We are Ireland online

Policy Advisory Committee

10th November 2022

Meeting - PAC#33

Policy Advisory Committee
Agenda PAC #33

1. Membership Matters
2. Minutes from the PAC #32 meeting
3. Matters arising
   - *Domain Alert System to protect CI products with geographical origin and reputation*
   - *Agorateka portal – EUIPO*
4. Handling of online abuse which uses the .ie namespace
   - *4.1 illegality online (GNCCB protocol)*
   - *4.2 tech abuse (Netcraft stats)*
   - *4.3 Anti Abuse policy proposal (parked ?)*
5. NIS 2 update
6. AOB
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 #32 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 (DIAS) 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)

4.2 Handling of technical abuse

Netcraft monitoring service

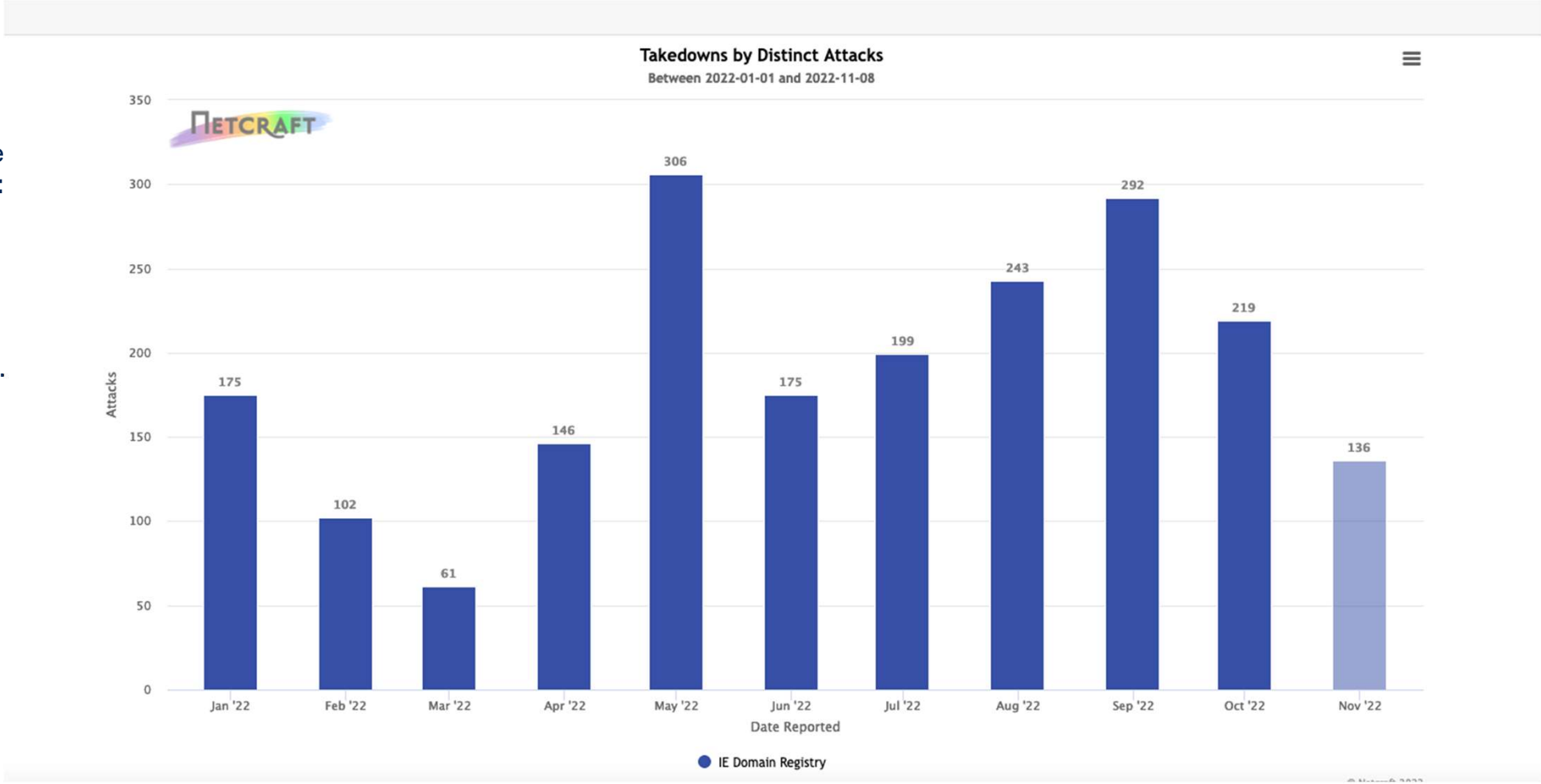
Recap

- 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…

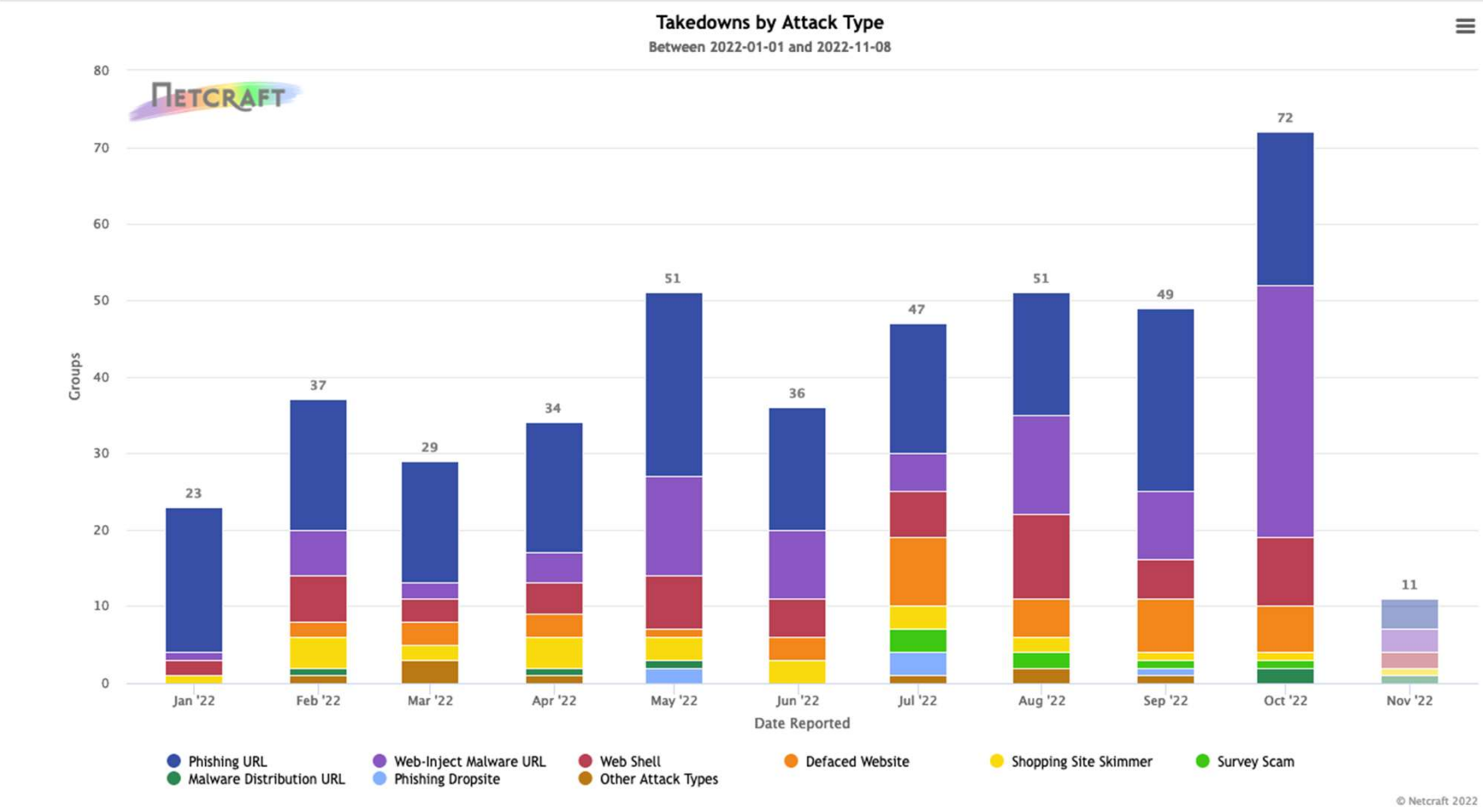
Netcraft service:· **2,054** attacks Jan-'22 to Jul-'22



4.2 Handling of technical abuse

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

Netcraft service:-
440 takedowns
Jan-'22 to Jul-'22



4.2 Handling of technical abuse

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

Netcraft service:-
2,054 attacks
Jan-'22 to Jul-'22

Attack Type	Total Groups	Total Attacks	Total IP Addresses	Percentage of Attacks
Phishing URL	181	1120	107	43%
Web-Inject Malware URL	96	172	62	22.8%
Web Shell	59	446	47	14%
Defaced Website	39	227	30	9.3%
Shopping Site Skimmer	18	50	17	4.3%
Survey Scam	7	10	5	1.7%
Phishing Dropsite	6	11	4	1.4%
Malware Distribution URL	6	6	6	1.4%
Other	9	12	8	2.2%

2,054

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 – Role for the PAC ?

Update on developments since PAC#32 :-

- Timing / Trilogues / and linking DSA & CER Directives.
- 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”

5. NIS 2 – Role for the PAC ?

How can we make progress on 'The Good'

5. NIS 2 – Role for the PAC ?

How can we make progress on 'The Good'

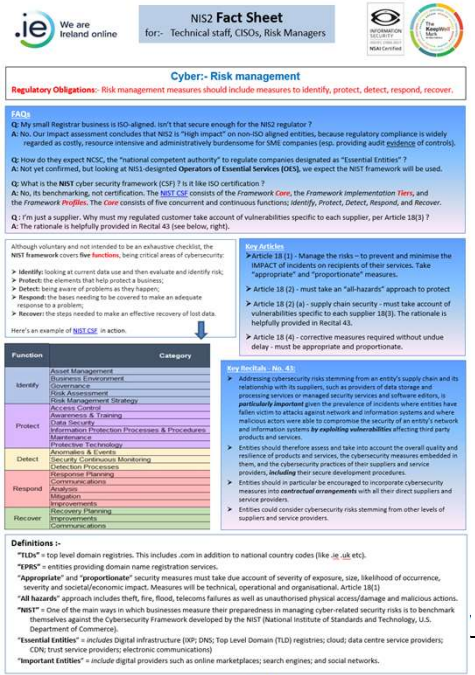
Action Items

- Action "**trigger**" is the publication in the EU Official Journal
- 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 service

5. NIS 2 – Role for the PAC ?

How can we make progress on 'The Good'

Action Items



		Financial	Operational	Reputational	Legal	Governance	Human Resources / Staffing
Data Accuracy Controls	Increase in Renewal time/Potential non renewal if not responsive	Medium	Critical	Low	Low	Medium	Null
Data Access requests	Potential impact on GDPR, WHOIS, RDAP and other data control.	Medium	Critical	High/ Critical	High	High	Null
Cyber Risk	Increased need for Certification/NIST alignment , ISO etc	Medium	Critical	Medium	Medium	High	Medium
Digital Supply Chain Risk	Increased need for Audit controls, alerting, Reviews, Contract changes	Medium	Critical	Medium	High	High	Low
Know your customer controls (KYC)	Increased costs to New Reg, Increased Time to Register	High	Critical	Medium	Low	Low	Medium

6. AOB

7. Next Meeting

Proposed date:

February 2023