Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

- Apakah itu Perisian Hasad?
- Siapakah yang Mencipta Perisian Hasad?
- Melindungi Diri Anda

Apakah itu Perisian Hasad?

Pengenalan

Anda mungkin pernah mendengar nama seperti virus, trojan, perisian tebusan atau rootkit apabila mendengar orang berbincang tentang keselamatan. Kesemua perkataan ini menerangkan perkara yang sama -jenis program yang digunakan penjenayah untuk menjangkiti komputer dan peranti. Nama yang biasa digunakan untuk menerangkan kesemua program yang berlainan ini adalah perisian hasad. Dalam surat berita ini kami akan menerangkan apakah itu perisian hasad, siapa yang menciptanya, dan yang paling penting apa yang anda boleh lakukan untuk melindungi diri anda daripadanya.

Editor Jemputan

Lenny Zeltser memberikan fokus kepada memelihara operasi IT pelanggan di NCR Corp dan mengajar memerangi perisian hasad di SANS Institute. Lenny aktif di Twitter sebagai **@lennyzeltser** dan menulis satu blog keselamatan di **zeltser.com**.

Apakah itu Perisian Hasad?

Dengan kata mudah, perisian hasad adalah satu perisian yang digunakan untuk melakukan tindakan yang berniat jahat. Malah, terma perisian hasad (malware) merupakan kombinasi dua perkataan iaitu perisian dan hasad (malicious software). Penjenayah siber memasang perisian hasad pada komputer atau peranti anda untuk mendapatkan kawalan ke atasnya atau mendapatkan capaian kepada kandungannya. Setelah dipasang, penyerang boleh menggunakan perisian hasad untuk mengintip aktiviti dalam talian anda, mencuri kata laluan atau fail, atau menggunakan sistem anda untuk menyerang sistem yang lain. Perisian hasad boleh menafikan akses kepada fail anda sendiri, dan menuntut anda menjelaskan tebusan untuk mendapatkan semula kawalan.

Banyak orang beranggapan bahawa perisian hasad adalah masalah untuk komputer Windows sahaja. Walaupun Windows banyak digunakan, dan menjadi sasaran yang besar, perisian hasad boleh menjangkiti sebarang peranti, termasuklah komputer Mac, telefon pintar, atau tablet. Semakin banyak komputer dan peranti yang dijangkiti penjenayah siber, semakin banyak wang yang mereka boleh peroleh. Oleh itu, semua orang merupakan sasaran, termasuklah anda.

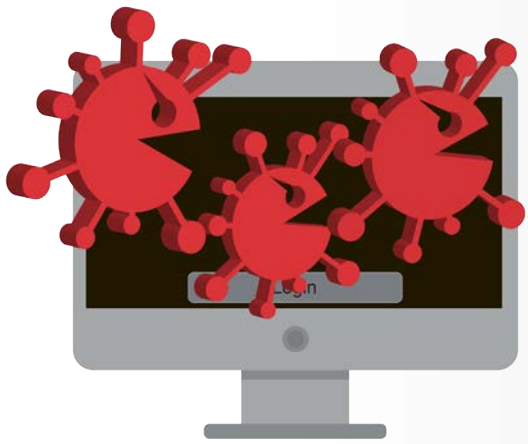
Siapa yang Mencipta Perisian Hasad?

Perisian hasad bukan lagi dicipta oleh penggemar yang ingin tahu atau penggodam amatur, tetapi oleh penjenayah siber yang canggih. Tujuan mereka adalah untuk mendapatkan wang dari komputer atau peranti anda yang telah dijangkiti, mungkin dengan menjual maklumat yang mereka curi dari anda, menghantar e-mel penipuan, melancarkan serangan penafian perkhidmatan, atau melakukan peras ugut. Mereka yang mencipta, mengedarkan dan mendapat manfaat dari perisian hasad boleh terdiri dari individu yang melakukan dengan sendiri kepada kumpulan penjenayah yang diatur dengan baik

© SANS Institute 2016

Apakah itu Perisian Hasad?

ataupun organisasi kerajaan. Mereka yang mencipta perisian hasad canggih hari ini selalunya melakukannya khusus untuk tujuan tersebut, membangunkan perisian hasad sebagai pekerjaan tetap mereka. Sebagai tambahan, setelah mereka membangunkan perisian hasad tersebut, mereka akan menjualnya kepada individu atau organisasi lain, bahkan membekalkan pelanggan mereka dengan kemas kini dankhidmat sokongan .



Lindungi diri anda dari perisian hasad dengan meragui pesanan yang mencurigakan, memastikan peranti anda di kemas kini dan mempunyai anti-virus terkini jika boleh.

Melindungi Diri Anda

Langkah biasa untuk melindungi diri anda adalah dengan memasang perisian anti-virus dari pembekal yang dipercayai. Kadang-kala ia dipanggil perisian anti-perisian hasad (anti malware), di bangunkan untuk mengesan dan menghentikan perisian hasad. Walau bagaimanapun, anti-virus tidak dapat menahan atau memadam kesemua program hasad. Penjenayah siber sentiasa berinovatif membangunkan perisian hasad baru yang lebih canggih yang berupaya mengelak dari dikesan. Dengan itu, pembekal anti-virus sentiasa mengemas kini produk mereka dengan keupayaan baru untuk mengesan perisian hasad. Dari pelbagai segi ianya menjadi perlumbaan persenjataan, dengan kedua-dua belah pihak cuba untuk mengakali satu sama lain. Malangnya penjahat selalunya berada satu langkah ke hadapan. Memandangkan anda tidak boleh bergantung kepada anti-virus sahaja, berikut merupakan langkah tambahan yang perlu anda ambil untuk melindungi diri anda:

- Penjenayah siber selalunya menjangkiti komputer atau peranti dengan mengeksploitasi kelemahan dalam perisian mereka. Semakin terkini perisian anda, semakin kurang kelemahan sistem anda dan menjadikannya sukar untuk penjenayah untuk menjangkitinya. Oleh itu, pastikan anda membolehkan pemasangan kemas kini secara automatik pada sistem operasi, aplikasi dan peranti anda.
- Cara biasa bagi penjenayah siber menjangkiti peranti mudah alih adalah dengan mencipta aplikasi mudah alih palsu dan meletakkannya di internet dan menggunakan helah supaya orang memuat turun dan memasangnya. Oleh itu, hanya muat turun dan pasang aplikasi dari kedai dalam talian yang dipercayai. Sebagai tambahan, hanya pasang aplikasi mudah alih yang telah lama dalam talian, telah di muat turun oleh ramai orang, dan ulasan positif yang banyak.
- Untuk komputer, gunakan akaun yang mempunyai keistimewaan terhad daripada akaun yang mempunyai keistimewaan seperti 'Administrator' atau 'root'. Ini memberikan perlindungan tambahan dengan menghalang pelbagai jenis perisian hasad dari terpasang dengan sendiri.
- Penjenayah siber sering memperdayakan orang untuk memasang perisian hasad untuk mereka. Sebagai contoh mereka mungkin menghantar e-mel yang tampak tulen dan mempunyai pautan atau lampiran. E-mel tersebut mungkin nampak dari bank atau rakan anda. Walaubagaimanapun, jika anda membuka lampiran tersebut atau klik

Apakah itu Perisian Hasad?

pada pautan tersebut, anda akan mengaktifkan kod hasad tersebut dan memasang perisian hasad ke dalam sistem anda. Jika pesanan tersebut menimbulkan perasaan yang mendesak, mengelirukan atau tampak terlalu bagus untuk dipercayai, ia berkemungkinan suatu bentuk serangan. Sentiasa curiga, logik akal merupakan pertahanan yang terbaik.

- Sandarkan sistem dan fail anda kepada perkhidmatan awan dengan kerap, atau simpan sandaran anda secara luar talian seperti pemacu luaran yang tidak disambungkan. Ini dapat melindungi sandaran anda sekiranya perisian hasad cuba untuk menyulitkan atau memadamnya. Sandaran adalah kritikal, ia selalunya merupakan satu-satunya cara anda dapat pulih semula dari jangkitan perisian hasad.

Akhir sekali, langkah paling mudah untuk melindungi dari perisian hasad adalah dengan memastikan perisian anda terkini, pasang perisian anti-virus dari pembekal yang dipercayai dan sentiasa waspada kepada sebarang percubaan untuk menipu atau memperdayakan anda untuk menjangkiti sistem 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 http://www.securingthehuman.org.

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
Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Securely Using Mobile Apps:	https://securingthehuman.sans.org/ouch/2015#january2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

OUCH! diterbitkan oleh program SANS “Securing The Human” dan diedarkan di bawah lesen Creative Commons BY-NC-ND 4.0. Kebenaran diberikan untuk mengedarkan surat berita ini atau mengunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus