OUCH! | Februari 2014

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Apa Itu Malware

Pengenalan

Anda mungkin pernah mendengar terma seperti virus, cecacing (worm), trojan horse atau rootkit apabila berbincang tentang keselamatan siber. Terma-terma ini menerangkan program yang digunakan oleh penjenayah siber untuk menjangkiti dan mengambil alih komputer dan peranti mudah alih. Kini kesemua terma yang berbeza ini dikenali sebagai malware. Dalam isu kali ini kami akan menerangkan apa itu malware, siapa yang membangunkannya dan mengapa dan apa yang anda boleh lakukan untuk melindungi diri anda daripadanya.

Editor Jemputan

Pengkhususan Lenny Zeltser adalah menjaga operasi IT pelanggan di NCR Corp dan mengajar cara memerangi malware di SANS Institute. Lenny aktif di Twitter sebagai **@lennyzeltser** dan menulis blog mengenai keselamatan di **blog.zeltser.com**.

Apa Itu Malware

Malware adalah perisian, program komputer yang digunakan untuk melakukan perbuatan yang berniat jahat. Malahan terma malware adalah kombinasi perkataan malicious dan software. Matlamat utama kebanyakan penjenayah siber adalah untuk memasang malware ke dalam komputer atau peranti mudah alih anda. Setelah di pasang, penyerang berpotensi untuk mendapatkan mengawal penuh peranti tersebut. Ramai yang beranggapan bahawa malware adalah masalah yang dihadapi oleh komputer Windows sahaja. Walaupun Windows banyak digunakan dan sering menjadi sasaran utama, malware boleh menjangkiti sebarang peranti berkomputer termasuk telefon pintar dan tablet. Pada hakikatnya, kekerapan malware menjangkiti peranti mudah alih kini semakin meningkat. Sebagai tambahan, perlu diingat bahawa semua orang adalah sasaran, termasuklah anda. Semakin banyak komputer dan peranti mudah alih yang dijangkiti penjenayah siber semakin banyak wang yang boleh mereka jana. Penjenayah selalunya tidak peduli siapa yang mereka jangkiti asalkan mereka dapat menjangkiti seramai mungkin.

Siapa dan Mengapa

Malware bukan lagi dicipta sebagai hobi atau dicipta oleh penggodam amatur tetapi oleh penjenayah siber yang canggih untuk membantu mereka mencapai matlamat tertentu. Matlamat ini termasuklah mencuri maklumat rahsia, menuai kata nama dan kata laluan, menghantar e-mel penipuan, melancarkan serangan penafian servis, memeras ugut atau mencuri identiti. Sebagai contoh, malware yang dikenali sebagai cryptolocker digunakan oleh penjenayah siber untuk menjangkiti dan mengenkripsi semua fail di dalam komputer anda. Setelah dijangkiti dan dienkripsi, penjenayah siber ini kemudiannya menuntut wang tebusan sebagai pertukaran untuk nyah enkripsi fail-fail anda.

Apa Itu Malware

Mereka yang mencipta, menyebarkan dan mendapat faedah daripada malware ini terdiri daripada individu yang bertindak bersendirian, kumpulan jenayah terancang atau organisasi kerajaan. Orang yang mencipta malware sofistikated ini selalunya berdedikasi dalam usaha tersebut dan membangunkan malware adalah pekerjaan sepenuh masa bagi mereka. Malahan, setelah mereka membangunkan malware, mereka sering menjualnya kepada individu atau organisasi dan kerap menyediakan updates dan khidmat sokongan kepada "pelanggan" mereka. Setelah membelinya, penjenayah lain pula membuat keuntungan dengan memasang malware tersebut pada jutaan sistem milik mangsa tanpa sedar, menjadikan ia satu sistem botnet yang dijangkiti. Botnet ini menjadi tentera yang dikawal dari jauh yang kemudiannya boleh digunakan oleh penjenayah siber untuk tujuan tersendiri atau menjual komputer yang dijangkiti kepada penjenayah siber yang lain.

Cara terbaik melindungi diri anda dan menentang malware adalah dengan memastikan peranti anda dikemas kini, mempunyai anti-virus yang terkini, dan akhirnya sentiasa berwaspada dengan serangan.

Melindungi Diri Anda

Langkah lazim untuk menjaga komputer dan peranti mudah alih daripada malware adalah dengan memasang perisian anti-virus daripada pembekal yang dipercayai. Anti-virus, kadang kala dipanggil anti-malware, adalah perisian keselamatan yang direka untuk mengesan dan menghentikan perisian yang berniat jahat. Walaubagaimanapun, anti-virus tidak boleh menyekat atau menghapuskan kesemua malware. Penyerang siber sentiasa membuat pembaharuan, membangunkan serangan yang lebih canggih dan baharu yang boleh menembusi program anti-virus. Sebaliknya pula, pembekal anti-virus sentiasa mengemas kini produk mereka dengan keupayaan baharu untuk mengesan malware baru. Secara tidak sengaja ini telah menjadi perlumbaan senjata dengan kedua-dua pihak cuba untuk menjadi lebih ke hadapan daripada pihak lawan. Malangnya, penjenayah siber hampir pasti mempunyai kelebihan. Dengan itu, sentiasa ingat bahawa anti-virus boleh mengesan dan menyekat kebanyakan malware, tetapi penyerang sentiasa mencipta versi baru yang akan terlepas. Akibatnya anda tidak boleh hanya bergantung kepada anti-virus untuk melindungi anda, anda perlu mengambil langkah tambahan untuk menjaga diri anda.

Pertama, pastikan sistem operasi anda dan aplikasi ditetapkan supaya kemas kini keselamatan dipasang secara automatik. Perisian terkini menyukarkan penjenayah siber untuk menjangkiti komputer atau peranti mudah alih anda.

Kedua, ingat bahawa andalah pertahanan yang terbaik untuk menentang malware. Jangkitan malware selalunya melibatkan kejuruteraan sosial di mana penyerang memperdaya atau mempermainkan anda untuk memasang malware untuk mereka. Salah satu contoh mudah ialah serangan phishing, ini adalah e-mel kelihatan sah tetapi sebenarnya ia palsu dan direka untuk memperdaya anda untuk menjangkiti komputer anda sendiri. Contohnya,

Apa Itu Malware

penjenayah siber mungkin menghantar e-mel dan menyamar sebagai bank anda dan meminta anda untuk klik pada satu pautan. Jika anda klik pada pautan tersebut anda akan dibawa ke satu laman sesawang yang membuat cubaan untuk menggodam dan menjangkiti komputer anda. Atau, mungkin mereka akan menghantar e-mel mengenai notis bungkusan yang tidak dapat dihantar dan meminta anda untuk membuka dokumen yang mengandungi maklumat untuk mengesan dan apabila dibuka komputer anda akan dijangkiti. Serangan kejuruteraan sosial juga berlaku merentasi teknologi lain seperti telefon. Sebagai contoh, penggodam mungkin menelefon anda dan menyamar menjadi sokongan teknikal Microsoft dan memaklumkan komputer anda telah dijangkiti. Maklumat yang disampaikan adalah satu penipuan, komputer anda berkemungkinan besar tiada masalah. Matlamat mereka adalah untuk memperbodohkan anda untuk percaya bahawa komputer anda telah dijangkiti, dan memperdaya anda supaya membenarkan capaian jarak jauh, atau membeli perisian keselamatan mereka yang mana ianya adalah malware. Gunakan logik. Jika sesuatu panggilan telefon atau pesanan kelihatan ganjil, mencurigakan atau terlalu bagus untuk dipercayai, berkemungkinan ianya suatu penipuan.

Akhirnya, antara cara terbaik untuk menentang malware adalah dengan memastikan perisian anda sentiasa dikemas kini, memasang anti-virus daripada pembekal yang dipercayai, ternama dan sentiasa berwaspada terhadap sesiapa yang cuba untuk menipu atau memperdayakan anda untuk menjangkiti komputer 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

OUCH Phishing:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
OUCH Securing Your Computer:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
You Are The Target Poster:
http://www.securingthehuman.org/resources/posters

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