Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- Pengenalan
- Bagaimana Antivirus Berfungsi
- Tip Antivirus

Apakah itu Antivirus?

Pengenalan

Antivirus adalah perisian keselamatan yang anda pasang pada komputer atau peranti mudah alih untuk melindunginya daripada dijangkiti malware. Terma “malware” merupakan perkataan yang merangkumi semua jenis malware seperti virus, cecacing, trojan dan perisian intipan. Sebenarnya, terma “malware” berasal daripada kombinasi perkataan “malicious software” (perisian berniat jahat). Jika komputer anda dijangkiti malware, penjenayah siber boleh menyimpan kesemua ketukan kekunci, mencuri dokumen atau menggunakan komputer anda untuk membuat serangan ke komputer yang lain. Bercanggah dengan pendapat sesetengah individu, mana-mana sistem operasi, termasuk Mac OS X dan Linux, juga boleh dijangkiti.

Editor Jemputan

Jake William merupakan pengasas Rendition Infosec (**www.renditioninsec.com**) dan merupakan salah seorang tenaga pengajar dan pengarang kursus yang bertauliah di SANS. Beliau aktif di Twitter **@MalwareJake** dan mempunyai laman blog sendiri **malwarejake.blogspot.com**.

Anda boleh membeli perisian antivirus sebagai penyelesaian kendiri, atau selalunya ia termasuk sebagai sebahagian daripada pakej keselamatan. Walaubagaimanapun, antivirus tidak mampu lagi mengikuti penyerang siber kerana mereka berterusan membangunkan malware baharu. Terlalu banyak versi malware yang dikeluarkan setiap hari sehinggakan tidak ada antivirus yang boleh mengesan dan melindungi komputer daripada semuanya. Anda harus faham bahawa antivirus dapat membantu melindungi komputer anda tetapi ia tidak dapat mengesan atau menghentikan kesemua jenis malware. Untuk memahami dengan lebih lanjut, mari kita fahami bagaimana kebanyakan program ini berfungsi.

Bagaimana Antivirus Berfungsi

Secara umumnya terdapat dua cara perisian antivirus mengenali pasti malware; pengesan tandatangan dan pengesan tingkah laku. Pengesan tandatangan berfungsi seperti sistem imunisasi manusia. Ia mengimbas komputer anda untuk ciri-ciri atau tanda malware yang diketahui. Ia bertindak dengan merujuk kepada kamus malware yang diketahui dan jika sesuatu di dalam komputer anda menyerupai corak di dalam kamus, program tersebut akan cuba untuk meneutralkannya. Pendekatan menggunakan kamus perlu dikemas kini dengan kerap untuk melindungi komputer daripada jenis malware yang baharu. Hal ini dianalogikan seperti suntikan vaksin selsema yang digunakan sebagai kemas kini untuk mengukuhkan sistem imunisasi manusia. Antivirus hanya boleh melindungi dari apa yang ia kenali sebagai berbahaya tetapi penyerang siber membangunkan malware dengan sangat pantas sehingga pembekal antivirus tidak dapat mengikutinya. Hasilnya, tidak kira sekerap mana anda mengemas kini antivirus, akan ada malware baru yang berpotensi melepasi perisian antivirus anda.

Apakah itu Antivirus?

Melalui cara pengesan tingkah laku, antivirus tidak cuba untuk mengenali malware, tetapi ia memantau tingkah laku perisian yang dipasang di dalam komputer anda. Apabila terdapat program bertindak mencurigakan, seperti cuba membuat capaian kepada fail yang dilindungi atau mengubahsuai program lain, antivirus yang menggunakan pengesan tingkah laku akan memantau aktiviti yang mencurigakan ini dan akan memberi peringatan kepada anda. Walaupun cara ini berkemungkinan memberi peringatan palsu, tetapi ianya memberikan perlindungan daripada malware baru yang tiada dalam sebarang kamus. Anda sebagai pengguna komputer, mungkin tidak pasti tentang apa yang boleh dan tidak untuk dibenarkan, malahan dari masa ke semasa pengguna menjadi kurang peka kepada semua amaran. Anda mungkin terdorong untuk klik accept pada setiap amaran, seterusnya membiarkan komputer anda terdedah kepada serangan atau jangkitan. Selain itu, sebaik sahaja tingkah laku dikesan, malware tersebut berkemungkinan besar telah lama berada di dalam mesin anda dan anda mungkin tidak tahu apakah yang telah dilakukan olehnya sebelum dikesan oleh perisian antivirus.

Walaupun antivirus merupakan bahagian penting untuk keselamatan anda, ia tidak dapat menghalang dan menghentikan semua serangan. Pada dasarnya, andalah perlindungan yang terbaik, bukannya teknologi semata-mata.

Antivirus merupakan komponen penting untuk melindungi komputer dan peranti mudah alih anda, jadi kami mengesyorkan anda memasang dan menggunakannya dengan sekerap mungkin. Walaupun begitu, harus diingat bahawa tidak kira bagaimana antivirus anda berfungsi, ia tidak akan dapat melindungi anda dari semua jenis malware. Anda sendiri merupakan pertahanan terbaik untuk menentang penyerang siber pada masa kini, bukannya teknologi semata-mata.

Tip Antivirus

1. Dapatkan perisian antivirus daripada sumber yang diketahui dan dipercayai. Penyerang siber kebiasaannya mengedar antivirus palsu yang sebenarnya adalah malware.
2. Pastikan anda memasang perisian antivirus versi terkini, membayar langganan tahunan dan mengaktifkan perisian antivirus. Selain itu, perisian antivirus anda harus diatur supaya kemas kini boleh dilakukan secara automatik.
3. Pastikan antivirus anda membuat imbasan secara automatik kepada media mudah alih seperti pemacu USB dan pastikan perlindungan masa nyata diaktifkan. Elakkan menangguh proses untuk mengemas kini perisian antivirus anda.
4. Beri perhatian kepada amaran dan peringatan pada skrin yang dijana oleh perisian antivirus anda. Kebanyakan peringatan mempunyai pilihan untuk memberikan lebih maklumat atau cadangan tentang langkah seterusnya. Jika anda mendapat peringatan pada komputer yang dibekalkan oleh majikan, pastikan anda menghubungi meja bantuan atau penyelia anda dengan segera.
5. Elakkan dari memadam atau melumpuhkan perisian antivirus jika ia melambatkan komputer, menyekat laman

Apakah itu Antivirus?

sesawang atau menghalang anda dari memasang sesuatu perisian atau program. Melumpuhkan antivirus anda akan mendedahkan anda kepada risiko malware dan boleh mengakibatkan insiden keselamatan yang serius. Jika masalah berlaku kepada komputer pejabat, hubungi meja bantuan. Jika masalah berlaku pada komputer peribadi, cuba hubungi pembekal antivirus dengan melawati laman sesawang mereka untuk mendapatkan maklumat lanjut atau menukar antivirus anda dengan produk yang lain.

6. Elakkan dari memasang beberapa program antivirus di dalam komputer dalam masa yang sama. Ia berkemungkinan akan menyebabkan konflik di antara satu sama lain dan ia berkemungkinan akan merendahkan tahap keselamatan komputer anda.
7. Belajar untuk mengenali amaran yang dijanakan oleh perisian antivirus anda. Penyerang siber boleh membangunkan laman sesawang berniat jahat yang akan memaparkan amaran antivirus palsu yang kelihatan realistik dan menawarkan bantuan membaiki komputer anda. Dengan menekan butang atau klik pada pautan laman sesawang sebegini sebenarnya boleh membahayakan 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

Anti-Virus Product Comparisons:	http://www.av-test.org/en/
Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
I'm Hacked, Now What?:	http://www.securingthehuman.org/ouch/2014#may2014

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

