BULETIN ICT
NEGERI MELAKA

Ancaman Keselamatan Siber

TOKOH
Tokoh Pemikir Keselamatan Siber

KERAJAAN
Insiden Keselamatan ICT

Bahagian K-Ekonomi Anjurkan Program ICON Windows Phone

INFORMASI
Perisian Antivirus Percuma 2013

Apakah itu Malware?

15 Malware Yang Terkenal

Tips Panduan Keselamatan Siber

Jenis-jenis Serangan Siber

PROGRAM
Seminar Digital Marketing

OGOS 2013

Bahagian K-Ekonomi
Jabatan Ketua Menteri Melaka

Pentadbiran Kerajaan Negeri Melaka

ingin merakamkan

Setinggi-tinggi Penghargaan

kepada

Seluruh Rakyat Negeri Melaka Yang Memeriahkan

Majlis Rumah Terbuka Malaysia Aidilfitri

BULETIN ICT

Perutusan Ketua ICT Negeri Melaka

BISMILLAHIRAHMANNIRAHIM

Assalamualaikum W.B.T dan Salam Sejahtera

Fenomena serangan siber kini telah melepasi tahap normal, dan telah menjadi satu perkara yang amat membimbangkan. Jika dilihat motif serangan siber ini, dahulunya ia bermula sebagai satu hobi untuk menunjukkan kebolehan menyerang komputer peribadi seperti virus Elk Cloner yang ditemui pada tahun 1981 yang disasarkan kepada Apple II serta virus Brain untuk IBM pada tahun 1986.

Penularan virus ini juga amat pantas, sebagai contoh pada tahun 2003 Sapphire/Slammer SQL hanya mengambil masa 10 minit untuk tersebar ke seluruh dunia. Manakala statistik tahun 2012 menunjukkan virus baru dicipta setiap 7 minit. Perkara yang menjadi dilema sesuatu virus baru itu ialah ia hanya boleh dikesan apabila telah berlakunya insiden, kesan dari tindakan virus berkenaan. Pada tahun 2005, satu terminologi diperkenalkan iaitu *Advanced persistent threat* (APT), ianya merujuk kepada serangan menggunakan teknik termaju dan berterusan sehingga sesuatu kejayaan diperolehi. Sasaran serangan siber ini bukan lagi pengguna komputer peribadi, tetapi telah beralih kepada maklumat kerajaan dan syarikat konglomerat.

Oleh yang demikian, bagi menjaga integriti dan kerahsiaan maklumat organisasi kita, langkah-langkah keselamatan perlu diambil terutama menangani isu yang dikaitkan dengan *Data Leakage Protection* (DLP). Kerjasama antara Pegawai Keselamatan ICT dengan semua kakitangan adalah suatu resipi kejayaan sesuatu sistem keselamatan di sesebuah organisasi.

Keselamatan ICT – Tanggungjawab Semua

Dr. Mohamed Sulaiman Sultan Suhaibuddeen
Ketua ICT Negeri Melaka @ Ketua Editor

ISI KANDUNGAN

Penaung
Y.A.B Datuk Wira Ir. Hj. Idris bin Hj. Haron
Ketua Menteri Melaka

Penasihat
YB Datuk Hj. Naim bin Abu Bakar
Setiausaha Kerajaan Negeri Melaka

Ketua Editor
Dr. Mohamed Sulaiman bin Sultan Suhaibuddeen
Ketua ICT Negeri Melaka

Editor
Muaz bin Ghazali

Sumbangan Bahan
Bahagian K-Ekonomi, Jabatan Ketua Menteri Melaka

Penerbit & Percetakan
Bahagian K-Ekonomi,
Inkubator K-Ekonomi, Jln Business City,
Bandar MITC, Hang Tuah Jaya,
75450 Ayer Keroh, Melaka.
No.Tel : 06-2324425/4436
No.Faks : 06-2331460
Laman Web : http://www.emelaka.gov.my

Ancaman Keselamatan Siber

PENGENALAN

Perkembangan teknologi komputer dan juga internet yang pesat pada masa kini telah memberikan impak yang sangat besar pada hidup manusia. Sama ada impak yang baik atau yang buruk, manusia sangat teruja dalam menggunakannya. Namun adakah kita sedar akan kesan buruk yang dibawa bersama dalam penggunaan teknologi ini. Rata-rata di antara kita tidak mengambil berat akan perkara yang dilihat begitu serius jika tidak ditangani dengan baik iaitu aspek keselamatan siber.

Apakah yang dimaksudkan dengan siber mahupun keselamatan siber? Menurut takrifan Dewan Bahasa dan Pustaka, siber boleh membawa maksud kepada apa-apa yang berkaitan dengan komputer dan juga internet. Oleh itu, keselamatan siber pula merangkumi aspek-aspek keselamatan terhadap komputer dan setiap peranti yang bersambungan kepada internet seperti telefon pintar, tablet dan juga server.

ANCAMAN

Rakyat di negara ini juga boleh dikategorikan sebagai masyarakat siber kerana akses kepada teknologi komputer dan internet sangat mudah diperolehi hasil daripada dasar dan inisiatif kerajaan dalam menjadikan negara kita tidak ketinggalan dalam bidang ICT.

Namun demikian, akses yang mudah boleh menjadikan negara kita dengan mudahnya diancam oleh pihak yang tidak bertanggungjawab sekiranya tidak dilindungi. Ancaman serangan siber ini bukan sahaja berlaku di negara kita malah di peringkat global juga fenomena ini menjadi ancaman utama kepada negara terlibat. Serangan siber pula boleh hadir dalam pelbagai bentuk seperti serangan malware dan virus komputer, penggodaman, pemalsuan data dan spam.

Insiden penggodaman terhadap dua sistem atas talian milik Jabatan Penerangan Malaysia iaitu sistem e-Press dan e-Akhbar pada 18 Februari 2013 yang lepas wajar dijadikan iktibar kepada semua pihak kerana insiden seperti ini bukan kali pertama kes laman web rasmi jabatan kerajaan digodam oleh individu dan pihak yang tidak bertanggungjawab.

Walaupun negara kita tidak hebat diancam dengan serangan siber seperti yang dialami negara Amerika Syarikat mahupun negara-negara membangun yang lain, namun langkah pencegahan dan keselamatan harus difikir dan dilakukan dari sekarang agar negara kita bersiap sedia sekiranya serangan siber dilancarkan kelak.

KERAJAAN

Kebanyakan pengguna Internet sering mengabaikan pelbagai peringatan kerajaan yang sentiasa menasihatkan pengguna supaya berwaspada dengan laman sesawang yang mencurigakan.

Pihak kerajaan sangat komited dalam memastikan masyarakat di negara ini mempunyai tahap kesedaran yang baik terhadap serangan siber kerana dengan pengetahuan yang baik, ia mampu menghalang pengguna daripada diserang oleh individu atau pihak yang tidak bertanggungjawab.

Datuk Seri Najib Tun Razak juga menyatakan bahawa kajian ke atas peruntukan undang-undang siber sedia ada telah siap dan ia akan membantu kerajaan menangani kegiatan tidak bermoral dan salah di sisi undang-undang. Menurut Perdana Menteri, kajian tersebut menumpukan kepada langkah-langkah untuk mengatasi kelemahan yang dikesan sekali gus memperkukuhkan undang-undang sedia ada.

Selain itu, penubuhan CyberSecurity Malaysia sebagai agensi pakar keselamatan siber nasional di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI) dilihat dapat memberikan perkhidmatan khusus dalam bidang keselamatan siber di negara ini.

TANGGUNGJAWAB

Tanggungjawab untuk melindungi pengguna daripada serangan siber bukan hanya terletak pada pihak kerajaan sahaja kerana semua pihak terutamanya pengguna itu sendiri haruslah bertanggungjawab dalam memastikan mereka tidak terdedah dengan mudah pada serangan siber. Sebagai seorang pengguna, penggunaan perisian Antivirus amatlah penting kerana dapat membantu memberikan perlindungan kepada pengguna dan mereka harus sentiasa kemaskini perisian Antivirus agar dilengkapi dengan perlindungan terkini.

Selain itu, bagi pengguna emel pula mereka tidak sepatutnya membuka lampiran (*attachment*) pada emel yang diterima sekiranya pengirim emel berkenaan dari sumber yang mencurigakan. Melayari laman sesawang yang mencurigakan juga boleh membuatkan seorang pengguna itu terdedah kepada serangan siber. Oleh itu, pengguna harus sedar bahawa serangan siber ini adalah satu bentuk ancaman yang boleh memberi kesan yang buruk kepada pengguna dan juga negara.

SERANGAN SIBER
Statistik 2012

Malaysia merupakan negara **keenam** di dunia **berisiko** terdedah ancaman **jenayah siber**

- Akhbar KOSMO, 16 Mei 2013

5 Negara Tertinggi 'Malware Hosting'

1. 2. 3. 4. 5.

5 Negara Paling Rendah Dijangkiti

1. 2. 3. 4. 5.

KASPERSKY lab

Negara Dengan Kekerapan Tertinggi Laman Web Diserang

1. Rusia
2. Tajikistan
3. Azerbaijan
4. Armenia
5. Kazakhstan

14. MALAYSIA

Sumber: www.kaspersky.com

Symantec

42%

Peningkatan pada serangan yang disasarkan

Sumber: www.symantec.com

32%

Peningkatan kes ancaman kecurian maklumat melalui peranti mudah alih

30%

Peningkatan kes serangan laman web yang disekat setiap hari

5,291

Vulnerabilities terbaru dijumpai

415

daripadanya adalah pada sistem pengoperasian peranti mudah alih

Insiden Keselamatan ICT

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat

Attempts/Hack Threats/Information Gathering

Percubaaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran, termasuk *spoofing*, *phishing*, *probing*, *war driving* dan *scanning*.

Pelanggaran Dasar (*Violation of Policy*)

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT

Harrassment/Threats

Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif peribadi dan atas sebab tertentu.

Pencerobohan (*Intrusion*)

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*

Pemalsuan (*Forgery*)

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft/espionage)* dan penipuan *(hoaxes)*.

Spam

Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

Malicious Code

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.

Kehilangan Fizikal (*Physical Loss*)

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

Sekiranya anda mengalami insiden seperti di atas, laporkan kepada:

Goverment Computer Emergency Response Team (GCERT)

No. Tel: 03-88725138 No. Faks: 03-88904253

Email: gcert@mampu.gov.my

Sumber: Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, MAMPU

Windows Store

Bahagian K-Ekonomi Anjur Program Pembangunan Aplikasi Windows Phone

Program Pembangunan Aplikasi atau juga dikenali dengan ICON adalah salah satu usaha kerajaan melalui Perbadanan Pembangunan Multimedia (MDeC) untuk memberikan peluang dan bantuan kepada rakyat tempatan dalam pembangunan aplikasi mudah alih. Program ICON ini telah mula diperkenalkan pada tahun 2009 dengan sambutan yang menggalakkan daripada pembangun tempatan sehingga ianya diteruskan pada tahun ini dengan sasaran yang lebih meluas lagi.

Pada tahun ini juga, Perbadanan Pembangunan Multimedia (MDeC) telah menjalinkan kerjasama dengan Nokia bagi membantu pembangun aplikasi tempatan membangunkan kandungan aplikasi mudah alih untuk platform baru Windows Phone 8.

Program ICON ini telah pun diadakan di Negeri Melaka baru-baru ini untuk pembangunan aplikasi mudah alih bagi platform Android dan iOS. Sehubungan dengan itu, Bahagian K-Ekonomi dengan kerjasama daripada MDeC dan syarikat Info Trek akan menganjurkan program pembangunan aplikasi mudah alih bagi platform Windows Phone 8 pada bulan September ini. Berikut merupakan keterangan lanjut mengenai program berkenaan:

Langkah 1: Sumbangkan Idea Anda

Persembahkan idea kreatif anda kepada kami untuk kami kagumi dan kami bawa idea anda menjadi realiti

Tarikh: 13 September 2013 (Jumaat)
Masa: 10 pagi - 5 petang
Tempat: Inkubator K-Ekonomi, MITC

Langkah 2: Sertai Bengkel

Bengkel selama 5 hari ini akan membantu anda membangunkan aplikasi yang akan diketuai oleh Jurulatih Profesional.

Tarikh: 30 September - 4 Oktober 2013
Masa: 9 pagi - 5 petang
Tempat: Inkubator K-Ekonomi, MITC

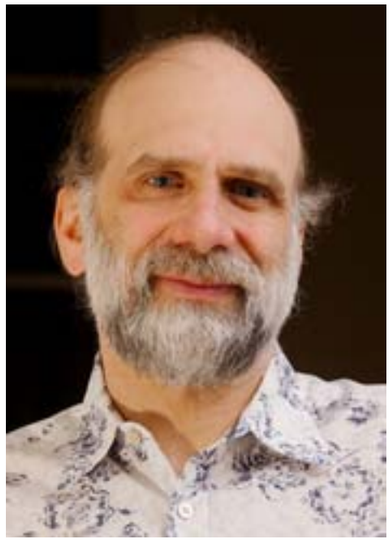
Langkah 3: Bangunkan Aplikasi

Selepas tamat bengkel, anda harus membangunkan aplikasi sendiri dan harus diterbitkan di Windows Phone Apps Store sebelum 31 Disember 2013

SERTAI KAMI

TAKLIMAT PROGRAM ICON WINDOWS
6 September 2013 (Jumaat) | 9 pagi - 11 pagi
Auditorium Seri Negeri

Bruce Schneier Tokoh Pemikir Keselamatan Siber



http://www.schneier.com/

Bruce Schneier

@schneierblog

Antara buku-buku yang ditulis oleh Schneier

Bruce Schneier dilahirkan di New York, Amerika Syarikat pada 15 Januari 1963. Beliau dikenali sebagai seorang kriptograf, pakar sekuriti komputer dan penulis. Beliau juga adalah pengarang kepada beberapa buah buku mengenai topik keselamatan umum, sekuriti komputer dan kriptografi.

Beliau merupakan graduan ijazah dalam bidang Fizik dari *University of Rochester* pada tahun 1984 dan melanjutkan pelajaran di peringkat sarjana dalam bidang sains komputer di *American University* pada tahun 1988. Pada tahun 2011 pula, beliau dianugerahkan dengan Ijazah Doktor Falsafah (Ph.D) oleh *University of Westminster* di England.

Bruce Schneier mempunyai sebuah weblog sendiri, Schneier on Security (www.schneier.com) di mana beliau berkongsi pendapat, pandangan dan nasihat dalam aspek sekuriti komputer, teknologi sekuriti, kriptografi. Selain itu, beliau juga mempunyai pengikut sendiri bagi Crypto-Gram iaitu risalah bulanan mengenai topik sekuriti yang diedarkan melalui emel.

Beliau banyak membantu masyarakat dunia dalam bidang sekuriti melalui penulisan buku-bukunya mengenai pelbagai topik sekuriti komputer dan juga telah terlibat dalam penciptaan algoritma kriptografi seperti algoritma *Hash Functions, Stream ciphers, Pseudo-random number generators* dan *Block ciphers*.

Beliau merupakan pengasas dan juga Ketua Pegawai Teknologi bagi syarikat BT Counterpane iaitu sebuah syarikat yang menjual perkhidmatan rangkaian keselamatan komputer secara terurus.

Beliau adalah individu yang begitu lantang memberikan pandangan dan nasihat dalam bidak keselamatan komputer. Beliau pernah memberi pandangan yang keras mengenai syarikat Microsoft pada tahun 2001 dan mengkritik Windows 2000 yang mempunyai banyak *security holes* berbanding versi-versi Windows lain.

Beliau juga menyatakan bahawa syarikat Microsoft lebih banyak menghabiskan duit dalam aspek perkhidmatan keselamatan daripada menghasilkan produk yang lebih selamat. "Apabila *security bug* dijumpai dalam produk Microsoft, mereka akan menafikannya sehingga mereka menyelesaikan masalah tersebut dan memberitahu kepada dunia bahawa betapa hebatnya mereka (Microsoft)," katanya.

Complexity is the enemy of security. As systems get more complex, they get less secure - Bruce Schneier

Sumber: PCWorld.com, Wikipedia.org, www.schneier.com

Jenis-jenis Serangan Siber

HACKING

Hacking dalam konteks keselamatan komputer adalah sebarang usaha teknikal yang bertujuan untuk mengeksploitasi kelemahan pada sistem mahupun rangkaian komputer. *Hacking* mungkin didorong oleh pelbagai sebab seperti mencari keuntungan, tanda protes, cabaran dan juga penambahbaikan. Konsep dan terma *hacking* ini mula diperkenalkan pada tahun 1960-an di *Massachusetts Institute of Technology*. Pada mulanya, terma *hacking* merupakan terma yang positif namun pada masa kini terma *hacking* dan *hacker* telah dikaitkan untuk setiap serangan siber yang berniat jahat di Internet dan di rangkaian.

PHISHING

Phishing adalah suatu tindakan untuk cuba mendapatkan maklumat seperti nama pengguna, kata laluan dan butiran kad kredit dengan dengan cara menyamar sebagai entiti yang boleh dipercayai. *Phishing* boleh menggunakan emel yang mengandungi pautan ke laman web yang dijangkiti *malware* atau laman web palsu yang kelihatan seperti laman web asli.

