BÁO CÁO KỸ THUẬT · KHUNG ĐỀ XUẤT · PHIÊN BẢN 1.0

Từ phát hiện đến triển khai biện pháp ứng phó

Một kiến trúc có thể đo lường cho hoạt động ứng phó DNS Abuse: nguồn gốc và chuỗi lưu giữ bằng chứng, hành động tương xứng, trách nhiệm giải trình công khai và cơ chế khiếu nại nhanh—được thiết kế để kiểm thử chứ không chỉ để tuyên bố.

Xuất bản ngày 2 tháng 8 năm 2026

PhishDestroy Nghiên cứu

Bản dự thảo lấy ý kiến công chúng

Chưa được bình duyệt

PD-WP-2026-01 · Phiên bản 1.0 · Xuất bản ngày 2 tháng 8 năm 2026
URL cố định: https://phishdestroy.io/vi/dns-abuse-enforcement-framework

TÓM TẮT

ĐỀ XUẤT ĐỘC LẬP · KHÔNG PHẢI LÀ CHƯƠNG TRÌNH "ICANN"

Kết luận trực tiếp. Hệ sinh thái hợp đồng thông minh (gTLD) tồn tại một khoảng cách có thể đo lường được giữa việc sử dụng tên miền với mục đích độc hại đã được xác thực về mặt kỹ thuật và các biện pháp giảm thiểu hiệu quả. Các nghiên cứu đã công bố cho thấy nhiều chiến dịch lừa đảo (phishing) diễn ra trong nhiều giờ hoặc nhiều ngày, trong khi các thủ tục tuân thủ hợp đồng có thể kéo dài trong khung thời gian của ngày làm việc. Mô hình kịch bản được công bố cho thấy cách thức sự chậm trễ làm tăng lợi nhuận dự kiến của chiến dịch; khoảng 60–85% là ước tính chính có thể kiểm chứng của bài báo về thiệt hại sau khi nhận thông báo, không phải là số liệu thống kê đã được xác lập cho tất cả các vụ lừa đảo trên toàn cầu. Ước tính chi phí kỹ thuật từ 100–150 USD liên quan đến việc thu thập và xử lý sơ bộ một tập dữ liệu được xác định trước về vùng tên miền, Certificate Transparency và dữ liệu nguồn cấp công khai, chứ không phải là toàn bộ chi phí cho việc xem xét pháp lý hoặc thực thi. Bài báo đề xuất bằng chứng có chữ ký, các mục tiêu phản hồi có thể đo lường được, việc tự động chuyển cấp các trường hợp đã được xác thực, các biện pháp khắc phục tương xứng, trách nhiệm giải trình công khai và thủ tục kháng cáo nhanh chóng. Bài báo không đề xuất việc cho phép người báo cáo truy cập trực tiếp vào các cơ chế kiểm soát việc đình chỉ tên miền.

● NGUỒN SƠ CẤP
Được chứng minh trực tiếp bằng một văn bản chính thức hoặc một nghiên cứu đã được công bố.

● MÔ HÌNH MINH HỌA
Một phép tính có thể tái hiện, trong đó các dữ liệu đầu vào là các giả định, chứ không phải các chỉ số trung bình của thị trường.

● ĐỀ XUẤT CHÍNH SÁCH
Một bản thiết kế được đưa ra để tham khảo ý kiến, thử nghiệm và chỉnh sửa.

01 Câu hỏi nghiên cứu, phạm vi và tiêu chuẩn chứng minh

Câu hỏi này hẹp hơn so với câu "Ai đã thất bại?": **Những sự chậm trễ nào có thể quan sát được giữa việc xác thực bằng chứng và việc thực hiện các biện pháp tương xứng là có thể ngăn chặn được, và biện pháp can thiệp nào có thể giảm thiểu thiệt hại cho nạn nhân mà không gây ra các**

trường hợp dương tính giả không thể chấp nhận được hoặc thiệt hại phụ?

Phạm vi nghiên cứu là hệ sinh thái gTLD theo hợp đồng: các chủ thể đăng ký, đại lý phân phối, nhà đăng ký tên miền, cơ quan quản lý tên miền và bộ phận đảm bảo tuân thủ hợp đồng của ICANN. Các nhà cung cấp dịch vụ lưu trữ, mạng phân phối nội dung (CDN), trình duyệt, dịch vụ thanh toán, nền tảng quảng cáo, các Trung tâm Ứng phó Sự cố Máy tính (CERT) quốc gia và các cơ quan tư pháp hình sự chỉ được đưa vào khi chúng ảnh hưởng đến chuỗi bằng chứng hoặc chuỗi phản ứng. Các TLD mã quốc gia có cơ chế quản trị khác nhau và không được coi là thuộc phạm vi áp dụng của các hợp đồng gTLD của ICANN.

Tình hình các luận điểm chính

- Bài viết này phân tích Hiệp hội Đăng ký Tên miền (ICANN) với tư cách là một tổ chức quản trị tư nhân và đảm bảo tuân thủ hợp đồng trong hệ sinh thái của Tổ chức Quản lý Tên miền Mở (gTLD). Hiệp hội Đăng ký Tên miền (ICANN) không phải là cơ quan quản lý nhà nước hay cơ quan thực thi pháp luật, nhưng tổ chức này cấp chứng nhận cho các đơn vị đăng ký tên miền, ký kết hợp đồng với các nhà điều hành cơ sở dữ liệu tên miền và đảm bảo việc thực thi các thỏa thuận đó; phạm vi nhiệm vụ hạn chế này không làm giảm trách nhiệm giải trình của tổ chức.
- Khoảng 60–85% là một ước tính định lượng cốt lõi trong mô hình đánh giá tác hại của bài báo. Con số này được trình bày như một ước tính có thể kiểm chứng, được suy ra từ các giả định rõ ràng và quan sát từ các trường hợp cụ thể — chứ không phải là một số liệu thống kê đã được xác lập sẵn cho tất cả các vụ gian lận trên toàn cầu. Việc công bố một bộ dữ liệu ở cấp độ sự cố, trong đó các mốc thời gian về phát hiện, thông báo, giảm thiểu và tác hại được đồng bộ hóa, là bước tiếp theo mang tính chứng cứ.
- Con số 100–150 USD là một ước tính ngân sách kỹ thuật có thể kiểm chứng cho việc thu thập liên tục và phân loại ban đầu trên một tập hợp đã xác định gồm dữ liệu vùng truy cập, dữ liệu Certificate Transparency và dữ liệu nguồn cấp công khai trên cơ sở hạ tầng thông dụng. Đây không phải là chi phí cho khả năng hiển thị toàn cầu hoàn chỉnh, rà soát pháp lý, kháng cáo, tính sẵn sàng cao hay việc thực thi. Do đó, bài báo coi đây là một tiêu chuẩn tham chiếu để tái hiện với khối lượng công việc đã công bố, danh mục nguồn và nhật ký chi phí — chứ không phải là một mức giá chung đã được chứng minh. Sự phân biệt này thu hẹp phạm vi khẳng định mà không làm mất đi sự bất đối xứng về chi phí đang được kiểm chứng.
- So sánh trong ba tuần của bài báo này tập trung vào độ trễ tuân thủ, chứ không phải là một thỏa thuận cấp độ dịch vụ (SLA) chung về việc ngừng hoạt động tên miền. Bài báo “ICANN” Câu hỏi thường gặp về tuân thủ hợp đồng theo đó, hầu hết các loại khiếu nại có thể trải qua ba giai đoạn phản hồi liên tiếp, mỗi giai đoạn kéo dài năm ngày làm việc, trước khi được chuyển lên cấp trên theo thủ tục chính thức, trong khi nhiều chiến dịch độc hại lại diễn ra trong vài giờ hoặc vài ngày. Các hợp đồng cũng quy định riêng rằng phải thực hiện các biện pháp giảm thiểu kịp thời và phù hợp ngay sau khi có bằng chứng đủ cơ sở để xử lý. [2] [4]
- Đối với một trường hợp đăng ký độc hại đã được xác minh và chỉ nhằm một mục đích duy nhất, `serverHold` Đây là một trong những biện pháp khắc phục ở cấp độ DNS gây gián đoạn nghiêm trọng nhất vì nó loại bỏ việc ủy quyền khỏi vùng. Biện pháp này không mang tính toàn diện: nó cũng có thể gây gián đoạn cho dịch vụ thư điện tử, các tên miền con và các dịch vụ hợp pháp; các

phản hồi được lưu trong bộ nhớ đệm có thể vẫn tồn tại cho đến khi hết hạn TTL; và các dịch vụ bị xâm phạm hoặc được chia sẻ có thể cần các biện pháp khắc phục có phạm vi hẹp hơn. [4] [7]

ĐÓNG GÓP NGHIÊN CỨU

Đề xuất này có thể kiểm chứng được. Một nghiên cứu thử nghiệm có thể so sánh giữa nhóm can thiệp và nhóm đối chứng về thời gian đến khâu phân loại, thời gian đến khâu giảm nhẹ, các chỉ số thay thế cho tổn thất nạn nhân, tỷ lệ tái phát, kết quả dương tính giả, thời gian đảo ngược và tác động phụ.

02 Những gì các nguồn tư liệu sơ cấp đã xác định

$165.1M

ICANN FY27 kinh phí hoạt động

Đã thông qua ngân sách "FY27". Quy mô theo bối cảnh; không phải chi tiêu "DNS Abuse". [1]

191,561

Các khiếu nại về lừa đảo qua email (phishing) và giả mạo (spoofing) năm 2025 của IC3

Loại khiếu nại IC3 có số lượng nhiều nhất; tổng thiệt hại được xác định trực tiếp là 215,8 triệu USD. [10]

24 giờ

Tuổi thọ trung vị theo một nghiên cứu năm 2021

Kết quả cụ thể cho bộ dữ liệu này trên 1.288 tên miền lừa đảo; không phải là thời gian tồn tại chung cho tất cả các tên miền. [11]

Không có SLA cố định

Thời hạn chung để gỡ bỏ nội dung

Các sửa đổi năm 2024 đề cập đến các biện pháp giảm thiểu "nhanh chóng" và "phù hợp", chứ không phải một thời hạn chung duy nhất. [2] [3]

ĐỀ XUẤT	TÌNH TRẠNG	CÓ THỂ KHẲNG ĐỊNH ĐIỀU GÌ
Phishing là DNS Abuse	ĐÃ ĐƯỢC XÁC MINH	Phishing được nêu rõ là một trong năm loại thuộc phạm vi các sửa đổi hợp đồng gTLD năm 2024. [2]
Nhà đăng ký tên miền phải hành động	ĐÃ ĐƯỢC XÁC MINH	Nhà đăng ký tên miền phải hành động kịp thời khi có bằng chứng có thể làm căn cứ hành động cho thấy một tên miền do họ bảo trợ đang được sử dụng cho DNS Abuse. [2]
Nhà vận hành cơ sở dữ liệu đăng ký phải hành động	ĐÃ ĐƯỢC XÁC MINH	Nhà vận hành cơ sở dữ liệu đăng ký phải hành động kịp thời khi họ xác định một cách hợp lý, dựa trên bằng chứng có thể làm căn cứ hành động, rằng một tên miền đã đăng ký đang được sử dụng cho DNS Abuse; biện pháp phù hợp vẫn phụ thuộc vào bối cảnh. [3]
`serverHold` hủy ủy quyền	ĐÃ ĐƯỢC XÁC MINH	Đây là trạng thái "EPP" do máy chủ thiết lập. Các kết quả được lưu trong bộ nhớ đệm từ DNS có thể vẫn tồn tại cho đến khi hết hạn, và thao tác này ảnh hưởng đến toàn bộ tên miền đã đăng ký. [7]
Mọi DNS Abuse đều có thể được quan sát qua CZDS hoặc CT	SAI	CZDS và Certificate Transparency là các cảm biến hữu ích, không phải cái nhìn đầy đủ hay theo thời gian thực về mọi hoạt động sử dụng tên miền. [8] [9]

Báo cáo sáu tháng đầu tiên của ICANN về việc thực hiện các yêu cầu hợp đồng theo các sửa đổi năm 2024 đã ghi nhận 192 cuộc điều tra, hơn 2.700 tên miền bị tạm ngưng, hơn 350 trang lừa đảo bị vô hiệu hóa và hai Thông báo vi phạm. Những con số này không chứng minh rằng các biện pháp kiểm soát hiện tại là đủ, nhưng chúng bác bỏ khẳng định tuyệt đối rằng hệ thống không có bất kỳ hành động nào. [5]

03 Tại sao độ trễ phản hồi vẫn là một chủ đề nghiên cứu chính đáng

Một số chiến dịch lừa đảo trực tuyến diễn ra trong khoảng thời gian tính bằng giờ hoặc ngày. Trong một nghiên cứu năm 2021, Bijmans và các cộng sự đã báo cáo rằng tuổi thọ trung bình quan sát được là 45 giờ và tuổi thọ trung vị là 24 giờ đối với 1.288 tên miền lừa đảo. [11] Một nghiên cứu năm 2026 về các tên miền lừa đảo mới được đăng ký đã chỉ ra một phân phối có độ lệch rất lớn: đối với 14.112 tên miền có thời gian tồn tại có thể đo lường được, giá trị trung bình là 8,6 ngày và giá trị trung vị là một ngày. [12] Cả hai ví dụ này đều không thể được áp dụng chung cho mọi loại mối đe dọa, nhưng cả hai đều cho thấy lý do tại sao việc đánh giá một quy trình chỉ dựa trên số ngày làm việc có thể bỏ sót các hoạt động lừa đảo và lừa đảo qua email có thời gian tồn tại ngắn.

SỰ LỆCH PHA THEO THỜI GIAN ĐƯỢC ĐO LƯỜNG

Các nghiên cứu này không xác định được tỷ lệ thiệt hại tài chính xảy ra sau khi nhận được thông báo, nhưng chúng đã chỉ ra sự không khớp về thời gian: một quy trình mà các giai đoạn tuân thủ không chính thức ban đầu có thể kéo dài tới mười lăm ngày làm việc thì bản thân nó không thể đóng vai trò là biện pháp ứng phó sự cố đối với các chiến dịch có thời gian tồn tại trung bình chỉ khoảng một ngày. Do đó, mốc 21 ngày dưới đây là một kịch bản về độ trễ tuân thủ, chứ không phải là nhãn hiệu cho một "SLA ICANN" phổ quát.

HÌNH 1 · KẾT QUẢ TÍCH LŨY MINH HỌA CỦA CHIẾN DỊCH LỪA ĐẢO VÀ ĐÁNH CẮP THÔNG TIN

MÔ HÌNH · KHOẢNG THỜI GIAN THEO LOG

Đường cong này minh họa kịch bản được trình bày trong Phần 4; đây không phải là dữ liệu thị trường thực tế. Việc sắp xếp theo chiều ngang giúp thu gọn các khoảng thời gian dài nhằm tăng tính dễ đọc. Nguồn: mô hình có thể tái tạo với các đầu vào đã được công bố.

THẬN TRỌNG VỀ MẶT NHÂN QUẢ

Thời gian tồn tại của tên miền ngắn hơn không tự động đồng nghĩa với việc ngăn chặn được tổn thất tài chính. Những kẻ tấn công có thể chuyển hướng, sử dụng các trang web đã bị xâm nhập, thay đổi kênh phân phối hoặc rút tiền trước khi bị phát hiện. Phải đo lường được mối quan hệ nhân quả, chứ không thể suy luận chỉ dựa trên tốc độ gỡ bỏ trang web.

04

Kinh tế học của hoạt động gian lận và phishing dưới dạng kịch bản có thể tái lập

Tài sản có giá trị kinh tế thường không phải là phí đăng ký, mà là lưu lượng truy cập, nội dung sáng tạo, cơ sở hạ tầng và niềm tin đã được tích lũy xung quanh một tên miền. Quan điểm này có cơ sở; mức độ của nó thay đổi tùy theo từng hoạt động lừa đảo và đánh cắp thông tin. Do đó, công cụ tính toán dưới đây hiển thị từng thông số đầu vào thay vì đưa ra một kết quả giả định dưới dạng giá trị trung bình quan sát được.

ĐỊNH NGHĨA MÔ HÌNH

```
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
```

Công cụ tính toán kịch bản

Thay đổi bất kỳ giả định nào. Các con số này chỉ mang tính minh họa và không phải là ước tính về thị trường phishing điển hình.

MÔ HÌNH MINH HỌA

Ngân sách hoạt động gian lận và phishing (USD)

5000

Số lượt thăm hàng ngày

2000

Tỷ lệ chuyển đổi nạn nhân (%)

1.5

Mức thiệt hại trung bình trên mỗi nạn nhân (USD)

2400

Tỷ lệ hao hụt khi chuyển thành tiền mặt (%)

25

Thời gian thực hiện (giờ)

24

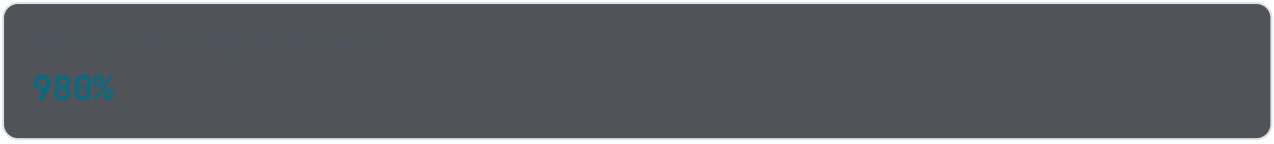
2,000

30

$54,000

$49,000

2.2 h



Vì mô hình biểu diễn giá trị kỳ vọng, số nạn nhân dự kiến có thể là số thập phân. Mô hình không tính đến suy giảm lưu lượng, thay đổi hành vi sau khi bị phát hiện, sự dịch chuyển của chiến dịch, nạn nhân trùng lặp hay phân phối bất định.

▶ Xem bảng nguồn của mô hình

05 Đo lường những tổn hại có thể phòng ngừa mà không cần tạo ra độ chính xác

"Thiệt hại sau khi phát hiện" chỉ có thể trở thành một kết quả hữu ích nếu các khái niệm "phát hiện", "giao nhận" và "thiệt hại" được định nghĩa một cách nhất quán. Dấu thời gian trên danh sách đen không phải là bằng chứng cho thấy nhà đăng ký đã nhận được bằng chứng có thể hành động. Một giao dịch ví điện tử không tự động được quy cho một tên miền cụ thể. Việc một tên miền trở nên không thể truy cập được không xác định được đối tượng nào đã gây ra sự thay đổi đó.

Cấu trúc sự kiện tối thiểu

SỰ KIỆN	DẤU THỜI GIAN BẮT BUỘC	BẰNG CHỨNG TỐI THIỂU
Quan sát đầu tiên	`t_obs`	Cảm biến, hàm băm yêu cầu/phản hồi, phương pháp ghi lại, nguồn đồng hồ.
Xác nhận kỹ thuật	`t_valid`	Chỉ số có thể tái tạo, danh tính người đánh giá, loại mối đe dọa và mức độ tin cậy.
Thông báo đã được gửi	`t_thông báo`	Phiếu xác nhận giao hàng đã được xác thực và phiên bản hồ sơ chứng cứ.
Bên chịu trách nhiệm thừa nhận	`t_ack`	Mã số vụ việc và vai trò của bên nhận: máy chủ, cơ quan đăng ký tên miền, cơ quan quản lý tên miền, nền tảng hoặc cơ quan có thẩm quyền.
Đã quan sát thấy các biện pháp giảm thiểu	`t_giảm thiểu`	DNS (thời gian phản hồi), HTTP, trạng thái thanh toán hoặc trạng thái nền tảng, được đo lường từ nhiều góc độ khác nhau.
khiếu nại / khôi phục	`t_restore`	Cơ sở ra quyết định, bằng chứng thay đổi và việc xác minh việc khôi phục.
Sự kiện gây hại	`t_harm`	Báo cáo về nạn nhân đã được ẩn danh, giao dịch có thể xác định được hoặc một bằng chứng thay thế khác đã được ghi chép.

CHỈ SỐ KẾT QUẢ ĐỀ XUẤT

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

Tử số và mẫu số phải tuân theo cùng một quy tắc gán nguồn. Kết quả cần báo cáo về nhóm đối tượng, khoảng tin cậy, kiểm duyệt bên phải, nguồn dữ liệu thiếu, cách xử lý trường hợp nạn nhân trùng lặp và độ nhạy cảm với khoảng thời gian quan sát. Nhãn "có thể phòng ngừa" nên được dành riêng cho thiết kế nghiên cứu nhân quả hoặc, ít nhất, so sánh có ghép đôi — không phải mọi sự kiện xảy ra sau khi có thông báo.

ƯỚC TÍNH THEO MÔ HÌNH TRUNG TÂM · 60–85%

Bài báo giữ mức 60–85% làm ước tính trung tâm cho tỷ lệ thiệt hại có thể quy trách nhiệm xảy ra sau khi phát hiện và thông báo trong nhóm sự cố đang được mô hình hóa. Đây là một ước tính kịch bản được suy ra từ các giả định đã công bố và quan sát các trường hợp cụ thể — chứ không phải là một số liệu thống kê được đo lường cho tất cả các vụ gian lận trên toàn thế giới. Ước tính này nên được sử dụng cho phân tích độ nhạy cho đến khi có một bộ dữ liệu cấp sự cố thống nhất các mốc thời gian về quan sát, bằng chứng đã được xác thực, quá trình thực hiện, biện pháp giảm thiểu và thiệt hại. Việc công bố bộ dữ liệu đó chính là bài kiểm chứng bằng chứng cho luận điểm, chứ không phải là lý do để loại bỏ luận điểm.

06 Bản đồ tổ chức: năng lực được phân bổ

Không có bất kỳ bên nào có thể quan sát hoặc kiểm soát toàn bộ sự việc. Cơ quan đăng ký (registrar) nắm rõ mối quan hệ với người đăng ký; cơ quan quản lý tên miền (registry) kiểm soát trạng thái tên miền do mình quản lý; máy chủ và các nhà cung cấp dịch vụ lưu trữ (CDN) kiểm soát việc phân phối nội dung; các trình duyệt và nhà cung cấp giải pháp bảo mật kiểm soát các cảnh báo; các nhà cung cấp dịch vụ thanh toán và ví điện tử có thể ngắt quãng các giao dịch chuyển tiền; các cơ quan chức năng có thể buộc phải bảo quản hoặc thu giữ dữ liệu. Hệ thống Giao dịch Tên miền (ICANN) soạn thảo và thực thi các hợp đồng trong hệ sinh thái Giao dịch Tên miền (gTLD) nhưng không vận hành một hệ thống điều khiển toàn cầu (EPP).

01 · TÍN HIỆU

Các nhà nghiên cứu và cảm biến

Theo dõi các chỉ dấu về nội dung, hạ tầng và nạn nhân; bảo toàn nguồn gốc và chuỗi lưu giữ bằng chứng.

02 · DỊCH VỤ

Người dẫn chương trình / CDN / nền tảng

Có thể xóa nội dung hoặc chặn truy cập một cách nhanh chóng, thường mà không cần thay đổi tên miền.

03 · BÊN BẢO TRỢ

Nhà đăng ký tên miền

Rà soát báo cáo DNS Abuse, liên hệ với chủ thể đăng ký và có thể đặt trạng thái EPP phía máy khách.

04 · KHU VỰC

Nhà vận hành cơ sở dữ liệu đăng ký

Kiểm soát trạng thái của bộ đăng ký “EPP” và việc ủy quyền vùng “TLD”.

05 · HỢP ĐỒNG

ICANN Tuân thủ

Kiểm tra việc tuân thủ của các bên ký hợp đồng; không xem xét xử lý từng vụ việc gian lận.

06 · LUẬT

CERT / các cơ quan chức năng

Phối hợp các biện pháp ứng phó và sử dụng các quyền hạn pháp lý theo quy định của từng khu vực pháp lý.

Khả năng phân tán không có nghĩa là trách nhiệm bị xóa bỏ. Một cơ quan đăng ký bảo trợ không thể từ bỏ nghĩa vụ hợp đồng của mình bằng cách ủy quyền việc xử lý các trường hợp lạm dụng cho một đại lý bán lại; cơ quan đăng ký kiểm soát trạng thái EPP được thiết lập trên máy chủ; ICANN đảm bảo việc tuân thủ hợp đồng. Dòng theo dõi kiểm toán phải ghi lại không chỉ ai đã thực hiện hành động, mà còn ai đã nhận được bằng chứng có thể hành động, chuyển hướng vụ việc, không phản hồi hoặc không thực hiện nghĩa vụ được giao. Quyền hạn pháp lý vẫn thuộc về người được ủy quyền áp dụng biện pháp; trách nhiệm giải trình cũng bao gồm các trường hợp không thực hiện nghĩa vụ đã được ghi chép.

Sự tập trung nguồn vốn và một giả thuyết về xung đột lợi ích có thể kiểm chứng

$165.1M

Kinh phí hoạt động của Chương trình "ICANN" năm tài chính 27

Đã thông qua ngân sách kịch bản cơ sở cho năm tài chính 27. [1]

≈98.1%

các nguồn thu từ phí đăng ký và phí nhà đăng ký

Khoảng 162,0 triệu USD trong tổng số 165,1 triệu USD của kế hoạch tài trợ. [1]

70.7%

chỉ riêng phí dựa trên giao dịch

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

Do đó, cơ cấu nguồn vốn chủ yếu tập trung vào các khoản thanh toán từ các bên ký hợp đồng mà ICANN chịu trách nhiệm thực thi các thỏa thuận, và một phần lớn trong số đó phụ thuộc vào các giao dịch đăng ký có thể tính phí. Điều này tạo ra sự phụ thuộc về mặt cấu trúc và đặt ra một vấn đề chính đáng liên quan đến xung đột lợi ích. Điều đó *không*, chỉ riêng điều đó, chưa đủ để chứng minh việc thi hành luật một cách cố ý lỏng lẻo hay tình trạng "chiếm đoạt quy định" đã hoàn toàn diễn ra. Giả thuyết về sự chiếm đoạt này cần được kiểm chứng dựa trên thời gian phản hồi ở cấp độ từng vụ việc, kết quả thi hành luật, các biện pháp xử phạt, tình trạng vi phạm lặp lại và vai trò của các bên liên quan được tài trợ trong các quyết định về chính sách và triển khai.

07 Mức cơ sở theo hợp đồng năm 2024 — và những điều mà mức này không quy định cụ thể

Các sửa đổi toàn cầu tháng 4 năm 2024 đối với Thỏa thuận Công nhận Nhà đăng ký và Thỏa thuận Cơ sở Đăng ký đã thiết lập nghĩa vụ rõ ràng nhằm giảm thiểu DNS Abuse. Nhà đăng ký tên miền phải hành động kịp thời khi có bằng chứng có thể làm căn cứ hành động cho thấy một tên miền do họ bảo trợ đang được sử dụng cho DNS Abuse. Nhà vận hành cơ sở dữ liệu đăng ký phải hành động kịp thời khi họ xác định một cách hợp lý, dựa trên bằng chứng có thể làm căn cứ hành động, rằng một tên miền đã đăng ký đang được sử dụng cho DNS Abuse. Trong cả hai trường hợp, biện pháp phù hợp phụ thuộc vào bối cảnh, mức độ nghiêm trọng và tác hại phụ. [2] [3]

Ba dòng thời gian thường bị nhầm lẫn với nhau

DÒNG THỜI GIAN	ÁP DỤNG CHO NHỮNG TRƯỜNG HỢP NÀO	ĐIỀU ĐÓ KHÔNG CÓ NGHĨA LÀ
24 giờ	Theo RAA §3.18.3, xem xét các báo cáo có căn cứ về Hoạt động bất hợp pháp do cơ quan thực thi pháp luật, bảo vệ người tiêu dùng, cơ quan bán chính phủ hoặc cơ quan tương tự gửi đến đầu mối liên hệ chuyên trách.	Đây không phải là thời hạn đình chỉ 24 giờ áp dụng cho tất cả các trường hợp.
"Ngay lập tức"	Thực hiện các biện pháp giảm thiểu phù hợp sau khi đạt đến ngưỡng bằng chứng có cơ sở để hành động.	Đây không phải là một số giờ cố định và không nhất thiết phải áp dụng cùng một biện pháp khắc phục trong mọi trường hợp.
21 ngày	Có thể được coi là thời hạn khắc phục sau khi nhận được Thông báo vi phạm hợp đồng chính thức.	Đây không phải là thời hạn hoạt động thông thường được cấp cho mọi tên miền độc hại đã được báo cáo.

Sự linh hoạt này mang lại những lợi ích: một tên miền của trường đại học bị xâm phạm không nên được xử lý giống như một tên miền lừa đảo chuyên dụng mới được đăng ký. Vấn đề về trách nhiệm giải trình nằm ở chỗ rất khó so sánh giữa "kịp thời" và "phù hợp" nếu không có dấu thời gian, phân loại trường hợp và mã kết quả được công bố. Đề xuất dưới đây bổ sung các biện pháp đánh giá và rà soát mà không giả định rằng một thời hạn duy nhất có thể áp dụng cho mọi trường hợp.

08 Vấn đề về ranh giới: lừa đảo qua email đã được đề cập; một số hình thức lừa đảo tài chính khác có thể chưa được đề cập

Phishing được nêu rõ trong định nghĩa hợp đồng của DNS Abuse. Ranh giới khó hơn liên quan đến các trang dùng tên riêng của mình để lừa người dùng thay vì mạo danh một bên thứ ba có thể xác định—chẳng hạn một số nền tảng đầu tư giả, cửa hàng gian lận, trò lừa khôi phục tiền và kế hoạch chữ ký ví. Tùy tình tiết, các trường hợp này có thể được xử lý như hành vi sai phạm ở lớp nội dung trang web, gian lận người tiêu dùng hoặc một loại pháp lý khác, thay vì DNS Abuse theo hợp đồng.

> NHÃN NGHIÊN CỨU ĐƯỢC ĐỀ XUẤT
>
> **Lạm dụng gây thiệt hại tài chính đã được xác minh (VFHA)**: việc sử dụng tên miền đã được ghi nhận nhằm lấy tiền, thông tin thanh toán, khóa riêng tư hoặc cụm từ hạt giống bằng thủ đoạn lừa dối, bất kể có mạo danh thương hiệu hay không. VFHA không phải thuật ngữ hiện hành của ICANN và tự nó không tạo ra thẩm quyền hợp đồng.

