



# **Latest Cyber Security Threats & Trends**

## **The Ways To Deal With Them**

Summ CHAN | Security Consultant | December 2019



## Agenda

- Latest Cyber Security Threats & Trends
- Cyber Attack & Defense
- Security Incidents Handling
- Security Advice Round Up

# About Us

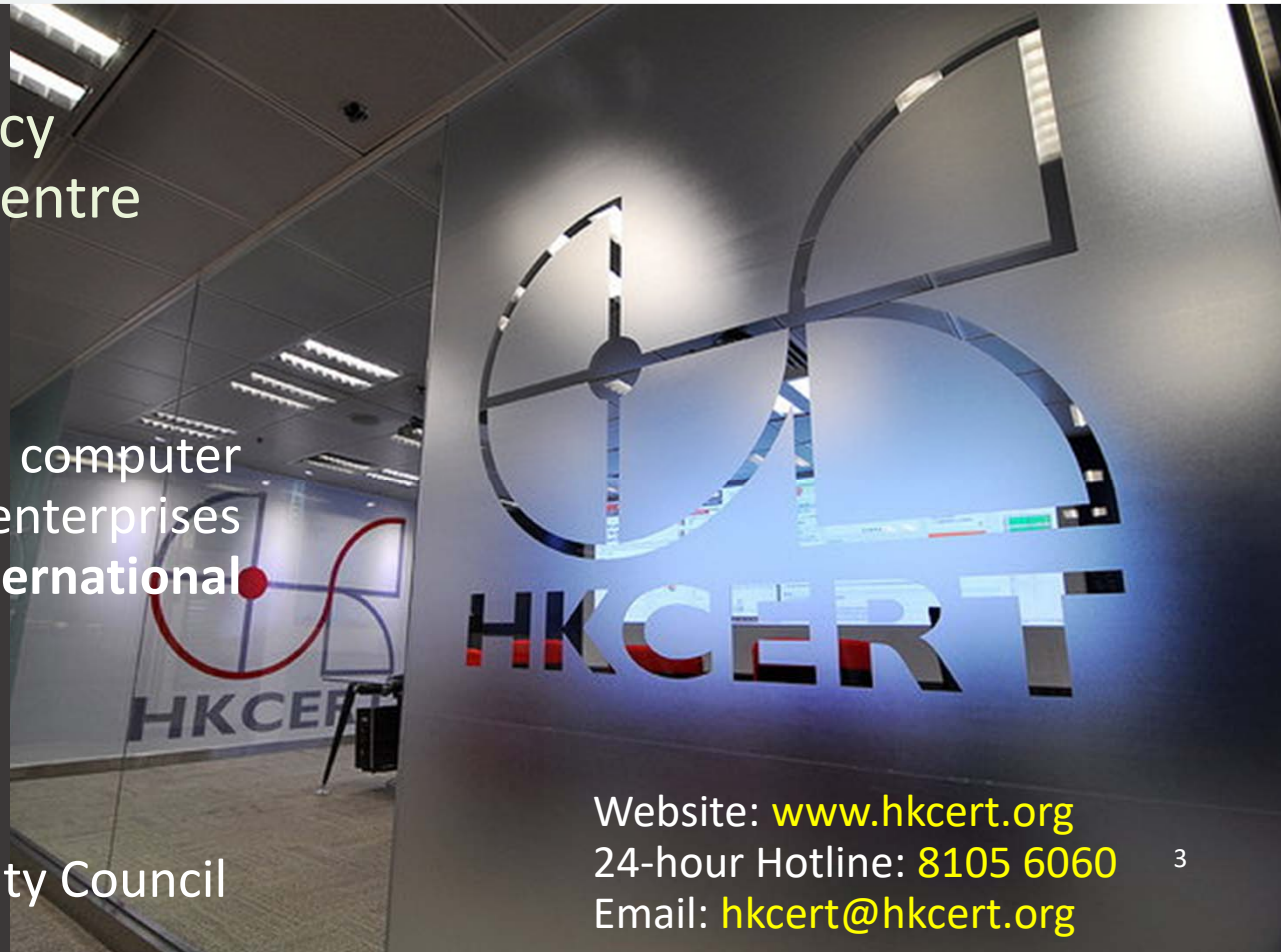
Hong Kong Computer Emergency  
Response Team Coordination Centre  
(香港電腦保安事故協調中心)

## Mission:

As the **Centre for coordination** of computer security incident response for local enterprises and Internet Users, and the **International Point-of-Contact**

- Founded in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council

asd



Website: [www.hkcert.org](http://www.hkcert.org)  
24-hour Hotline: 8105 6060  
Email: [hkcert@hkcert.org](mailto:hkcert@hkcert.org)



