.id Expressing Your Freedom

LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID

Indonesia Anti-Phishing Data Exchange

IDADX

Periode Q1 2023

Januari – Maret 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, Google Web Risk dan menerima 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

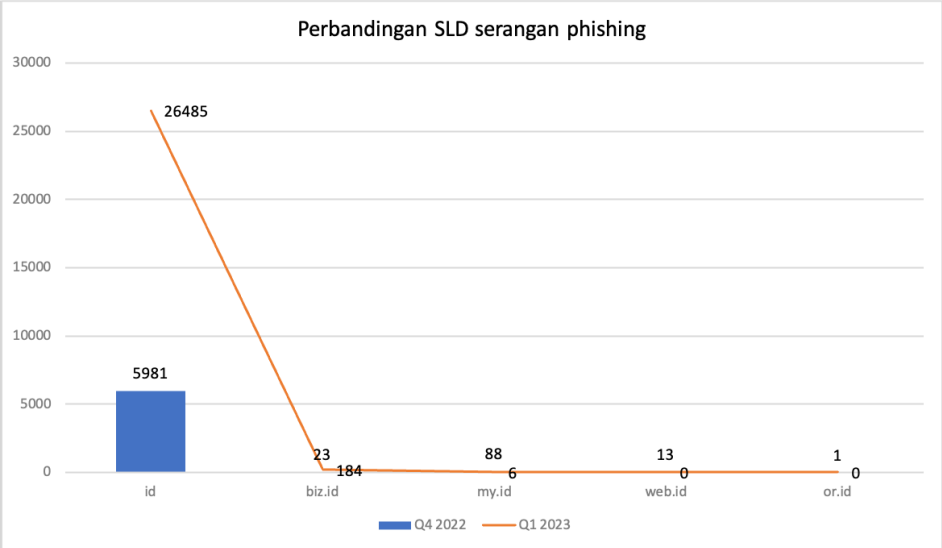
Jumlah phishing dalam kurun waktu 5 tahun terakhir	69.117
Jumlah serangan phishing yang dilaporkan pada Q1 2023	26.675
Organisasi yang paling menjadi sasaran serangan phishing pada Q1 2023	Facebook
Industri yang menjadi sasaran serangan phishing pada Q1 2023	Media Sosial
Jumlah domain yang digunakan untuk serangan phishing pada Q1 2023	207

Statistik Laporan Phishing Pada Q1 2023

Jumlah laporan phishing yang diterima oleh IDADX dalam kuartal pertama tahun 2023 mencerminkan kenaikan yang signifikan dimana pada Q1 2023 terdapat sebanyak 26.675 laporan phishing sedangkan pada Q4 2022 terdapat 6.106 laporan phishing. Hal tersebut mengalami kenaikan sebanyak 20.569 laporan phishing. Berdasarkan laporan phishing tersebut, sebanyak 26.464 laporan phishing merupakan data phishing https://s.id.

Pada Q1 2023 terdapat beberapa SLD yang menjadi sasaran phishing yaitu id, biz.id, dan my.id. Sasaran phishing pada SLD id sebanyak 26.485 laporan. Selain itu, pada SLD biz.id terdapat kenaikan serangan phishing sebanyak 161 laporan dimana pada Q4 2022 terdapat 23 serangan phishing dan pada Q1 2023 terdapat sebanyak 184 serangan phishing. Hal

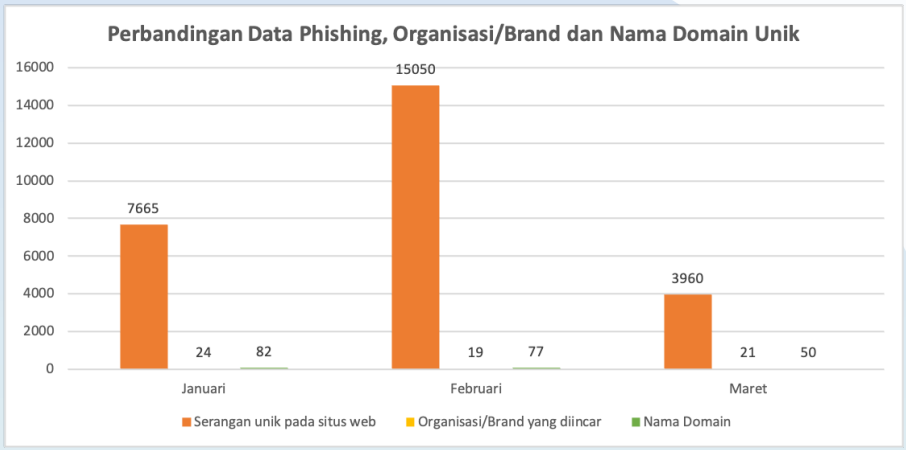
tersebut memungkinkan dengan adanya peningkatan jumlah nama domain SLD biz.id pada tahun 2022.



Organisasi/Brand yang menjadi sasaran serangan 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. URL link biasanya dikirimkan melalui email, seolah-olah email tersebut sah dan mengajak pelanggan untuk mengakses link tersebut.
- **Nama organisasi**, setiap URL yang dilaporkan mengandung nama organisasi/brand yang dicantumkan. Jumlah nama organisasi/brand unik diambil berdasarkan kelompok organisasi/brand yang unik/tidak sama.
- **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 Februari merupakan jumlah laporan phishing tertinggi selama periode kuartal pertama.

Pengelompokan Serangan Phishing	Januari	Februari	Maret
Serangan unik pada situs web	7665	15050	3960
Organisasi/Brand yang diincar	24	19	21
Nama Domain	82	77	50

Berikut ini merupakan daftar 10 nama organisasi/brand yang menjadi target serangan phishing pada Q1 2023:

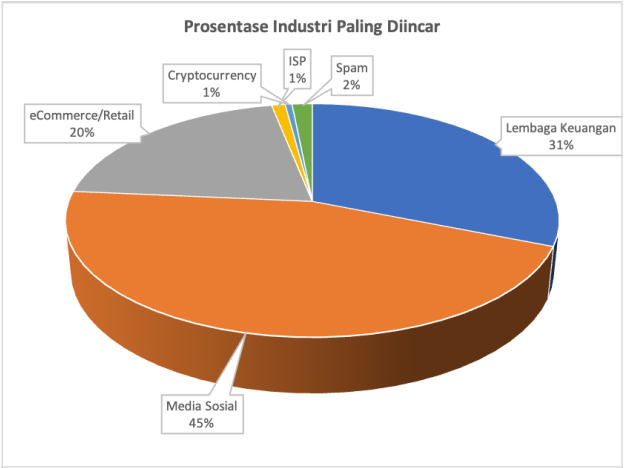
No	Organisasi/Brand
1	Facebook
2	Microsoft
3	First national bank of south africa
4	Bnp paribas nickel
5	Kbc
6	BNP paribas bnl
7	Royal mail
8	BNP paribas bcef
9	Malicious domain
10	Swiss post

Negara yang Menghosting Situs Phishing Domain .id

Indonesia menempati posisi teratas sebagai negara yang menghosting situs phishing domain .id selama Q1 tahun 2023 dan dilanjutkan pada posisi kedua yaitu United States.

Negara	Januari	Februari	Maret
Indonesia	98.97%	99.48%	98.76%
United States	0.94%	0.49%	1.21%
Austria	0.01%	-	-
Singapore	0.04%	-	-
None	0.04%	0.04%	0.03%

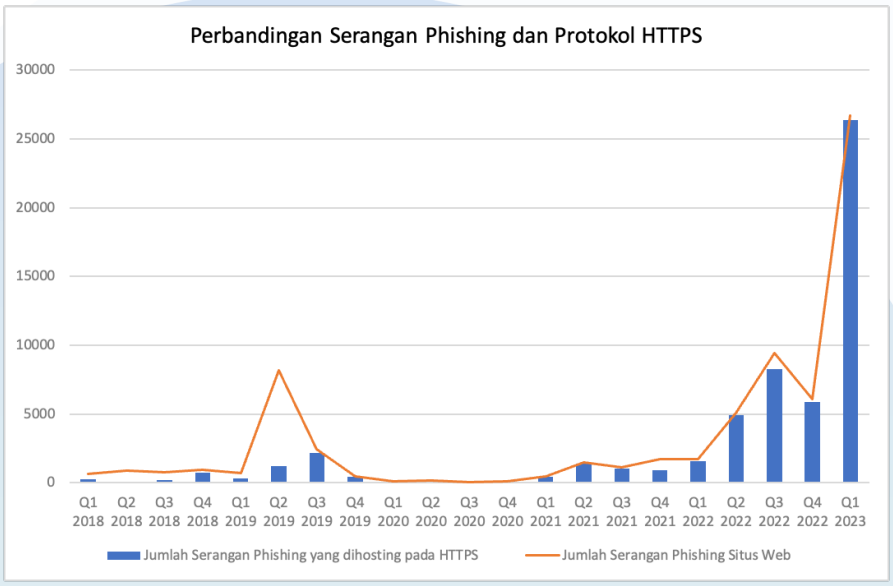
Industri Sasaran Phishing



Sektor industri yang paling ditargetkan untuk serangan phishing yaitu media sosial sebesar 45%, yang selanjutnya diikuti pada posisi kedua yaitu sektor Lembaga keuangan sebesar 31%. Posisi tersebut mengalami perubahan pada beberapa kuartal sebelumnya dimana lembaga keuangan berada pada posisi teratas. Namun, jenis sektor industri yang menjadi serangan phishing pada Q1 2023 mengalami kenaikan dari sektor media sosisal sebesar 38% dari Q4 2022.

Serangan Phishing Pada Situs Web yang Terenkripsi

Berdasarkan data yang terkumpul pada dashboard IDADX, dilakukan analisa terhadap situs phishing yang menggunakan protocol HTTPS. HTTPS digunakan untuk mengamankan komunikasi dengan mengenkripsi data yang dipertukarkan antara browser seseorang dan situs web yang dia kunjungi. Penggunaan HTTPS sangat dianjurkan, terlebih bagi website yang menyimpan data pelanggan seperti toko online atau website membership.



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 keempat tahun 2022.

Berdasarkan dari grafik tersebut, sejak Q3 tahun 2019 hingga Q1 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 permasalahan 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. Bagi yang memiliki laporan seputar phishing dapat dilaporkan melalui email helpdesk@pandi.id.