Defending the End User

Kellman Meghu
Security Engineering Manager for Check Point Canada
How Long Will You Survive?

Distributed Intrusion Detection System

DShield.org

Records Added

<table>
<thead>
<tr>
<th>Last Month</th>
<th>Last Week</th>
<th>Today</th>
<th>Survival Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>746,026,237</td>
<td>195,852,192</td>
<td>27,033,471</td>
<td>16 min.</td>
</tr>
</tbody>
</table>

As of Tue Feb 21 04:09:25 2006 UTC
Threat Landscape

Virus
- In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Thus, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

Worm
- A program or algorithm that replicates itself over a computer network.

Trojan
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Spyware
- gathers information about Internet users without their knowledge or consent and delivers that information to advertisers or others who have access to the information. Users can get spyware in their systems by downloading certain programs or in the form of a virus.

Root Kit
- a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge.
Effects of Spyware

- Performance Degradation
  - Disk thrashing
  - Slow application/web access
  - Changing registry settings
  - Network congestion
  - Data corruption
  - Help Desk calls

- Annoying
  - Pop ups
  - Home page hijacking
  - Slow application/web access

- Security Threat
  - Keyloggers
  - Screen captures
  - File scans
  - Email snooping
  - Changing registry settings
  - Data corruption
  - Intellectual property theft
  - Opens back doors
Spyware By the Numbers

Corporate SpyAudit  Averages from Oct 7, 2004 to Dec 1, 2004

Instances of Spyware per Scanned Desktop: 20
Adware Installations per Scanned Desktop: 2.5
System Monitor Installations per 100 scans: 5
Trojan Horse Installations per 100 scans: 5.5

Total Number of SpyAudit Scans: 10,305
Total Number of Distinct Audits: 4,104

Activity caught. . .

- 127 connections in 60 seconds to 84 sites
- Each connection ~1-2 Kbytes
- In 24 hours, our ‘idle’ PC transferred almost 5 MBps of data
How Did It Get There?
Propagation Methods

- Vulnerabilities
- Email
- Web
- Peer to Peer
- Phishing
- Just ask. . . .
Birth of a BotNet
Explosion of a BotNet
Propagation
It's no surprise that organized crime and professional programmers—especially those in low-wage locations such as Eastern Europe, South America, and Russia—are attracted to the dark side of Internet commerce.
On August 25, 2004, Jay R. Echouafni, CEO of Orbit Communication, and five others were indicted in connection with the first successful investigation of a large-scale DDoS attack used for a commercial purpose. Echouafni and a business partner hired computer hackers to launch relentless DDoS attacks against Orbit's online competitors. They used the services of computer hackers in Arizona, Louisiana, Ohio, and the United Kingdom to attack the Web sites of RapidSatellite.com, ExpertSatellite.com, and Weaknees.com. The sustained attacks began in October 2003 and caused the victims to lose more than $2 million in revenue and costs associated with responding to the attacks.
Hacking for dollars

Calin Mateias, a Romanian computer hacker, was indicted in August 2004 for hacking into Ingram Micro's online ordering system and fraudulently ordering more than $10 million in computer equipment from the Santa Ana, Calif., company, the largest technology distributor in the world. Ingram Micro was only able to intercept less than half the orders before the items were shipped.

Using information obtained from his illegal hacking activity, Mateias bypassed Ingram's online security safeguards, posed as legitimate customers, and ordered computer equipment to be sent to Romania. When Ingram Micro blocked all shipments to Romania in early 1999, Mateias directed that the equipment be sent to dozens of addresses scattered throughout the United States as part of an Internet fraud ring. Mateias recruited four Americans from Internet chat rooms to provide him with U.S. addresses to use as "mail drops" for the fraudulently ordered equipment. In turn, the four Americans recruited others, including high school students, to provide additional addresses and to accept the stolen merchandise. The U.S. members would either sell the equipment and send the proceeds to Mateias or repackage the equipment and send it to Romania.
In March, Rio de Janeiro police nabbed Valdir Paulo de Almeida, the leader of an 18-member phishing group that spammed a Trojan horse to approximately 3 million email accounts on a daily basis. The Trojan included a keystroke logger that recorded account usernames and passwords, and then fed them back to the gang. The gang stole as much as $37 million from online bank accounts causing serious monetary losses for the financial institutions involved. Although the gang targeted Brazilians, it also siphoned funds from bank accounts abroad, Brazilian federal police told Reuters.
Who Can You Trust?

WMF Vulnerability

- Late December, a vulnerability in the handling of wmf files is ‘discovered’.
- Within a week, over 100 different instances of exploitation are released.
- Exploit ‘generation’ tool quickly renders AV signatures out of date
- Software engineers who have looked closely at the Windows code that enables the vulnerability have concluded that, for whatever reason, it is operating exactly the way its designers intended it to.
Who Left The Backdoor Open?

- http://www.grc.com/wmf/wmf.htm

M.I.C.E

Metafile Image Code Execution
Many Endpoint Threats

- Keystroke logger capturing ID, PW
- Unauthorized access to Web server
- Rogue wireless access
- Latest worm or virus
- Backdoor listening for inbound connection
- Spyware download via P2P and IM
Protecting the End Point from themselves
A Case Study in Endpoint Security

Power mad hungry firewall admin
What About...

Power mad hungry firewall admin
Application Control

- Know your applications
- White List vs Black List
- End user services are available
- Understand you are at risk
A Look Ahead
Questions?

Got a **BUG**?