Copyright © September 2023

Pertemuan X

10. Pengenalan dan Penanggulangan Spyware, Adware dan Spam

10.1 SPYWARE

Spyware pada awalnya digunakan untuk hal – hal yang positif. Pertama kali muncul dipublik pada bulan Oktober 1995 di Usenet dalam sebuah artikel yang ditujukan pada proses bisnis Microsoft.

Usenet adalah sistem diskusi internet terstruktur dimana pengguna nya dapat berikirm email. Ada dugaan juga bahwa 2 tahun sebelumnya tehnik mata – mata ini sudah digunakan oleh militer pada hardware untuk melakukan spionase data. Alat ini ditemukan terpasang pada komputer korban, pada server jaringan maupun juga pada ISP (Internet Service Provider).

Dalam tahun – tahun Spyware mulai banyak bermunculan dan dikenal sebagai peralatan mengintip atau kamera tersembunyi yang ada dalam komputer. Pertama kali Spyware dapat ditangkap oleh Honeypot dan berawal dari ide Clifford Stoll yang ingin membuat sistem untuk monitoring aktifitas penyerang (hacker).

Lalu pada tahun 1999 Steve Gibson menemukan adanya aplikasi yang memasang iklan dengan menampilkan pop – up window di komputer nya. Gibson juga mendapati aplikasi ini ternyata mampu mengambil informasi yang ada pada komputernya. Kemudian pada tahun 2000 barulah keberadaan Spyware dipopulerkan oleh Gregor Freund sang pendiri Zone-labs. Hal ini dilakukan pada peluncuran Firewall Zonealarm.

Pada tahun 2005 AOL dan National Cyber Security Alliance mengadakan survey terhadap komputer – komputer yang ada di Amerika. Dan hasilnya cukup mengejutkan ketika ditemukan fakta bahwa 61% pengguna komputer telah terinfeksi Spyware. Data lain juga dimunculkan pada tahun 2006 yakni ketika perusahaan Webroot yang membuat aplikasi Spy Sweeper juga mengeluarkan laporan bahwa 9 dari 10 yang terhubung ke internet telah terinfeksi Spyware. Pada saat itu browser Internet Explorer adalah yang paling rentan tereksploitasi Spyware.

Spyware adalah Software yang melacak penggunaan Internet dan melaporkannya ke pihak lain, seperti pembuat Iklan. Biasanya proses pelacakan tidak diketahui oleh pengguna software tersebut.

Copyright © September 2023

Dewasa ini spyware sudah dijadikan alat untuk mencari data pribadi pada sebuah computer dan menjadikan komputer korban sebagai mata-mata tanpa diketahui pemiliknya.

Lanjutan

Spyware adalah jenis program yang menyerang komputer dengan memata-matai komputer. spyware dan malware memiliki kesamaan yaitu kemampuan untuk mengumpulkan dan mendistribusikan informasi pribadi tanpa izin Anda. Spyware juga dapat mengirim dan membuat sumber daya komputer dan informasi yang tersedia untuk penerima tidak dikenal atau pengguna remote tanpa sepengetahuan atau izin.

Spyware dan malware adalah metode yang mungkin untuk pencurian identitas sejak pemilik atau pengguna komputer tidak tahu tentang atau tidak memberikan izin mereka untuk instalasi dan penggunaan program tersembunyi atau file.

10.2 mengenali Spyware

Salah satu cara kerja dari Spyware agar bisa menyusup ke komputer tanpa diketahui adalah dengan menyusup ke situs tertentu sebelumnya atau bahkan melalui email. Jadi ketika anda mengklik situs tersebut maka secara tidak langsung membuka jalan bagi Spyware, hal yang sama juga terjadi melalui pesan email oleh karena itu hindari membuka pesan yang mencurigakan dalam email anda.

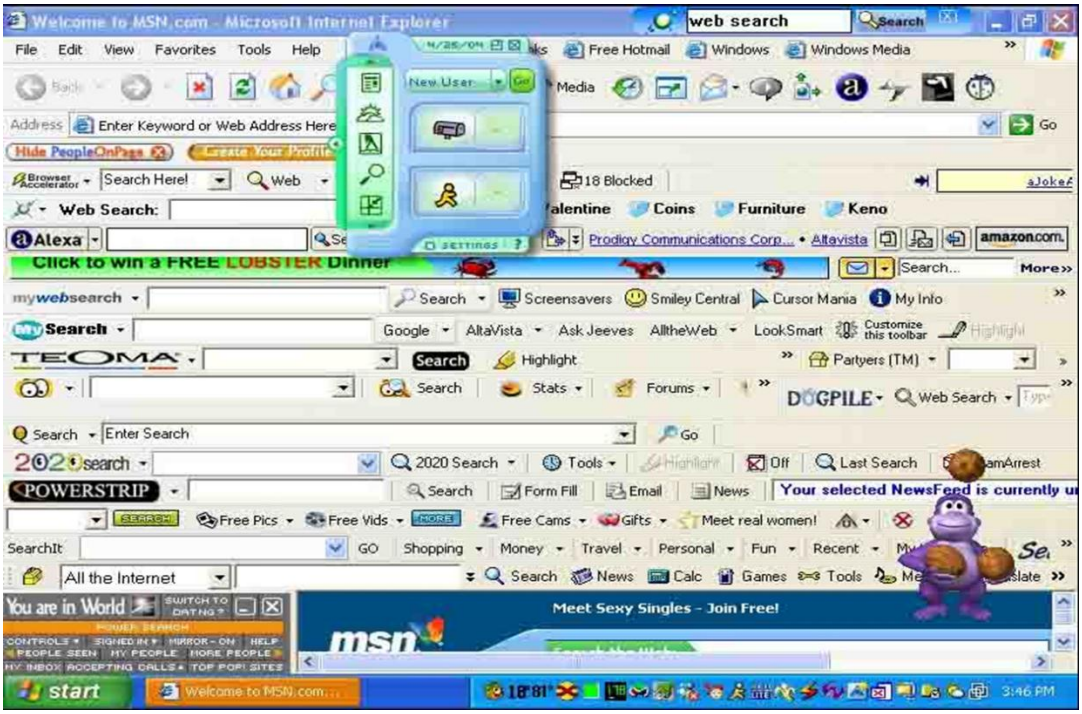
Selain itu cara paling umum dalam penyusupan Spyware adalah ketika anda menginstall Freeware (software gratis). Sebelum menginstall biasanya terdapat kesepakatan lisensi EULA (End User License Agreement) yang secara implisit menjelaskan bahwa pengguna menyetujui segala tindakan pengembang dengan tujuan untuk meningkatkan layanan, termasuk juga dengan menanam Spyware ke dalam komputer anda. Dengan adanya kesepakatan ini juga membuat penyebaran Spyware lolos dari jerat hokum karena menggunakan campur tangan pengguna juga.

Gejala computer terkena spyware :

1. Komputer menjadi lambat, bahkan jika dijalankan tanpa menggunakan banyak program.
2. Perubahan setting browser dimana user merasa tidak pernah merubah atau menginstalnya. Banyak kasus start page browser berubah tanpa sebab yang jelas dan bahkan tidak bisa dirubah walaupun secara manual.
3. Gejala lain munculnya toolbar yang menyatu dengan komponen toolbar browser.
4. Aktivitas mencurigakan. Banyak user melaporkan komputer mengakses harddisk tanpa campur tangan user. Koneksi Internet menunjukkan aktivitas, meskipun user tidak menggunakannya.
5. Munculnya icon-icon baru yang tidak jelas pada tray icon. Semuanya ini menandakan adanya aktivitas background yang sedang bekerja pada komputer user.

6. Muncul iklan pop up setiap kali user terkoneksi dengan Internet. Pop up ini akan muncul terus-menerus walaupun sudah diclose secara manual. Isi dari pop up tersebut bahkan tidak ada hubungannya dengan situs yang sedang dibuka oleh user. Pop up tersebut dapat berupa tampilan situs porno atau junk site lainnya.

10.2.1 Contoh Spyware



10.2.2 Bagaimana Cara Penularan SPYWARE ?

1. Umumnya program jenis spyware masuk secara langsung dengan mengelabuhi pemakai internet. Bisa saja seseorang yang membuka sebuah website dan secara tidak sengaja menerima sebuah peringatan dan melakukan apa yang di kehendaki oleh si pembuat web.
2. Spyware dapat menular lewat beberapa software yang di gunakan untuk pertukaran file video, musik dan gambar.

