VeriSign

iDEFENSE
A VeriSign Company

# Targeted Malicious Code

## iDefense Intelligence Operations

Nov. 3, 2005

Where it all comes together.

# Presentation Agenda

I. About iDefense

II. What is a Targeted Attack

III. Current Targeted Attack Trends

IV. Codes Utilized in Recent Attacks

V. Recent Examples & Notable Targets to Date

VI. 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

- 175 Submissions Confirmed & Verified
  - Have been published or submitted to clients and the vendor
- 13 Microsoft exclusives have gone public in 11 different MS05-xxx Microsoft Bulletins
  - 11/51 (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

# Total Number of Malicious Code in 2005

- TOTAL: 13224
  - Extreme: 1
  - HIGH: 38
  - MEDIUM: 327
  - LOW: 12858
- Spyware: 259
- Adware: 311

# 2,966 Malcode in ’05 Exploiting Microsoft Vulnerabilities

- Microsoft Virtual Machine Access Validation Vulnerability: 1
- UPnP vulnerability: 148
- Microsoft Internet Explorer Local File Script Design Vulnerability: 2
- SQL Server vulnerability: 150
- RPC Locator vulnerability: 36
- WebDAV vulnerability: 447
- Microsoft Internet Explorer IFRAME vulnerability: 1
- DCOM RPC vulnerability: 5
- Microsoft Windows DCERPC DCOM Heap Overflow: 156
- Workstation vulnerability: 239
- Microsoft ASN.1 BERDecBitString() Buffer Overflow Vulnerability: 207
- LSASS vulnerability: 1010
- IIS5 SSL DoS vulnerability: 73
- Cumulative Update for Microsoft RPC/DCOM: 272
- Vulnerability in WINS Could Allow Remote Code Execution: 9
- Microsoft IE hhctrl.ocx Help ActiveX Control Local Zone Security Restriction Bypass Vulnerability: 8
- Microsoft Windows Cursor, Icon Format Handling Vulnerability: 3
- Message Queuing Vulnerability: 1
- Microsoft IE JVIEW Profiler (Javaprxy.dll) Heap Overflow Vulnerability: 3
- Microsoft Plug-and-Play Buffer Overflow Vulnerability: 194
- Microsoft Windows 2000/XP Plug and Play Service Buffer Overflow Vulnerability: 1

# Presentation Agenda

I. About iDefense

II. What is a Targeted Attack

III. Current Targeted Attack Trends

IV. Codes Utilized in Recent Attacks

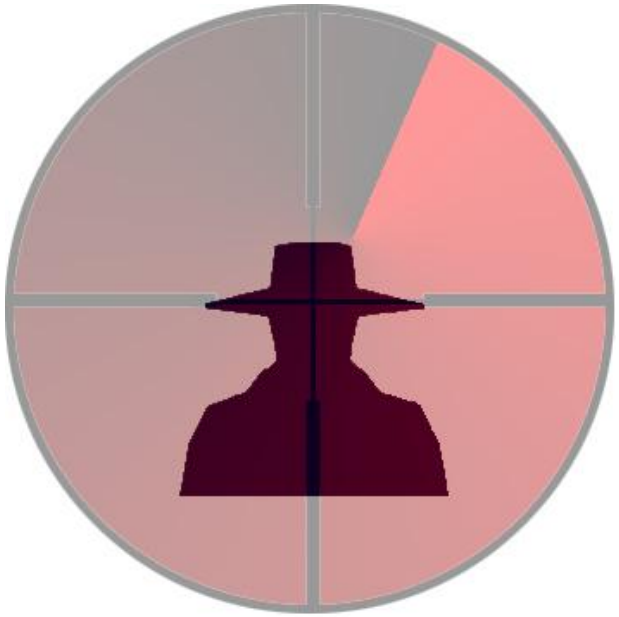
V. Recent Examples & Notable Targets to Date

VI. Q & A

# What is a Targeted Attack?

- Focuses on a specific sector, organization or individual.

