Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Perisian Tebusan

Apa itu Perisian Tebusan?

Perisian tebusan adalah sejenis perisian hasad khas yang aktif disebarkan melalui Internet pada masa kini di mana ia digunakan untuk mengancam mangsa dengan memusnahkan dokumen dan fail yang telah dijangkiti. Perisian hasad adalah sejenis perisian komputer yang digunakan untuk melakukan tindakan yang berniat jahat. Walaupun perisian tebusan hanyalah salah satu daripada pelbagai jenis perisian hasad, ia telah menjadi sesuatu yang biasa digunakan kerana ia sangat mendatangkan keuntungan kepada penjenayah. Apabila perisian tebusan menjangkiti komputer anda, ia menyulitkan fail tertentu atau mungkin keseluruhan cakera keras anda. Anda kemudiannya akan dikunci keluar daripada keseluruhan sistem atau tidak boleh mengakses fail-fail penting seperti dokumen atau gambar anda. Perisian hasad tersebut kemudiannya memberitahu bahawa satu-satunya cara untuk menyahsulit fail dan memulihkan sistem anda adalah dengan membayar wang tebusan kepada penjenayah siber tersebut. Kebiasaannya, wang tebusan perlu dibayar dalam bentuk wang digital seperti Bitcoin. Perisian tebusan disebarkan seperti perisian hasad yang lain. Kaedah yang paling biasa digunakan adalah dengan menghantar e-mel berniat jahat kepada mangsa di mana penjenayah siber menipu anda untuk membuka lampiran yang dijangkiti atau mengklik pada pautan yang akan membawa anda ke laman sesawang penyerang tersebut.

Editor Jemputan

Lenny Zeltser berfokus kepada memelihara operasi IT di NCR Corp dan mengajar memerangi perisian hasad di SANS Insitute. Lenny aktif di Twitter sebagai **@lennyzeltser** dan menulis blog keselamatan di **zeltser.com**.

Adakah Anda Perlu Membayar Wang Tebusan?

Itu adalah sesuatu yang sukar. Masalahnya adalah apabila lebih kerap mangsa membayar penjenayah setelah dijangkiti, penjenayah akan lebih bermotivasi untuk menjangkiti orang lain. Lagipun, anda mungkin tidak mempunyai pilihan lain untuk mendapatkan semula fail anda. Sebagai amaran, walaupun anda membayar wang tebusan, tidak ada jaminan anda akan mendapat semula fail anda kembali. Anda berurusan dengan penjenayah, dan mereka mungkin tidak boleh menyahsulit fail, atau mereka mungkin memberikan anda kaedah penyahsulitan sebagai pertukaran untuk pembayaran,sesuatu yang buruk mungkin terjadi semasa proses penyahsulitan atau komputer anda mungkin dijangkiti perisian hasad yang lain.

Sandaran Fail Anda

Mungkin cara terbaik untuk pulih daripada jangkitan perisian tebusan dan tidak membayar wang tebusan adalah dengan memulihkan fail anda dari sandaran. Dengan cara ini, walaupun anda dijangkiti perisian tebusan, anda mempunyai kaedah untuk memulihkan semula fail selepas membina semula atau membersihkan komputer anda. Perlu diingat bahawa jika

Perisian Tebusan

sandaran boleh di akses daripada sistem yang dijangkiti, perisian tebusan berkeupayaan untuk memadam atau menyulitkan fail sandaran. Oleh itu, adalah penting untuk membuat sandaran menggunakan perkhidmatan berasaskan awan yang bereputasi atau menyimpan sandaran ke dalam pemacu luaran yang jarang disambungkan ke sistem anda. Di samping itu, satu kesilapan yang sering diulang semasa membuat sandaran adalah dengan menganggap bahawa ia berfungsi tanpa menguji sama ada mereka benar-benar boleh mendapatkan semula fail. Pastikan anda kerap menguji sandaran dan mengesahkan bahawa anda boleh mendapatkan semula fail yang anda perlukan sekiranya sistem dijangkiti dengan perisian tebusan. Sandaran adalah penting kerana ia juga membantu anda memulihkan semula apabila anda secara tidak sengaja memadam fail atau cakera keras anda rosak.

Perisian tebusan adalah perisian hasad di mana apabila ia menjangkiti komputer anda, ia akan menyulit semua fail pada komputer anda dan menafikan akses anda ke atas komputer tersebut.

Langkah-langkah Perlindungan Lanjut

Anda boleh melindungi diri anda daripada jangkitan perisian tebusan dengan menggunakan cara yang sama digunakan ke atas perisian hasad yang lain.. Mulakan dengan memastikan anda mempunyai perisian anti-virus terkini daripada vendor yang dipercayai. Peralatan tersebut, di mana ia kadang-kadang dipanggil perisian anti-hasad, direka untuk mengesan dan menyekat perisian hasad. Bagaimanapun, anti-virus tidak boleh menghalang atau menghapuskan semua perisian berniat jahat. Penjenayah siber sentiasa membuat pembaharuan, membangunkan perisian hasad yang lebih baru dan canggih yang mampu mengelak daripada dikesan. Sebaliknya, vendor anti-virus sentiasa mengemas kini produk mereka dengan keupayaan terkini untuk mengesan perisian hasad. Dalam erti kata lain, ia telah menjadi satu perlumbaan di mana kedua-dua pihak cuba untuk mengakali satu sama lain. Malangnya, orang berniat jahat sentiasa berada satu langkah di hadapan. Itulah sebabnya anda perlu memastikan sandaran fail sentiasa dibuat dan ambil langkah-langkah tambahan berikutnya untuk melindungi diri anda:

- Penjenayah siber sering menjangkiti komputer atau peranti dengan mengeksploitasi kerentanan pada perisian anda. Lebih terkini perisian anda, lebih kurang kerentanan pada sistem anda yang diketahui dan semakin sukar untuk penjenayah siber menjangkiti sistem tersebut. Oleh itu, pastikan sistem operasi, aplikasi dan peranti boleh sentiasa dikemas kini dengan membenarkan fungsi automatik.
- Pada komputer anda, gunakan akaun standard yang mempunyai keistimewaan terhad daripada menggunakan akaun ‘pentadbir’ atau ‘akar’. Ini memberikan perlindungan tambahan dengan menghalang pelbagai jenis perisian hasad daripada dapat memasang diri sendiri ke dalam sistem.
- Penjenayah siber sering menipu orang ramai untuk memasang perisian hasad. Sebagai contoh, mereka mungkin

Perisian Tebusan

menghantar e-mel yang kelihatan sah dan mengandungi lampiran atau pautan. Berkemungkinan e-mel yang dihantar datang daripada bank atau rakan anda. Walaubagaimanapun, sekiranya anda ingin membuka fail yang dilampirkan atau klik pada pautan, anda akan mengaktifkan kod berniat jahat yang akan memasang diri sendiri ke dalam sistem anda. Jika mesej tersebut bermaksud terlalu mendesak, mengelirukan, terlalu bagus untuk dipercayai, atau mempunyai kesalahan tatabahasa, ia berkemungkinan adalah serangan. Sentiasa curiga, logik akal sering menjadi pertahanan anda yang terbaik.

Lindungi diri anda daripada perisian hasad dengan kekal berhati-hati apabila membuka lampiran e-mel atau mengklik pada pautan, pastikan anda sentiasa mengemas kini perisian anti-virus dan mengesahkan fail anda sentiasa disandarkan dan boleh dipulihkan.

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

Social Engineering: https://securingthehuman.sans.org//ouch/2015#december2015

Apa Itu Perisian Hasad: https://securingthehuman.sans.org/ouch/2016#march2016

Penyulitan: https://securingthehuman.sans.org/ouch/2016#june2016

Sandaran: https://securingthehuman.sans.org/ouch/2015#august2015

Artikel Microsoft: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

SANS FOR610 Course - Reverse Engineering Malware: https://sans.org/for610

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