Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Penipuan Menyasar Individu

Pengenalan

Penjenayah siber terus mencipta cara yang lebih kreatif untuk menipu. Salah satu jenis penipuan yang sedang meningkat popular adalah penipuan yang menyasarkan individu. Penjenayah mencari atau membeli maklumat berjuta orang di alam maya lalu menggunakan maklumat tersebut untuk menjadikan serangan mereka lebih peribadi. Kami akan menunjukkan bagaimana penipuan ini dilakukan dan memberikan beberapa contoh biasa. Lebih banyak yang anda tahu tentang penipuan ini, semakin mudah untuk menilai dan menghentikannya.

Bagaimana Penipuan Ini Dilakukan?

Penipuan e-mel atau telefon bukanlah baru. Sudah bertahun lamanya penjenayah siber menggunakan cara ini untuk menipu. Contohnya adalah 'Anda Telah Memenangi Loteri' atau penipuan putera raja Nigeria. Bagaimanapun, dalam penipuan tradisional ini penjenayah siber tidak mengetahui siapa yang mereka sasarkan. Mereka hanya menghantar e-mel yang sama kepada berjuta penerima. Oleh kerana e-mel ini kelihatan serupa, ia selalunya mudah dikenali. Penipuan yang menyasarkan individu adalah berbeza, penjenayah siber akan menyelidik dahulu dan mencipta mesej yang sesuai untuk setiap mangsa. Penjenayah siber mendapatkan maklumat mangsa seperti nama, kata laluan, nombor telefon dan lain-lain maklumat dengan mencari atau membelinya. Maklumat ini mudah didapati disebabkan laman-laman sesawang ini pernah digodam. Ia juga mudah didapati daripada laman media sosial dan rekod kerajaan yang boleh dicapai awam. Selepas itu penjenayah hanya perlu menyasarkan semua orang berpandukan maklumat yang mereka ada.

Salah satu cara lazim digunakan penjenayah siber adalah dengan menakut-nakutkan atau mengugut mangsa lalu memaksa mereka memindahkan wang kepada penjenayah. Berikut adalah cara serangan ini dilakukan. Mereka mencari atau membeli maklumat log masuk dan kata laluan yang didapati dari laman yang pernah digodam. Mereka kemudiannya mencari maklumat akaun mangsa di dalam pangkalan data dan menghantar mangsa e-mel yang mengandungi maklumat mangsa, termasuklah kata laluan asal yang digunakan pada laman yang telah digodam tersebut. Penjenayah kemudiannya membuat rujukan kepada kata laluan anda sebagai 'bukti' bahawa mereka telah menggodam komputer atau peranti anda, yang mana ianya tidak benar. Mereka kemudiannya akan membuat dakwaan bahawa terdapat bukti mangsa melayari laman pornografi. E-mel tersebut kemudiannya akan mengugut mangsa untuk menyebarkan bukti perbuatan tidak senonoh ketika berada dalam talian ini kepada keluarga dan rakan-rakan jika mangsa tidak membayar wang pemerasan.

Natijahnya disini, dalam hampir kesemua situasi seperti ini penjenayah siber tersebut tidak pernah menggodam sistem mangsa. Mereka tidak mengenali mangsa atau kegiatan dalam talian anda. Penipu tersebut cuba untuk menggunakan beberapa maklumat

yang mereka peroleh mengenai mangsa dan cuba membuatkan mangsa mempercayai bahawa mereka telah menggodam komputer atau peranti dan memperdaya supaya mangsa membuat pindahan wang. Kaedah ini juga boleh digunakan untuk penipuan telefon.

Apa yang Perlu Anda Lakukan

Ingat bahawa sebarang e-mel atau panggilan telefon seperti ini adalah satu penipuan. Perasaan takut apabila seseorang mempunyai maklumat peribadi anda adalah biasa. Bagaimanapun ingat bahawa penghantar sedang melakukan penipuan. Serangan seperti ini adalah sebahagian daripada serangan automatik berskala besar, bukan suatu serangan yang menyerang anda secara peribadi. Kebelakangan ini amat mudah bagi penjenayah siber untuk mencari atau membeli maklumat peribadi, oleh itu penipuan bersifat peribadi seperti ini akan bertambah. Berikut adalah klu untuk dilihat.

⚠

- **Sentiasa waswas setiap kali anda menerima e-mel, pesanan atau panggilan telefon. Jika seseorang bermain dengan emosi seperti menakut-nakutkan atau menimbulkan rasa cemas, mereka sedang mendesak anda untuk melakukan kesilapan.**
- **Apabila seseorang mendesak bayaran dilakukan dalam bentuk BitCoin, kad hadiah atau cara lain yang tidak dapat dikesan.**
- **Apabila anda menerima e-mel yang mencurigakan, buat carian Google untuk melihat jika ada individu lain yang pernah melaporkan serangan yang serupa.**

Pada dasarnya pertimbangan akal adalah pertahanan terbaik anda. Sungguhpun begitu, kami mengesyorkan anda supaya sentiasa menggunakan kata laluan yang panjang dan unik untuk setiap akaun dalam talian anda. Jika anda tidak mampu untuk menghafal kesemua kata laluan gunakan pengurus kata laluan. Sebagai tambahan, sentiasa bolehkan verifikasi dua-langkah jika ianya tersedia.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Editor Jemputan

Lenny Zeltser *adalah seorang veteran dalam bidang keselamatan siber. Beliau membangunkan penyelesaian untuk anti-perisian hasad dan mengajar di kelas-kelas SANS Institute. Beliau juga berpengalaman dalam menguruskan perkhidmatan keselamatan dan juga perunding. Ikuti beliau di* zeltser.com *dan* @lennyzeltser *di Twitter.*

Sumber

Social Engineering:	https://www.sans.org/u/MUU
Stop That Phish:	https://www.sans.org/u/MUZ
Search Yourself Online:	https://www.sans.org/u/MV4
Password Manager:	https://www.sans.org/u/MV9

OUCH! diterbitkan oleh program SANS Security Awareness dan diedarkan di bawah lesen Creative Commons BY-NC-ND 4.0 license. Kebenaran diberikan untuk mengedarkan surat berita ini atau mengunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal. Untuk edisi lepas atau versi diterjemahkan, lawati www.sans.org/security-awareness/ouch-newsletter. Editor: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie