LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID

Indonesia Anti-Phishing Data Exchange

IDADX

Periode Q3 2023

Juli – September 2023

Daftar Isi

Ruang Lingkup Laporan Phishing

Laporan tren aktivitas phishing IDADX menganalisis serangan phishing dan pencurian identitas lainnya pada nama domain .id. Laporan ini didapatkan dari hasil data APWG yang dilaporkan oleh anggotanya di http://www.apwg.org, dan melalui email kiriman ke reportphishing@antiphishing.org.
Dalam laporan ini, kami juga mengumpulkan data phishing dari Netcraft yang dikirimkan melalui email. Selain itu, IDADX juga mendapatkan laporan dari anggotanya yang dilaporkan melalui situs web http://idadx.id, dan laporan phishing dari masyarakat.

Definisi Phishing

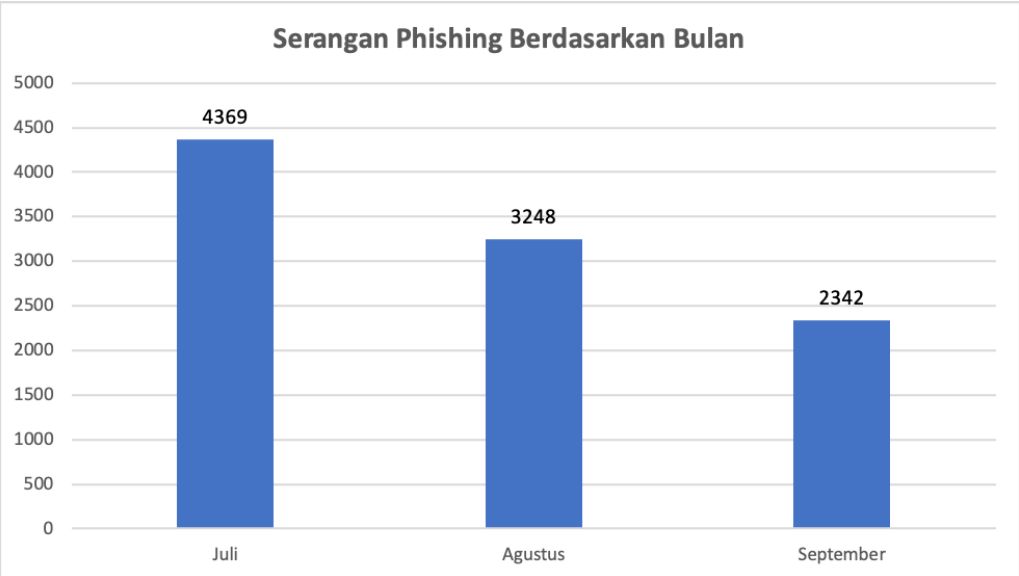
Phishing adalah sebuah kejahatan dengan upaya mendapatkan informasi pribadi seseorang hingga kredensial akun keuangan. Pada saat ini, phishing biasanya dilakukan dengan skema *social engineering* dan *technical subterfuge*. *Social engineering* mengincar korban yang tidak waspada dengan memanipulasi mereka agar percaya bahwa mereka berurusan dengan pihak yang tepercaya dan sah, seperti mengirimkan pesan penipuan melalui alamat email. *Technical Subterfuge* menanam malware ke komputer untuk mencuri informasi kredensial dari korban, biasanya menggunakan sistem yang mencegat nama pengguna dan kata sandi atau mengarahkan pengguna ke situs web palsu. Sebagai akibat dari penipuan ini, semakin banyak konsumen yang menderita penipuan kartu kredit, pencurian identitas, dan kerugian finansial.

