Where Internet Threats Fit in the Overall Security Picture

Alfred Huger
Senior Director, Engineering
Symantec Security Response

Agenda

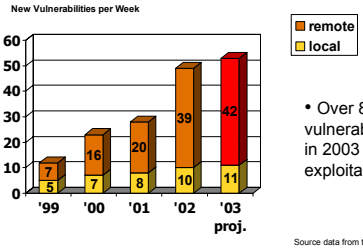
1. Trends in Vulnerabilities & Malicious Code
2. Threat life cycles, propagation and severity
3. Leadership, what do we need moving forward?
4. Greater Vigilance is needed
5. Vulnerability Disclosure and labeling
6. Richard Clark Intro
7. Conclusion

Trends in the threat landscape – Vulnerabilties and Malicious Code

- The way we speak about and think of Malicious Code is changing. Malicious Code is now largely synonymous with Software Vulnerabilities and vice verse.
- In order to gauge one we must understand and be able to gauge the other.

Vulnerability Trends

Vulnerability Research is now being focused on remote exploitability

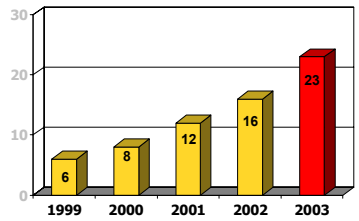


- Over 80% of the vulnerabilities reported in 2003 are remotely exploitable

Source data from the DeepSight Vulnerability Database

Vulnerability Trends

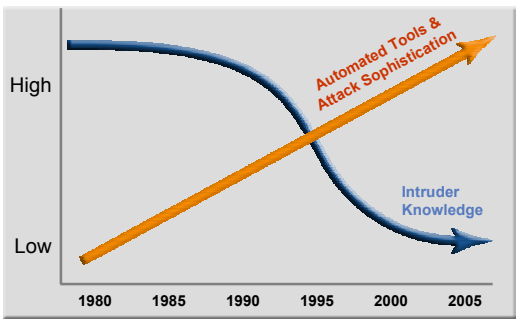
Discovery of high impact vulnerabilities which result in full system compromise is rising



- High impact issues for Windows operating systems

Source data from the DeepSight Vulnerability Database

Vulnerability Trends



Vulnerability Trends

- CORE IMPACT
- CANVAS

OpenSource Exploitation Frameworks

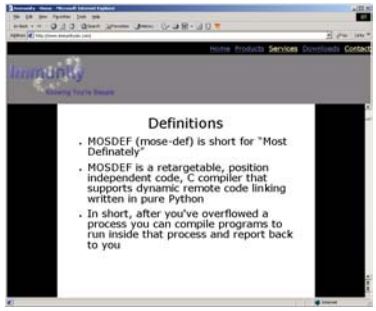
- MetaSploit

OpenSource Exploitation Frameworks

- InlineLibEgg

OpenSource Exploitation Frameworks

- MOSDEF

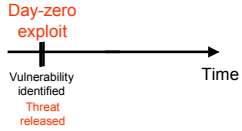


Vulnerability Threat Evolution: Day-Zero Threats

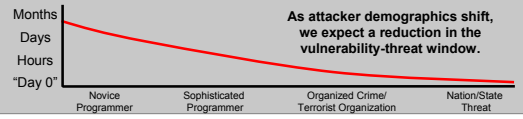
A day-zero threat exploits a previously unknown, and therefore unprotected vulnerability.

Vulnerability Threat Evolution: Day-Zero Threats

A day-zero threat exploits a previously unknown, and therefore unprotected vulnerability.



Time Until Exploitation



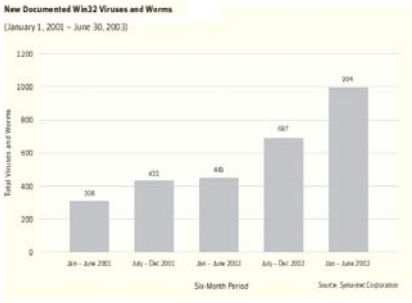
Malicious Code Trends

- On the Rise
  - – Windows32 - Win32 Viruses/Worms have increased by 123% for 1H 2003 compared to 1H 2002
  - – Instant Messaging (IM)/Peer-to-Peer (P2P) Networks viruses and worms have increased by 400% during 1H 2003
  - – Malicious Code is now being used to target particular demographics.
  - – Submissions of Malicious Code to Symantec containing backdoors has risen by 50%.

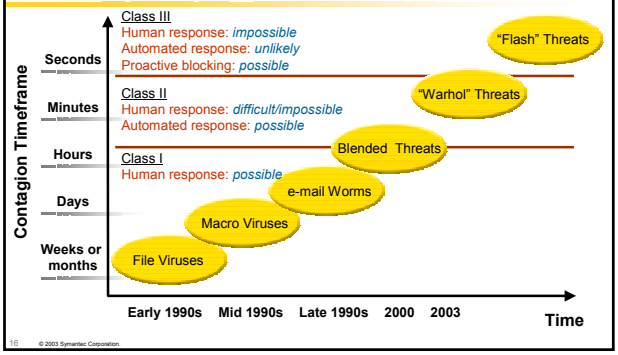
Malicious Code Trends

- In the wild (Honeynet Activity)
  - – Since September 1/03 to current the Symantec Honeynet has captured 75 previously unidentified viruses
  - – With an average of 90 infections a day 25% of those are pre-infected
  - – Up to 35% of the infections are a result of automated Bot networks using worms or auto-rooters to expand their networks
  - – Windows compromises outshadow Linux compromises by a 40 to 1 basis. Even when both machines are vulnerable to well known problems

Malicious Code Trends



Overall Threat Evolution



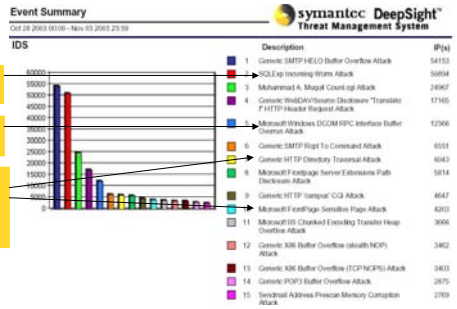
The acceleration of threats and their lifecycle

- Code Red and Nimda were destructive, but fairly slow
- Code Red took about 12 hours for most of its spread
- Klez traveled around the world in 2.5 hours
- Slammer infected 75,000 hosts in ten minutes
- Threat landscape is shifting toward more complex, fast-spreading attacks

The acceleration of threats and their lifecycle

- Threats such as CodeRed & CodeRedII are still seen in large numbers. Including newly infected systems
- New computers which are not patched up to current levels contribute heavily to the problem
- Average life expectancy for an unpatched Windows system newly connected to the Internet is less than 15 minutes (average) before infected with malcode

The acceleration of threats and their lifecycle



The acceleration of threats and their lifecycle

These issues are made worse by end users still suffering from easily addressed security issues:

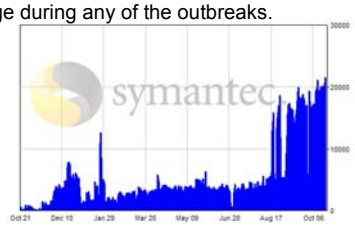
- 18% report NetBIOS vulnerabilities
- 49% report a browser privacy vulnerabilities
- 26% are still not running antivirus software
- 6% report a virus or Trojan horse infections

Source: Over 2.4 million results submitted to Symantec Security Check website.
All statistics are as of January 2003

Increasing pressure on security resources

This chart shows the number of IP addresses attacking a typical 600 node network over the last year.

Despite an increase in the number of attackers, this number did not change during any of the outbreaks.



Source data from the DeepSight Incident Database

Importance of strong leadership

- This problem cannot be solved in technology alone
  - Large scale education is required in order to make this problem approachable. This must be done both by Government and Private Enterprise
  - Government should be funding education for students, both post secondary and otherwise
  - Corporation need to educate their staff
  - Regional and National ISP's need to start being held accountable for what comes out of their address space
  - Operating System vendors must be more vigilant with their coding practices

Greater vigilance is needed…….

- Corporate IT Security needs to be considered an infrastructure cost, not simply an IT line item
- Corporate IT Staffing should be commensurate with the size of the assets managed and their relative importance to national infrastructure
- Government funded ISAC's and Critical National Infrastructure initiatives should be seen in every sovereign state with an Internet presence

Vulnerability Disclosure

- What are common views on disclosure?
  - Full Disclosure
  - Responsible Disclosure
  - Anti Disclosure

"I can tell you I wish those people just would be quiet. It would be best for the world. That's not going to happen, so we have to work in the right fashion with these security researchers," – *Steve Ballmer, Microsoft's Worldwide Partner Conference in New Orleans.*

Vulnerability Labeling

- Poses a serious problem in terms of vendor con-conformity
  - For Software Vulnerabilities each vendor generally names the threat a different name, virus names largely share the same problem
  - This is again compounded by the threat being referred to again by altogether different names in NIDS', HIDS', vulnerability scanners, alerting services and SIM's.
  - These names are further complicated by being almost exclusively in English

Vulnerability Labeling

- Initiatives to solve this problem:
  - MITRE CVE (Common Vulnerabilities & Exposures)
  - MITRE CIEL (Common Intrusion Event List)
  - MITRE OVAL (Open Vulnerability Assessment Language)
  - Bugtraq ID

Removing the roadblock

Introduce Richard Clarke for his presentation on:

What are some concrete steps that can be taken to remove the roadblock that are preventing the IT Revolution from achieving its full potential?

Conclusion

- Include one slide to summarize