symantec™

Metricon '06

Top Network Vulnerabilities Over Time

Vik Solem

August 1, 2006

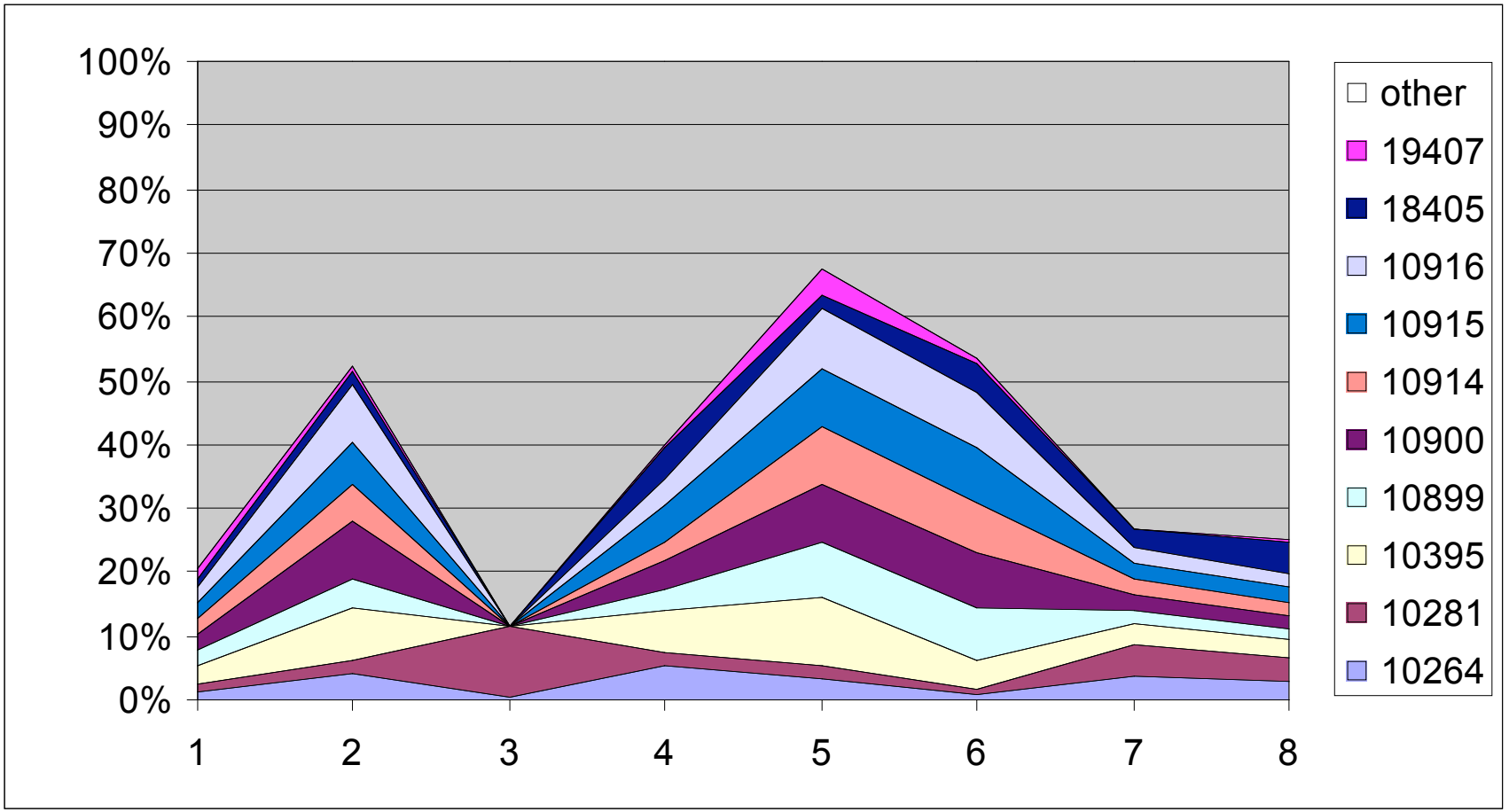
Network Vulnerabilities Data

- Size of Data
  - More than 1,000,000 vulnerability instances
  - More than 1 year of data available
- Type of Data
  - Standard Nessus Vulnerability IDs
- Set Selection
  - Only Nessus Data
  - 8 consecutive months of data
  - No Informational Level Entries

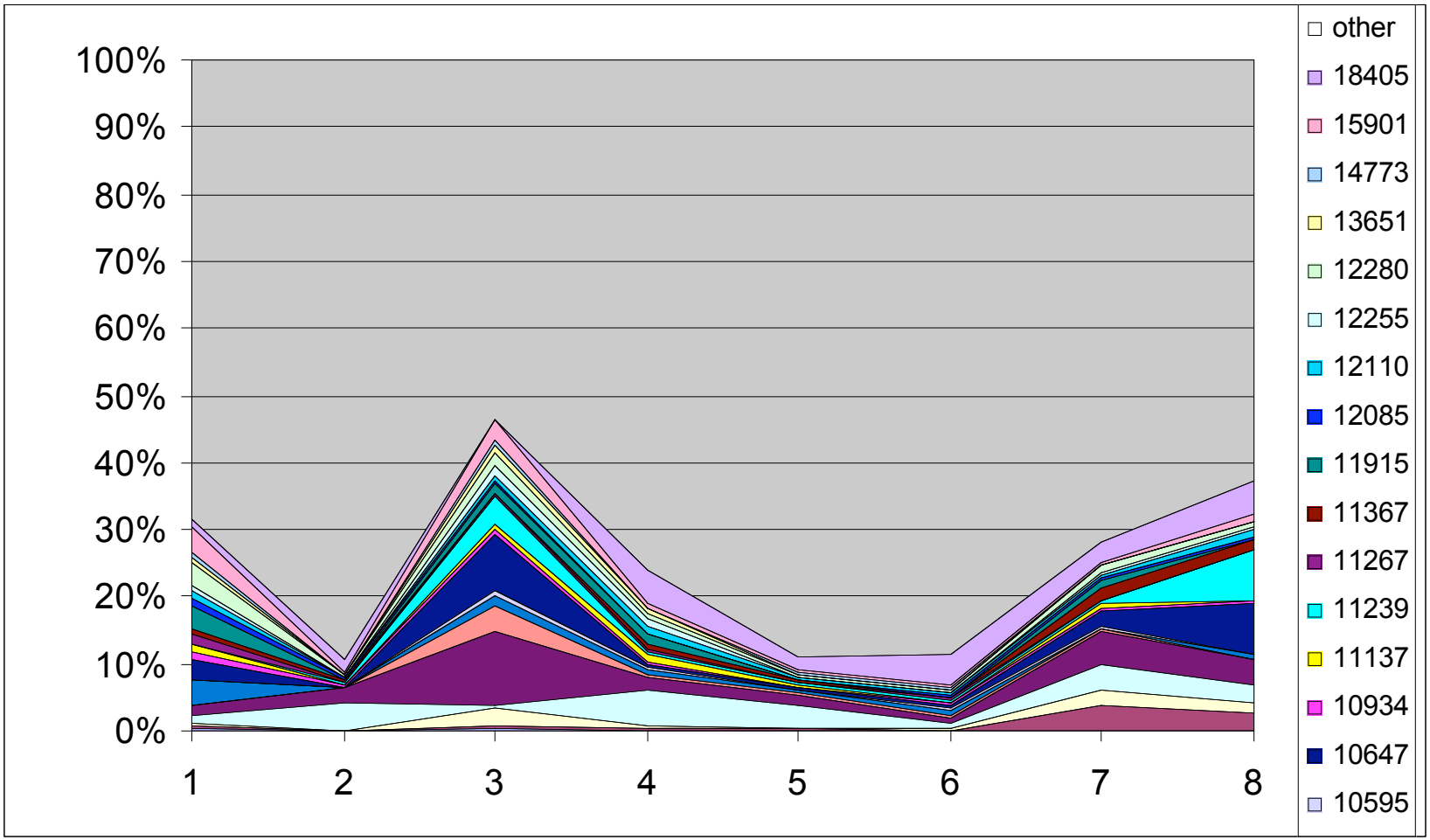
Network Vulnerabilities

- Top 10 Vulnerabilities
  - 10 most reported vulnerabilities in the entire data set
  - Shown over 8 months compared with all other vulnerabilities
- Vulnerabilities Found In All Time Periods
  - Only 23 vulnerabilities occurred in all periods
  - Shown over 8 months
  - Shown with top 10

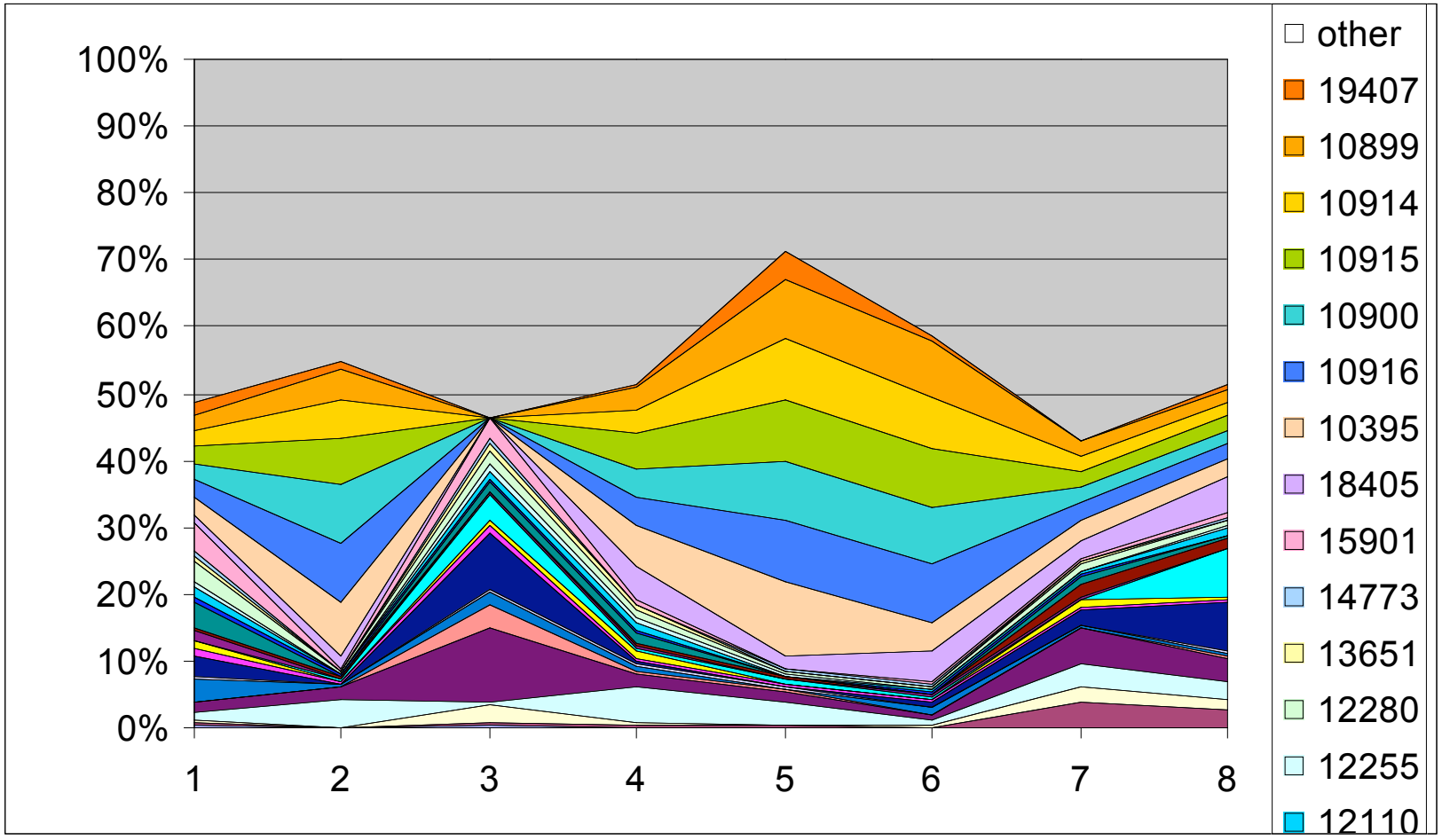
Top 10 Vulnerabilities Over 8 Months

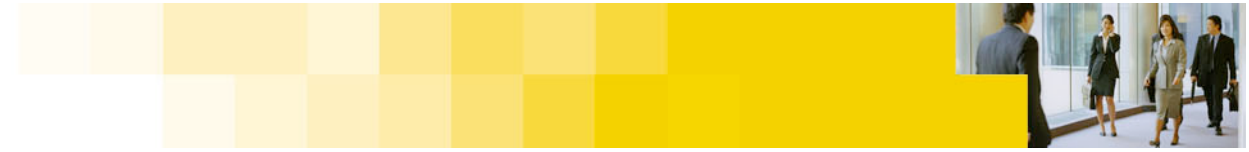


Vulnerabilities Found in All Time Periods



Top 10 Plus Those in All Time Periods



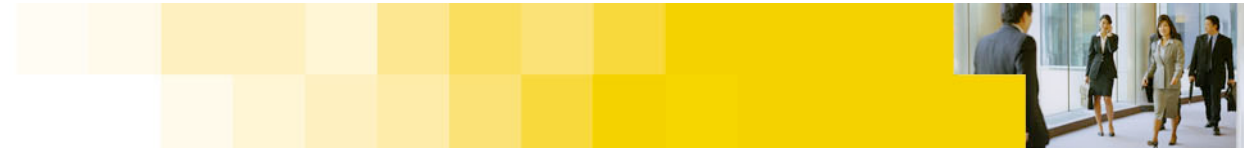


Top 10 Vulnerabilities

1. 10264: SNMP Default Community Names
2. 10281: Telnet Server Detection
3. 10395: SMB Shares Enumeration
4. 10899: Win Domain User Info (never logged in)
5. 10900: Win Domain User Info (password never expires)
6. 10914: Win Local User Info (never changed password)
7. 10915: Win Local User Info (never logged in)
8. 10916: Win Local User Info (password never expires)
9. 18405: Windows Remote Desktop MitM vuln
10. 19407: Windows Printer Spooler Vuln

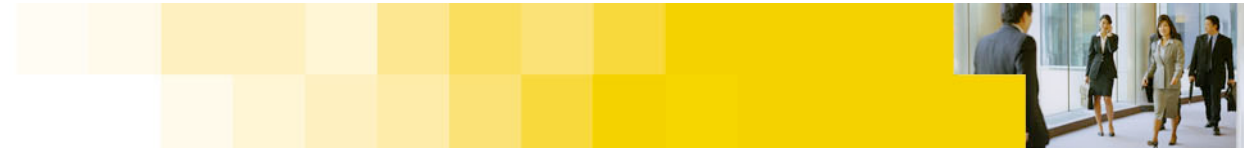
Symantec Threat Report Top 10 Attacks (July-December 2005)

1. Microsoft SQL Server Resolution Service Stack Overflow Attack
2. Generic HTTP Directory Traversal Attack
3. Generic ICMP Flood Attack
4. Generic WebDAV/Source Disclosure HTTP Header Request Attack
5. Generic HTTP CONNECT TCP Tunnel Attack
6. Sendmail Header Processing/Prescan corruption Buffer Overflow Attack
7. Generic Cross-Site Scripting in URL Attack
8. Microsoft FrontPage Sensitive Page Attack
9. Generic X86 Buffer Overflow (TCP NOPS) Attack
10. Possible Incoming Malicious Attachment Event



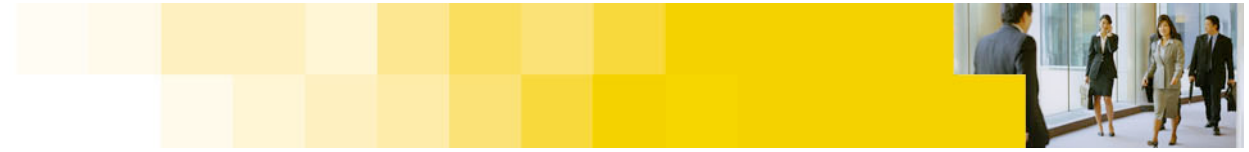
Qualys "Laws of Vulnerabilities Report" Most Common Vulns (January 2006)

- Part 1
  - MS Object Library Buffer Overflow (CVE-2005-0057)
  - MS Queuing Buffer Overflow (CVE-2005-0059)
  - MS DoS & Priv Escalation (CVE-2005-0061)
  - MS Exchange Remote Code Execution (CVE-2005-0560)
  - MS Web Client Service Remote Code Exec (CVE-2005-1207)
  - MS Color Mgt Module Remote Code Execution (CVE-2005-1219)
  - MS PnP Remote Code Execution (CVE-2005-1983)
  - MS Client Service Netware Buf Ovrflow (CVE-2005-1985)
  - MS PnP Remote Code Execution (CVE-2005-2120)
  - MS DirectShow Remote Code Execution (CVE-2005-2128)
  - MSDTC & COM+ Remote Code Execution (CVE-2005-1980)
  - MS Graphics Engine WMF Format Code (CVE-2005-4560)



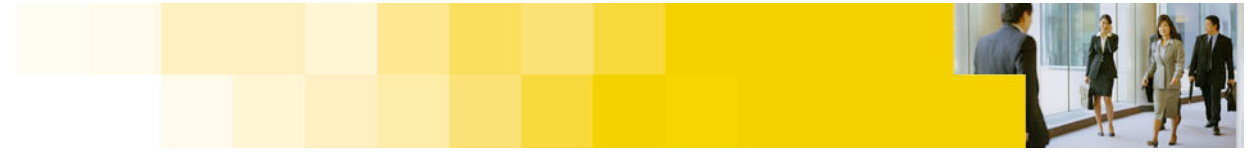
Qualys “Laws of Vulnerabilities Report” Most Common Vulns (January 2006)

- Part 2
  - MS SMB Remote Code Execution (CVE-2005-1206)
  - MS Print Spooler Remote Code Execution (CVE-2005-1984)



Next Steps

- Split Data for Different Report Types
  - Types of scans (internal vs. external)
  - Types of scanners (Nessus vs. others)
- Summarize Data for Vulnerability Categories
  - Our top 10 includes 5 which could be called “Windows Information Leakage”
- Generate in Real Time in the Attack Center
  - As a job is completed display and compare to
    - Other jobs within the client
    - Other jobs overall
    - Other networks/scans of similar types



Questions?

Thank You.

Vik Solem

Principal Consultant

T. 617-768-2709

M. 617-308-3728

vik_solem@symantec.com