Building a Cooperative Model to Counter New Methods in Phishing Distribution

Presented by:
Alban Kwan, regional director, East Asia

November 24, 2022 | Proprietary and Confidential

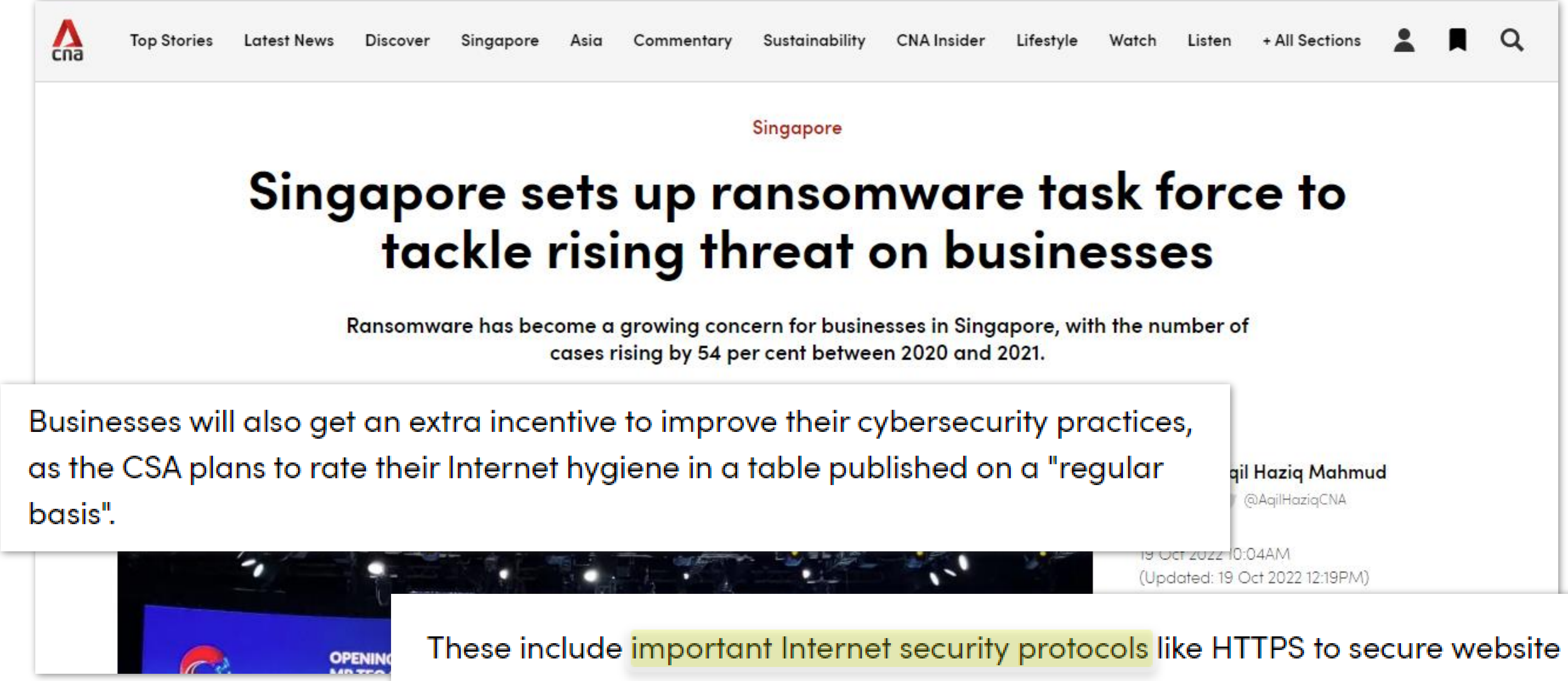
Topic of discussion

How can anti-phishing be improved by including the ‘crowd’?

Who are the ‘crowd’?

What problem does it solve that is otherwise unsolvable?

New Cybersecurity Initiative by Singapore Government



Singapore

Singapore sets up ransomware task force to tackle rising threat on businesses

Ransomware has become a growing concern for businesses in Singapore, with the number of cases rising by 54 per cent between 2020 and 2021.

qil Haziq Mahmud
@AqilHaziqCNA

19 Oct 2022 10:04AM
(Updated: 19 Oct 2022 12:19PM)

Businesses will also get an extra incentive to improve their cybersecurity practices, as the CSA plans to rate their Internet hygiene in a table published on a "regular basis".

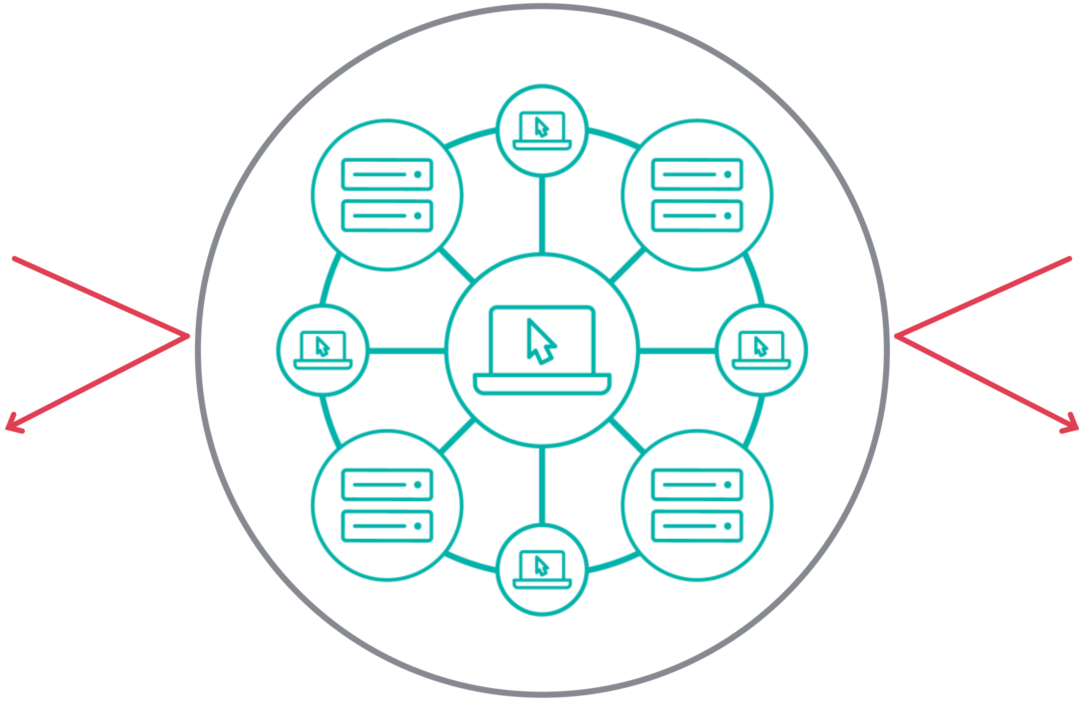
These include important Internet security protocols like HTTPS to secure website communications between parties, DNSSEC to prevent DNS spoofing, hijacking and cache poisoning, and DMARC to prevent email spoofing.

Businesses will be given a green tick, yellow tick or red cross, depending on how many Internet best practices they have implemented.

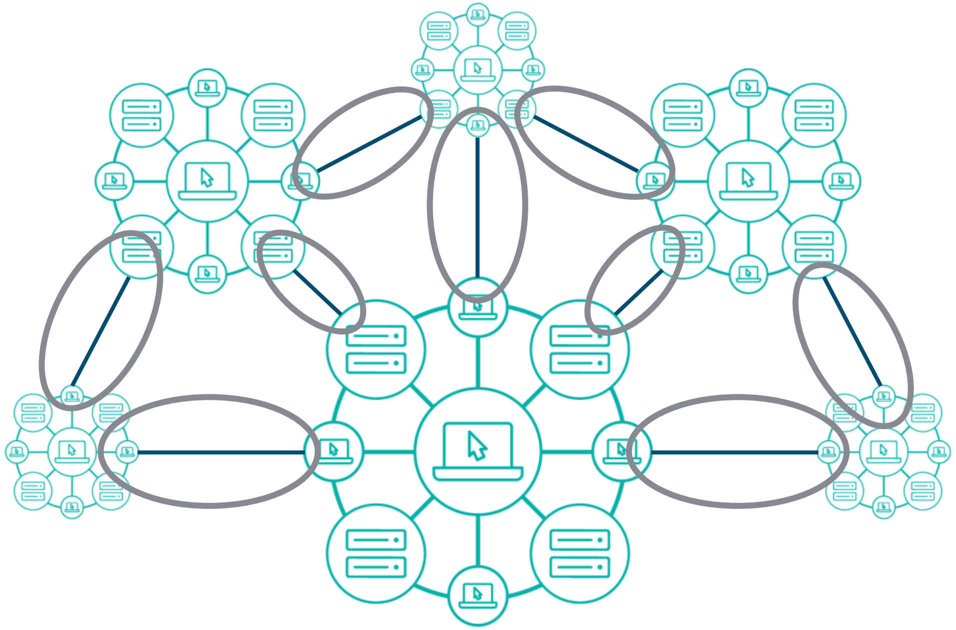
https://www.channelnewsasia.com/singapore/ransomware-task-force-singapore-internet-cybersecurity-practices-3014046

We Live Under Two Systems: Network and Inter-Network

NETWORK SECURITY



INTER-NETWORK SECURITY

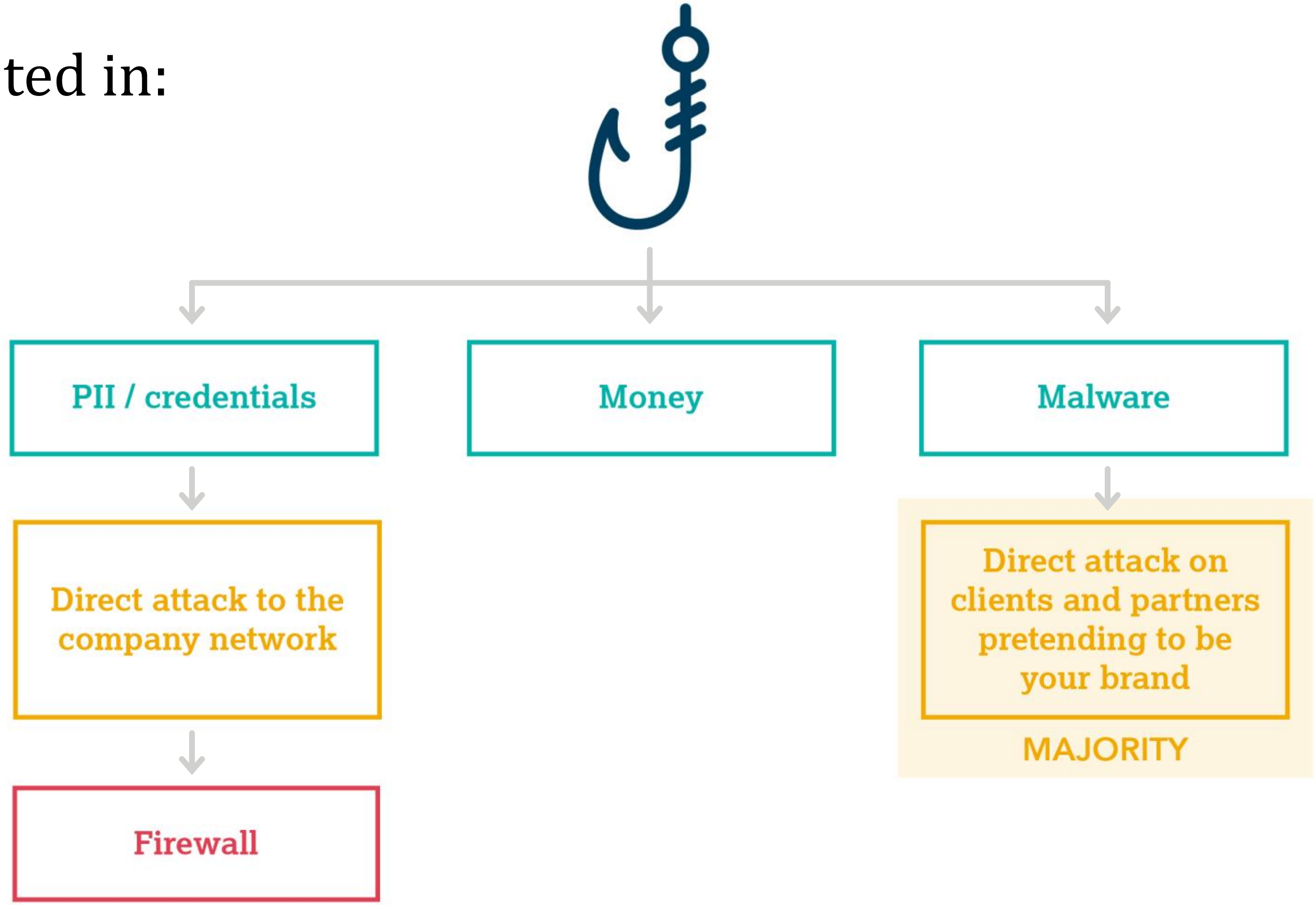


CSC

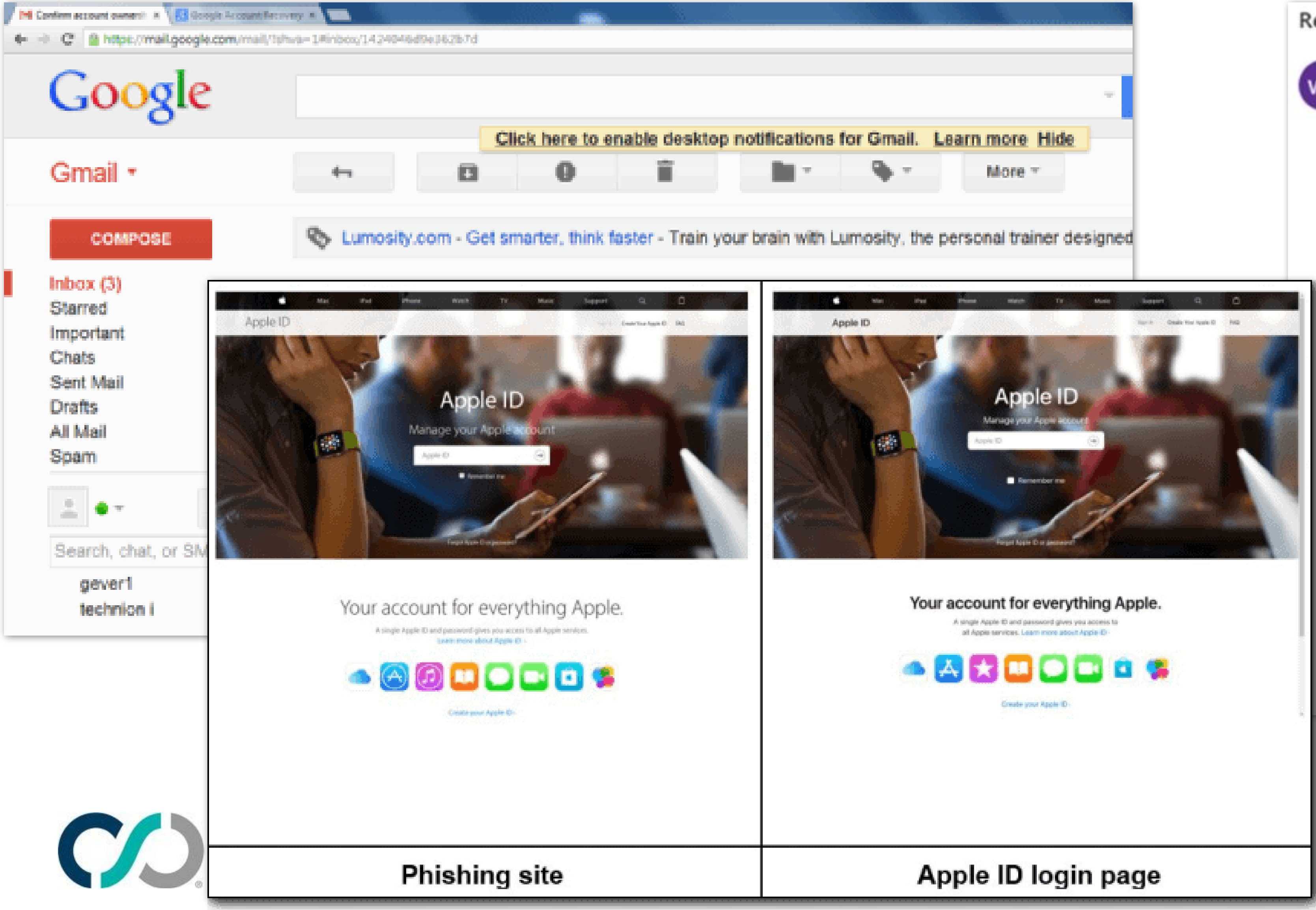
Two Types of Phishing Attacks

Corporations most likely have invested in:

- Firewall
- Anti-phishing email gateway
- Domain detection
- DMARC


PII / credentials
Money
Malware
Direct attack to the company network
Firewall
Direct attack on clients and partners pretending to be your brand
MAJORITY

Example: Phishing Using Your Brand



Click here to enable desktop notifications for Gmail. Learn more Hide

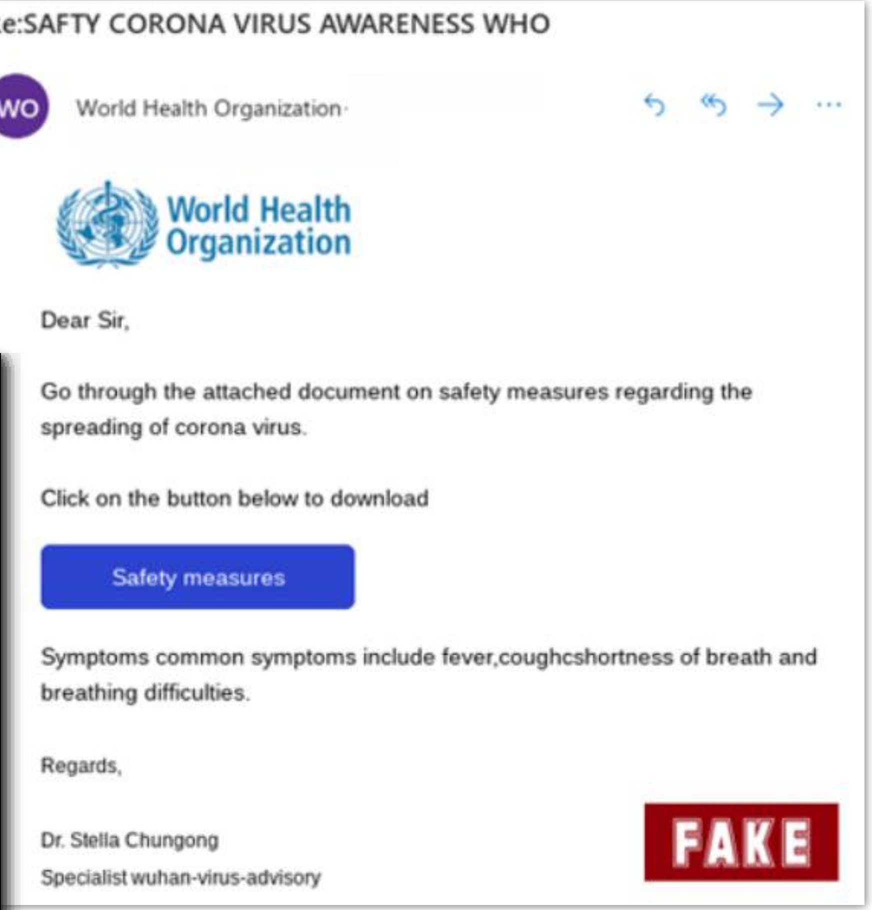
Lumosity.com - Get smarter, think faster - Train your brain with Lumosity, the personal trainer designed

Your account for everything Apple.

Your account for everything Apple.

Phishing site

Apple ID login page



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

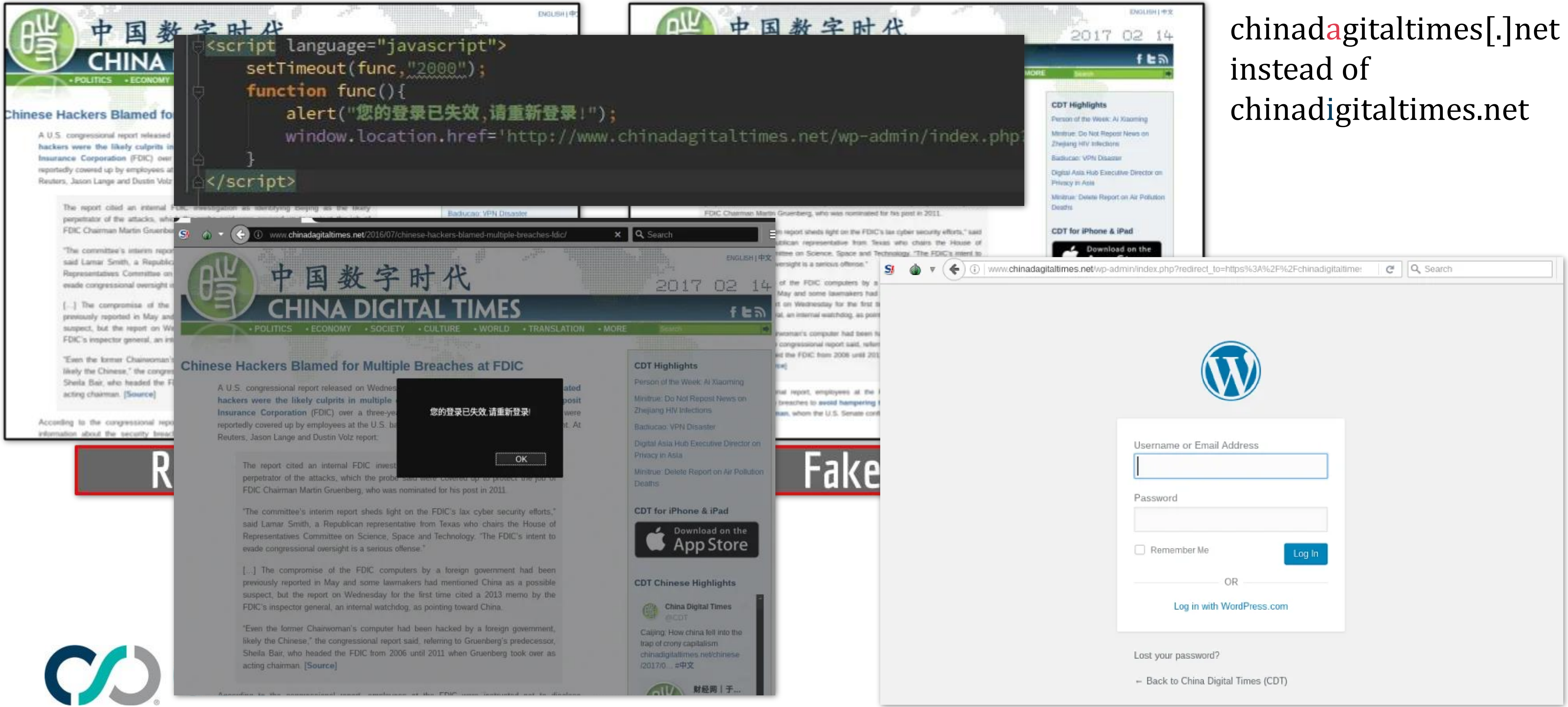
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

Chinese Phishing Case From CitizenLab



```
<script language="javascript">
    setTimeout(func,"2000");
    function func(){
        alert("您的登录已失效,请重新登录!");
        window.location.href='http://www.chinadagitaltimes.net/wp-admin/index.php
    }
</script>
```

www.chinadagitaltimes.net/2016/07/chinese-hackers-blamed-multiple-breaches-fdic/

中国数字时代 CHINA DIGITAL TIMES 2017 02 14

Chinese Hackers Blamed for Multiple Breaches at FDIC

A U.S. congressional report released on Wednes… hackers were the likely culprits in multiple … Insurance Corporation (FDIC) over a three-ye… were reportedly covered up by employees at the U.S. ba… At Reuters, Jason Lange and Dustin Volz report:

The report cited an internal FDIC invest… perpetrator of the attacks, which the probe said were covered up to protect the job of FDIC Chairman Martin Gruenberg, who was nominated for his post in 2011.

"The committee's interim report sheds light on the FDIC's lax cyber security efforts," said Lamar Smith, a Republican representative from Texas who chairs the House of Representatives Committee on Science, Space and Technology. "The FDIC's intent to evade congressional oversight is a serious offense."

[…] The compromise of the FDIC computers by a foreign government had been previously reported in May and some lawmakers had mentioned China as a possible suspect, but the report on Wednesday for the first time cited a 2013 memo by the FDIC's inspector general, an internal watchdog, as pointing toward China.

"Even the former Chairwoman's computer had been hacked by a foreign government, likely the Chinese," the congressional report said, referring to Gruenberg's predecessor, Sheila Bair, who headed the FDIC from 2006 until 2011 when Gruenberg took over as acting chairman. [Source]

您的登录已失效,请重新登录!

CDT Highlights

Person of the Week: Ai Xiaoming

Minitrue: Do Not Repost News on Zhejiang HIV Infections

Baducao: VPN Disaster

Digital Asia Hub Executive Director on Privacy in Asia

Minitrue: Delete Report on Air Pollution Deaths

CDT for iPhone & iPad

CDT Chinese Highlights

China Digital Times @CDT

Caijing: How china fell into the trap of crony capitalism chinadigitaltimes.net/chinese/2017/0… #中文

www.chinadagitaltimes.net/wp-admin/index.php?redirect_to=https%3A%2F%2Fchinadigitaltime

Username or Email Address

Password

□ Remember Me

OR

Log in with WordPress.com

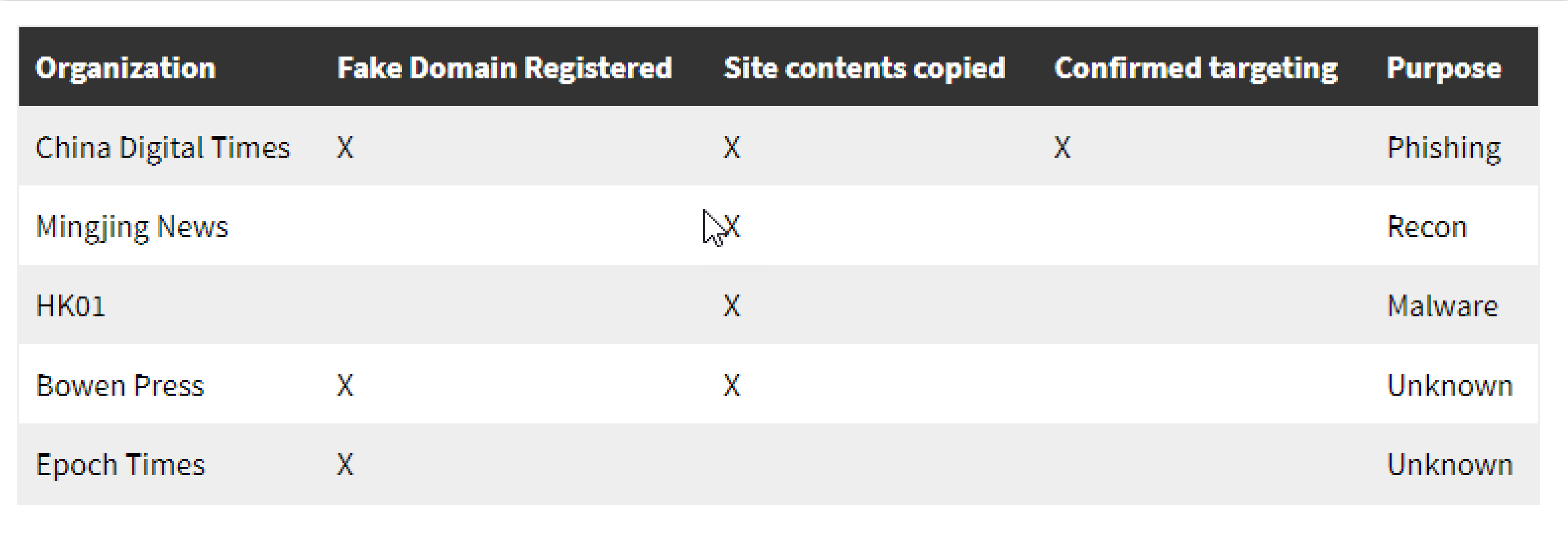
Lost your password?

← Back to China Digital Times (CDT)

chinadagitaltimes[.]net instead of chinadigitaltimes.net

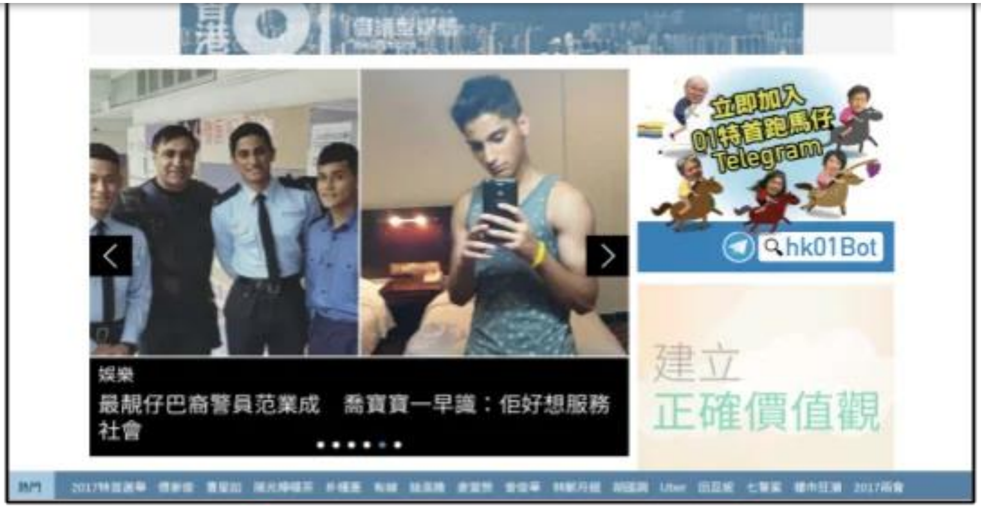
https://citizenlab.ca/2017/07/insider-information-an-intrusion-campaign-targeting-chinese-language-news-sites/

Chinese Phishing Case From CitizenLab

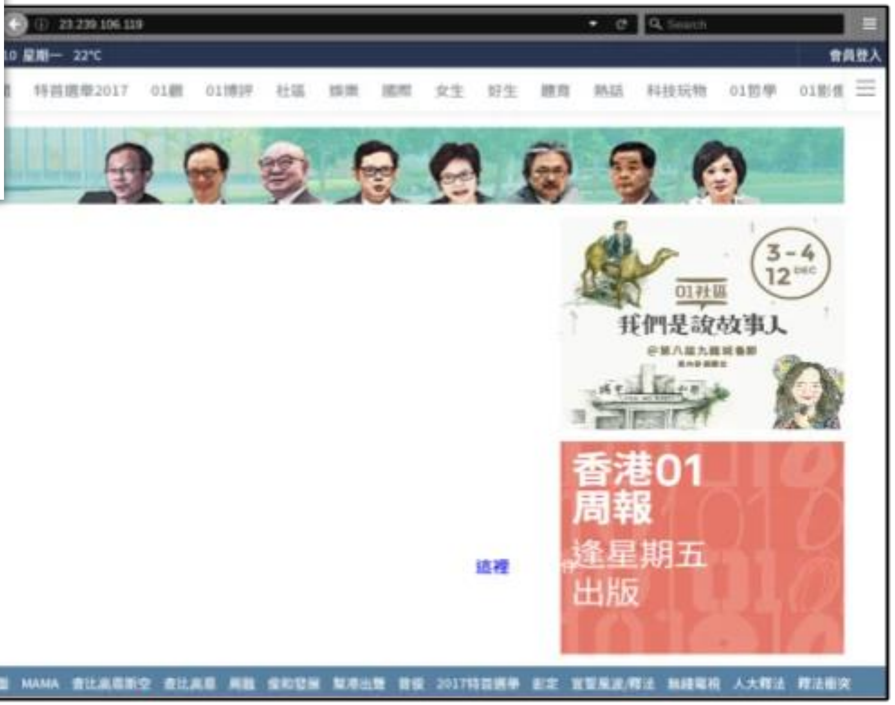


Organization	Fake Domain Registered	Site contents copied	Confirmed targeting	Purpose
China Digital Times	X	X	X	Phishing
Mingjing News		X		Recon
HK01		X		Malware
Bowen Press	X	X		Unknown
Epoch Times	X			Unknown

Hosted by HK based hosting provider
Cloudie HK

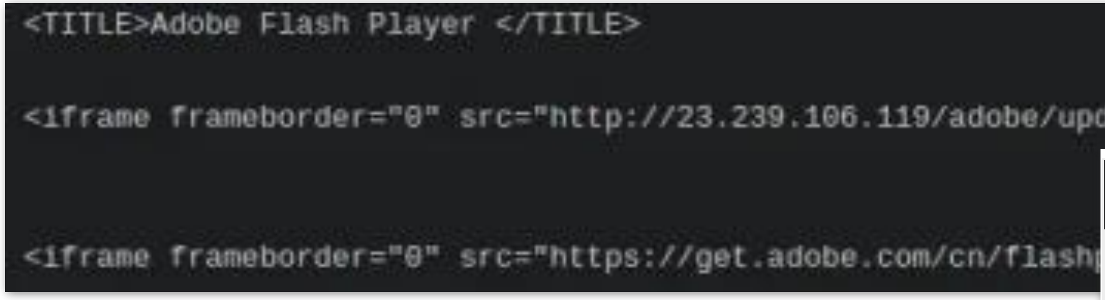


Real HK01 Site



Fake HK01 Site

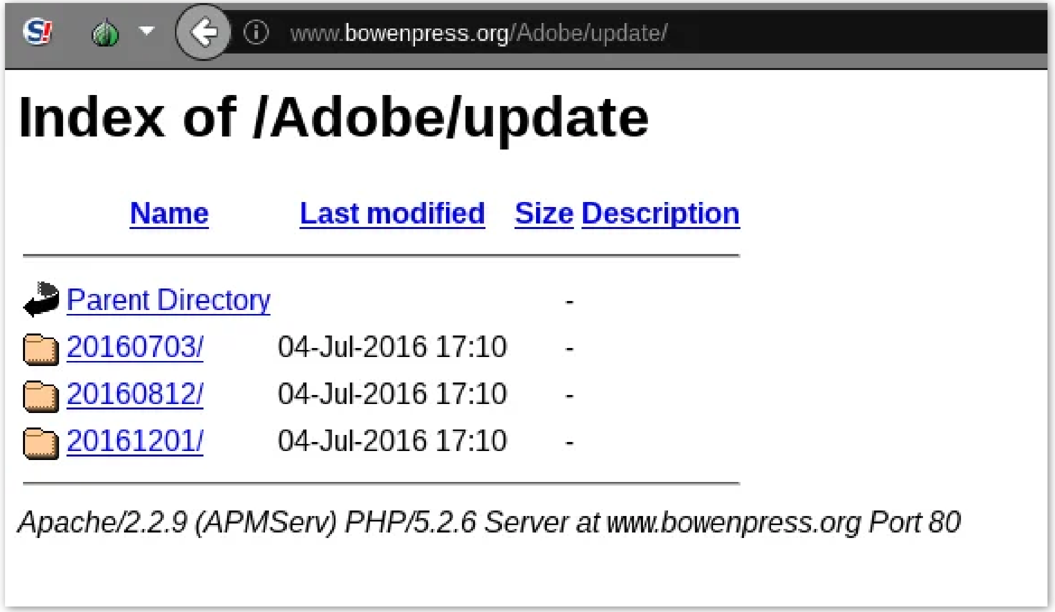
Chinese Phishing Case From CitizenLab



```
<TITLE>Adobe Flash Player </TITLE>

<iframe frameborder="0" src="http://23.239.106.119/adobe/update/20161201/AdobeUpdate20161201.exe" width="0" height="0"> </iframe>

<iframe frameborder="0" src="https://get.adobe.com/cn/flash
```

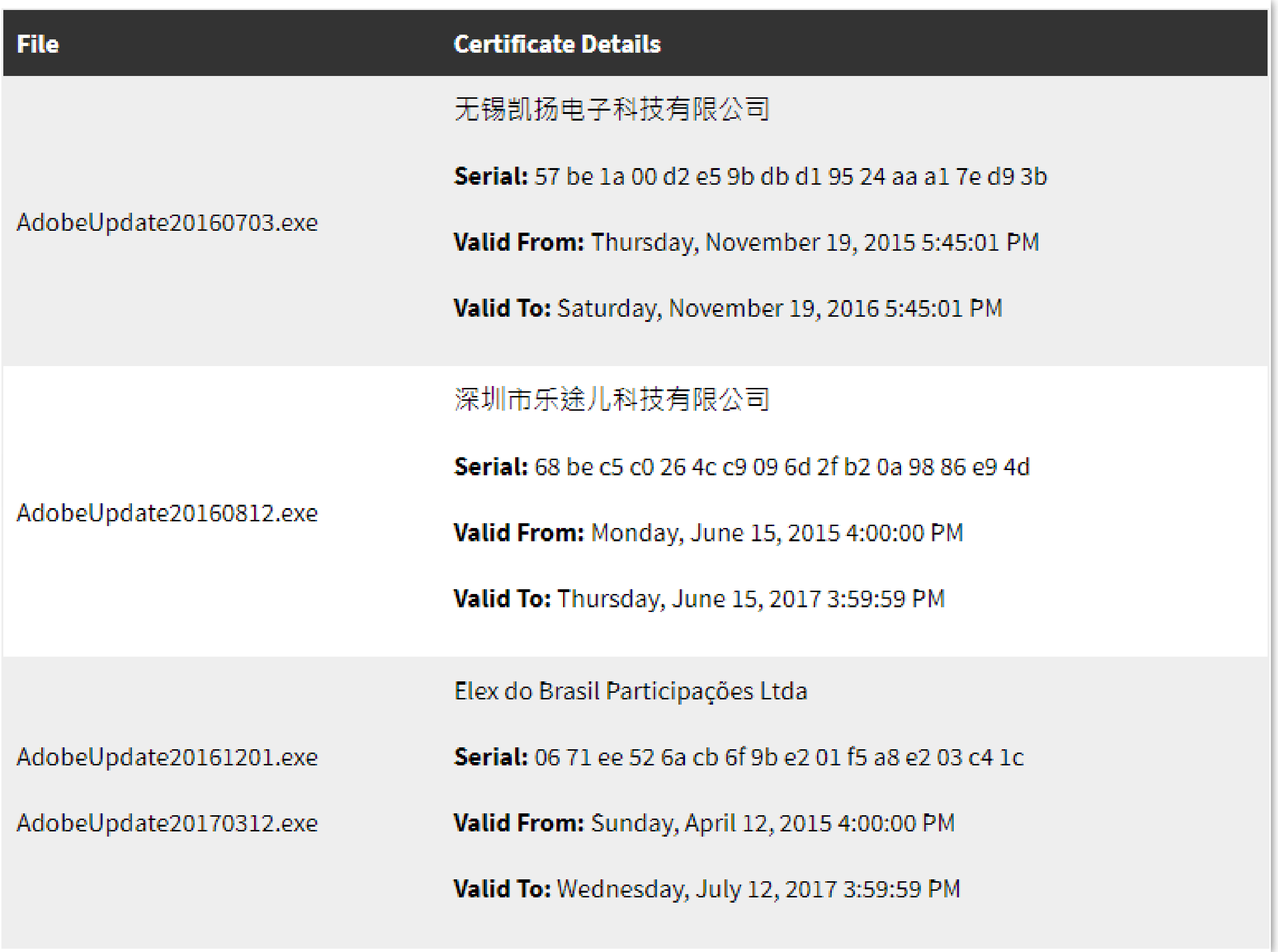


Index of /Adobe/update

```
      Name            Last modified      Size  Description
------------------------------------------------------------
 Parent Directory                          -
 20160703/        04-Jul-2016 17:10       -
 20160812/        04-Jul-2016 17:10       -
 20161201/        04-Jul-2016 17:10       -
------------------------------------------------------------
Apache/2.2.9 (APMServ) PHP/5.2.6 Server at www.bowenpress.org Port 80
```

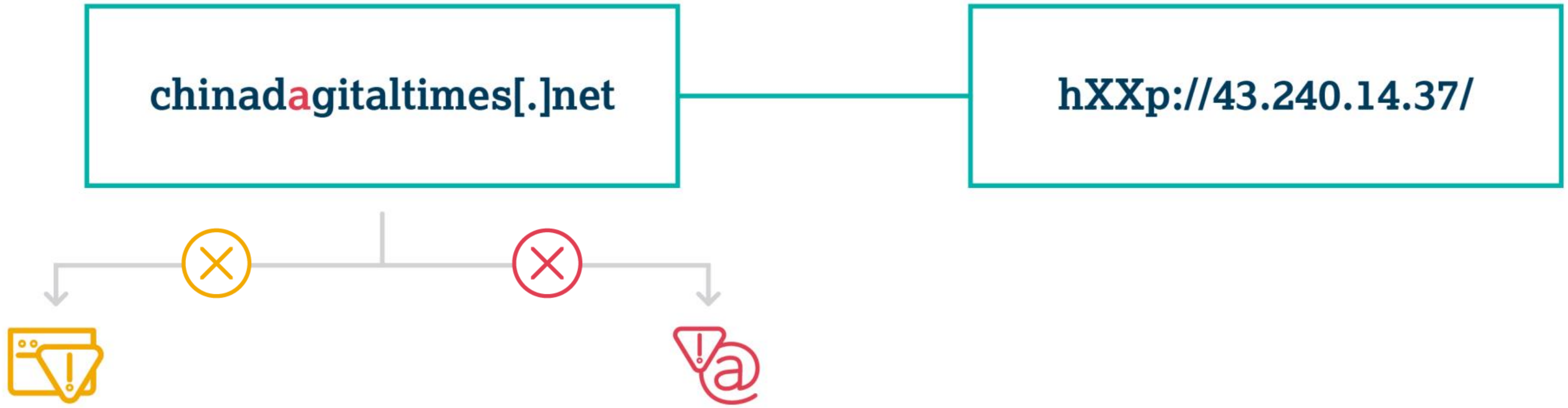
Netwire RAT

(Remote Access Tool)



File	Certificate Details
AdobeUpdate20160703.exe	无锡凯扬电子科技有限公司 **Serial:** 57 be 1a 00 d2 e5 9b db d1 95 24 aa a1 7e d9 3b **Valid From:** Thursday, November 19, 2015 5:45:01 PM **Valid To:** Saturday, November 19, 2016 5:45:01 PM
AdobeUpdate20160812.exe	深圳市乐途儿科技有限公司 **Serial:** 68 be c5 c0 26 4c c9 09 6d 2f b2 0a 98 86 e9 4d **Valid From:** Monday, June 15, 2015 4:00:00 PM **Valid To:** Thursday, June 15, 2017 3:59:59 PM
AdobeUpdate20161201.exe AdobeUpdate20170312.exe	Elex do Brasil Participações Ltda **Serial:** 06 71 ee 52 6a cb 6f 9b e2 01 f5 a8 e2 03 c4 1c **Valid From:** Sunday, April 12, 2015 4:00:00 PM **Valid To:** Wednesday, July 12, 2017 3:59:59 PM

Why is it Hard to Detect This?



chinadagitaltimes[.]net

hXXp://43.240.14.37/

DOMAIN MONITORING

What if they use another domain that is hard to detect?

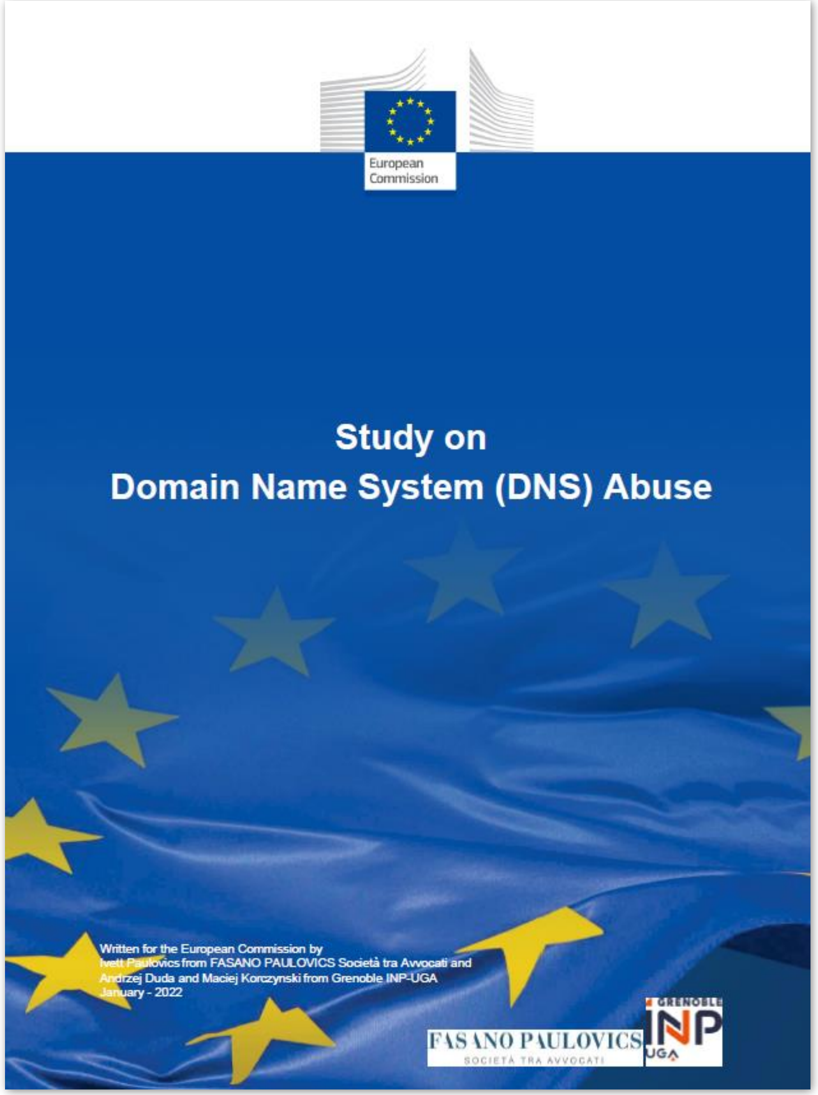
EMAIL TRAPS

What if this is distributed via **private or social channels**

- Telegram
- SMS
- WeChat
- Facebook®

The Nature of Phishing Attacks

- Phishing is defined as part of **DNS ABUSE**
- Recognized by the Internet Industries
  - ICANN
  - UN’s Internet Governance Forum (IGF)
  - INTA
  - Internet Society (ISOC)
- A high priority by global governments
  - One of the highest priorities in GAC (Government Advisory Committee) within ICANN



European Commission

Study on
Domain Name System (DNS) Abuse

Written for the European Commission by
Ivett Paulovics from FASANO PAULOVICS Società tra Avvocati and
Andrzej Duda and Maciej Korczynski from Grenoble INP-UGA
January - 2022

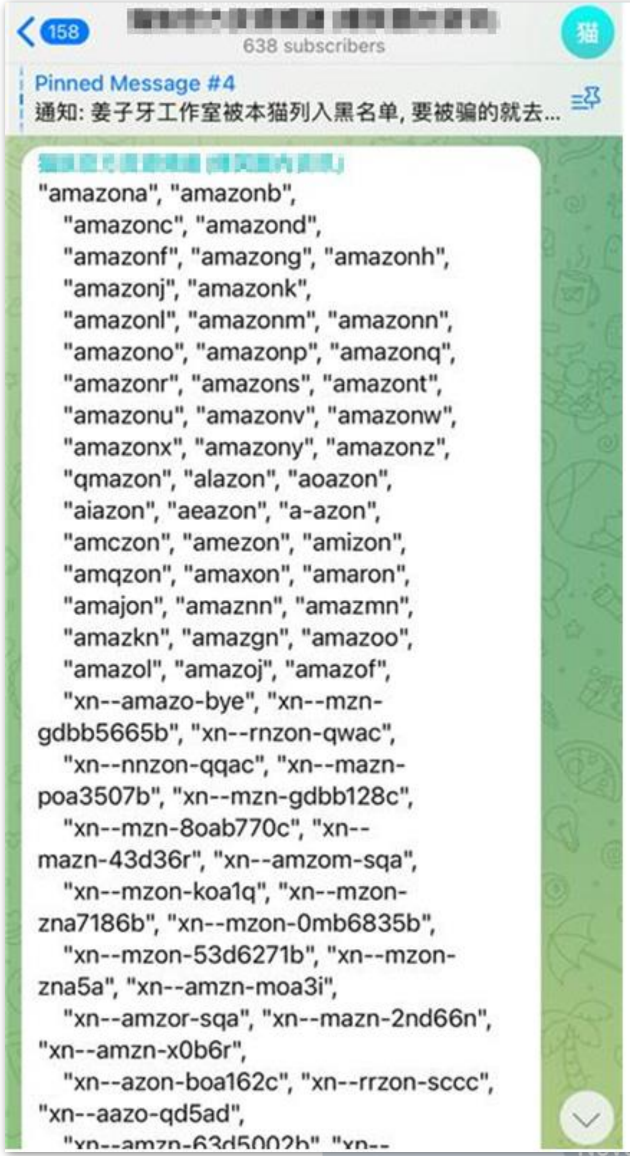
FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

CSC

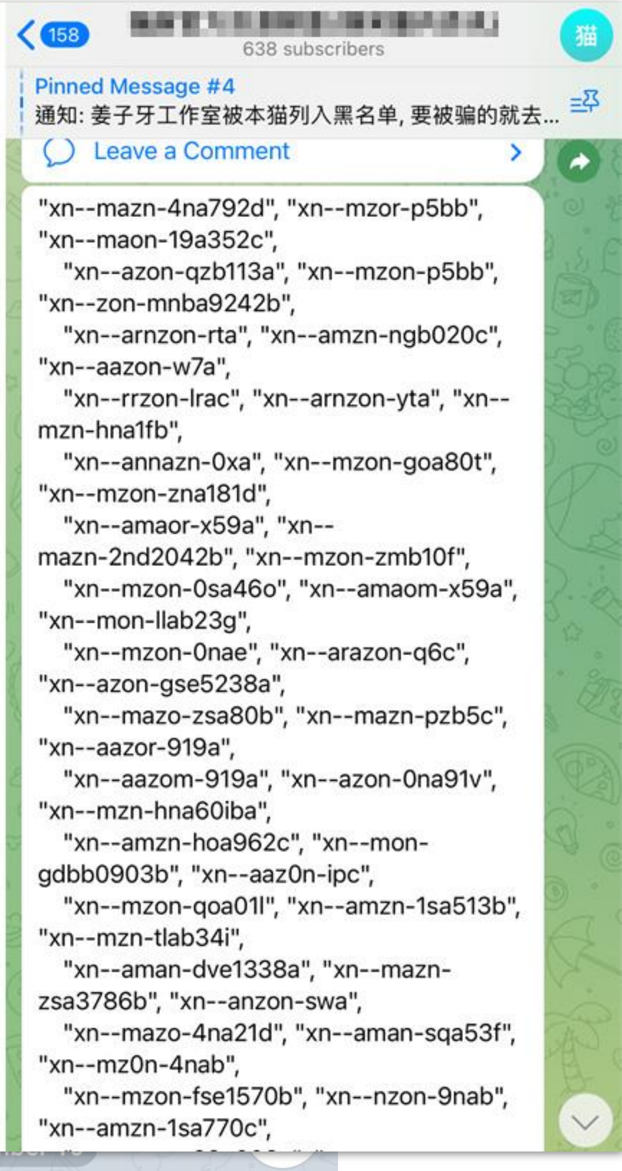
Domain as a Cornerstone of Phishing Attack

- Telegram phishing group – Chinese
- Sending out all the different variations of domains to be used to phish against “Amazon”
    - Typo
    - Fuzzy
    - Cousin
    - IDN homoglyph



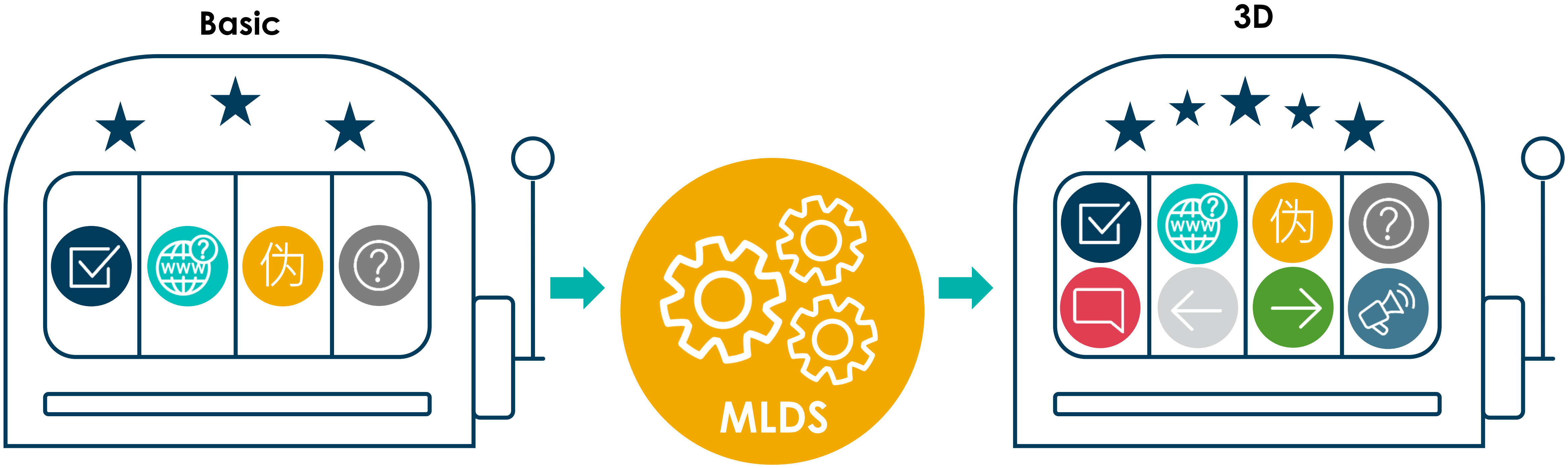
[redacted]

```
"amazona", "amazonb",
   "amazonc", "amazond",
   "amazonf", "amazong", "amazonh",
   "amazonj", "amazonk",
   "amazonl", "amazonm", "amazonn",
   "amazono", "amazonp", "amazonq",
   "amazonr", "amazons", "amazont",
   "amazonu", "amazonv", "amazonw",
   "amazonx", "amazony", "amazonz",
   "qmazon", "alazon", "aoazon",
   "aiazon", "aeazon", "a-azon",
   "amczon", "amezon", "amizon",
   "amqzon", "amaxon", "amaron",
   "amajon", "amaznn", "amazmn",
   "amazkn", "amazgn", "amazoo",
   "amazol", "amazoj", "amazof",
   "xn--amazo-bye", "xn--mzn-
gdbb5665b", "xn--rnzon-qwac",
   "xn--nnzon-qqac", "xn--mazn-
poa3507b", "xn--mzn-gdbb128c",
   "xn--mzn-8oab770c", "xn--
mazn-43d36r", "xn--amzom-sqa",
   "xn--mzon-koa1q", "xn--mzon-
zna7186b", "xn--mzon-0mb6835b",
   "xn--mzon-53d6271b", "xn--mzon-
zna5a", "xn--amzn-moa3i",
   "xn--amzor-sqa", "xn--mazn-2nd66n",
"xn--amzn-x0b6r",
   "xn--azon-boa162c", "xn--rrzon-sccc",
"xn--aazo-qd5ad",
   "xn--amzn-63d5002b", "xn--
```



```
"xn--mazn-4na792d", "xn--mzor-p5bb",
"xn--maon-19a352c",
   "xn--azon-qzb113a", "xn--mzon-p5bb",
"xn--zon-mnba9242b",
   "xn--arnzon-rta", "xn--amzn-ngb020c",
"xn--aazon-w7a",
   "xn--rrzon-lrac", "xn--arnzon-yta", "xn--
mzn-hna1fb",
   "xn--annazn-0xa", "xn--mzon-goa80t",
"xn--mzon-zna181d",
   "xn--amaor-x59a", "xn--
mazn-2nd2042b", "xn--mzon-zmb10f",
   "xn--mzon-0sa46o", "xn--amaom-x59a",
"xn--mon-llab23g",
   "xn--mzon-0nae", "xn--arazon-q6c",
"xn--azon-gse5238a",
   "xn--mazo-zsa80b", "xn--mazn-pzb5c",
"xn--aazor-919a",
   "xn--aazom-919a", "xn--azon-0na91v",
"xn--mzn-hna60iba",
   "xn--amzn-hoa962c", "xn--mon-
gdbb0903b", "xn--aaz0n-ipc",
   "xn--mzon-qoa01l", "xn--amzn-1sa513b",
"xn--mzn-tlab34i",
   "xn--aman-dve1338a", "xn--mazn-
zsa3786b", "xn--anzon-swa",
   "xn--mazo-4na21d", "xn--aman-sqa53f",
"xn--mz0n-4nab",
   "xn--mzon-fse1570b", "xn--nzon-9nab",
"xn--amzn-1sa770c",
```

New Engine Developed To Address Next-Generation Domain Monitoring



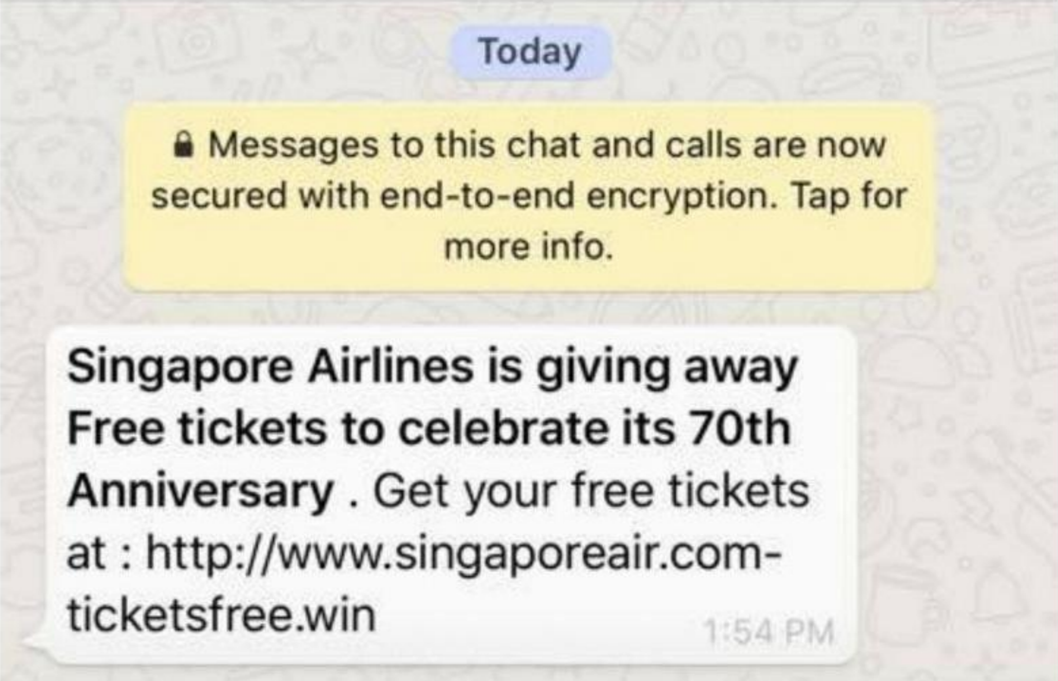
Exact match: cscglobal123.com
Typo: csbglobal.com
IDN: 美国人 *Chinese Domain Variation*
Wildcard Search: csc?lobal.com

Exact match: cscglobal123.com
Typo: csbglobal.com
IDN: 美国人 *Chinese Domain Variation*
Wildcard Search: csc?lobal.com
Regex: csceglobal.com

Fuzzy: cscg1obal.com
Homoglyphs: ćscglobal.com
Homophones: siesiglobal.com
Cousin: cscglobal.jp
AND Left side, Right side….

What if They Send It Through Private Channels?

Singapore Airlines warns of phishing scam promising free plane tickets



Today

🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

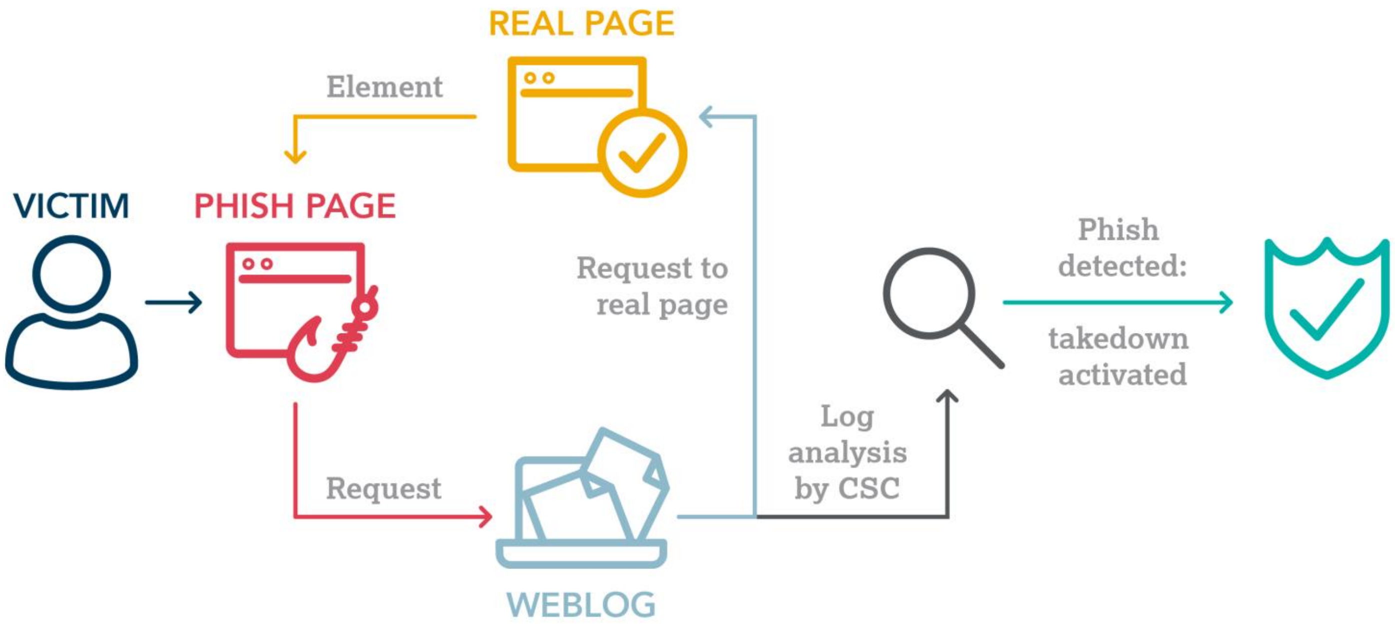
Singapore Airlines is giving away Free tickets to celebrate its 70th Anniversary . Get your free tickets at : http://www.singaporeair.com-ticketsfree.win

1:54 PM

A WhatsApp message included a link to a website masquerading as SIA's own, which offered free tickets as prizes before asking for personal data. PHOTO: ST READER

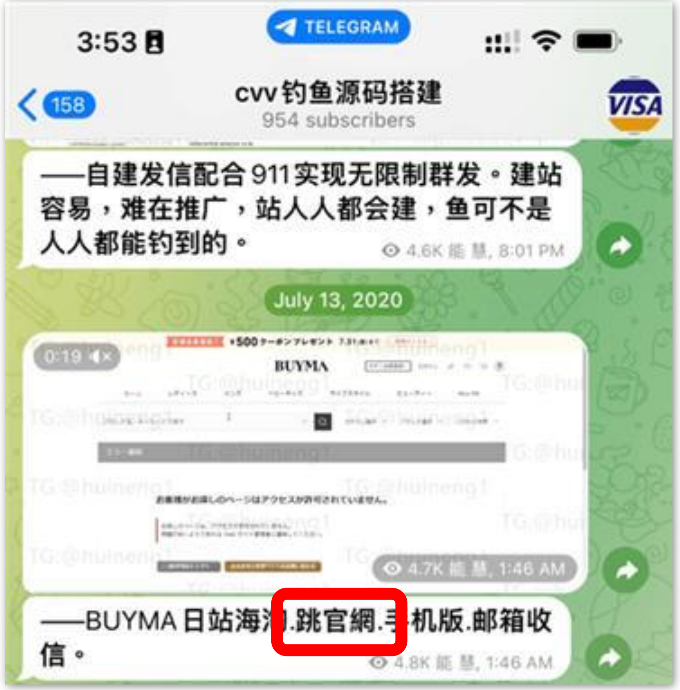
Capturing Phishing Via Private Channel

- No active monitoring possible
- Method is to cooperate with the brand with weblog integration
- The phishing page requests an element or circles back to the real site
- The scammer tests the page before the phishing campaign is sent
- Redirect victim back to real site to lower their awareness



CSC

Phishing Kit Promotion by Chinese Phisher “CVV”



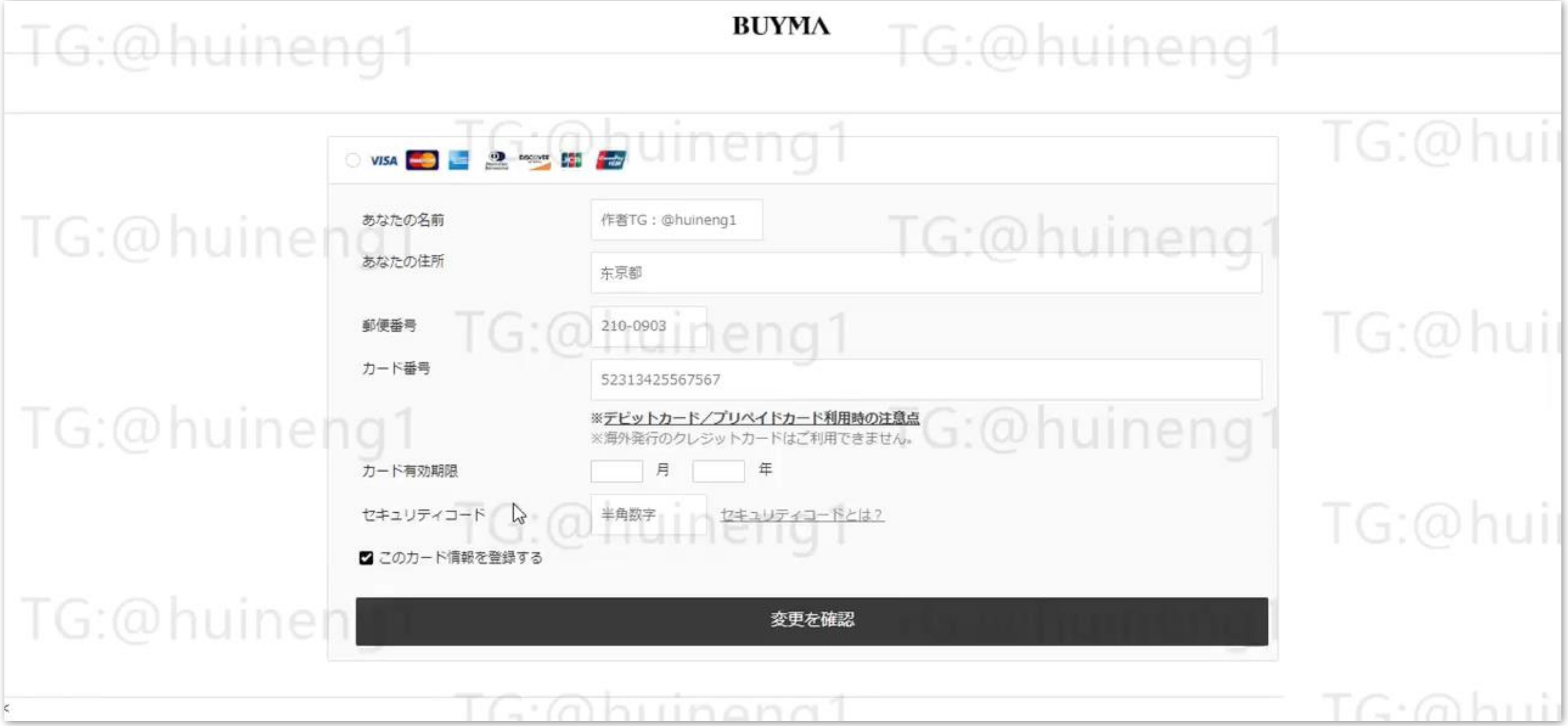
cvv钓鱼源码搭建
954 subscribers

——自建发信配合 911实现无限制群发。建站容易，难在推广，站人人都会建，鱼可不是人人都能钓到的。
4.6K 能 慧, 8:01 PM

July 13, 2020

0:19
4.7K 能 慧, 1:46 AM

——BUYMA 日站海淘.跳官網.手机版.邮箱收信。
4.8K 能 慧, 1:46 AM



BUYMA

あなたの名前	作者TG：@huineng1
あなたの住所	东京都
郵便番号	210-0903
カード番号	52313425567567

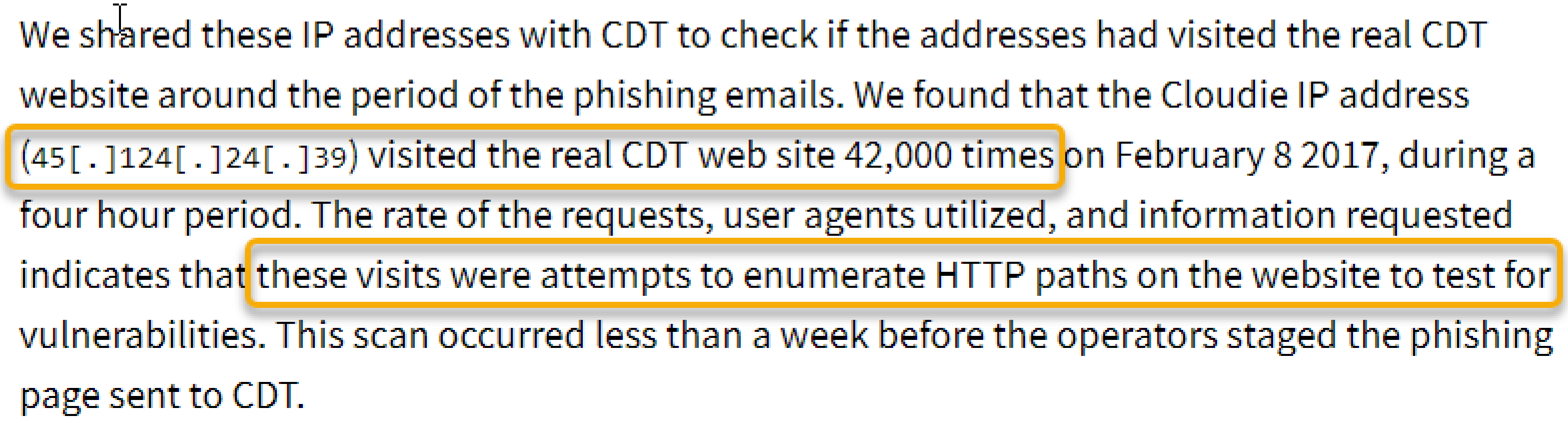
※デビットカード／プリペイドカード利用時の注意点
※海外発行のクレジットカードはご利用できません。

