We are Ireland online

Policy Advisory Committee

28th July 2022

Meeting - PAC#32

Policy Advisory Committee
Agenda PAC #32

1. Membership Matters
2. Minutes from the PAC #31 meeting
3. Matters arising
   - *Domain Alert System to protect products with geographical origin and reputation*
4. Handling of online abuse which uses the .ie namespace
   - *4.1 GNCCB*
   - *4.2 Netcraft*
   - *4.3 Anti Abuse policy proposal*
5. NIS 2 update
6. AOB
   - *CER Directive // Agorateka portal – EUIPO // ADRP stats*
7. Next Meeting

1. Membership Matters

- Please keep **microphones muted** throughout the call
- Please **“raise a hand”** to ask a question or **add comments** in the chat box
- Request to allow the meeting be **recorded** to assist with minute drafting
  - Recording will deleted once the Minutes are approved by PAC

2. Minutes of the PAC #31 Meeting

- Meeting minutes are circulated to the membership promptly after each meeting
- Comments/feedback accepted over a two week period
- If clarifications/edits are requested, and consensus exists, these are reflected in the Minutes
- Meeting minutes, and supporting slides, are published on weare.ie after the comment period has ended
- Published online at https://www.weare.ie/policy-development-process/

3. Matters arising

- Domain Alert System to protect products with geographical origin and reputation:-
  - craft and industrial products (e.g Donegal Tweed)
  - wine, spirit drinks & agricultural products

4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

Recap

- Agreement reached with the Garda National Cyber Crime Bureau (GNCCB)
- Common ground & Goodwill is substantial
- Key engagement at meeting on 10 March 2022 (esp. mutual understanding & due process)
- Agreement confirmed by email 17 May 2022 (circulated with Minutes)

4.1 Handling of illegality and criminal abuse in the .ie namespace

GNCCB - Suspension Request protocol document

Action Items

- Publicity & Communications
- Regular Forum for GNCCB engagement :- invitation to Registrar Day
- Single points of contact (SPOCs)
- Conduit for Engagement with other Garda units

4.2 Handling of technical abuse

Netcraft monitoring service

Recap

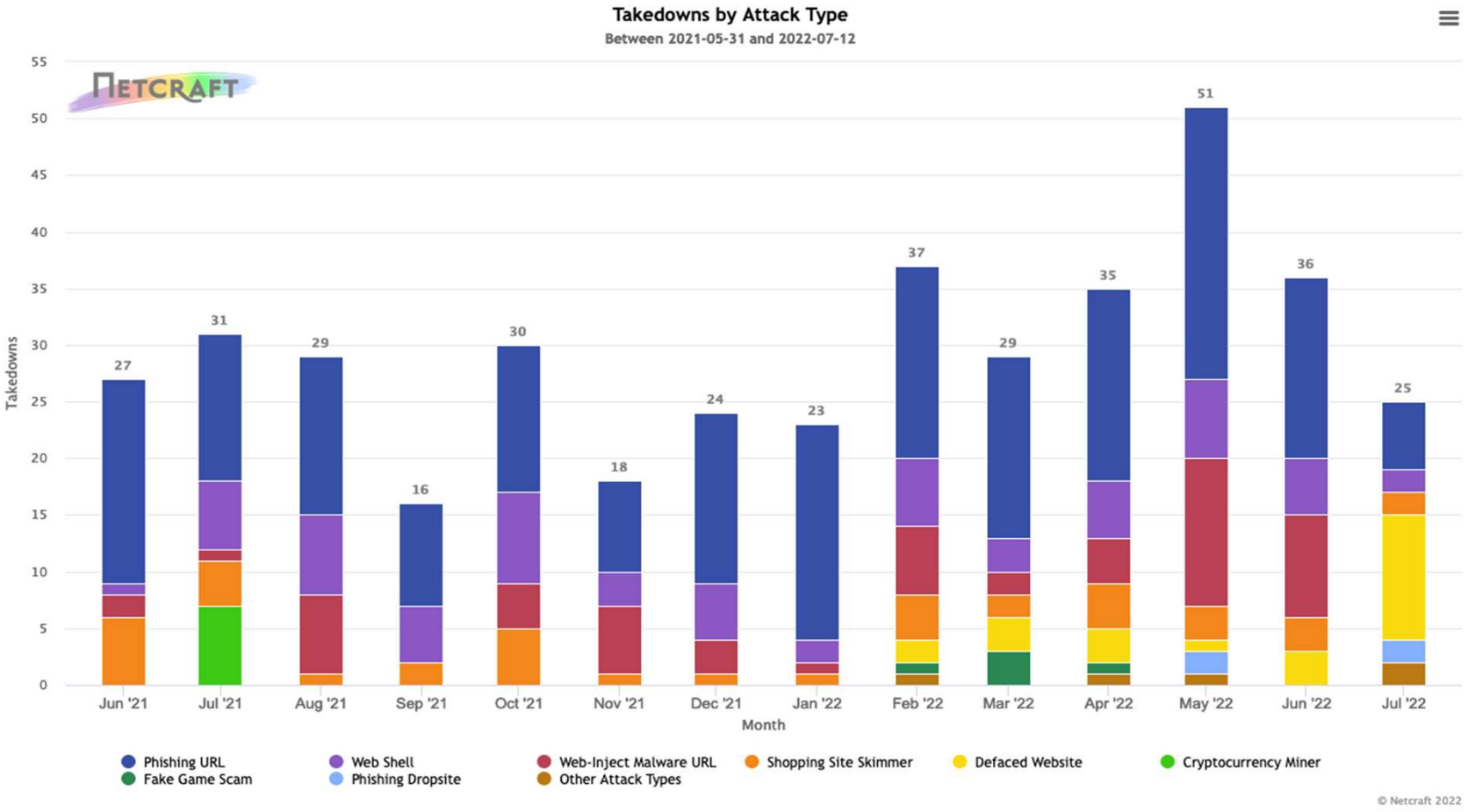
- Consensus from PAC members
- Service commenced March 2021
- Registrar's role
- Financed by .IE
- Benefits:
  - Proactively respond to technical abuse (e.g. malware, phishing or botnets)
  - Helps innocent victims (e.g. SMEs who might be unaware that they have experienced a cyber attack)
  - Notification allows them to take the required remediation action

4.2 Handling of technical abuse

Handling of online **Technical abuse:-** use of Phishing, Malware, botnets etc

Netcraft service:- **409** attacks Jun-'21 to Jul-'22

June-21 to July-22	
Phishing URL	203
Web Shell	65
Web-Inject Malware URL	58
Shopping Site Skimmer	39
Defaced Website	23
Cryptocurrency Miner	7
Fake Game Scam	5
Phishing Dropsite	4
Other Attack Types	5
	409



4.3 DNS Abuse – time for a formal .IE Policy ?

(more accurately 'Abuse that uses the DNS'….)

Recap

- Proposal for new, formal .ie policy
- Rationale for an Anti-Abuse policy
- Context :- digitally transformed post-Covid world (malware, phishing, scams)
- EU* regulators attention
- Self-regulation provides confidence, builds trust through transparency
- ccTLDs may (eventually) follow gTLDs - obliged to have a policy

Discussion deferred

*The European Commission has just published its study on DNS abuse. The study assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures. The study proposes a **set of recommendations** in the field of **prevention, detection and mitigation** of DNS abuse.

