LAPORAN AKTIVITAS ABUSE DOMAIN .ID

Indonesia Domain Abuse Data Exchange

IDADX

Periode Q1 2026

Januari – Maret

pandi.id | domain.id

Daftar Isi

Pendahuluan

Seiring perkembangan ekosistem digital diikuti dengan meningkatnya risiko penyalahgunaan domain untuk berbagai aktivitas ilegal dan berbahaya. Domain sering dimanfaatkan sebagai media untuk menjalankan aktivitas seperti phishing, penyebaran malware, spam, hingga konten ilegal lainnya.

Sebagai registry domain .id, Pengelola Nama Domain Internet Indonesia (PANDI) memiliki tanggung jawab strategis dalam menjaga keamanan dan integritas ekosistem domain .id. Dalam konteks tersebut, Indonesia Domain Abuse Data Exchange (IDADX) dikembangkan sebagai platform terintegrasi untuk mengelola, menganalisis, dan merespons data terkait domain abuse secara terstruktur dan kolaboratif. IDADX berfungsi sebagai pusat pertukaran data (data exchange) yang mengintegrasikan berbagai sumber informasi terkait penyalahgunaan domain .id.

Ruang Lingkup

Ruang lingkup IDADX mencakup identifikasi, pemantauan, analisis, dan penanganan berbagai bentuk penyalahgunaan domain .id yang berpotensi mengganggu keamanan serta kepercayaan ekosistem digital. Dalam pelaksanaannya, IDADX memantau kategori ancaman seperti phishing, malware, spam, judi online, pornografi, serta konten ilegal atau berisiko lainnya.

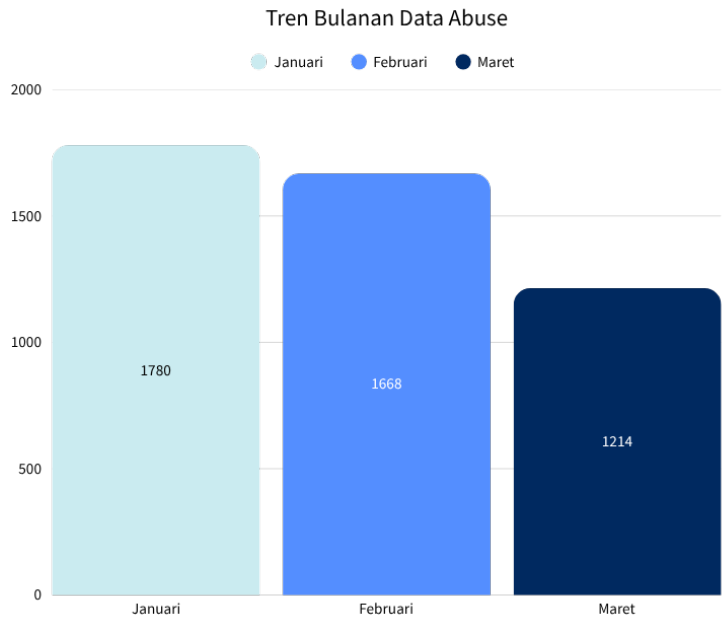
IDADX memanfaatkan data dari berbagai sumber yaitu Registrar PANDI, laporan publik, BIMA (Breach Identification and Monitoring Assistant), kerja sama dengan berbagai mitra keamanan siber (CleanDNS, Netcraft), dan instansi pemerintah terkait (Komdigi dan BSSN).

Ringkasan Eksekutif

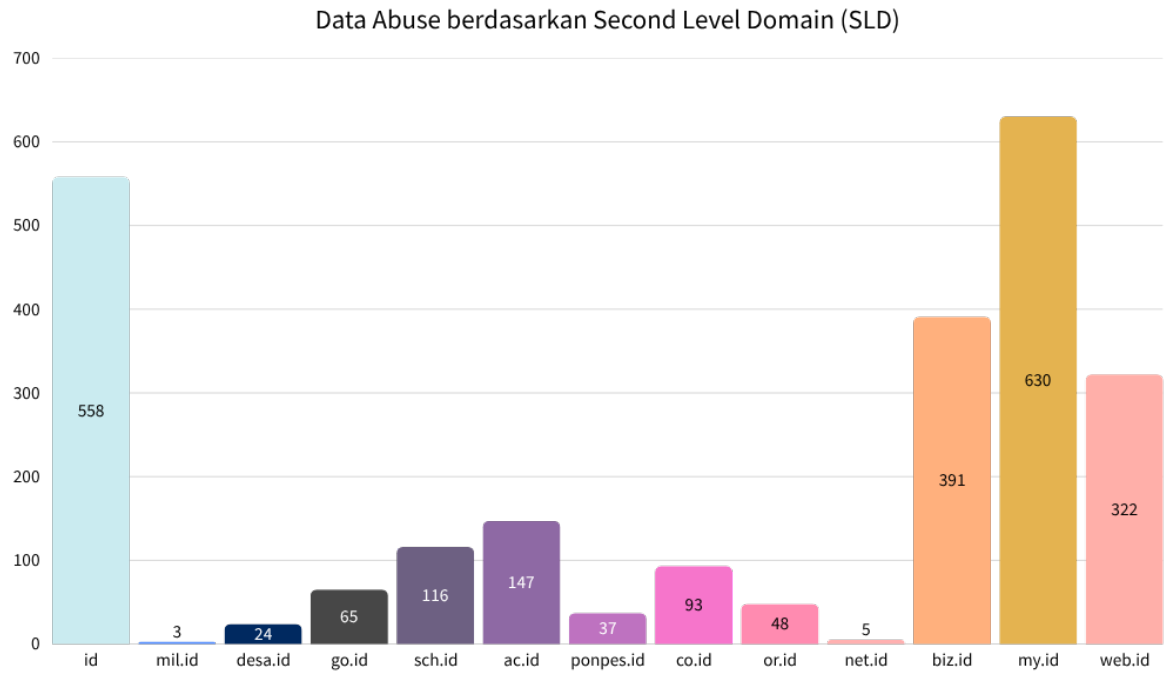
- Selama Quartal 1 tahun 2026, IDADX mencatat total 4.662 link abuse dengan total 2.439 nama domain.
- Penyalahgunaan domain terkonsentrasi pada beberapa SLD utama, terutama my.id, id, biz.id, dan web.id. Konsentrasi ini menunjukkan bahwa pelaku cenderung memanfaatkan domain yang lebih fleksibel, mudah didaftarkan, dan memungkinkan rotasi cepat.
- Berdasarkan kategori ancaman, phishing dan online gambling merupakan ancaman paling dominan.
- Berdasarkan kategori industri, sektor financial menjadi target utama dengan kontribusi 36,3%. Komposisi ini menegaskan bahwa platform berbasis transaksi, akun pengguna, dan interaksi digital tinggi merupakan sasaran utama abuse domain.
- Secara keseluruhan, hasil Q1 2026 menunjukkan bahwa ancaman domain abuse masih berfokus pada phishing, perjudian online, dan impersonasi brand, sehingga penguatan kebijakan registrasi, deteksi dini, analisis berbasis risiko, dan kolaborasi lintas pihak tetap menjadi prioritas strategis IDADX.

Statistik Abuse Domain Pada Q1 2026

Selama Quartal 1 tahun 2026, IDADX mencatat total 4.662 link abuse dengan tren penurunan yang konsisten dari bulan ke bulan, yaitu 1.780 kasus pada Januari, 1.668 kasus pada Februari, dan 1.214 kasus pada Maret. Secara umum, terlihat adanya tren penurunan jumlah kasus dari bulan ke bulan sepanjang periode tersebut.



Berdasarkan grafik distribusi penyalahgunaan domain per Second-Level Domain (SLD) dibawah ini, terlihat bahwa penyalahgunaan tidak tersebar secara merata, melainkan terkonsentrasi pada beberapa SLD tertentu. SLD dengan jumlah kasus tertinggi adalah my.id sebanyak 630 kasus, diikuti oleh id sebanyak 558 kasus, biz.id sebanyak 391 kasus, dan web.id sebanyak 322 kasus. Keempat SLD ini secara signifikan mendominasi total temuan dibandingkan SLD lainnya.



Dominasi pada SLD seperti my.id, id, biz.id, dan web.id mengindikasikan bahwa pelaku cenderung memilih domain yang memiliki karakteristik lebih fleksibel, mudah didaftarkan, serta tidak terlalu ketat dalam proses verifikasi. SLD tersebut umumnya memungkinkan registrasi yang cepat dan masif, sehingga lebih mudah dimanfaatkan untuk aktivitas seperti phishing dan judi online yang membutuhkan rotasi domain secara cepat. Sebaliknya, SLD seperti mil.id, go.id, dan ac.id yang memiliki proses verifikasi lebih ketat menunjukkan tingkat penyalahgunaan yang jauh lebih rendah, sehingga mencerminkan efektivitas kontrol administratif dalam menekan potensi abuse.

2.439
Total Abuse Domain

600
Total Domain Baru
(<60 hari)

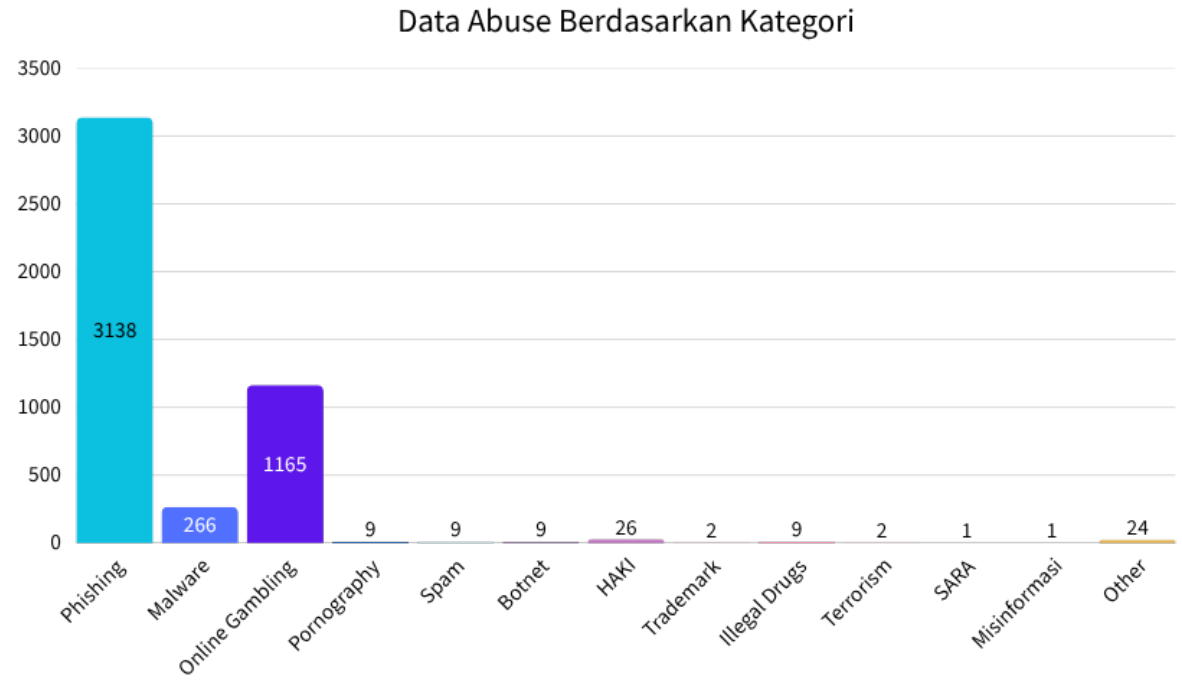
1.839
Total Domain Lama
(≥60 hari)

Berdasarkan analisis usia domain, mayoritas penyalahgunaan domain pada Quartal 1 dilakukan menggunakan domain lama (75,4%), yang mengindikasikan

adanya pemanfaatan domain yang telah terdaftar sebelumnya atau kemungkinan domain yang telah dikompromikan. Di sisi lain, sebesar 24,6% domain merupakan domain baru (kurang dari 60 hari), yang menunjukkan bahwa pelaku juga memanfaatkan domain yang baru didaftarkan sebagai bagian dari strategi untuk menghindari deteksi.