Tham vấn chính sách có thể xem xét liệu một loại hẹp, có yêu cầu bằng chứng như VFHA nên thuộc hợp đồng tương lai, khung chuyển tiếp liên ngành hay pháp luật quốc gia. Việc mở rộng phải đòi hỏi

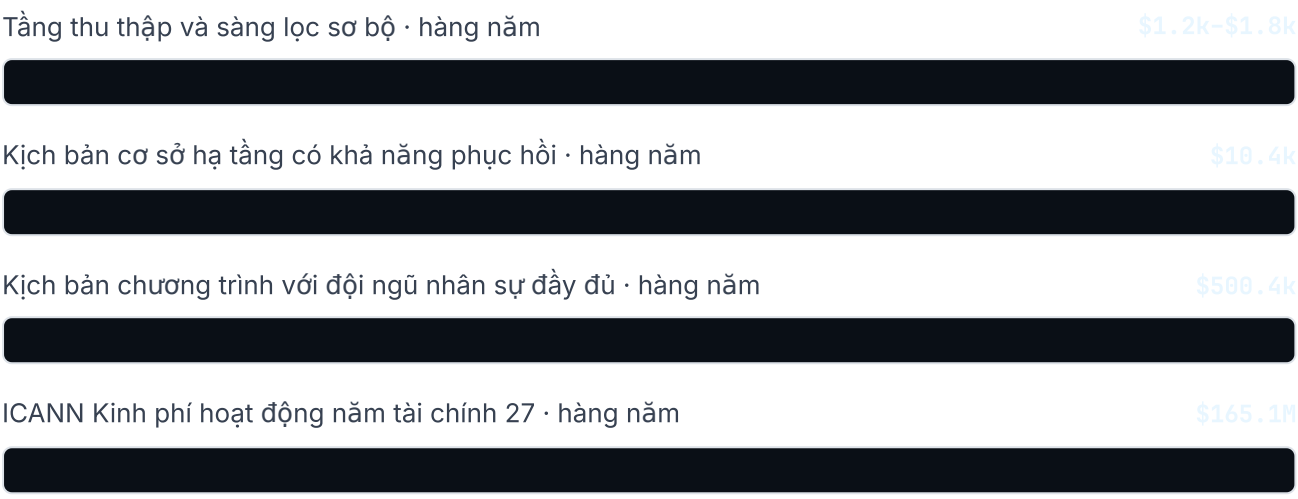
tiêu chí thiệt hại chính xác, bằng chứng đáng tin cậy, biện pháp tương xứng, rà soát thẩm quyền và cơ chế khiếu nại. Nhãn "lừa đảo" mơ hồ là không đủ.

09 Những điều mà tuyên bố về chi phí giám sát 100–150 USD/tháng phải chứng minh được — và những điều nó không thể chứng minh

Một máy chủ thông dụng có thể tải xuống các bản chụp nhanh có thể truy cập được từ các tệp vùng gTLD tham gia và tính toán các thay đổi tại địa phương, thu thập các sự kiện Certificate Transparency được chọn và các nguồn cấp dữ liệu mở, chuẩn hóa các chuỗi ký tự, tính toán hàm băm và sắp xếp thứ tự ưu tiên cho các ứng viên. Đó là một tiêu chuẩn kỹ thuật hữu ích và có thể kiểm chứng — chứ không phải là "việc giám sát toàn diện Internet". Trong quý 2 năm 2026, Verisign đã báo cáo có 401,6 triệu đăng ký trên tất cả các TLD; CZDS bao gồm các tệp vùng gTLD tham gia thay vì tất cả các TLD, và CT ghi lại các chứng chỉ hoặc chứng chỉ sơ bộ được ghi lại công khai thay vì mọi tên miền đang hoạt động hoặc có hại. [8] [9] [17]

NĂNG LỰC	NGUYÊN MẪU PHỔ THÔNG	DỊCH VỤ CÔNG ÍCH Ở QUY MÔ SẢN XUẤT
Tiếp nhận vùng/CT/nguồn cấp	Khả thi với tập nguồn xác định	Bộ thu thập dự phòng, hợp đồng nguồn, giám sát khoảng trống
Phân loại chuỗi/hàm băm	Khả thi	Đánh giá chuẩn, phát hiện sai lệch, nghiên cứu âm tính giả
Kết xuất trình duyệt	Tập con lấy mẫu nhỏ	Cụm thực thi cô lập, điểm quan sát khu vực, cô lập mã độc
Xác định pháp lý	Không bao gồm	Chuyên gia đủ năng lực, lập bản đồ thẩm quyền và quyền hạn
Tính sẵn sàng cao / lưu giữ bằng chứng	Thường không có	Chữ ký dựa trên HSM, nhật ký kiểm toán, sao lưu và ứng phó sự cố
Khiếu nại và khôi phục	Không bao gồm	Vận hành 24/7, leo thang độc lập và mục tiêu dịch vụ

HÌNH 2 · BỐI CẢNH VỀ CẤP ĐỘ CHIỀU RỘNG LOGARITH · CHI PHÍ KHÔNG THỂ SO SÁNH TRỰC TIẾP



Độ rộng theo logarit giúp các giá trị nhỏ vẫn hiển thị rõ ràng. Ba con số đầu tiên là các giả định kỹ thuật hoặc chương trình đã được công bố, yêu cầu có điểm chuẩn được công bố và không phải là báo giá của nhà cung cấp. ICANN Kinh phí vận hành là con số đã được xác minh ở quy mô tổ chức. Đây là các ngân sách được thiết kế cố ý không tương đương: việc so sánh nhằm kiểm tra xem việc thu thập và phân loại cơ bản có phải là chi phí vốn dĩ quá cao hay không, chứ không phải để xác định liệu một chương trình thực thi hoàn chỉnh có tốn 100 đô la mỗi tháng hay không.

10 Khung ứng phó DNS Abuse đã xác minh được đề xuất

Khung đề xuất này là một kiến trúc tham chiếu, chứ không phải là một công tắc ngắt toàn cầu tự động. Nó tiêu chuẩn hóa các yếu tố cấu thành vụ việc, hồ sơ quyết định và dấu thời gian, đồng thời cho phép người vận hành được ủy quyền lựa chọn biện pháp hiệu quả gây ít gián đoạn nhất.

01 · NHẬP LIỆU

Thu thập và bảo tồn

Thu thập báo cáo và ghi chép quan sát; xử lý dữ liệu thô; đồng bộ hóa đồng hồ.

02 · nguồn gốc và chuỗi lưu giữ bằng chứng

Chuẩn hóa bằng chứng

Ghi lại nguồn gốc, phương pháp, lịch sử xử lý và các phụ thuộc nguồn.

03 · XÁC MINH

Xác nhận

Tái hiện hành vi gây hại và phân biệt các bằng chứng độc lập.

04 · ĐÁNH GIÁ

Rủi ro và tài sản thế chấp

Phân loại các trường hợp đăng ký độc hại, dịch vụ bị xâm phạm, dịch vụ lưu trữ chia sẻ và mức độ nghiêm trọng.

05 · TRẢ LỜI

Thông báo và giảm thiểu

Xác định đơn vị chịu trách nhiệm, thời hạn thực hiện và biện pháp khắc phục hiệu quả gây ít ảnh hưởng nhất.

06 · ĐÁNH GIÁ

Kiểm toán và khiếu nại

Công bố siêu dữ liệu về kết quả, đo lường tác động và hỗ trợ việc khắc phục nhanh chóng.

Các cấp độ bằng chứng

E1 Tín hiệu chưa được xác minh

Một nguồn thông tin, khớp từ vựng hoặc cáo buộc dựa trên danh tiếng. Thích hợp để làm cơ sở quan sát, nhưng không bao giờ đủ để làm căn cứ đình chỉ.

E2 Hành vi được tái hiện

Bản ghi có dấu thời gian cho thấy hành vi đánh cắp thông tin đăng nhập, phát tán phần mềm độc hại hoặc lộ trình giao dịch gian lận.

E3 Sự xác nhận độc lập

Ít nhất hai nguồn thông tin thực sự độc lập hoặc một bằng chứng kỹ thuật có thể tái hiện, kèm theo việc kiểm tra quyền sở hữu và bối cảnh.

E4 Xác nhận đủ điều kiện

Cơ quan có thẩm quyền, dịch vụ bị ảnh hưởng, chủ sở hữu thương hiệu hoặc bằng chứng về nạn nhân đã được xác thực, kèm theo chuỗi lưu giữ bằng chứng đảm bảo quyền riêng tư.

