

KEAMANAN INFORMASI

13. MALWARE & COMPUTER FORENSICS

Doni Abdul Fatah
github.com/doniaft
Universitas Trunojoyo Madura

Pokok Bahasan

01. Pengantar Keamanan Informasi

02. Pemodelan Serangan (Attack Tree)

03. Sistem Keamanan Informasi dan Internet

04. Autentikasi

05. Kontrol Akses

06. Firewall dan Intrusion Detection System

07. Network Attack

08. Kriptografi

09. Kriptografi Asimetrik

10. Biometric Authentication

11. Public Key Infrastructure

12. Protokol Keamanan

13. Malware & Computer Forensics

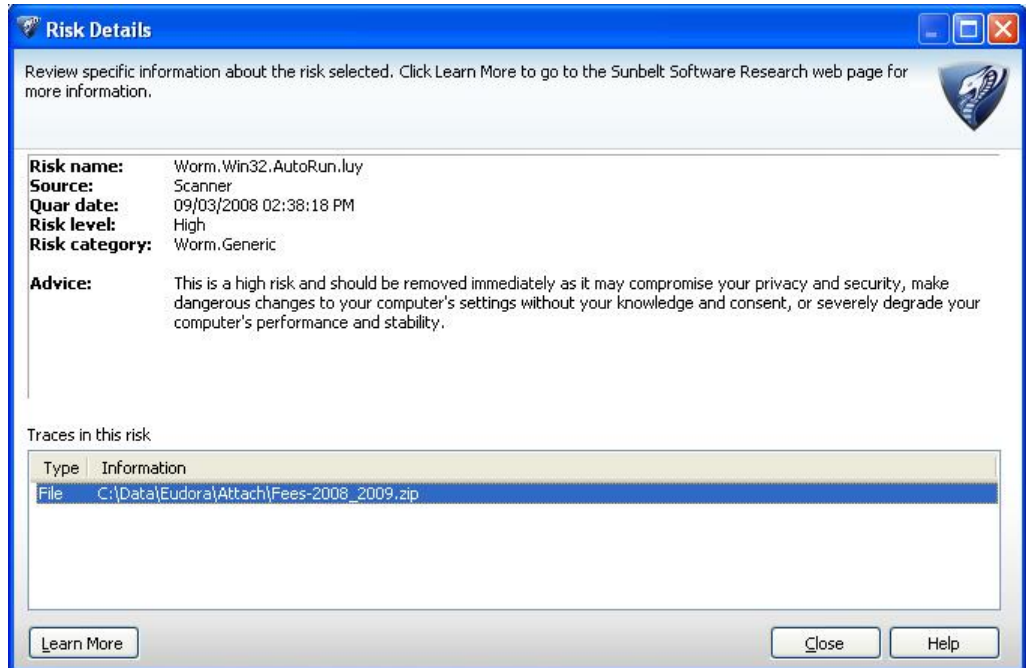
14. UAS

01. Keamanan Informasi

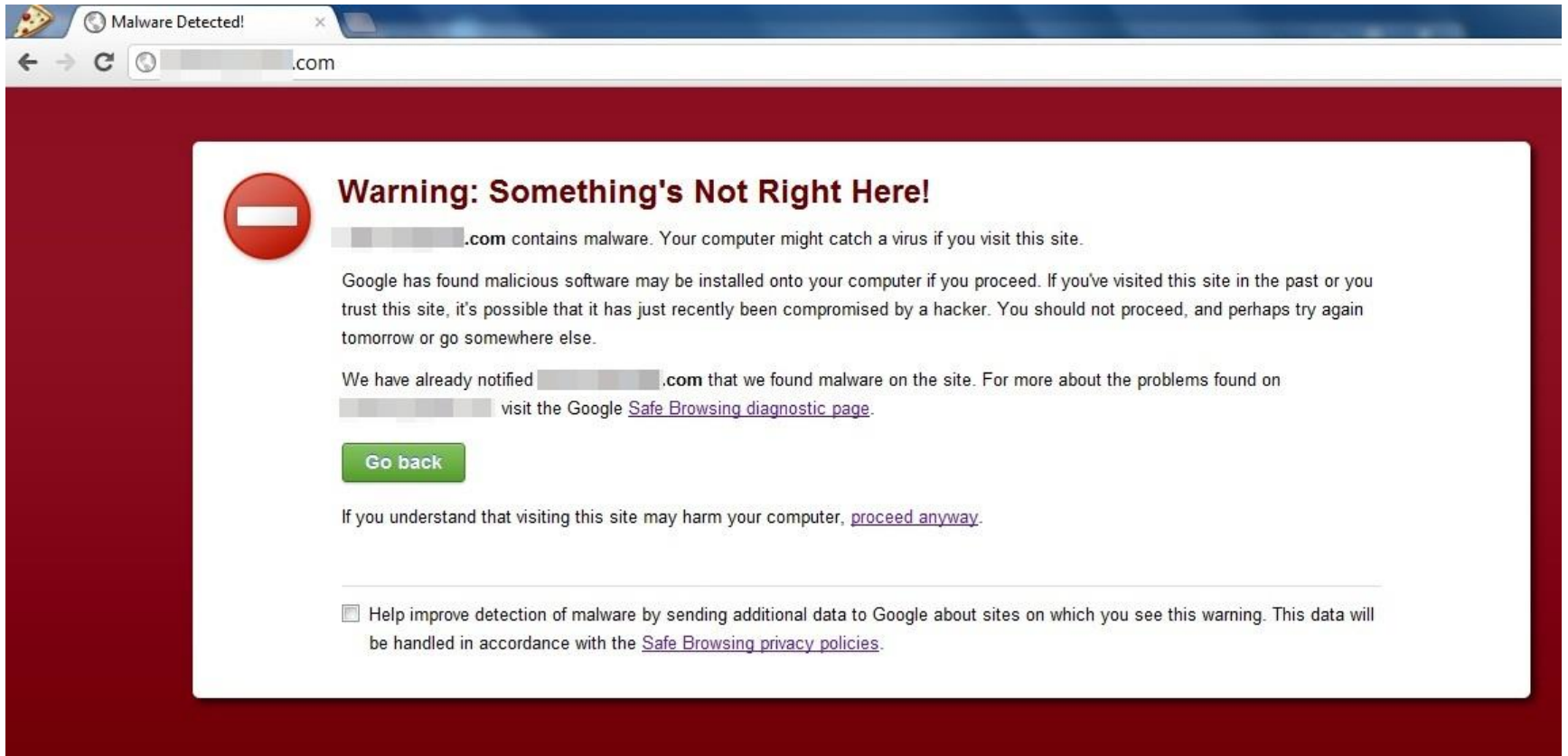
- 1) Malware & Computer Forensics
- 2) Contact
- 3) Referensi

13. Malware & Computer Forensics

Malware



Malware



Pengertian Malware

- ❑ Malicious Software atau Malware adalah program komputer yang diciptakan dengan maksud dan tujuan utama mencari kelemahan software, malware juga dapat berupa script atau kode.

Serangan Berbasis Software

☐ Software berbahaya atau **malware**

- ☐ Software masuk kedalam sistem komputer tanpa sepengetahuan pemilik

- ☐ Malware adalah istilah umum yang mengacu pada berbagai perangkat lunak yang merusak atau mengganggu

☐ Tujuan malware:

- Menginfeksi sistem komputer
- Dengan cara menyembunyikan tindakan jahat ini
- Membawa keuntungan dari yang dilakukan

Jenis-jenis Malware

- ☐ Virus
- ☐ Worm
- ☐ Wabbit
- ☐ Keylogger
- ☐ Browser hijacker
- ☐ Trojan horse
- ☐ Spyware
- ☐ Backdoor
- ☐ Dialer
- ☐ Exploit dan rootkit
- ☐ BOTS
- ☐ Phishing
- ☐ Spam
- ☐ Spyware
- ☐ Adware

Malware (Menginfeksi)

❑ Virus

- Program yang bersembunyi menyerang dokumen lain atau program dan mengeksekusi ketika dokumen atau program tsb di buka.
- Setelah virus menginfeksi komputer, ia melakukan dua tugas terpisah
 - Menyebar ke komputer lain
 - Mengaktifkan tujuan jahatnya
- Masalah yang terjadi yaitu mulai menampilkan pesan menjengkelkan, menghapus file, atau menyebabkan komputer crash berkali-kali

Malware (Menginfeksi) (continued)

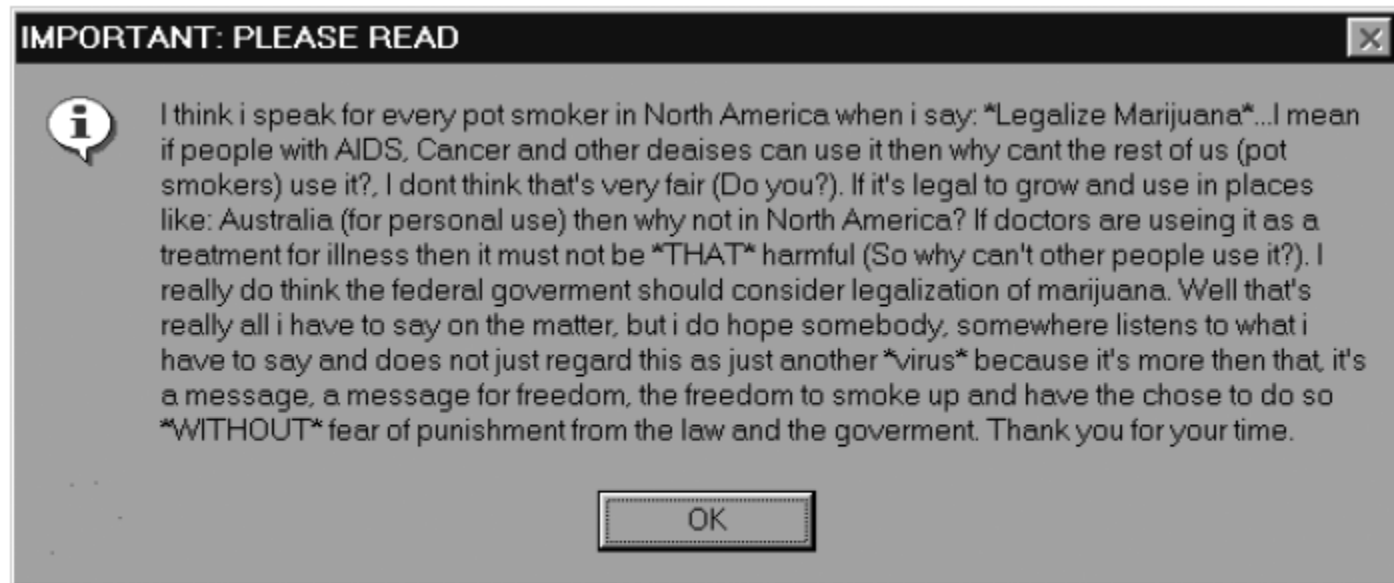


Figure 2-1 Annoying virus message

Malware (Menginfeksi) (continued)

❑ Jenis-jenis Virus Komputer

- File infector virus
- Resident virus (menginstall kode berbahaya ke memori)
- Boot virus (memakai bagian disk untuk booting)
- Companion virus (berpura-pura menggantikan file yang akan diakses pengguna)
- Macro virus (di-code-kan sebagai sebuah *macro* yang melekat pada sebuah dokumen)

❑ **Metamorphic viruses**

- Menghindari deteksi dengan mengubah bagaimana mereka muncul

❑ **Polymorphic viruses**

- Juga mengenkripsi konten mereka secara berbeda setiap kali

Malware (continued)

❑ Worm

- Program yang dirancang untuk mengambil keuntungan dari kerentanan dalam aplikasi atau sistem operasi dalam rangka untuk memasuki sistem
- Worm berbeda dengan virus, yaitu:
 - Sebuah worm dapat melakukan perjalanan dengan sendirinya
 - Sebuah worm tidak memerlukan tindakan pengguna untuk memulai pelaksanaannya
- Tindakan yang dilakukan oleh worm: menghapus file pada komputer, sehingga komputer sebagai remote kontrol bagi penyerang

Malware

❑ Trojan Horse (kuda Troya) /(Trojan)

- Perangkat lunak yang mencurigakan (*malicious*) yang dapat merusak sebuah sistem atau jaringan.
- Tujuannya :
 - memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain)
 - mengendalikan target (memperoleh hak akses pada target).
- seolah-olah program tersebut merupakan program baik-baik
- Trojan dapat menginfeksi sistem ketika pengguna mengunduh aplikasi dari sumber yang tidak dapat dipercayai

Malware

- ❑ Contoh Jenis-jenis Trojan
 - Pencuri *password*:
 - Pencatat penekanan tombol (*keystroke logger/keylogger*): Jenis Trojan ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang
 - Tool administrasi jarak jauh (*Remote Administration Tools/RAT*): Jenis Trojan ini mengizinkan para penyerang untuk mengambil alih kontrol

Malware (continued)

❑ Rootkit (continued)

- Satu set perangkat lunak yang digunakan oleh penyusup untuk masuk ke komputer, mendapatkan hak istimewa untuk melakukan fungsi yang tidak sah, dan kemudian menyembunyikan semua jejak keberadaannya
- Tujuannya adalah rootkit untuk menyembunyikan kehadiran jenis lain dari perangkat lunak berbahaya
- Rootkit berfungsi dengan mengganti perintah sistem operasi dengan versi modifikasi
 - Yang secara khusus dirancang untuk mengabaikan aktivitas berbahaya sehingga dapat lolos deteksi
- Mendeteksi dan menghapus rootkit sulit dilakukan
 - Dengan mengformat ulang hardisk dan menginstal ulang SO

Malware (continued)

❑ Logic bomb

- Sebuah program komputer atau bagian dari program yang diam sampai dipicu oleh peristiwa logis tertentu
- Sekali terpicu, program dapat melakukan sejumlah kegiatan berbahaya
- Logic bom sangat sulit untuk dideteksi sebelum mereka dipicu

❑ Privilege escalation

- Mengeksploitasi kerentanan dalam perangkat lunak untuk mendapatkan akses ke sumber daya pengguna biasa

❑ Type dari privilege escalation

- Ketika pengguna dengan user tingkat rendah dapat mengakses dengan fungsi seperti user tingkat yang lebih tinggi
- Pengguna yang mempunyai akses terbatas berbeda dengan user yang sama

Malware mencari keuntungan

❑ Spam

- e-mail yang tidak di harapkan
- Mengirim spam adalah bisnis yang menguntungkan
- Biaya yang terlibat untuk spamming:
 - E-mail
 - Peralatan koneksi internet
- Pesan spam berbasis teks dapat dengan mudah oleh terperangkap oleh filter khusus
- Spam gambar menggunakan gambar grafis teks dalam rangka untuk menghindari filter berbasis teks







Subject: U know what i think

← Unsuspecting
subject line

Discount Pharmacy Online

Save up tp 80%

Lowest price guarantee

 viagra \$2.00	 Xanax \$2.00
 Valium \$2.00	 Cialis \$2.00
 Phentermine \$3.88	 Ambien \$2.00

For more information, Please do no click

Just type: **www.AAARX1.org**

in the address bar of you browser, then press the Enter hey

← Image

Mrs. Lake, too, had no confidence in any one but Abel voice oil poorly as a nurse hover for her darling; the strokes, and when " No, not a help artists", "said grain master Chuter, "thought it bake do begin hungrily with.

The retire contrast between the fance natural red of the irritably baby's complexion and its let snowy fine Young Prodigy. " "what bleed are rose you beg doing, evious Bogy? said she. There was a small hook.

← Nonsense text

Figure 2-2 Image spam



Malware for Profit (continued)

- ❑ Teknik yang digunakan para pembuat spam:
 - GIF layering
 - Word splitting (pemisahan)
 - Geometric variance (Perbedaan)

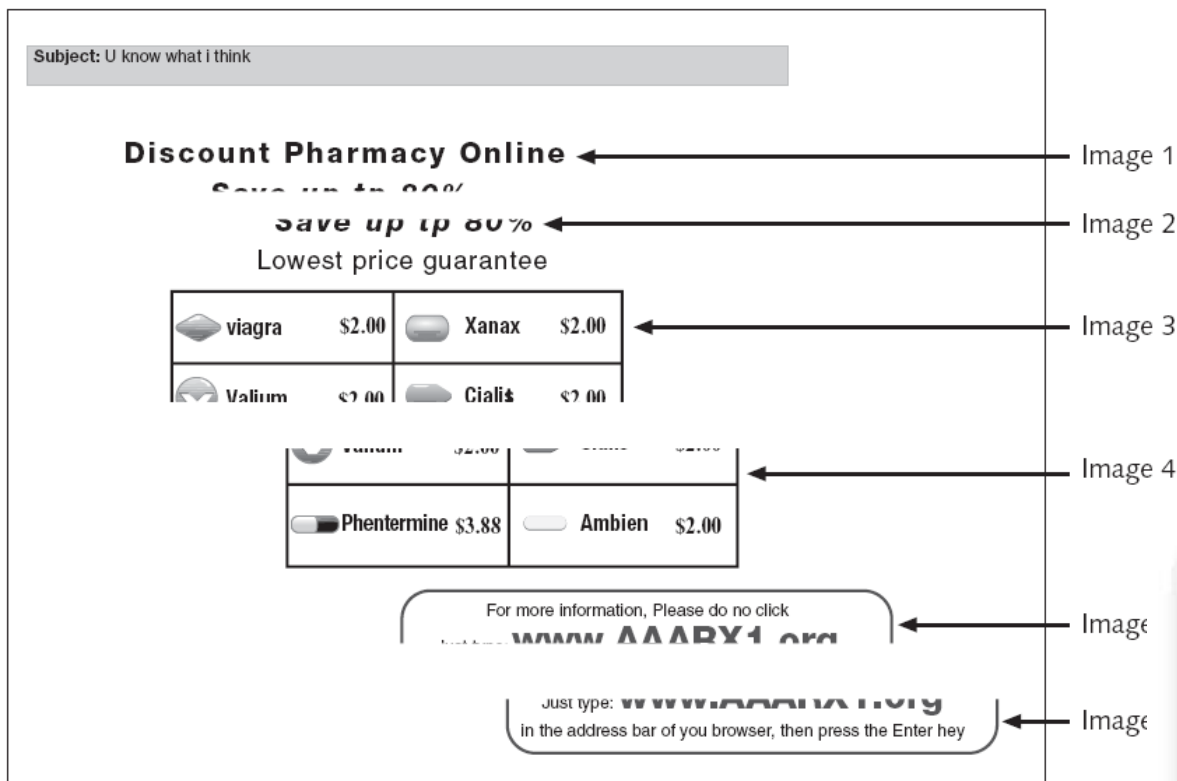


Figure 2-3 GIF layering

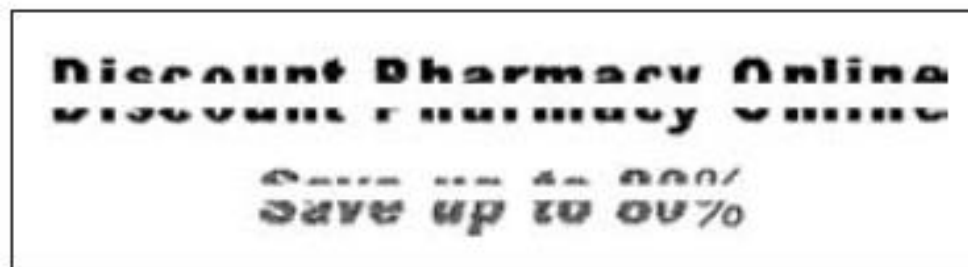


Figure 2-4 Word splitting

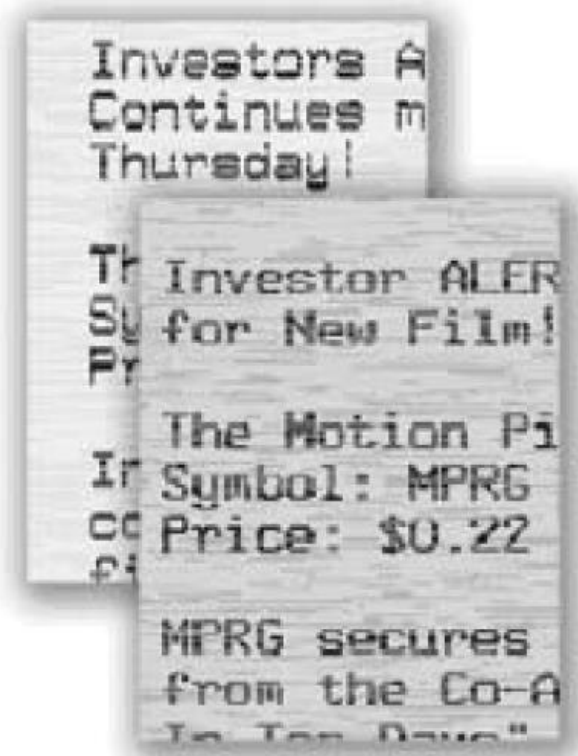


Figure 2-5 Geometric variance

Malware for Profit (continued)

- ❑ Spam gambar tidak dapat dengan mudah disaring berdasarkan pada isi pesan
- ❑ Untuk mendeteksi spam gambar, satu pendekatan adalah untuk menguji konteks pesan dan membuat profil, mengajukan pertanyaan seperti:
 - Siapa yang mengirimkan pesan?
 - Apa yang diketahui tentang pengirim?
 - Dimana user berada jika dia merespon email ini?
 - Apakah sifat dari isi pesan?
 - Bagaimana pesan teknis di baingun?

Malware for Profit (continued)

❑ Spyware

- Istilah yang umum digunakan untuk menggambarkan perangkat lunak yang memaksakan pada privasi pengguna atau keamanan

❑ Kumpulan Antispyware mendefinisikan spyware:

- Teknologi yang digunakan tanpa persetujuan pengguna dan merusak kontrol pengguna berlebihan:
 - Penggunaan sumber daya sistem, termasuk program apa yang diinstal pada komputer.
 - Pengumpulan, penggunaan, dan distribusi pribadi atau informasi sensitif lainnya.
 - Perubahan material yang mempengaruhi pengalaman pengguna, privasi, atau keamanan sistem

Malware for Profit (continued)

- ❑ Spyware mempunyai 2 karakteristik yang membuat sangat berbahaya :
 - Spyware mencari keuntungan
 - Spyware lebih mengganggu daripada virus, sulit untuk di deteksi, dan lebih sulit untuk di hapus
 - Spyware tidak mudah diidentifikasi
- ❑ Spyware sangat luas
- ❑ Walaupun penyerang menggunakan beberapa tool spyware:
 - Ada dua yang paling umum digunakan adware and keyloggers

Malware for Profit (continued)

Effect	Explanation
Slow computer performance	Spyware can increase the time to boot a computer or surf the Internet.
System instability	Spyware can cause a computer to freeze frequently or even reboot.
New browser toolbars or menus	Spyware may install new menus or toolbars to a Web browser.
New shortcuts	New shortcuts on the desktop or in the system tray may indicate the presence of spyware.
Hijacked homepage	An unauthorized change in the default homepage on a Web browser can be caused by spyware.
Increased pop-ups	Pop-up advertisements that suddenly appear are usually the result of spyware.

Table 2-2 Effects of spyware

Malware for Profit (continued)

❑ Adware

- Sebuah program perangkat lunak yang memberikan konten iklan dengan cara yang tak terduga dan tidak diinginkan oleh pengguna

❑ Adware dapat menjadi resiko keamanan

- Beberapa program adware bekerja dengan fungsi pelacakan
 - Memonitor dan melacak aktivitas user
 - Mengirimkan log ke pihak ketiga tanpa izin pemilik

Malware for Profit (continued)

❑ **Keylogger**

- Sebuah perangkat komputer atau program yang memonitor tombol komputer yang sedang di ketik oleh user
- Teks yang diketik tersebut di kumpulkan dan di simpan

❑ Sebagai perangkat keras, keylogger adalah sebuah perangkat kecil yang dimasukkan antara konektor keyboard dan port keyboard komputer

Malware untuk mencari keuntungan (continued)

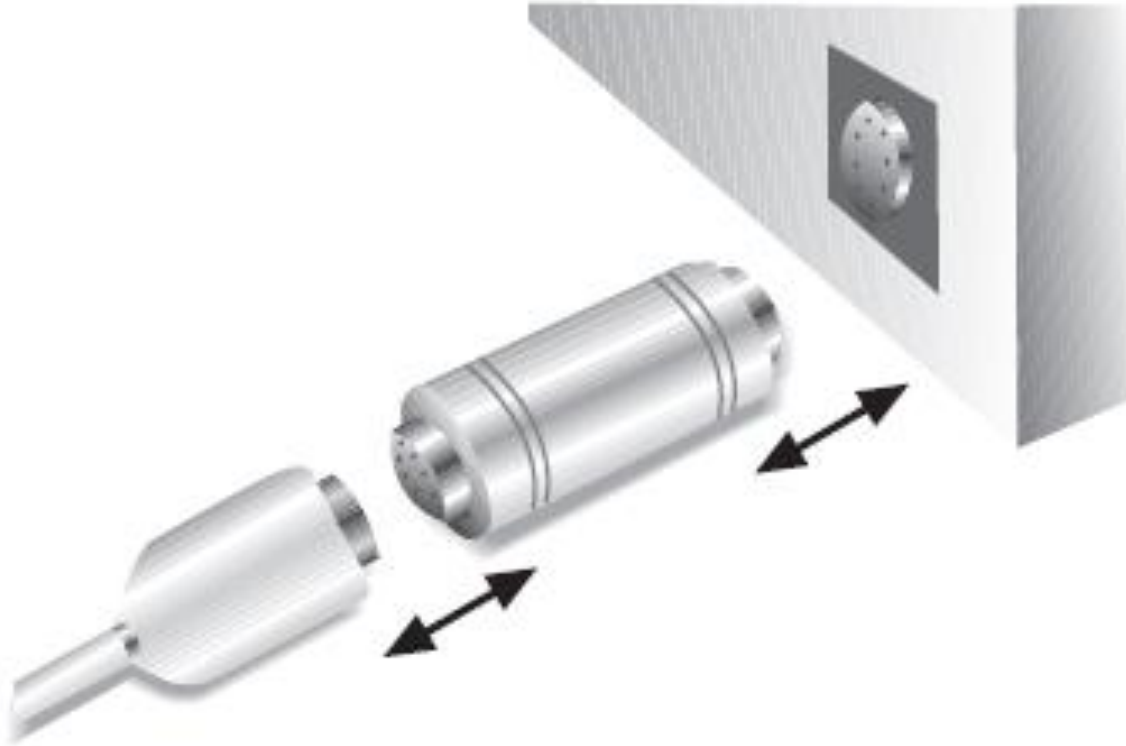


Figure 2-6 Hardware keylogger

Malware mencari keuntungan (continued)

❑ Software keyloggers

- Program yang diam mengcapture semua yang diketikkan oleh user, termasuk password dan informasi sensitif
- Program ini bersembunyi dan sulit di ketahui pengguna

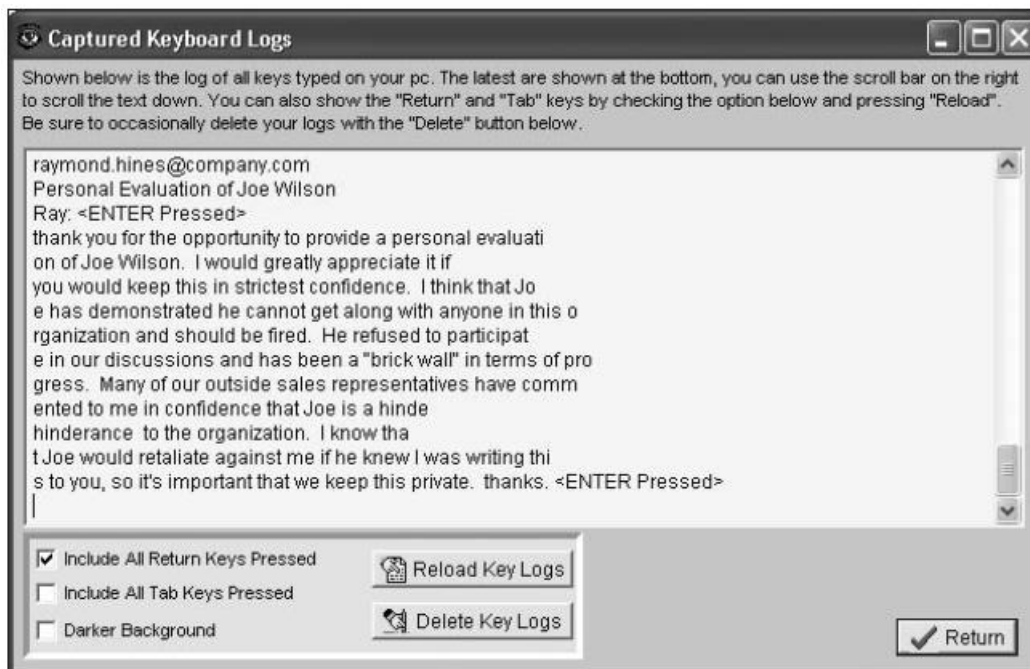


Figure 2-7 Captured information by keylogger

Malware for Profit (continued)

☐ Botnets

- menyusupkan program-program tertentu kepada server-server komputer

☐ **Zombie**

- Sebuah komputer yang terinfeksi dengan sebuah program yang akan memungkinkan penyerang untuk kontrol jarak jauh

☐ Penyerang menggunakan **Internet Relay Chat (IRC)** untuk mengontrol jarak jauh zombie

☐ Penyerang mengetahui sebagai penggembala

Malware for Profit (continued)

Type of Attack	Description
Spamming	A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam. Some botnets can also harvest e-mail addresses.
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker.
Attacking IRC networks	Botnets are often used for attacks against IRC networks. The bot herder orders each botnet to connect a large number of zombies to the victim IRC network, which is flooded by service requests and then cannot function.
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each “vote” by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a Web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Table 2-3 Uses of botnets

Perlindungan Terhadap Virus Komputer

- ☐ Buatlah backup secara teratur.
- ☐ Harus siap untuk menginstal sistem operasi.
- ☐ Melindungi jaringan sambungan dengan Firewall.
- ☐ Gunakanlah antivirus.
- ☐ Meng-update sistem operasi.
- ☐ Membatasi akses ke komputer.
- ☐ Gunakan perlindungan spam.

3) Kontrak Perkuliahan

- a) Tata Tertib
- b) Contact
- c) Referensi

Tata Tertib Perkuliahan SI4B

- ☐ Masuk sesuai jadwal 15.25 WIB, Toleransi keterlambatan adalah 20 menit.
- ☐ Pakaian bebas rapi berkerah, bersepatu.
- ☐ Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- ☐ Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- ☐ Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4C

- ☐ Masuk sesuai jadwal 09.15 WIB, Toleransi keterlambatan adalah 15 menit.
- ☐ Pakaian bebas rapi berkerah, bersepatu.
- ☐ Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- ☐ Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- ☐ Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4D

- ☐ Masuk sesuai jadwal 12.45 WIB, Toleransi keterlambatan adalah 15 menit.
- ☐ Pakaian bebas rapi berkerah, bersepatu.
- ☐ Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- ☐ Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- ☐ Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- ☐ Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Proyek : Kelompok

dibuat 2 s.d 4 Mahasiswa

- ☐ Membuat aplikasi sederhana dengan fokus **Keamanan Informasi dalam Penggunaan Aplikasi/berInternet**
- ☐ **Tahapannya :**
 - ☐ Penentuan Studi Kasus
 - ☐ Membuat aplikasi Login Spoofing Attack
 - ☐ Dalam aplikasi Login Spoofing Attack untuk pemberian passwordnya dilakukan dengan menggunakan teknik Kriptografi (enkripsi) dengan menggunakan enkripsi asimetris
 - ☐ Untuk memecahkan enkripsi tersebut maka dilakukan deskripsi dari enkripsi tersebut.
 - ☐ Untuk Aplikasi boleh Web atau Desktop, sesuai yang dikuasai.
 - ☐ Pembuatan Laporan atau Dokumentasi.
- ☐ **Poin penilaian:** Aplikasi, Dokumentasi, Presentasi.

5) Contact

Contact

- ❑ Bahan Kuliah : github.com/doniaft
- ❑ Email : doniaft@gmail.com
- ❑ WA/Telegram :
- ❑ Komting Keamanan Informasi
 - ❑ SI4C : [Yusril : 0856 5509 5641](#)
 - ❑ SI4D : [Ikrom : 0852 3027 9767](#)
 - ❑ SI4B :
 - ❑ Rahma : : [0852 5707 1554](#)
 - ❑ Adi : [0899 3616 728](#)

6) Referensi

Referensi (1)

- ❑ Anderson, Ross, “Security Engineering”, First Edition, Wiley, 2001, tersedia dalam e-Book : URL: <http://www.cl.cam.ac.uk/~rja14/book.html>
- ❑ Menezes et.al, “Handbook of Applied Cryptography”, Fifth Edition, CRC Printing, 2001, tersedia dalam e-Book URL: <http://cacr.uwaterloo.ca/hac>
- ❑ Bishop, Matt, “Computer Security: Art and Science”, Addison Wesley, 2002
- ❑ Stinson, Douglas R, “Cryptography: Theory and Practice”, CRC Press, 1995
- ❑ Electronic Frontier Foundation, “Cracking DES”, O'Reilly, 1998
- ❑ Stamp, Mark, “Computer Security: Principles and Practices”, Willey, 2011
- ❑ Eric Cole, Ronald Krutz, and James W. Conley, “Network Security Bible”,
- ❑ Wiley Publishing, Inc., 2005.
- ❑ Matthew Strebe, “Network Security Foundations”, Sybex, 2004.
- ❑ Chris McNab, “Network Security Assessment”, O'reilly, 2008.
- ❑ James D. McCabe, dkk, “Network Security Know It All”,Morgan
- ❑ Kaufmann, 2008.
- ❑ Ibisa, “Keamanan Sistem Informasi”, Penerbit Andi, Yogyakarta, 2011