DOCUMENTO TECNICO · QUADRO DI RIFERIMENTO PROPOSTO · VERSIONE 1.0

Dal rilevamento alla mitigazione

Un'architettura misurabile per la risposta al DNS Abuse: provenienza delle prove, azione proporzionata, responsabilità pubblica e ricorso rapido — concepita per essere verificata, non semplicemente affermata.

Pubblicato il 2 agosto 2026

PhishDestroy Ricerca

Bozza per la consultazione pubblica

Non sottoposto a revisione tra pari

PD-WP-2026-01 · Version 1.0 · 2026-08-02
https://phishdestroy.io/it/dns-abuse-enforcement-framework

SINTESI

PROPOSTA INDIPENDENTE · NON È UN PROGRAMMA DI ICANN

Conclusione diretta. L'ecosistema contrattuale dell'gTLDe presenta un divario misurabile tra l'uso malevolo di un dominio, tecnicamente verificato, e l'efficace mitigazione dello stesso. Gli studi pubblicati dimostrano che molte campagne di phishing operano per ore o giorni, mentre le procedure di conformità contrattuale possono svolgersi nell'arco di giorni lavorativi. Il modello di scenario divulgato mostra come il ritardo aumenti i rendimenti attesi delle campagne; l'intervallo del 60–85% rappresenta la stima centrale verificabile del danno post-notifica riportata nel documento, non una statistica consolidata per tutte le frodi globali. La stima tecnica di 100–150 dollari riguarda la raccolta e l'elaborazione iniziale di un corpus definito di dati relativi alle zone, alla Certificate Transparency e ai feed pubblici, non il costo totale della revisione legale o dell'applicazione delle norme. Il documento propone prove firmate, obiettivi di risposta misurabili, escalation automatica dei casi convalidati, rimedi proporzionati, responsabilità pubblica e ricorso rapido. Non propone di concedere ai segnalanti l'accesso diretto ai controlli di sospensione dei domini.

● FONTE PRIMARIA
Supportato direttamente da un documento ufficiale o da uno studio pubblicato.

● MODELLO ILLUSTRATIVO
Un calcolo riproducibile i cui dati di input sono ipotesi, non medie di mercato.

● PROPOSTA POLITICA
Un progetto sottoposto a consultazione, verifica e revisione.

01 Domanda di ricerca, ambito di applicazione e livello di prova

La domanda è più circoscritta di «chi ha fallito?» : **quali ritardi osservabili tra prove validate e un'azione proporzionata sono evitabili, e quale intervento riduce il danno alle vittime senza generare falsi positivi o danni collaterali inaccettabili?**

L'ambito di applicazione è costituito dall'ecosistema contrattuale di gTLD: registranti, rivenditori, registrar, registri e la funzione di conformità contrattuale di ICANN. I fornitori di servizi di hosting, i CDN, i browser, i servizi di pagamento, le piattaforme pubblicitarie, i CERT nazionali e le forze dell'ordine sono inclusi solo nella misura in cui incidono sulla catena probatoria o di risposta. I TLD con

codice paese hanno una governance diversa e non si presume che siano soggetti ai contratti gTLD di ICANN.

Stato delle tesi principali

- Il documento analizza l'ICANN come istituzione di governance privata e di garanzia del rispetto dei contratti nell'ambito dell'ecosistema dell'gTLD. L'ICANN non è un'autorità di regolamentazione governativa né un organismo preposto all'applicazione della legge, ma accredita i registrar, stipula contratti con gli operatori di registro e garantisce il rispetto di tali accordi; tale mandato limitato non esclude la responsabilità istituzionale.
- L'intervallo compreso tra il 60% e l'85% rappresenta una stima quantitativa centrale nel modello di valutazione del danno presentato nell'articolo. Esso viene presentato come una stima verificabile, derivata da ipotesi esplicite e osservazioni di casi concreti, e non come un dato statistico già consolidato relativo a tutte le frodi a livello globale. La pubblicazione di un set di dati a livello di singolo incidente che allinei i timestamp relativi al rilevamento, alla notifica, alla mitigazione e al danno rappresenta il prossimo passo probatorio.
- La cifra compresa tra 100 e 150 dollari rappresenta una stima di budget ingegneristica verificabile per la raccolta continua e lo smistamento iniziale su un insieme definito di dati relativi alle zone accessibili, alla Certificate Transparency e ai feed pubblici su infrastrutture di base. Non si tratta del costo della visibilità globale completa, della revisione legale, dei ricorsi, dell'alta disponibilità o dell'applicazione delle norme. Il documento lo considera quindi un punto di riferimento da riprodurre con un carico di lavoro pubblicato, un inventario delle risorse e un registro dei costi, non come un prezzo universale già comprovato. Tale distinzione restringe la portata dell'affermazione senza cancellare l'asimmetria dei costi oggetto di verifica.
- Il confronto di tre settimane presentato nell'articolo riguarda la latenza di conformità, non uno SLA universale relativo alla chiusura dei domini. ICANN's Domande frequenti sulla conformità contrattuale afferma che la maggior parte delle tipologie di reclami può passare attraverso tre periodi consecutivi di risposta di cinque giorni lavorativi prima di essere sottoposta a un'escalation formale, mentre molte campagne malevole rimangono attive per ore o giorni. I contratti prevedono inoltre, separatamente, l'adozione di misure di mitigazione tempestive e adeguate una volta acquisite prove sufficienti per un'azione legale. [2] [4]
- Nel caso di una registrazione malevola verificata e con un unico scopo, `serverHold` È una delle misure correttive a livello di DNS più invasive, poiché rimuove la delega dalla zona. Non è una soluzione universale: può infatti compromettere anche la posta elettronica, i sottodomini e i servizi legittimi; le risposte memorizzate nella cache potrebbero permanere fino alla scadenza del TTL; inoltre, i servizi compromessi o condivisi potrebbero richiedere misure di mitigazione più mirate. [4] [7]

> CONTRIBUTO ALLA RICERCA
>
> La proposta è falsificabile. Un progetto pilota può confrontare coorti di trattamento e controllo in termini di tempo di triage, tempo di mitigazione, indicatori delle perdite subite dalle vittime, ricorrenza, falsi positivi, tempo di revoca e impatto collaterale.

02

Cosa emerge dalle fonti primarie

$165.1M

Finanziamento operativo ICANN per l'esercizio 2027

Bilancio approvato per l'esercizio 2027. Scala contestuale; non rappresenta la spesa per il DNS Abuse. [1]

191,561

Denunce relative a phishing e spoofing nel 2025 (IC3)

Categoria di reclami IC3 più numerosa; perdite attribuite direttamente pari a 215,8 milioni di dollari. [10]

24 ore

Durata di vita mediana secondo uno studio del 2021

Risultato specifico per il set di dati relativo a 1.288 domini di phishing; non si tratta di una durata universale. [11]

Nessuno SLA fisso

Termine universale di disattivazione

Le modifiche del 2024 impongono una mitigazione «tempestiva» e «adeguata», non un'unica scadenza globale. [2] [3]

PROPOSTA	STATO	COSA SI PUÒ AFFERMARE
Il phishing è DNS Abuse	VERIFICATO	Il phishing è esplicitamente una delle cinque categorie coperte dalle modifiche contrattuali del 2024 applicabili ai gTLD. [2]
I registrar devono agire	VERIFICATO	I registrar devono agire tempestivamente quando dispongono di prove utilizzabili che un nome da essi sponsorizzato è impiegato per DNS Abuse. [2]
Gli operatori di registro devono agire	VERIFICATO	Gli operatori di registro devono agire tempestivamente quando determinano ragionevolmente, sulla base di prove utilizzabili, che un nome registrato è impiegato per DNS Abuse; la misura appropriata resta dipendente dal contesto. [3]
`serverHold` rimuove la delega	VERIFICATO	È uno stato EPP impostato dal server. Le risposte DNS memorizzate nella cache possono permanere fino alla scadenza e l'azione riguarda l'intero dominio registrato. [7]
Tutto il DNS Abuse è visibile in CZDS o CT	FALSO	CZDS e Certificate Transparency sono sensori preziosi, ma non offrono una visione completa o in tempo reale di ogni utilizzo dei domini. [8] [9]

Il primo rapporto semestrale ICANN sull'attuazione delle modifiche del 2024 ha registrato 192 indagini, oltre 2.700 domini sospesi, più di 350 pagine di phishing disattivate e due notifiche formali di violazione contrattuale (Notices of Breach). I dati non dimostrano che i controlli attuali siano sufficienti, ma escludono l'affermazione assoluta secondo cui il sistema non interviene. [5]

03

Perché la latenza di risposta rimane un obiettivo di ricerca legittimo

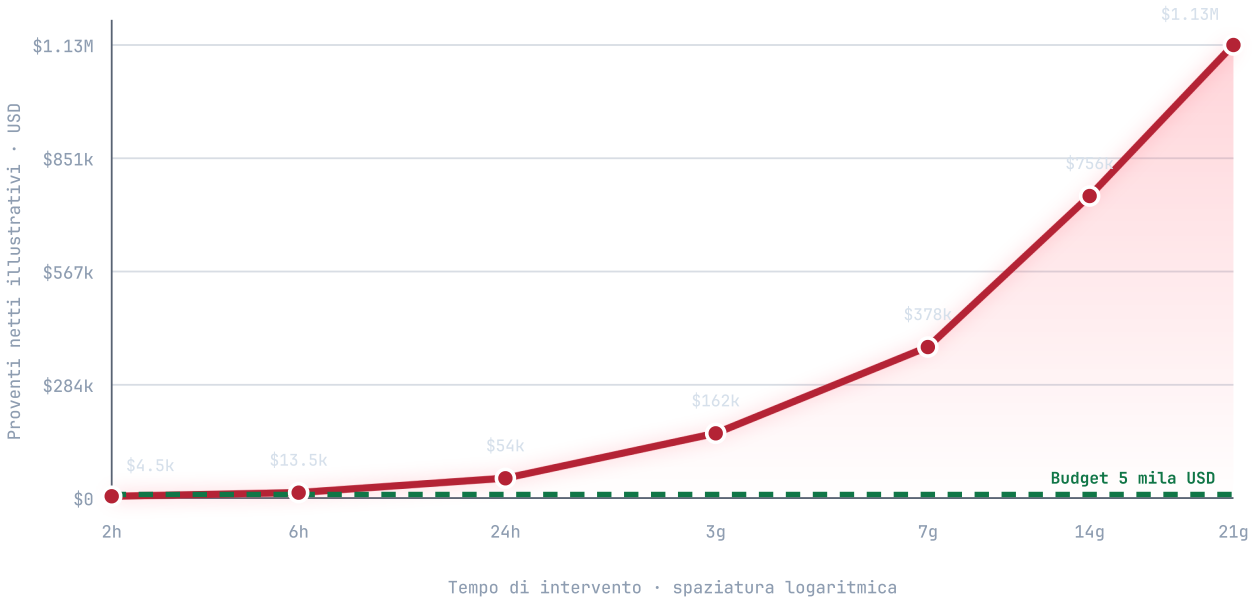
Alcune campagne di phishing hanno una durata che va da poche ore a qualche giorno. In uno studio del 2021, Bijmans et al. hanno riportato una durata media osservata di 45 ore e una mediana di 24 ore per 1.288 domini di phishing. Uno studio del 2026 sui domini di phishing di nuova registrazione ha riportato una distribuzione fortemente asimmetrica: per 14.112 domini con durata misurabile, la media era di 8,6 giorni e la mediana di un giorno. Nessuno dei due campioni può essere generalizzato a tutte le classi di minacce, ma entrambi dimostrano perché un processo misurato solo in giorni lavorativi possa tralasciare campagne di breve durata. [11] [12]

LO SFASAMENTO TEMPORALE MISURATO

Questi studi non stabiliscono la quota di danno finanziario che si verifica dopo la notifica, ma evidenziano uno sfasamento temporale: un processo le cui prime fasi di conformità informale possono richiedere fino a quindici giorni lavorativi non può di per sé fungere da risposta agli incidenti per campagne con una durata mediana vicina a un giorno. Il punto relativo ai 21 giorni riportato di seguito rappresenta quindi uno scenario di latenza nella conformità, non una definizione di uno SLA universale denominato “ICANN”.

FIGURA 1 · RISULTATO CUMULATIVO ILLUSTRATIVO DELLA CAMPAGNA

MODELLO · INTERVALLI TEMPORALI DI TIPO LOGARITMICO



La curva illustra lo scenario descritto nella Sezione 4; non si tratta di dati di mercato osservati. La rappresentazione orizzontale comprime gli intervalli più lunghi per facilitare la lettura. Fonte: modello riproducibile con input resi noti.

CAUTELA CAUSALE

Una durata più breve del dominio non equivale automaticamente alla prevenzione di perdite finanziarie. Gli autori degli attacchi potrebbero spostarsi, utilizzare siti compromessi, cambiare i canali di distribuzione o incassare i proventi prima di essere individuati. L'effetto causale deve essere misurato, non dedotto esclusivamente dalla rapidità con cui il sito viene rimosso.

04 L’economia delle campagne fraudolente come scenario riproducibile

L’asset economicamente rilevante spesso non è la quota di registrazione, ma il traffico, i materiali creativi, l’infrastruttura e la fiducia accumulati attorno a un dominio. L’intuizione è plausibile, ma la sua entità varia tra campagne fraudolente. Il calcolatore espone quindi ogni input, anziché presentare un risultato ipotetico come media osservata.

DEFINIZIONE DEL MODELLO

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Calcolatore di scenari

Modifica qualsiasi ipotesi. I valori sono puramente indicativi e non rappresentano stime relative al mercato tipico del phishing.

MODELLO ILLUSTRATIVO

Budget della campagna (USD)

5000

Visite giornaliere

2000

Tasso di conversione delle vittime (%)

1.5

Perdita media per vittima (USD)

2400

Attrito nel cash-out (%)

25

Tempo di azione (ore)

24

Vittime

2,000

Vittime previste

30

Incasso lordo

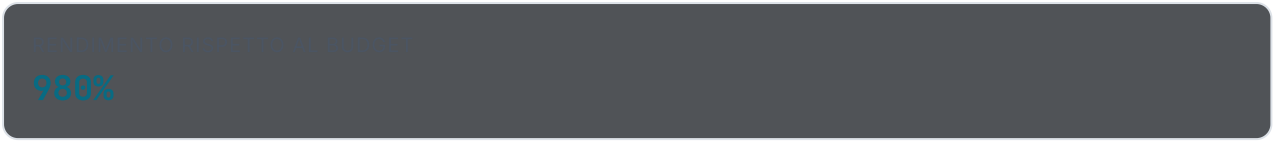
$54,000

Incasso netto previsto

$49,000

Tempo di azione

2.2 h



Il numero atteso di vittime può essere frazionario perché il modello esprime un valore atteso. Non tiene conto del calo del traffico, della retroazione dovuta al rilevamento, della migrazione, delle vittime ripetute e delle distribuzioni di incertezza.

▶ Visualizza la tabella delle fonti del modello

05 Misurare i danni evitabili senza inventarsi la precisione

Il concetto di “perdita dopo l’individuazione” può diventare un parametro utile solo se i termini “individuazione”, “consegna” e “danno” vengono definiti in modo coerente. La data e l’ora di inserimento in una lista nera non costituiscono prova del fatto che il registrar abbia ricevuto prove utilizzabili. Una transazione da un wallet non è automaticamente attribuibile a un determinato dominio. Il fatto che un dominio diventi irraggiungibile non permette di identificare quale soggetto abbia causato tale cambiamento.

Schema minimo dell'evento

EVENTO	DATA E ORA OBBLIGATORIE	PROVA MINIMA
Prima osservazione	`t_obs`	Sensore, hash richiesta/risposta, metodo di acquisizione, sorgente di clock.
Convalida tecnica	`t_valid`	Indicatore riproducibile, identità del revisore, categoria di minaccia e livello di affidabilità.
Notifica consegnata	`t_notice`	Ricevuta di consegna autenticata e versione dell’evidence envelope.
Presa in carico dell’attore responsabile	`t_ack`	ID del caso e ruolo destinatario: host, registrar, registro, piattaforma o autorità.
Mitigazione osservata	`t_mitigate`	Stato DNS, HTTP, dei pagamenti o della piattaforma, misurato da più punti di osservazione.
Ricorso / ripristino	`t_restore`	Fondamento della decisione, prove sopravvenute e verifica del ripristino.
Evento dannoso	`t_harm`	Segnalazione della vittima in forma anonima, transazione attribuibile o altro indicatore documentato.

INDICATORE DI RISULTATO PROPOSTO

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

Il numeratore e il denominatore devono seguire la stessa regola di attribuzione. I risultati dovrebbero riportare la coorte, l'intervallo di confidenza, la censura a destra, le fonti mancanti, la gestione delle vittime duplicate e la sensibilità alla finestra di osservazione. L'etichetta «prevenibile» dovrebbe essere riservata a un disegno causale o, come minimo, a un confronto abbinato — non a ogni evento successivo alla notifica.

STIMA MODELLIZZATA CENTRALE · 60–85%

Il documento mantiene il 60–85% come stima centrale della quota di danno attribuibile che si verifica dopo l'individuazione e la notifica nella classe di incidenti oggetto del modello. Si tratta di una stima di scenario derivata da ipotesi rese note e osservazioni di casi specifici, non di una statistica misurata relativa a tutte le frodi a livello mondiale. Dovrebbe essere utilizzata per l'analisi di sensibilità fino a quando un set di dati a livello di singolo incidente non allinei le tempistiche relative a osservazione, prove convalidate, consegna, mitigazione e danno. La pubblicazione di tale set di dati costituisce la verifica probatoria della tesi, non un motivo per respingerla.

06 La mappa istituzionale: le competenze sono distribuite

Nessun singolo attore vede o controlla l'intero incidente. Il registrar conosce il rapporto con il registrante; il registro controlla lo stato del dominio impostato a livello di registro; l'host e il CDN controllano la distribuzione dei contenuti; browser e fornitori di sicurezza controllano gli avvisi; i fornitori di pagamenti e wallet possono interrompere i trasferimenti; le autorità possono imporre conservazione o sequestro. ICANN redige e fa rispettare i contratti nell'ecosistema gTLD, ma non gestisce un piano di controllo EPP universale.