SPAM

Suatu teknik yang menghantar banyak salinan mesej yang sama kepada penerima menerusi emel walaupun tidak diminta oleh penerimanya. Kebanyakan email spam adalah pengiklanan komersial, skim cepat kaya cepat, atau perkhidmatan yang seakan-akan undang-undang. Pautan dalam emel spam boleh menghantar pengguna untuk laman web *phishing* atau laman web yang mempunyai *malware*.

SPOOFING

Spoofing adalah satu bentuk serangan penipuan di mana pihak berniat jahat menyamar menjadi peranti atau pengguna lain dalam rangkaian (*network*) untuk melancarkan serangan terhadap *network host*, mencuri data, penyebaran malware, atau memintas kawalan akses. Terdapat beberapa jenis serangan *spoofing* yang digunakan oleh pihak-pihak yang berniat jahat. Antara kaedah-kaedah yang paling biasa termasuk serangan penipuan alamat IP, serangan penipuan menipu ARP, dan serangan penipuan *DNS Server*. Penipuan *(spoofing)* alamat IP adalah kaedah penipuan yang sering berlaku pada masa kini di mana pihak tidak bertanggungjawab menghantar *IP Packet* dari sumber alamat yang palsu bagi menyembunyikan dirinya. *Email spoofing* ialah bentuk serangan penipuan menerusi emel dengan alamat penghantar yang palsu.

DDoS ATTACK

DDoS attack atau *Distributed Denial of Service* ialah sejenis serangan web yang bertujuan untuk mengganggu fungsi normal rangkaian komputer yang disasarkan. Serangan DDoS adalah berbeze dengan serangan DoS di mana serangan DDoS menyerang banyak sambungan Internet dan komputer manakala serangan DoS hanya menyerang satu sambungan Internet pada satu komputer sahaja. Matlamat serangan DDoS ini adalah untuk mengwujudkan kehadiran *traffic* palsu yang luar biasa sehingga penggunaan Internet bagi pengguna menjadi perlahan dan lambat.

SQL INJECTION

SQL Injection adalah salah satu mekanisme serangan web yang digunakan oleh penggodam untuk mencuri data dari sesuatu organisasi. Ia adalah jenis serangan yang mengambil kesempatan daripada kod yang tidak betul pada aplikasi web yang membolehkan penggodam untuk menyuntik arahan SQL dan mendapat akses kepada data yang disimpan dalam pangkalan data. Menurut *Open Web Application Security Project (OWASP)*, pada tahun 2013, *SQL Injection* telah dinobatkan di tangga pertama dalam senarai serangan aplikasi laman web.

Sumber: Wikipedia.org

INFORMASI

avast! Free Antivirus

avast! be free

Keperluan Sistem

Windows 8
Windows 7
Windows Vista
Windows XP SP2

Pentium 3 Processor

600 MB (free)

128 MB RAM

www.avast.com

AVG Antivirus FREE 2013

AVG

Keperluan Sistem

Windows 8
Windows 7
Windows Vista
Windows XP Pro
Windows XP

Intel Pentium 1.8GHz

1350 MB (free)

512 MB RAM

free.avg.com

Avira Free Antivirus 2013

AVIRA

Keperluan Sistem

Windows 8
Windows 7
Windows XP SP3
Windows XP SP2

Intel Pentium 1GHz

150 MB (free)

1GB RAM

www.avira.com

PERISIAN ANTIVIRUS PERCUMA 2013

Bitdefender Antivirus Free Edition

Bitdefender

Keperluan Sistem

Windows 8
Windows 7
Windows Vista
Windows XP SP3

Tidak dinyatakan

1GB (free)

512 GB RAM

www.bitdefender.com

ZoneAlarm Free Antivirus + Firewall 2013

ZONEALARM

Keperluan Sistem

Windows 8
Windows 7
Windows Vista
Windows XP SP2

Intel Pentium 2GHz

250 MB (free)

1 GB RAM

www.zonealarm.com

Comodo Antivirus

COMODO Creating Trust Online®

Keperluan Sistem

Windows 8
Windows 7
Windows Vista
Windows XP SP2

Tidak dinyatakan

400 MB (free)

152 MB RAM

www.comodo.com

Apakah itu Malware?