カード有効期限	月 年
セキュリティコード	半角数字 セキュリティコードとは？

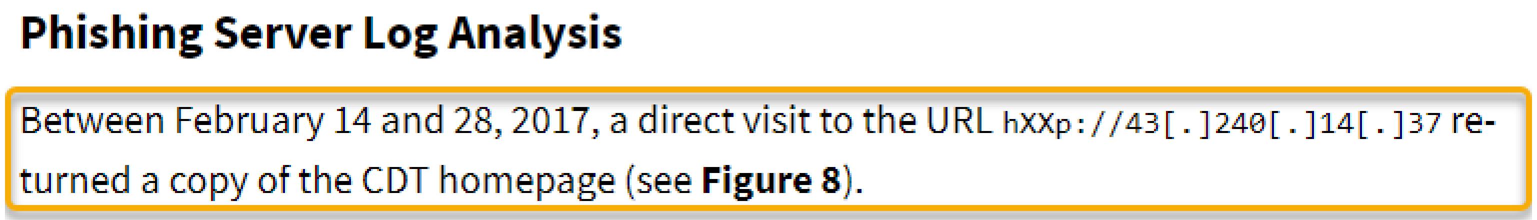
☑ このカード情報を登録する

CSC

Back to the China Digital Times Case



We shared these IP addresses with CDT to check if the addresses had visited the real CDT website around the period of the phishing emails. We found that the Cloudie IP address (`45[.]124[.]24[.]39`) visited the real CDT web site 42,000 times on February 8 2017, during a four hour period. The rate of the requests, user agents utilized, and information requested indicates that these visits were attempts to enumerate HTTP paths on the website to test for vulnerabilities. This scan occurred less than a week before the operators staged the phishing page sent to CDT.



Phishing Server Log Analysis

Between February 14 and 28, 2017, a direct visit to the URL `hXXp://43[.]240[.]14[.]37` returned a copy of the CDT homepage (see **Figure 8**).

Benefits of Weblog Integration

PREEMPTIVE DETECTION

Detect fraud as it’s being configured and before a phishing campaign is launched.

ODD EMAIL

Identify fraud attempts not found on regular fraud channels.

TARGET METRICS

Assess the number of potential victims derived from each scam.

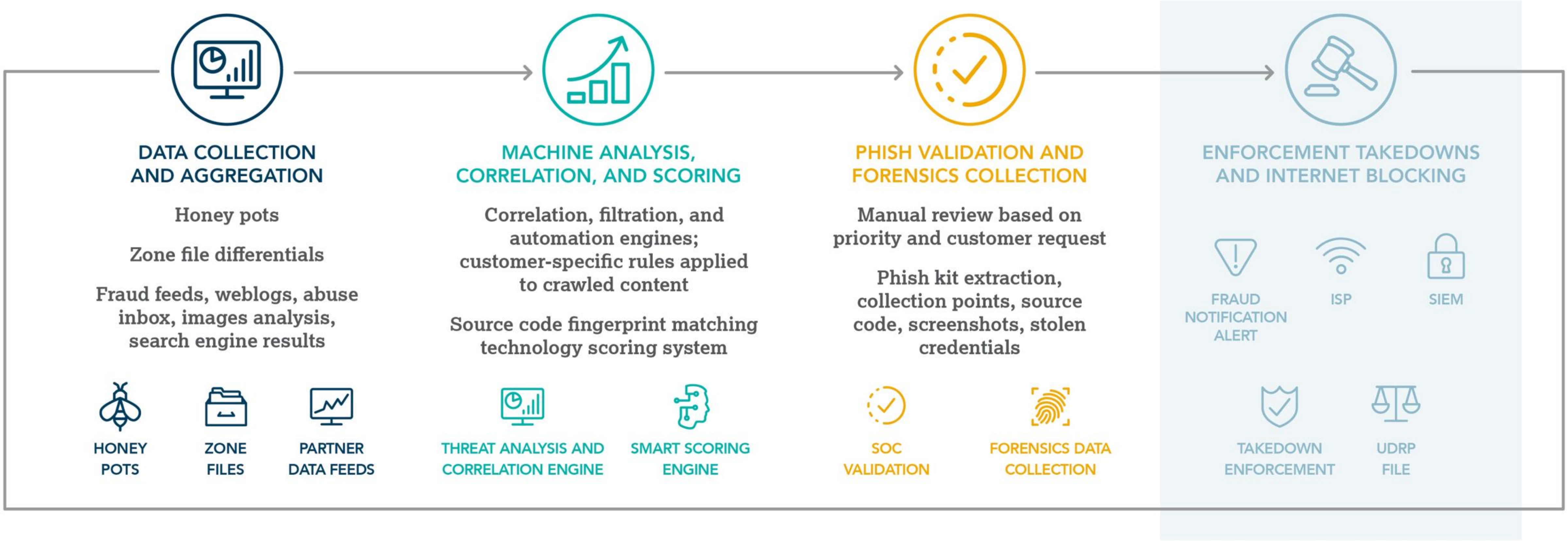
CLOSER TO LIVE PROTECTION

Increased frequency in weblog data sharing brings our clients closer to live detection.

1st Cooperation model:

Anti-fraud monitoring provider and brand owner

Fraud Protection Architecture



DATA COLLECTION AND AGGREGATION

Honey pots

Zone file differentials

Fraud feeds, weblogs, abuse inbox, images analysis, search engine results

HONEY POTS

ZONE FILES

PARTNER DATA FEEDS

MACHINE ANALYSIS, CORRELATION, AND SCORING

Correlation, filtration, and automation engines; customer-specific rules applied to crawled content

Source code fingerprint matching technology scoring system

THREAT ANALYSIS AND CORRELATION ENGINE

SMART SCORING ENGINE

PHISH VALIDATION AND FORENSICS COLLECTION

Manual review based on priority and customer request

Phish kit extraction, collection points, source code, screenshots, stolen credentials

SOC VALIDATION

FORENSICS DATA COLLECTION

ENFORCEMENT TAKEDOWNS AND INTERNET BLOCKING

FRAUD NOTIFICATION ALERT

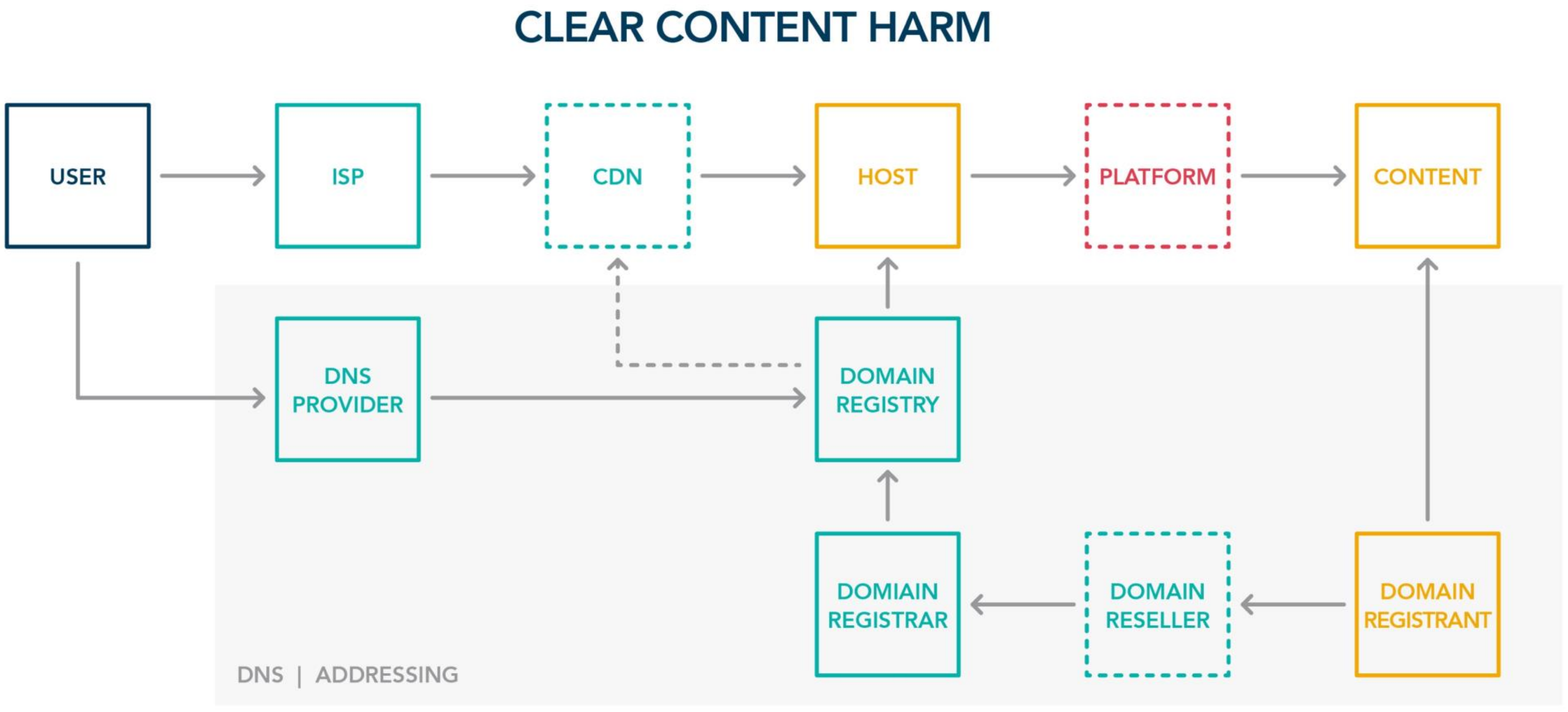
ISP

SIEM

TAKEDOWN ENFORCEMENT

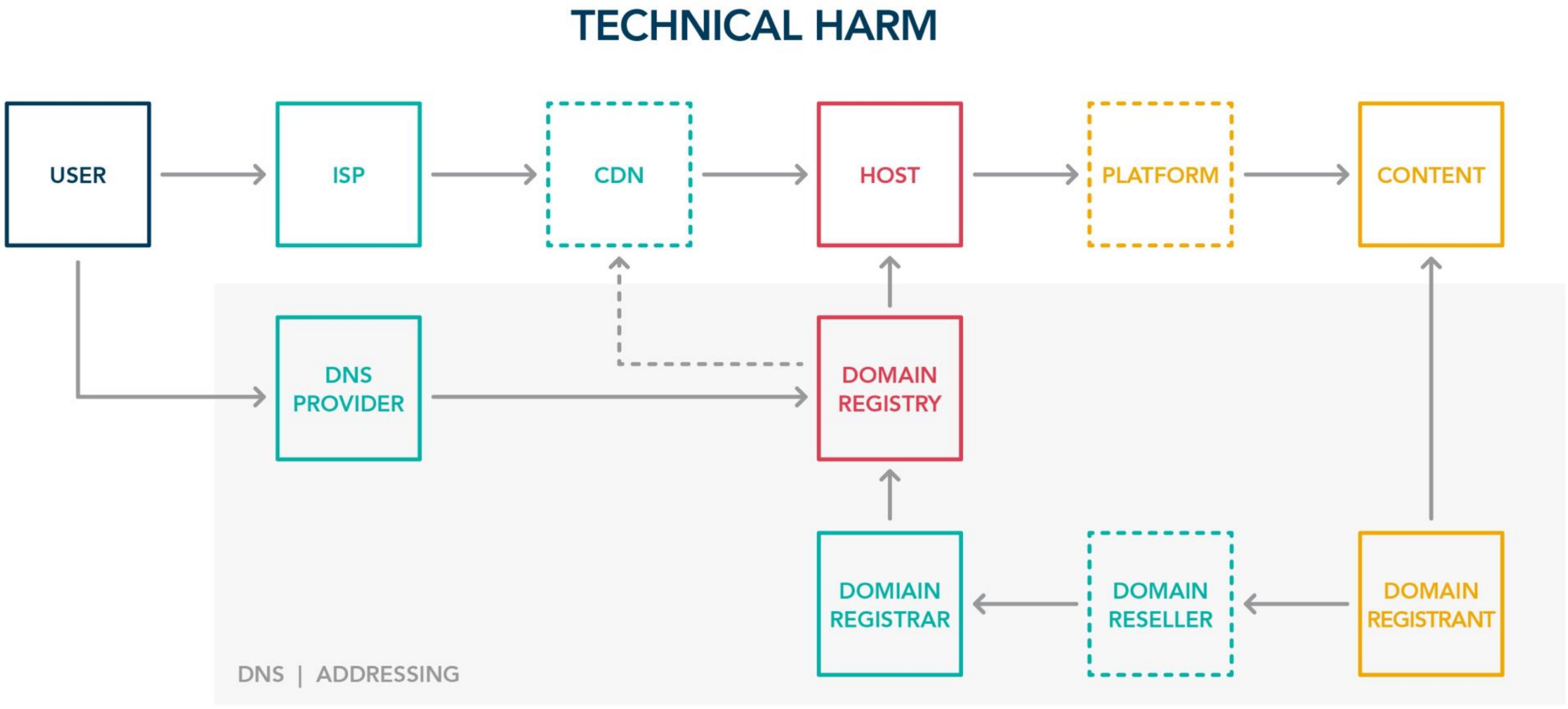
UDRP FILE

Problems with Enforcement



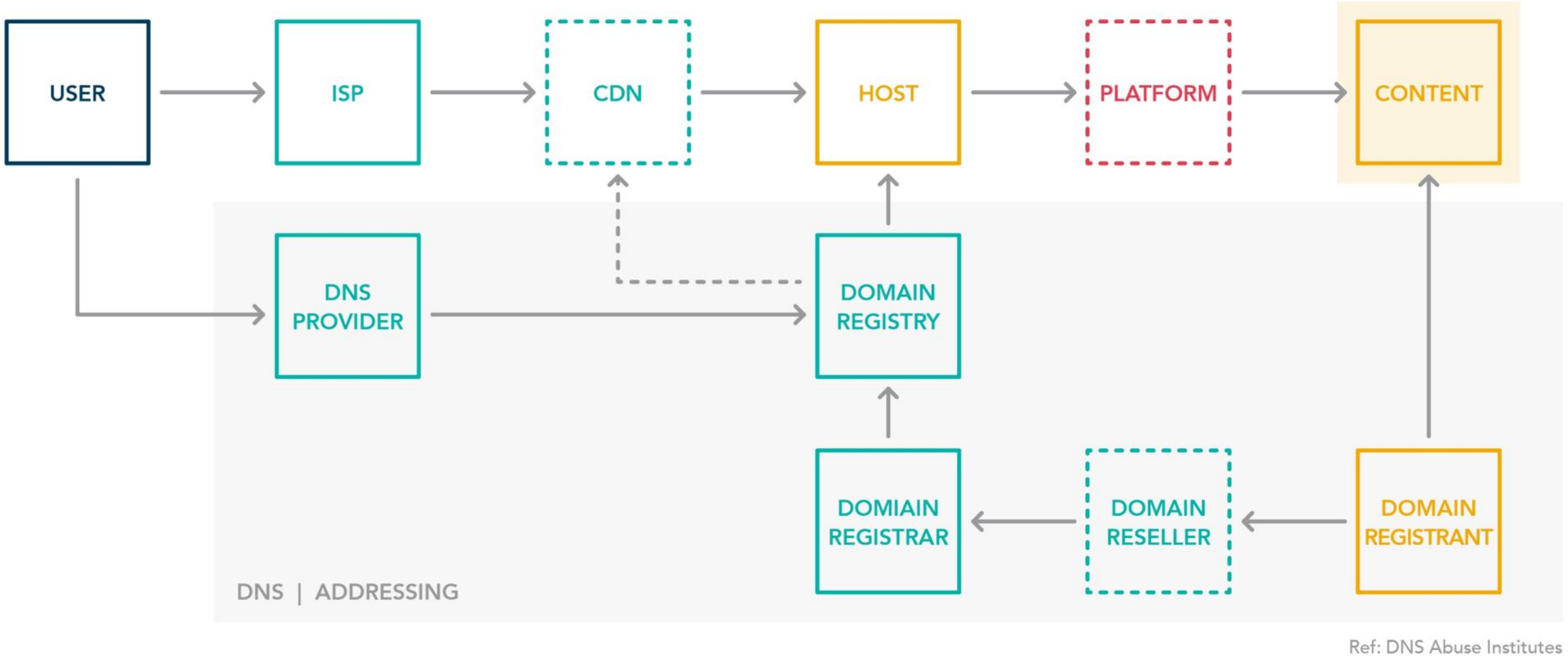
Ref: DNS Abuse Institutes

Problems with Enforcement



Ref: DNS Abuse Institutes

CSC-Led Industry Cooperation

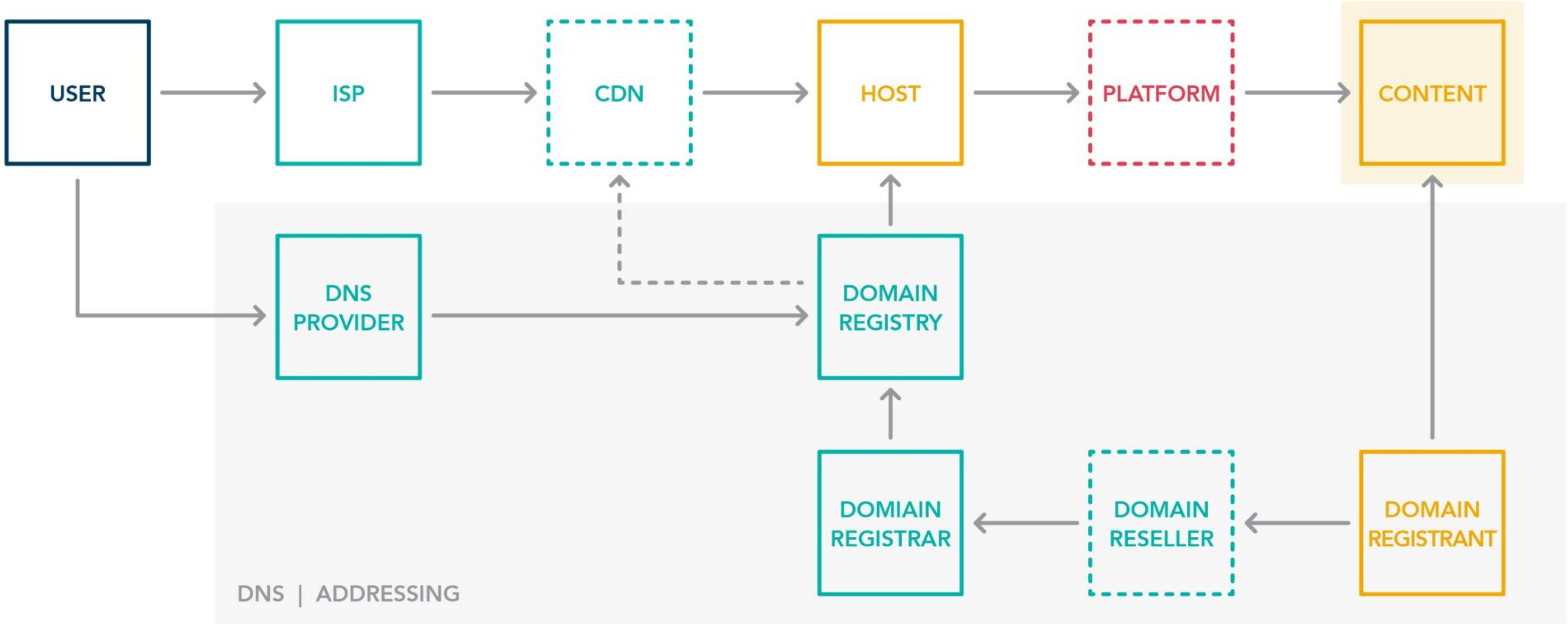


Ref: DNS Abuse Institutes

Google® Chrome™ browser 65.52%

Effective termination of the impact of phishing: make it **unresolvable**

CSC-Led Industry Cooperation



Ref: DNS Abuse Institutes

Trusted notifier

Effective termination
of the impact of the
phishing itself:
make it **unrevivable**

2nd Cooperation model:

Cooperation with browser to build DomainCast network

3rd Cooperation model:

Cooperation with domain name industry to establish Trusted Notifier network

Summary

1. Proper anti-phishing requires you to include **securing your digital identity** as part of your cybersecurity posture

2. Phishing is a DNS Abuse – Critical to have advanced domain monitoring in place

3. New cooperative mindset:
    1. You and your anti-fraud partner – Share your weblog data to uncover unmonitorable phishing attacks
    2. Your anti-fraud partner and the industry – Blocking network + Trusted Notifier

CSC

CSC

Questions?

Alban Kwan

✉ alban.kwan@cscglobal.com

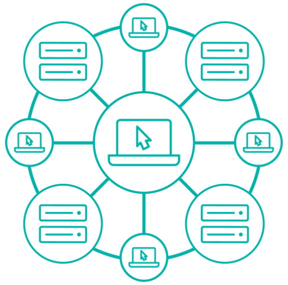
in linkedin.com/in/albankwan/

cscdbs.com

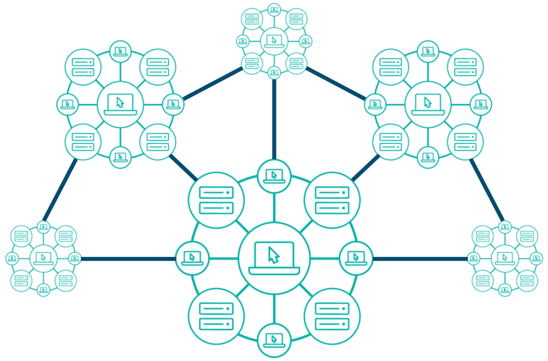
in CSC Digital Brand Services

@cscdbs

We Live Under Two Systems: Network and Inter-Network



NETWORK
ZERO trust



INTER-NETWORK
Trust

Primary concern: Intrusion prevention

OSI model

Created by ISO

- IDS
- Software patching
- End point security
- Malware
- **Prevent phishing attacks to your employees via firewall and email gateway**

Primary concern: Identity abuse

TCP | IP model

Created by U.S. Department of Defense

- Domain hijacking or DNS Kaminsky attack
- DNSSEC and DMARC deployment
- HTTPS deployment strategy
- Fake social media, websites, and apps
- **Phishing for login or PII from customers and partners by mimicking your organization name**