LAPORAN AKTIVITAS ABUSE DOMAIN .ID

Indonesia Domain Abuse Data Exchange

IDADX

Periode Q3 2026

Juli – September

pandi.id | domain.id

Daftar Isi

Pendahuluan 1
Ruang Lingkup 1
Ringkasan Eksekutif 2
Statistik Abuse Domain Pada Q3 2026 2
Statistik Abuse Domain Berdasarkan Kategori 4
Organisasi/Brand Sasaran Abuse Domain 5
Industri Sasaran Abuse Domain 7

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.

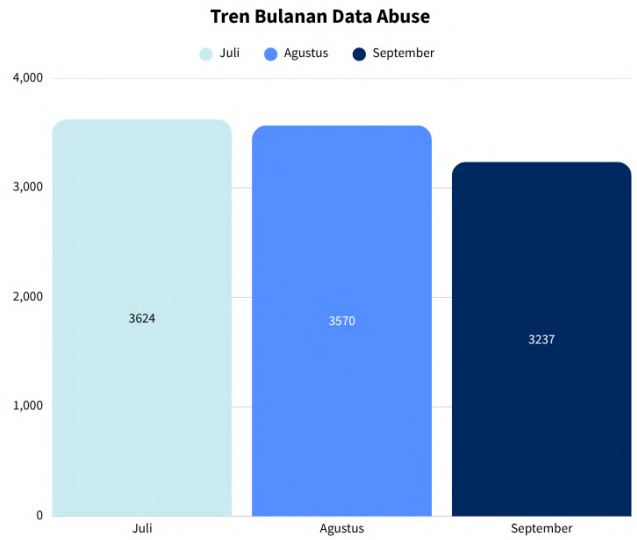
IDADX memanfaatkan data dari berbagai sumber yaitu Registrar PANDI, laporan publik, BIMA (Breach Identification and Monitoring Assistant), kerja sama dengan berbagai mitra keamanan siber (CleanDNS, Netcraft, dan TNN), dan instansi pemerintah terkait (Komdigi dan BSSN).

Ringkasan Eksekutif

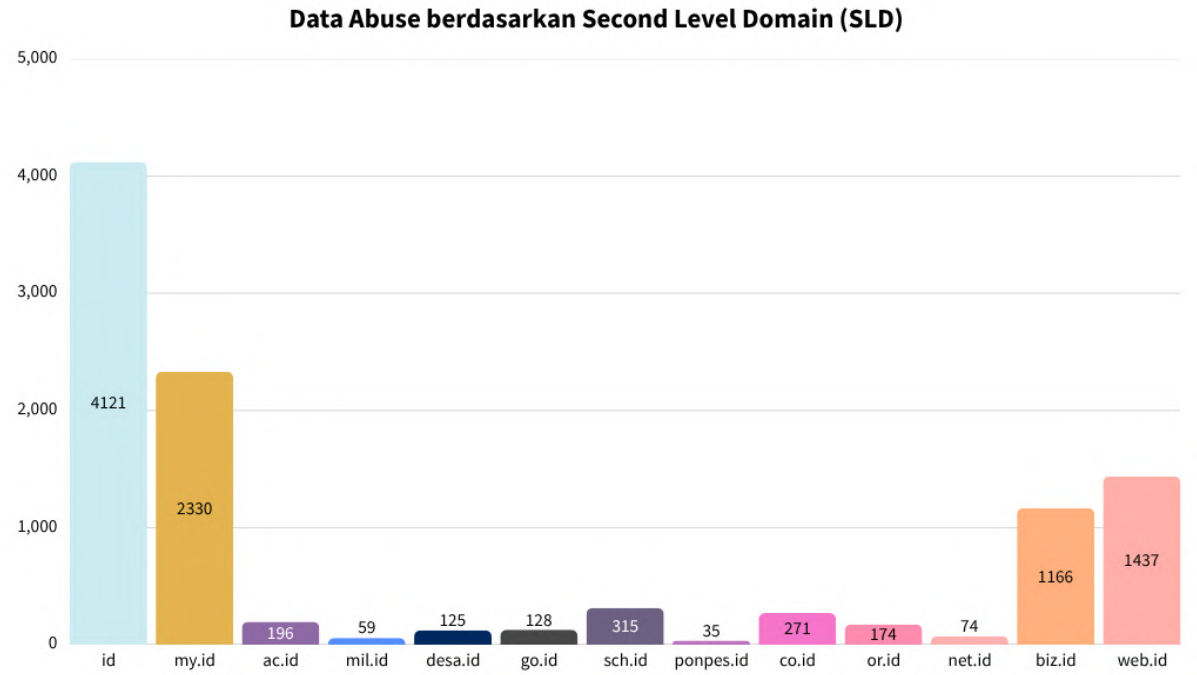
- Selama Kuartal 3 tahun 2026, IDADX mencatat total 10.431 link abuse dengan total 8.245 nama domain, turun sekitar 62,6% dibandingkan Kuartal 2 (27.872 link abuse).
- Penyalahgunaan domain terkonsentrasi pada beberapa SLD utama, terutama id, my.id, web.id, dan biz.id yang secara gabungan mencakup 86,8% dari total kasus. Konsentrasi ini menunjukkan bahwa pelaku cenderung memanfaatkan domain yang lebih fleksibel, mudah didaftarkan, dan memungkinkan rotasi cepat.
- Berdasarkan kategori ancaman, online gambling (67,9%) dan phishing (28,6%) merupakan ancaman paling dominan. Online gambling masih menyumbang porsi terbesar, namun proporsi phishing meningkat signifikan dibandingkan Kuartal 2.
- Berdasarkan kategori industri, sektor financial menjadi target utama dengan kontribusi 51,03%, diikuti oleh sektor gaming dengan 19,5% dan social networking dengan 11,4%. Komposisi ini menegaskan bahwa platform berbasis transaksi, akun pengguna, dan interaksi digital tinggi merupakan sasaran utama abuse domain.
- Secara keseluruhan, hasil Q3 2026 menunjukkan penurunan volume abuse domain, namun ancaman masih berfokus pada perjudian online, phishing, 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 Q3 2026

Selama Kuartal 3 tahun 2026, IDADX mencatat total 10.431 link abuse dengan tren yang cenderung menurun dari bulan ke bulan, yaitu 3.624 kasus pada Juli, 3.570 kasus pada Agustus, dan 3.237 kasus pada September. Penurunan paling terlihat terjadi pada September, yaitu turun 9,3% dibandingkan Agustus. Secara kuartalan, jumlah kasus turun sekitar 62,6% dibandingkan Kuartal 2 (27.872 kasus), setelah lonjakan tajam yang terjadi pada Juni 2026.



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 id sebanyak 4.121 kasus (39,5%), diikuti oleh my.id sebanyak 2.330 kasus (22,3%), web.id sebanyak 1.437 kasus (13,8%), dan biz.id sebanyak 1.166 kasus (11,2%). SLD id masih mendominasi total temuan, sementara my.id justru mengalami peningkatan dibandingkan Kuartal 2, dari 1.765 kasus menjadi 2.330 kasus.



Dominasi pada SLD seperti id, my.id, web.id, dan biz.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 ponpes.id, mil.id, net.id, dan desa.id yang memiliki proses verifikasi lebih ketat menunjukkan tingkat penyalahgunaan yang jauh lebih rendah, sehingga mencerminkan efektivitas kontrol administratif dalam menekan potensi abuse. Meski demikian, temuan pada SLD terverifikasi seperti sch.id (315 kasus), ac.id (196 kasus), dan go.id (128 kasus) tetap perlu diwaspadai karena kemungkinan besar berasal dari situs yang dikompromikan.

8.245	5.291	2.954
Total Abuse Domain	Total Domain Baru (<60 hari)	Total Domain Lama (≥60 hari)