> QUY TẮC ĐỘC LẬP
>
> Ba nguồn cấp sao chép cùng một danh sách chặn thượng nguồn chỉ là một nguồn, không phải ba. Đồ thị nguồn gốc và chuỗi lưu giữ bằng chứng phải cho thấy nguồn chung, quá trình đồng bộ và việc nhà cung cấp tái công bố.

11 Gói bằng chứng tối thiểu và API có khả năng tương tác

Hệ thống Đăng ký Tên miền (API) cần tạo ra một trường hợp có thể xác minh được và khởi động bộ đếm thời gian phản hồi có thể kiểm toán; người báo cáo không được phép trực tiếp đưa ra lệnh tạm giữ. Nếu một trường hợp E3/E4 liên quan đến việc đăng ký có mục đích duy nhất nhằm gây hại và hết hạn mà không có quyết định có căn cứ hoặc biện pháp khắc phục hiệu quả, hệ thống sẽ tự động chuyển vụ việc lên nhà điều hành cơ quan đăng ký hoặc một bên khác có thẩm quyền theo hợp đồng hoặc pháp luật. A `serverHold` Lệnh chỉ có thể được phát ra từ một chủ thể được ủy quyền. Việc tự động nâng cấp quyền hạn và quyền hạn của cơ quan đăng ký để thực hiện các hành động khi hết hạn

là những đề xuất thay đổi chính sách, chứ không phải là những khẳng định về quyền hạn hiện có. Mỗi lần chuyển đổi trạng thái đều được ký xác nhận và ghi vào nhật ký kiểm toán.

POST /V1/CASES · VÍ DỤ

```
{
  "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:…"
}
```

Một phản hồi thành công sẽ trả về mã vụ việc, cơ quan tiếp nhận, mức độ bằng chứng, các lỗi về tính đầy đủ, thời gian xem xét dự kiến và một URL công khai về tính minh bạch. Phản hồi này không được hứa hẹn bất kỳ biện pháp khắc phục cụ thể nào trước khi cơ quan có thẩm quyền đánh giá thẩm quyền và tác động phụ.

12 Các mục tiêu phản hồi được đề xuất, chứ không phải các thời hạn gỡ bỏ áp dụng chung cho tất cả các trường hợp

Các mục tiêu về mức độ dịch vụ cần được phân tách *lời cảm ơn*, *phân loại bệnh nhân*, *quyết định* và *giảm thiểu hiệu quả*. Điều này giúp có thể đo lường hiệu quả mà không cần giả định rằng việc đình chỉ luôn là kết quả đúng đắn.

TÓM TẮT VỤ ÁN	XÁC NHẬN	MỤC TIÊU PHÂN LOẠI BỆNH NHÂN	MỤC TIÊU RA QUYẾT ĐỊNH	CÁC PHƯƠNG ÁN TRẢ LỜI ĐIỂN HÌNH
Việc đánh cắp thông tin xác thực thanh toán E3/E4 hoặc cụm từ hạt giống trên một tài khoản đăng ký độc hại chuyên dụng	15 phút	1 giờ	4 giờ	Khối nội dung; việc tạm giữ bởi nhà đăng ký/tổ chức quản lý tên miền khi được ủy quyền; các cảnh báo liên quan đến trình duyệt và thanh toán.
Lừa đảo nhắm vào thương hiệu E3 hoặc phân phối phần mềm độc hại	30 phút	2 giờ	6 giờ	Loại bỏ máy chủ/CDN, giảm thiểu rủi ro tên miền, chuyển hướng lưu lượng vào hố chìm hoặc hiển thị cảnh báo tùy theo điểm kiểm soát.
Tên miền hợp pháp bị xâm phạm hoặc tài khoản người dùng chung trên nền tảng SaaS	1 giờ	4 giờ	12 giờ	Cách ly đường dẫn/tài khoản và khôi phục quyền sở hữu; tránh việc tạm ngưng tên miền đã đăng ký nếu có thể.
Hành vi gian lận tài chính liên quan đến việc phân loại đang có tranh cãi	4 giờ	12 giờ	24 giờ	Bảo tồn, can thiệp về nền tảng/thanh toán, chuyển tuyến từ cơ quan có thẩm quyền và quyết định có căn cứ.
Tín hiệu E1 hoặc báo cáo không đầy đủ	Tự động	24 giờ	Chưa có cho đến khi được xác thực	Theo dõi, bổ sung và yêu cầu cung cấp bằng chứng.

Đây là các mục tiêu thí điểm. Các giá trị chính xác cần được xác định dựa trên thời gian tồn tại của các mối đe dọa đã quan sát được, số lượng nhân sự, chi phí do sai sót gây ra và các ràng buộc pháp lý, sau đó được công bố kèm theo phân phối mức độ đạt được thay vì chỉ một giá trị trung bình duy nhất.

13 An toàn, thủ tục pháp lý đúng quy định, quyền riêng tư và các tình huống sự cố

Việc phản ứng nhanh chóng mà không có các biện pháp bảo vệ có thể khiến dữ liệu sai lệch trở thành nguyên nhân dẫn đến kiểm duyệt, phá hoại thương mại hoặc sự cố ngừng hoạt động của hạ tầng. Do đó, một kiến trúc hợp lý phải coi các trường hợp báo động sai và tác động phụ tiêu cực là những thất bại an ninh nghiêm trọng hàng đầu.

CHẾ ĐỘ HỎNG HÓC	KIỂM SOÁT BẮT BUỘC	CHỈ SỐ CÓ THỂ KIỂM TOÁN
Báo cáo vu khống nhằm vào đối thủ cạnh tranh	Xác thực phóng viên, uy tín của nguồn tin, việc tái tạo độc lập và các biện pháp xử phạt đối với việc sử dụng kỹ thuật với mục đích xấu	Tỷ lệ báo cáo bị từ chối theo từng người báo cáo; các trường hợp thao túng đã được xác nhận
Tính tuần hoàn trong chuỗi cung ứng được ngụy trang dưới vỏ bọc của sự đồng thuận	Đồ thị nguồn gốc bằng chứng và khử trùng lặp nguồn thượng nguồn	Số lượng nguồn độc lập trước và sau khi hiệu chỉnh dòng dõi
Tạm ngưng toàn bộ các tên miền hợp pháp bị xâm phạm	Phân loại ý định đăng ký và ưu tiên giảm thiểu ở cấp độ lộ trình	Tỷ lệ tên miền bị xâm phạm; các dịch vụ hợp pháp bị ảnh hưởng
Dữ liệu về nạn nhân hoặc chi tiết về lỗ hổng bảo mật bị rò rỉ ra công chúng	Công bố thông tin theo từng cấp độ, che giấu thông tin, chứng cứ được niêm phong và thời hạn lưu giữ	Các sự cố liên quan đến quyền riêng tư; kết quả rà soát việc che giấu thông tin
Hành vi sai trái vẫn tiếp diễn	Tiếp nhận yêu cầu bồi thường theo Chương trình Bảo hiểm Xe hơi Toàn diện (khiếu nại) 24/7, chuyên gia đánh giá độc lập và quy trình phục hồi được xác thực	Thời gian đảo chiều ở mức trung vị và ở phân vị thứ 95
Việc tạm giữ trong sổ đăng ký gây ra sự cố ngừng hoạt động của email/tên miền con	Tài sản thế chấp, tính tương xứng của biện pháp khắc phục và giám sát sau khi thực hiện biện pháp	Số lượng dịch vụ bị gián đoạn trên mỗi hành động; tỷ lệ khôi phục

Các đảm bảo tối thiểu về thủ tục pháp lý

1. Mã lý do, mức độ bằng chứng và người ra quyết định chịu trách nhiệm được ghi lại đối với mỗi biện pháp hạn chế.
2. Người đăng ký có thể nhận được bản giải trình lý do đảm bảo quyền riêng tư và nộp bằng chứng phản bác.
3. Các trường hợp khẩn cấp khiếu nại sẽ được xem xét bởi một người không phải là người đã đưa ra quyết định ban đầu.
4. Việc đảo ngược được truyền qua cùng một kênh có dấu như hành động ban đầu.
5. Thống kê tổng hợp về lỗi và khôi phục là thông tin công khai; các bằng chứng nhạy cảm vẫn được kiểm soát quyền truy cập.

14 Từ “chỉ số độc tính” đến Chỉ số Chất lượng Phản ứng có thể chịu trách nhiệm

Điểm đánh giá nhà đăng ký công khai có thể góp phần nâng cao tính minh bạch, nhưng các bảng xếp hạng đơn thuần thường bị sai lệch do quy mô danh mục, phạm vi dữ liệu đầu vào, cơ cấu khách hàng, cũng như việc các tên miền có bị đăng ký với mục đích xấu hay sau này bị xâm phạm hay không. Điểm đánh giá này tuyệt đối không được dùng làm căn cứ để áp dụng biện pháp chặn tập thể đối với toàn bộ khách hàng của một nhà đăng ký.

VECTƠ CHẤT LƯỢNG ĐƯỢC ĐỀ XUẤT

```
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.
```

Nếu cần sử dụng mô hình tổng hợp cho mục đích quản trị, cần thiết lập các hệ số trọng số trước khi đánh giá, tiến hành kiểm tra độ nhạy và kiểm tra hồi quy trên các trường hợp được tách riêng. Kết quả cần được phân tầng theo loại tên miền (TLD), quy mô cơ quan đăng ký, loại mối đe dọa và nguồn bằng chứng. Kết quả đầu ra là một tín hiệu trách nhiệm — chứ không phải là phán quyết tự động về tên miền.

15 Cơ sở dữ liệu minh bạch công khai, phân tầng về DNS Abuse

Một hệ thống đăng ký minh bạch có thể loại bỏ các tranh chấp liên quan đến việc liệu một thông báo có tồn tại hay không, thời điểm nó được gửi đi và các hành động tiếp theo là gì. Tuy nhiên, việc công bố mọi bằng chứng có thể làm lộ danh tính nạn nhân, dữ liệu cá nhân, phương pháp điều tra và các lỗ hổng bảo mật đang được khai thác. Giải pháp là cơ chế truy cập theo cấp độ.

P

Hồ sơ công khai

Mã vụ việc, chỉ số, danh mục tổng quát, các mốc thời gian chính, mức độ tin cậy của bằng chứng, vai trò của các bên liên quan, mã kết quả, trạng thái “khiếu nại” và các giá trị băm của các bằng chứng đã được niêm phong.

C

Góc nhìn của bên ký hợp đồng

Bằng chứng kỹ thuật có thể tái tạo, kênh liên lạc, bối cảnh liên quan và hướng dẫn bảo quản.

R

Chế độ xem có quyền hạn bị giới hạn

Dữ liệu về nạn nhân, phân tích nguồn gốc tài chính, tài liệu điều tra đang được tiến hành và hồ sơ lưu giữ chứng cứ chưa được che giấu thông tin.

Mỗi bản cập nhật chỉ cho phép ghi thêm, được gắn dấu thời gian và ký điện tử. Các chỉnh sửa không xóa bỏ lịch sử; chúng chỉ thêm một bản ghi mới thay thế bản cũ. Tính năng tìm kiếm công khai phải tuân thủ các quy tắc lưu trữ, ngăn chặn việc phát hiện hàng loạt nạn nhân và cung cấp biện pháp khắc phục đối với dữ liệu cá nhân không chính xác.

16 Một chương trình thí điểm kéo dài sáu tháng kèm theo đánh giá dựa trên đăng ký trước

Một dự án thí điểm hữu ích cần có quy mô vừa đủ nhỏ để dễ quản lý và vừa đủ lớn để kiểm chứng chuỗi nhân quả. Phạm vi đề xuất: ba cơ quan đăng ký tình nguyện, hai nhà điều hành cơ sở dữ liệu đăng ký, một đối tác cung cấp dịch vụ lưu trữ/CDN, hai nguồn dữ liệu nghiên cứu độc lập và một hội đồng chuyên gia khiếu nại đủ tiêu chuẩn. Phác đồ nghiên cứu và các định nghĩa về kết quả cần được đăng ký trước khi phân bổ các trường hợp nghiên cứu.

THÁNG 1

Phân tích quy trình và khung pháp lý

Xác định các danh mục, cơ quan có thẩm quyền, các cấp độ bằng chứng, đánh giá tác động đến quyền riêng tư và các điều kiện ngừng thực hiện.

THÁNG 2

Tối ưu hóa quy trình hiện có

Đo lường các mốc thời gian ban đầu và kết quả mà không làm thay đổi hành vi phản hồi.

THÁNG THỨ 3

Vận hành gói bằng chứng

Áp dụng nguồn gốc bằng chứng có chữ ký, khử trùng lặp và phân loại tác động phụ.

THÁNG THỨ 4

Các mục tiêu phản hồi thử nghiệm

Phân bổ ngẫu nhiên các trường hợp đủ điều kiện hoặc áp dụng phương pháp triển khai theo từng giai đoạn; theo dõi các lỗi hàng ngày.

THÁNG THỨ 5

Bài tập “khiếu nại” và những thất bại

Tổ chức các cuộc diễn tập khôi phục hệ thống, thực hiện các báo cáo về các cuộc tấn công giả định từ phía “đội đỏ” và kiểm toán các biện pháp kiểm soát truy cập.

THÁNG THỨ 6

Đánh giá độc lập

Công bố các chỉ số hiệu ứng, khoảng tin cậy, dữ liệu thiếu, các sự cố bất lợi, chi phí và tài liệu tái hiện.

Kết quả chính của chương trình thí điểm

- Thời gian trung vị và thời gian ở phân vị thứ 90 từ khi có bằng chứng được xác thực đến khi thực hiện các biện pháp giảm thiểu hiệu quả.
- Sự khác biệt về mức độ tổn hại có thể quy cho sau khi nhận thông báo hoặc một chỉ số thay thế về mức độ phơi nhiễm của nạn nhân đã được xác định trước.
- Tỷ lệ dương tính giả, mức độ nghiêm trọng của hành động sai lầm và thời gian khôi phục trung vị.
- Tái diễn ở cùng chủ thể đăng ký, cụm hạ tầng và cấp độ hoạt động gian lận/phishing.
- Chi phí hoạt động trực tiếp trên mỗi trường hợp được xác nhận và trên mỗi biện pháp giảm thiểu hiệu quả.

QUY TẮC RA QUYẾT ĐỊNH

Chỉ nên mở rộng quy mô nếu chương trình thí điểm cho thấy hiệu quả giảm thiểu đáng kể mà không vượt quá các giới hạn đã đăng ký trước về kết quả dương tính giả, sự cố liên quan đến quyền riêng tư, độ trễ của dịch vụ “khiếu nại” hoặc sự gián đoạn dịch vụ liên quan.

17 Kết luận và các khuyến nghị có thể kiểm chứng

Ứng phó DNS Abuse không chỉ là một bộ lọc kỹ thuật, cũng không phải vấn đề mà một tổ chức có thể tự giải quyết. Các sửa đổi hợp đồng năm 2024 đã đặt ra nghĩa vụ giảm thiểu đáng kể, nhưng vẫn dành quyền cân nhắc rộng về bằng chứng, thời điểm và biện pháp khắc phục. Quyền cân nhắc này cần thiết để bảo đảm tính tương xứng; tuy nhiên, khi không có hồ sơ có thể so sánh, hiệu quả thực hiện cũng khó được đánh giá.

1. **Chuẩn hóa gói bằng chứng.** Áp dụng các trường chung về nguồn gốc bằng chứng, dấu thời gian và kết quả giữa bên báo cáo, nhà đăng ký, cơ sở dữ liệu đăng ký và nhà cung cấp hạ tầng.
2. **Đo từng giai đoạn riêng biệt.** Công bố thời gian xác nhận tiếp nhận, phân loại, ra quyết định, giảm thiểu và giải quyết khiếu nại theo từng loại mối đe dọa và cấp độ bằng chứng.
3. **Phân biệt đăng ký có chủ đích xấu với dịch vụ hợp pháp bị xâm nhập.** Ưu tiên khắc phục theo đường dẫn/tài khoản cho dịch vụ hợp pháp bị xâm nhập và chỉ áp dụng biện pháp trên toàn miền

khi biện pháp đó tương xứng.

4. **Thí điểm các mục tiêu ứng phó.** Kiểm thử mục tiêu theo giờ đối với đăng ký độc hại có độ tin cậy cao, chỉ phục vụ một mục đích, thay vì tuyên bố một thời hạn chung.
5. **Công bố dữ liệu về trách nhiệm giải trình đảm bảo quyền riêng tư.** Sử dụng hệ thống đăng ký minh bạch theo cấp độ với lịch sử đã được ký xác nhận và bằng chứng bị hạn chế.
6. **Đánh giá tác động nhân quả.** Không đồng nhất việc đình chỉ nhanh hơn với số tiền được bảo toàn cho đến khi một nghiên cứu đăng ký trước đo lường tác động đối với nạn nhân và sự dịch chuyển của mối đe dọa sang kênh khác.

Kết luận mang tính xây dựng ở đây không phải là vấn đề ban đầu sẽ biến mất một khi các khẳng định liên quan được điều chỉnh. Mà là các khẳng định cốt lõi giờ đây có thể được kiểm chứng: khoảng tỷ lệ thiệt hại sau khi phát hiện từ 60–85% là một giả thuyết định lượng rõ ràng; $100–150 là giả định ngân sách kỹ thuật có thể kiểm chứng cho một lớp cảm biến và phân loại được xác định rõ; và các mục tiêu phản ứng trong phạm vi giờ có thể được thử nghiệm đối với các trường hợp đăng ký độc hại có độ tin cậy cao và mục đích duy nhất. Công bố khối lượng công việc, chi phí, dấu thời gian và kết quả, so sánh chúng với mức cơ sở, và đo lường sự chênh lệch và sai số. Việc xác nhận sẽ là cơ sở hợp lý để thay đổi hợp đồng và chính sách; việc bác bỏ sẽ xác định giả định nào đã thất bại.

Thông báo về nội dung biên tập và phương pháp nghiên cứu. PhishDestroy là một dự án tình báo về mối đe dọa độc lập, phi thương mại. Ấn phẩm này là một đề xuất về chính sách và kỹ thuật, không phải là tư vấn pháp lý, chương trình "ICANN" hay bài báo được bình duyệt. Các khoảng ngân sách được ghi là "mô hình" là những giả định trong quá trình lập kế hoạch. Các nguồn tham khảo chính được liên kết ở phần dưới. Các chỉnh sửa có thể được gửi qua các kênh liên hệ và kênh tiết lộ có trách nhiệm của trang web.

QUAN ĐIỂM TỪ GÓC NHÌN CỦA NGƯỜI TRONG CUỘC · TRÁCH NHIỆM GIẢI TRÌNH PHẢI HẠN CHẾ CẢ VIỆC KHÔNG HÀNH ĐỘNG LẪN VIỆC LẠM QUYỀN

Một ranh giới cá nhân đối với quyền lực thi hành

Tôi không yêu cầu — và cũng không muốn — được truy cập trực tiếp vào công cụ chặn tên miền. Quyền hạn đó đòi hỏi phải có sự xem xét độc lập, nhật ký kiểm toán công khai, thủ tục kháng cáo nhanh chóng và khả năng đảo ngược quyết định.

Tôi tin rằng có rất nhiều công ty có năng lực và có trách nhiệm, đủ điều kiện để được giao phó một phần công việc này. Dựa trên kinh nghiệm của bản thân và những bài viết tôi đã công bố, tôi không xếp NameSilo vào nhóm đó.

Tôi không khuyên các công ty hợp pháp của Mỹ nên giao phó các chức năng nhạy cảm liên quan đến lạm dụng hoặc an ninh cho các nhà thầu cụ thể, những người mà các xung đột lợi ích, năng lực hoặc hành vi của họ không thể chịu được sự kiểm tra độc lập. Vấn đề ở đây là những hành động đã được ghi nhận, chứ không phải quốc tịch: việc có nguồn gốc từ Nga bản thân nó không chứng minh được điều gì, cũng giống như địa chỉ trụ sở của một công ty Mỹ cũng không chứng minh được điều gì.

Tôi muốn công lý và sự chịu trách nhiệm thực sự đối với các nhà đăng ký tên miền đã thu được doanh thu từ việc đăng ký và gia hạn các tên miền được ghi nhận là một phần của các chiến dịch lừa đảo lặp đi lặp lại. Trong trường hợp bằng chứng cho thấy hành vi đó không chỉ là sự cẩu thả mà còn có khả năng là sự tiếp tay có chủ ý — dù là sự tham gia trực tiếp vào hoạt động hay đóng vai trò là trung gian có đầy đủ thông tin, với chức năng duy trì việc đăng ký và hoạt động trực tuyến của tên miền gây hại bất chấp các cảnh báo lặp đi lặp lại — thì hành vi đó cần được điều tra độc lập và, nếu được xác minh, phải chịu các hậu quả tương ứng. Tôi không coi sự nghi ngờ là sự thật đã được xác định; nhưng tư cách trung gian không được phép mang lại sự miễn trừ khỏi sự giám sát.

Xem xét lại cuộc điều tra liên quan ↗

A

Tài liệu tham khảo và chú thích nguồn

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf
Nguồn cho 165,1 triệu USD kinh phí hoạt động FY27 và cơ cấu các dòng tài trợ.

[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
Nguồn hợp đồng chính về nghĩa vụ DNS Abuse của nhà đăng ký tên miền.

[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
Nguồn hợp đồng chính về nghĩa vụ giảm thiểu của nhà vận hành cơ sở dữ liệu đăng ký.

[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

Diễn giải vận hành, yêu cầu báo cáo và ví dụ về biện pháp giảm thiểu phù hợp.

[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

Báo cáo thực hiện sáu tháng, gồm số liệu điều tra và giảm thiểu.

[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

Bối cảnh về khả năng tương tác của báo cáo DNS Abuse và chất lượng bằng chứng.

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

Định nghĩa kỹ thuật về các giá trị trạng thái miền EPP, bao gồm cả trạng thái do máy chủ thiết lập.

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

Các quy định kỹ thuật chính thức và giới hạn của cảm biến điện dung (CT) với tư cách là một cảm biến.

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

Phạm vi và mô hình truy cập đối với các tệp vùng tham gia trong Hệ thống Tên miền Phân cấp (gTLD).

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Số liệu về các khiếu nại và tổn thất được báo cáo, bao gồm số vụ lừa đảo qua email (phishing) và giả mạo (spoofing).

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

Các số liệu đo lường cụ thể theo bộ dữ liệu về cơ sở hạ tầng lừa đảo và thời gian tồn tại được ghi nhận.

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020

Các bằng chứng thực nghiệm gần đây về các tên miền lừa đảo mới được đăng ký và phân bố theo thời gian tồn tại.

[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 - Phân tích được tài trợ về các trường hợp đăng ký tên miền độc hại và các yếu tố của hệ sinh thái; những hạn chế liên quan đối với các khẳng định về mối quan hệ nhân quả.

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

Dự báo của nhà cung cấp về lượng tiền đổ vào từ các vụ lừa đảo trên chuỗi vào năm 2025; không được tính vào tổng số vụ lừa đảo qua tên miền.

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

Các cuộc tấn công lừa đảo/URL đã được ghi nhận; các chỉ số này không tương đương với số lượng tên miền đã đăng ký duy nhất.

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

Phân loại các cuộc tấn công đã được ghi nhận, các tên miền duy nhất và các tên miền được đăng ký với mục đích xấu.

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

Nguồn số liệu về 401,6 triệu lượt đăng ký được báo cáo trên tất cả các TLD.