All About
Security & Virus

IndocommIT
12 September 2007
Jakarta Convention Center

Author : Harry Sufehmi
Email : harry@rimbalinux.com
Revision : 20070908

All About the Author

Now : Managing Director @ Rimbalinux.com : Making IT Works. Husband & Father of Four.

2000 – 2005 : Senior Analyst @ Birmingham City Council

Achievements

- Taking control of Nimda epidemic (10.000 desktops, all over a city the size of Bandung)
- Best eGovernment @ Europe http://www.birmingham.gov.uk

1998 : Head of IT @ Asuransi Takaful

History of Virus

FUN / BRAGGING RIGHTS **FINANCIAL/MALICIOUS INTENT**

- 1970 : Creeper : Menyerang Tenex operating system, menyebar melalui ARPANET (cikal bakal Internet)
- 1986 : (c) Brain : Virus pertama yang menyerang PC
- 1987 : Jerusalem : Wabah virus dalam skala global. Menghancurkan file exe setiap Friday 13th
- 1988 : Morris worm : Pertama yang menyebar melalui Internet & memperkenalkan attack vector : *buffer overrun*.
- 1996 : 1260 : first polymorphic virus
- 1999 : Melissa : first wide-scale macro virus
- 2000 : ILOVEYOU : menyebabkan kerugian US$ 5,5 milyar.

History of Virus

FUN / BRAGGING RIGHTS **FINANCIAL/MALICIOUS INTENT**

➔2001 : Ramen / Lion : first worm for (RedHat) Linux (via wu-ftpd, rpc-statd, lpd)

➔ 2003 – 2004 : Slammer, Blaster, Welchia, Sobig, Sober, MyDoom, Witty, Sasser : Menyerang platform Windows, multiple attack vectors.

➔ 2004 : MyDoom : Email worm tercepat, dibuat oleh spammer, 1 juta komputer yang terinfeksi menyerang sco.com (lenyap dari internet, pindah ke thescogroup.com). Biggest DDoS attack. Melumpuhkan Google pada tanggal 26 Juli 2004.

➔ 2005 : Zotob : menginstall malware & menjalankan credit card forgery scam, korban a/l CNN, NYT, ABC, AP, US Dept. Homeland Security, dll. Microsoft mengumumkan imbalan US$ 250.000 bagi yang menangkap pembuatnya, mengerahkan 50 detektif.

➔ 2006 : lOrdOfthenOOse : Menyerang 70 juta anggota MySpace.com

Spread : Virus

- **Executables** : EXE, COM, ..
- **Removable media** : floppy, flashdisc, ..
- **Macro** : Email, Office files, ..

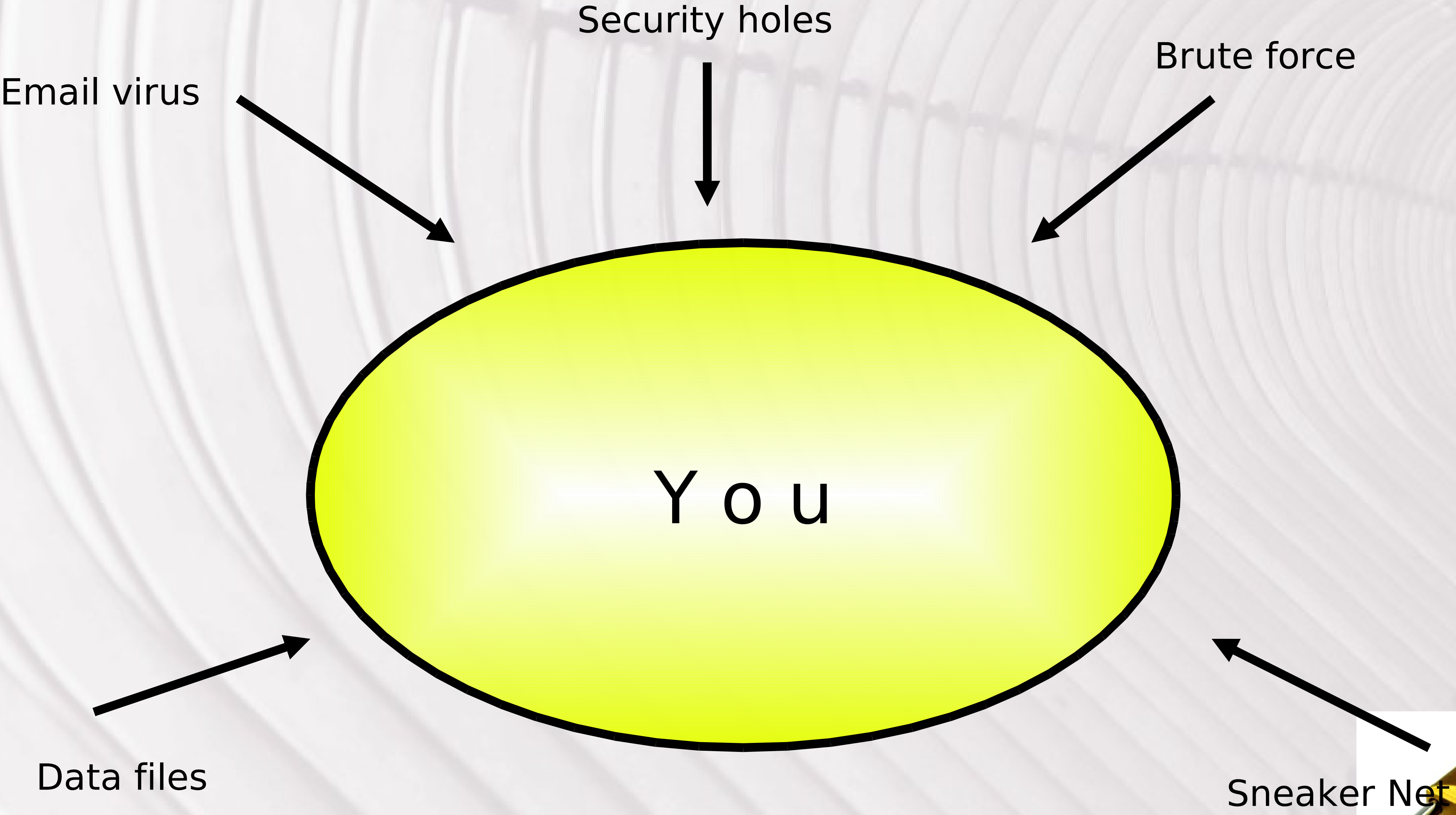
- **Server security holes** : IIS, SQL server..
- **Client security holes** : IE holes, ..
- **Web-app vulnerability** : Santy virus, ..
- **Data files** : JPG, MP3, ..

The Evolution

Ways to avoid detection

- Anti-debugging code
- Stealth : the early “rootkit”
- Polymorphic code : triggered “heuristic” scanners
- Metamorphic code : Total transformation, Huge virus size

The E(x)ternal Threat : The Security Shell Model



Keeping Them Out : Prevention

- Network Firewall : Close All, then Open Selectively
- App Firewall : mod_security
- Server hardening
- Anti Virus @ Email gateway
- Anti Virus @ Web gateway
- Security Patch Management
- User education : against PEBKAC

The Internal Threat :

Hello mate, trust me

- Data theft :
  workstation lock-down
- System sabotage :
  access control & audit
- Social engineering :
  user education
- Physical security :
  lock, procedures

Monitoring :
Did we really stop them ?

- IDS : Intrusion Detection System

  Problem : false positive

  Enhancement : context-aware IDS

- Local Anti Virus : against sneaker net, etc

- Vulnerability scanners : proactive

- Log files monitor : Access audit

Summary

- Layered Security Approach :
  - Biggest bang for the buck first
- Monitoring
- Preparing for the rainy day :
  - Disaster Recovery

- Be Paranoid : One breach = All at risk
- The chain is only as strong as its weakest link

Thank You