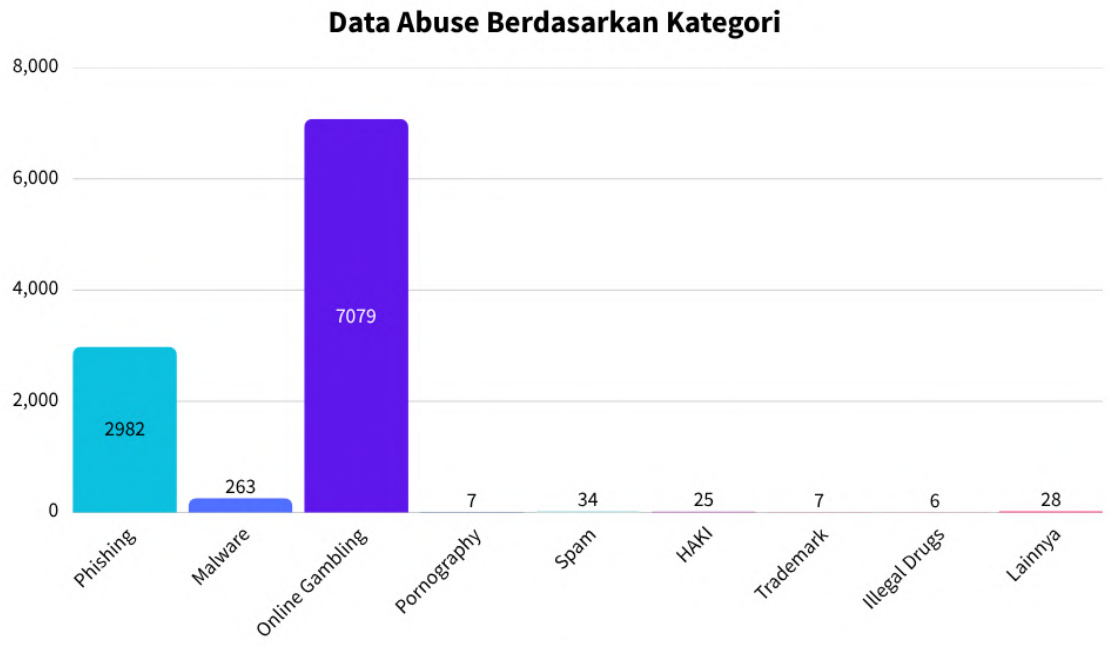
Berdasarkan analisis usia domain, mayoritas penyalahgunaan domain pada Kuartal 3 menggunakan domain baru yang terdaftar kurang dari 60 hari (64,2%, atau 5.291 domain), yang mengindikasikan bahwa pelaku banyak mendaftarkan domain baru secara khusus untuk aktivitas penyalahgunaan guna menghindari deteksi dan pemblokiran dini. Di sisi lain, sebesar 35,8% (2.954 domain) merupakan domain lama, yang kemungkinan telah dikompromikan atau dimanfaatkan kembali setelah sebelumnya terdaftar untuk keperluan lain. Proporsi domain lama ini meningkat dibandingkan Kuartal 2 (25,1%), sehingga pengamanan terhadap domain yang sudah lama terdaftar perlu mendapat perhatian lebih.

Statistik Abuse Domain Berdasarkan Kategori

Berdasarkan grafik distribusi kategori penyalahgunaan domain, terlihat bahwa ancaman sangat terkonsentrasi pada beberapa kategori utama, khususnya online gambling dan phishing. Kategori online gambling merupakan yang paling dominan dengan total 7.079 kasus, diikuti oleh phishing sebanyak 2.982 kasus dan malware sebanyak 263 kasus.

Distribusi ini menunjukkan bahwa sekitar 96% penyalahgunaan domain didorong oleh motif ekonomi, yaitu melalui aktivitas perjudian online dan penipuan (phishing), dengan online gambling saja menyumbang sekitar 68% dari keseluruhan kasus. Jumlah kasus online gambling turun tajam sebesar 69,7% dibandingkan Kuartal 2, sementara phishing relatif stabil (turun 11,0%) sehingga porsinya naik dari sekitar 12% menjadi 28,6%. Hal ini menunjukkan bahwa

phishing tetap menjadi ancaman signifikan sebagai sarana impersonasi terhadap layanan terpercaya, khususnya di sektor finansial dan platform digital.



Di sisi lain, kategori seperti malware, spam, HAKI, trademark, pornography, dan illegal drugs 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	Juli	Agustus	September
Situs Web Abuse	3.624	3.570	3.237
Organisasi/Brand yang diincar	94	129	86
Nama Domain	2.624	3.012	2.745

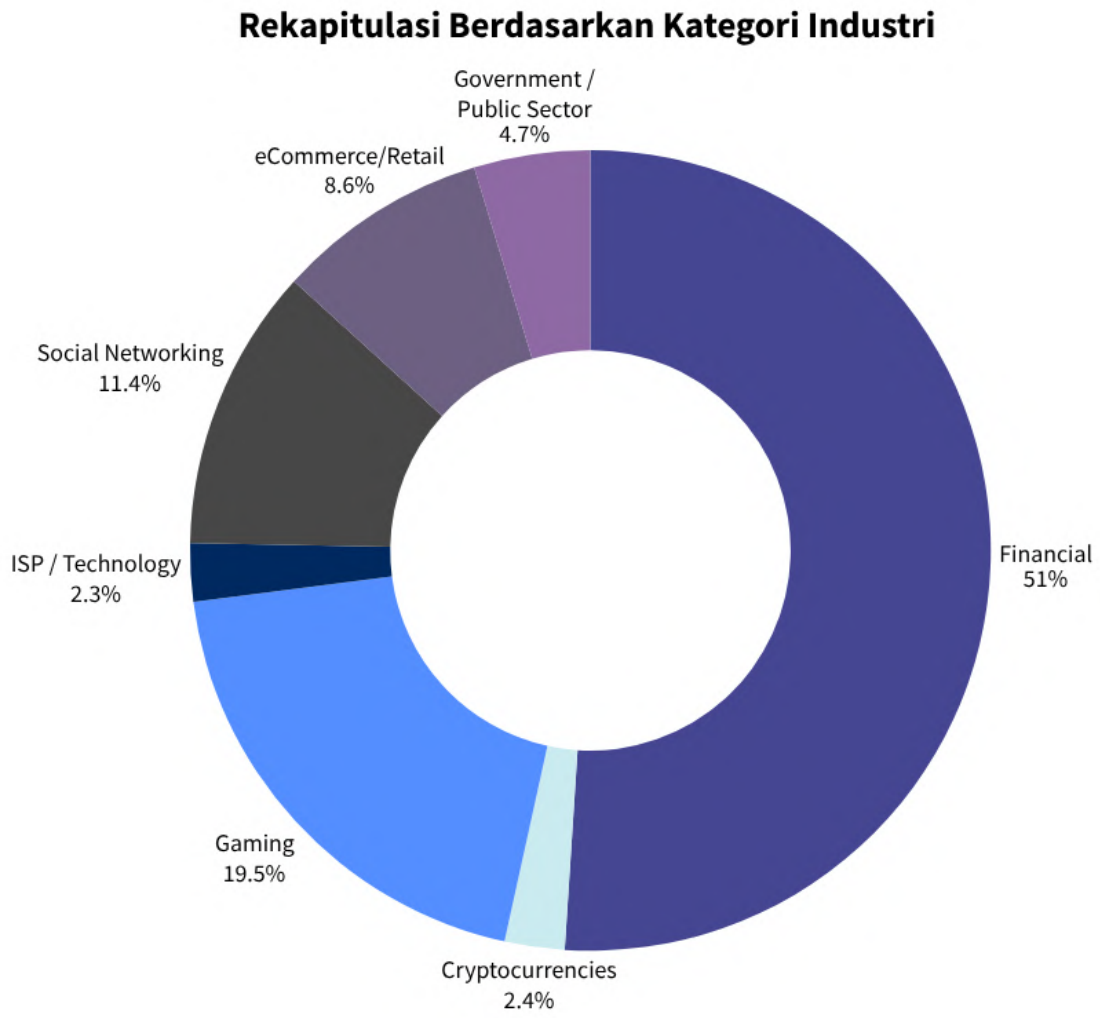
Berikut ini merupakan daftar urutan 10 organisasi/brand yang menjadi target abuse domain pada Q3 2026:

Peringkat	Brand
1	DANA
2	Mobile Legends
3	BCA
4	WhatsApp
5	Shopee
6	Facebook
7	Israelpost
8	Naver
9	Maybank Indonesia
10	Maxis

Berdasarkan hasil agregasi brand, terlihat bahwa target penyalahgunaan domain paling dominan pada Kuartal 3 adalah DANA, diikuti dengan Mobile Legends, BCA, WhatsApp, dan Shopee. Temuan ini menunjukkan bahwa pelaku tidak hanya menargetkan sektor keuangan, tetapi juga platform digital dengan basis pengguna besar, termasuk layanan gim, perpesanan, dan e-commerce. Selain itu, munculnya brand luar negeri seperti Israelpost, Naver, dan Maxis menunjukkan bahwa domain .id juga dimanfaatkan dalam kampanye phishing yang menyasar pengguna di luar Indonesia.

Di sisi lain, kemunculan brand seperti WhatsApp, Shopee, dan Facebook 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 51,03%, jauh di atas kategori lainnya. Hal ini konsisten dengan pola ancaman phishing dan online gambling yang berorientasi pada pencurian data dan keuntungan finansial.

Di posisi kedua, sektor gaming menyumbang 19,5%, meningkat signifikan dibandingkan Kuartal 2 (8,1%). Hal ini menunjukkan bahwa platform dengan basis pengguna besar dan keterlibatan tinggi menjadi target signifikan, baik untuk pencurian akun maupun penyebaran tautan berbahaya, sejalan dengan posisi Mobile Legends sebagai brand kedua yang paling banyak diincar. Sementara itu, sektor Government/Public Sector yang pada Kuartal 2 melonjak hingga 23,3% tidak lagi menjadi kategori dominan pada Kuartal 3. Selanjutnya, sektor eCommerce/Retail menyumbang 8,6%, yang mencerminkan tingginya aktivitas pengguna dan potensi transaksi yang dapat dieksploitasi oleh pelaku.

Kategori social networking sebesar 11,4% memperkuat indikasi bahwa media sosial masih menjadi sarana utama dalam mendukung social engineering dan distribusi phishing. Sementara itu, kategori cryptocurrencies menyumbang 2,4% dan ISP/technology sebesar 2,3%. Meskipun porsinya kecil, kategori cryptocurrencies tetap memiliki tingkat risiko tinggi mengingat nilai transaksi yang besar.

Kontak Kami

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