01 · SEGNALE

Ricercatori & sensori

Osservano gli indicatori relativi a contenuti, infrastruttura e vittime; ne preservano la provenienza.

02 · SERVIZIO

Host / CDN / piattaforma

Può rimuovere rapidamente i contenuti o bloccarne l'accesso, spesso senza modificare il dominio.

03 · SPONSOR

Registrar

Esamina l'abuso, contatta il registrante e può impostare lo stato lato client.

04 · ZONA

Operatore di registro

Controlla lo stato EPP definito nel registro e la delega della zona TLD.

05 · CONTRATTO

Conformità contrattuale ICANN

Indaga sulla conformità delle parti contraenti; non decide ogni singolo caso di frode.

06 · DIRITTO

CERT / autorità

Coordinano la risposta ed esercitano i poteri giuridici propri della giurisdizione.

La distribuzione delle competenze non implica l'estinzione delle responsabilità. Un registrar sponsor non si sottrae ai propri obblighi contrattuali delegando la gestione degli abusi a un rivenditore; il registro controlla lo stato EPP dei server; ICANN garantisce il rispetto dei termini contrattuali. La traccia di audit deve registrare non solo chi ha agito, ma anche chi ha ricevuto prove utilizzabili, ha reindirizzato il caso, non ha risposto o non ha adempiuto a un dovere assegnato. L'autorità legale rimane in capo al soggetto autorizzato ad applicare una misura; la responsabilità riguarda anche l'inadempienza documentata.

Concentrazione dei finanziamenti e un'ipotesi verificabile sul conflitto di incentivi

$165.1M

Finanziamenti per le operazioni dell'ICANNe per l'anno fiscale 27

È stato approvato il bilancio di riferimento per l'anno fiscale 27. [1]

≈98.1%

flussi di entrate derivanti dal registro e dai servizi di registrazione

Circa 162,0 milioni di dollari del piano di finanziamento da 165,1 milioni di dollari. [1]

70.7%

solo le commissioni basate sulle transazioni

$116.8M tied to billable domain transactions. [1]

La struttura di finanziamento è quindi fortemente concentrata sui pagamenti provenienti dalle parti contraenti, i cui accordi sono garantiti dICANN, e una quota consistente varia in base alle transazioni di registrazione fatturabili. Ciò determina una dipendenza strutturale e solleva una legittima questione relativa al conflitto di incentivi. Ciò *non*, di per sé, non dimostrano un'applicazione intenzionalmente insufficiente delle norme né una vera e propria "cattura normativa". L'ipotesi della cattura dovrebbe essere verificata alla luce dei tempi di risposta a livello di singolo caso, dei risultati dell'applicazione delle norme, delle sanzioni, della recidiva e del ruolo delle parti interessate che beneficiano dei finanziamenti nelle decisioni relative alle politiche e alla loro attuazione.

07 Il quadro contrattuale di riferimento per il 2024 — e ciò che non specifica

Le modifiche globali dell'aprile 2024 al Registrar Accreditation Agreement e al Base Registry Agreement hanno introdotto obblighi espressi di mitigazione del DNS Abuse. I registrar devono agire tempestivamente quando dispongono di prove utilizzabili che un nome da essi sponsorizzato è impiegato per DNS Abuse. Gli operatori di registro devono agire tempestivamente quando determinano ragionevolmente, sulla base di prove utilizzabili, che un nome registrato è impiegato per DNS Abuse. In entrambi i casi, la misura appropriata dipende dal contesto, dalla gravità e dall'impatto collaterale. [2] [3]

Tre linee temporali che vengono spesso confuse tra loro

CRONOLOGIA	A COSA SI APPLICA	COSA NON SIGNIFICA
24 ore	Esame, ai sensi del § 3.18.3 del RAA, delle segnalazioni fondate di attività illegali («Illegal Activity») inviate al contatto dedicato da forze dell'ordine, autorità per la tutela dei consumatori, enti parastatali o autorità analoghe.	Non si tratta di un termine universale di 24 ore per la sospensione.
«Tempestivamente»	Adottare una mitigazione adeguata una volta raggiunta la soglia applicabile di prove utilizzabili.	Non equivale a un numero fisso di ore e non impone lo stesso rimedio in ogni caso.
21 giorni	Può configurarsi come un periodo di rimedio successivo a una formale comunicazione contrattuale di inadempimento.	Non si tratta della durata standard assegnata a ogni dominio dannoso segnalato.

Questa flessibilità presenta dei vantaggi: un dominio universitario compromesso non dovrebbe essere trattato come un dominio di phishing monouso appena registrato. Il problema della responsabilità risiede nel fatto che è difficile confrontare i concetti di "tempestività" e "adeguatezza" in assenza di timestamp pubblicati, categorie di casi e codici di esito. La proposta riportata di seguito introduce meccanismi di misurazione e revisione senza pretendere che un'unica scadenza sia adatta a tutti i casi.

08 Il problema dei confini: il phishing è contemplato; alcune frodi finanziarie potrebbero non esserlo

Il phishing rientra esplicitamente nella definizione contrattuale di DNS Abuse. Il confine più difficile riguarda i siti che ingannano sotto un nome originale invece di impersonare un terzo identificabile: alcune piattaforme di investimento fittizie, negozi fraudolenti, recovery scam e schemi finalizzati a ottenere firme di wallet. A seconda dei fatti, possono essere trattati come abuso dei contenuti web, frode ai consumatori o altra categoria giuridica, anziché come DNS Abuse contrattuale.

TERMINE DI RICERCA PROPOSTO

Verified Financial Harm Abuse (VFHA): uso documentato di un dominio per ottenere mediante inganno fondi, credenziali di pagamento, chiavi private o seed phrase, indipendentemente dall'impersonificazione di un marchio. VFHA non appartiene alla terminologia ICANN vigente e non crea, di per sé, alcuna autorità contrattuale.

