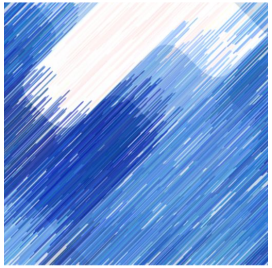
Domain Name Abuse:
Online Scams and Financial Crime

Wednesday, 11 June 2025 (13:45-15:00 local, UTC +2)

Session Chair: Nick Wenban-Smith (.uk), DASC Chair

- Gabriel Andrews, Federal Bureau of Investigation
- Keith Drazek, Internet Infrastructure Forum
- Mon Perez, .sg
- Bruce Tonkin, .au

We'll use Mentimeter for live audience input during the session, so keep your phone or laptop handy to take part.



About the ccNSO DNS Abuse Standing Committee (DASC)

1. Share information, insights and practices
2. Raise understanding and awareness
3. Promote open and constructive dialogue
4. Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

Introduction

- The DASC 2022 and 2024 Surveys have highlighted that for many ccTLDs criminal content is a major abuse issue which is actionable at the DNS level in some circumstances
- We heard from the Nigerian registry about the plague of cryptocurrency scams
- In the UK fraud accounts for 40% of all crime with 80% of payment fraud originating from social media or fake websites
- There is a high degree of overlap between phishing (technical DNS Abuse) and online fraud
- The full DASC meeting in Seattle settled upon this topic as the highest priority topic for further community discussion
- Let's hear from some experts and start examining this issue and what more can be done!

Definition

A scam is a fraudulent invitation, request, notification, or offer, designed to obtain personal information or money, or otherwise obtain a financial benefit by deceptive means. There is frequently (but not always) a maliciously registered domain name as a critical part of these deceptions.

ICANN83

- Raising Awareness
- Highlighting ccTLDs' Role

ICANN84

- Deepening the discussion with other stakeholders and from various perspectives

Mentimeter instructions

Join at menti.com | use code 7508 1124

ICANN | ccNSO

Please indicate your level of agreement with the following statements:

Our registry is well prepared to detect domain abuse linked to financial crime.

Our registry is well prepared to respond to domain abuse linked to financial crime.

Strongly disagree

Strongly agree

Federal Bureau of Investigation
Internet Crime Report
2024

2024 BY THE NUMBERS[1]

859,532 Total Complaints in 2024

$16.6 Billion Losses in 2024

33% Increase in Losses from 2023

256,256 Complaints with Actual Loss

$19,372 Average Loss

“IC3 received complaints from more than 200 countries in 2024”

INTERNATIONAL COMPLAINT COUNTRIES

TOP 20 FOREIGN COUNTRIES WITH CITIZENS SUBMITTING COMPLAINTS TO IC3

Country	Complaints	Country	Complaints
United Kingdom	102,692	Mexico	1,116
Canada	6,951	South Africa	1,075
India	4,189	Pakistan	979
France	2,223	Indonesia	895
Philippines	1,790	Italy	761
Australia	1,533	Sweden	732
Germany	1,524	China	651
Japan	1,492	Turkey	649
Brazil	1,472	Spain	639
Honduras	1,352	Netherlands	598

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424

Phishing // Business Email Compromise

2024 CRIME TYPES

BY COMPLAINT COUNT	
Crime Type	Complaints
Phishing/Spoofing	193,407

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS	
Crime Type	Loss
Investment	$6,570,639,864
Business Email Compromise	$2,770,151,146

From: Bill Papariella
[mailto:biilp@flyietedge.com]
Sent: Wednesday, August 19, 2015 12:13 PM
To: Geetha Ramadas
<gramadas@flyjetedge.com>
Subject: Fwd: Payment

Please find the attached invoice to be settled today, confirm receipt of mail

Bill

Sent from my iPhone

Phishing // Business Email Compromise

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints
Phishing/Spoofing	193,407

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss
Investment	$6,570,639,864
Business Email Compromise	$2,770,151,146

From: Bill Papariella
[mailto:biilp@flyietedge.com]

i

WHOIS on "flyietedge.com" (from 2015)

Subpoena or Court Order

```
Domain Name: FLYIETEDGE.COM
Domain ID: 1954431182_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2016-08-25T03:37:20Z
Creation Date: 2015-08-21T16:10:51Z
Registrar Registration Expiration Date: 2016-08-21T16:10:51Z
Sponsoring Registrar: TUCOWS, INC.
Sponsoring Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Vistaprint
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: VistaPrint Technologies Ltd
Registrant Organization: VistaPrint Technologies Ltd
Registrant Street: Canon's Court 22 Victoria Street
Registrant City: Hamilton
Registrant State/Province:
Registrant Postal Code: HM12
Registrant Country: BM
Registrant Phone: +1.7816526199
Registrant Phone Ext:
Registrant Fax: +1.7816526096
Registrant Fax Ext:
Registrant Email: csadmin@vistaprint.com
```

Phishing // Business Email Compromise

2024 CRIME TYPES

BY COMPLAINT COUNT	
Crime Type	Complaints
Phishing/Spoofing	193,407

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS	
Crime Type	Loss
Investment	$6,570,639,864
Business Email Compromise	$2,770,151,146

From: Bill Papariella
[mailto:biilp@flyietedge.com]

i

~ weeks or months later….

Customer info,
Payment info,
… andmore victim domains:

- *exanplevictim2.com*
- *exanplevictim3.com*
- *exanplevictim4.com*
- *exanplevictim5.com*
- *exanplevictim6.com*
- *exanplevictim7.com*
- *exanplevictim8.com*
- *exanplevictim9.com* ….

Ransomware

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424

WHOIS = Preventing Ransomware

CISA
CYBER+INFRASTRUCTURE

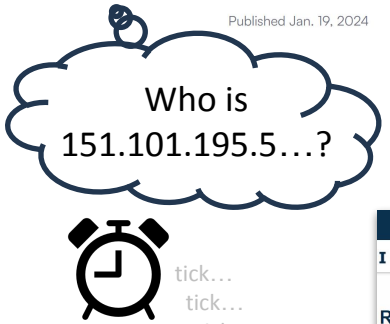
CISA's 1,200 pre-ransomware alerts saved organizations millions in damages

The federal agency's early warning system notified organizations across multiple critical infrastructure sectors of potential impending attacks.

Published Jan. 19, 2024

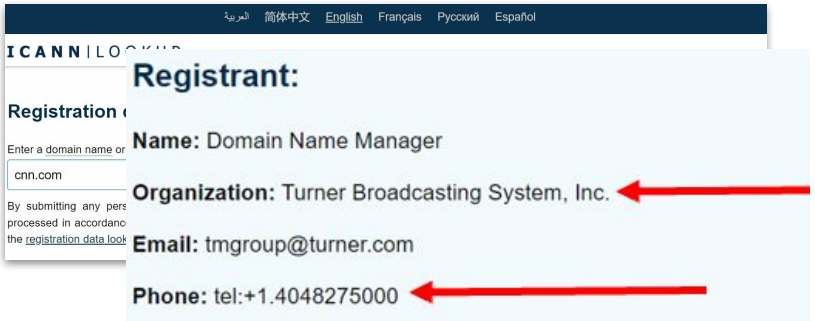
- ✓ **1,213** Pre-Ransomware Notifications in 2023
- ✓ **2,414** in 2024
- ✓ **~8.7B in Value**

"White Hat" cybersecurity researcher



Reverse DNS Lookup

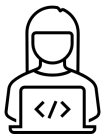
This is cnn.com



monitors

Known Ransomware Server

New Victim



151.101.195.5

UNCLASSIFIED

Cryptocurrency Investment Fraud

2024 CRIME TYPES

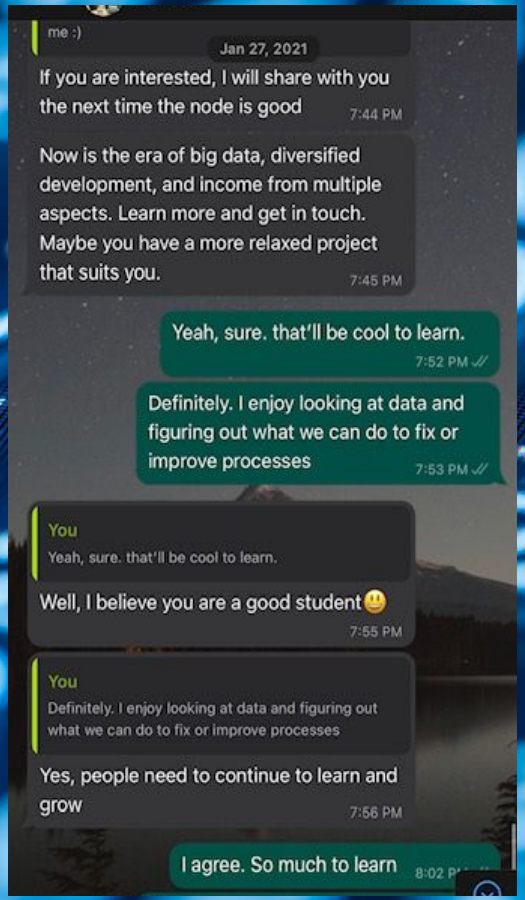
BY COMPLAINT COUNT

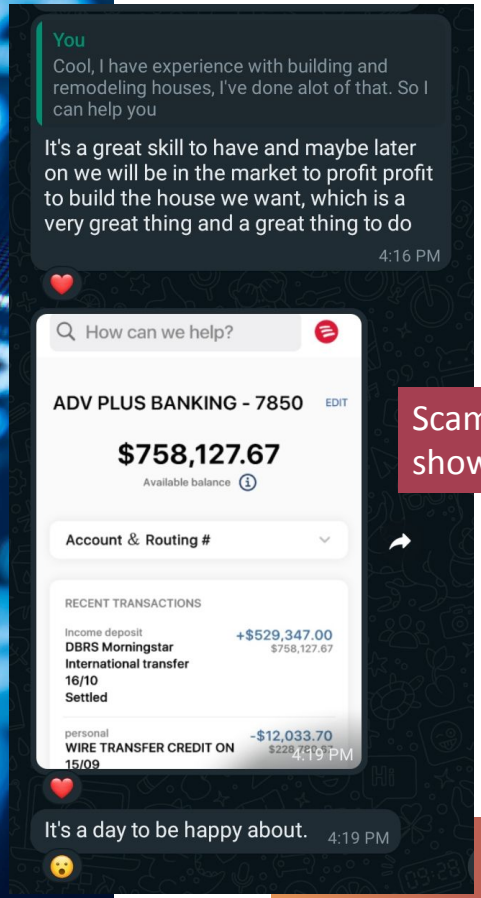
Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945

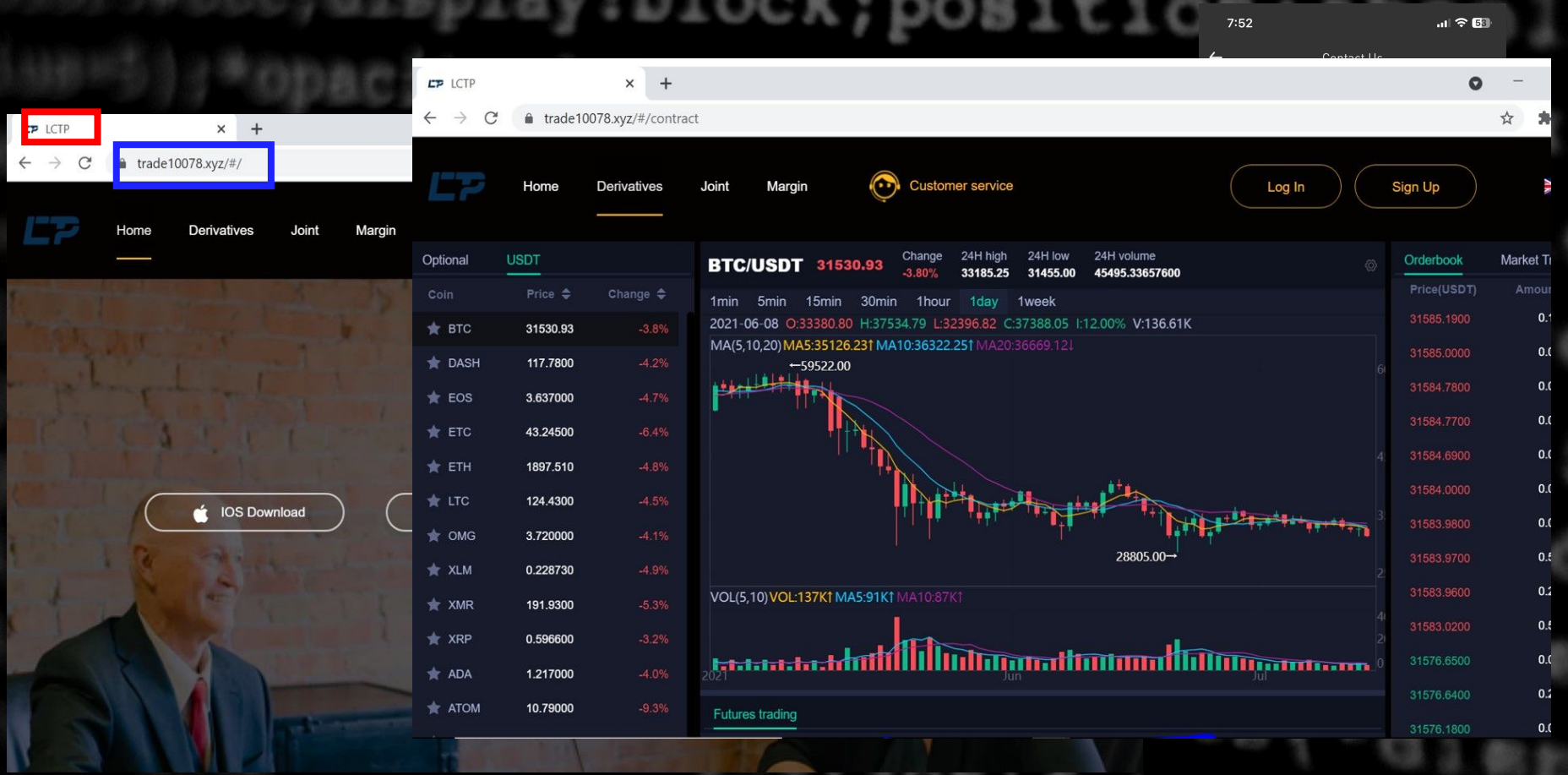




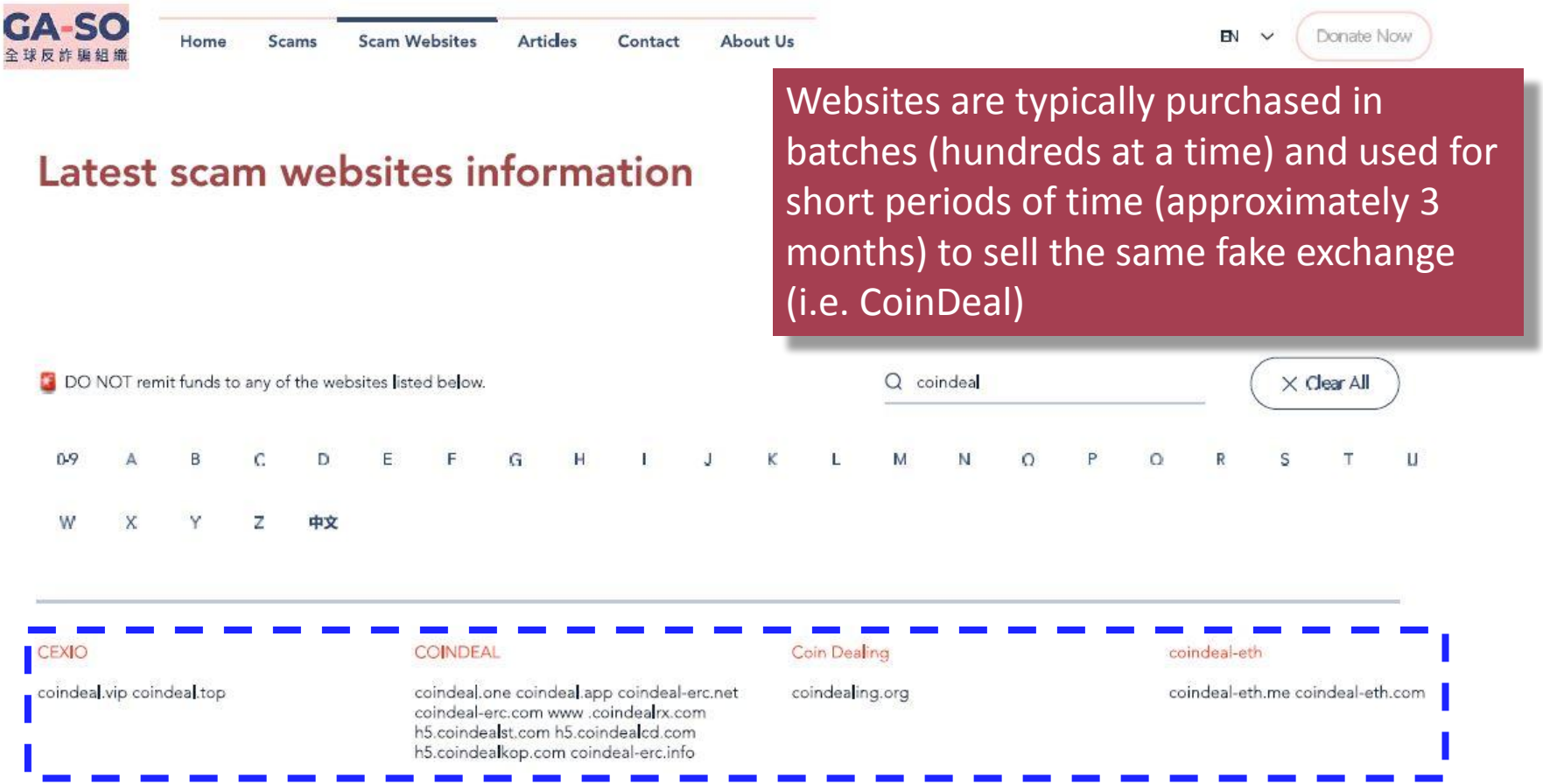
(FAKE) DIGITAL TRADING ACCOU

Scammers send screen grabs of their own “accounts” showing huge earnings to add legitimacy to the scam

TRADING PLATFORM EXAMPLES



DOMAINE PURCHASES



Websites are typically purchased in batches (hundreds at a time) and used for short periods of time (approximately 3 months) to sell the same fake exchange (i.e. CoinDeal)

Examples of Investigative Tools (U.S. perspective)

"What's publicly known?"

"Who is the customer?"

"How did they pay?"

"What IP address(es) did the customer connect from?"

"Can we find these specific things in the Subject's….
… home?
… emails?
… phone?"

"Can we ask a foreign Law Enforcement Agency to conduct similar investigations on our behalf?"

Level of Time + Effort

Same Day

6-12 Months

WHO IS

Google

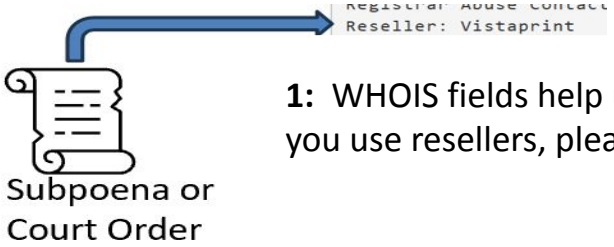
Subpoena

2703 D Order

Search Warrant

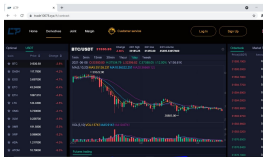
Mutual Legal Assistance Treaty Request

Recap



1: WHOIS fields help us to route court orders & legal process to the right place. If you use resellers, please list them.

2: Public safety agencies use WHOIS to prevent harm to victims in danger.



3: Cryptocurrency Investment Fraud Operators register websites in **bulk** to promote their (FAKE) exchanges.

4: Investigations across borders are SLOW…. Voluntary response to foreign LE requests makes a huge difference.

Internet Infrastructure Forum (IIF)

IIF Goals:

- Connect infrastructure operators around their common coordination challenges, exchange experiences, share best practices, and develop new communication channels.
- Inform participants about the prevalence of different types of abuses, existing mitigation procedures and standards, and the distribution of roles and responsibilities.
- Develop cooperation mechanisms and workflows for abuse reporting and handling, to reduce the burden of dealing with abuses online.

SGNIC’s Efforts Against Online Scams and Financial Crimes

Mon Perez
11 June 2025

RESTRICTED

FINANCIAL CRIME - MAJOR ISSUE

- Cause **financial loss** and damages public **trust of .sg** domain names.
- **8,500** phishing attempts in **2022**. Mostly from other TLDs.
- **80%** of the phishing attempts : Bank & Financial Services, Government and Logistics.

Sources:

https://isomer-user-content.by.gov.sg/36/42a7c8f9-8a22-4608-94aa-f0f2bf40b6dd/Singapore-Cyber-Landscape-2022.pdf

RESTRICTED

ABUSES IN SGNIC CONTEXT

- *In some areas we feel more effective measures can be done by SGNIC.

ICANN DNS ABUSE	Abuses that SGNIC is concerned about	SGNIC additional checks that could be precursor to abuse
Malware	* Malware	Objectionable Domain Names
Phishing	* Phishing	Sale of Domain Names
Spam	Spam	Cybersquatting
Botnets	* Identity Theft or Fake Identity	Registration in Wrong Category
Pharming	Socially / Politically Sensitive Content	Incomplete / Incorrect Registration Details
	Pornographic	
	Copyright Violations	
	Fake Drugs	
	Scams	

SGNIC'S PREVENTIVE AND DETECTIVE MEASURES

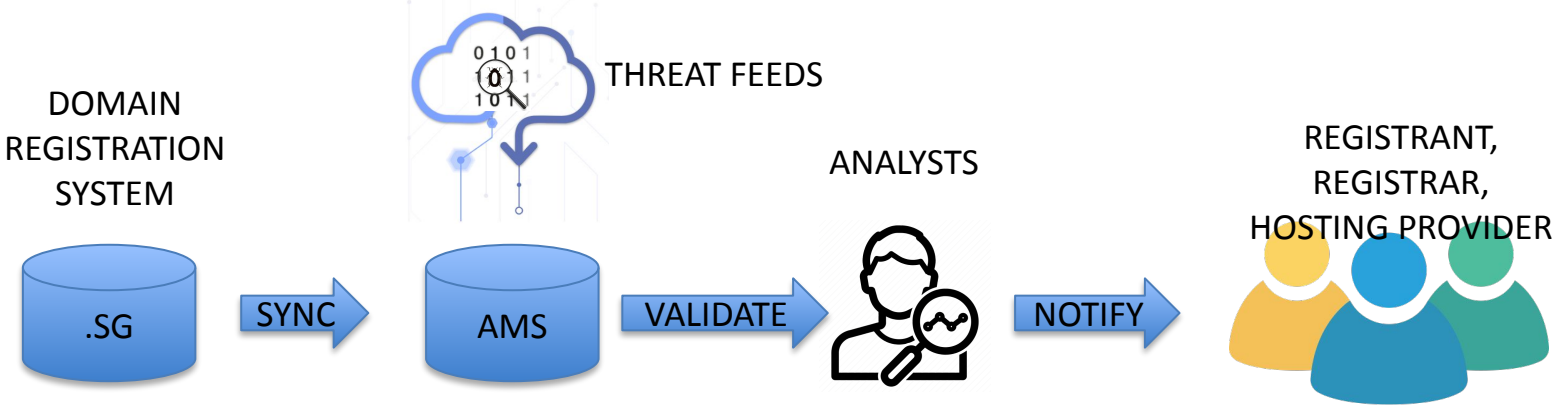
- **VerifiedID@SG** - Ensures domain name registrations undergo verification using Singpass (Singapore's National Digital Identity) - reducing identity theft.

- **RegistryLock** - Free security feature to help .sg registrants mitigate the risk of "domain name hijacking" or unauthorised modifications.

- **Abuse Management System (AMS)** – Internal system that monitors for malicious .sg websites (e.g., phishing/malware) and alerts stakeholders for necessary action.

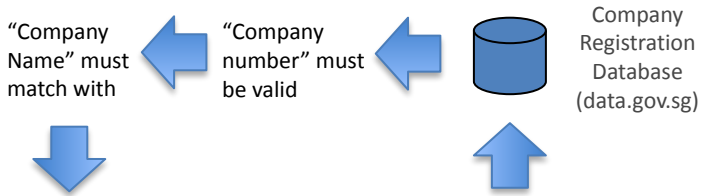
ABUSE MANAGEMENT SYSTEM – MALWARE AND PHISHING

- Detects and tracks domain name abuses - malware/phishing, incorrect/suspicious registration information, DNS wildcard usage and bulk registration.
- Notify stakeholders (registrant, registrar, hosting provider) for necessary action.
- Initially collaborated with SingCERT to provide expert opinion. Thereafter SGNIC took on the role since commercial feeds provide sufficient data to detect malicious content.



ABUSE MANAGEMENT SYSTEM – INCORRECT/SUSPICIOUS REGISTRATION

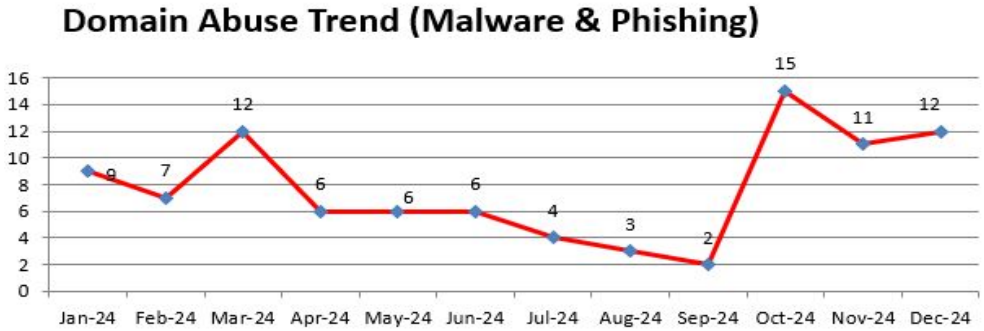
- Check if business registration no. matches the company name.
- Check if the domain name contains a reserved word.



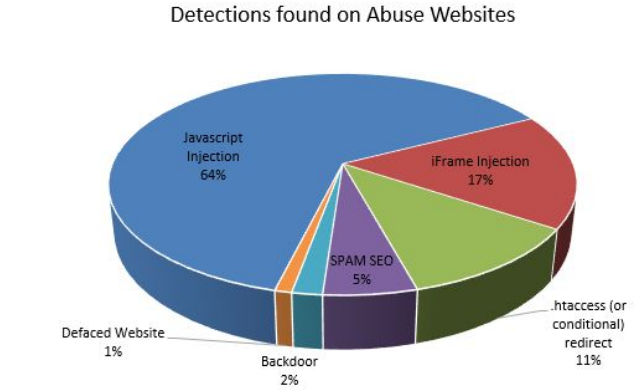
abc.sg **2025-01-01 03:00:00** **VerifiedID: YES**	**[OWNER] : ABC Pte Ltd [Com No.:200709805A]** **[ADDRESS]: 79, ROBINSON RD, ABC BUILDING #03-00 Singapore 111111** **[PHONE] : +65.22223333** **[EMAIL] : buy@abccompany.sg**

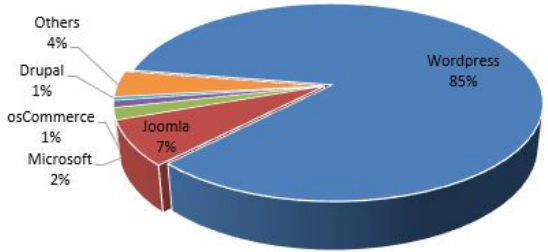
ABUSE MANAGEMENT SYSTEM – MALWARE AND PHISHING

- Provides threat insights on common attacks and applications targeted.



* Increase from Oct 2024 was due to a supply chain attack (Polyfill.io)





SUCCESS STORY FROM SGNIC'S EFFORTS

- **0 reported incidents** on domain name hijacking.
- **Measure resolution rate –** keeping it to 80% resolved cases per month.
- **Well informed** on ongoing or emerging threats .
- **Notable Incident:** July 2012 - a popular web hosting platform was exploited.
  - ~100 .SG domain names were used for phishing.
  - SGNIC identified a common hosting provider and coordinated with the administrators.
  - Issue was **resolved within hours**.

Sources:

https://labs.sucuri.net/your-know-there-is-a-vulnerability-in-plesk-when/

https://thehackernews.com/2012/07/plesk-zero-day-exploit-in-wild.html

EMERGING TREND – SUPPLY CHAIN ATTACK

- Compromised Open-Source Library in 2024
  - Threat actor bought the domain and GitHub account of a popular open-source library.
  - Malicious code was added to the library.

- Widespread Impact
  - Websites using the script unknowingly spread the malicious code.
  - Visitors were redirected to scam sites and malware was auto-downloaded.
  - Affected ~40 .sg domains in 2024 which were notified via AMS

Sources:

Polyfill.io Supply Chain Attack | Qualys Security Blog

Polyfill.io supply chain attack hits 100,000+ websites — all you need to know

MITIGATION CHALLENGES

- **Education / Awareness** – Some registrants don't know what to do or some hosting providers don't know what to patch.

- **Delay in resolution** – Some registrants need time to contact their provider, and some providers take time to implement the necessary patch.

- **Inability** to easily **takedown** high risk abused domains (e.g., web shell) due to negative impact to the victim's business.

IMPACT OF MITIGATION STRATEGY

- **Maintain a low abuse level: ~5 confirmed abuse cases/month** on normal occasions.
- **Community Awareness:** Through targeted email notifications from AMS, domain owners are more **aware of potential threats** and how to **safeguard their domains/websites**.
- **Sustained Trust in .sg:** .sg namespace continues to be viewed as **secure and trustworthy** by the public and businesses.
- **Increased Government Confidence:** Our efforts in running and ensuring trust in .sg have paid off - SGNIC was entrusted to operate the **SMS Sender ID Registry (SSIR)**, which plays a key role in combating **SMS-based scams**.

THANK YOU

31 May 2025

Financial Scams

DASC Online Scams and Financial Crimes
11 June 2025, ICANN, Prague

.au Domain Administration Ltd

.auDA

Australian Gov’t Initiatives

- Scam Prevention Framework:
  - https://treasury.gov.au/publication/p2025-623966
- National Anti-Scam Centre
  - https://www.nasc.gov.au/
- Online gambling compliance and investigations
  - https://www.acma.gov.au/online-gambling-compliance-and-investigations

Scam Prevention Framework

- Scam Prevention Framework:
  - https://treasury.gov.au/publication/p2025-623966
- National Anti-Scam Centre
  - https://www.nasc.gov.au/
- Online gambling compliance and investigations
  - https://www.acma.gov.au/online-gambling-compliance-and-investigations

Scam Prevention Framework (SPF)

- A **scam** must **involve deception** and if successful, would result in a **loss or harm to the consumer**
- A **consumer** includes **Australian residents** (including Australians abroad using Australian services), **visitors to Australia**, and **small businesses** will be protected.
- **Actionable scam intelligence** is information a business has that indicates possible **scam activity** on or related to their business.

Scam Prevention Framework Principles

Governance

Have policies procedures, metrics and targets for combatting scams.

Prevent

Take reasonable steps to stop scam activity from reaching or impacting consumers.

Detect

Take reasonable steps to detect, including identifying consumers that may be

Disrupt

Take reasonable steps to disrupt scams and prevent losses.

Respond

Have a way for consumers to report scams, an internal dispute resolution (IDR) mechanism and join an external dispute resolution (EDR) scheme.

Report

Share information about scam activity with the ACCC. The ACCC may then share information with other parties to prevent and disrupt scams.

Domains used in scams

- Two categories: Malicious and Compromised
- **Malicious**
  - Usually the registrant has used false information
  - .au has an Australian presence requirement which can make it easier to detect false information
  - If the domain name has been registered with false information – it results in a takedown
- **Compromised**
  - Small business websites with unmoderated pages for submitting blogs, comments
  - Hacked websites
  - Notify registrar which works with registrant to remove the offending content
  - Registrants generally surprised and willing to address

auDA Approach

- **Governance** – we centrally track all reports and our own investigations and report information to auDA Board
- **Prevent** – tighten processes for validation of Australian presence
- **Detect** – screen new registrations and look for patterns associated with scams – often results in immediate takedown for domains registered with false information
- Disrupt – pro-actively look for any related domains – use search engines to look for domains with related content as well as registry data
- **Respond** – we have relationship with Australian law enforcement agencies and will review the registration information associated with domain names suspected of being used for scams. Less than 1% of cases.
- **Report** – a work in progress –we use many information feeds but don't yet produce an information feed of domains associated with scams

Questions?

Mentimeter instructions

Join at menti.com | use code 7508 1124

ICANN | ccNSO

Please indicate your level of agreement with the following statements:

Our registry is well prepared to detect domain abuse linked to financial crime.

Our registry is well prepared to respond to domain abuse linked to financial crime.

Strongly disagree

Strongly agree

DASC: resources and activities to date

- Resources
  - DNS Abuse Library: https://icann-community.atlassian.net/wiki/x/JEJ2Bg
  - Dedicated email and contact list: https://icann-community.atlassian.net/wiki/x/JkR2Bg
- Understanding the landscape and how to best serve ccTLDs
  - Survey among ccTLDs 2022
  - Survey among ccTLDs 2024
- Sessions
  - Tools & measurements
  - Amendments to the gTLD Base Registry Agreement (Base RA) and gTLD Registrar Accreditation Agreement (RAA) to Modify DNS Abuse Contract: what do ccTLDs need to know?
  - The role of accurate domain name registration data in combating DNS abuse

Useful resources for ccTLDs

assist ccTLD Managers to detect and/or mitigate DNS Abuse incidents

Resource library

- Presentations and reports
- Tools
- Definitions, policies
- Articles, commentaries

Geared at ccTLDs, vetted by the DASC editorial board

- Consult & propose additional content

https://icann-community.atlassian.net/wiki/x/JEJ2Bg

Dedicated email and contact list

- Subscribe up to 4 contacts per ccTLD
- Quarterly contact list summary
- Closed, but not confidential
- Subscription requests: require authentication

- Share information

DASC-mailing-contacts@icann.org

- Subscribe and read more

https://icann-community.atlassian.net/wiki/x/JkR2Bg

Join at menti.com | use code 7508 1124

ICAN

ICANN83 Online Fraud & Financial Crime

How would you rate this session?

0	0	0	0
Excellent	Good	Just okay	Not great

Thank you!

ccnsosecretariat@icann.org

Next session: Joint session between ccNSO & RySG