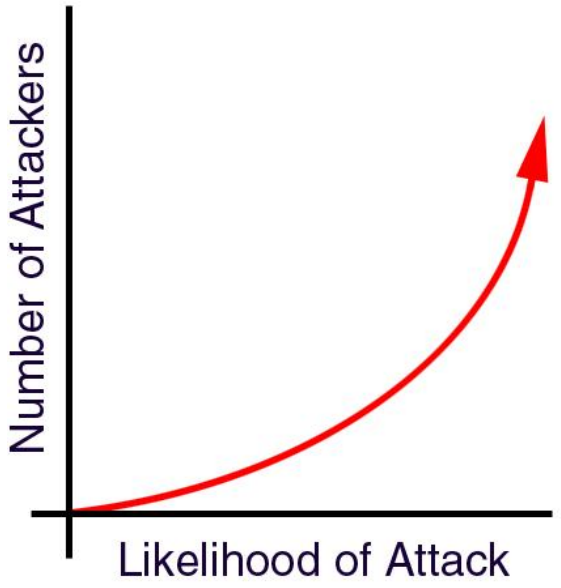
- Typical examples of such attacks include:



  - A hacker defacing US government websites for political reasons
  - A company hiring hackers to steal information from rivals or perform DDoS attacks to shut down their websites
  - Malicious actors targeting specific individuals are targeted to steal money from them or gain elevated privileges on a network

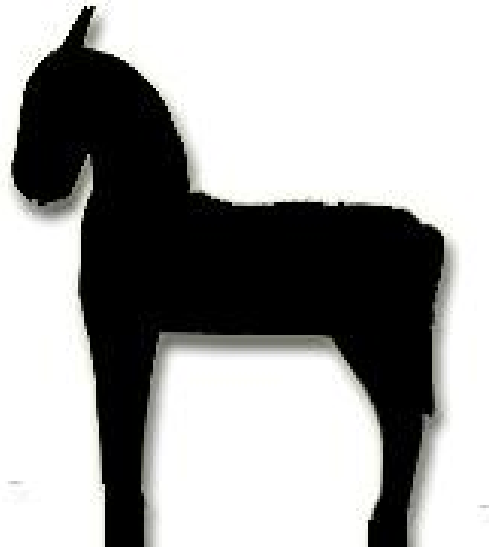
# Current Targeted Attack Trends

- Not sophisticated, performed by low-level attackers (*major factor impacting likelihood*)
- Targets are often profiled well ahead of attacks
- Target high level executives and persons of interest
- Often rely upon social engineering and e-mail delivery for success
- Often attempts to exploit older vulnerabilities (1-3 years old)
- Low-level frequency to avoid detection



# Codes Often Used in Attacks: Outdated

- Exploits
  - Exploit-MhtRedir (MS04-013) Exploit
  - VBS/Psyme (knowledgebase article 870669) Exploit
  - Microsoft Word (MS03-050) Exploit
  - Visual Basic (MS03-037) Exploit
  - Exploit-ByteVerify (MS03-011) Exploit
  - Index Server (MS01-033) Exploit
- Codes
  - Agent
  - Bancos
  - Dloader
  - Lmir
  - MultiJoiner
  - Nethief
  - Riler



# Operation Horse Race: Hotworld Scandal

- May 2005: Israel's largest espionage case ever
- Involves private-investigation firms using Trojan horse programs to steal proprietary data
- More than 20 people allegedly involved in the incident arrested in Israel and the United Kingdom
- 80 companies were involved  over an 18 month period

+Multiple variants of the previously unknown Trojan, Hotworld, utilized in the attacks

+Michael Haephrati, a 41-year-old programmer, arrested

+Paid $3,600 for each customized Trojan; 15+ to date ($54,000 +)

# NISCC Report: June 20, 2005


- High-ranking or well-known company employees of four targeted domains
- Probable industrial espionage motive
- Designed to exploit a vulnerability in Microsoft Word (MS03-050)
- At least three instances of a Petite-packed Trojan horse were reportedly intercepted by MessageLabs in just a few days in early July 2005
- Appears to utilize an abused .CN e-mail address and server.

# CERT Report: July 8, 2005


- "These attacks appear to target US information for exfiltration"
- Trojans sent to targeted e-mail addresses
- Customized to evade anti-virus protection
- Communicates back to attacker over port 80 to defeat firewalls
- Designed to steal sensitive data
  - usernames and passwords for e-mail accounts
  - critical system information
  - network drive enumeration
  - upload additional programs to further compromise the network

# Notable Targets to Using Low-Level Tactics

- Brazilian Businesses via Bancos Trojans
- Strategic US military personnel sent military related e-mails
- High ranking public officials in UK businesses
- High ranking public officials in government and enterprise in India and the US

# Conclusions

- Targeted attacks not caught by A/V
- Keep your systems patched
- Educate key executives & entire organization on social engineering
- Hardening critical systems
  - Limit user access
  - Regularly scheduled maintenance for client machines
- When you encounter Anomalous issues, send it to your security intelligence provider
  - iDefense tracks all Malcode
  - iDefense is tracking malicious actors and methods

VeriSign

iDEFENSE
A VeriSign Company

# Q & A

Where it all comes together.