Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Pengendalian Sosial

Pengenalan

Salah satu tanggapan salah kebanyakan orang terhadap penyerang siber adalah mereka hanya menggunakan alatan dan teknik yang canggih untuk menggodam komputer atau akaun orang lain. Ini sama sekali tidak betul. Penyerang siber mendapati bahawa cara paling mudah untuk mencuri maklumat, menggodam akaun atau menjangkiti sistem adalah dengan memperdayakan anda untuk melakukan kesilapan. Dalam surat berita ini anda akan mempelajari bagaimana serangan yang dipanggil pengendalian sosial ini berfungsi dan apa yang anda boleh lakukan untuk melindungi diri.

Editor Jemputan

James Lyne (@jameslyne) merupakan seorang pengajar bertauliah SANS dan merupakan Ketua Penyelidikan di Sophos. Beliau melakukan kejuruteraan balikan terhadap ciptaan penjenayah siber yang terbaru dan paling canggih. Beliau juga merupakan penulis untuk kelas Metasploit (SEC580) dan Social Engineering (SEC567) di SANS.

Apakah Pengendalian Sosial

Pengendalian sosial adalah serangan psikologi apabila penyerang memperdayakan anda untuk melakukan sesuatu yang tidak patut anda lakukan. Konsep pengendalian sosial bukan baru, ia telah hadir sejak beribu tahun. Untuk memberikan gambaran umum, mereka ini sama seperti penipu (scammers). Apa yang menjadikan penyerang siber ini sangat efektif adalah anda tidak dapat melihat mereka secara fizikal, mereka boleh menjadi apa dan siapa sahaja dengan mudah dan mensasarkan berjuta orang diseluruh dunia, termasuklah anda. Sebagai tambahan, serangan pengendalian sosial boleh melepasi kebanyakan teknologi keselamatan. Cara paling mudah untuk anda fahami bagaimana serangan ini dilakukan dan melindungi diri anda adalah dengan melihat dua contoh sebenar ini.

Anda menerima panggilan telefon dari seseorang yang mengaku dirinya dari syarikat sokongan komputer, ISP anda atau mungkin dari Sokongan Teknikal Microsoft. Pemanggil menerangkan bahawa komputer anda sedang melakukan imbasan ke internet, mereka percaya ianya dijangkiti dan ditugaskan untuk membantu anda membersih komputer anda. Mereka kemudiannya menggunakan beberapa variasi terma teknikal dan membawa anda kepada langkah-langkah yang mengelirukan dan meyakinkan anda bahawa komputer anda telah dijangkiti. Sebagai contoh, mereka akan meminta anda untuk melihat jika terdapat fail tertentu dan mengajar anda bagaimana untuk mencarinya. Apabila anda menjumpai fail tersebut, pemanggil akan memberi jaminan bahawa fail tersebut telah dijangkiti sedangkan ia hanyalah fail sistem biasa yang terdapat hampir di setiap komputer di seluruh dunia. Setelah berjaya memperdayakan anda untuk percaya bahawa komputer anda dijangkiti, mereka akan memberi tekanan untuk anda membeli perisian sekuriti mereka atau memberikan mereka capaian jarak jauh bagi membolehkan mereka membaikinya. Bagaimanapun, perisian yang mereka jual adalah program

Pengendalian Sosial

hasad. Jika anda membeli dan memasang bukan sahaja mereka berjaya menipu untuk menjangkiti komputer anda, tetapi anda juga membayar mereka untuk melakukannya. Jika anda memberikan mereka capaian jarak jauh kepada komputer, mereka akan mengawalnya, mencuri maklumat anda atau menggunakannya sesuka hati.

Akal adalah pertahanan terbaik anda untuk mengenal pasti dan menghentikan kebanyakan serangan pengendalian sosial.

Satu lagi contoh adalah serangan emel yang dipanggil penipuan CEO (CEO fraud), selalunya berlaku di tempat kerja. Ianya berlaku apabila penyerang siber membuat kajian terhadap organisasi anda di dalam talian dan mengenalpasti nama bos atau rakan sekerja anda. Penyerang kemudiannya menyamar dan mengarang emel sebagai mereka dan menghantarnya kepada anda. Emel tersebut mengarahkan anda melakukan sesuatu dengan terburu-buru, seperti memindahkan wang atau menghantar maklumat sensitif pekerja. Selalunya emel sebegini akan menyatakan ia tindakan yang mustahak dan memerlukan anda melepasi prosedur keselamatan standard.Sebagai contoh mereka mungkin mahu anda menghantar maklumat sensitif ke akaun peribadi @gmail.com. Apa yang menjadikan serangan yang disasarkan seperti ini bahaya adalah penyerang siber melakukan kajiansebelum melakukannya. Sebagai tambahan, teknologi keselamatan seperti anti-virus atau firewall tidak boleh mengesan atau menghentikan serangan sebegini kerana tiada perisian hasad atau pautan hasad yang digunakan.

Ingat, serangan pengendalian sosial seperti ini tidak terhad kepada panggilan telefon atau emel, ia boleh berlaku di dalam bentuk lain termasuk mesej teks pada telefon, media sosial atau juga secara peribadi. Kuncinya adalah untuk tahu apa yang perlu di cari, anda adalah perlindungan terbaik diri anda.

Mengesan / Menghentikan Serangan Pengendalian Sosial

Mujurlah menghentikan serangan seperti ini lebih mudah dari yang anda sangkakan – lojik akal adalah perindungan terbaik anda. Jika sesuatu tampak curiga atau agak pelik, ia mungkin suatu bentuk serangan. Klu yang paling kerap dan biasa untuk serangan pengendalian sosial termasuk:

- Seseorang menaikkan perasan yang sangat cemas, mereka cuba memperbodohkan anda untuk melakukan kesilapan
- Seseorang meminta maklumat yang mereka tidak punya capaian atau sepatutnya mereka sudah tahu, seperti nombor akaun anda
- Seseorang meminta kata laluan anda.Tiada organisasi sah yang akan meminta kata laluan anda
- Seseorang memaksa anda untuk mengelak atau tidak mengikuti proses atau prosedur keselamatan yang perlu anda patuhi ketika bekerja

Pengendalian Sosial

- Sesuatu yang terlalu bagus untuk dipercayai. Sebagai contoh anda dimaklumkan telah memenangi loteri atau iPad, sedangkan anda tidak pernah memasuki sebarang loteri.
- Anda menerima emel yang pelik dari seorang kawan atau rakan sekerja, yang mengandungi perkataan pelik dan tidak seperti kebiasaan mereka. Penyerang siber mungkin telah menggodam akaun mereka dan sedang mencuba untuk menipu anda. Untuk melindungi diri anda, semak permintaan seperti itu dengan menghubungi rakan anda menggunakan kaedah komunikasi berbeza, seperti menggunakan telefon atau secara peribadi.

Jika anda syak seseorang sedang mencuba untuk menipu anda, jangan berkomunikasi dengannya lagi. Jika serangan tersebut berkaitan dengan kerja, pastikan anda membuat laporan kepada meja bantuan atau pasukan keselamatan maklumat dengan segera. Ingat, akal merupakan pertahanan terbaik anda.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di securingthehuman.sans.org/ouch/archives.

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/.

Sumber

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Fraud:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie

