



# Malicious Code on Linux-Based Systems



iDefense Intelligence Operations

November 17, 2005

Where it all comes together:

# Presentation Agenda

---

- + About iDefense
- + Linux Based Malicious Code
  - History
  - Trends
  - Recent Developments
  - Future Developments
- + Q&A

# About iDefense: Overview

---

- + iDefense, a VeriSign Company, is a leader in cyber threat intelligence
- + Industry-Leading Service Offerings
  - Intelligence is all that iDefense does
- + Marquee Customer and Partner Base
  - Government, financial services, retail, telecom and others
- + Experienced Intelligence Teams
  - iDefense Labs
  - Vulnerability Aggregation Team (VAT)
  - Malicious Code (Malcode) Team
  - Threat Intelligence Team
  - Rapid Response Team
- + In business since 1998, iDefense became a VeriSign Company in July 2005

# iDefense – Trusted Experts

“...some of the most incisive analysis in the business, particularly about Russian hackers.” – *BusinessWeek*

“iDefense, which generates cybercrime intelligence for government and financial industry clients.” – *NY Times*

“..by then iDefense had sifted out the 20 culprit PCs, breaking the state-of-the art encryption...and handing the information to the DHS, FBI and Canadian law enforcement officials.” – *Forbes*

“So far this year, the company is credited with the responsible disclosure of 36 security bulletins, including major flaws in products sold by CA, RealNetworks and Apple.” – *eWEEK*



# iDefense Intelligence Services

---

## Daily / Hourly Research Deliverables

- + Comprehensive Vulnerability Feed
  - Most comprehensive, timely, technical feed in the industry
- + iDefense Exclusive Vulnerabilities
  - 250+ contributors around the globe
  - Released to vendor and iDefense customers only
  - More than 160 iDefense Exclusive vulnerabilities so far in 2005
- + Malicious Code Research and Reporting

# iDefense Intelligence Services

---

## Weekly / Semi-Monthly Research deliverables

- + Weekly Threat Report
  - Weekly compilation of worldwide threats
  - Critical Infrastructure, State of the Hack, Cyber Crime, Terrorism and Homeland Security, Global Threat
  
- + iDefense Topical Research Papers
  - **Examples:**
    - Security of Enterprise Web-Based E-Mail Interfaces
    - Security Comparisons: Internet Explorer vs. Firefox
    - Phishing and Pharming: A Comparison
    - Mitigating the Threat from Keyloggers
  
- + Focused Threat Intelligence Reporting
  - Topics specific to individual customers

# iDefense Exclusives – Last 12 Months

---

- + 200+ Submissions Confirmed and Verified
  - Have been published or submitted to clients and the vendor
- + 13 Microsoft exclusives have gone public in 11 different MS05-xxx Microsoft Bulletins
  - 11/52 (21%) Microsoft Bulletins in 2005 have included our vulnerabilities
- + 119 days average lead time for Microsoft issues
  - Customers had workarounds 119 days before the advisory was public
  - 45 days average lead time across all vendors

# Total Number of Malicious Code in 2005

---

- + TOTAL: 13,224
  - Extreme: 1
  - HIGH: 38
  - MEDIUM: 327
  - LOW: 12,858
  
- + Spyware: 259
  
- + Adware: 311

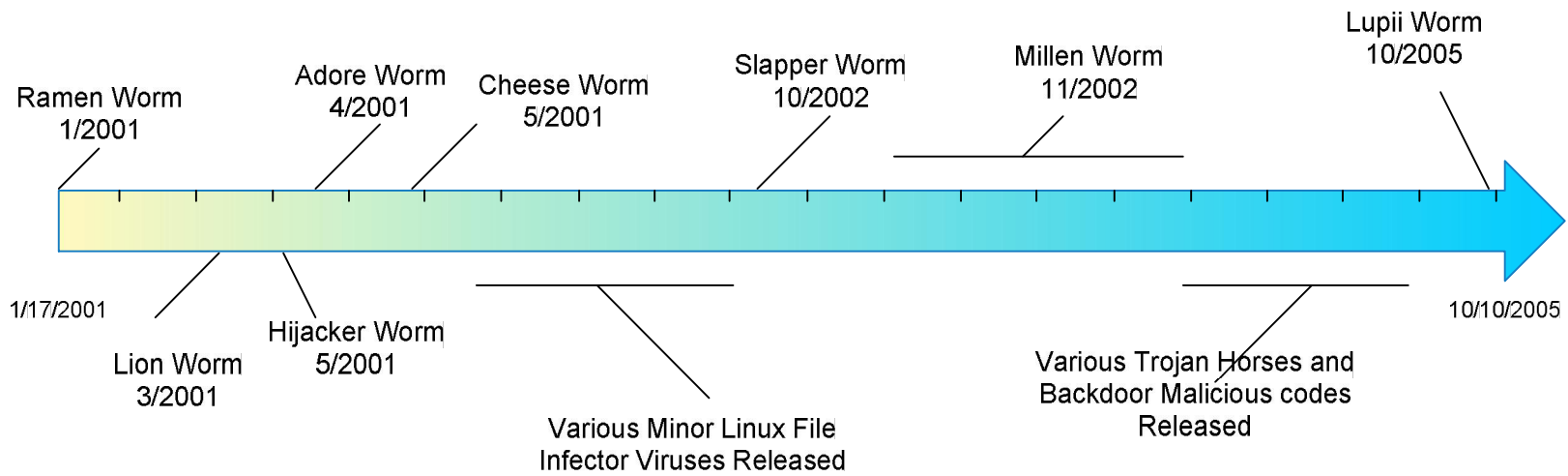


# Presentation Agenda

---

- + About iDefense
- + Linux Based Malicious Code
  - History
  - Trends
  - Recent Developments
  - Future Developments
- + Q&A

# History



# Notable Linux Based Malicious Code

---

- + Ramen Worm (January 2001)
  - First Real Linux Worm
  - Targeted three vulnerabilities in only one OS (Red Hat 6.2 and 7.0)
  - Only defaced the *index.html* file on the web server of the infected machine
  
- + Svat Virus (May 2002)
  - Infects both PE and ELF executables

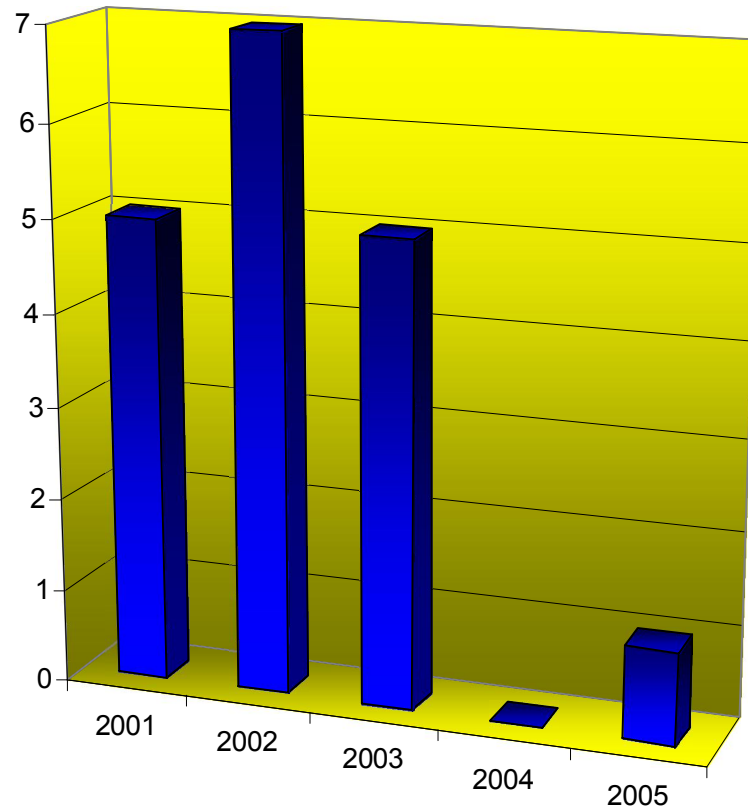
# Notable Linux Based Malicious Code

---

- + Similie Virus (May 2002)
  - Entry-point obscuring, metamorphism and polymorphic decryption, infects both PE and ELF executables
  
- + Slapper Worm (October 2002)
  - Exploits an Apache SSL vulnerability
  - Targets multiple flavors of Linux
  - Performs DDoS attack

# Trends

- + Overall decrease in the number of code targeting Linux



# Trends

---

- + First Linux worm targeted vulnerabilities in the base OS; all worms since have targeted third-party applications
- + Popular open-source packages have been the biggest target of these worms
- + Linux malicious code has not been popular with malicious code writers for several years

# Recent Developments - Conclusions

---

## + Lupii Worm (November 2005)

- Three variants to date
- Downloads ELF binary, no destructive payload
- Targets three vulnerabilities in third party Linux Applications

# Lupii Worm – Vulnerabilities Exploited

---

- + XML-RPC for PHP Code Injection Vulnerability
  - Input validation vulnerability resulting from a quote mismatch, allowing attackers to escape data and inject code
  - Numerous OS's and applications utilize vulnerable code
  
- + AWStats Rawlog Plugin Input Validation Vulnerability
  - Open-source tool for generating web, FTP or mail server statistics graphically
  - Lack of sanitization of logfile URL data passed to awstats.pl allows for passing of shell meta-characters directly to server
  
- + Webhints Remote Command Execution Vulnerability
  - Open-source tool for generating hint scripts
  - Lack of sanitization of user input allows for code execution



# Future Developments

---

- + No great increase in Linux targeting malicious code
- + Whatever does appear will be likely target third-party applications, especially open-source ones
- + Source code repositories will be a target for malicious code writers



# Q & A



Where it all comes together: