operations [April 01 to June 20- 2015]



Malware Analysis



Best Practices

- Never use default passwords
  - Printers
  - Network attached storage
  - Cameras
- Check before buy
- Update firmware
- Block port not used
- Block remote access

Ransomware

WannaCry


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

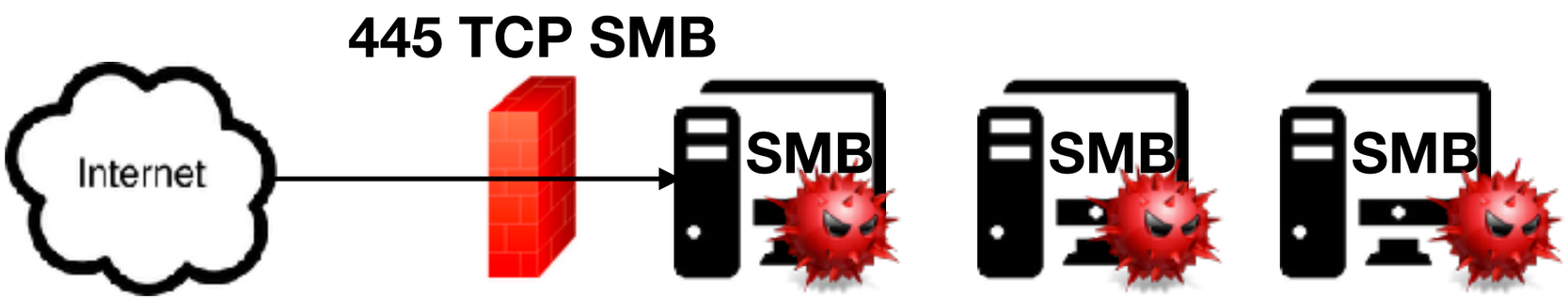
World Infection

Figure 3. Heatmap showing Symantec detections for WannaCry, May 11 to May 15

Encrypt 176 different file types
10,000 org, 200,000 individuals and 150 countries

https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Infection Flow



- **External Blue SMB exploit (heap spraying)**
- **DoublePulsar backdoor (install additional malware - WannaCry)**

Ref - https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/

Best Practices

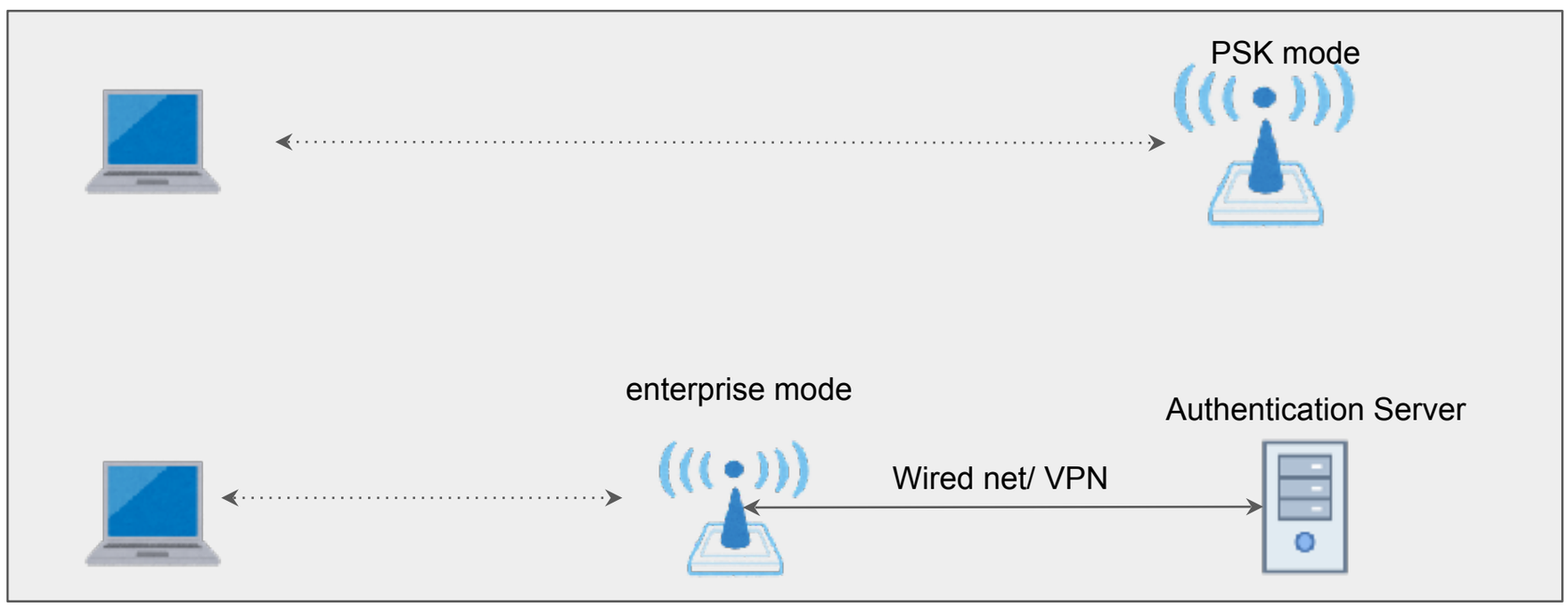
- Never pay
- Backup important data
- Keep OS and other software update
- Be aware of unexpected mails with links and attachments
- Disable unused services
- Block unused incoming port

Wireless Attacks

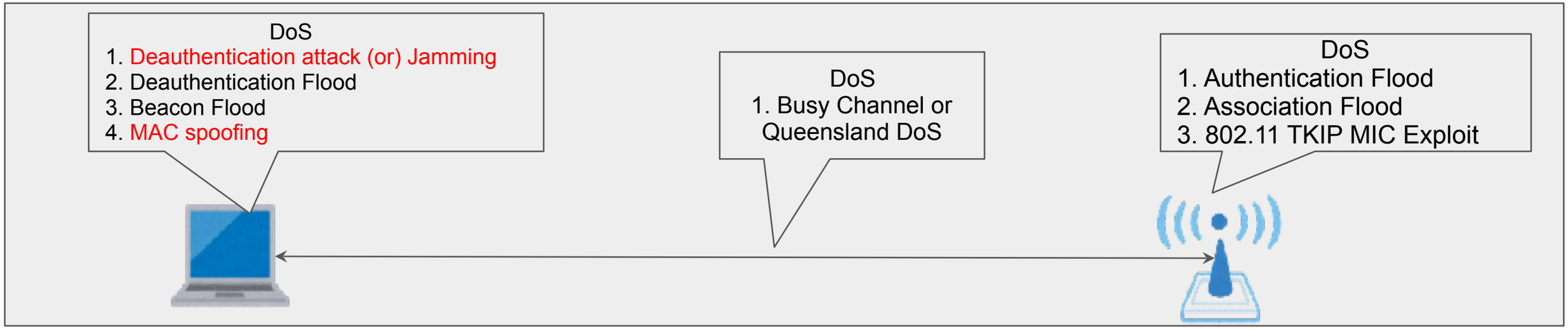
Wireless Modes

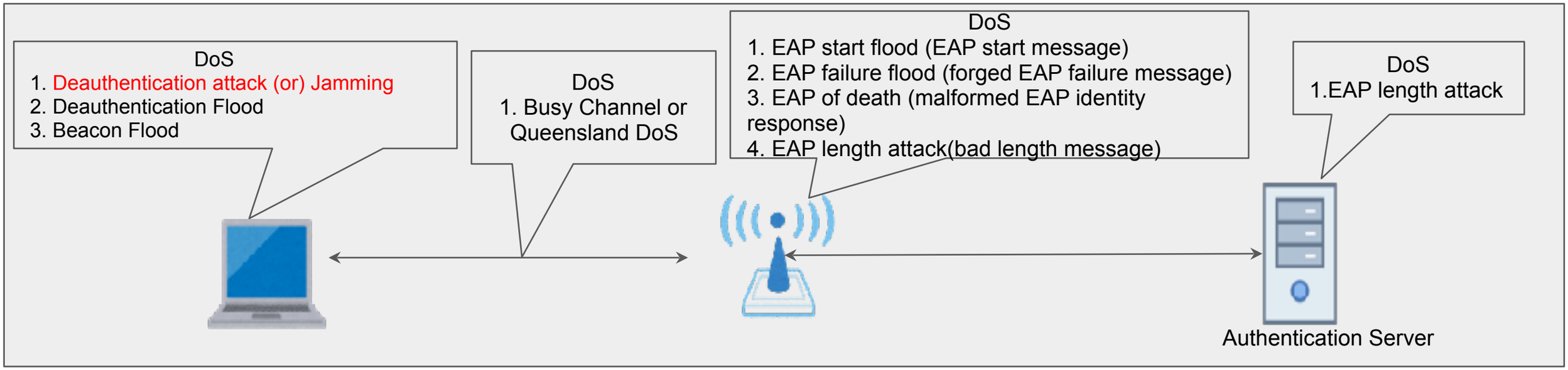
Ad hoc Mode

Infrastructure Mode



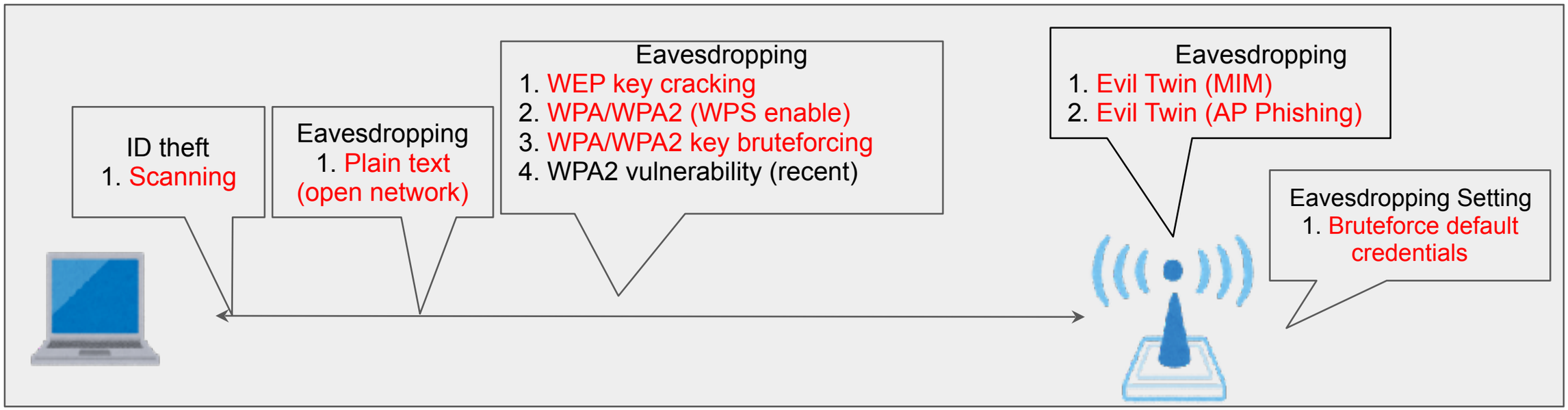
Availability (DoS)

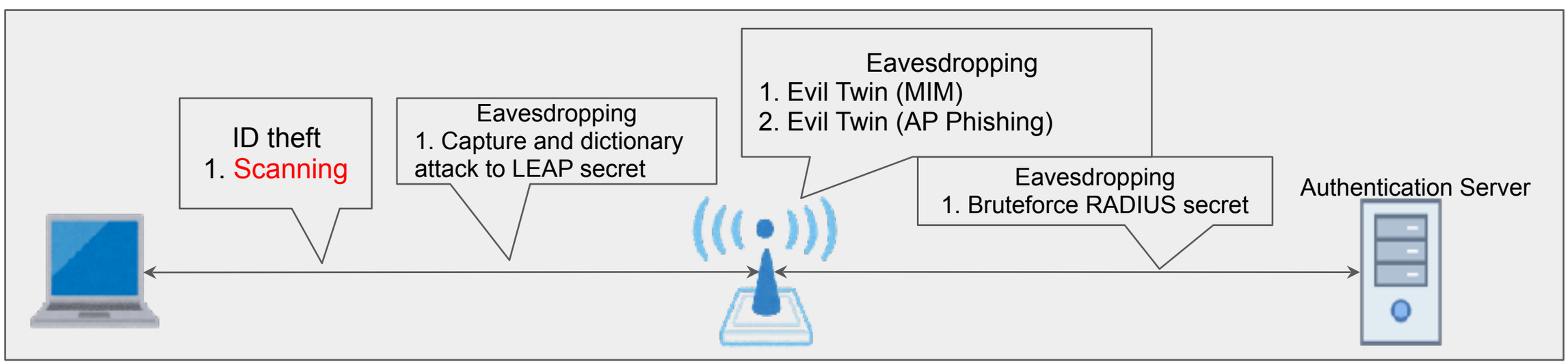




Red colored text = practical attack
Black colored text = theoretical attack

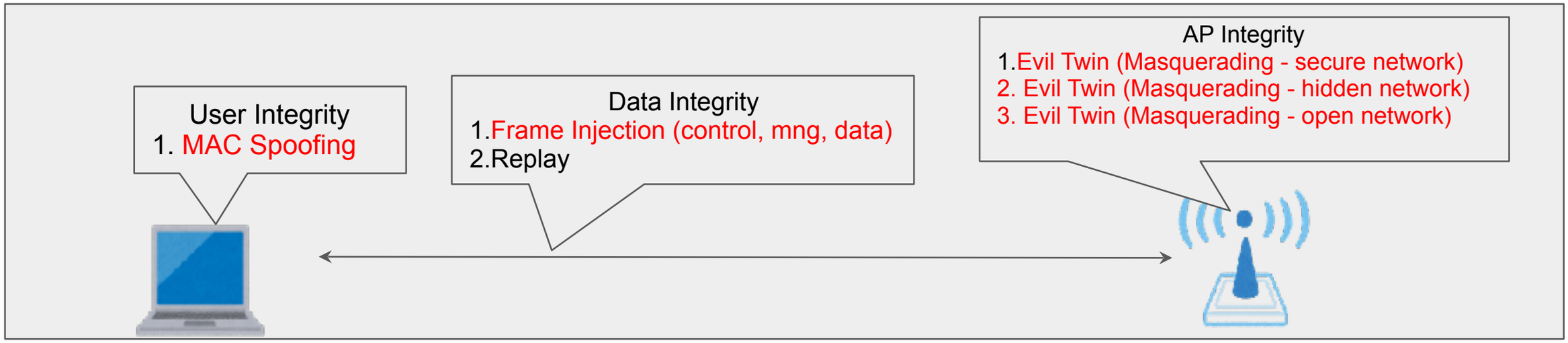
Confidentiality (Eavesdropping/ ID theft)

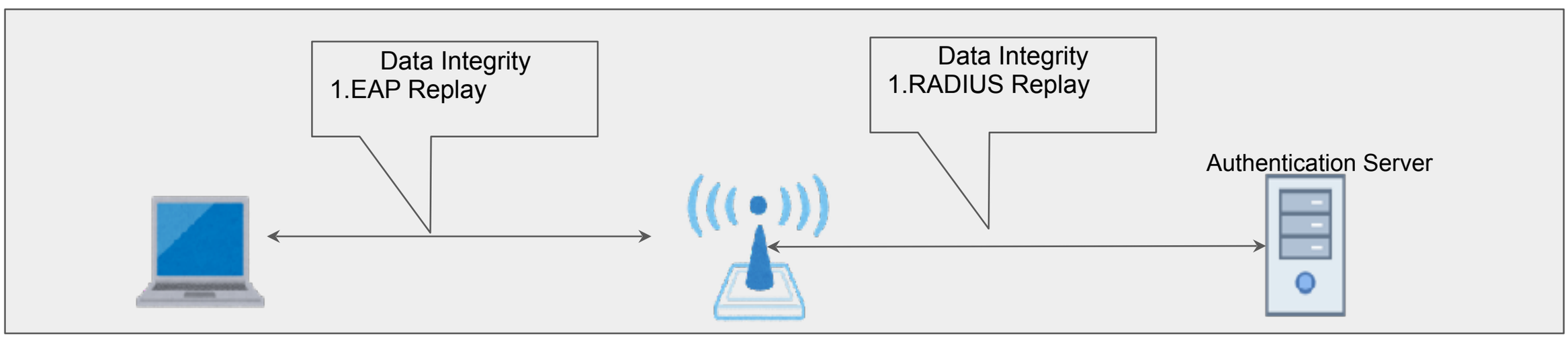




Red colored text = practical attack
Black colored text = theoretical attack

Integrity





Red colored text = practical attack
Black colored text = theoretical attack

Best Practices

- Use WPA - 2
- Use enterprise mode
- Use strong passwords
- Never use default login id/ passwords

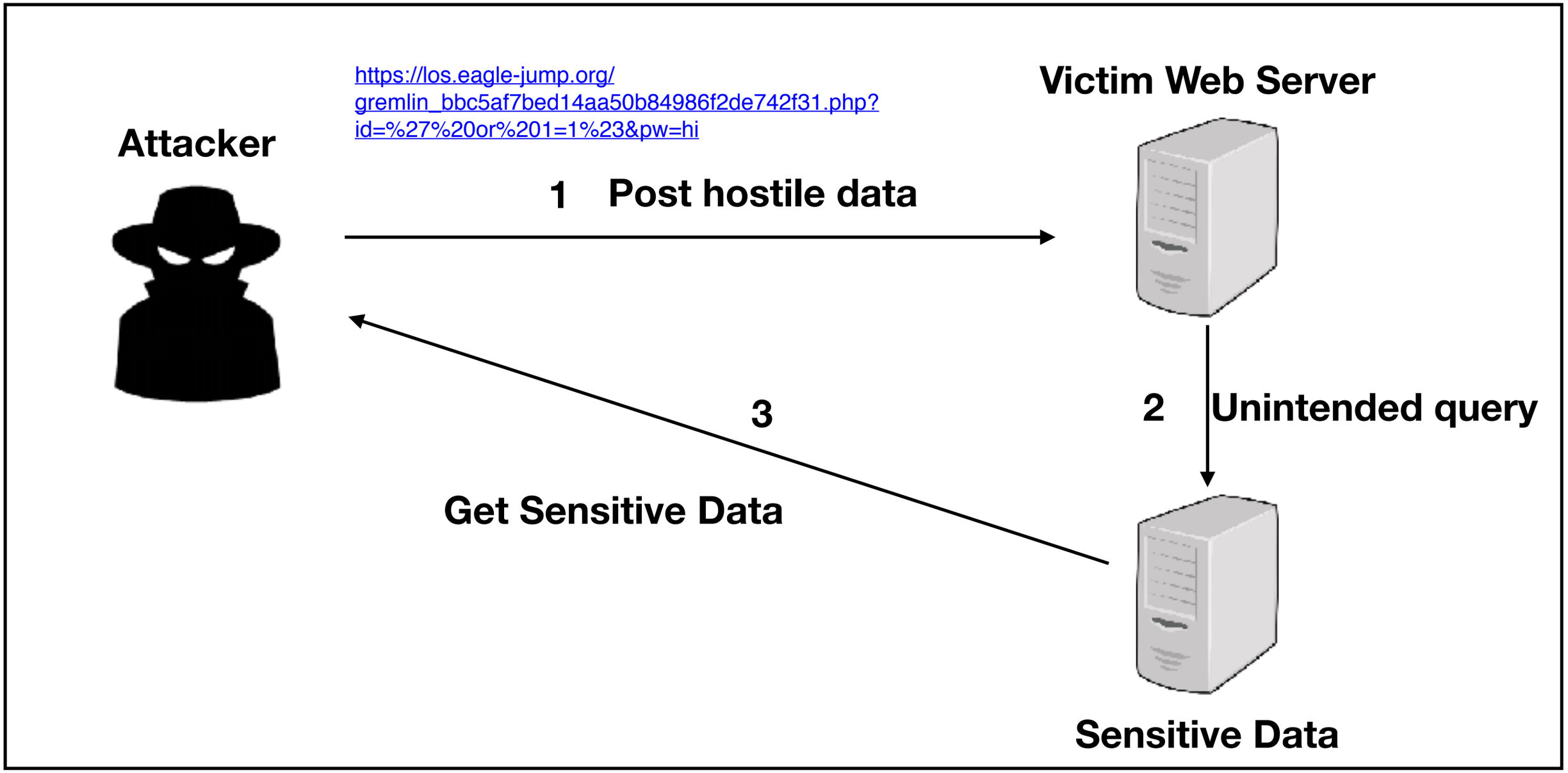
Web Attacks

OWSAP - Top 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

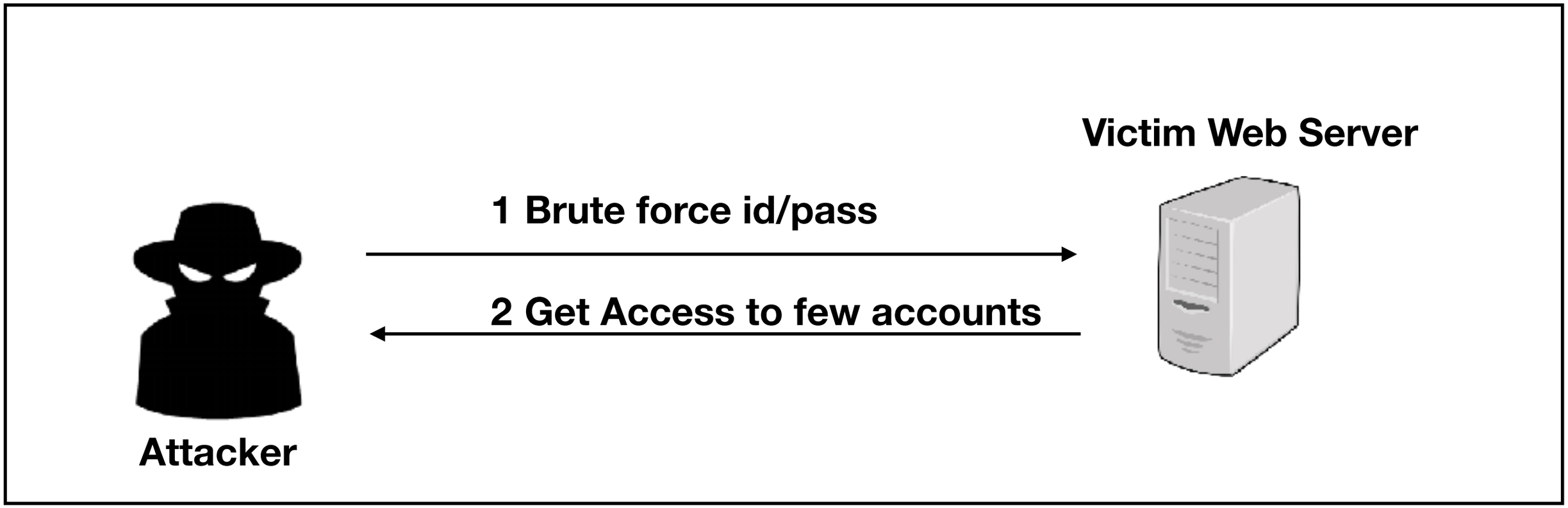
Ref: OWSAP

Injection



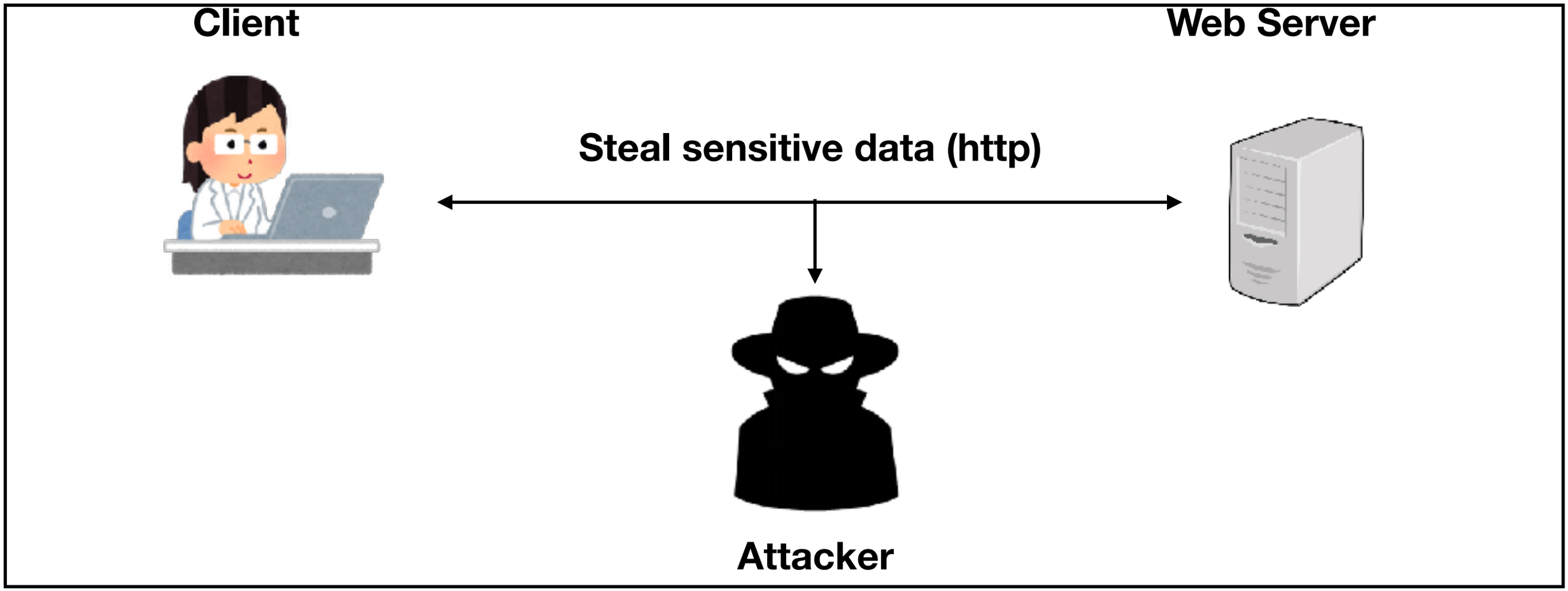
- SQL, NoSQL, OS, LDAP injections