**01**

Security Alert Monitoring  
and Early Warning

**02**

Report and Response

**03**

Publication of Security  
Guidelines and Information

**04**

Promotion of Information  
Security Awareness





# **Cyber Security Threats & Trends**

# Summary of HKCERT Security Incident Reports

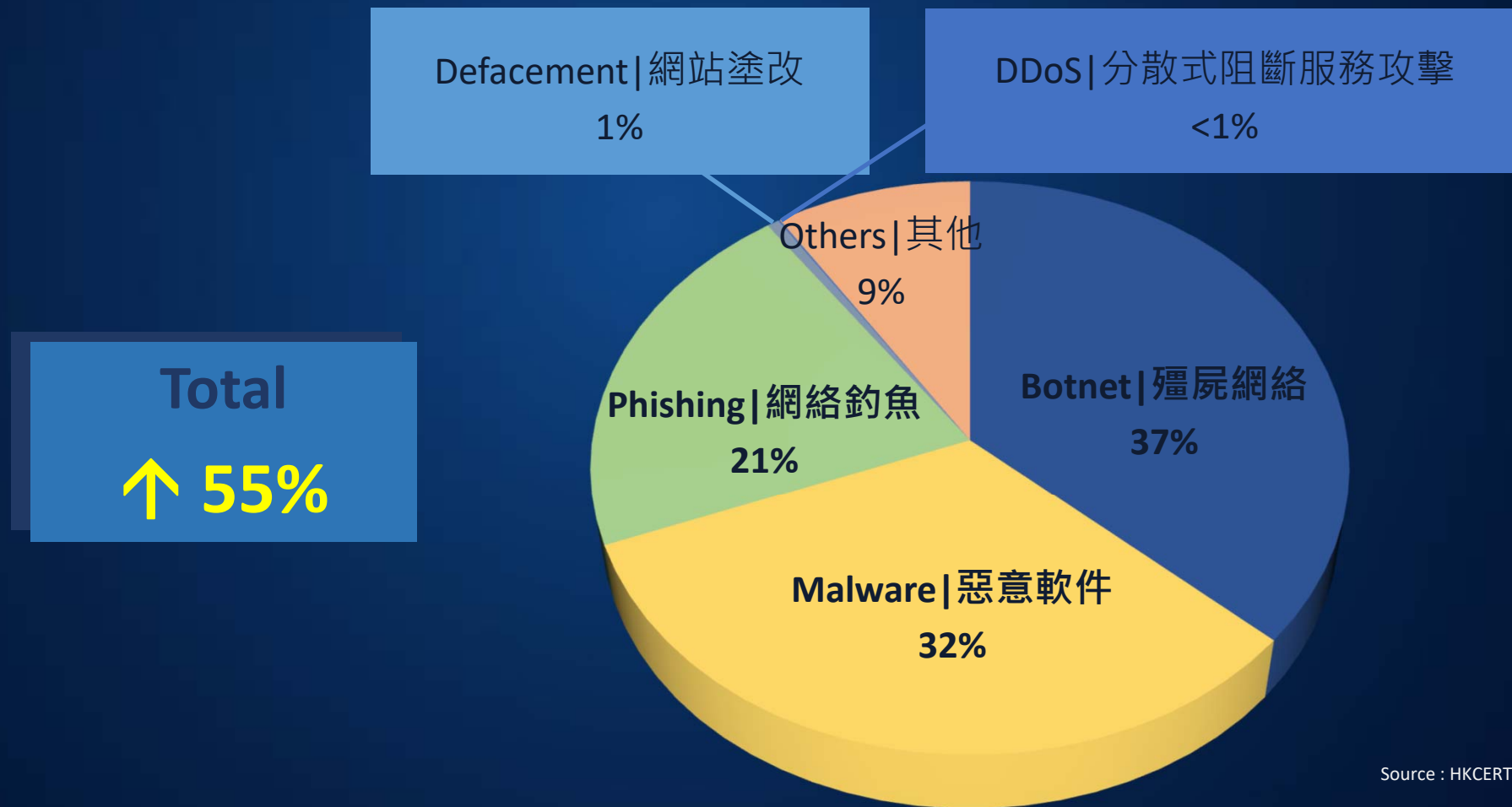


YoY **↑ 55%**



Referred case contributed 95%

# Summary of HKCERT Security Incident Reports



Source : HKCERT

Copyright © 2019 HKPC All rights reserved



# **Cyber Attack & Defense**



# #Cyber\_Attacks

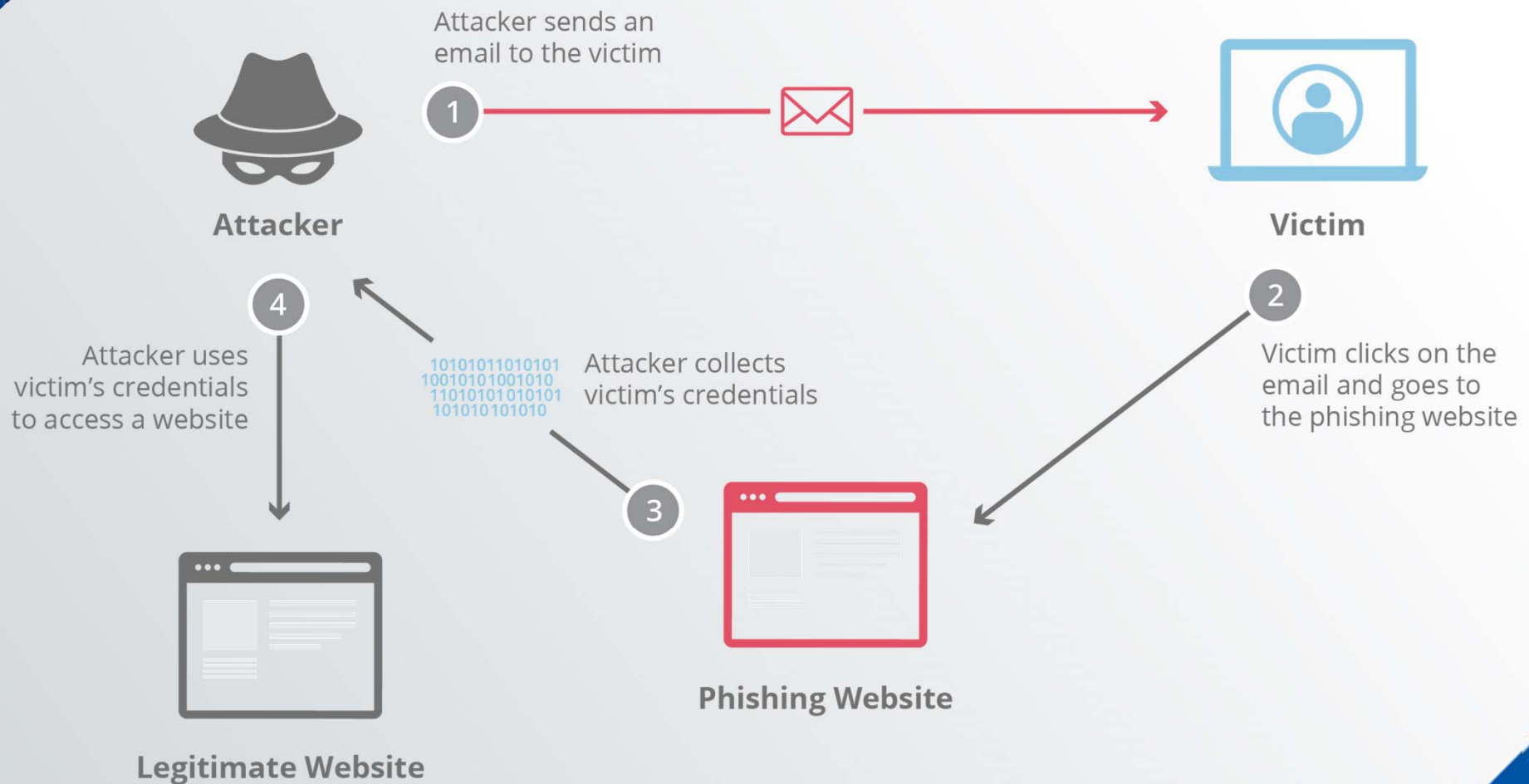
A person wearing a dark hoodie is seen from behind, sitting at a desk in a dimly lit room. They are looking at several computer monitors. The monitors display various types of data, including lines of code, graphs, and system logs. The overall atmosphere is dark and technical, with a blueish tint to the lighting. The text "#Cyber\_Attacks" is overlaid in a large, white, sans-serif font across the upper right portion of the image.

Image credit: <https://economictimes.indiatimes.com/tech/internet/69-indian-firms-face-serious-cyber-attack-risk-study/articleshow/69305216.cms>

A close-up photograph of a white telephone handset. A white rectangular label is placed on the side of the handset, featuring the word "Phishing" in a bold, red, sans-serif font. The handset is positioned diagonally, and its coiled cord is visible in the background. The lighting is bright, creating soft shadows and highlighting the texture of the handset's surface.

**Phishing**

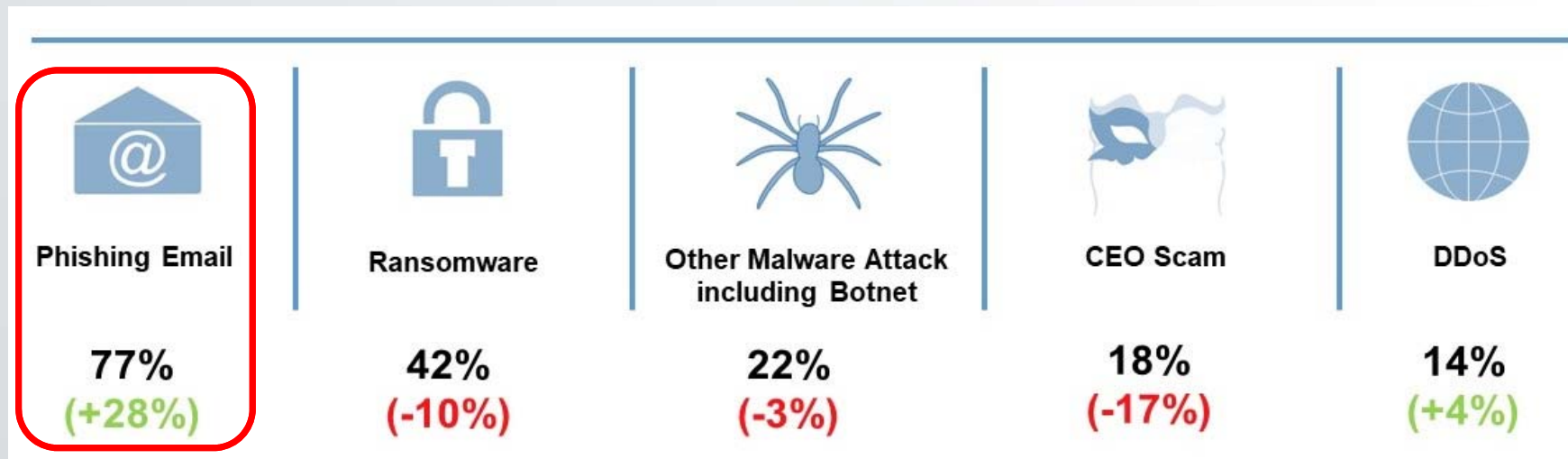
# What is Phishing?



# Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)

350 Large Enterprises and SMEs interviewed

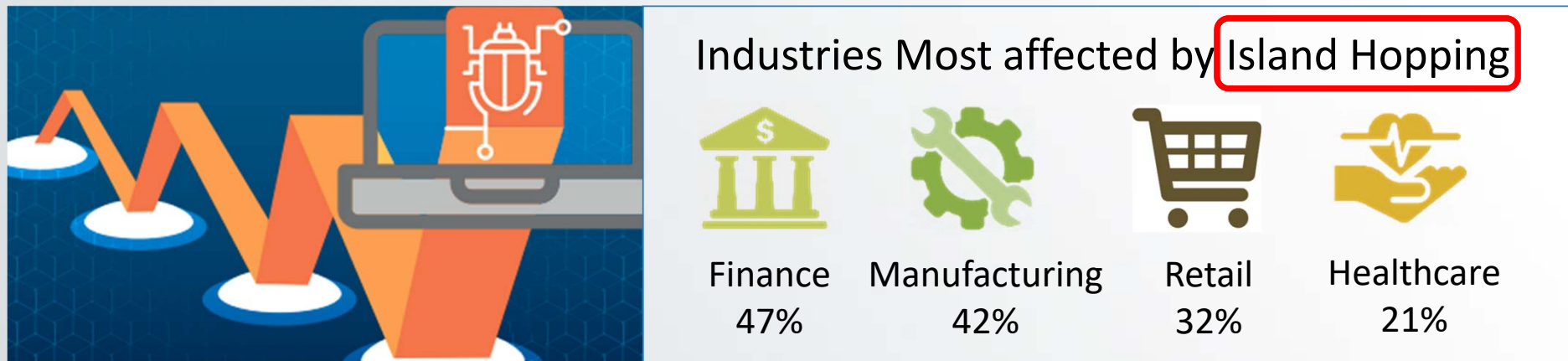
## Top 5 External Attacks



Source: SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2019, HKPC



# Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)



- Hop to connected network (enterprise internal) – lateral movement
- Reverse Business Email Compromise – take over mail server (enterprise internal)
- Website waterhole (trap customers)

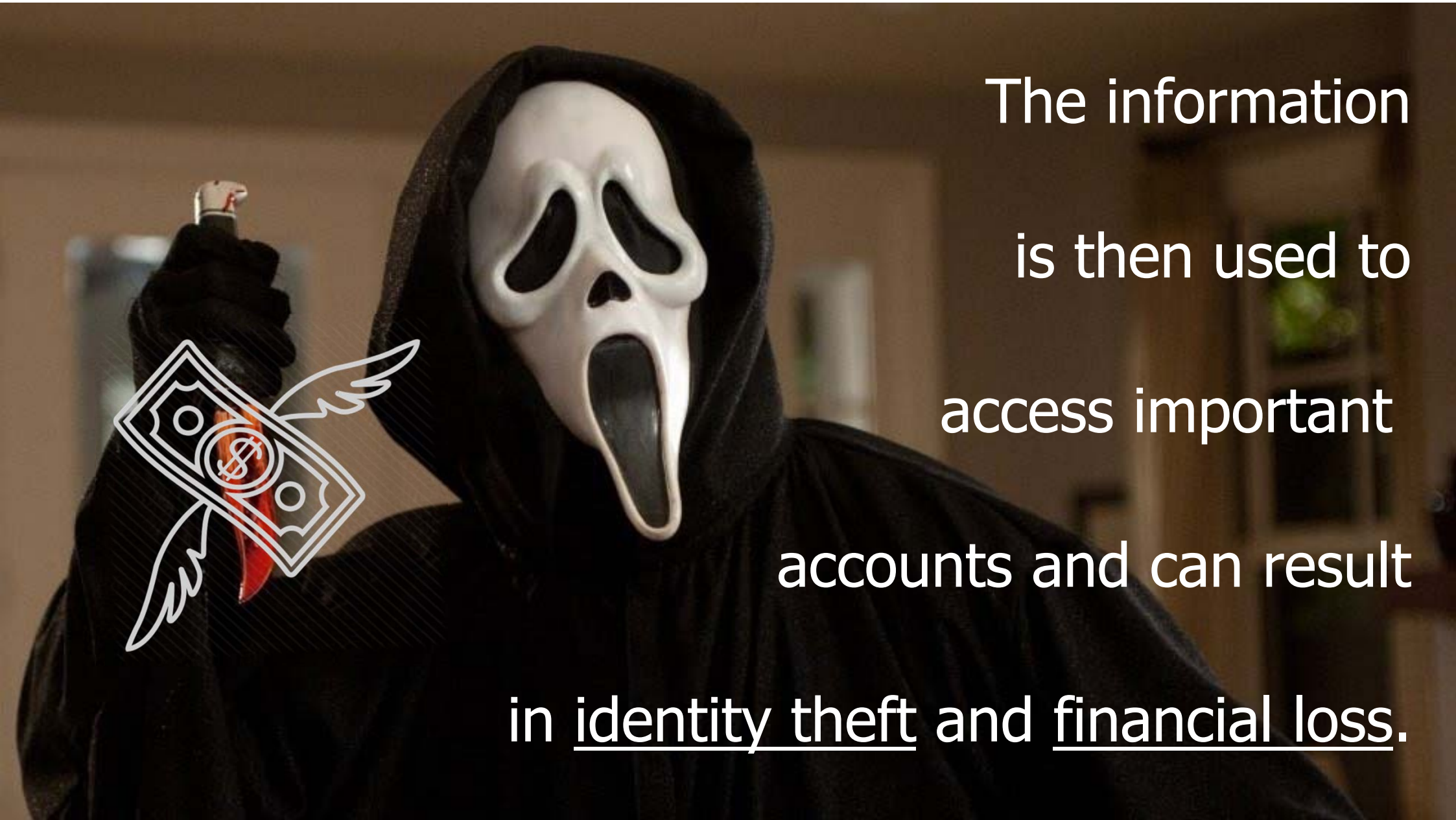
Source: **Global Incident Response Threat Report, 2019-Q1, Carbon Black**



PHISHING . . . .

the begin of a cyber attack story

Image credit: <https://people.com/celebrity/beauty-and-the-beast-live-action-movie-with-emma-watson-all-about-disney-film/>



The information  
is then used to  
access important  
accounts and can result  
in identity theft and financial loss.

# Phishing Tactics: New Developments (1)

APPLE

mail.xn--pple-zna.com.

-->

mail.apple.com.

ns1.xn--appl-ou5a.com.

-->

ns1.apple.com.

ns2.xn--appl-ou5a.com.

-->

ns2.apple.com.

www.xn--le-m1aa24e.com.

-->

www.apple.com.

www.xn--pple-9na.cf.

-->

www.apple.cf.

## ■ Use of HTTPS



58% of phishing using HTTPS  
(APWG 2019 Q1 Report)





# Phishing Tactics: New Developments (2)

## ■ Multi-level Social Engineering

- Attacker created a post in LinkedIn and built trust on the post with comments and dialogue with the “friends” for some time.
- Attacker sent email to victim with reference to the post

## ■ Evade spam filter by using image

- Ransom email in image
- Payment bitcoin address in QR code

**Fraudsters deepfake CEO's voice to trick manager into transferring \$243,000**



by RAVIE LAKSHMANAN — 9 days ago in SECURITY











**How To Distinguish**

**PHISHING  
SCAM**



# TOP 10 GENERAL EMAIL SUBJECTS

HACKOLOGY

	Password Check Required Immediately	19%
	Your Order with Amazon.com/Your Amazon Order Receipt	16%
	Announcement: Change in Holiday Schedule	11%
	Happy Holidays! Have a drink on us.	10%
	Problem with the Bank Account	8%
	De-activation of [[email]] in Process	8%
	Wire Department	8%
	Revised Vacation & Sick Time Policy	7%
	Last reminder: please respond immediately	6%
	UPS Label Delivery 1ZBE312TNY00015011	6%

Source: <https://www.securitybrigade.com>



**GREED**

**URGENCY**

**CURIOSITY**

**FEAR**





# How to distinguish Phishing Scams?

## Sample 1

URGENCY

GREED

Lucky Draw & Rewards



# How to distinguish Phishing Scams?

## Sample 2

URGENCY

FEAR

Online Service

**From:** Microsoft office365 Team [<mailto:cyh11241@lausd.net>]

**Sent:** Monday, September 25, 2017 1:39 PM

**To:**

**Subject:** Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

Microsoft Security Assistant  
Microsoft office365 Team! ©2017 All Rights Reserved

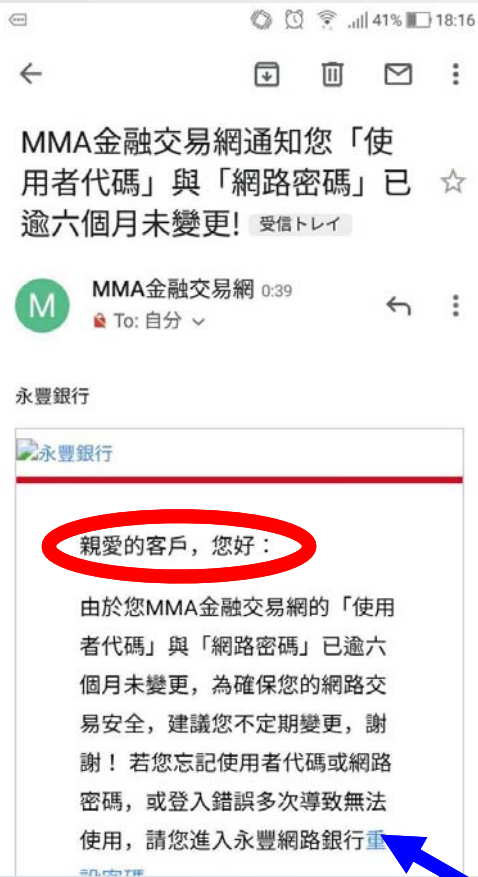
# How to distinguish Phishing Scams?

## Sample 3

URGENCY

GENERAL GREETING

Banking & Finance



Retail

From: apple, Inc <Update\_account\_confirmed@altervista.org>  
To:  
Sent: Thursday, April 24, 2014 12:35 PM  
Subject: Update your Account information !



Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

[Get Started](#)

If you need help logging in, go to our Help left by clicking the Help link located in the upper right-hand corner of any Apple page. .

Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

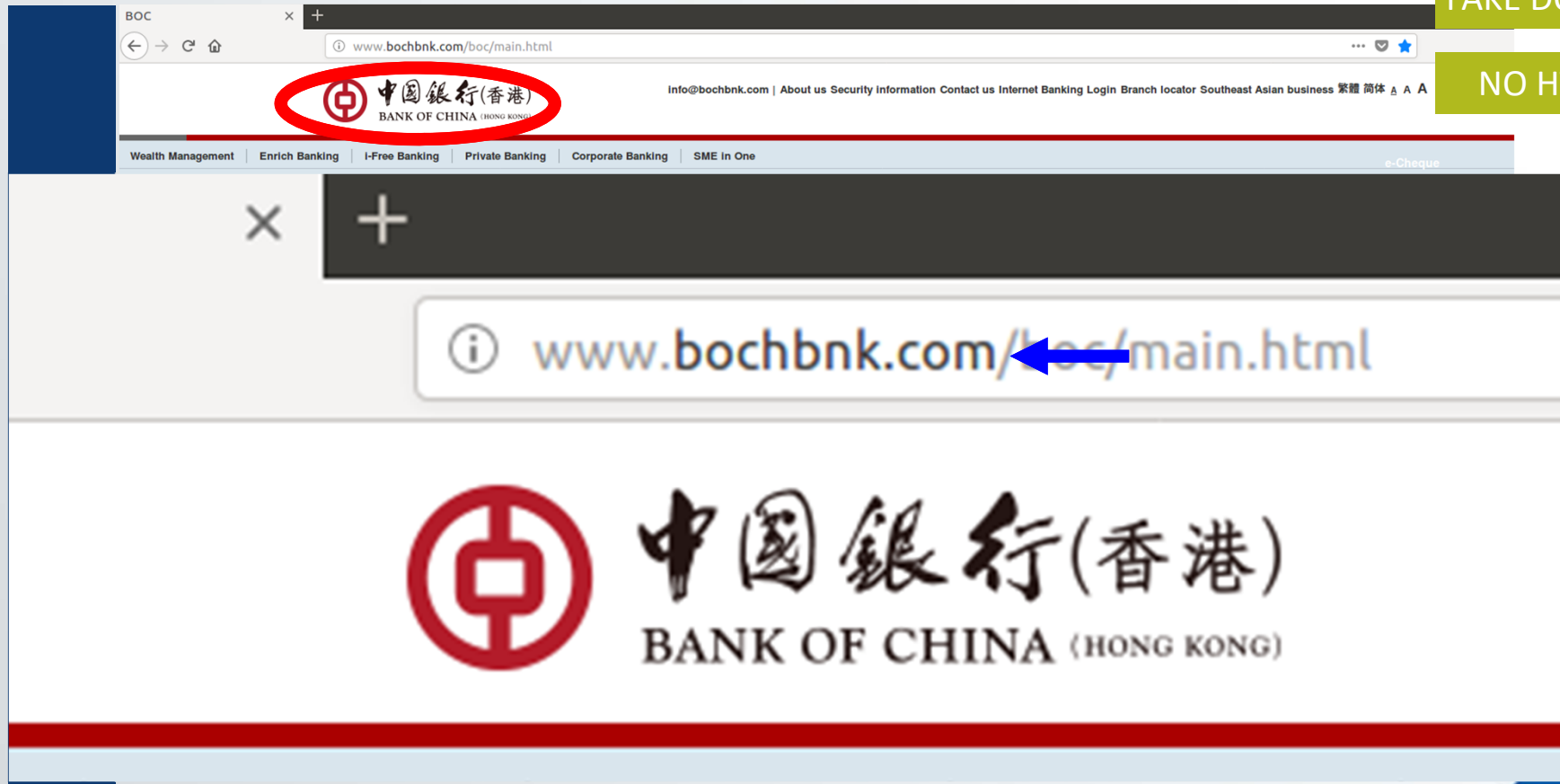
# How to distinguish Phishing Scams?

## Sample 4

URGENCY

FAKE DOMAIN

NO HTTPS



# How to distinguish Phishing Scams?

## Sample 5

FEAR

HTTPS

Enter the URL on your own

Internet Service Provider





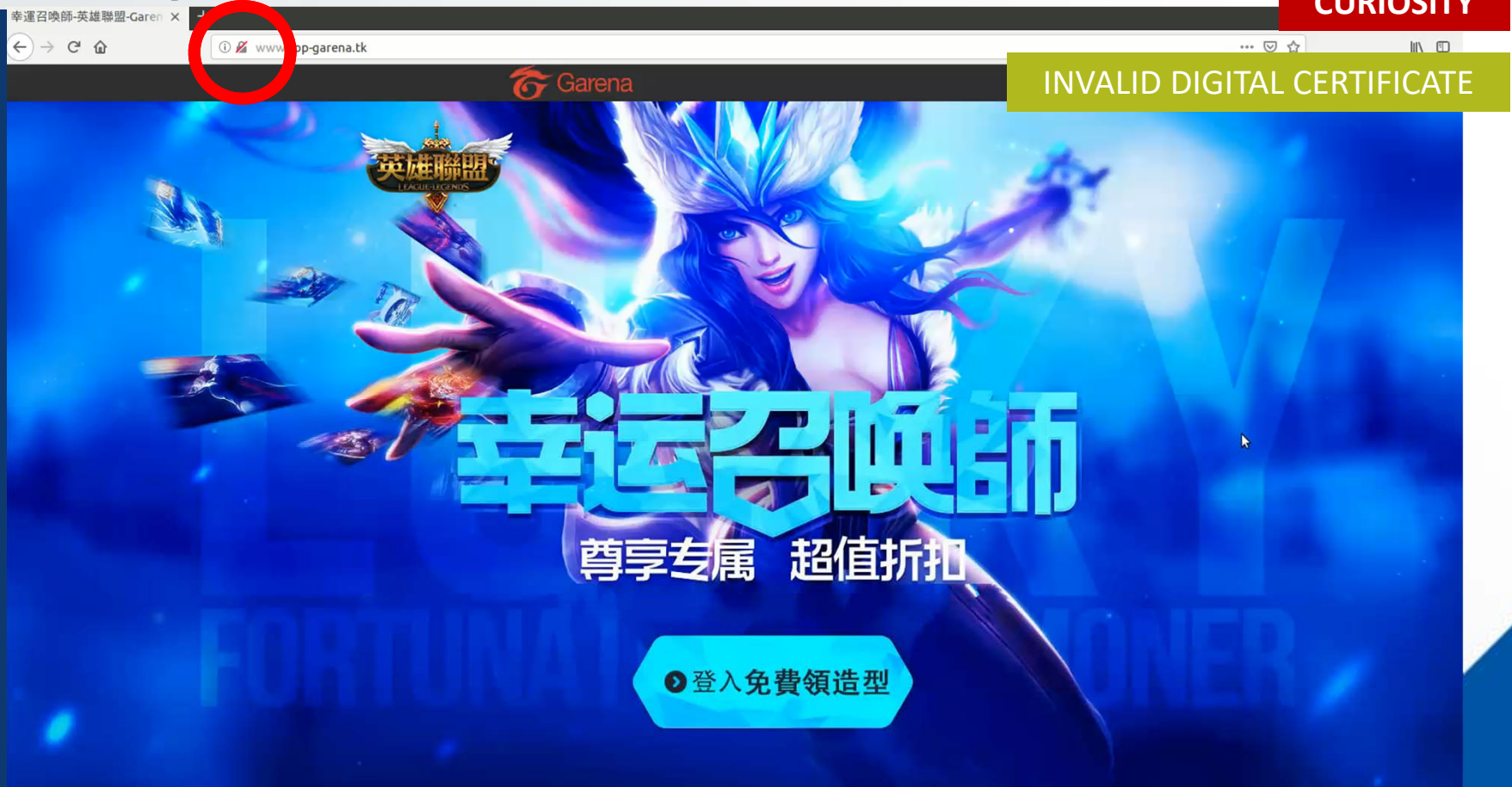
# How to distinguish Phishing Scams?

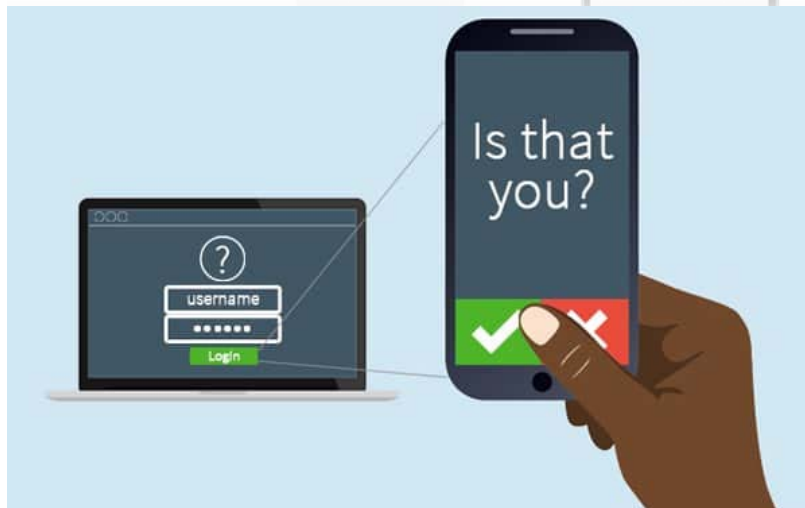
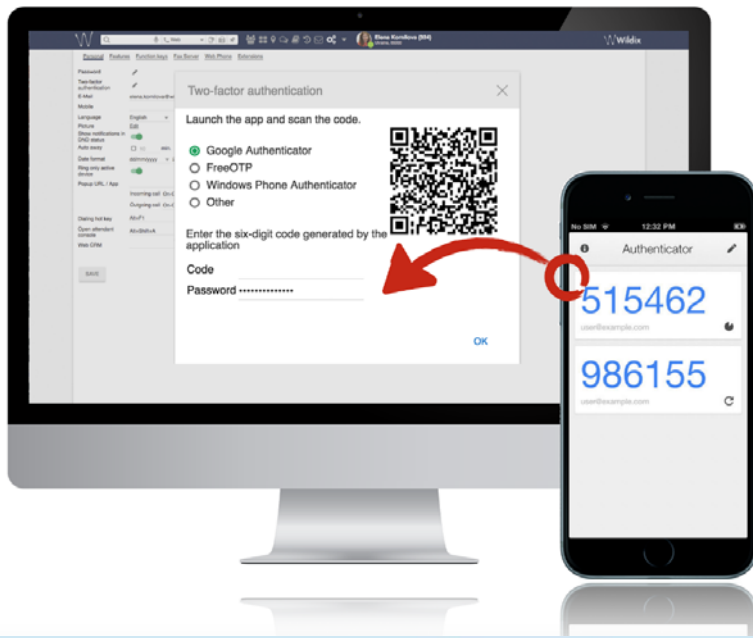
## Sample 6

