LAPORAN TEKNIS · KERANGKA KERJA YANG DIUSULKAN · VERSI 1.0

Dari Deteksi hingga penerapan langkah tanggapan

Arsitektur terukur untuk tanggapan DNS Abuse: asal-usul dan rantai penguasaan bukti, tindakan proporsional, akuntabilitas publik, dan banding cepat—dirancang untuk diuji, bukan sekadar dinyatakan.

- Diterbitkan pada 2 Agustus 2026
- PhishDestroy Penelitian
- Draf konsultasi publik
- Belum melalui proses peninjauan sejawat

PD-WP-2026-01 · Versi 1.0 · Diterbitkan pada 2 Agustus 2026
URL permanen: https://phishdestroy.io/id/dns-abuse-enforcement-framework

ABSTRAK

USULAN INDEPENDEN · BUKAN BAGIAN DARI PROGRAM “ICANN”

Kesimpulan langsung. Ekosistem kontrak yang diatur oleh Undang-Undang Perlindungan Konsumen (gTLD) menunjukkan adanya kesenjangan yang dapat diukur antara penggunaan domain secara jahat yang telah diverifikasi secara teknis dan upaya mitigasi yang efektif. Studi yang telah dipublikasikan menunjukkan bahwa banyak kampanye phishing beroperasi selama berjam-jam atau berhari-hari, sementara prosedur kepatuhan kontrak dapat berlangsung dalam rentang waktu hari kerja. Model skenario yang diungkapkan menunjukkan bagaimana penundaan meningkatkan hasil yang diharapkan dari kampanye; kisaran 60–85% merupakan perkiraan utama yang dapat diuji dalam makalah ini mengenai kerugian pasca-pemberitahuan, bukan statistik yang telah ditetapkan untuk semua penipuan global. Perkiraan biaya teknik sebesar $100–150 berkaitan dengan pengumpulan dan pemrosesan awal kumpulan data zona, Transparansi Sertifikat, dan umpan publik yang telah ditentukan, bukan biaya penuh untuk tinjauan hukum atau penegakan hukum. Makalah ini mengusulkan bukti yang ditandatangani, target respons yang dapat diukur, eskalasi otomatis untuk kasus yang telah divalidasi, tindakan perbaikan yang proporsional, akuntabilitas publik, dan proses banding yang cepat. Makalah ini tidak mengusulkan pemberian akses langsung kepada pelapor ke kontrol penangguhan domain.

● SUMBER PRIMER
Didukung secara langsung oleh dokumen resmi atau penelitian yang telah dipublikasikan.

● MODEL ILUSTRATIF
Perhitungan yang dapat diulang, di mana masukan yang digunakan adalah asumsi, bukan rata-rata pasar.

● USULAN KEBIJAKAN
Sebuah desain yang diajukan untuk konsultasi, pengujian, dan revisi.

01 Pertanyaan penelitian, ruang lingkup, dan standar pembuktian

Pertanyaannya lebih spesifik daripada “siapa yang gagal?”: **Penundaan apa saja yang dapat dicegah antara bukti yang telah diverifikasi dan tindakan yang proporsional, serta intervensi mana yang dapat mengurangi**

kerugian yang dialami korban tanpa menimbulkan hasil positif palsu yang tidak dapat diterima atau dampak sampingan?

Ruang lingkupnya mencakup ekosistem gTLD yang terikat kontrak: pemegang nama domain, pengecer, pendaftar nama domain, lembaga pendaftaran, serta fungsi kepatuhan kontrak ICANN. Penyedia layanan hosting, CDN, peramban, layanan pembayaran, platform periklanan, CERT nasional, dan otoritas peradilan pidana hanya dimasukkan jika mereka memengaruhi rantai bukti atau rantai tanggapan. TLD kode negara memiliki tata kelola yang berbeda dan tidak dianggap tunduk pada kontrak gTLD dari ICANN.

Status tesis-tesis utama

- Makalah ini menganalisis ICANN sebagai lembaga tata kelola swasta dan penegakan kepatuhan kontrak dalam ekosistem gTLD. ICANN bukanlah regulator pemerintah atau badan penegak hukum, namun lembaga ini memberikan akreditasi kepada registrar, menandatangani perjanjian dengan operator registry, dan menegakkan perjanjian-perjanjian tersebut; lingkup kewenangan yang terbatas tersebut tidak menghilangkan pertanggungjawaban kelembagaan.
- Rentang 60–85% merupakan perkiraan kuantitatif utama dalam model dampak yang diuraikan dalam makalah ini. Angka tersebut disajikan sebagai perkiraan yang dapat diuji, yang diperoleh dari asumsi-asumsi eksplisit dan pengamatan kasus—bukan sebagai angka statistik yang sudah mapan untuk seluruh kasus penipuan di seluruh dunia. Penerbitan kumpulan data tingkat insiden yang menyelaraskan cap waktu deteksi, pemberitahuan, mitigasi, dan dampak merupakan langkah pembuktian berikutnya.
- Angka $100–150 merupakan perkiraan anggaran teknik yang dapat diuji untuk pengumpulan berkelanjutan dan penyaringan awal atas sekumpulan data yang telah ditentukan, meliputi zona yang dapat diakses, Certificate Transparency, dan data umpan publik mengenai infrastruktur komoditas. Angka ini bukanlah biaya untuk visibilitas global yang lengkap, tinjauan hukum, banding, ketersediaan tinggi, atau penegakan hukum. Oleh karena itu, makalah ini memperlakukannya sebagai tolok ukur yang dapat direproduksi dengan beban kerja, inventaris sumber, dan catatan biaya yang dipublikasikan—bukan sebagai harga universal yang telah terbukti. Perbedaan tersebut mempersempit klaim tanpa menghilangkan asimetri biaya yang sedang diuji.
- Perbandingan selama tiga minggu dalam makalah ini berkaitan dengan latensi kepatuhan, bukan SLA penutupan domain secara universal. ICANN's Pertanyaan Umum (FAQ) tentang Kepatuhan Kontrak disebutkan bahwa sebagian besar jenis keluhan dapat melewati tiga periode tanggapan berturut-turut masing-masing selama lima hari kerja sebelum ditindaklanjuti secara formal, sementara banyak kampanye jahat beroperasi selama berjam-jam atau berhari-hari. Kontrak-kontrak tersebut secara terpisah mensyaratkan tindakan mitigasi yang cepat dan tepat setelah adanya bukti yang dapat ditindaklanjuti. [2] [4]
- Untuk pendaftaran berbahaya yang telah diverifikasi dan memiliki tujuan tunggal, `serverHold` merupakan salah satu langkah mitigasi tingkat DNS yang paling mengganggu karena menghapus delegasi dari zona tersebut. Langkah ini tidak bersifat universal: langkah ini juga dapat mengganggu layanan email, subdomain, dan layanan yang sah; jawaban yang tersimpan dalam

cache mungkin tetap ada hingga masa berlaku TTL habis; dan layanan yang disusupi atau digunakan bersama mungkin memerlukan langkah mitigasi yang lebih spesifik. [4] [7]

KONTRIBUSI PENELITIAN

Usulan ini dapat diuji kebenarannya. Sebuah uji coba dapat membandingkan kelompok perlakuan dan kelompok kontrol berdasarkan waktu hingga triase, waktu hingga mitigasi, indikator pengganti korban, kekambuhan, hasil positif palsu, waktu pembalikan, dan dampak sampingan.

02 Apa yang dibuktikan oleh sumber-sumber primer

$165.1M

ICANN FY27 pendanaan operasional

Telah disetujui anggarFY27. Skala kontekstual; bukan pengeluarDNS Abuse. [1]

191,561

Keluhan terkait phishing/spoofing pada tahun 2025 IC3

Kategori pengaduan IC3 terbanyak berdasarkan jumlah; kerugian yang ditetapkan secara langsung sebesar $215,8 juta. [10]

24 jam

Umur rata-rata menurut sebuah studi tahun 2021

Hasil yang spesifik untuk kumpulan data tersebut mencakup 1.288 domain phishing; bukan masa aktif yang berlaku secara universal. [11]

Tidak ada SLA yang tetap

Batas waktu penarikan universal

Amandemen tahun 2024 menggunakan istilah “segera” dan “tepat” dalam konteks mitigasi, bukan satu batas waktu global. [2] [3]

USULAN	STATUS	APA YANG DAPAT DIKATAKAN
Phishing adalah DNS Abuse	TERVERIFIKASI	Phishing secara eksplisit merupakan salah satu dari lima kategori yang dicakup oleh amandemen kontraktual gTLD tahun 2024. [2]
Registrar wajib bertindak	TERVERIFIKASI	Registrar wajib bertindak segera ketika memiliki bukti yang dapat ditindaklanjuti bahwa nama yang disponsorinya digunakan untuk DNS Abuse. [2]
Operator registri wajib bertindak	TERVERIFIKASI	Operator registri wajib bertindak segera apabila, berdasarkan bukti yang dapat ditindaklanjuti, mereka secara wajar menentukan bahwa suatu nama terdaftar digunakan untuk DNS Abuse; tindakan yang tepat tetap bergantung pada konteks. [3]
`serverHold` mencabut pendelegasian	TERVERIFIKASI	Ini adalah status "EPP" yang ditetapkan oleh server. Jawaban yang disimpan dalam cache (DNS) mungkin tetap ada hingga masa berlakunya habis, dan tindakan ini berlaku untuk seluruh domain yang terdaftar. [7]
Semua DNS Abuse dapat terlihat di CZDS atau CT	SALAH	CZDS dan Certificate Transparency adalah sensor yang bernilai, bukan gambaran lengkap atau waktu nyata atas seluruh penggunaan domain. [8] [9]

Laporan enam bulan pertama ICANN mengenai pelaksanaan persyaratan kontrak berdasarkan amandemen tahun 2024 mencatat 192 penyelidikan, lebih dari 2.700 domain yang ditangguhkan, lebih dari 350 halaman phishing yang dinonaktifkan, dan dua Pemberitahuan Pelanggaran. Angka-angka tersebut tidak membuktikan bahwa pengendalian saat ini sudah memadai, tetapi angka-angka tersebut membantah klaim mutlak bahwa sistem tidak mengambil tindakan apa pun. [5]

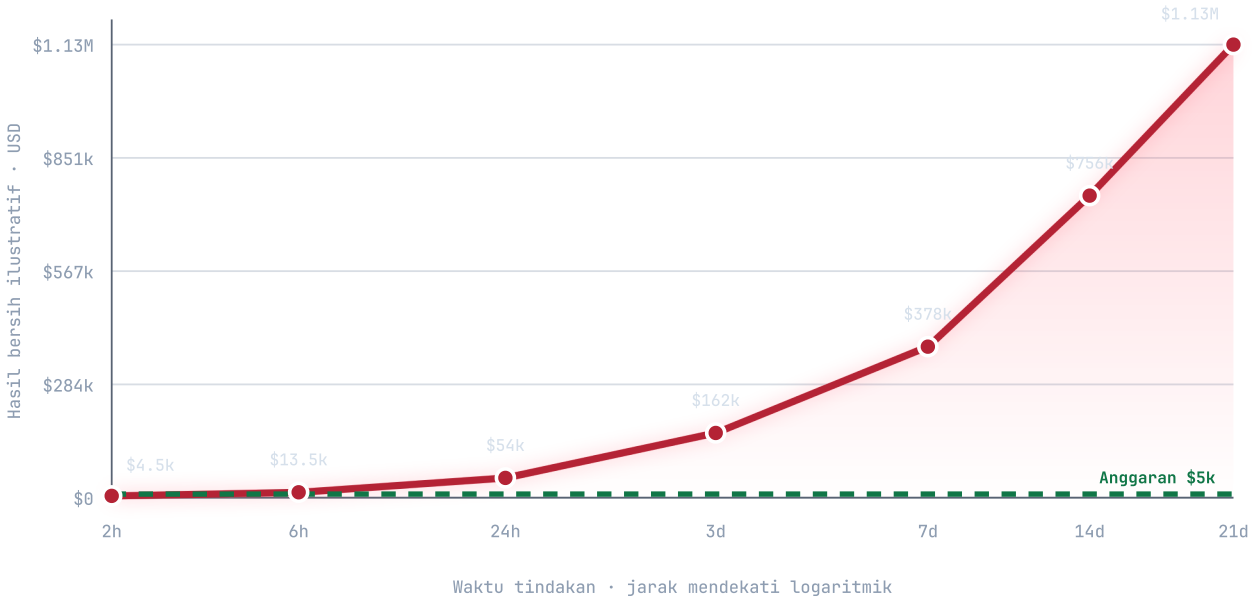
03 Mengapa latensi respons tetap menjadi objek penelitian yang sah

Beberapa operasi phishing berlangsung dalam rentang waktu beberapa jam atau beberapa hari. Bijmans dkk. melaporkan bahwa masa aktif rata-rata yang teramati adalah 45 jam dan mediannya 24 jam untuk 1.288 domain phishing dalam sebuah studi tahun 2021. [11] Sebuah studi tahun 2026 mengenai domain phishing yang baru terdaftar melaporkan distribusi yang sangat tidak seimbang: dari 14.112 domain dengan masa aktif yang dapat diukur, rata-rata masa aktifnya adalah 8,6 hari dan mediannya satu hari. [12] Kedua sampel tersebut tidak dapat digeneralisasikan untuk setiap kategori ancaman, namun keduanya menunjukkan mengapa proses yang hanya diukur dalam satuan hari kerja dapat melewatkan operasi penipuan dan phishing yang berlangsung singkat.

> **KETIDAKSESUAIAN WAKTU YANG DIUKUR**
>
> Studi-studi ini tidak menentukan porsi kerugian finansial yang terjadi setelah pemberitahuan, namun studi-studi tersebut menunjukkan adanya ketidaksesuaian waktu: suatu proses yang tahap-tahap kepatuhan informalnya di awal dapat memakan waktu hingga lima belas hari kerja tidak dapat, dengan sendirinya, berfungsi sebagai respons insiden untuk kampanye dengan masa hidup median mendekati satu hari. Oleh karena itu, titik 21 hari di bawah ini merupakan skenario latensi kepatuhan, bukan label untuk “SLA ICANN” yang bersifat universal.

GAMBAR 1 · ILUSTRASI HASIL KUMULATIF DARI OPERASI PENIPUAN DAN PHISHING

MODEL · JARAK WAKTU SEJENIS LOGARITMA



Kurva tersebut menggambarkan skenario yang dijelaskan pada Bagian 4; ini bukanlah data pasar yang sebenarnya. Penempatan secara horizontal dilakukan untuk memperpendek rentang waktu yang panjang demi kemudahan pembacaan. Sumber: model yang dapat direproduksi dengan masukan yang diungkapkan.

KEHATI-HATIAN KAUSAL

Masa aktif domain yang lebih singkat tidak secara otomatis berarti kerugian finansial dapat dicegah. Para penyerang mungkin berpindah, memanfaatkan situs yang telah diretas, mengubah saluran distribusi, atau mencairkan hasil kejahatan sebelum terdeteksi. Hubungan sebab-akibat tersebut harus diukur, bukan hanya disimpulkan berdasarkan kecepatan penutupan situs saja.

04 Ekonomi operasi penipuan dan phishing sebagai skenario yang dapat direplikasi

Aset yang secara ekonomi relevan seringkali bukanlah biaya pendaftaran, melainkan lalu lintas, konten kreatif, infrastruktur, dan kepercayaan yang terakumulasi di sekitar sebuah domain. Intuisi tersebut masuk akal; besarannya bervariasi tergantung pada operasi penipuan dan phishing. Oleh karena itu, kalkulator di bawah ini menampilkan setiap nilai masukan, alih-alih menyajikan hasil hipotetis sebagai rata-rata yang teramati.

DEFINISI MODEL

```
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
```

Kalkulator skenario

Ubah asumsi apa pun. Angka-angka tersebut hanya bersifat ilustratif dan bukan perkiraan pasar phishing pada umumnya.

`MODEL ILUSTRATIF`

Anggaran operasi penipuan dan phishing (USD)

5000

Kunjungan harian

2000

Tingkat konversi korban (%)

1.5

Rata-rata kerugian per korban (USD)

2400

Penyusutan saat pencairan dana (%)

25

Waktu pelaksanaan (jam)

24

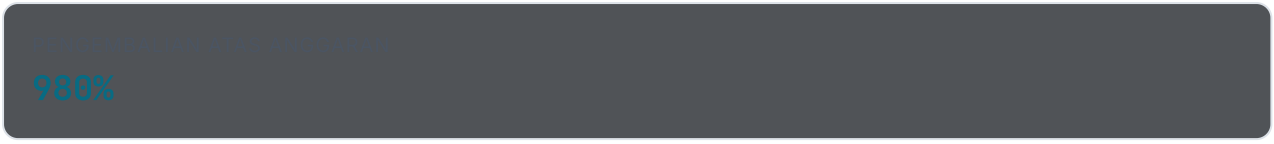
2,000

30

$54,000

$49,000

2.2 h



Karena model menyatakan nilai harapan, perkiraan jumlah korban dapat berupa bilangan desimal. Model tidak memperhitungkan penurunan trafik, perubahan perilaku setelah deteksi, perpindahan kampanye, korban berulang, atau distribusi ketidakpastian.

▶ Lihat tabel sumber model

05 Mengukur kerugian yang dapat dicegah tanpa memaksakan tingkat ketepatan

"Kerugian setelah deteksi" hanya dapat menjadi hasil yang berguna jika deteksi, penyampaian, dan kerugian didefinisikan secara konsisten. Cap waktu pada daftar hitam bukanlah bukti bahwa pendaftar domain telah menerima bukti yang dapat ditindaklanjuti. Transaksi dompet digital tidak secara otomatis dapat dikaitkan dengan satu domain tertentu. Domain yang menjadi tidak dapat diakses tidak menunjukkan pelaku mana yang menyebabkan perubahan tersebut.

Skema acara minimum

ACARA	CAP WAKTU YANG DIPERLUKAN	BUKTI MINIMUM
Pengamatan pertama	`t_obs`	Sensor, hash permintaan/respons, metode penangkapan, sumber jam.
Validasi teknis	`t_valid`	Indikator yang dapat direproduksi, identitas peninjau, kategori ancaman, dan tingkat keyakinan.
Pemberitahuan telah disampaikan	`t_pengumuman`	Versi tanda terima pengiriman yang telah diverifikasi dan paket bukti.
Pihak yang bertanggung jawab mengakui	`t_ack`	ID Kasus dan peran tujuan: host, pendaftar, pendaftar tingkat atas, platform, atau otoritas.
Tindakan mitigasi yang teramati	`t_mitigasi`	DNS (RTP), HTTP, status pembayaran, atau status platform, yang diukur dari berbagai sudut pandang.
banding / pemulihan	`t_restore`	Dasar pengambilan keputusan, bukti yang berubah, dan verifikasi pemulihan.
Peristiwa bahaya	`t_harm`	Laporan korban yang telah dianonimkan, transaksi yang dapat diidentifikasi, atau indikator pengganti lain yang terdokumentasi.

METRIK HASIL YANG DIUSULKAN

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

Pembilang dan penyebut harus menggunakan aturan atribusi yang sama. Hasil harus melaporkan kohort, interval kepercayaan, sensor kanan, sumber data yang hilang, penanganan korban ganda, dan sensitivitas terhadap jendela pengamatan. Label “dapat dicegah” harus disediakan khusus untuk desain kausal atau, setidaknya, perbandingan yang dipasangkan — bukan setiap kejadian setelah pemberitahuan.

PERKIRAAN MODEL SENTRAL · 60–85%

Makalah ini mempertahankan angka 60–85% sebagai perkiraan utama untuk porsi kerugian yang dapat dikaitkan yang terjadi setelah deteksi dan pemberitahuan dalam kategori insiden yang dimodelkan. Ini merupakan perkiraan skenario yang diperoleh dari asumsi yang diungkapkan dan pengamatan kasus—bukan statistik terukur untuk seluruh kasus penipuan di seluruh dunia. Perkiraan ini sebaiknya digunakan untuk analisis sensitivitas hingga dataset tingkat insiden menyelaraskan pengamatan, bukti yang tervalidasi, waktu terjadinya, mitigasi, dan cap waktu kerugian. Publikasi dataset tersebut merupakan uji bukti terhadap tesis ini, bukan alasan untuk menghapus tesis tersebut.

06 Peta kelembagaan: kapabilitas tersebar

Tidak ada satu pihak pun yang dapat memantau atau mengendalikan seluruh kejadian tersebut secara menyeluruh. Pihak pendaftar (registrar) mengetahui hubungan dengan pihak yang mendaftar (registrant); pihak registri (registry) mengendalikan status domain yang ditetapkan oleh registri; pihak host dan penyedia layanan penamaan (CDN) mengendalikan penyampaian konten; peramban (browser) dan penyedia layanan keamanan mengendalikan peringatan; penyedia layanan pembayaran dan dompet digital dapat menghentikan transfer; sementara pihak berwenang dapat memaksa pelestarian atau penyitaan data. Pihak yang mengendalikan (ICANN) menyusun dan menegakkan kontrak dalam ekosistem pendaftaran nama domain (gTLD), namun tidak mengoperasikan sistem kendali universal (EPP).

01 · SINYAL

Para peneliti & sensor

Amati indikator konten, infrastruktur, dan korban; pertahankan asal-usul dan rantai penguasaan bukti.

02 · LAYANAN

Penyelenggara / CDN / platform

Dapat menghapus konten atau memblokir akses dengan cepat, seringkali tanpa mengubah domain.

03 · SPONSOR

Registrar

Memeriksa penggunaan teknis yang berbahaya, menghubungi pemegang nama domain, dan dapat mengatur status di sisi klien.

04 · ZONA

Operator registri

Mengatur status "EPP" pada registri serta delegasi zona "TLD".

05 · KONTRAK

ICANN Kepatuhan

Menyelidiki kepatuhan pihak yang terikat kontrak; tidak menangani setiap kasus penipuan.

06 · HUKUM

CERT / pihak berwenang

Mengkoordinasikan tanggapan dan memanfaatkan kewenangan hukum yang berlaku di yurisdiksi masing-masing.

Kemampuan terdistribusi tidak berarti hilangnya tanggung jawab. Pendaftar sponsor tidak melepaskan kewajiban kontraktualnya dengan mendelegasikan penanganan penyalahgunaan kepada reseller; registri mengendalikan status EPP yang ditetapkan server; ICANN menegakkan kepatuhan kontraktual. Jejak audit harus mencatat tidak hanya siapa yang bertindak, tetapi juga siapa yang menerima bukti yang dapat ditindaklanjuti, mengalihkan kasus, gagal merespons, atau gagal melaksanakan tugas yang ditugaskan. Kewenangan hukum tetap berada pada pihak yang berwenang untuk menerapkan tindakan; pertanggungjawaban juga mencakup ketidakpatuhan yang terdokumentasi.

Konsentrasi pendanaan dan hipotesis konflik insentif yang dapat diuji

$165.1M

Dana Operasional "ICANN" Tahun Anggaran 27

Anggaran skenario dasar Tahun Anggaran 27 telah disetujui. [1]

≈98.1%

aliran pendapatan dari pendaftaran dan layanan pendaftaran

Sekitar $162,0 juta dari rencana pendanaan sebesar $165,1 juta. [1]

70.7%

biaya berbasis transaksi saja

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

Oleh karena itu, struktur pendanaan sangat terkonsentrasi pada pembayaran dari pihak-pihak yang terikat kontrak, yang perjanjiannya ditegakkan oleh ICANN, dan sebagian besar bergantung pada transaksi pendaftaran yang dapat ditagih. Hal ini menimbulkan ketergantungan struktural serta pertanyaan yang sah mengenai konflik insentif. Hal ini memang *tidak*, dengan sendirinya, tidak cukup untuk membuktikan adanya penegakan hukum yang sengaja dilemahkan atau terjadinya "regulatory capture" yang sudah terjadi sepenuhnya. Hipotesis "regulatory capture" tersebut perlu diuji dengan membandingkannya terhadap waktu respons pada tingkat kasus, hasil penegakan hukum, sanksi, pelanggaran berulang, serta peran pemangku kepentingan yang menerima pendanaan dalam pengambilan keputusan terkait kebijakan dan pelaksanaannya.

07 Dasar kontrak tahun 2024 — dan hal-hal yang tidak disebutkan di dalamnya

Amandemen global April 2024 terhadap Perjanjian Akreditasi Registrar dan Perjanjian Registri Dasar menetapkan kewajiban tegas untuk memitigasi DNS Abuse. Registrar wajib bertindak segera ketika memiliki bukti yang dapat ditindaklanjuti bahwa nama yang disponsorinya digunakan untuk DNS Abuse. Operator registri wajib bertindak segera apabila, berdasarkan bukti yang dapat ditindaklanjuti, mereka secara wajar menentukan bahwa suatu nama terdaftar digunakan untuk DNS Abuse. Dalam kedua kasus, tindakan yang tepat bergantung pada konteks, tingkat keparahan, dan dampak sampingan. [2] [3]

Tiga garis waktu yang sering disamakan

GARIS WAKTU	HAL INI BERLAKU UNTUK	APA YANG TIDAK DIMAKSUDKAN
24 jam	Peninjauan, berdasarkan RAA §3.18.3, atas laporan yang beralasan kuat mengenai Kegiatan Ilegal yang disampaikan kepada kontak khusus oleh lembaga penegak hukum, perlindungan konsumen, lembaga semi-pemerintah, atau otoritas sejenis.	Ini bukanlah batas waktu penangguhan 24 jam yang berlaku secara universal.
“Segera”	Melakukan langkah-langkah mitigasi yang tepat setelah ambang batas bukti yang dapat dijadikan dasar tindakan terpenuhi.	Jumlah jamnya tidak tetap dan tidak selalu memerlukan penanganan yang sama dalam setiap kasus.
21 hari	Dapat muncul sebagai masa penyelesaian setelah diterbitkannya Pemberitahuan Pelanggaran kontrak secara resmi.	Ini bukanlah masa aktif biasa yang diberikan kepada setiap domain berbahaya yang dilaporkan.

Fleksibilitas ini memiliki manfaat: domain universitas yang diretas tidak seharusnya ditangani seperti domain phishing tujuan tunggal yang baru didaftarkan. Masalah akuntabilitasnya adalah bahwa istilah “segera” dan “tepat” sulit untuk dibandingkan tanpa adanya cap waktu yang dipublikasikan, kategori kasus, dan kode hasil. Usulan di bawah ini menambahkan mekanisme pengukuran dan peninjauan tanpa menganggap bahwa satu batas waktu berlaku untuk setiap kasus.

08 Masalah batas cakupan: phishing sudah tercakup; beberapa bentuk penipuan keuangan mungkin tidak tercakup

Phishing secara eksplisit termasuk dalam definisi kontraktual DNS Abuse. Batas yang lebih sulit menyangkut situs yang menipu pengguna dengan nama aslinya sendiri, alih-alih menyamar sebagai pihak ketiga yang dapat dikenali—misalnya platform investasi palsu, toko penipuan, penipuan pemulihan dana, dan skema tanda tangan dompet. Bergantung pada fakta, kasus tersebut dapat diperlakukan sebagai pelanggaran pada lapisan konten situs, penipuan konsumen, atau kategori hukum lain, bukan DNS Abuse kontraktual.

> USULAN LABEL PENELITIAN
>
> **Penyalahgunaan yang Menimbulkan Kerugian Finansial Terverifikasi (VFHA)**: penggunaan domain yang terdokumentasi untuk memperoleh dana, kredensial pembayaran, kunci privat, atau frasa seed melalui penipuan, terlepas dari adanya peniruan merek. VFHA bukan terminologi ICANN saat ini dan tidak dengan sendirinya menciptakan kewenangan kontraktual.

Konsultasi kebijakan dapat mempertimbangkan apakah kategori sempit berbasis bukti seperti VFHA sebaiknya dimasukkan ke dalam kontrak mendatang, kerangka rujukan lintas sektor, atau hukum

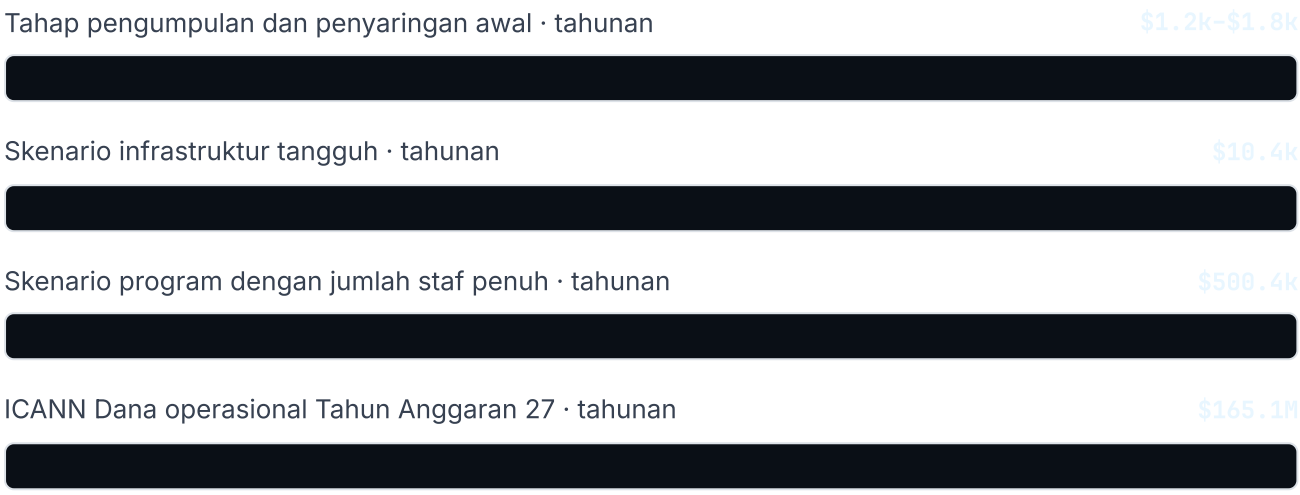
nasional. Perluasan harus mensyaratkan uji kerugian yang tepat, bukti andal, pemulihan proporsional, tinjauan yurisdiksi, dan banding. Label “penipuan” yang samar tidak memadai.

09 Apa yang harus dibuktikan oleh klaim pemantauan senilai $100–150 per bulan—dan apa yang tidak dapat dibuktikannya

Sebuah server komoditas dapat mengunduh snapshot yang dapat diakses dari berkas zona gTLD yang berpartisipasi dan menghitung perubahannya secara lokal, mengimpor peristiwa Certificate Transparency yang dipilih serta umpan terbuka, menormalisasi string, menghitung hash, dan memprioritaskan kandidat. Ini merupakan tolok ukur teknik yang berguna dan dapat diuji—bukan “pemantauan Internet secara menyeluruh.” Pada kuartal kedua tahun 2026, Verisign melaporkan 401,6 juta pendaftaran di seluruh TLD; CZDS mencakup berkas zona gTLD yang berpartisipasi, bukan semua TLD, dan CT mencatat sertifikat atau pra-sertifikat yang tercatat secara publik, bukan setiap domain yang aktif atau berbahaya. [8] [9] [17]

KEMAMPUAN	PROTOTIPE KOMODITAS	LAYANAN KEPENTINGAN PUBLIK SKALA PRODUKSI
Penerimaan zona/CT/feed	Layak untuk kumpulan sumber tertentu	Kolektor redundan, kontrak sumber, pemantauan kesenjangan
Triase string/hash	Layak	Pembandingan, deteksi pergeseran, studi negatif palsu
Perenderan peramban	Subhimpunan sampel kecil	Armada terisolasi, titik pengamatan regional, pembatasan malware
Penentuan hukum	Tidak termasuk	Peninjau berkualifikasi, pemetaan yurisdiksi dan kewenangan
Ketersediaan tinggi / retensi bukti	Biasanya tidak tersedia	Tanda tangan berbasis HSM, log audit, cadangan, dan respons insiden
Banding dan pemulihan	Tidak termasuk	Operasi 24/7, eskalasi independen, dan target layanan

GAMBAR 2 · KONTEKS ORDE BESAR — LEBAR LOGARITMIK · BIAYA YANG TIDAK SETARA



Lebar logaritmik memastikan nilai-nilai kecil tetap terlihat. Tiga angka pertama merupakan asumsi teknik atau program yang diungkapkan secara terbuka yang memerlukan tolok ukur yang dipublikasikan dan bukan penawaran harga dari vendor. ICANN Pendanaan operasional merupakan angka berskala institusional yang telah diverifikasi. Angka-angka ini sengaja dibuat tidak setara: perbandingan ini bertujuan untuk menguji apakah pengumpulan dan penyortiran dasar merupakan biaya yang secara inheren terlalu mahal, bukan untuk menguji apakah program penegakan hukum yang lengkap berharga $100 per bulan.

10 Usulan Kerangka Tanggapan DNS Abuse Terverifikasi

Kerangka kerja yang diusulkan ini merupakan arsitektur acuan, bukan “kill switch” global otomatis. Kerangka kerja ini menstandarkan format kasus, catatan keputusan, dan cap waktu, sekaligus memungkinkan operator yang berwenang untuk memilih tindakan efektif yang paling minim menimbulkan gangguan.

01 · PENGOLAHAN DATA

Memperoleh & melestarikan

Mengumpulkan laporan dan pengamatan; mengolah artefak mentah; menyinkronkan jam.

02 · asal-usul dan riwayat penanganan bukti

Menyusun bukti secara sistematis

Catat asal, metode, riwayat penanganan, dan ketergantungan sumber.

03 · MEMVERIFIKASI

Menguatkan

Ulangi perilaku yang merugikan tersebut dan bedakan bukti-bukti yang independen.

04 · MENILAI

Risiko & jaminan

Klasifikasikan pendaftaran berbahaya, layanan yang disusupi, hosting bersama, dan tingkat kritisnya.

05 · MENJAWAB

Berikan pemberitahuan & lakukan mitigasi

Tentukan pihak yang bertanggung jawab, batas waktu, dan langkah perbaikan yang efektif serta seminimal mungkin menimbulkan gangguan.

06 · ULASAN

Audit dan banding

Menerbitkan metadata hasil, mengukur dampak, dan mendukung perbaikan cepat.

Tingkat bukti

E1

Sinyal yang belum diverifikasi

Sumber informasi tunggal, kecocokan leksikal, atau klaim reputasi. Cocok untuk pengamatan, namun tidak pernah cukup jika digunakan sendirian sebagai dasar penangguhan.

E2

Perilaku yang ditiru

Rekaman berstempel waktu yang menunjukkan pencurian kredensial, penyebaran malware, atau jalur transaksi yang menipu.

E3

Pembuktian independen

Setidaknya dua sumber yang benar-benar independen atau satu bukti teknis yang dapat direproduksi, ditambah verifikasi kepemilikan dan konteks.

E4

Konfirmasi yang sah

Pihak berwenang, layanan yang terdampak, pemilik merek, atau bukti korban yang telah diverifikasi, dengan rantai pengendalian yang menjamin privasi.

ATURAN KEMERDEKAAN

Tiga feed yang menyalin daftar blokir hulu yang sama adalah satu sumber, bukan tiga. Grafik asal-usul dan rantai penguasaan bukti harus memperlihatkan sumber bersama, sinkronisasi, dan publikasi ulang oleh vendor.

11 Paket bukti minimal dan API yang interoperabel

API harus membuat kasus yang dapat diverifikasi dan memulai penghitung waktu respons yang dapat diaudit; seorang pelapor tidak boleh dapat mengeluarkan perintah penangguhan secara langsung. Jika kasus E3/E4 berkaitan dengan pendaftaran berbahaya yang bertujuan tunggal dan kedaluwarsa tanpa keputusan yang beralasan atau mitigasi yang efektif, sistem secara otomatis akan meneruskannya ke operator registri atau pihak lain yang memiliki kewenangan kontraktual atau hukum. A `serverHold` Perintah hanya dapat berasal dari pihak yang berwenang. Eskalasi otomatis dan kewenangan pendaftaran untuk bertindak saat masa berlaku habis merupakan usulan perubahan kebijakan, bukan klaim mengenai kewenangan yang sudah ada. Setiap transisi status ditandatangani dan dicatat dalam log audit.

POST /V1/CASES · CONTOH

```
{
  "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:…"
}
```

Respons yang berhasil akan mengembalikan ID kasus, pihak penerima, tingkat bukti, kesalahan kelengkapan, waktu peninjauan yang ditargetkan, dan URL transparansi publik. Respons tersebut tidak boleh menjanjikan tindakan perbaikan tertentu sebelum pihak yang berwenang mengevaluasi kewenangan dan dampak sampingan.

12 Target tanggapan yang diusulkan, bukan batas waktu penghapusan yang berlaku secara universal

Sasaran tingkat layanan sebaiknya dibedakan *ucapan terima kasih*, *triase*, *keputusan* dan *mitigasi yang efektif*. Hal ini memungkinkan kinerja diukur tanpa mengasumsikan bahwa penangguhan selalu merupakan hasil yang tepat.

PROFIL KASUS	MENGAKUI	TARGET TRIASE	TARGET KEPUTUSAN	PILIHAN JAWABAN YANG UMUM
Pencurian kredensial pembayaran E3/E4 atau frasa benih pada pendaftaran berbahaya yang dirancang khusus untuk tujuan tertentu	15 menit	1 jam	4 jam	Blok konten; penangguhan oleh registrar/registry jika diizinkan; peringatan terkait browser dan pembayaran.
Penipuan bermerek E3 atau penyebaran malware	30 menit	2 jam	6 jam	Penghapusan Host/CDN, mitigasi domain, sinkhole, atau peringatan sesuai dengan titik kendali.
Domain sah yang diretas atau penyewa SaaS bersama	1 jam	4 jam	12 jam	Isolasi jalur/akun dan pemulihan pemilik; hindari penangguhan domain terdaftar sebisa mungkin.
Penipuan keuangan dengan klasifikasi yang diperdebatkan	4 jam	12 jam	24 jam	Pelestarian, intervensi platform/pembayaran, rujukan oleh otoritas, dan keputusan yang didasarkan pada pertimbangan.
Sinyal E1 atau laporan yang tidak lengkap	Otomatis	24 jam	Belum ada sampai diverifikasi	Pantau, perkuat, dan minta bukti.

Ini adalah target awal. Nilai yang tepat harus ditentukan berdasarkan masa aktif ancaman yang teramati, jumlah personel, biaya kesalahan, dan batasan hukum, kemudian dipublikasikan bersama distribusi pencapaian, bukan hanya nilai rata-rata tunggal.

13 Keamanan, prosedur yang semestinya, privasi, dan skenario kegagalan

Tanggapan yang cepat tanpa langkah-langkah pengamanan dapat memperparah masalah data yang salah hingga berujung pada sensor, sabotase komersial, atau gangguan infrastruktur. Oleh karena itu, arsitektur yang tepat menganggap hasil positif palsu dan dampak sampingan sebagai kegagalan keamanan yang sangat serius.

MODE KEGAGALAN	KONTROL YANG DIPERLUKAN	TINDAKAN YANG DAPAT DIAUDIT
Laporan yang berniat jahat terhadap pesaing	Verifikasi jati diri jurnalis, reputasi sumber, reproduksi independen, dan sanksi atas penggunaan teknis yang bersifat jahat	Tingkat penolakan laporan berdasarkan pelapor; kasus manipulasi yang terkonfirmasi
Sirkularitas pasokan yang menyamar sebagai konsensus	Grafik asal-usul bukti dan penghapusan duplikat sumber hulu	Penghitungan dari sumber independen sebelum dan sesudah koreksi garis keturunan
Domain sah yang diretas ditangguhkan secara massal	Klasifikasi niat pendaftaran dan preferensi mitigasi pada tingkat jalur	Pembagian domain yang disusupi; layanan sah yang terdampak
Data korban atau rincian eksploitasi bocor ke publik	Pengungkapan berjenjang, penyuntingan, barang bukti yang disegel, dan batas waktu penyimpanan	Insiden privasi; hasil tinjauan penyuntingan
Tindakan yang tidak semestinya terus berlanjut	Layanan penerimaan 24/7 melalui banding, peninjau independen, dan jalur pemulihan yang terverifikasi	Waktu pembalikan median dan persentil ke-95
Penangguhan registri menyebabkan gangguan layanan email/subdomain	Inventaris jaminan, proporsionalitas tindakan hukum, dan pemantauan pasca-tindakan	Gangguan layanan per tindakan; tingkat pemulihan

Jaminan prosedur hukum yang layak minimal

1. Kode alasan, tingkat bukti, dan pengambil keputusan yang bertanggung jawab dicatat untuk setiap tindakan pembatasan.
2. Seorang pendaftar dapat memperoleh pernyataan alasan yang menjamin privasi dan mengajukan bukti tandingan.
3. Kasus-kasus yang bersifat mendesak (banding) ditinjau oleh seseorang yang tidak terlibat dalam pengambilan keputusan awal.
4. Pembalikan menyebar melalui saluran bertanda yang sama dengan tindakan aslinya.
5. Statistik kesalahan dan pemulihan secara keseluruhan bersifat terbuka untuk umum; sedangkan bukti-bukti sensitif tetap dikendalikan aksesnya.

14 Dari “skor toksisitas” menuju Indeks Kualitas Respons yang Akuntabel

Skor pendaftar publik dapat meningkatkan akuntabilitas, namun peringkat yang dibuat secara sembarangan dapat terdistorsi oleh ukuran portofolio, cakupan data, komposisi pelanggan, serta apakah domain tersebut didaftarkan dengan niat jahat atau kemudian diretas. Skor tersebut tidak boleh dijadikan alasan untuk melakukan pemblokiran massal terhadap seluruh pelanggan dari sebuah pendaftar.

VEKTOR KUALITAS YANG DIUSULKAN

```
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.
```

Jika diperlukan penilaian gabungan (composite) untuk tujuan tata kelola, bobot harus ditetapkan sebelum evaluasi, diuji sensitivitasnya, dan diuji kembali (backtest) terhadap kasus-kasus yang disisihkan. Hasilnya harus dikelompokkan berdasarkan jenis ancaman (TLD), ukuran pendaftar (registrar size), kelas ancaman (threat class), dan sumber bukti. Hasil akhirnya adalah sinyal akuntabilitas — bukan putusan otomatis mengenai domain.

15 Basis Data Transparansi Publik DNS Abuse dengan akses berjenjang

Pendaftaran transparansi dapat menghilangkan perselisihan mengenai apakah suatu pemberitahuan pernah ada, kapan pemberitahuan tersebut disampaikan, dan tindakan apa yang diambil selanjutnya. Namun, mempublikasikan setiap bukti dapat membahayakan identitas korban, data pribadi, metode investigasi, dan jalur eksploitasi yang masih aktif. Solusinya adalah sistem akses berjenjang.

P

Catatan publik

ID Kasus, indikator, kategori umum, penanda waktu utama, tingkat bukti, peran pelaku, kode hasil, status "banding", dan hash dari artefak yang disegel.

C

Tampilan pihak yang terikat kontrak

Bukti teknis yang dapat direproduksi, saluran komunikasi, konteks tambahan, dan petunjuk pelestarian.

R

Tampilan dengan wewenang terbatas

Data korban, atribusi keuangan, bahan penyelidikan yang sedang berlangsung, dan rantai penguasaan barang bukti yang belum disunting.

Setiap pembaruan bersifat "append-only", dilengkapi cap waktu, dan ditandatangani. Koreksi tidak menghapus riwayat; melainkan menambahkan catatan yang menggantikan catatan sebelumnya. Pencarian publik harus mematuhi aturan penyimpanan, mencegah pengungkapan massal identitas korban, dan menyediakan mekanisme ganti rugi atas data pribadi yang tidak akurat.

16 Program percontohan selama enam bulan dengan evaluasi berbasis pendaftaran awal

Sebuah uji coba awal yang bermanfaat harus cukup kecil agar dapat dikelola dengan baik dan cukup besar untuk menguji rantai kausal. Cakupan yang disarankan: tiga pendaftar sukarela, dua operator registri, satu mitra hosting/CDN, dua sumber data penelitian independen, dan panel banding yang berkualifikasi. Protokol penelitian dan definisi hasil harus didaftarkan sebelum kasus-kasus dialokasikan.

BULAN 1

Pemetaan protokol dan hukum

Tentukan kategori, otoritas, tingkatan bukti, penilaian dampak privasi, dan kondisi penghentian.

BULAN KE-2

Menerapkan proses yang sudah ada

Ukur cap waktu awal dan hasil tanpa mengubah perilaku respons.

BULAN KE-3

Jalankan paket bukti

Terapkan asal-usul bukti bertanda tangan, penghapusan duplikat, dan klasifikasi dampak sampingan.

BULAN KE-4

Target respons uji

Lakukan pengacakan terhadap kasus-kasus yang memenuhi syarat atau gunakan pendekatan peluncuran bertahap; pantau kesalahan setiap hari.

BULAN KE-5

Latihan "banding" dan kegagalan

Melaksanakan simulasi pemulihan, laporan serangan simulasi (red-team), dan audit terhadap kontrol akses.

BULAN KE-6

Evaluasi independen

Publikasikan ukuran efek, interval kepercayaan, data yang hilang, kejadian tidak diinginkan, biaya, dan bahan replikasi.

Hasil utama program percontohan

- Waktu median dan persentil ke-90 dari bukti yang telah divalidasi hingga penerapan mitigasi yang efektif.
- Perbedaan dalam kerugian yang dapat dikaitkan setelah pemberitahuan atau indikator paparan korban yang telah ditentukan sebelumnya.
- Tingkat hasil positif palsu, tingkat keparahan tindakan yang keliru, dan waktu pemulihan median.
- Pengulangan pada pendaftar, klaster infrastruktur, dan tingkat operasi penipuan/phishing yang sama.
- Biaya operasional langsung per kasus yang telah diverifikasi dan per langkah mitigasi yang efektif.

ATURAN PENGAMBILAN KEPUTUSAN

Lakukan penskalaan hanya jika uji coba menunjukkan mitigasi efektif yang secara signifikan lebih cepat tanpa melampaui batas-batas yang telah ditetapkan sebelumnya terkait hasil positif palsu, insiden privasi, penundaan dalam layanan "banding", atau gangguan layanan yang tidak disengaja.

17 Kesimpulan dan rekomendasi yang dapat diuji

Respons terhadap DNS Abuse bukan sekadar filter teknis, dan bukan pula masalah yang dapat diselesaikan oleh satu lembaga saja. Perubahan kontrak tahun 2024 menetapkan kewajiban mitigasi yang bermakna, tetapi tetap memberikan keleluasaan besar terkait bukti, waktu, dan tindakan pemulihan. Keleluasaan itu diperlukan demi proporsionalitas; tanpa catatan yang dapat dibandingkan, kinerja juga sulit dievaluasi.

1. **Standarkan paket bukti.** Gunakan bidang bersama untuk asal-usul bukti, stempel waktu, dan hasil di antara pelapor, registrar, registri, dan penyedia infrastruktur.
2. **Ukur setiap tahap secara terpisah.** Publikasikan waktu konfirmasi penerimaan, triase, keputusan, mitigasi, dan banding berdasarkan kelas ancaman dan tingkat bukti.
3. **Bedakan pendaftaran berbahaya dari kompromi layanan.** Prioritaskan pemulihan pada tingkat jalur/akun untuk layanan sah yang terkompromi, dan gunakan tindakan seluruh domain hanya

ketika proporsional.

4. **Uji coba target respons.** Uji sasaran berskala jam untuk pendaftaran berbahaya dengan keyakinan tinggi dan tujuan tunggal, alih-alih menetapkan tenggat universal.
5. **Publikasikan data akuntabilitas yang menjamin privasi.** Gunakan sistem pendaftaran transparansi berjenjang yang dilengkapi dengan riwayat yang telah ditandatangani dan bukti yang dibatasi aksesnya.
6. **Evaluasi dampak kausal.** Jangan menyamakan penangguhan yang lebih cepat dengan uang yang terselamatkan sebelum studi praregistrasi mengukur dampak terhadap korban dan perpindahan ancaman ke saluran lain.

Kesimpulan yang konstruktif bukanlah bahwa masalah awal akan hilang begitu klaim-klaimnya dikualifikasi. Melainkan bahwa klaim-klaim inti kini dapat diuji: rentang kerugian pasca-deteksi sebesar 60–85% merupakan hipotesis kuantitatif yang eksplisit; $100–150 merupakan asumsi anggaran teknik yang dapat diuji untuk lapisan sensor dan triase yang telah didefinisikan; dan target respons dalam skala jam dapat diuji coba untuk pendaftaran jahat yang memiliki tingkat keyakinan tinggi dan tujuan tunggal. Publikasikan beban kerja, biaya, cap waktu, dan hasilnya, bandingkan dengan garis dasar, lalu ukur pergeseran dan kesalahannya. Konfirmasi akan membenarkan perubahan kontrak dan kebijakan; penolakan akan mengidentifikasi asumsi mana yang gagal.

Pengungkapan mengenai editorial dan metode. PhishDestroy merupakan proyek intelijen ancaman yang independen dan non-komersial. Publikasi ini merupakan usulan kebijakan dan teknis, bukan nasihat hukum, program "ICANN", atau makalah yang telah melalui tinjauan sejawat. Kisaran anggaran yang disebut sebagai "model" merupakan asumsi perencanaan. Klaim yang bersumber langsung dari sumber primer tercantum dalam tautan di bawah ini. Koreksi dapat disampaikan melalui saluran kontak dan saluran pengungkapan bertanggung jawab di situs ini.

POSISI ORANG PERTAMA · AKUNTABILITAS HARUS MEMBATASI BAIK KELAMBANAN MAUPUN TINDAKAN YANG MELAMPAUI BATAS

Batasan pribadi atas kewenangan penegakan hukum

Saya tidak meminta — dan tidak menginginkan — akses langsung ke alat pemblokiran domain. Kewenangan tersebut memerlukan peninjauan independen, catatan audit yang terbuka untuk umum, mekanisme banding yang cepat, serta kemampuan untuk membatalkan keputusan.

Saya yakin ada banyak perusahaan yang kompeten dan bertanggung jawab yang dapat dipercaya untuk menangani sebagian pekerjaan ini. Berdasarkan pengalaman saya dan catatan yang telah saya publikasikan, saya tidak memasukkan NameSilo ke dalam kelompok tersebut.

Saya tidak akan menyarankan perusahaan-perusahaan AS yang sah untuk mempercayakan fungsi-fungsi sensitif terkait penyalahgunaan atau keamanan kepada kontraktor tertentu yang konflik kepentingan, kompetensi, atau perilakunya tidak dapat bertahan dari pemeriksaan independen. Ini berkaitan dengan tindakan yang tercatat, bukan kewarganegaraan: asal-usul Rusia itu sendiri tidak membuktikan apa-apa, sama halnya dengan alamat perusahaan di AS yang juga tidak membuktikan apa-apa.

Saya menginginkan keadilan dan pertanggungjawaban yang sesungguhnya bagi penyedia layanan pendaftaran domain yang memperoleh pendapatan dari pendaftaran dan perpanjangan domain yang tercatat sebagai bagian dari kampanye penipuan berulang. Apabila bukti menunjukkan bahwa hal tersebut melampaui kelalaian dan mengarah pada kemungkinan adanya fasilitasi yang disengaja—baik melalui keterlibatan operasional langsung maupun bertindak sebagai perantara yang mengetahui situasi, yang fungsinya adalah mempertahankan pendaftaran dan akses online domain berbahaya tersebut meskipun telah menerima peringatan berulang kali—maka perilaku tersebut harus diselidiki secara independen dan, jika terbukti, harus dikenakan sanksi. Saya tidak menyajikan kecurigaan ini sebagai fakta yang telah terbukti; namun, status sebagai perantara tidak boleh memberikan kekebalan dari pengawasan.

Tinjau penyelidikan yang mendasari ↗

A

Daftar Pustaka dan Catatan Sumber

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Sumber untuk pendanaan operasi FY27 sebesar $165.1 juta dan komposisi aliran pendanaan.

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Sumber kontraktual utama untuk kewajiban DNS Abuse registrar.

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Sumber kontraktual utama untuk kewajiban mitigasi operator registri.

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (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
Interpretasi operasional, persyaratan laporan, dan contoh mitigasi yang tepat.

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
Laporan implementasi enam bulan, termasuk jumlah investigasi dan mitigasi.

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
Latar belakang interoperabilitas laporan DNS Abuse dan kualitas bukti.

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
Definisi teknis mengenai nilai-nilai status domain EPP, termasuk status yang ditetapkan oleh server.

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
Spesifikasi protokol yang sah dan batasan-batasan CT sebagai sensor.

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
Cakupan dan model akses untuk berkas zona gTLD yang berpartisipasi.

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
Jumlah pengaduan dan laporan kerugian, termasuk jumlah kasus phishing/spoofing.

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
Pengukuran infrastruktur phishing yang spesifik untuk setiap kumpulan data serta masa aktif yang teramati.

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
Bukti empiris terkini mengenai domain phishing yang baru terdaftar dan distribusi masa aktifnya.

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

ICANN -analisis yang didanai mengenai pendaftaran domain berbahaya dan faktor-faktor ekosistem; batasan-batasan yang relevan terkait klaim kausalitas.

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/

Perkiraan vendor mengenai arus masuk dana dari penipuan on-chain pada tahun 2025; tidak dimasukkan ke dalam total penipuan phishing berbasis domain.

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Serangan phishing/URL yang terdeteksi; metrik ini tidak sama dengan jumlah domain terdaftar yang unik.

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Memisahkan serangan yang terdeteksi, domain unik, dan domain yang didaftarkan dengan tujuan jahat.

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Sumber data mengenai 401,6 juta pendaftaran yang dilaporkan di seluruh TLD.