Malware adalah nama ringkas bagi *malicious software* yang merupakan sebuah perisian yang diprogramkan oleh individu atau pihak tertentu untuk mengganggu operasi komputer, mengumpul maklumat sensitif atau mendapatkan akses kepada sistem komputer peribadi. Malware adalah istilah umum yang digunakan untuk merujuk kepada pelbagai bentuk perisian yang berniat jahat. Berikut merupakan **antara** jenis malware yang terdapat pada masa kini.

Virus Komputer

Sebuah program perisian yang direka untuk disebarkan dari satu komputer kepada komputer yang lain dan menggangu operasi komputer tersebut. Virus komputer boleh merosakkan atau memadam data pada komputer anda, menggunakan program emel untuk menyebarkan dirinya ke komputer lain, atau boleh memadam segala-galanya data yang ada di dalam *hard disk* anda.

Virus komputer pada masa sekarang kerap disebarkan melalui lampiran (*attachment*) di emel, melalui muat turun fail/program di Internet serta melayari laman web yang berbahaya.

Spyware

Spyware adalah istilah umum yang digunakan untuk menggambarkan perisian yang melakukan tingkah laku tertentu tanpa mendapat persetujuan daripada pengguna seperti pengiklanan, mengumpul maklumat peribadi dan melakukan perubahan pada sistem konfigurasi komputer anda.

Spyware juga sering dikaitkan dengan perisian yang memaparkan iklan yang dipanggil adware atau perisian yang menjejak maklumat peribadi atau sensitif.

Worm

Worm adalah sejenis malware yang boleh disebarkan tanpa interaksi manusia. Ianya kerap disebarkan melalui rangkaian (*network*) dari satu komputer ke satu komputer yang lain dengan mengambil *valuable memory* dan *network bandwitch* komputer yang dijangkitinya dan menyebabkan komputer tidak bertindak balas. Selain itu, worm juga membolehkan penyebarnya mendapatkan akses komputer anda daripada jauh.

Trojan Horse

Trojan Horse atau Trojan merupakan sejenis malware yang berbahaya namun tidak *replicate* secara automatik seperti virus komputer. Istilah Trojan Horse berasal daripada kisah Trojan Horse dalam Mitologi Yunani. Kesan dijangkiti Trojan Horse mungkin berbeza-beza seperti membuat gangguan, melakukan kerosakan atau memusnahkan fail-fail, folder dan program di komputer anda.

Trojan juga boleh mengwujudkan *backdoors* yang memberi jalan kepada penggodam akses kepada komputer yang dijangkitinya. Menurut Kaspersky Lab, cara biasa seorang pengguna dijangkiti Trojan Horse adalah dengan menerima emel atau fail kemaskini komputer seperti biasa dan dari sumber yang dipercayai, namun apabila pengguna membuka fail tersebut tiada apa yang berlaku. Tetapi, sedar ataupun tidak mereka telah dijangkiti dengan Trojan Horse.

Selain itu, Trojan Horse boleh dijangkiti dengan membuka lampiran (*attachment*) emel, muat naik perisian di Internet, dan menerimanya dari perkhidmatan mesej segera (*instant messaging*).

Rootkit

Rootkit adalah sebuah perisian yang direka untuk menyembunyikan proses atau program-program tertentu daripada kaedah pengesanan yang biasa dan membenarkan akses istimewa secara berterusan kepada komputer. Pemasangan (*installation*) Rootkit boleh secara automatik atau individu yang berniat jahat boleh memasangnya sendiri setelah mendapat akses pentadbir (*administrator*) daripada komputer berkenaan. Pengesanan Rootkit adalah sukar kerana Rootkit mampu memusnahkan perisian yang bertujuan untuk mengesannya.

Sumber: Wikipedia.org

INFORMASI

15 Malware Terkenal YANG HARUS ANDA TAHU !

1 ILOVEYOU

- Juga dikenali sebagai LoveLetter ialah sejenis worm yang menyebarkan dirinya melalui emel dengan menggunakan tajuk ILOVEYOU.
- Worm ini mula tersebar ke seluruh dunia pada 4 Mei 2000.

2 Brain

- Virus komputer yang pertama untuk MS-DOS pada tahun 1986
- Virus ini dibangunkan oleh dua orang adik beradik daripada Lahore, Pakistan iaitu Basit Farooq Alvi dan Amjad Farooq Alvi

3 Klez

- Klez adalah sejenis Worm yang disebarkan melalui emel pada tahun 2001 menerusi fail lampiran (*attachment*) dan tersebar apabila pengguna membuka fail lampiran atau hanya preview mesej email bekenaan

4 MyDoom

- Sejenis Worm yang menjejaskan Microsoft Windows yang boleh mewujudkan *backdoor* dalam sistem operasi komputer mangsa dan merebak melalui emel dan rangkaian *Peer-to-peer* (P2P).

5 Cabir

- Juga dikenali dengan Caribe adalah sejenis Worm yang disebarkan untuk pengguna telefon OS Symbian pada tahun 2004 dan merupakan Worm pertama menyerang telefon bimbit.

6 Morris Worm

- Worm pertama yang tersebar melalui Internet iaitu pada tahun 1988 yang dibangunkan oleh Robert Tappan Morris, seorang pelajar di Universiti Cornell pada ketika itu.
- Dilaporkan Morris Worm telah mengakibatkan kerugian yang dianggarkan sekitar $100,000 - $10,000,000 kepada komputer yang dijangkitinya.
- Robert Tappan Morris disabitkan dengan kesalahan penipuan komputer dan dijatuhkan hukuman tiga tahun percubaan, 400 jam khidmat masyarakat dan denda sebanyak $10,000

7 Nimda

- Sejenis Worm yang mendapat perhatian pada tahun 2001 kerana kepantasan Worm ini merebak iaitu hanya mengambil masa selama 22 minit sahaja untuk menjadi ancaman utama pada ketika itu.

8 Elk Cloner

- Virus Elk Cloner dibangunkan oleh Richard Skrenta pada tahun 1982. Virus ini ditulis untuk Sistem Apple II yang menjadi komputer yang dominan pada ketika itu dan menggunakan floppy disk sebagai medium penyebarannya.

9 Conficker

- Conficker adalah sejenis Worm yang mula dikesan pada tahun 2008 dan disasarkan pada kelemahan Sistem Pengoperasian Windows.
- Mampu untuk melumpuhkan perisian keselamatan sistem seperti Windows Defender atau Microsoft Security Essentials

10 Melissa

- Sejenis virus yang dibangunkan oleh David L. Smith pada Mac 1999. Virus Melissa disebarkan melalui mesej emel dan menamakannya Melissa sempena nama seorang penari eksotik dari Florida.

11 SQL Slammer

- Sejenis Worm yang menyebabkan penafian perkhidmatan pada beberapa *host* Internet dan menyebabkan trafik Internet perlahan
- Ia mengeksploitasi kelemahan dalam Microsoft SQL Server dan produk pangkalan data Desktop Engine.

12 Sasser and Netsky

- Dua jenis worm yang berbeza tetapi dibangunkan oleh orang yang sama iaitu Sven Jaschan yang berasal dari German
- Sven Jaschan dijatuhi hukuman percubaan selama satu tahun sembilan bulan serta perlu melengkapkan khidmat masyarat selama 30 jam.

13 Storm Worm

- Sejenis program Trojan Horse yang dipercayai dicipta di Russia dan mula mejangkiti komputer peribadi pada Januari 2007 dengan menggunakan emel dengan tajuk, *'230 dead as storm batters Europe'* .

14 Stuxnet

- Sejenis Worm yang dihasilkan bersama di antara Amerika Syarikat dan Israel untuk menyerang kemudahahan nuklear di Iran pada tahun 2010
- Kajian penyebaran Stuxnet oleh Symantec menunjukkan Iran, Indonesia dan India adalah negara yang paling terjejas semasa permulaan penyebaran worm ini.
- Penyebaran Stuxnet ke atas kemudahan nuklear di Iran adalah melalui *USB stick*

15 Code Red

- Code Red adalah sejenis worm yang menyerang Web Server Microsoft IIS dan serangannya diketahui umum pada bulan Julai 2001.
- Dipercayai dilancarkan dari negara China, Code Red mengekploitasi kelemahan pada perisian Microsoft IIS yang membolehkan penyerang mengakses dan mengawal Server
- Dua minggu selepas penyebaran Code Red, tersebar pula Code Red II, sejenis worm seperti Code Red.

Tips Panduan Keselamatan Siber

1 Antivirus

Gunakan perisian antivirus sebagai pelindung utama komputer anda dan pastikan perisian antivirus anda sentiasa dikemaskini *(up to date)*

2 Emel

Jangan buka emel atau lampiran daripada sumber yang tidak diketahui. Sentiasa merasa curiga terhadap apa-apa lampiran emel yang tidak dijangka walaupun anda menerimanya daripada orang yang anda tahu

3 Katalaluan

Gunakan kombinasi katalaluan yang sukar untuk diceroboh seperti gabungan huruf besar, huruf kecil, nombor dan simbol. Tukar kata laluan setiap 6 bulan

4 Internet

Putuskan sambungan Internet sekiranya tidak digunakan

5 Akses Komputer

Jangan berkongsi akses komputer anda dengan orang yang tidak dikenali. Pelajari risiko perkongsian fail. Elakkan menulis maklumat akses di tempat yang mudah dilihat

6 *Backup*

Sentiasa melakukan *backup* pada komputer anda dan simpan di tempat lain (*External Hard Disk, DVD, USB Flash Drive*)

7 *End Point Protection*

Gunakan aplikasi *Firewall* untuk melindungi komputer anda daripada penceroboh Internet

8 *Patching/Update*

Kerap memuat turun kemaskini keselamatan dan *patch* untuk sistem operasi dan perisian lain

Sumber: www.georgiahealth.edu

Arab Saudi ancam penggantungan aplikasi popular Telefon Pintar

Aplikasi Viber yang menyediakan kemudahan kepada penggunanya untuk melakukan panggilan percuma, permesejan segera dan perkongsian fail melalui internet telah pun diharamkan oleh Suruhanjaya Komunikasi dan Teknologi Maklumat, Arab Saudi (CITC). Pengharaman ini adalah kerana aplikasi Viber gagal untuk mematuhi keperluan peraturan dan undang-undang yang dikuatkuasakan di negara berkenaan.

Selain aplikasi Viber, aplikasi Skype dan Whatsapp juga menerima amaran daripada pihak suruhanjaya untuk menyediakan Server di negara Arab Saudi bagi memantau kegiatan pengguna. Pengharaman aplikasi Viber ini juga dilihat sebagai satu amaran jelas dari Kerajaan Arab Saudi bagi aplikasi WhatsApp dan Skype mematuhi apa yang diminta oleh negara berkenaan.

Sumber: uk.reuters.com

Seminar Digital Marketing

LES' COPAQUE PRODUCTION SDN. BHD

media prima skali

PENGENALAN

Pemasaran digital boleh ditakrifkan sebagai mempromosi jenama atau produk dan perkhidmatan yang menggunakan segala bentuk pengiklanan digital. Pemasaran digital menggunakan televisyen, radio, Internet, telefon bimbit dan apa-apa bentuk media digital untuk mencapai pelanggan tepat pada masanya, relevan, peribadi dan kos efektif.

OBJEKTIF

Seminar ini mempunyai objektif untuk memberi maklumat kepada para peserta mengenai potensi *digital marketing* sebagai satu kaedah pemasaran yang berkesan dan efektif untuk mempromosi dan menjual produk atau perkhidmatan kepada pelanggan.

KETETAPAN

TARIKH : 3 September 2013
MASA : 9.00 pagi - 1.00 petang
TEMPAT : Auditorium Seri Negeri
BAYARAN : PERCUMA

SKMM
Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

MAKLUMAT STATISTIK KOMUNIKASI DAN MULTIMEDIA SUKU 1 2013 NEGERI MELAKA

Peratusan Kadar Penembusan Jalur Lebar Per 100 Isi Rumah	3.9% ↓ 64.9%
Bilangan Lokasi Hotspot	30% ↑ 1319 lokasi
Kadar Penembusan Talian Ibusawat Terus Per 100 Isi Rumah	6.5% ↓ 47.1%

Sumber: SKMM

Tertekan
dengan masalah keselamatan siber yang sering anda hadapi ?

Cyber999

Hubungi Pusat Bantuan Cyber999 untuk melaporkan aduan anda

CyberSecurity MALAYSIA

Maklumat Lanjut:

http://www.cybersecurity.my

CARANYA :

ADUAN MELALUI LAMAN WEB
http://mycert.org.my/report_incidents/online_form.html

ADUAN MELALUI EMEL
cyber999@cybersecurity.my

ADUAN MELALUI SMS
Taip [CYBER999 REPORT] [emel] [aduan] hantar ke 15888

ADUAN MELALUI TELEFON
Dail 1 300 88 2999 (waktu bekerja)
Dail 019-2665850 (24 jam)

ADUAN MELALUI FAKS
Hantar kepada 03-89453442 (waktu bekerja)