OUCH! | Jun 2017

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Pengajaran Dari WannaCry

Pengenalan

Baru-baru ini anda mungkin menonton liputan media yang meluas tentang serangan siber terbaru yang diberi nama 'WannaCry'. 'WannaCry' telah menjangkiti lebih 200,000 komputer, mengunci pelbagai organisasi dari data mereka termasuklah hospital-hospital di United Kingdom. Terdapat beberapa sebab mengapa serangan ini mendapatbanyak tumpuan. Pertama, ia merebak dari komputer ke komputer dengan menyerang kelemahan yang terdapat pada komputer Windows. Kedua, serangan tersebut merupakan satu perisian hasad yang dipanggil perisian tebusan (ransomware). Ini bermakna jika komputer anda dijangkiti ia akan menyulitkan kesemua fail, dan mengunci anda daripada data anda. Satu-satunya cara untuk mendapatkan kembali data tersebut adalah dari sandaran atau atau dengan membuat bayaran tebusan USD300 kepada penyerang untuk menyahsulitkan data anda. Ketiga dan yang paling penting, serangan ini tidak sepatutnya berlaku. Kelemahanpada komputer Windows yang diserang 'WannaCry' telah diketahui oleh Microsoft, dan Microsoft telahpun mengeluarkan tampalan untuk membaikinya berbulan sebelum ini. Tetapi banyak organisasi gagal untuk memasang pembaikan ini, atau masih lagi menggunakan sistem operasi seperti Windows XP yang terlalu lama sehinggakan tiada tampalan yang boleh digunakan untuknya. Berikut merupakan tiga langkah mudah yang boleh anda ambil untuk memastikan serangan seumpama 'WannaCry' tidak boleh menjangkiti anda.

Editor Jemputan

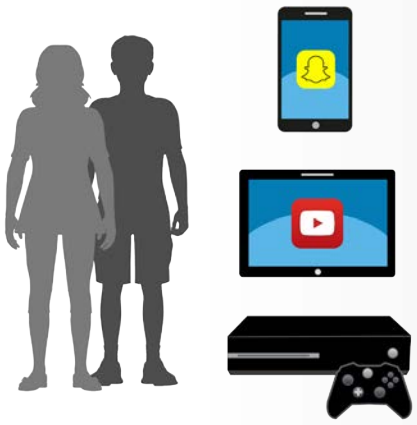
Dr. Johannes Ullrich merupakan Dekan Penyelidikan untuk **SANS Technology Institute** dan pengasas Dshield.org. Beliau bertanggungjawab untuk SANS Internet Storm Center yang memantau ancaman keselamatan siber. Beliau mengajar Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) and IPv6 (**SEC546**).

Tampalan

Pertama sekali, pastikan komputer, peranti mudah alih, aplikasi dan perkakasan lain anda yang berhubung dengan Internet di kemaskini. Penjenayah siber sentiasa mencari kelemahan dalam perisian peranti anda. Apabila mereka menemui kerentanan tersebut, mereka menggunakan program khas untuk menggodam peranti yang anda gunakan. Sementara itu, syarikat yang mencipta perisian untuk peranti bekerja keras untuk membaiki kelemahan dengan mengeluarkan kemas kini. Dengan memastikan komputer dan peranti mudah alih anda dipasang kemas kini tersebut, adalah sukar untuk sesiapa menggodam anda. Itulah sebabnya penyebaran WannaCry amat menyedihkan. Kemas kini untuk menghalang serangan ini telah dikeluarkan oleh Microsoft hampir dua bulan lalu. Jika organisasi mengemaskini komputer mereka, serangan tidak mungkin berlaku. Untuk memastikan peranti anda sentiasa dikemas kini, bolehkan kemas kini automatik jika mungkin.

Pengajaran Dari WannaCry

Peraturan ini digunapakai hampir ke seluruh teknologi yang berhubung dengan rangkaian, bukan sahaja komputer dan peranti mudah alih anda tetapi TV bersambung Internet, router rumah, konsol permainan atau mungkin satu hari nanti kereta anda. Jika sistem operasi atau peranti anda terlalu lama sehingga ianya tidak lagi disokong dengan kemas kini keselamatan, seperti Windows XP, gantikan ia dengan yang baru dan mempunyai sokongan.



Kunci untuk melindungi diri anda dari serangan seperti WannaCry adalah tiga langkah mudah; pastikan komputer anda dikemas kini, hati-hati dengan serangan memancing data dan sandarkan sistem anda.

Sandaran

Dalam sesetengah kes, serangan siber seperti perisian tebusan boleh menjangkiti sistem yang telah dikemas kini. Cara kedua untuk melindungi diri adalah dengan melakukan sandaran. Sandaran adalah salinan maklumat yang disimpan di tempat selain dari komputer atau peranti mudah alih anda. Sekiranya kehilangan data bernilai, anda boleh memulihkan semula data tersebut dari sandaran tersebut. Malangnya, terlalu ramai dari kita gagal untuk melakukan sandaran dengan kerap, walaupun ianya murah dan mudah. Terdapat dua cara untuk menyandar data anda: media fizikal atau storan berpengkalan diawan. Setiap pendekatan mempunyai kabaikan dan keburukan. Anda boleh gunakan kedua-dua pendekatan pada masa yang sama jika anda tidak pasti kaedah mana yang mahu digunakan.

Media fizikal adalah peranti yang anda kawal seperti pemacu USB luaran atau pemacu bersambung rangkaian yang terletak di rumah atau pejabat. Kelebihan menggunakan media fizikal sendiri adalah ia membolehkan anda membuat sandaran dan memulihkan data yang besar dengan pantas. Keburukan pendekatan sedemikian adalah jika anda dijangkiti dengan perisian hasad seperti perisian tebusan, ada kemungkinan ia boleh merebak je sandaran anda. Jika menggunakan media fizikal sebagai sandaran anda seharusnya menyimpan salinan sandaran di luar kawasan ditempat yang selamat. Pastikan sebarang sandaran yang anda simpan dilabel dengan baik. Penyelesaian berpengkalan diawan merupakan perkhidmatan dalam talian untuk menyandar fail di Internet. Selalunya satu program akan dipasang pada komputer anda yang akan menyelesaikan segalanya. Kelebihan menggunakan penyelesaian awan adalah keringkasannya. Sebagai tambahan, jika anda dijangkiti perisian tebusan, jangkitan tersebut tidak boleh mencapai sandaran berpengkalan diawan. Kelemahannya pula adalah ia boleh mengambil masa yang sangat lama untuk membuat sandaran dan pemulihan data yang besar. Pastikan anda selidik privasi dan keselamatan sandaran awan. Adakah perkhidmatan sandaran tersebut menyediakan keselamatan yang kukuh seperti penyulitan dan pengesahan kukuh?

Pengajaran Dari WannaCry

Memancing Data

Akhir sekali, penjahat sentiasa mengemaskini dan menukar cara serangan mereka. Penjenayah siber sering menggunakan serangan lain yang dipanggil memancing data (phishing) unuk menyerang dan menjangkiti mangsa. Memancing data adalah apabila penjenayah siber menghantar satu emel untuk memperdayakan anda supaya membuka lampiran yang dijangkiti atau melawati laman hasad. Jika anda melakukan salah satunya, komputer anda mungkin anda dijangkiti. Walaupun 'WannaCry' tidak menggunakan serangan ini, kebiasaannya ia digunakan untuk serangan lain, termasuklah kebanyakan jenis perisian hasad. Sebagai tambahan, penjenayah siber yang membangunkan WannaCry semestinya akan mengemaskini cara serangan dalam bulan-bulan yang akan datang dan menggunakan teknik seperti memancing data untuk menjangkiti lebih banyak komputer. Kunci untuk melindungi diri anda dari serangan sedemikian adalah dengan menggunakan akal. Jika sesuatu emel nampak ganjil, sangsi atau terlalu bagus untuk dipercayai, kemungkinan besar ianya adalah satu serangan.

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 securingthehuman.sans.org/ouch/archives.

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

What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Using the Cloud Securely:	https://securingthehuman.sans.org/ouch/2016#november2016

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie