Waspada terhadap serangan “Kejuruteraan Sosial”

EXPERTS (/EXPERTS)

Waspada terhadap serangan “Kejuruteraan Sosial”

8 May 2020

Sejak kebelakangan ini kita sering mendengar tentang panggilan “tipu daya” atau scammer. Panggilan seperti ini digunakan bagi “mencuri” duit mangsa dengan paksa rela. Dalam bidang komputer serangan seperti ini dinamakan “social engineering” atau kejuruteraan sosial. Serangan secara ini merupakan serangan yang paling "untung" dan merangkumi semua peringkat pengguna. Ia sukar untuk dikesan kerana melibatkan kepercayaan yang mana kepercayaan merupakan lumrah semula jadi manusia.

Setiap serangan siber mempunyai tujuan tertentu dan antara panggilan “tipu daya” ini adalah untuk mengaut keuntungan (kemewahan, terdesak, Robin Hood); dendam atau dengki dan seronok. Namun kebanyakan mereka yang menggunakan serangan kaedah ini untuk mendapatkan keuntungan.

Terdapat empat langkah yang biasa digunakan pihak penyerang bagi menjayakan proses serangan panggilan tipu daya mereka. Langkah pertama adalah mengumpul maklumat. Penyerang akan mengumpul maklumat mangsa melalui pelbagai cara antaranya menggunakan halaman media sosial seperti Facebook, Instagram, WhatsApp, Telegram dan seumpamanya. Keduanya menggunakan laman sesawang syarikat bagi mereka yang bekerja dan ketiga membeli maklumat daripada mereka yang mempunyai maklumat ramai seperti bank, telcos dan organisasi kerajaan. Media yang paling mudah yang digunakan oleh pengodam bagi mendapat maklumat adalah media sosial. Oleh yang demikian dinasihatkan agar kita melihat atau meneliti kembali maklumat yang hendak dikongsi.

Langkah kedua terhadap penggubalan skrip sama ada berbentuk teks untuk serangan melalui Whatsapp atau skrip lisan melalui panggilan telefon. Penggubalan skrip, berdasarkan pengalaman mereka dan senario yang biasa digunakan dalam perbankan dan mahkamah. Skrip berbentuk teks lebih mudah berbanding skrip lisan kerana dengan menggunakan teks mereka akan fokus kepada individu yang mempunyai ikatan sama ada ahli keluarga, kawan rapat dan kenalan yang biasa dihubungi.

Langkah ketiga adalah serangan, iaitu mereka membuat panggilan dengan nada yang cukup menyakinkan dengan mengikut skrip yang telah dihasilkan. Langkah keempat pujukan sama ada dengan ugutan, belas ihsan dan kepercayaan. Ini merupakan langkah penentu sama ada serangan yang dibuat berjaya atau sebaliknya.

Oleh kerana serangan ini merupakan serangan kepercayaan sosial, untuk mengesan serangan ini adalah sangat sukar. Kita perlu mempunyai kemahiran dan pengetahuan untuk mengesan sama ada panggilan yang kita terima adalah panggilan tipu daya atau sebaliknya.

Antara tips yang boleh digunakan untuk mengesan sama ada panggilan itu panggilan tipu daya adalah sekiranya melalui aplikasi WhatsApp (teks), pengguna hendaklah membuat panggilan ke nombor tersebut dan sekiranya tiada maklum balas, maka itu adalah panggilan tipu daya. Selain itu, pengguna boleh membuat panggilan kepada kawan atau ahli keluarga yang mengenali nombor atau orang yang menghubungi kita melalui WhatsApp untuk bertanyakan perkara yang dimaklumkan kepada kita sama ada betul ataupun tipu semata.

Sekiranya menerima panggilan telefon sama ada melalui pihak bank, kebiasaannya skripnya sangat ringkas. Antara kandungan skrip daripada pihak bank…. “Boleh saya bercakap dengan Encik Fatih. Encik Fatih saya dari bank....ingin memaklumkan kepada encik ada tertunggak bayaran hutang kereta, pihak bank mohon encik membuat bayaran sebelum 23 April.” itu sahaja. Pihak bank tidak akan membuat pengesahan yang terperinci sekiranya pihak mereka yang membuat panggilan. Manakala selebihnya pihak bank atau organisasi kewangan berdaftar atau kerajaan akan menghantar surat rasmi berkenaan perkara tersebut.

Sekiranya kita dapat mengesan panggilan adalah panggilan tipu daya, terdapat beberapa tindakan yang boleh kita lakukan iaitu pertama memutuskan panggilan telefon tersebut dengan segera. Keduanya, menyekat nombor panggilan tersebut atau ketiga mendapatkan pengesahan pihak bank atau organisasi yang terlibat. Sekiranya perlu langkah keempat adalah membuat laporan polis. Putuskan panggilan telefon dengan segera merupakan tindakan yang sangat penting bagi

mengelak serangan rantai yang lain berlaku. Antara serangan rantaian yang boleh berlaku adalah pengesanan lokasi dan penanaman program malware yang akan digunakan untuk membuat serangan selanjutnya kepada sistem.

Apa sahaja serangan siber yang wujud di era ini, solusi utama adalah kesedaran pengguna. Penggunaan teknologi seperti anti virus dan rewall hanya memberi perlindungan minimum dalam membantu pengguna alam maya melindungi mereka daripada program malware yang biasa digunakan dalam mengumpul maklumat pengguna.

Disediakan oleh Dr. Noorhuzaimi @Karimah Mohd. Noor yang merupakan pensyarah kanan Fakulti Komputeran. E-mel: nhuzaimi@ump.edu.my (mailto:nhuzaimi@ump.edu.my)

TAGS / KEYWORDS

MALWARE (/malware)

FK (/fk)