Program yang di distribusikan bersama spyware

- BearShare [39]
- Bonzi Buddy[40]
- Dope Wars[41]
- ErrorGuard[42]

Copyright © September 2023

- Grokster[43]
- Kazaa[44]
- Morpheus[45]
- RadLight[46]
- WeatherBug[47]
- EDonkey2000[45]
- Sony's Extended Copy Protection termasuk memasukan spyware pada cd instalasinya melalui autorun. Hal ini mengundang kontroversi ketika ditemukan.
- WildTangent[48], Antispyware program seperti CounterSpy mengatakan tidak masalah menggunakan WildTangent, tetapi dikemudian hari mengatakan software tersebut ternyata mendistribusikannya bersama adware. [1]

10.2.3 Bahaya Spyware

1. Dapat menghabiskan resource system komputer ,

   seperti memori dan space hard disk.
2. Mengganggu privasi user dengan memberikan informasi keluar mengenai kebiasaan user menggunakan komputer.
3. Jika suatu program spyware menginstall program "keylogger", maka program tersebut dapat merekam aktivitas pengetikan tombol keyboard dan mengirimkannya ke pihak lain.
4. Beberapa program spyware kenyataannya adalah Trojan yang memungkinkan seseorang masuk kedalam komputer user dan menggunakannya untuk mengirimkan email spam ataupun serangan-serangan "tak bertuan" ke komputer lain dalam jaringan Internet.

10.2.4 Pencegahan SPYWARE ?

- Memperhatikan apa saja file yang di download atau di jalankan.
  - ✓ Jangan mendownload file dari sumber yang tidak jelas termasuk web link atau program yang dikirimkan via email atau messenger (YM, IM dll).
  - ✓ Mencari informasi tentang software yang akan di download atau digunakan.
- Tidak melakukan browsing ke situs-situs yang berbahaya

  seperti situs porno, situs penyedia Cracks atau situs lyric lagu.
- Lakukan windows update secara teratur

10.2.5 Kebiasaan yang baik dalam browsing internet

- Tidak meng-klik kata next pada situs tertentu. Umumnya situs yang memiliki program kutu internet mencoba mengakali pemakai internet. Cara menjebak pemakai banyak dilakukan oleh site site porno gratis atau software gratis misalnya dengan memberikan warning anda harus berumur 17 tahun dan anda harus menyetujui dengan meng-click icon mereka.
- Jangan meng-click sebuah link bila anda tidak yakin mendapatkan sebuah email yang tidak jelas pengirimnya.
- Berhati hati dengan aplikasi program yang digunakan secara gratis / freeware.

Untuk keamanan lebih baik, gunakan browser alternatif Misalnya Mozilla FireFox, AdvantBrowser, NetCaptor yang memiliki tambahan sistem pengaman untuk melakukan blocking pop windows.

Gunakan program Anti Spyware untuk dapat mencegah masuknya program yang akan mengganggu dan menyerang computer, diantaranya :

1. Spyware Doctor
2. Xoftspy SE Antispyware
3. Norton Internet Security
4. Webroot Spy Sweeper
5. CounterSpy
6. Yahoo Toolbar with Anti-Spy

10.3 ADWARE

Adware adalah istilah dalam dunia teknologi yang berasal dari bahasa Inggris. Dalam bahasa tersebut, adware terdiri dari dua kata: Ad yang berarti iklan dan Ware yang berarti barang atau aplikasi.

Adware adalah bentuk lain dari malware dan persis seperti namanya, perangkat lunak dengan tujuan promosi atau iklan. Adware biasanya terdapat didalam software freeware yang kita download.

Meskipun beberapa program memberikan pilihan untuk tidak menginstal adware ekstra, banyak sekali software gratis menambahkan adware didalamnya tanpa sepengetahuan kita.Adware sebenarnya difungsikan sebagai promosi atau iklan berbentuk banner yang dimasukan secara tersembunyi oleh pembuat program. Umumnya program diberikan secara gratis, tetapi dengan kompensasi pemakai harus menerima iklan pada program.

Copyright © September 2023

Iklan yang ditampilkan oleh Adware berbeda, ada beberapa yang sangat menjengkelkan, seperti tampilan pop-up di desktop atau iklan yang ditampilkan di browser menggunakan mesin pencari khusus.

Dengan semakin mudahnya akses di Internet, kita dapat dengan mudah mengambil informasi yang kita butuhkan. Kebutuhan informasi kami sangat tinggi melalui media internet ini sehingga digunakan oleh sekelompok orang untuk menghasilkan pendapatan material. Ada banyak cara untuk mendapatkan uang dari Internet, dari cara yang sangat bersih hingga cara yang tidak adil.

Terkadang pemakai ingin mengunakan program shareware tetapi didalamnya terdapat program yang difungsikan sebagai Adware.

Contoh Adware:

1. Misalnya Program A yang diberikan secara gratis, ternyata memiliki jendela kecil pada program dan terus berganti ganti gambar iklan.
2. Yahoo messenger dan pemilik Yahoo menempatkan banner iklan pada sebuah bagian di program Yahoo chat.

10.3.1 Pencegahan Adware :

1. Tidak membuka email atau lampiran email dari pengirim yang tidak dikenal.
2. Block atau tidak mengklik jendela pop-up yang mencurigakan.
3. Jangan membuka file yang tergolong terkait dengan malware seperti .bat, .com, .exe, .pif, .txt.vbs, .htm.exe atau .vbs dan sebagainya
4. Tidak download dan menginstall aplikasi selain dari sumber terpercaya.
5. Hindari penipuan berupa phising, atau hal hal yang mencurigakan
6. Gunakan update software anti-virus dan anti-spyware secara teratur.

10.4 SPAM

Spam adalah suatu e-mail yang membawa pesan-pesan yang sifatnya komersial (bisa menjual jasa, barang atau menawarkan sesuatu hal yang menarik). Bisa dianalogikan sebagai suatu junk e-mail yang masuk ke dalam mailbox. Spam sering kali tidak membawa pesan yang penting bagi pemilik email dan sangat merugikan pengguna E-mail

Lanjutan

kata spam itu sendiri adalah singkatan dari Sending and Posting Advertisement in Mass. Ini berarti salah satu ciri khas pesan spam adalah pesan promosi yang dikirimkan secara massal.

Pesan spam seringkali ditemukan dalam kotak masuk email dan bahkan inbox ponsel Anda. Biasanya, pesan ini berisi konten iklan yang tidak diinginkan oleh penerima pesan.

Motif utama dari spam adalah untuk mempromosikan sebuah produk atau layanan. Bahkan, Spam Laws menunjukan bahwa 36% dari seluruh pesan spam yang dikirim tiap harinya berisi iklan.

10.4.1 Sejarah SPAM

Spam pertama terjadi pada bulan Mei 1978 di jaringan Arpanet sebelum internet terbatas dalam lingkup militer dan akademis diprakarsai oleh seorang pekerja Digital Equipment Corporation (DEC).

Spammer pertama tersebut menyalin daftar alamat e-mail pada pengguna Arpanet dan mengetiknya satu persatu dalam field *carbon copy* (CC) yang hanya mampu menampung sebanyak 320 alamat E-mail. Setelah Arpanet berkembang menjadi Internet, pesan yang tergolong kedalam spam pertama dikirimkan seorang mahasiswa bernama Dave Rhodes, dengan judul E-mail “Make.Money.Fast!!” dan mem-postingnya di Usenet (*newsgroup*).

Masih pada tahun yang sama, dua orang pengacara AS, Cantor dan Siegel mengirimkan pesan iklan “Green Card Lottery” kepada 6000 newsgroup dalam waktu yang bersamaan sehingga menyebabkan server Usenet collapse sebanyak 15 kali.

10.4.1.1 Jenis –Jenis pesan SPAM:

1. Spam Promosi

Jenis spam pertama adalah spam promosi yang memiliki tujuan untuk mempromosikan sebuah produk atau layanan yang ditawarkan oleh sebuah brand. Spam jenis ini relatif tidak berbahaya dan tidak menimbulkan ancaman bagi penerima.

2. Spam Malware

Jenis spam yang sering ditemui kedua adalah spam malware. Pesan spam malware biasanya berisi file jahat yang bertujuan untuk menyebarkan virus dan menginfeksi sistem operasi perangkat penerima.

Copyright © September 2023

Tujuan utama dari virus malware ini juga bervariasi. Seringnya, spam jenis ini digunakan untuk mencuri data penerima atau untuk merusak data yang ada perangkat.

Metode yang digunakan untuk memasukan malware ke perangkat biasanya ada dalam format unduhan, gambar, atau external link yang akan dibuka penerima.

Baca Juga: 10 Cara Menghilangkan Malware Paling Efektif

3. Spam Phishing

Sebenarnya, phishing scam adalah salah satu bagian dari spam malware. Sejatinya, phishing adalah praktik penipuan dimana spammer berpura-pura menjadi brand terkenal yang memberikan promosi dan hadiah.

Tujuan utama dari phising spam adalah agar korban bersedia untuk memberikan informasi penting kepada spammer tanpa curiga.

Biasanya, pesan spam phishing akan terlihat persis seperti brand yang ditiru. Mulai dari headline, subject pesan, hingga nama dari pengirim.

Namun jika Anda perhatikan baik baik, biasanya nomor dan alamat email pengirim spam phising bukan berasal dari nomor atau email bisnis yang valid.

4. Spam Penipuan

Spam penipuan bisa dianggap sebagai salah satu jenis spam paling berbahaya untuk penerima. Tujuan utama pesan ini adalah untuk menipu penerima dengan penawaran hadiah yang cukup besar.

Spammer akan mengirimkan pesan yang berisi tentang pengumuman event undian hadiah atau semacamnya.

Copyright © September 2023

Nantinya, saat penerima membalas pesan tersebut, spammer akan meminta penerima untuk mengirimkan data pribadi dan sejumlah uang sebelum mereka bisa mendapatkan hadiah yang dimenangkan.

Metode lain dari spam penipuan bisa terjadi dalam bentuk "mama minta pulsa" yang sempat viral beberapa tahun lalu itu.

Spammer akan berpura-pura menjadi sosok dekat yang dipercaya oleh korban dan mereka akan meminta bantuan dalam bentuk uang.

Biasanya, spammer akan berpura-pura berada dalam masalah besar agar korban mau mengirimkan uangnya dengan segara.

10.4.1.2 contoh Spam di kehidupan sehari-hari

1. Spam Email

Spam melalui email adalah spam yang paling sering ditemukan saat ini. Bentuk spam email ini adalah mengirimkan surat elektronik komersial secara massal yang tidak diminta oleh si penerima email.

Pengiriman spam email ini bisa dilakukan melalui 'jaringan zombie' jaringan virus yang telah menginfeksi komputer pribadi maupun kantor di seluruh dunia. Namun, spam email juga banyak terjadi karena pengguna internet mendaftarkan email mereka pada website tertentu.

2. Spam SMS

Spam SMS atau pesan instan juga cukup jamak terjadi saat ini. Tujuan spam SMS pun cukup beragam, namun kebanyakan bertujuan untuk promosi barang atau jasa, dan penipuan.

Spam SMS ini dilakukan dengan menggunakan software SMS blast yang dapat mengiriman pesan instan secara massal ke nomor ponsel.

3. Spam Komentar di Blog

Spam melalui komentar di blog juga merupakan salah satu momok yang cukup mengganggu para blogger atau pemilik website. Pasalnya, saat ini komentar spam di blog dilakukan dengan menggunakan software khusus sehingga komentar spam di sebuah blog jumlahnya sangat banyak.

4. Spam Mesin Pencari

Spam mesin pencari disebut juga dengan spamdexing, singkatan dari spamming dan indexing. Tujuan spamdexing ini adalah untuk menempatkan halaman-halaman situs spam di mesin pencari dengan pencarian yang relevan sehingga mendapatkan trafik dari mesin pencari.

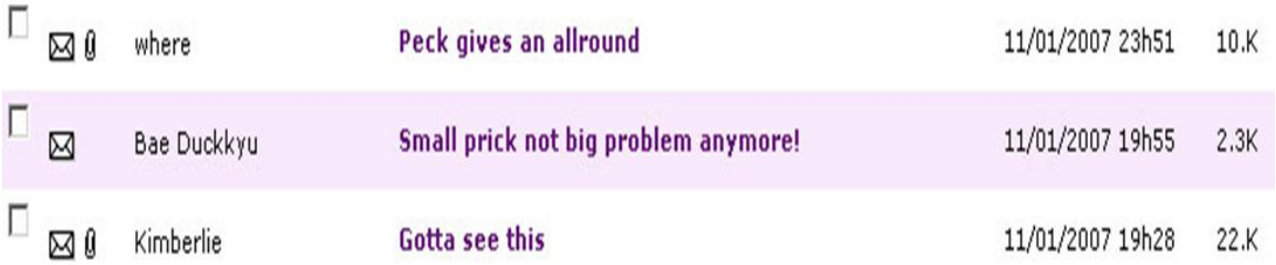
10.4.2 Mencegah Penyebaran SPAM

- Memfilter e-mail yang masuk kedalam mail box dengan mensetting konfigurasi pada e-mail tersebut.

  Contoh: Yahoo.com, Gmail.com dsb.

- Untuk outlook express, firebird, dan program email client yang lainnya dapat di atur dari setting/konfigurasi software tersebut.

Contoh Email Spam



where	Peck gives an allround	11/01/2007 23h51	10.K
Bae Duckkyu	Small prick not big problem anymore!	11/01/2007 19h55	2.3K
Kimberlie	Gotta see this	11/01/2007 19h28	22.K

Copyright © September 2023

Copyright © September 2023

Copyright © September 2023

Copyright © September 2023