Reti di Calcolatori II

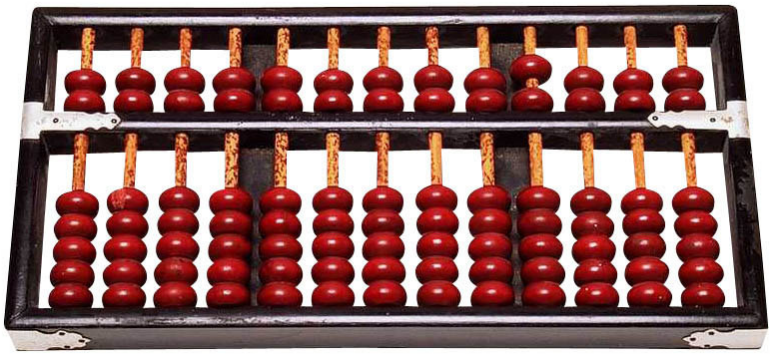
Introduction to Information Warfare

Parte I

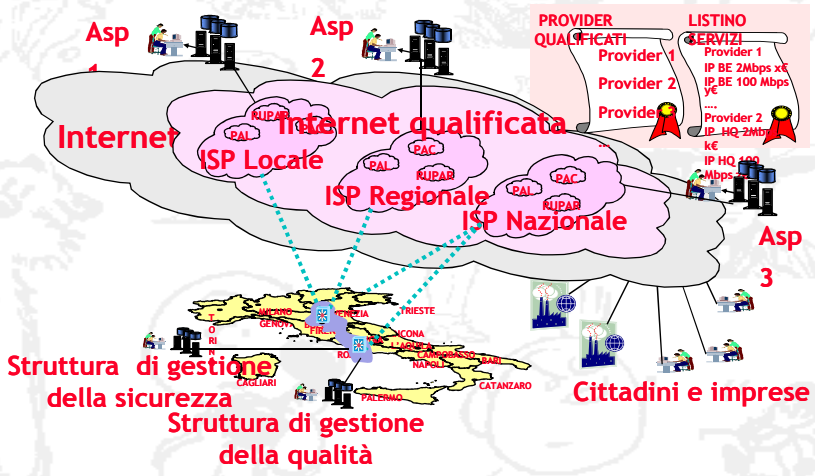
Giorgio Ventre
Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II

Nota di Copyright

L'unico calcolatore sicuro!



Purtroppo la realtà è ben differente



Tipi di e-Crime

- Virus or malicious code
- Spyware
- Phishing
- Illegal generation of Spam
- Unauthorized access
- DoS attacks
- Rogue WAP
- Exposure of private or sensitive data
- Fraud
- Identity theft
- Password sniffing
- Theft of intellectual property
- Zombie machines on network
- Theft of other proprietary info.
- Sabotage
- Web site defacement
- Extortion
- Other

Qualche dato statistico

2005 e-Crime Watch Survey

- Sources of e-Crime:
  - 82% Virus or Malicious Code
  - 61% Spyware
  - 57% Phishing (era il 31% nel 2004)
  - 48% Illegal Spam Generation
- Losses from Crimes:
  - 55% Operational
  - 28% Financial ($506,670 – media)
  - 12% Harm to reputation
- Culprit: 80% Outsiders, 20% Insiders

Gruppi a rischio Cyber Threat*

- Hackers – 37%
- Current employees – 18%
- Foreign entities – 6%
- Former employees – 5%
- Information brokers – 3%
- Current service providers/consultants/contractors – 2%
- Terrorists – 2%
- Customers – 2%
- Suppliers/business partners – 1%
- Competitors – 1%
- Former service providers/consultants/ contractors – 1%
- Not sure – 21%

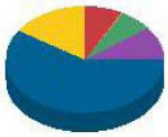
*** 2005 E-Crime Watch Survey**

US-CERT Cyber Security Incident Categories

Category	Description
CAT 1 Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2 Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3 Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are *not* required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
CAT 4 Improper Usage	A person violates acceptable computing use policies.
CAT 5 Scans, Probes, or Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6 Investigation	*Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

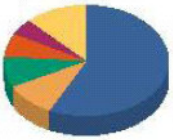
US-CERT: Dec. 2007 data

Figure 1: Incidents by Category



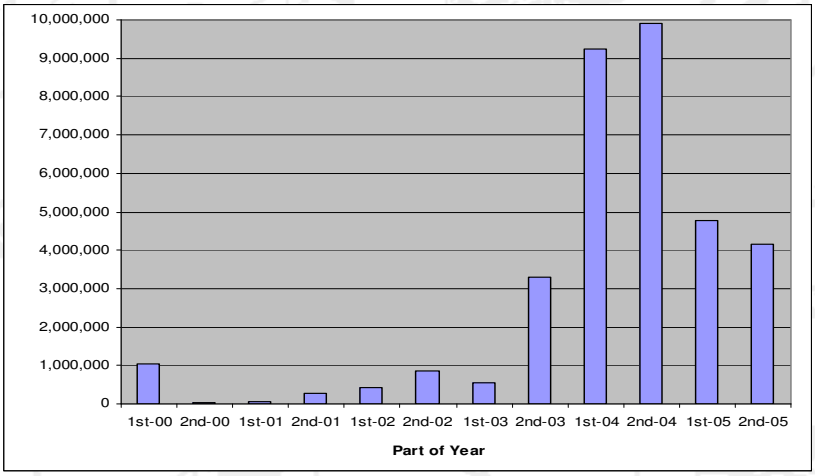
01-Unauthorized Access	7.6%
02-Denial of Service	0.2%
03-Malicious Code	6.9%
04-Improper Usage	10.3%
05-Scans/Probes/Attempted Access	59.0%
06-Investigation	16.0%
Total:	100.0%

Figure 2: Top Five Incidents vs. All Others



Phishing	57.6%
Policy Violation	9.6%
Non Cyber	9.2%
Equipment Theft/Loss	6.7%
Malware	4.6%
Others	12.3%
Total:	100.0%

Computer Viruses & File Stripping

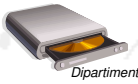


Un quadro un po' fosco…

Certo una realtà complessa

Come sono cambiate le cose
Hardware

Component	1970s	Now
User Interface	Mainframe terminals	Desktops, Laptops, PDAs, Cell Phones
Connection	Direct Connection	Direct connection, LANs, WAN, wireless, ISDN, DSL
Monitors	Monochrome character display using vacuum tubes	Full color pixel-based matrix display, PDAs
Unit of storage capacity	Kilobytes and megabytes	Gigabytes and terabytes
Processor Speed	Kilobytes per second	Gigabits per second
Processor	Sequential processing	Multitasking/multiprocessing
Storage interface	80-column hole-punch cards	Desktops, workstations, terminals, laptops, wireless devices
Storage Media	Magnetic Tapes	Floppy disks, Hard drives, CDs, CDRs, CDRW, DVDR, Zip drives, Dongle



Come sono cambiate le cose
Software & Dati

Area of Concern	1970s	Now
Operating System	Mainframe Specific: IBM, Unisys, Honeywell, HP, etc.	Microsoft (2000/XP), UNIX (e.g. Solaris, SGI, AIX), Linux, MAC OS X
Type of Data	Characters/Text	Text, graphics, audio, video, IM, IRC, VOIP, etc.
Word Processor	N/A – Manual typewriter	Word, WordPerfect, AmiPro
Calculations	N/A - Paper, Calculators	Spreadsheet (e.g. Excel, Lotus 1-2-3)
Scheduling	N/A – Paper calendar	Outlook, GroupWise
Presentations	N/A - Special order clear slides	PowerPoint
Music	N/A - Radio	MP3 files
Architecture design	N/A - Paper blueprints used	CAD software
Video	N/A – TV	Stored and real-time AVI, WAV files; cameras on desktop, doorways, etc.
Pictures	N/A – Camera	Digital files, Cell phones, Web Cams
Programming Language	COBOL	Visual Basic, Java, HTML, etc.