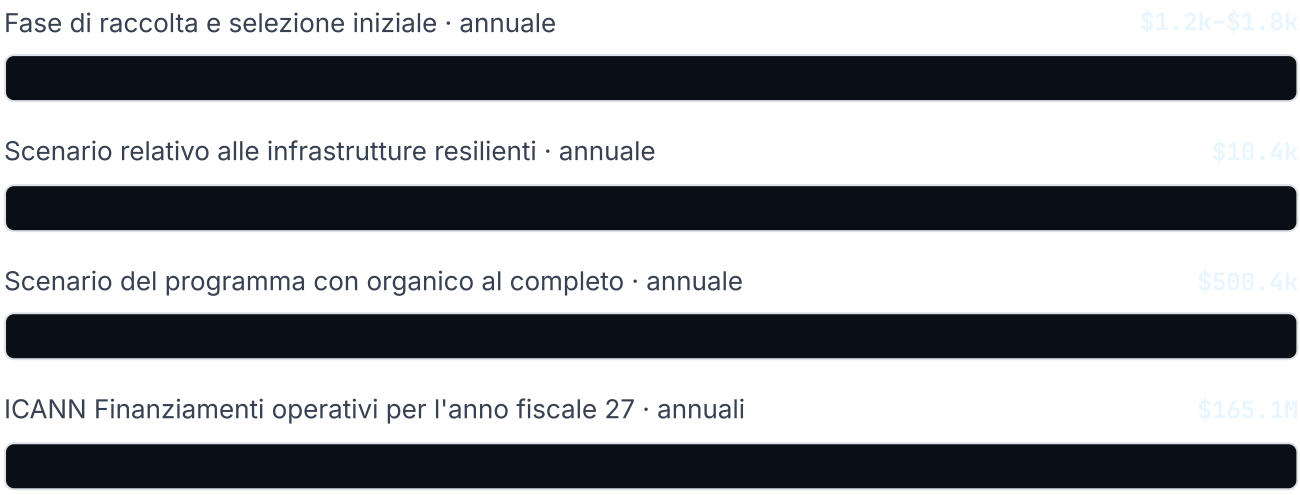
Una consultazione pubblica potrebbe esaminare se una categoria circoscritta e sostenuta da prove, come VFHA, debba rientrare in futuri contratti, in un quadro di rinvio intersettoriale o nel diritto nazionale. Ogni estensione dovrebbe richiedere una prova precisa del danno, elementi probatori affidabili, rimedi proporzionati, verifica della giurisdizione e ricorso. Etichette vaghe come «truffa» non sono sufficienti.

09 Cosa deve dimostrare l'affermazione relativa al monitoraggio da 100–150 dollari al mese — e cosa non può dimostrare

Un server standard è in grado di scaricare istantanee accessibili dei file di zona gTLD dei partecipanti e di calcolare le modifiche a livello locale, acquisire eventi selezionati relativi alla Certificate Transparency e feed aperti, normalizzare le stringhe, calcolare gli hash e stabilire le priorità dei candidati. Si tratta di un benchmark ingegneristico utile e verificabile, non di un "monitoraggio completo di Internet". Nel secondo trimestre del 2026, Verisign ha riportato 401,6 milioni di registrazioni su tutti i TLD; il CZDS copre i file di zona gTLD partecipanti anziché tutti i TLD, mentre il CT registra certificati o precertificati registrati pubblicamente anziché ogni dominio attivo o dannoso. [8] [9] [17]

CAPACITÀ	PROTOTIPO SU INFRASTRUTTURA STANDARD	SERVIZIO DI PRODUZIONE DI INTERESSE PUBBLICO
Ingestione di zone/CT/feed	Fattibile per un insieme definito di fonti	Collettori ridondanti, contratti con le fonti e monitoraggio delle lacune
Selezione di stringhe/hash	Fattibile	Analisi comparativa, rilevamento delle derive, studi sui falsi negativi
Rendering del browser	Sottogruppo di campioni di piccole dimensioni	Flotta isolata, punti di osservazione regionali, contenimento del malware
Accertamento giuridico	Non incluso	Revisori qualificati, giurisdizione e mappatura delle competenze
Alta disponibilità / conservazione delle prove	Di solito assente	Firme protette da HSM, registri di audit, backup e risposta agli incidenti
Ricorsi e riabilitazione	Non incluso	Operatività 24 ore su 24, 7 giorni su 7, procedura di escalation autonoma e obiettivi di servizio

FIGURA 2 · CONTESTO DELL'ORDINE DI GRANDEZZA AMPIEZZA LOGARITMICA · COSTI NON COMPARABILI



Le larghezze logaritmiche mantengono visibili i valori più piccoli. Le prime tre cifre sono ipotesi tecniche o di programma rese note che richiedono un benchmark pubblicato e non costituiscono preventivi dei fornitori. ICANN Il finanziamento delle operazioni è un dato verificato su scala istituzionale. Si tratta di bilanci volutamente non equivalenti: il confronto verifica se la raccolta e lo smistamento di base rappresentino un costo intrinsecamente proibitivo, non se un programma completo di applicazione della legge costi 100 dollari al mese.

10 Quadro proposto per la risposta agli abusi verificati

Il quadro proposto è un'architettura di riferimento, non un «interruttore di arresto» globale automatico. Standardizza l'evidence envelope, il fascicolo decisionale e i timestamp, consentendo all'operatore autorizzato di scegliere la misura efficace con il minore impatto collaterale.

01 · INGESTIONE

Acquisire & preservare

Raccogliere segnalazioni e osservazioni; calcolare gli hash degli artefatti grezzi; sincronizzare gli orologi.

02 · PROVENIENZA

Normalizzare le prove

Registrare l'origine, il metodo, la cronologia di gestione e le dipendenze relative alle fonti.

03 · CONVALIDA

Confermare

Riprodurre il comportamento dannoso e individuare le prove indipendenti.

04 · VALUTARE

Rischio & impatto collaterale

Classificare registrazioni malevole, servizi compromessi, hosting condiviso e gravità.

05 · RISPONDI

Segnalare e mitigare

Indicare il soggetto responsabile, il termine previsto e la soluzione efficace che comporti il minor disagio possibile.

06 · RIESAME

Audit & ricorso

Pubblicare metadati sugli esiti, misurare l'impatto e agevolare una rapida revoca.

Livelli di evidenza

E1 — **Segnale non verificato**

Segnalazione isolata, corrispondenza lessicale o denuncia basata sulla reputazione. Adatto a fini di osservazione, ma mai sufficiente da solo per giustificare una sospensione.

E2 — **Comportamento riprodotto**

Acquisizione con data e ora che mostra il furto di credenziali, la diffusione di malware o un percorso di transazione ingannevole.

E3 — **Conferma indipendente**

Almeno due fonti realmente indipendenti oppure una prova tecnica riproducibile, accompagnata da verifiche relative alla proprietà e al contesto.

E4 — **Conferma qualificata**

Autorità, servizio interessato, titolare del marchio o prove validate delle vittime, con una catena di custodia rispettosa della privacy.

REGOLA DELL'INDIPENDENZA

Tre feed che copiano la stessa blacklist a monte costituiscono un'unica fonte, non tre. Il grafico di provenienza deve evidenziare l'origine condivisa, la sincronizzazione e la ripubblicazione da parte del fornitore.

11

Un evidence envelope minimo e un'API interoperabile

L'APIe dovrebbe creare un caso verificabile e avviare un timer di risposta verificabile; un segnalante non deve poter emettere direttamente un comando di sospensione. Se un caso E3/E4 riguarda una registrazione dolosa a scopo unico e scade senza una decisione motivata o una mitigazione efficace, il sistema lo inoltra automaticamente all'operatore del registro o a un altro soggetto dotato di autorità contrattuale o legale. A `serverHold` Il comando può provenire esclusivamente da un soggetto autorizzato. L'escalation automatica e l'autorità del registro di intervenire alla scadenza sono modifiche proposte alla politica, non affermazioni relative all'autorità esistente. Ogni transizione di stato viene firmata e aggiunta al registro di audit.

POST /V1/CASES · ESEMPIO

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Una risposta positiva restituisce l'ID del caso, l'attore destinatario, il livello di prova, gli errori di completezza, il tempo di revisione previsto e un URL pubblico di trasparenza. Non deve promettere uno specifico rimedio prima che un attore competente ne valuti la propria competenza e l'impatto collaterale.

12 Obiettivi di risposta proposti, non termini universali di disattivazione

Gli obiettivi del livello di servizio devono distinguere *presa in carico*, *triage*, *decisione* e *mitigazione efficace*. Ciò consente di misurare le prestazioni senza presumere che la sospensione sia sempre l'esito corretto.

PROFILO DEL CASO	RICONOSCERE	OBIETTIVO DI TRIAGE	OBIETTIVO DELLA DECISIONE	OPZIONI DI RISPOSTA TIPICHE
Furto E3/E4 di credenziali di pagamento o seed phrase mediante una registrazione malevola a scopo unico	15 min	1 ora	4 ore	Blocco del contenuto; sospensione da parte del registrar o del registro, ove autorizzata; avvisi del browser e del prestatore di pagamento.
Phishing di marchio E3 o distribuzione di malware	30 min	2 ore	6 ore	Rimozione da host/CDN, mitigazione del dominio, sinkhole o avviso in base al punto di controllo.
Dominio legittimo compromesso o tenant SaaS condiviso	1 ora	4 ore	12 ore	Isolamento del percorso/account e ripristino del proprietario; evitare, ove possibile, la sospensione del dominio registrato.
Frode finanziaria con classificazione contestata	4 ore	12 ore	24 ore	Conservazione, intervento relativo alla piattaforma/al pagamento, rinvio all'autorità competente e decisione motivata.
Segnale E1 o rapporto incompleto	Auto	24 ore	Nessuno fino alla convalida	Monitorare, integrare e richiedere prove.

Si tratta di obiettivi pilota. I valori corretti dovrebbero essere ricavati sulla base della durata osservata delle minacce, del personale disponibile, del costo degli errori e dei vincoli normativi, per poi essere pubblicati indicando le distribuzioni di raggiungimento anziché un unico valore medio.

13 Sicurezza, garanzie procedurali, privacy e modalità di guasto

Una risposta rapida, se priva di misure di salvaguardia, può trasformare dati errati in censura, sabotaggio commerciale o interruzioni delle infrastrutture. Un'architettura corretta considera quindi i falsi positivi e i danni collaterali come gravi falle di sicurezza.

MODALITÀ DI GUASTO	CONTROLLO OBBLIGATORIO	MISURA VERIFICABILE
Segnalazione malevola contro un concorrente	Autenticazione dei segnalanti, reputazione delle fonti, riproduzione indipendente e sanzioni in caso di abuso	Tasso di segnalazioni respinte per segnalante; casi confermati di manipolazione
Circolarità dei feed presentata come consenso	Grafo di provenienza e deduplicazione delle fonti a monte	Conteggio delle fonti indipendenti prima e dopo la correzione della discendenza
Sospensione generalizzata di un dominio legittimo compromesso	Classificazione dell'intento di registrazione e preferenza per la mitigazione a livello di percorso	Quota di domini compromessi; servizi legittimi interessati
I dati delle vittime o i dettagli dell'attacco sono trapelati pubblicamente	Divulgazione graduale, omissione di informazioni, prove secretate e termini di conservazione	Incidenti relativi alla privacy; esiti della revisione delle operazioni di oscuramento
Persiste un'azione indebita	Ricezione dei ricorsi 24/7, revisore indipendente e percorso di ripristino autenticato	Tempo mediano e al 95° percentile per la revoca
Una sospensione del registro interrompe posta elettronica o sottodomini	Inventario dell'impatto collaterale, proporzionalità del rimedio e monitoraggio successivo all'azione	Servizi interrotti per azione; tasso di revoca

Garanzie minime di equo processo

1. Per ogni misura restrittiva vengono registrati il codice motivo, il livello di evidenza e il responsabile della decisione.
2. Il registrante può ottenere una motivazione che rispetti la privacy e presentare prove contrarie.
3. I ricorsi urgenti vengono esaminati da una persona che non ha preso la decisione originaria.
4. La revoca si propaga attraverso lo stesso canale firmato dell'azione originale.
5. Le statistiche aggregate relative agli errori e al ripristino sono di dominio pubblico; l'accesso alle prove sensibili rimane soggetto a controlli di accesso.

14 Da un "punteggio di tossicità" a un indice di qualità della risposta trasparente

Un punteggio pubblico attribuito a un registrar può migliorare la responsabilità, ma classifiche semplicistiche sono distorte dalle dimensioni del portafoglio, dalla copertura dei feed, dalla composizione della clientela e dalla distinzione tra registrazione malevola e compromissione successiva. Un punteggio non deve mai giustificare il blocco collettivo di tutti i clienti di un registrar.

VETTORE DI QUALITÀ PROPOSTO

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Se ai fini della governance è necessario un indice composito, i pesi devono essere definiti prima della valutazione, sottoposti a test di sensibilità e verificati con un backtest su casi esclusi dall'analisi. I risultati devono essere stratificati per TLD, dimensioni del registrar, classe di minaccia e fonte delle prove. Il risultato è un segnale di responsabilità — non un verdetto automatico sul dominio.

15 Database pubblico multilivello sulla trasparenza del DNS Abuse

Un registro di trasparenza può eliminare le controversie relative all'esistenza di una notifica, alla data di consegna e alle azioni intraprese in seguito. La pubblicazione di ogni elemento, tuttavia, potrebbe compromettere la privacy delle vittime, i dati personali, i metodi investigativi e le strategie di attacco ancora in uso. La soluzione è un accesso a più livelli.

P

Registro pubblico

ID del caso, indicatore, categoria generale, timestamp chiave, livello di prova, ruoli degli attori, codice dell'esito, stato del ricorso e hash degli artefatti sigillati.

C

Panoramica delle parti contraenti

Prove tecniche verificabili, canale di contatto, contesto collaterale e istruzioni di conservazione.

R

Vista riservata alle autorità

Dati delle vittime, attribuzione finanziaria, materiale di indagini attive e catena di custodia non oscurata.

Ogni aggiornamento è di tipo "append-only", provvisto di data e ora e firmato. Le correzioni non cancellano la cronologia, ma aggiungono un record che sostituisce quello precedente. La ricerca pubblica dovrebbe rispettare le norme di conservazione, impedire l'identificazione di massa delle vittime e offrire un rimedio in caso di dati personali inesatti.

16 Un progetto pilota di sei mesi con valutazione preregistrata

Un progetto pilota utile deve essere abbastanza circoscritto da poter essere governato e abbastanza ampio da verificare la catena causale. Ambito suggerito: tre registrar volontari, due operatori di registro, un partner di hosting/CDN, due feed di ricerca indipendenti e un collegio qualificato per i ricorsi. Il protocollo dello studio e le definizioni degli esiti devono essere registrati prima dell'assegnazione dei casi.

MESE 1

Mappatura dei protocolli e degli aspetti giuridici

Definire le categorie, le autorità competenti, i livelli di prova, la valutazione d'impatto sulla privacy e le condizioni di interruzione.

MESE 2

Strumentare il processo esistente

Misurare i timestamp e gli esiti di riferimento senza modificare il comportamento della risposta.

MESE 3

Sperimentare l'evidence envelope

Introdurre provenienza firmata, deduplicazione e classificazione dell'impatto collaterale.

MESE 4

Verificare gli obiettivi di risposta

Randomizzare i casi ammissibili o adottare un'introduzione graduale; monitorare quotidianamente gli errori.

MESE 5

Testare ricorsi e modalità di guasto

Effettuare esercitazioni di ripristino, simulazioni di segnalazioni malevole condotte da un red team e audit dei controlli di accesso.

MESE 6

Valutazione indipendente

Pubblicare le dimensioni dell'effetto, gli intervalli di confidenza, i dati mancanti, gli eventi avversi, i costi e il materiale necessario per la replicazione.

Risultati primari dello studio pilota

- Tempo mediano e al 90° percentile che intercorre tra l'acquisizione di prove validate e l'attuazione di misure di mitigazione efficaci.
- Differenza nel danno attribuibile successivo alla notifica o in un indicatore prestabilito dell'esposizione delle vittime.
- Tasso di falsi positivi, gravità delle azioni errate e tempo mediano di ripristino.
- Ricorrenza a livello dello stesso registrante, dello stesso cluster di infrastrutture e della stessa campagna.
- Costo operativo diretto per caso convalidato e per misura di mitigazione efficace.

REGOLA DECISIONALE

Ampliare solo se il progetto pilota dimostra una mitigazione efficace sostanzialmente più rapida senza superare i limiti preregistrati per falsi positivi, violazioni della privacy, ritardi nei ricorsi o interruzioni collaterali del servizio.

17 Conclusioni e raccomandazioni verificabili

La risposta al DNS Abuse non è né un filtro puramente tecnico né un problema che una singola istituzione possa risolvere da sola. I contratti vigenti dal 2024 hanno introdotto obblighi significativi di mitigazione, ma lasciano un'ampia discrezionalità in materia di prove, tempistiche e rimedi. Tale discrezionalità è necessaria alla proporzionalità; senza dati comparabili, rende anche difficile valutare le prestazioni.

1. **Standardizzare l'evidence envelope.** Adottare campi comuni per provenienza, timestamp ed esiti tra segnalanti, registrar, registri e fornitori di infrastrutture.
2. **Misurare le fasi separatamente.** Pubblicare i tempi relativi alla conferma, alla valutazione, alla decisione, alla mitigazione e al ricorso, suddivisi per classe di minaccia e livello di evidenza.
3. **Distinguere una registrazione dolosa da una compromissione.** Privilegiare la risoluzione dei problemi a livello di percorso/account per i servizi legittimi compromessi e riservare le misure a

livello di dominio ai casi in cui siano proporzionate.

4. **Sperimentare obiettivi di risposta.** Verificare obiettivi su scala oraria per registrazioni malevole a scopo unico e ad alta affidabilità, anziché dichiarare un termine universale.
5. **Pubblicare dati di responsabilità rispettosi della privacy.** Utilizzare un registro di trasparenza multilivello con cronologie firmate e prove ad accesso ristretto.
6. **Valutare l'impatto causale.** Non si deve equiparare una sospensione più rapida a un risparmio economico finché uno studio pre-registrato non avrà misurato l'impatto sulle vittime e il fenomeno dello spostamento.