- Use static source (SAST) and dynamic application test (DAST) tools
- Use safe API
- Use whitelist server side input validation
- Escape Special Characters
- Use LIMIT and other SQL controls

Broken Authentication



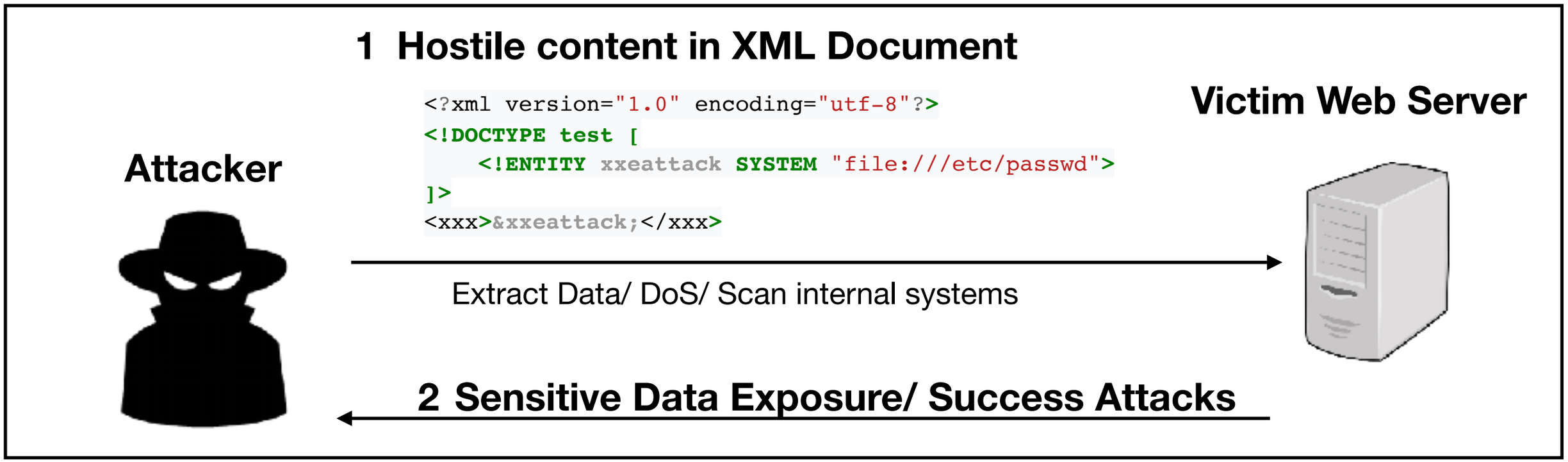
- Implement multi-factor authentication
- No default credentials
- Implement weak password checks using weak password lists from OWSAP
- Align password length, complexity, rotational policies (NIST guidelines)
- Limit login attempts
- Session ID
  - Random, not in URL, securely stored, invalidated after logout, idle

Sensitive Data Exposure



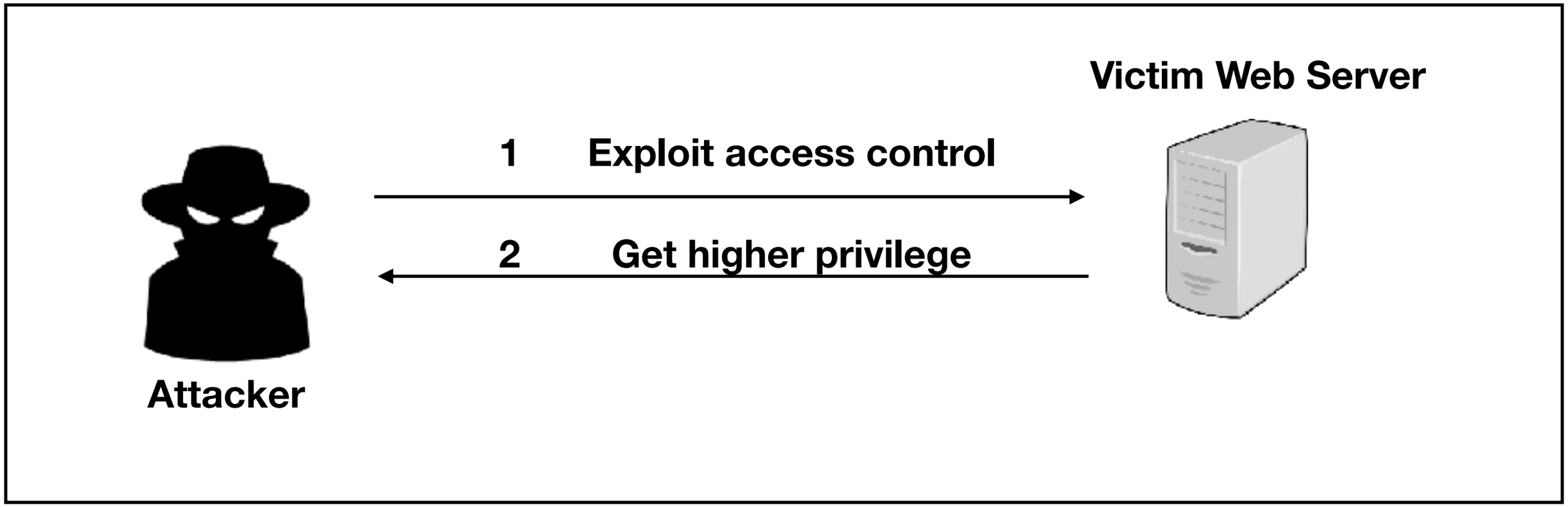
- Classify sensitive data and control it
- Encrypt all sensitive data at rest
- Use proper key management (encryption key)
- Encrypt all data in transit
- Disable caching for responses that contain sensitive data
- Store passwords using strong adaptive and salted hashing functions with delay factor using Argon2, scrypt, bcypt, PBKDF2

XML External Entities



- Use less complex data format such as JSON
- Patch or Upgrade all XML processors and libraries in use
- Disable XML external entities
- Implement server side input validation
- Use SAST tool to check

Broken Access Control



- Disable web server directory listing
- Log access control failures and alert to admin
- Rate limit API and controller access

External Document

Defense

Minimum Defense Mechanisms

- Prevention
  - Firewall
  - WAF (Web application firewall)
  - IPS
  - End point Security
  - Assessment such as (Red Team Exercises)
  - CERT (Computer Emergency Response Team)
  - SOC (Security Operation Center)
  - Security Policy
  - Training
- Detection
  - IDS
  - Penetration Testing
  - Security Appliance (Sandbox)
- Recovery
  - Backup
  - Incident response manual

20 CIS controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

Download the First 5 CIS Controls

Secure Your Organization

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

Download All 20 CIS Controls

CIS SecureSuite™ Membership

Become a member

Learn More

Useful Links

- www.owasp.org
- www.cisecurity.org
- www.yinminnpapa.com

- Contact mail
  - yinminpapa@gmail.com

Q&A