GREED

CURIOSITY

Electronic Sports





Think before you click



Pick up the phone to verify



Use two-factor authentication (2FA) across all accounts



Use different passwords for different services



Use email filtering technology & make sure the technique is up-to-dated



Conduct phishing drill exercises for all general staff



1wyua+616itPoZw1hPshGevmbC+MLjtRYES5HoBM0FaOMo+Q+2nmU+4Pvhb33E2EW9izNayFjwQ0qcWvjUBQUYV/FuFyLPcdp1jh  
/CCbmpHye5RUaeOT/G6yPezgZFEfqS2CE8nz9GBt+ab3Pbo9On2MMYgn1h1zTNyzIBOKb01FqQFbsXCMgCKz4b+iQwIAtv6z1TFM  
ws6UJEA/4jdrS1390q8q1cwm0J7LYVvQThyzBt61KDPEXN6vBRGz27RY+6NtXFqs901XNREF3kIjnaKWiKzBSbvWleTXn12Hxt/  
Db+geLNkXIR5T5BDR9ZLdr2sOM5WZXGp7j05EFFFqisVJXO/K0pL4IqouZo11tHHjFn1SBPUgoF/3GhmMyOC9dGO708qXz+vSe9/  
SFC/8myp//VPLFK0wx2sqA+SGBYLj9KAFveev5vD/PRWGZE3NPwXT0V9b1zeCzhuTc+N7vkxi/pkmUA5YtBeHUG7OKTQt2tIQDM  
Ct6yWj11EjUI3i1KrjUe2Aj5ZiacGpRAp14KEhFRHf1z6wgYJ1Y30axsQKGoHMPFsQ9b4AtTfIbgZtu1QGjftVOq+jdZeAWBfcZ/  
7bHyiRKih8FuawqegyYltSSD18PYKvtSWBFZ+1IZ0pjqqoD7wbqa4ndvpUUOWdftdtG5yGMHbmdZrz/hYv0IAprhi6kBosCdfE9/  
jeqNVgFLj4gcOeOdaKww10cp4OuSed7IGV/y6PzhqV8Buc2VBVG/JzpQkz2ythFc5i2zHpbFCGWTPttwqF0v7jAHmmj2yg715n1c  
TPW5Fu2yyXC79YaasImkxc9XSe1u63G3Kx0k3m08dRtbhHEQf4rM9TDLvLqteM2T2NtB15HVnk8ThZ4OZ7F6Crnghtqzk0x1Ragr  
z0tP1smgX1/BEeRB4PkgB6fSufCOK/wgcDHexCuyeHxoS+jtL/nkn14xTkseSCYMGyDsCzrpDGFEiMeGcXtBW0+R0bqunup4fmyk7  
k1k4Pi86UzV3z67CY10DIDgxoFyA3awS7Tdvdv3/boP+qGAOWB+PGXPniC9TioZ6P3PFbUSrf1GCCxe1ojKMfYncAAzqDh0rkFo  
KgIr0yqv2/uRVgMXg41Xi5Tc4xDdAza+45Nw34PwVxcUPRJNgubbsxVbTanJWLqvaD06xU2N8m8jWYA/03hD8ikaIQjT+y43q/z  
Ayg9WmuDfg00HLht4Gwj/6qLe0ofc1khjY6756JQADKmxKDubmCTL6UgAMoeF2P5GXYQH31cB04n1Cy4Ua3D3UJjsGe5U/YozY6  
waVPZT/Z6wow/G8I1aak003Rqo8tL+HqyIHNCrMIu10pDEB+6XPzXqkuHnfptYRzSGsv9Zphi/h/eMNF1JxamtM6y/iZOX3d49r  
+Mpmi+pLq0pC9gJJg38H6PuUZS0UOX1TGbeLnx9uOTbB8vo7ZrvjmdMrehvZ1FI+wiPlgRT3SuV1zz6rgC47pD6M3GvG4VCm0M0  
h4itLix009JevudvwLoLUjZ0VzGro8Ufn9G3Av7Eo7nJfLqYBit54HPF9TVXSIueGykkHnt2wuqfQd9FJJmgynvpsRiB3Su4Ez7r  
sD8BkuBqEB1Qv0qkv0tfjHa0078KovcdkzbEDY/TpedLxfBJEJCyU6zhyWCzX7zsXX5xc7mhqOBstc0B7aE29Kogtvrf/iRuILJ  
wiRXMPcFcgnagGglZBsJbZTG+qoCKDo3Nj1IzmnJPvnLp7fNZjZYUFP5bjvb4jbfS6si1RnZh19Fd1f6SdNZSH+Nw8xCL9j4pBJ  
PiBVCdq4UuLEawlVXLaze24FAEdbpDNgt4Bqt0ArcVxHU0sTtU1qsARQuD0Zmyf5a9YnByQGTI6rrICRiAFZj1+teNjiA2T3nt  
+JCATd0UyHx13Ks/tCyIA6BBMW6NVg/VLKnffzyCPdkZfRLa7WUjVqgXhASRXys7xR9677Mp37+nEaFdbwViin9hhG6HSJ9Ykv  
zonn1JHpP2GhLf8FvVx7NZw1ak/tnsOpte/9xnTjwnYGpwQyKF1<QYps2dYg3eCyADFPjPvhc6kPL7HSy7v1555  
Ajs/FsgXHmk7+fttbYE71yIId/noyN93TOJB1y3IuPXETYS5R/vo8ye+4HPMLShvvd5TF571b42TK263,  
fk86q06Ayaib1vRjo9dv5TzjL6xyyGf4XiYj1gxkMCuyQZ9/d5ehmUPLo4c4hIXAXuKHfUUhVtXV2qdhbEGn1VycsYP9jrmxfqN  
6e8vtLynwmJ2Sdor1411hZYP9TgwJFO0K2pCeQo4c8VpdtZNeqduayPT3LtNjm17kaafOFa9ixokanVOYmba1NGUUTaHTK3OXi2  
PW8tCg1H+QuqY/b1MwgsAoFF835uZrmyCS7z9WNSfa0RptYkiZ

# RANSOMWARE

Image credit: <https://www.kratikal.com/blog/ransomware-attacks-shook-world/>

EDITION: AS ▼

**ZDNet**



VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO

# Over **500 US schools** were hit by **ransomware in 2019**

Fifteen US school districts, accounting for 100 schools, were hit in the past two weeks alone :



By [Catalin Cimpanu](#) for [Zero Day](#) | [October 1, 2019 -- 14:24 GMT](#)  
(22:24 GMT+08:00) | Topic: [Security](#)

## East Texas Attack

Port Neches-Groves schools attacked by ransomware, pay money for restoration

BY ISAAC WINDES

## Texas School District Pays Ransom to Regain Access to Files

Port Neches-Groves schools paid an undisclosed amount via bitcoin to a suspected overseas cyberattacker who encrypted millions of the district's files and issued a four-day deadline to respond to the criminal demands.

BY ISAAC WINDES, BEAUMONT ENTERPRISE / NOVEMBER 20, 2019



- The ransomware attack was discovered on July 19.



## Shade Ransomware Is the Most Actively Distributed Malware via Email

By [Sergiu Gatlan](#)