Statistik Abuse Domain Berdasarkan Kategori

Berdasarkan grafik distribusi kategori penyalahgunaan domain, terlihat bahwa ancaman sangat terkonsentrasi pada beberapa kategori utama, khususnya phishing dan online gambling. Kategori phishing merupakan yang paling dominan dengan total 3.138 kasus, diikuti oleh online gambling sebanyak 1.165 kasus.
Distribusi ini menunjukkan bahwa lebih dari 85–90% penyalahgunaan domain didorong oleh motif ekonomi, yaitu melalui penipuan (phishing) dan aktivitas perjudian online. Tingginya angka phishing mengindikasikan bahwa domain masih menjadi sarana utama untuk melakukan impersonasi terhadap layanan terpercaya, khususnya di sektor finansial dan platform digital.



Di sisi lain, kategori seperti malware, botnet, dan spam yang relatif kecil tidak berarti tidak berbahaya, melainkan menunjukkan bahwa pola ancaman saat ini lebih berfokus pada eksploitasi berbasis sosial (social engineering) dibandingkan eksploitasi teknis murni. Hal ini menjadi indikasi bahwa pelaku lebih mengandalkan manipulasi perilaku pengguna daripada kerentanan sistem.

Organisasi/Brand Sasaran Abuse Domain

Data berikut merupakan gabungan dari informasi terkait situs web penyalahgunaan, nama organisasi/brand, dan nama domain. Berikut penjelasan masing-masing kategori data:

- **Situs web penyalahgunaan**, merupakan tolok ukur utama dari penyalahgunaan domain yang dikumpulkan melalui dashboard IDADX.
- **Nama organisasi/brand**, setiap URL yang dilaporkan mengandung nama organisasi atau brand yang dicantumkan. Jumlah nama organisasi/brand dihitung berdasarkan entitas yang unik.
- **Nama domain**, URL penyalahgunaan domain mengandung nama domain yang bersifat unik. Umumnya, penyalahgunaan domain dilakukan melalui subdomain, di mana beberapa subdomain berbeda dapat memuat konten yang sama. Oleh karena itu, data ini dihitung berdasarkan nama domain unik untuk menghindari redundansi.

Kategori	Januari	Februari	Maret
Situs Web Abuse	1.780	1.668	1.214
Organisasi/Brand yang diincar	60	63	72
Nama Domain	929	949	678

Berikut ini merupakan daftar urutan 10 organisasi/brand yang menjadi target abuse domain pada Q1 2026:

