OUCH! | April 2016

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Saya Digodam, Apa yang Harus Saya Lakukan?

Pengenalan

Kami tahu anda ambil berat untuk menjaga komputer dan peranti mudah alih anda dan mengambil langkah-langkah untuk menjaganya. Walau bagaimanapun, seselamat mana pun anda menggunakan teknologi, lambat-laun pasti anda akan digodam. Dalam surat berita ini anda akan belajar bagaimana mengenal pasti sama ada komputer atau peranti mudah alih anda telah digodam dan apa yang boleh anda lakukan jika ianya berlaku apa yang boleh anda lakukan. Selalunya, lagi cepat anda mengesan sesuatu yang tidak kena dan lebih cepat anda bertindak, lebih tinggi peluang untuk anda kurang kesan dari serangan tersebut.

Editor Jemputan

Samantha Davison (**@sam_e_davison**) merupakan Pengurus Program Pendidikan dan Kesedaran Keselamatan di Uber mendidik pekerja mereka di lebih 350 bandar di seluruh dunia.

Petunjuk Anda Telah Digodam

Ianya agak sukar untuk mengenal pasti jika anda telah digodam kerana selalunya tiada cara yang mudah untuk anda mengetahuinya. Sebaliknya penggodam meninggalkan beberapa petunjuk, biasanya dipanggil penunjuk. Semakin hampir sistem anda menyamai petunjuk ini, semakin besar kemungkinan anda telah digodam.

- Program antivirus anda telah memaparkan amaran bahawa sistem anda telah dijangkiti, terutama jika tertera ia tidak dapat membuang atau kuarantin fail yang terjejas.
- Laman utama pelayar anda bertukar dengan sendiri atau pelayar anda membawa anda kepada laman sesawang yang anda tidak mahu pergi.
- Terdapat akaun baru yang bukan anda cipta di dalam komputer atau peranti anda, atau program yang bukan anda pasang tetapi berjalan.
- Komputer atau aplikasi anda sentiasa terpadam “(crash)”, terdapat ikon untuk aplikasi yang tidak diketahui atau terdapat menu pop timbul pelik yang sering keluar.
- Program yang meminta kebenaran anda untuk membuat perubahan kepada sistem anda, sedangkan anda tidak membuat sebarang kemas kini atau memasang sebarang aplikasi.
- Kata laluan anda tidak lagi boleh digunakan apabila anda mahu log masuk ke dalam sistem atau akaun dalam talian anda, walaupun anda tahu kata laluan anda adalah betul.
- Rakan-rakan yang bertanya mengapa anda menghantar e-mel penipuan sedangkan anda tidak pernah menghantarnya.
- Peranti mudah alih anda dicas dengan kadar premium untuk penghantaran SMS.

Saya Digodam, Apa yang Harus Saya Lakukan?

- Peranti mudah alih anda dengan tiba-tiba mempunyai penggunaan data atau bateri yang tinggi.

Lambat laun komputer atau peranti anda mungkin akan digodam, lebih cepat anda mengesan sesuatu kejadian dan lebih cepat anda membuat sesuatu, lebih baik.

Bagaimana untuk Bertindak-balas

Jika anda percaya bahawa komputer atau peranti anda telah digodam, lebih cepat anda bertindak, lebih baik. Jika komputer atau peranti anda dibekalkan oleh majikan atau digunakan untuk kegunaan kerja, jangan cuba untuk betulkan dengan sendiri masalah tersebut. Bukan sahaja anda boleh melakukan lebih kerosakan dari kebaikan, tetapi anda boleh merosakkan bukti yang bernilai yang boleh digunakan untuk siasatan. Sebaliknya laporkan kejadian tersebut kepada majikan anda denganseberapa pantas, selalunya dengan menghubungi meja bantuan, pasukan sekuriti atau penyelia. Jika anda tidak dapat menghubungi organisasi anda, atau anda takut ianya akan memakan masa, putuskan komputer atau peranti anda dari rangkaian dan tukarkan mod kepada tidur “(sleep)”, tangguh “(suspend)” atau kapal terbang “(airplane)”. Walaupun anda tidak pasti anda telah digodam, adalahianya lebih baik untuk melaporkan sekarang sebagai langkah berjaga-jaga. Jika komputer atau peranti adalah untuk kegunaan sendiri, ini merupakan beberapa langkah yang boleh anda ambil.

- **Tukar Kata Laluan Anda**. Ini termasuklah menukar kata laluan bukan sahaja komputer dan peranti mudah alih anda, tetapi untuk semua akaun dalam talian anda. Pastikan anda tidak menggunakan komputer yang telah digodam untuk menukar kata laluan anda. sebaliknya gunakan komputer atau peranti yang anda pasti ianya selamat untuk menukar kata laluan anda.
- **Anti-virus**. Jika perisian anti-virus anda memberitahu fail yang dijangkiti, anda boleh ikut langkah yang dicadangkan. Ini termasuklah dengan kuarantin fail tersebut, membersihkan fail atau memadam fail yang dijangkititersebut. Kebanyakan perisian anti-virus mempunyai pautan yang boleh anda ikuti untuk mengetahui dengan lebih lanjut tentang jangkitan tersebut. Jika anda ragu-ragu, kuarantinkan fail yang terlibat tersebut. Jika pilihan initersebut tidak ada, padam sahaja fail tersebut.
- **Bina Semula**. Jika anda tidak berjaya membaiki jangkitan atau anda mahu pastikan sistem anda berjaya dibaiki, pilihan yang lebih selamat adalah membinanya semula. Untuk komputer, ikut arahan pengeluar sistem anda. Selalunya ini bermakna menggunakan utiliti terbina dalam untuk memasang semula sistem operasi. Jika utiliti ini hilang, rosak atau dijangkiti, hubungi pengeluar anda untuk bantuan atau kunjungi laman sesawang mereka. Jangan memasang semula sistem operasi dari sandaran, ianya berkemungkinan mempunyai kelemahan keterdedahan yang membolehenarkan penggodam masuk pada awalnyaasalnya. Sandaran hanya digunakan untuk mengembalikan maklumat anda. Untuk peranti mudah alih ikuti arahan dari pengeluar atau penyedia perkhidmatan, sepatutnya ia

Saya Digodam, Apa yang Harus Saya Lakukan?

terdapat dalam laman sesawang mereka. Selalunya ianya semudah mengembalikan peranti mudah alih anda kepada tetapan kilang. Jika anda tidak selesa dengan proses bina semula tersebut, pertimbangkan untuk menggunakan khidmat pakar untuk melakukannya. Jika komputer atau peranti anda telah lama, ianya mungkin lebih mudah dan murah untuk membeli yang baru. Akhir sekali, apabila anda membina semula komputer atau peranti anda, atau membeli yang baru, pastikan anda mengemas kini dan membenarkan kemas kini automatik jika boleh.

- **Sandaran**. Antara langkah penting yang boleh anda ambil untuk melindungi diri anda adalah dengan bersedia lebih awal dengan sandaran yang kerap. Lebih kerap anda buat sandaran lebih baik. Sesetengah produk akan membuat sandaran untuk fail baru atau perubahan setiap sejam. Tidak kira pilihan sandaran mana yang anda pilih semak secara berkala jika anda boleh memulihkan semula fail-fail tersebut. Sering kali Mmendapatkan maklumat anda semula dari sandaran sering kali merupakan cara terakhir untuk anda pulih selepas digodam.
- **Penguat Kuasa Undang-undang**. Jika anda berasa terancam, lapur kejadian tersebut kepada penguat kuasa undang-undang tempatan.

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

Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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