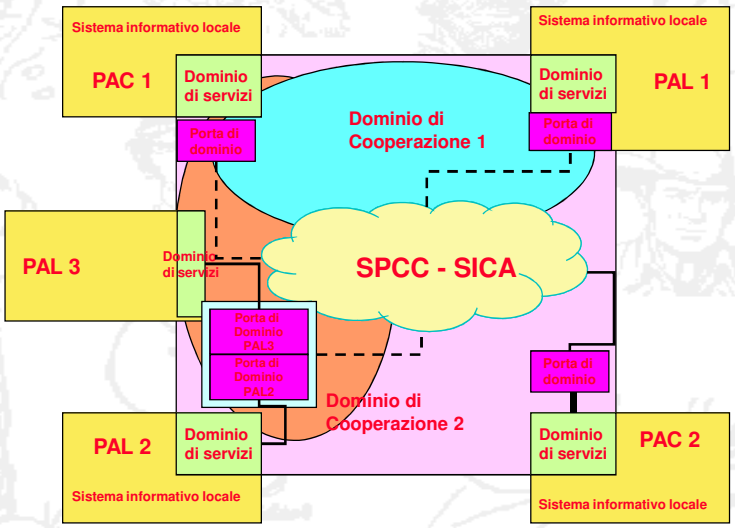
Come sono cambiate le cose
La Sicurezza IT

Subject/Topic	1970s	Now
Users	Limited to those with direct connect terminals	Anyone on the Internet
System architecture	Single mainframe (terminals in star configuration)	Many interconnected networks of various configurations
System Access	Only required a terminal with direct wiring	Network access with User ID, password, authentication, single sign-on
Data Connection	Clear text	Clear and encrypted
Data Availability	By request	Available on the Internet
Access Concerns	Internal access via terminal at desk	Internal access, anyone on LAN, Internet users
Data security	Tape library	Data on disks, CDs, hard drive, laptops, PDAs, and other media
Data storage	Clear text	Compressed, encrypted, large volume
Communications protocols	Vendor specific for terminal access	Many: HTTP, FTP, SSL, Telnet, SSH, IMAP, IDENT, UDP, TCP, etc.
Environment protection	Building, rooms, lock boxes, fire suppressors	Same plus firewalls (network and personal), IDS, routers, anti-virus software

Come sono cambiate le cose
La Sicurezza IT (2)

Subject/Topic	1970s	Now
System software	Mainframe specific	Various operating systems, utilities, software packages
Software problem resolution	Mainframe vendors	Anyone who supplies software [upgrades, patches, help desk]
Access methods	Power up terminal	Direct connection to network, dial-in, hacker attacks via Internet, DSL, VPNs
Awareness	Primarily limited to computer center staff	Everyone must be diligent
Security software	Mainframe utilities	Operating system configuration, anti-virus, vulnerability scanners, IDS, communications monitoring
Security audit activities	Audit computer center	Audit network, computer center, applications, communication servers, Internet activity, penetration testing, etc.
Threat Source	Anyone who has access to the computer center	Anyone who has access to the computer center, desktop, and the Internet.

La Cooperazione Applicativa



I problemi aperti

- Siamo di fronte ad uno scenario di notevole complessità e rischio
  - Molteplicità di sistemi
  - Molteplicità di tecnologie
  - Molteplicità di responsabilità
- … con due problemi da risolvere
  - Security Awareness
  - Gestione della complessità

Security Awareness

Esempio 1: Social Engineering

Esempio 2: Phishing

Esempio 3: Terminali mobili

Social Engineering

- Salta gli Intrusion Detection Systems
- Praticamente gratis
- Basso rischio di essere scoperto
- Nessun log
- Efficace al 100%
- Nessuno se lo aspetta

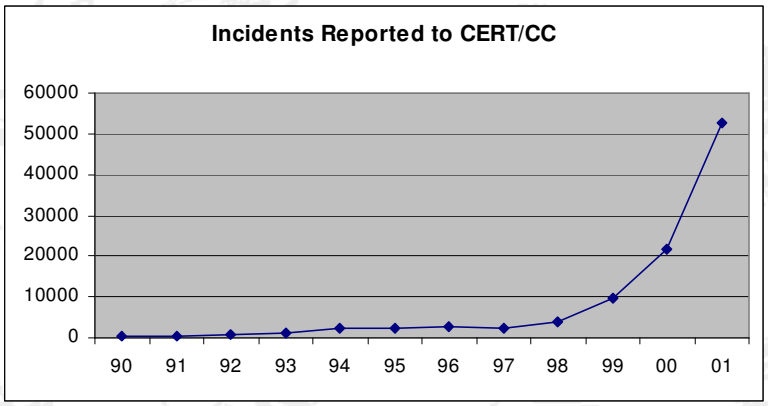
Gestione della complessità

- **Firewalls - automated virus scanning**
- **Physical security systems**
- **Spyware/adware detection software**
- **Intrusion detection systems**
- **Patch management**
- **Configuration management**
- **Controllo dell'accesso**
- **Wireless monitoring**
- **Encryption**
- **Autenticazione**

Nature of Cyber Attacks

- How bad is it?
- Who does it and why?
- What do they do?
- Why so many attacks?
- What about the future?

Incident Trends

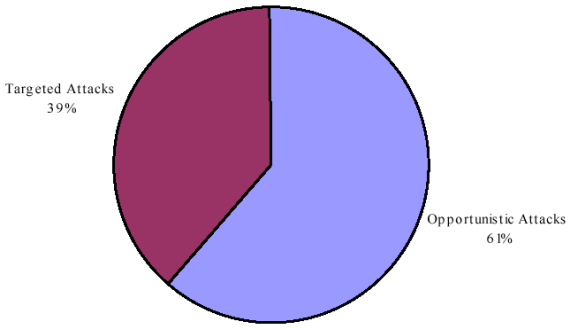


Riptech Threat Reports

- Reports issued in Jan 02 and July 02 for preceding 6 months
- Data obtained from monitoring over 400 companies in over 30 countries
- Over 11 billion firewall logs and IDS alerts analyzed in 2nd report
- Over 180,000 cyber attacks investigated in 2nd report
- Events characterized by severity level
  - informational – scans for vulnerabilities
  - warning – bypassed firewall, but did not compromise system
  - critical – required action by Riptech or client to prevent compromise
  - emergency – security breach occurred

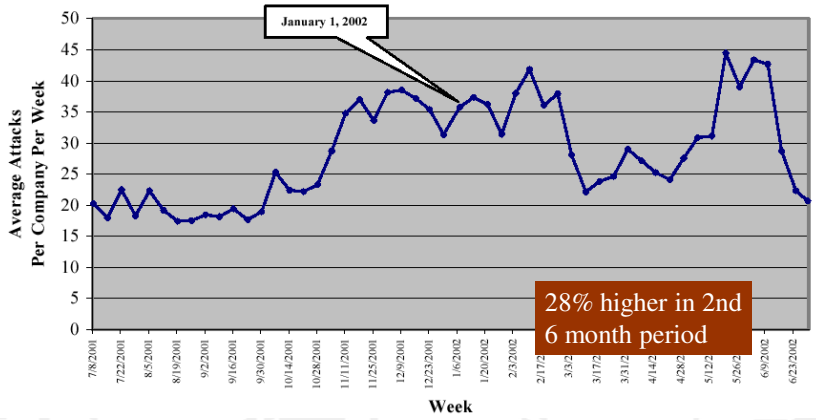
Intent of Attack

FIGURE 7—ATTACKS BY ATTACKER INTENT



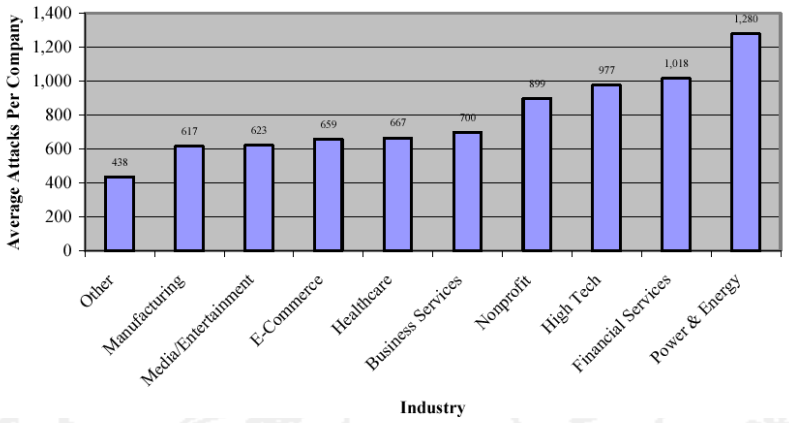
Source: Riptech, Inc.

