Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Hentikan Perisian Hasad

Pengenalan

Anda mungkin pernah mendengar terma seperti virus, Trojan, perisian tebusan atau kit akar apabila bercakap tentang keselamatan siber. Ini adalah program hasad yang berbeza yang dipanggil perisian hasad, yang digunakan oleh penjenayah siber untuk menjangkiti komputer dan peranti. Setelah dipasang, penjenayah siber tersbut boleh melakukan apa yang mereka mahukan. Pelajari apakah itu perisian hasad, bahaya yang dibawa, dan yang paling penting apa yang boleh anda lakukan untuk melindungi diri daripadanya.

Apakah Perisian Hasad?

Dengan kata mudah, perisian hasad adalah perisian—iaitu program komputer—yang digunakan untuk tindakan berniat jahat. Terma ini adalah kombinasi perkataan hasad dan perisian (malicious dan software). Penjenayah siber memasang perisian hasad pada komputer atau peranti anda untuk mengawalnya. Setelah dipasang, perisian hasad tersebut membolehkan penjenayah mengintip aktiviti dalam talian, mencuri kata laluan, atau menggunakan sistem anda untuk menyerang orang lain. Perisian hasad boleh mengawal fail-fail anda dan meminta wang tebusan untuk mendapatkannya semula. Ramai orang percaya bahawa perisian hasad adalah masalah komputer Windows sahaja. Malangnya perisian hasad boleh menjangkiti sebarang peranti, dari komputer Mac dan telefon pintar sehinggalah DVR dan kamera keselamatan. Lagi banyak komputer dan peranti dijangkiti penjenayah siber, bertambah banyak wang yang boleh mereka dapat. Oleh itu semua orang adalah sasaran, termasuklah anda.

Lindungi Diri Anda – Hentikan Perisian Hasad

Anda mungkin berfikir dengan memasang program keselamatan seperti perisian anti-virus anda selamat dari dijangkiti. Malang sekali anti-virus tidak boleh menghentikan semua perisian hasad. Penjenayah siber sentiasa membangunkan perisian hasad canggih yang mampu mengelak dari dikesan. Oleh yang demikian, pembekal anti-virus sentiasa mengemaskini produk mereka dengan keupayaan baru untuk mengesan perisian hasad. Jika dilihat ia seolah-olah perlumbaan senjata, dan orang jahat sentiasa berada satu langkah di hadapan. Memandangkan anda tidak boleh bergantung kepada anti-virus semata-mata, berikut adalah beberapa langkah yang boleh diambil untuk melindungi diri:

Penjenayah siber selalunya menjangkiti komputer atau peranti dengan mengeksploitasi kelemahan di dalam perisian. Semakin terkini perisian, semakin kurang kelemahan yang terdapat dan ini menyukarkan penjenayah siber untuk menjangkitinya. Pastikan sistem operasi, aplikasi, pelayar dan pemalam pelayar, dan peranti senantiasa dikemaskini. Cara paling mudah untuk memastikannya adalah dengan membolehkan kemaskini automatik.

Cara lazim yang digunakan penjenayah siber untuk menjangkiti komputer atau peranti mudah alih adalah dengan mencipta program atau aplikasi mudah alih palsu, memuat naik ke internet, dan memperdaya anda untuk memuat turun dan memasangnya. Hanya muat turun dan pasang program atau aplikasi dari kedai dalam talian yang dipercayai. Jauhi dari aplikasi mudah alih yang baru, mempunyai ulasan positif yang sedikit, jarang di kemaskini atau muat turun yang sedikit. Jika tidak lagi menggunakan program komputer atau aplikasi mudah alih padamkannya.

Penjenayah siber selalunya menggunakan muslihat supaya pengguna memasang perisian hasad untuk mereka. Sebagai contoh mereka mungkin menghantar suatu e-mel yang tampak sah dan mempunyai lampiran atau pautan. E-mel tersebut mungkin nampak seperti dihantar oleh bank atau rakan. Walaubagaimanapun jika fail tersebut dibuka atau klik pada pautan tersebut, kod hasad akan dipasang pada sistem anda. Jika mesej tersebut tampak seperti memerlukan tindakan yang segera, atau terlalu bagus untuk dipercayai, ia mungkin adalah suatu serangan. Sentiasa curiga, pertahanan terbaik adalah menggunakan akal.

Sandarkan sistem dan fail anda dengan kerap ke perkhidmatan berasaskan awan atau simpan sandaran anda secara luar talian seperti pemacu luaran yang tidak berhubung. Ini melindungi sandaran sekiranya terdapat cubaan perisian hasad untuk menyulitkan atau memadamnya. Sandaran adalah kritikal, ia mungkin satu-satunya cara untuk pulih dari serangan jangkitan perisian hasad.

Akhir sekali, cara terbaik untuk melindungi diri dari perisian hasad adalah dengan memastikan semua perisian dan peranti anda dikemaskini, pasang perisian anti-virus yang dipercayai dan berjaga-jaga dengan muslihat untuk memperdayakan dari menjangkiti sistem anda sendiri. Jika semua ini gagal, sandaran yang kerap adalah satu-satunya cara untuk memulihkan.

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 *memerangi perisian hasad dengan mencipta produk keselamatan titik akhir di Minerva Labs dan mengajar di SANS Institute. Lenny aktif di Twitter dengan @lennyzeltser dan menulis blog keselamatan di zeltser.com.*

Sumber

Perisian Hasad:	https://www.sans.org/u/EdI
Sandaran:	https://www.sans.org/u/EdN
Hentikan Pancing Data:	https://www.sans.org/u/EdS