Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- Pengenalan
- Tanda-tanda Sistem telah Dikompromi
- Cara Bertindak

Digodam, Apa Perlu Saya Lakukan?

Pengenalan

Kami tahu anda mengambil berat mengenai perlindungan komputer, maklumat yang ada di dalamnya dan telahpun mengambil langkah-langkah untuk melindungi kedua-duanya. Namun seperti memandu kereta, walaupun anda pemandu yang berhemah, kita tidak dapat menjangka apa yang boleh berlaku kelak. Dalam isu kali ini kami akan mengajar cara-cara untuk mengetahui sama ada komputer anda telah digodam, dan jika benar, apa yang anda boleh lakukan seterusnya. Pada dasarnya, kepantasan anda mengenal pasti sama ada komputer anda telah digodam dan bertindak terhadapnya, kemudaratan kepada anda mahupun organisasi anda akan mampu ditangani dengan lebih baik.

Editor Jemputan

Jake Williams (@MalwareJake; malwarejake.blogspot.com) merupakan Ketua Saintis di CSRgroup Computer Security Consultants. Beliau juga merupakan penulis bersama untuk kursus Memory Forensics (FOR526) and Malware Reverse Engineering (FOR610) di SANS.

Tanda-tanda sistem telah dikompomi

Pertama, anda mesti faham bahawa dalam kebanyakan kes, tiada langkah mudah yang boleh diambil untuk menentukan komputer anda telah digodam. Sebaliknya, ada beberapa petunjuk yang boleh membantu. Jika anda dapat mengenal pasti salah satu daripada kombinasi berikut, ianya bermakna komputer anda telah digodam. Berikut adalah beberapa contoh:

- Program anti virus anda memberi amaran bahawa komputer anda telah dijangkiti, terutamanya jika ia memaparkan mesej tidak boleh memadam atau mengasingkan fail yang telah dijangkiti.
- Laman utama pelayar anda bertukar secara tiba-tiba atau pelayar anda membawa anda ke laman sesawang yang tidak diminta.
- Terdapat akaun-akaun baharu dalam komputer anda yang bukan anda buka.
- Terdapat program-program baharu yang berjalan yang bukan anda pasang.
- Komputer anda kerap terpadam dengan sendirinya atau berfungsi dengan sangat perlahan.
- Program dalam komputer anda meminta untuk mengubah tetapan pada sistem walaupun anda tidak memasang atau mengemas kini sebarang aplikasi.
- Firewall memberi amaran bahawa suatu program yang tidak dikenali meminta kebenaran untuk membuat mengakses internet.

Digodam, Apa Perlu Saya Lakukan?

Cara Bertindak

Jika anda yakin komputer anda telah dikompromi; lebih pantas anda bertindak, lebih baik. Jika komputer yang anda gunakan untuk kerja milik majikan, jangan cuba untuk membaikinya sendiri dan jangan matikannya. Bukan sahaja anda mungkin akan menambah kerosakan, anda juga mungkin akan merosakkan bukti-bukti yang berguna untuk siasatan. Sebaliknya, laporkan kejadian tersebut kepada majikan anda secepat mungkin, biasanya dengan menghubungi meja bantuan, pasukan keselamatan atau penyelia. Jika di atas sebab-sebab yang tidak diketahui, anda tidak dapat menghubungi organisasi anda atau bimbang berlakunya kelewatan, putuskan hubungan komputer dengan rangkaian dan letakkannya dalam mod sleep, suspend atau hibernate. Walaupun anda tidak pasti sama ada anda telah digodam atau tidak, lebih baik ia dilaporkan dengan segera sebagai langkah berjaga-jaga. Organisasi anda mungkin mempunyai proses-proses tertentu dan pasukan untuk menangani situasi seperti ini, jadi biar mereka yang menguruskannya.

Lambat laun komputer anda mungkin dikompromi. Lebih cepat anda mengesan insiden dan lebih cepat anda bertindak, lebih baik.

Jika komputer tersebut kepunyaan anda, berikut adalah langkah-langkah yang boleh anda ambil:

- **Backups**. Langkah paling penting yang perlu anda boleh lakukan ialah bersedia untuk masa depan dengan menyediakan backup. Terutamanya membuat backup maklumat dengan kerap dan semak sama ada anda berjaya mengembalikan fail daripada backup. Biasanya apabila komputer digodam, antara pilihan anda adalah memadam sistem cakera keras dan memasang semula sistem operasi atau membeli komputer baharu. Walau apa pun, anda tetap memerlukan backup untuk mengembalikan maklumat peribadi anda.
- **Tukar Kata Laluan**. Pastikan semua kata laluan anda ditukar. Ini tidak terhad kepada kata laluan pada komputer dan peranti mudah alih, tetapi semua kata laluan dalam talian anda. Pastikan anda menukar semua kata laluan dalam talian daripada komputer yang lain yang anda pasti ianya selamat dan boleh dipercayai.
- **Anti-virus**. Jika perisian anti-virus anda memberitahu bahawa terdapat fail yang dijangkiti, ikutlah langkah yang dicadangkannya. Selalunya, ia mencadangan pengasingkan fail, pembersihan atau pemadaman fail tersebut. Kebanyakan perisian anti-virus mempunyai pautan yang boleh anda ikuti untuk lebih mempelajari tentang jangkitan tersebut. Jika masih ragu-ragu, asingkan fail tersebut. Jika itu tidak boleh dilakukan, padamkannya sahaja.
- **Memasang Semula**. Jika anda tidak boleh membersihkan komputer anda dengan anti-virus, salah satu cara yang paling selamat untuk memulihkannya adalah dengan membina semula komputer berkenaan dari mula. Pertama, putuskan hubungan komputer daripada rangkaian. Kemudian ikut arahan yang telah diberikan oleh

Digodam, Apa Perlu Saya Lakukan?

pengeluar sistem anda, dalam kebanyakan kes, ini bermakna anda perlu menggunakan sekatan cakera pemulihan yang telah disiap-pasang. Jika cakera pemulihan hilang, rosak atau dijangkiti, hubungi pengeluar dan minta mereka hantar DVD pemulihan. Jangan pasang semula sistem operasi daripada backup. Backup anda mungkin mempunyai kelemahan yang membolehkan penggodam masuk pada mulanya. Gunakan backup anda untuk memulihkan maklumat peribadi anda. Jika komputer anda telah lama atau belum dikemas kini, ianya mungkin lebih mudah (atau mungkin lebih murah) untuk membeli komputer baharu daripada menghabiskan masa untuk memasangnya semula.

- **Bantuan Profesional**. Jika anda bimbang komputer anda telah digodam, tetapi anda tidak mempunyai kemahiran atau kepakaran untuk membaikinya, anda mungkin perlu menghantarnya kepada mereka yang profesional. Sebagai contoh, selepas digodam anda mungkin berasa bahawa backup anda bukanlah yang terkini atau telah ketinggalan zaman. Anda mungkin mahu memindahkan fail kritikal seperti gambar, dokumen atau video daripada komputer yang dijangkiti kepada komputer yang baharu. Walaubagaimanapun dengan cara ini anda mungkin menjangkiti komputer baharu anda. Cara yang lebih selamat adalah dengan membawa komputer yang dijangkiti kepada juruteknik yang bertauliah, yang boleh mengembalikan fail-fail tersebut dengan selamat tanpa memindahkan jangkitan tersebut.

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! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! What Is Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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