Attack Intensity Jul 01 - Jun 02



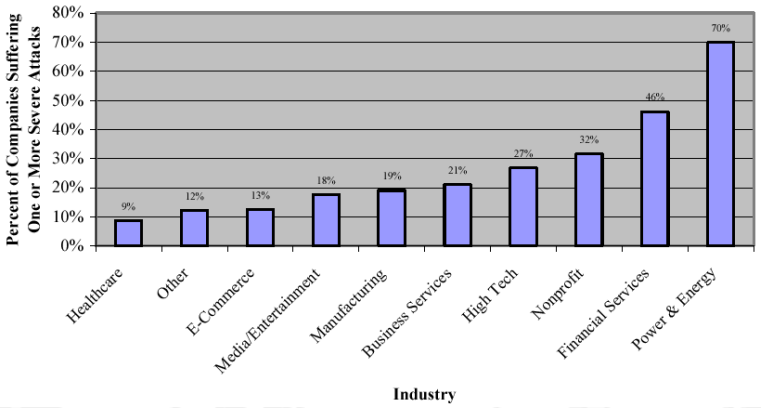
Riptech Internet Security Threat Report, July 2002

Attacks by Industry Jan – Jun 02



Riptech Internet Security Threat Report, July 2002

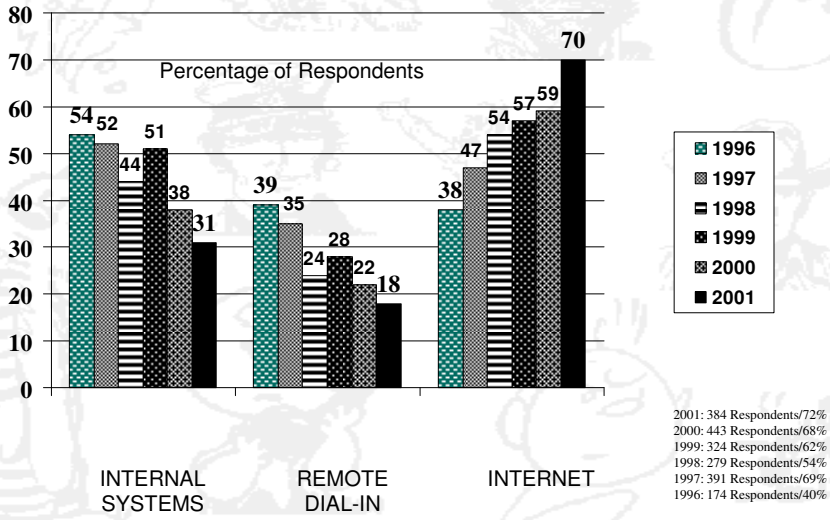
Severe Attacks by Industry Jan – Jun 02



Riptech Internet Security Threat Report, July 2002

Point of Attack

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute



2001: 384 Respondents/72%
2000: 443 Respondents/68%
1999: 324 Respondents/62%
1998: 279 Respondents/54%
1997: 391 Respondents/69%
1996: 174 Respondents/40%

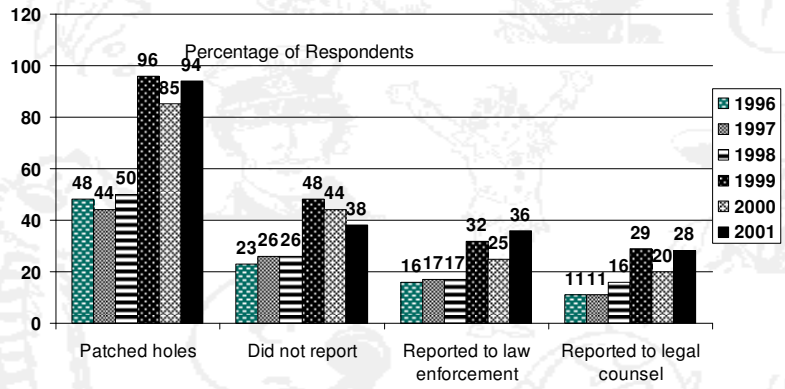
Financial Losses

CSI/FBI 2002 Computer Crime and Security Survey
Of those willing and able to quantify losses:

- 1997: 249 respondents (59%), $ 100,119,555
- 1998: 241 respondents (42%), $ 136,822,000
- 1999: 163 respondents (31%), $ 123,779,000
- 2000: 273 respondents (42%), $ 265,589,940
- 2001: 196 respondents (37%), $ 377,828,700
- 2002: 223 respondents (44%), $ 455,848,000

Source: Computer Security Institute

Actions Taken in Response to Intrusions



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

2001: 345 Respondents/64%
2000: 407 Respondents/63%
1999: 295 Respondents/57%
1998: 321 Respondents/72%
1997: 317 Respondents/56%
1996: 325 Respondents/76%

Attacks Against Critical Infrastructures

- Swedish hacker jammed 911 in central Florida in 1997
- Juvenile hacker penetrated and disabled a telco computer servicing Worcester Airport in March 1997
  - » phone service to FAA control tower, airport fire department, airport security, … cut off for 6 hours
- Brisbane hacker used radio transmissions to create raw sewage overflows on Sunshine coast in 2000
- Hackers broke into Gazprom's system controlling gas flows in pipelines in 1999
  - » world's largest as producer and supplier to Western Europe
- Hackers got into California Independent Service Operator (ISO) development network for regional power grid in spring 2001
- Numerous denial-of-service attacks against ISPs – some shut down

Attack on Sewage System

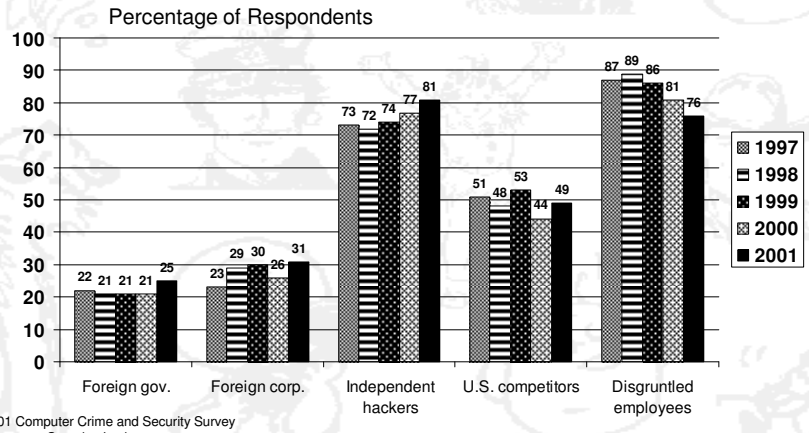
- Australian man (49) hacked into waste management system of Maroochy Shire, Queensland
- Laptop used to access and control the system
- Caused raw sewage overflows
  - » millions of litres of sewage spilled into local parks, rivers, and hotel grounds
  - » marine life died, creek turned black, stench unbearable
- Made at least 46 attempts in March, April 2000
- Attacks response to being rejected for job
- Was employed by firm that installed software
- Sentenced to 2 years in prison

Potential Attackers

- Hackers and script kiddies
- Insiders
- Criminals
- Activists
- Terrorists
- Governments

Perceived Threats

2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/83%
1997: 503 Respondents/89%



CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Hacker Quotes

"It's really just a bunch of really smart kids trying to prove themselves. I know I was."

– Splurge, sm0ked crew

"It's power at your fingertips. You can control all these computers from the government, from the military, from large corporations. … That's power; it's a power trip."

– anonymous

"You do get a rush from doing it – definitely."

"I'm like your nosy neighbor on steroids, basically."

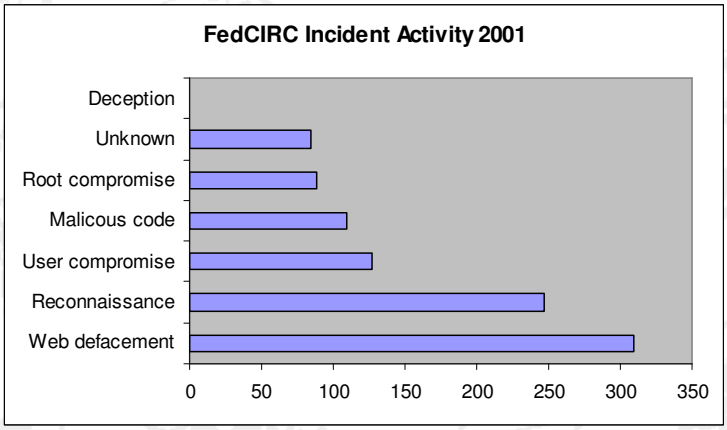
– Raphael Gray (aka Curador)

[stole/posted 26,000 Cr. Card numbers]

Types of Attack

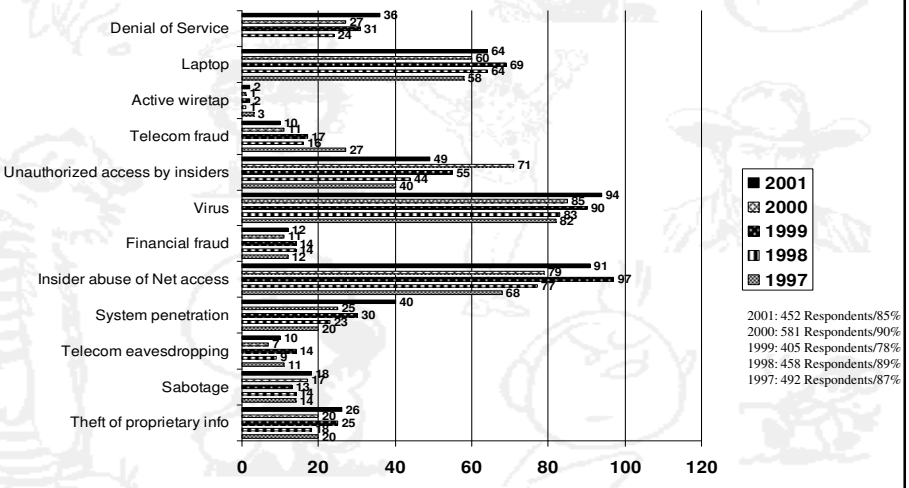
- Confidentiality
  - host penetrations (user and root)
  - network sniffers
- Integrity
  - computer viruses, worms, and Trojan horses
  - Web defacements
  - domain redirection (DNS hacks)
  - sabotage of information and systems
- Availability
  - denial and disruption of service

Incident Types



Types of attack or misuse detected in the last 12 months (by percent)

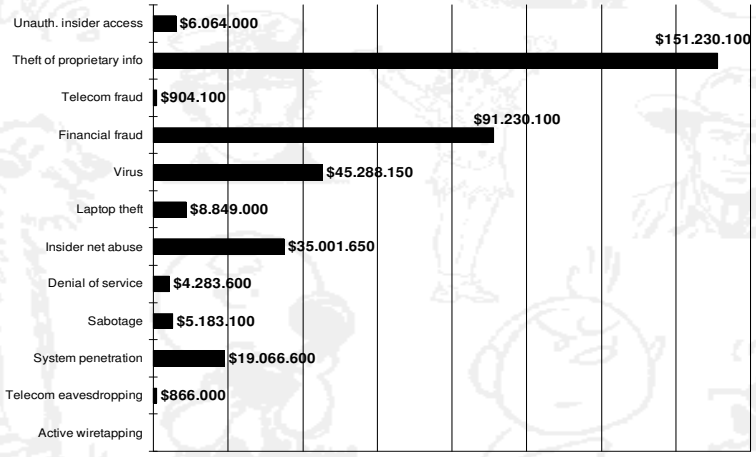
CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute



2001: 452 Respondents/85%
2000: 581 Respondents/90%
1999: 405 Respondents/78%
1998: 458 Respondents/89%
1997: 492 Respondents/87%

Dollar Amount of Losses by Type

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute



2001: 196 Respondents/37%