4.3 DNS Abuse – time for a formal .IE Policy ?

We are Ireland online

POLICY CHANGE REQUEST – draft for consideration

	Policy change proposal / New Policy proposal	
1	**Proposal Originator** *(name: email: telephone: organisation)* David Curtin, CEO, .IE dcurtin@weare.ie	
2	**Date** 26th May 2022	
3	**Policy Proposal Name:** "Anti-Abuse policy" to handle abusive use(s) of .ie domain names	
4	**Policy Proposal type**: *new, modify, or delete* New policy	
5	**Purpose and benefits of the proposal :** *Please state the purpose of your proposal* ➢ The purpose of the proposal is to formalise the policy and process for handling mis-use of the DNS. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general, noting that abusive use includes the wrongful or excessive use of power, position or ability. *Please state the benefits of your proposal* ➢ The benefits of the proposal include the formalisation and transparency of .IE's current policy, process and procedures for handling technical abuse using the DNS ➢ Improves the confidence and trust of consumers, policy makers and of business in the .ie namespace. ➢ Such a policy may empower industry participants to proactively handle instances of abuse using the DNS:- ○ to protect the integrity and stability of the registry; ○ to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; ○ to avoid any liability, civil or criminal, on the part of .IE, as well as its officers, directors, and employees; ○ to comply with the terms of the registration agreement or	

6	**Please indicate any perceived problems (issues you envisage)** ➢ Legal Powers ? – no national legislation (yet). Registry currently empowered by its own T&Cs. ➢ Best practice alignment ? – internationally many ccTLDs have not (yet) adopted a formal anti-abuse policy. gTLDs have contractual obligations with ICANN. ➢ Efficacy ? purpose is 'handling of…' not 'prevention of….' ➢ Stakeholder objection ? .IE does not envisage objections from the domain industry to the change of the policy per se, particularly as most channel partners & Registrars already react promptly to technical abuse, when notified. ➢ Uncertainty ? Anticipate transposition of imminent EU cyber security regulations	
7	**Policy proposal grounds:** *please indicate the reasons for your proposal (what is wrong/missing/inadequate etc. with the status quo?)* ➢ Abusive use(s) of domain names is currently handled within the Dispute Resolution Policy and procedures, and in particular by protocols with national regulatory agencies and similar bodies with legislative responsibilities. These protocols generally deal with illegality of content, not technical abuse arising from mis-use of the DNS. ➢ Current responses are reactive in nature	
8	**Policy term proposal:** *temporary, permanent, or renewable* Permanent	
9	**Policy statement/text**: *New Policy Text* None proposed at this time. *Note that Section 3 of the Terms and Conditions of Registration may require amendment if there is stakeholder consensus on this policy change request.*	

5. NIS 2 – update

Update on developments since PAC#31 :-

- Timing / Trilogues / and linking DSA & CER Directives.
- Czech Presidency continuing where French left off…
- 12 May – Final stage of Trilogue negotiations
- 17 June - EU Council published latest version of NIS 2 text
- Known as the 4-column doc *(472 pages)*

- Some positive proposed edits from the **Council** draft…..
- Impact Assessment required
  - Article 23 – “accurate and complete information, including verification procedures”
  - KYC is costly, resource heavy, and introduces friction in automated online processes
  - GDPR in Whois proposals - identifying “legal person” in .com TLD world
  - Data Access – to legitimate access seekers – lawful and duly justified requests
  - Member States have 21 months to transpose
  - Scope – registries, registrar **and** resellers – “entities providing registration services”
  - Member States shall “require” Vs shall “ensure”

We are Ireland online

5. NIS 2 – update

Whois – *rancorous debates during GDPR*

Whois result: aib.ie

The result of your domain name search is detailed below:
You can see your Whois result below:

Domain Name: aib.ie
Registry Registrant ID: 387117-IEDR
Registrant Name: AIB Group
Registry Domain ID: 750948-IEDR
Registrar WHOIS Server: whois.weare.ie
Registrar URL: http://www.csccorporatedomains.com/
Updated Date: 07/07/2022
Creation Date: 11/06/2001
Registry Expiry Date: 30/06/2023
Registrar: CSC Domains Inc
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8009279801
Domain Status: Server delete prohibited, Server transfer prohibited, Server update prohibited
Registry Admin ID: 4047-IEDR
Registry Tech ID: 12592-IEDR
Name Server: ns1.netnames.net, ns2.netnames.net, ns6.netnames.net
DNSSEC: Unsigned

Whois result: sfa.ie

The result of your domain name search is detailed below:
You can see your Whois result below:

Domain Name: sfa.ie
Registry Registrant ID: 260878-IEDR
Registrant Name: REDACTED FOR PRIVACY
Registry Domain ID: 661540-IEDR
Registrar WHOIS Server: whois.weare.ie
Registrar URL: https://www.blacknight.com
Updated Date: 12/04/2022
Creation Date: 03/03/2000
Registry Expiry Date: 03/03/2023
Registrar: Blacknight Solutions
Registrar Abuse Contact Email: abuse@blacknight.com
Registrar Abuse Contact Phone: +353.599183072
Domain Status: Registered
Registry Admin ID: 174999-IEDR
Registry Tech ID: 3159-IEDR
Name Server: ns1.blacknight.com, ns2.blacknight.com, ns3.blacknight.com, ns4.blacknight.com
DNSSEC: Unsigned

5. NIS 2 – update

Article 23:- implications for data accuracy & completeness

Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

- What is accurate?
- What is complete?
- What is maintain?
- Who are legitimate access seekers?

5. NIS 2 – update

Legitimate access seekers

Recital (60)

Legitimate access seekers mean any legal or natural person making a request based on Union or national law.

They include but are not limited to **competent authorities** under Union or national law for the prevention, investigation or prosecution of criminal offences, and national CERTs, or CSIRTs.

TLD registries **and** the entities providing domain name registration services should be required **to enable lawful access** to specific domain name registration data, which are **strictly necessary** for the purpose of the access request, to legitimate access seekers in accordance with Union and national law.

The request from legitimate access seekers should be accompanied with a **statement of reasons** permitting the assessment of the necessity of access to the data.

5. NIS2 – update

Evidence of good practices

NIS 2018:-

Regulation 17(1) provides that
Operators of Essential Services shall –

- take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which it uses in its operations, and

- take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used by it ……with a view to ensuring the continuity of the provision by it of those services.

We are Ireland online

5. NIS 2 – update

How can we make progress on 'The Good'

- Legislation is c.21 month away, but **cyber threats** are here today
- **Awareness** building – "Just inform" via Newsletter, Blogs, Webinars, YouTube clips
  - *Audience* - RAR channel, SMEs in the Supply Chains, TDs & policy makers,
  - *Messaging* :- KYC is costly; Start now on cyber defences, think about ISO alignment 1st;
- Share **Impact Assessment** document – cyber benefits, regulatory cost burden, need for eID,
- **Lobby** letter - to those transposing into national legislation – do's & dont's; ask for early clarifications
- **Engagement** - Channel needs a clear legal framework (esp. re conflicts with GDPR provisions)
- Cyberthreats – how to improve **current** resilience and incident response capacities of critical services

6. AOB

- CER - Directive for the resilience of critical entities (CER Directive).
- Agorateka portal – EUIPO helping users find legally available digital content
  (The portal links to national portals that themselves link to websites containing legal offers)
- Alternative dispute resolution process (ADRP).

6. AOB

Alternative Dispute Resolution process (ADRP)

Summary ADRP completed cases

13 cases completed since December 2020

11 were transferred to the complainant for the reasons below:

- 5 reached a settlement
- 4 determined to have been registered in 'bad faith'
- 1 determined to have been registered abusively
- 1 determined to be potentially harmful to public health
- 2 cases were denied:
  - 1 - the complainant was unable to provide sufficient evidence against the registrant
  - 2 - no action was initially taken under the ADRP process (although transferred since)

We are Ireland online

7. Next Meeting

Proposed date:

Thursday 20th October 2022

We are Ireland online

Policy Advisory Committee

28th July 2022

Meeting - PAC#32