Badan Siber
dan Sandi Negara

BESTI

Berita Edukasi Siber Sosial Terkini

JUNI 2023

SOCIAL CYBER EDUCATION

Diulas kembali oleh:
Tim Peningkatan Budaya Keamanan Informasi

www.bssn.go.id

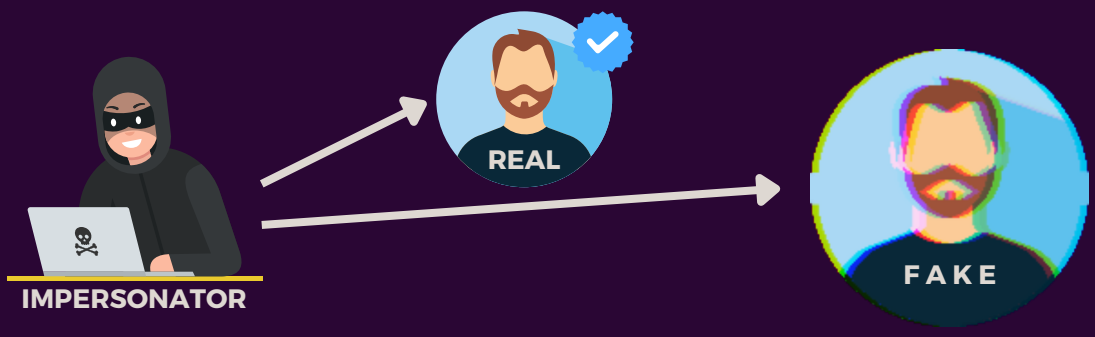
BESTI
Berita Edukasi Siber Sosial Terkini

JUNI 2023

PUBLIKASI:
15/06/2023

WASPADA
SPEAR-PHISING
BERKEDOK AKUN IMPERSONATOR

Influencer dan pemilik akun media sosial dengan *followers* yang besar harus berhati-hati. Saat ini peretas sedang mengincar akun-akun tersebut dengan membuat akun *impersonator* (tiruan) untuk keuntungan pribadi. Namun penyalahgunaan akun *impersonator* ini bisa terjadi pada siapa saja. Simak ulasan berikut untuk melihat skema penipuan yang dilakukan oleh pelaku!



Peretas pertama-tama akan melakukan serangan pengintaian untuk mengidentifikasi akun-akun *influencer* yang berpotensi. Akun *influencer* berpotensi yang dimaksud adalah informasi apapun yang disebarkan akun tersebut akan dipercaya oleh *follower* (pengikut). Karena sebagian besar akun *influencer* menggunakan kombinasi nama pribadi, sehingga pelaku menggunakan celah ini untuk membuat akun tiruan dengan embel-embel nama *influencer*.

Setelah membuat akun *impersonator*, peretas mengumpulkan data dan informasi yang cukup untuk meniru gaya bahasa dalam setiap postingan *influencer* tersebut. Kemudian peretas menyebarkan tautan jebakan di salah satu postingan. *Follower* tidak akan curiga dan akan mengira bahwa tautan tersebut adalah tautan yang valid sehingga tidak akan ragu untuk mengeklik tautan tersebut.

> *Follower* yang sudah mengeklik akan diarahkan ke halaman yang meminta data pribadi atau mengunduh suatu *file* yang ternyata adalah *malware*.

Malware adalah singkatan dari *malicious software* dan merupakan program yang dibuat secara khusus untuk menyusup. *Malware* bisa berada dalam sebuah sistem dalam waktu yang lama dan menyamar menjadi program yang bersih.

> Penyebaran tautan dari pelaku *impersonator* yang seolah tautan asli merupakan contoh dari beberapa *file* kebocoran data dan harus diwaspadai.

Didapati dugaan bahwa pelaku ingin melakukan serangan dengan teknik *social engineering* berjenis *spearphishing* untuk mendapatkan akses masuk ke jaringan internal pihak yang mengakses.

Dampak

Kebocoran Data Pribadi

Apabila ada masyarakat yang terlanjur percaya dan mengeklik tautan yang diberikan oleh *impersonator*, maka kemungkinan pelaku dapat mengakses dan menyalahgunakan data pribadi yang ada pada perangkat milik korbannya.

Penyebaran Malware

Terdapat upaya penyebaran *malware* oleh pelaku melalui tautannya, korban akan seolah-olah diarahkan untuk mengunduh sebuah contoh *file* yang diduga merupakan hasil dari kebocoran data.

Kegaduhan di Ruang Siber

Aktifitas publikasi data tersebut dapat menciptakan keriuhan di ruang siber dan dapat menggiring opini publik bahwa ruang siber tidak aman.

⚠ CAUTION

Pelaku menggunakan teknik ***spear-phishing*** yang merupakan modus kejahatan *online* yang menggabungkan teknik *phishing* dengan modus *social engineering* (rekayasa sosial).

Tips Mitigasi dari BESTI!!

Selalu periksa sumber tautan atau lampiran. Cara untuk mengkonfirmasi keabsahan tautan adalah dengan mengarahkan kursor ke tautan untuk menampilkan alamat lengkap tautan.

Jika terlanjur mengeklik tautan *phising*, jangan memasukkan data apapun. Segera matikan koneksi internet untuk mengurangi risiko penyebaran *malware* ke perangkat jaringan lain.

Lakukan *backup* data secara rutin dan berkala.

Gunakan kanal pelaporan akun tiruan milik influencer yang disediakan platform media sosial.

Lakukan pemeriksaan terhadap jumlah pengikut dan waktu pembuatan akun. Akun resmi biasanya sudah memiliki banyak pengikut dan waktu pembuatan akun yang sudah lama.

Lakukan pemeriksaan keabsahan semua akun dengan nama yang mirip dengan akun resmi dari berbagai media sosial.

Selalu waspada terhadap bentuk ancaman serangan siber termasuk upaya *social engineering*, yang selalu menggunakan cara-cara yang baru dalam mengelabui target.

#TimPBKI

#TimPBKI
SOCIAL CYBER EDUCATION

BESTI
Berita Edukasi Siber Sosial Terkini