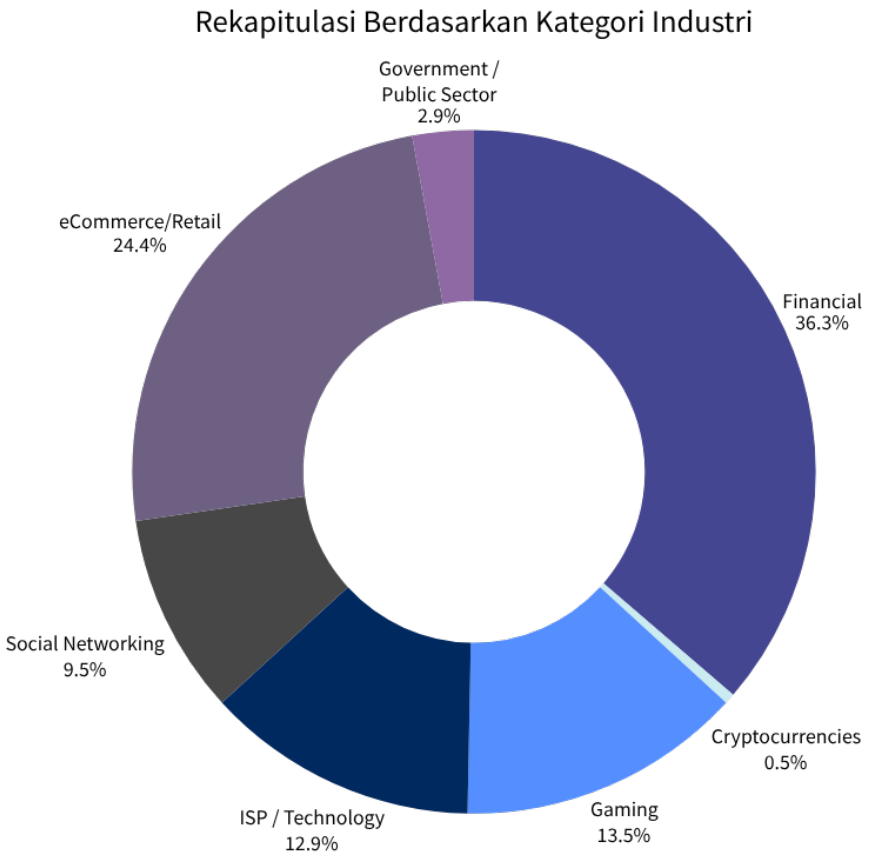
Peringkat	Brand
1	Dana
2	Canva
3	Mobile Legends
4	Microsoft
5	Bank Central Asia (BCA)
6	Shopee
7	UOB
8	Mabes TNI
9	Naver
10	Whatsapp

Berdasarkan hasil agregasi brand, terlihat bahwa target penyalahgunaan domain paling dominan pada Quartal 1 adalah Dana, diikuti dengan Canva, Mobile

Legends, Microsoft, dan Bank Central Asia (BCA). Temuan ini menunjukkan bahwa pelaku tidak hanya menargetkan sektor keuangan, tetapi juga platform digital dengan basis pengguna besar, termasuk layanan desain, gim, komunikasi, dan produktivitas.

Di sisi lain, kemunculan brand seperti Shopee dan WhatsApp menunjukkan bahwa platform dengan intensitas interaksi pengguna yang tinggi tetap menjadi sasaran utama dalam skema impersonasi dan phishing. Secara umum, pola ini menegaskan bahwa reputasi brand, jumlah pengguna, dan kedekatan layanan dengan aktivitas harian masyarakat merupakan faktor utama yang memengaruhi tingkat eksploitasi.

Industri Sasaran Abuse Domain



Distribusi kategori menunjukkan bahwa sektor financial masih menjadi target utama penyalahgunaan domain dengan kontribusi sebesar 36,3%, jauh di atas kategori lainnya. Hal ini konsisten dengan pola ancaman phishing yang berorientasi pada pencurian data dan keuntungan finansial.

Di posisi kedua, sektor eCommerce/Retail menyumbang 24,4%, yang mencerminkan tingginya aktivitas pengguna dan potensi transaksi yang dapat dieksploitasi oleh pelaku. Selanjutnya, kategori gaming (13,5%) dan ISP/technology (12,9%) menunjukkan bahwa platform dengan basis pengguna besar dan keterlibatan tinggi juga menjadi target signifikan, baik untuk pencurian akun maupun penyebaran tautan berbahaya.

Kategori social networking sebesar 9,5% memperkuat indikasi bahwa media sosial masih menjadi sarana utama dalam mendukung social engineering dan distribusi phishing. Sementara itu, kategori government dan cryptocurrencies relatif kecil, masing-masing sebesar 2,9% dan 0,5%, namun tetap memiliki tingkat risiko tinggi, terutama pada sektor kripto yang berkaitan dengan nilai transaksi yang besar.

Kontak Kami

Email : helpdesk@pandi.id
Telepon : +62-2130-0557-77
Whatsapp : +62-8118-8055-30