November 19, 2019



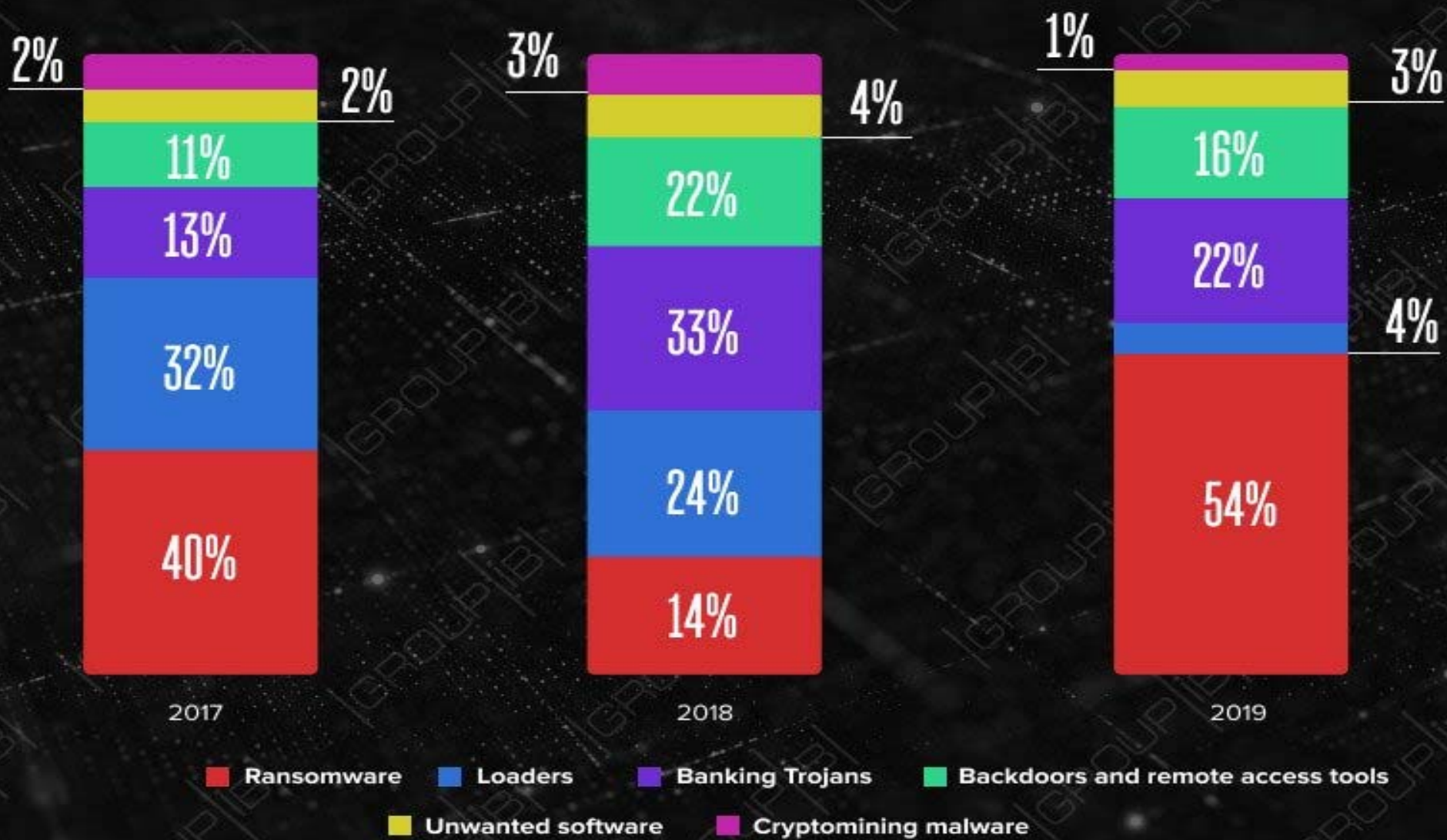
01:00 AM



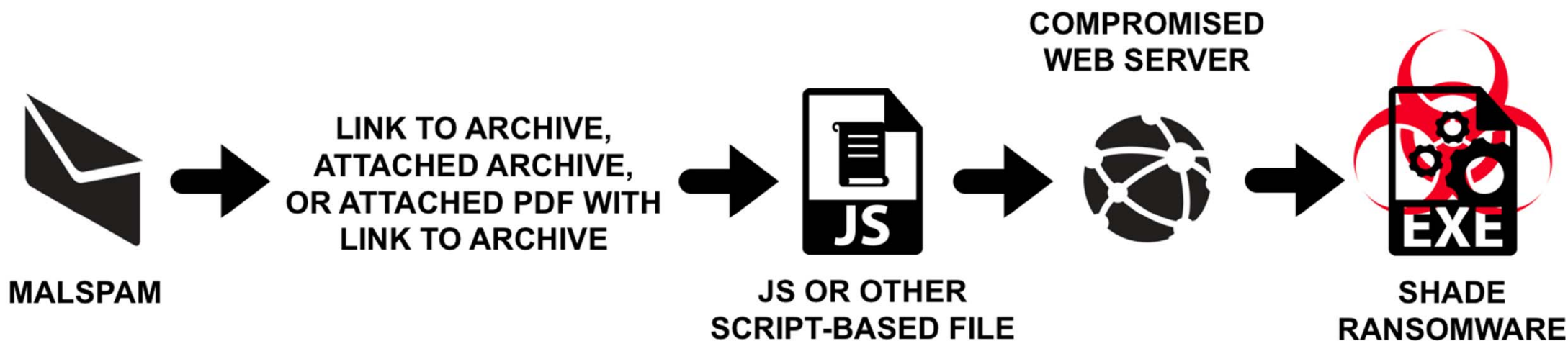
0

Source : <https://www.bleepingcomputer.com/news/security/shade-ransomware-is-the-most-actively-distributed-malware-via-email/>

## MALWARE CONCEALED IN EMAILS



# MALSPAM-BASED SHADE RANSOMWARE INFECTION:



Source : <https://unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/>

# Ransomware



Untargeted attack  
**Pay 2 Bitcoins** ransom



Targeted attack; Time-bomb  
Ransom **based on company size** (from 2 to 400 BTC)



Pay ransom to get your  
**DATA** back



Pay ransom on time or  
your **DATA** is **DESTROYED**

Jigsaw



Pay ransom on time or  
your **DATA** is **PUBLICIZED**

Doxware



Pay ransom or **INFECT 2 friends** to get **DATA** back

Popcorn time

# Protection against Ransomware



Isolate infected computer immediately



Do NOT pay ransom nor contact attacker



Perform regular backups on important data  
and keep an **offline** copy



Ensure that OS, software and anti-virus  
signatures are kept updated regularly



Do NOT open suspicious email attachments  
and website links



# Experts: **Don't reboot your computer** after you've been infected with ransomware

Rebooting may lead to restarting a crashed file-encryption process, potential loss of encryption keys stored in-memory.



By [Catalin Cimpanu](#) for [Zero Day](#) | November 5, 2019 --  
(23:28 GMT+08:00) | Topic: [Security](#)

Source: <https://www.zdnet.com/article/experts-dont-reboot-your-computer-after-youve-been-infected-with-ransomware/>

Method	Proportion
Restarted computer	30%
Online tool	18%
Restored computer from backup	22%
Removed by someone else	13%
Reformatted computer	5%
Removed using AV software	5%
Paid ransom	4%
Other means	3%

Table 5: *Self-reported means of dealing with the attack.*



# **Security Incidents Handling**

# SWT5



# Incident Reporting Basics (1)

- What actually happened?
- What the incident might mean for the organization?
- What is the impact?
- What system affected?
- What service affected?
- What actions had been taken?
- and etc.

**WHAT**



- Threat actor / IP address
- Attack source
- Hacking group
- Attack target
- Owner of targeted system
- Owner of involved business function
- Customers affected
- Parties involved
  - Internal
  - External
- and etc.

**WHO**



## Incident Reporting Basics (2)

- When the incident happened?
- When the incident being detected?
- Incident duration
- Incident timeline
  - Actions
  - Decisions
  - Information collected
- and etc.

**WHEN**



- Where is the attacks originated from?
- Attack paths
- Lateral movement
- Logical
  - Network zone
- Physical
  - Cloud
  - On-premises
- and etc.

**WHERE**





## Incident Reporting Basics (3)

- How does it happened?
- How the systems infected?
- What vulnerabilities exploited?
- Attack method
- Intrusion method
- Command and control
- Evade detection
- Obfuscation
- and etc.

**HOW**



- Why does it happened?
- Root cause
- and etc.

**WHY**



# Case Study | British Airways Data Breach Incident

EDITION: AS ▼



VIDEOS

EXECUTIVE GUIDES

SECURITY

CLOUD

INNOVATION

CXO

HARDWARE

MORE ▼

NEWSLETTERS

ALL WRITERS



MUST READ: [Mobile malware attacks are booming in 2019: These are the most common threats](#)

## GDPR: British Airways faces record £183m fine for customer data breach

Information Commissioner's Office intends to fine airline for "poor security arrangements" - British Airways says it's "surprised and disappointed" by planned penalty.



By [Danny Palmer](#) | July 8, 2019 -- 07:50 GMT (15:50 GMT+08:00) | Topic: [Security](#)



## Case Study | British Airways Data Breach Incident

### ❑ What affected?

- *Online booking website and the mobile app*

### ❑ What data had been stolen?

- *Customer's personal data (Names, billing address, email address)*
- *Credit card or debit card details*

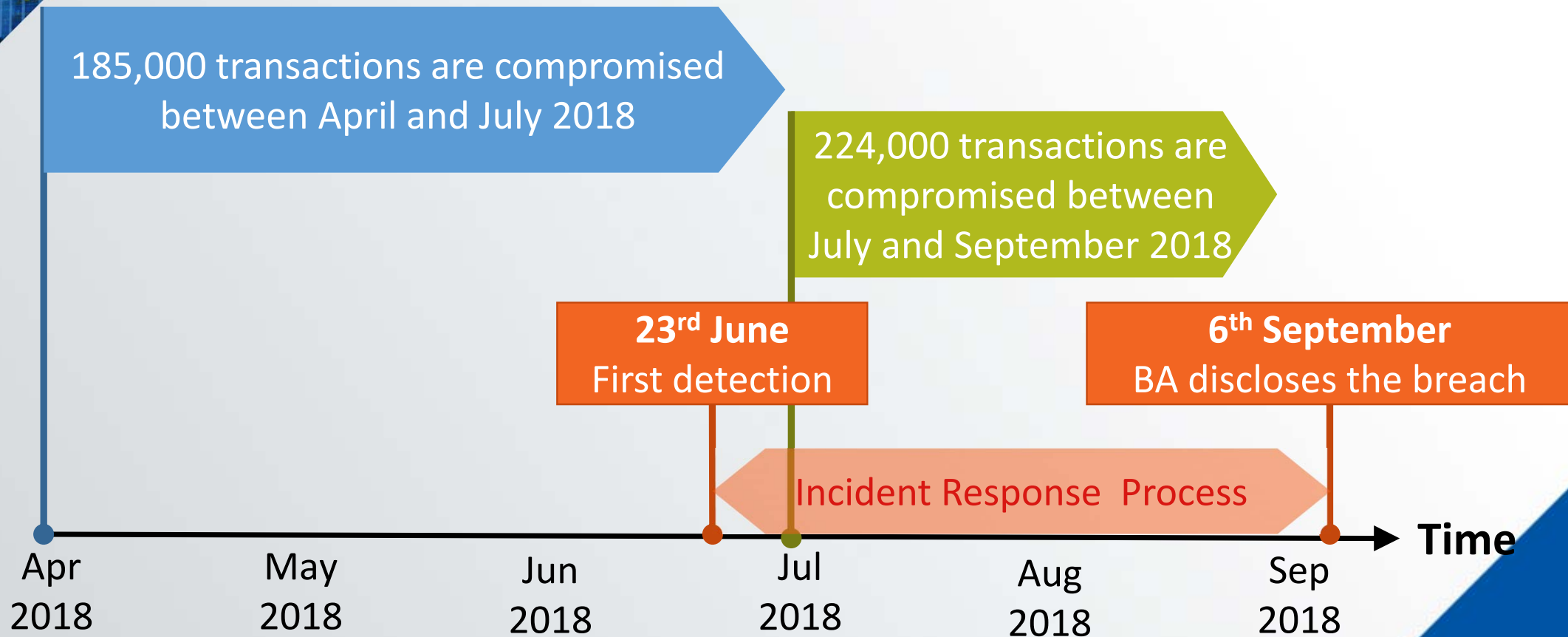
### ❑ How was it happened?

- *Breaching by hiding JavaScript code known as Magecart*
- *Customer booking data was sent to malicious site on submission*

### ❑ Why was it happened?

- *Vulnerabilities being exploited that cause JavaScript injection on Modernizr module*

# Case Study | British Airways Data Breach Incident





# **Security Advice Round Up**





# Being HACKED!?

A fisherman in a green jacket and hat is wading in a lake, holding a fishing rod and a net. A fish is on the line, and another fish is jumping out of the water nearby. The background shows a lake with hills in the distance under a cloudy sky.

What to do next???



If you have provided  
**login credentials**  
in suspicious  
website, please  
**reset password**  
and review the  
security settings in  
the related online  
service accounts

If you have  
provided **financial  
information**,  
such as credit card  
number, and incur  
financial loss,  
please **contact  
your bank  
immediately**







POLICE

You should **report to nearby police station** if any **financial loss** is incurred



If someone **spoofs**  
**your identity** to send  
email to your family,  
friends and business  
partners, you should  
**alert them by other**  
**trusted**  
**communication**  
**channels.**





The background is a blue-toned digital illustration of a server room. On the left, there are server racks. In the center, a person's silhouette is walking away from the viewer down a perspective-lined aisle. On the right, there are large, white, 3D gears of varying sizes. The floor is covered with binary code (0s and 1s). The ceiling has rectangular light fixtures. A semi-transparent white rectangular box is overlaid in the center-right, containing the text.

**Contact your  
IT Department** immediately!  
if you have one...



電腦資訊保安  
小錦囊

HKCERT Hotline

81056060

[www.hkcert.org](http://www.hkcert.org)





**Not being hack . . .**

**just YET !!!**

Image credit: <http://www.damazine.com/fishing-a-good-way-of-relaxing/>



# Cybersec Infohub

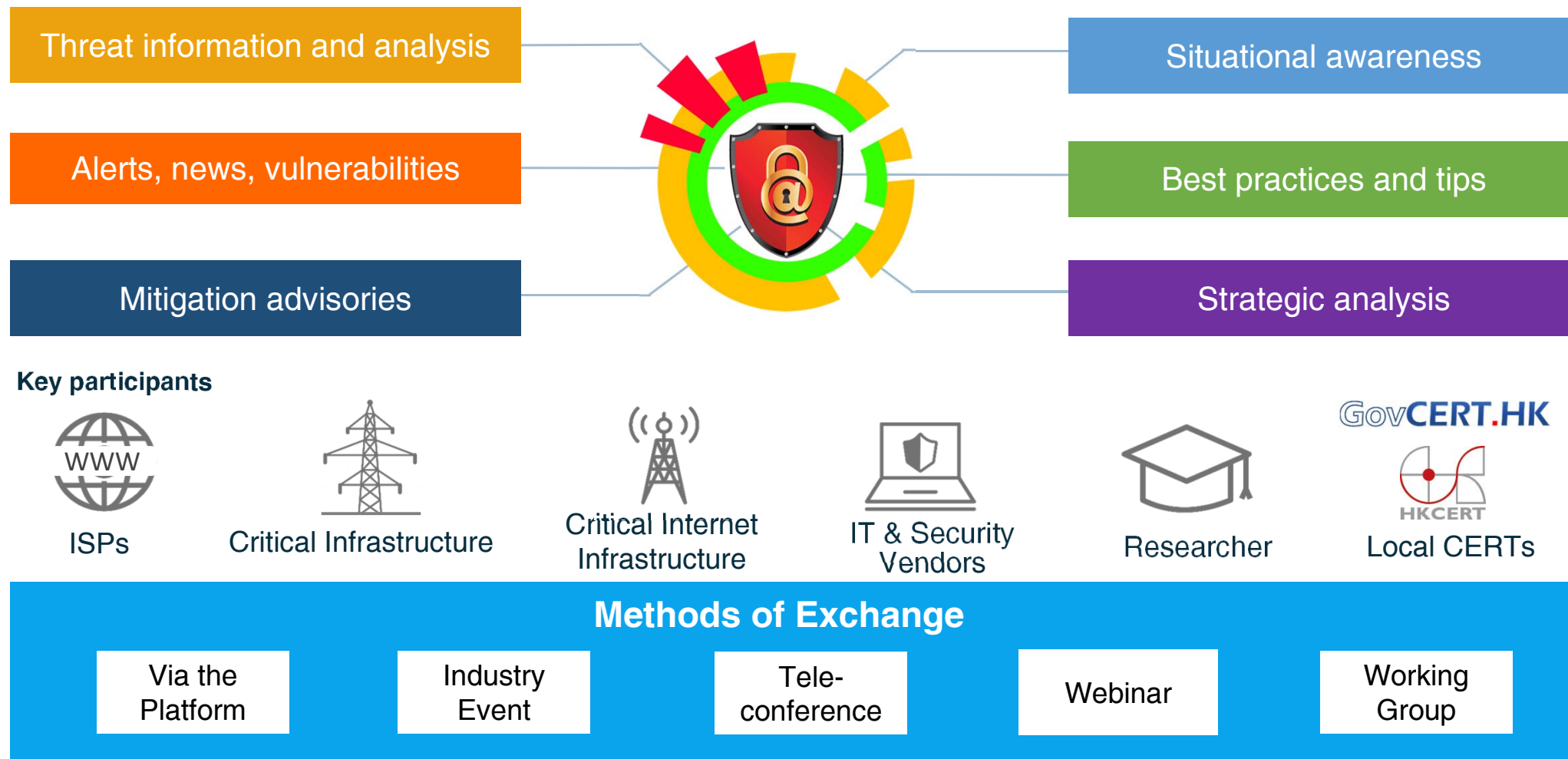
**Sharing**



**Trust**

**Collaboration**

# Cybersec Infohub





# Cybersechub.hk | Public Zone



# Cybersechub.hk | Members Zone

Traffic Light  
Protocol

User Anonymity

Export IOCs for  
Operation

Social Media  
“Like” Feature

“KOL” of  
Cybersechub.hk

Trusted Groups  
Discussion

Private  
Messaging

Directory for  
Connections



## Our Community

TLP:WHITE

**141**  
MEMBERS

---

**431**  
REPRESENTATIVES

### Distribution of Top Five Sectors



TLP:WHITE

## Our Community

**141**  
MEMBERS

---

**431**  
REPRESENTATIVES

### Distribution of Top Five Sectors



## Hot Discussion Topics

Top posts shared on Cybersecub.hk with good responses from members in August 2019:

- [iPhone Alert: Apple Accidentally Introduced A Critical Security Vulnerability In New iOS 12.4](#)
- [MAS Directive on Cyber Hygiene](#)
- [New Vulnerabilities in Remote Desktop Service \(RDS\) Affecting Most Current Windows Versions](#)
- [Shade 勒索軟件進一步活躍](#)
- [The Threat of BlueKeep \(CVE-2019-0708\) Becomes Imminent](#)
- [全能挖礦病毒 GroksterMiner 本報](#)

Note: The above posts are accessible to members only.

## Active Contributors

Our applause to the following representatives for their active contributions to Cybersecub.hk in August 2019:

<b>Ban CHENG</b> Sangfor Technologies (Hong Kong) Limited	<b>Chester LAU</b> Palo Alto Networks	<b>Claudius LAM</b> Trend Micro TrendLabs
<b>Harry POON</b> SmarTone Mobile Communications Limited	<b>Nick NG</b> Fortinet International, Inc.	<b>Peony CHUI</b> Lapcom Limited

# Hot Discussion Topics

Top posts shared on Cybersechub.hk with good responses from members in August 2019:



- [iPhone Alert: Apple Accidentally Introduced A Critical Security Vulnerability In New iOS 12.4](#)
- [MAS Directive on Cyber Hygiene](#)
- [New Vulnerabilities in Remote Desktop Service \(RDS\) Affecting Most Current Windows Versions](#)
- [Shade 勒索軟件進一步活躍](#)
- [The Threat of BlueKeep \(CVE-2019-0708\) Becomes Imminent](#)
- [全能挖礦病毒 GroksterMiner 來襲](#)

*Note: The above posts are accessible to members only.*

# Tips



## Change your password regularly

As a security best practice, user passwords for the Members Zone are configured to expire in every 180 days.

You can change your password anytime via the “Change Password” function at “Settings”.



## Want to share your professional advice to the public?

Create a TLP:WHITE post under “Advisories” or “Insights”, then click “Publish”.

Post will appear in the Public Zone upon confirmation by the Service Desk.



## Want to create a group for close-group discussion?

From menu “Group”, click “Create Group Request”. Fill in the required information and send the request to the Service Desk.

Communication within a Group is accessible to the Group members only.



## Events

### **Our first Cybersec Infohub Webinar –“Threat Intelligence and Exchange from Past to Future” on 16 August 2019**

On 16 August 2019, the first Cybersec Infohub webinar was held successfully, as a new channel to shore up our collaborative network. Thank you all the participants for joining the webinar, and we hope it was a fruitful one for everybody.



Can't wait for the next webinar? Stay tuned!



If you have missed the valuable sharing, you may find the presentation slides, video recording and follow-up discussions in the Members Zone.


(<https://www.cybersechub.hk/platform/threat/620?nav=informationSharing:General%20Discussion>)

# Cybersec Infohub



[cybersechub.hk](https://cybersechub.hk)

## Bring these messages back to your school.....

1. Everyone can be targeted, even you are just a **small potato** in your organization!!!!!!!!!!!!!!!!!!!!
  2. Set a **strong password** & enable **2FA** whenever possible
  3. Make sure your software / App are **up-to-date** & only download from reliable sources
  4. Do the **SAME** to your **home PC/laptop/mobile devices**
  5. Build your own **Human Firewall**
- 



# Question?





**Thank You** 



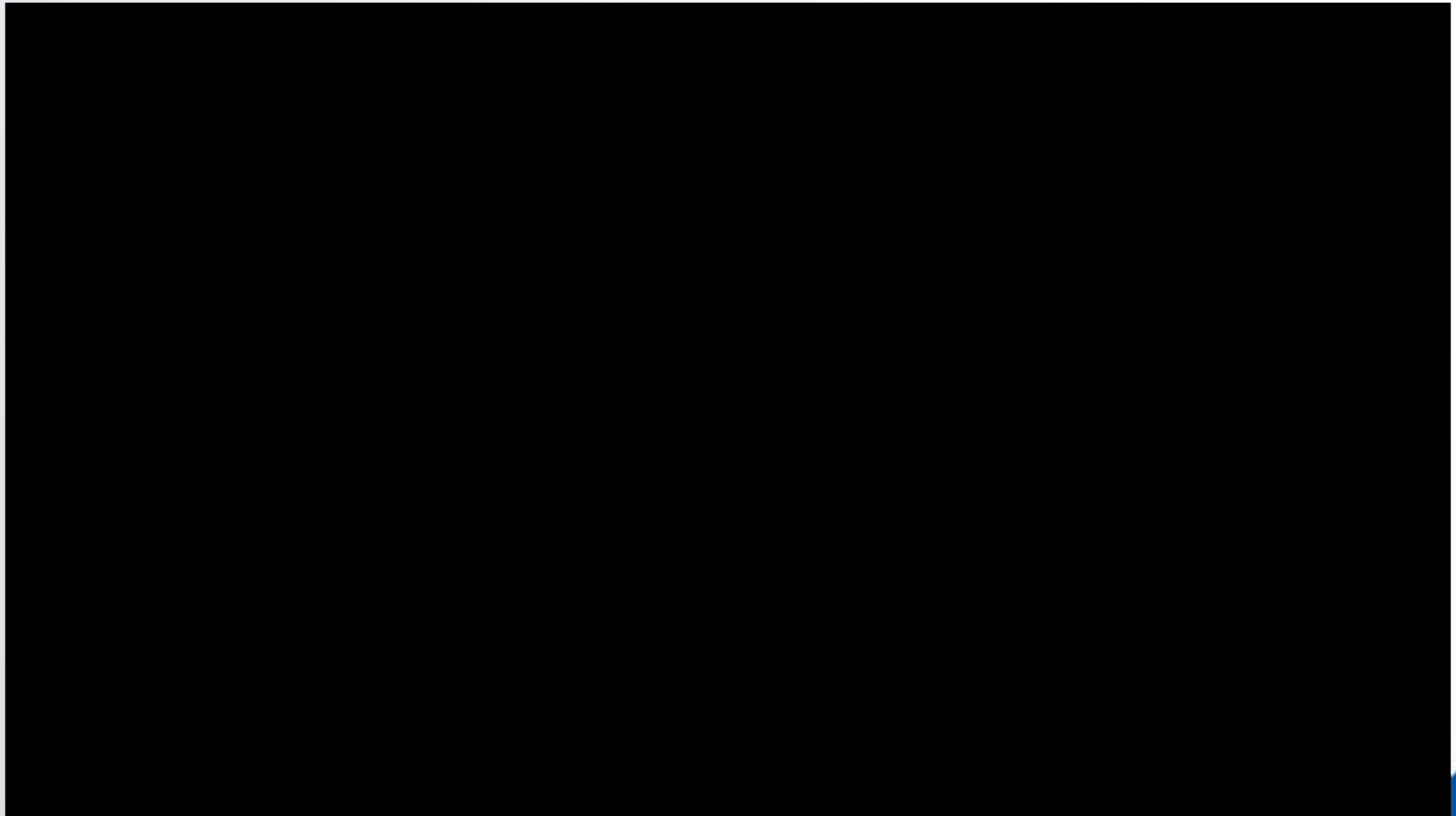




**Hong Kong Productivity Council**  
**香港生產力促進局**

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong  
香港九龍達之路78號生產力大樓  
**+852 2788 6168** [www.hkpc.org](http://www.hkpc.org)

## Canon DSLR Camera Infected with Ransomware Over the Air ANYTHING Can Be Targeted [video]



Source: <https://www.bleepingcomputer.com/news/security/canon-dslr-camera-infected-with-ransomware-over-the-air/>

## 中學生唔想上堂及考試！14歲仔驚天詭計又關DeepWeb事？



- Crime-as-a-Service
- Launch of cyber attacks are much easier than we can think of nowadays!



- Are you ready to face all these challenges?

數碼生活

👍 讚好 0

撰文：黃正軒

🕒 2019-04-15 16:30

最後更新日期：2019-05-02 20:00



Image credit: [Rawpixel.com](https://www.rawpixel.com)



## Malware | *Propagation Channels*

### Executable

- Fake security software / mobile app
- Fake video player codec

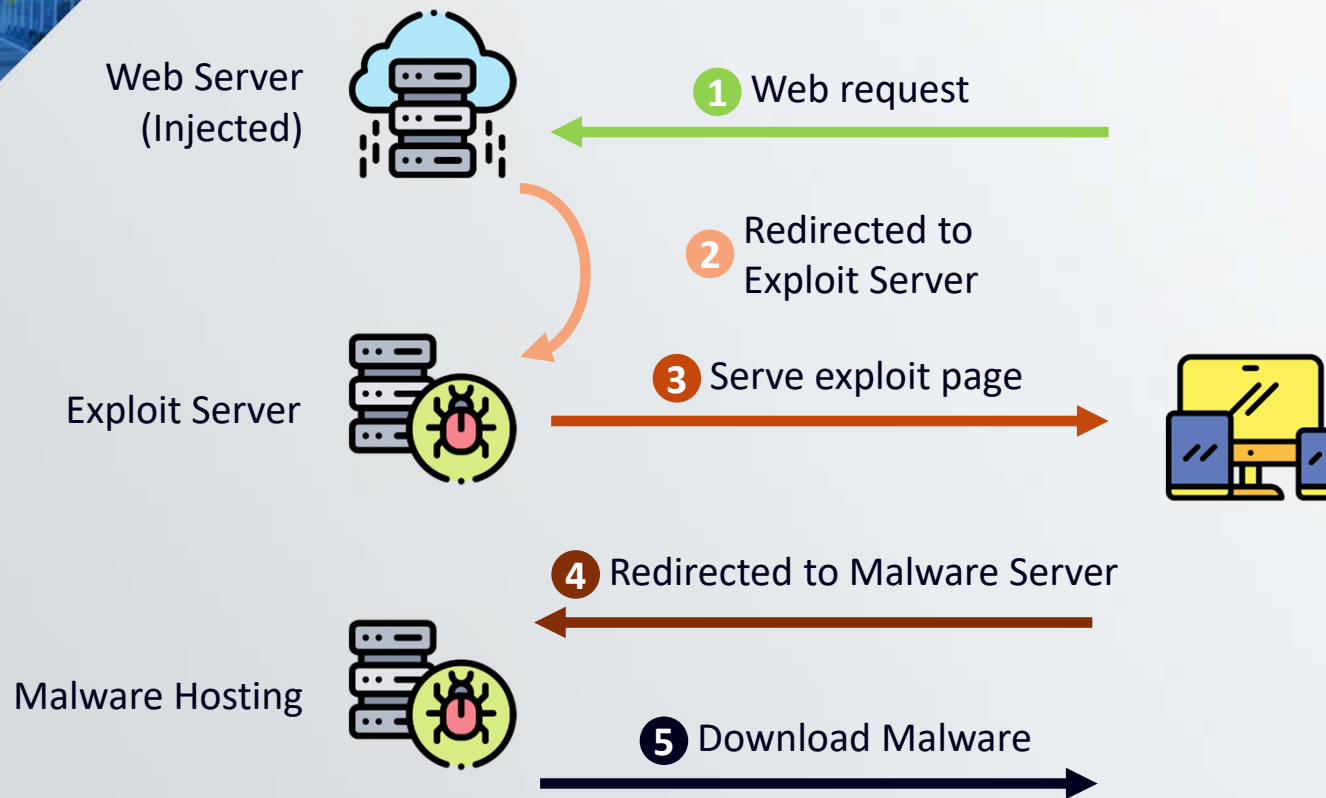
### Document Malware ★

- Embedded malware in PDF or Office files
- Botnet served PDF malware

### Website ★★

- Legitimate and trusted websites compromised
- Web admin incapable to detect and mitigate the risks

# Multi-Stage Malware Infection | *Drive-by Download*



- Exploits imported from other servers via iframes, redirects
- When compromised, dropper download and install the actual bot malware

# Botnet (roBot Network)

Infrastructure of Controlled Victim Computers (BOTs)

