GAC Capacity Development Workshop on DNS Abuse

DNS Security Threats reported to Law Enforcement, and by Law Enforcement

Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)
Gabriel Andrews (US Federal Bureau of Investigation, GAC PSWG member)

ICANN77
11 June 2023
UK - Reporting Volume

Computer misuse offences reported to Action Fraud (Crime in England and Wales, Appendix tables, year ending September)

- Total reported computer misuse offences
- Hacking - social media and email
- Computer viruses and malware
- Hacking - personal
- Hacking (extortion)
UK - Business breaches

Businesses - % among those who identified a breach who identified an attack vector of phishing

Businesses - % among those who identified a breach who identified an attack vector of others impersonating organisation in emails or online
UK Action Fraud

- Action Fraud is the UK's national reporting centre for fraud and cyber crime.

- In 2020 - 2021 (most recent public report)
  - Action Fraud received 875,622 reports of fraud
  - leading to £2.35bn reported losses.

- 80% of reported fraud was cyber enabled.

- The report identified phishing emails as the key enabler for criminals to initiate cyber attacks and fraud
Complaints and Losses over the Last Five Years*

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
<th>Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>351,937</td>
<td>$2.7 Billion</td>
</tr>
<tr>
<td>2019</td>
<td>467,361</td>
<td>$3.5 Billion</td>
</tr>
<tr>
<td>2020</td>
<td>791,790</td>
<td>$4.2 Billion</td>
</tr>
<tr>
<td>2021</td>
<td>847,376</td>
<td>$6.9 Billion</td>
</tr>
<tr>
<td>2022</td>
<td>800,944</td>
<td>$10.3 Billion</td>
</tr>
</tbody>
</table>

3.26 Million
Total Complaints

$27.6 Billion
Total Losses
“DNS Abuse” is not tracked as a category.

BUT…

There are categories of DNS Abuse which are tracked in IC3 reports:
Case Study - Phishing

- Information received from Police report that a victim's social media account had been hacked.
- The victim who was a 17 year old reported that the hacker was asking for more passwords.
- They reported loss of accounts including Snapchat, Instagram, TikTok and their Gmail account.
- Suspect identified
- History of hacking social media
- Warrant at home address finding active phones.
- Evidence on mobile phones of mass phishing.
Case Study - Phishing

The Suspect used the phones to send out hundreds of phishing messages to young girls. The accounts used were hacked accounts of other young girls.

From rio (owner)
Hi hun, sorry to bother you but I'm not sure if you are aware but there's a website that is posting inappropriate pictures of girls without their permission and one post claimed to be yours. I'm only messaging you about it because it has your socials linked

27/06/2022 10:39:14(UTC+1)

From rio (owner)
https://clm/ZW52N3YxWjQw

24/06/2022 06:05:11(UTC+1)

From Chlo
Can u send me the link?

24/06/2022 05:43:43(UTC+1)
Case Study - Phishing
Case Study: Reporting Phishing Attacks in the Real World

Here’s a real domain (but redacted by me):

usaauth.VENDOR.TLD
Case Study: Reporting Phishing Attacks in the Real World

Here’s a real domain (but redacted by me): 

usaauth.VENDOR.TLD

Here’s a phishing domain (also redacted): 

usaauth-signin.VENDOR.TLD
## Case Study: Reporting Phishing Attacks in the Real World

**Whois Record for VENDOR.TLD**

### Domain Profile

<table>
<thead>
<tr>
<th>Registrant</th>
<th>REDACTED FOR PRIVACY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant Org</td>
<td>REDACTED FOR PRIVACY</td>
</tr>
<tr>
<td>Registrant Country</td>
<td>CH</td>
</tr>
<tr>
<td>Registrar</td>
<td>Registrar</td>
</tr>
<tr>
<td>IANA ID:</td>
<td>####</td>
</tr>
<tr>
<td>URL: <a href="http://www">http://www</a>.</td>
<td>URL</td>
</tr>
<tr>
<td>Whois Server:</td>
<td>whois_server</td>
</tr>
<tr>
<td>abuse:</td>
<td>@registrar.email</td>
</tr>
<tr>
<td>(p)</td>
<td>+555-555-5555</td>
</tr>
</tbody>
</table>

### Registrar Status

- ok

### Dates

- Created on: 2023-05-11
- Expires on: 2024-05-11
- Updated on: 2023-05-11

### Name Servers

- ARYANNA.NS.CLOUDFLARE.COM (has 26,036,787 domains)
- DILBERT.NS.CLOUDFLARE.COM (has 26,036,787 domains)

### Tech Contact

- REDACTED FOR PRIVACY
- REDACTED FOR PRIVACY
- REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
- info@registrar.email
  - (p) REDACTED FOR PRIVACY x REDACTED FOR PRIVACY (f)
  - REDACTED FOR PRIVACY x REDACTED FOR PRIVACY

### IP Address

- 104.21.31.155 - 739 other sites hosted on this server

### IP Location

- California - San Jose - Cloudflare Inc.

### ASN

- AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)

---

**Summary of facts:**

1. Domain looks like an important login portal to a federal agency
2. Vendor is target of ongoing phishing attacks
3. Domain is newly created (reported within 1 day of registration by Law Enforcement)
## Case Study: Reporting Phishing Attacks in the Real World

### Desired Action:
Registrar (clientHOLD) and/or Registry (serverHOLD)

### What happened:

**May 12** - Cloudflare adds interstitial warning of fraud

**May 14** - Registry: ‘as we don’t host nor register the domain’, ‘not in position to act’ absent a court order

**May 15** - Registrar “we are merely the registrar” and don’t control use of the domain, will notify Reseller

**May 16** - Registrar confirms Reseller deleted domain.
Case Study: Reporting Phishing Attacks in the Real World

>> so why not get a court order?

>> if domain is suspended by the Registrar or Registry, is the domain still dangerous?

>> if the content Host removes the content, is the domain still dangerous?
Taking action “at the DNS Level”...

... vs at “Hosting Level”

<table>
<thead>
<tr>
<th>DOMAIN NAME</th>
<th>TTL</th>
<th>TYPE</th>
<th>RECORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>RALNBOWBANK.COM.</td>
<td>160</td>
<td>A</td>
<td>101.14.66.2</td>
</tr>
<tr>
<td>RALNBOWBANK.COM.</td>
<td>160</td>
<td>A</td>
<td>222.14.10.4</td>
</tr>
<tr>
<td>RALNBOWBANK.COM.</td>
<td>160</td>
<td>A</td>
<td>23.124.228.102</td>
</tr>
<tr>
<td>RALNBOWBANK.COM.</td>
<td>160</td>
<td>A</td>
<td>101.14.66.22</td>
</tr>
</tbody>
</table>

Registrar & Registry control this

Hosting Provider controls this
Key Takeaway

- **Phishing** is DNS Abuse
- **Phishing** is top reported Internet crime
- **Phishing enables** many other crimes
- Swift action against Maliciously Registered Domains has **BIG IMPACT** on DNS Abuse (and cybercrime)
Prior GAC Contributions on DNS Abuse

- **GAC Statement on DNS Abuse** (18 Sep. 2019)
  - Protecting the public from security threats and DNS Abuse is an important public policy issue.
  - If the public is to trust and rely upon the Internet for communications and transactions, those tasked with administering the DNS infrastructure must take steps to ensure that this public resource is safe and secure.

- Since the GAC’s endorsement of the Law Enforcement Due Diligence Recommendations ([Brussels Communiqué](#), June 2010) the GAC has continuously sought to increase the effectiveness of ICANN contracts and their enforcement in mitigating DNS Abuse with Registrars ([Dakar Communiqué](#), Oct 2011) and with New gTLD Registries ([Beijing Communiqué](#) Safeguards Advice, Apr. 2013)

- In the [Beijing Communiqué](#) Safeguards Advice (11 April 2013) the GAC advised that “six safeguards should apply to all new gTLDs and be subject to contractual oversight” including:
  - Security checks — While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.
/Questions?