La conclusione costruttiva non è che il problema originario scompaia una volta che le sue affermazioni siano state qualificate. È piuttosto che le affermazioni centrali possono ora essere verificate: l'intervallo di danno post-rilevamento compreso tra il 60 e l'85% costituisce un'ipotesi quantitativa esplicita; 100–150 dollari rappresentano un'ipotesi di budget ingegneristico verificabile per un livello definito di sensori e triage; e gli obiettivi di risposta su scala oraria possono essere sperimentati per registrazioni malevole a scopo unico e ad alta affidabilità. Pubblicare il carico di lavoro, i costi, i timestamp e i risultati, confrontarli con un valore di riferimento e misurare lo scostamento e l'errore. Una conferma giustificherebbe modifiche contrattuali e politiche; un rifiuto identificherebbe quale ipotesi si è rivelata errata.

Informativa editoriale e metodologica. PhishDestroy è un progetto indipendente e non commerciale di intelligence sulle minacce. Questa pubblicazione è una proposta di politica pubblica e ingegneria, non una consulenza legale, un programma di ICANN o un articolo sottoposto a revisione tra pari. Gli intervalli di bilancio indicati come «modelli» sono ipotesi di pianificazione. Le affermazioni tratte da fonti primarie sono collegate di seguito. Le correzioni possono essere inviate tramite i canali di contatto e di divulgazione responsabile del sito.

POSIZIONE IN PRIMA PERSONA · LA RESPONSABILITÀ DEVE LIMITARE SIA L'INAZIONE CHE L'ECCESSO

Un limite personale al potere esecutivo

Non sto chiedendo — né desidero — l'accesso diretto a uno strumento di blocco dei domini. Tale potere richiede una revisione indipendente, registri di audit accessibili al pubblico, un procedimento di ricorso rapido e la reversibilità.

Credo che esistano molte aziende competenti e responsabili a cui si potrebbero affidare alcune parti di questo lavoro. Sulla base della mia esperienza e dei dati che ho pubblicato, non includo NameSilo in tale gruppo.

Non consiglierei alle aziende statunitensi legittime di affidare funzioni delicate relative agli abusi o alla sicurezza a determinati appaltatori i cui conflitti di interesse, la cui competenza o la cui condotta non reggano a un esame indipendente. Si tratta di azioni documentate, non di nazionalità: l'origine russa di per sé non prova nulla, proprio come non prova nulla l'indirizzo di una società americana.

Voglio giustizia e una vera assunzione di responsabilità per i registrar che hanno ricavato introiti dalla registrazione e dal rinnovo di domini segnalati nell'ambito di ripetute campagne fraudolente. Laddove le prove indichino, al di là della semplice negligenza, una possibile complicità consapevole — sia che si tratti di un coinvolgimento operativo diretto, sia che si tratti di un ruolo di intermediario informato la cui funzione era quella di mantenere registrato e online un dominio dannoso nonostante ripetuti avvertimenti — tale condotta dovrebbe essere oggetto di un'indagine indipendente e, se confermata, comportare delle conseguenze. Non presento il sospetto come un fatto accertato; tuttavia, lo status di intermediario non deve conferire immunità dal controllo.

Esaminare l'indagine alla base del caso ↗

A

Riferimenti e note sulle fonti

[1] **ICANN: bilancio approvato per l'anno fiscale 27 (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Fonte dei finanziamenti operativi per l'anno fiscale 27, pari a 165,1 milioni di dollari, e composizione dei flussi di finanziamento.

[2] **ICANN: Emendamento globale del 2024 al Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Fonte contrattuale primaria degli obblighi dei registrar in materia di DNS Abuse.

[3] **ICANN: Emendamento globale 2024 all'Accordo di registrazione di base gTLD** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Fonte contrattuale primaria per gli obblighi di mitigazione a carico del gestore del registro.

[4] **Conformità contrattuale ICANN: avviso sugli obblighi relativi al DNS Abuse (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

Interpretazione operativa, requisiti delle segnalazioni ed esempi di mitigazione adeguata.

[5] **ICANN: attuazione dei requisiti di mitigazione del DNS Abuse (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf

Rapporto semestrale di attuazione e conteggio delle indagini e delle misure di mitigazione.

[6] **ICANN SSAC, SAC115: Relazione su un approccio interoperabile alla gestione degli abusi (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf

Contesto relativo all'interoperabilità delle segnalazioni di abusi e alla qualità delle prove.

[7] **Hollenbeck, RFC 5731: Mappatura dei nomi di dominio EPP (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

Definizione tecnica dei valori di stato del dominio EPP, compreso lo stato impostato dal server.

[8] **Laurie et al., RFC 9162: Certificate Transparency versione 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html

Specifica autorevole del protocollo e limiti di CT come sensore.

[9] **ICANN, Servizio centralizzato di dati sulle zone** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

Ambito di applicazione e modello di accesso per i file di zona dei gTLD partecipanti.

[10] **Centro di segnalazione dei reati informatici dell'FBI (IC3), Relazione annuale IC3 2025** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Dati relativi alle denunce e alle perdite segnalate, compresi i casi di phishing e spoofing.

[11] **Bijmans et al., "Catching Phishers By Their Bait" (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf

Misurazioni specifiche per ciascun set di dati relative all'infrastruttura di phishing e alla durata osservata.

[12] **Domini di nuova registrazione e durata delle attività di phishing, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020

Recenti dati empirici sui domini di phishing di nuova registrazione e sulla distribuzione nel corso del loro ciclo di vita.

[13] **Analisi inferenziale dei domini registrati a scopo doloso — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
Analisi finanziata da ICANN sulle registrazioni malevole e sui fattori dell'ecosistema; limiti pertinenti per le inferenze causali.

[14] **Chainalysis, Tendenze delle truffe nel settore delle criptovalute nel 2026** · https://www.chainalysis.com/blog/crypto-scams-2026/
Stima del fornitore relativa agli afflussi derivanti da truffe on-chain nel 2025; non considerata una stima complessiva del phishing basato su domini.

[15] **APWG, Rapporto sulle tendenze delle attività di phishing, primo trimestre 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf
Attacchi di phishing/URL rilevati; i dati riportati non corrispondono al numero di domini registrati unici.

[16] **Centro informazioni sulla criminalità informatica / Interisle, Panorama del phishing 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025
Distingue tra attacchi rilevati, domini unici e domini registrati a scopo doloso.

[17] **Verisign, Rapporto sul settore dei nomi di dominio, secondo trimestre 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/
Fonte dei dati relativi alle 401,6 milioni di registrazioni riportate per tutti i TLD.