Ringkasan Laporan Phishing

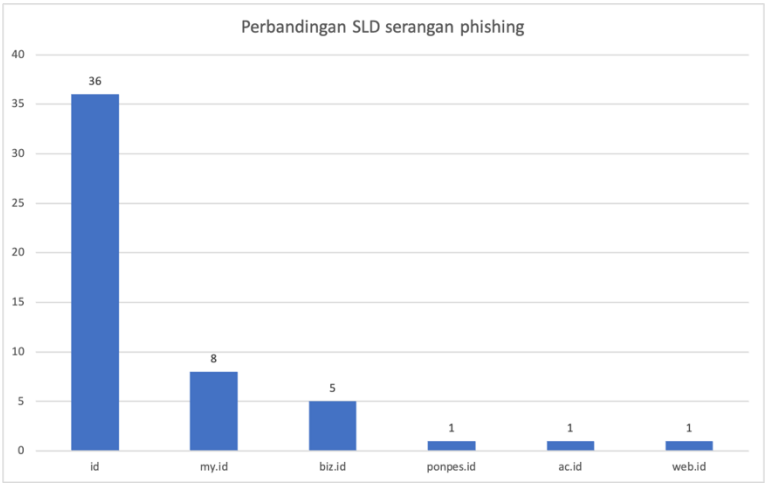
- IDADX mendapatkan laporan phishing sebanyak 98.645 selama kurun waktu 5 tahun terakhir sejak tahun 2018.
- Jumlah serangan phishing pada Q3 2023 sebanyak 9.823 dimana mengalami penurunan dari kuratal sebelumnya.
- Total domain yang digunakan phishing pada Q3 2023 sebanyak 52 nama domain.
- Sektor media sosial paling sering menjadi serangan phishing sejak kuartal pertama hingga kuartal ketiga tahun ini dengan persentase 55,45%.
- Jumlah merek/brand yang diserang sebanyak 69 brand.
- Serangan terhadap lembaga keuangan mengalami penurunan di tahun 2023. Namun pada kuartal ketika 2023, lembaga keuangan menempati urutan kedua dengan persentase sebanyak 22.7%.

Statistik Laporan Phishing Pada Q3 2023

Jumlah laporan phishing yang diterima oleh IDADX dalam kuartal ketiga 2023 sebanyak 9.823, dimana mengalami penurunan sebanyak 10.507 laporan phishing dari kuartal kedua 2023. Berdasarkan laporan phishing tersebut, sebanyak 9.648 laporan phishing merupakan data phishing https://s.id.



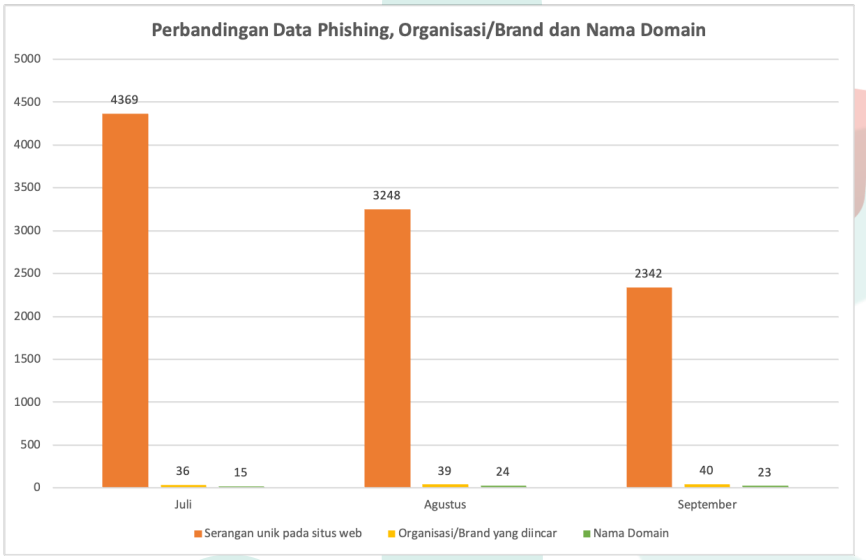
Pada Q3 2023 terdapat sebanyak 9.823 url phishing, dimana data tersebut berasal dari 52 domain yang berbeda. Beberapa SLD yang menjadi sasaran phishing yaitu id, my.id, biz.id, ponpes.id, ac.id, dan web.id.



Organisasi/Brand yang menjadi sasaran phishing

Grafik berikut menggabungkan statistik berdasarkan situs web phishing unik, nama merek unik, dan nama domain unik. Berikut ini penjelasan dari masing-masing data:

- **Situs web phishing**, hal ini merupakan tolok ukur utama phishing yang dikumpulkan pada dashboard IDADX.
- **Nama organisasi**, setiap URL yang dilaporkan mengandung nama organisasi/brand yang dicantumkan. Jumlah nama organisasi/brand diambil berdasarkan kelompok organisasi/brand yang unik.
- **Nama domain,** URL link mengandung nama domain yang sifatnya unik. Beberapa serangan phishing menggunakan subdomain. Biasanya, dari beberapa subdomain yang berbeda, berisi jenis phishing yang sama. Metrik ini mengukur jumlah nama domain unik sehingga tidak ada redudansi data nama domain.



Pada data tersebut dapat dilihat bahwa, pada bulan Juli merupakan jumlah laporan phishing tertinggi selama periode kuartal ketiga.

Pengelompokan Serangan Phishing	Juli	Agustus	September
Total Phishing	4369	3248	2342
Organisasi/Brand yang diincar	36	39	40
Nama Domain	15	24	23

Berikut ini merupakan daftar 10 nama organisasi/brand yang menjadi target serangan phishing pada Q3 2023:

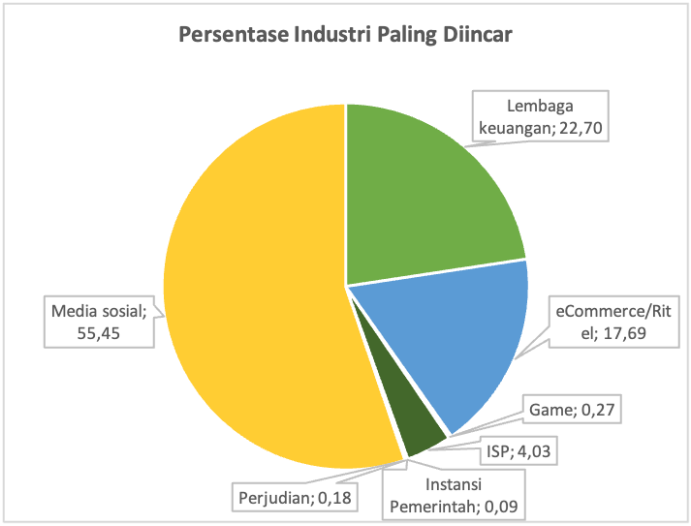
No	Organisasi/Brand
1	Facebook
2	Instagram
3	DHL
4	First National Bank of South Africa
5	British Telecom
6	KBC
7	NBT Bank
8	USPS
9	Poste Italiane
10	Meta

Negara yang Menghosting Situs Phishing Domain .id

Indonesia menempati posisi teratas sebagai negara yang menghosting situs phishing domain .id selama Q3 tahun 2023 dan dilanjutkan pada posisi kedua yaitu United States. Pada kuartal ketiga ini negara yang digunakan menghosting situs phishing domain lebih bervariasi daripada kuartal sebelumnya.

Negara	Juli	Agustus	September
Indonesian	89.77%	90.67%	83.35%
United States	8.7%	8.62%	14.18%
Singapore	0.02%	0.03%	0.9%
Germany	-	0.22%	0.21%
Cyprus	0.07%	-	-
Malaysia	0.02%	-	-
Israel	0.02%	-	-
Russia	0.05%	0.12%	0.94%
Philippines	-	0.06%	-
Netherlands	-	-	0.04%
Australia	-	-	0.09%
None	1.35%	0.28%	0.3%

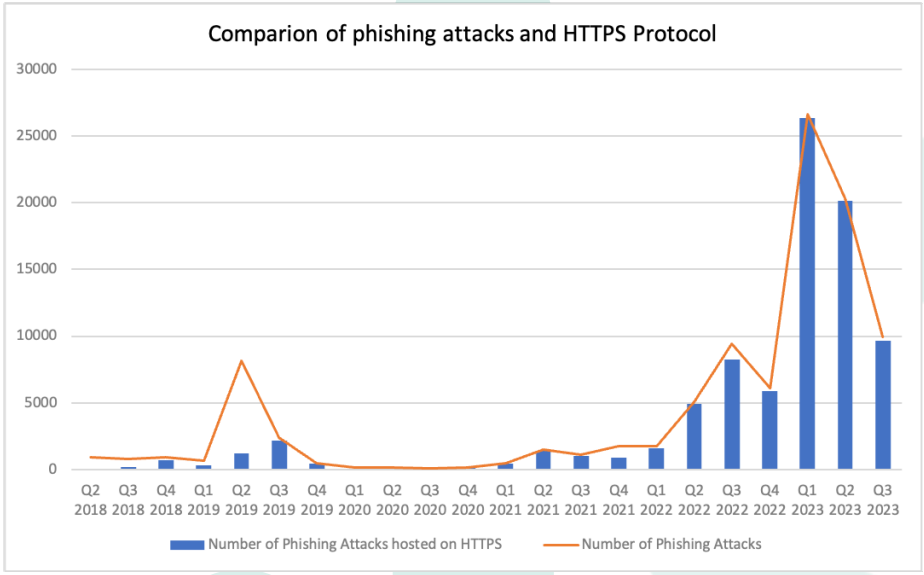
Industri Sasaran Phishing



Sektor industri yang paling ditargetkan untuk serangan phishing yaitu media sosial sebesar 55,45%, yang selanjutnya diikuti pada posisi kedua yaitu lembaga keuangan sebesar 22,70%. Posisi tersebut mengalami perubahan pada beberapa kuartal sebelumnya dimana lembaga keuangan berada pada posisi teratas.

Serangan Phishing Pada Situs Web yang Terenkripsi

Berdasarkan data yang terkumpul pada dashboard IDADX, dilakukan analisa terhadap situs phishing yang menggunakan protocol HTTPS.
Pada saat ini situs web phishing yang digunakan kebanyakan menggunakan protocol HTTPS. Kami melakukan perbandingan antara jumlah serangan phishing pada situs web dan situs web yang menggunakan protokol HTTPS. Dapat dilihat dari tahun 2021, jumlah protocol HTTPS lebih banyak digunakan hingga kuartal kedua tahun 2023.



Berdasarkan dari grafik tersebut, sejak Q3 tahun 2019 hingga Q3 tahun 2023 jumlah serangan phishing pada situs web yang menggunakan protokol HTTPS mengalami peningkatan. Hal ini menunjukkan bahwa, situs web yang terenkripsi banyak digunakan untuk phishing dan memiliki celah untuk diretas.

Tentang IDADX

Indonesia Anti-Phishing Data Exchange (IDADX) didirikan pada tahun 2021 dibawah kepengurusan Pengelola Nama Domain Internet Indonesia (PANDI). IDADX adalah sebuah inisiasi untuk meningkatkan keamanan siber nasional dengan memfasilitasi respons global terhadap kejahatan internet di sektor pemerintah, penegakan hukum, industri, dan komunitas internet.

Pada saat ini kami bekerjasama dengan para Registrar PANDI untuk memerangi adanya phishing. Kami tentunya tidak hanya berhenti sampai disini, kami akan mengembangkan dashboard phishing ini dengan menambah sumber data kami dan bekerjasama dengan pihak lainnya agar data yang kami miliki terpercaya dan terbaru.

IDADX mengelola situs web publik https://www.idadx.id dimana masyarakat bisa melaporkan url yang menggunakan domain .id sebagai phishing. Selain itu, laporan seputar phishing juga dapat dilaporkan melalui email helpdesk@pandi.id.