Evolution and Current State of DDoS Attacks

Eli Jellenc and Josh Lincoln

Threat Intelligence Team

iDefense, a VeriSign Company

Where it all comes together.

Agenda

+ iDefense Overview

+ Availability of Information

+ Timeline of DoS/DDoS Evolution

+ Attack Motivations

+ Attack Tools and Methods

+ Command and Control

+ Defenses

+ Case Study: US Financial Services Firm

+ 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 Team (Malcode)
  - Threat Intelligence Team
  - Rapid Response Team

+ In business since 1998, iDefense became a VeriSign Company in July 2005

iDEFENSE
A VeriSign Company

iDefense Intelligence Services

Daily / Hourly Research Deliverables

+ Comprehensive Vulnerability Feed
  - Most comprehensive, timely, technical feed in the industry

+ iDefense Exclusive Vulnerabilities
  - More than 250 contributors around the globe
  - Released to vendor and iDefense customers only
  - More than 180 iDefense Exclusive vulnerabilities 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

+ Bi-Weekly Malicious Code Review
  - Summary of previous two weeks malcode activity
  - In-depth analysis of specific malcode from the Malcode Lab

+ 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
A VeriSign Company

Agenda

+ Availability of Information

+ Timeline of DoS/DDoS Evolution

+ Attack Motivations

+ Attack Tools and Methods

+ Command and Control

+ Defenses

+ Case Study: US Financial Services Firm

+ Q&A

iDEFENSE
A VeriSign Company

Availability of Information

+ Little incentive for victims to report the event
  - Negative publicity
  - Potential legal compliance ramifications

+ Lack of accepted research strategies
  - Inferential models only at embryonic stages
  - Data collection methods are limited

+ Varied attack characteristics
  - International origins
  - Evolving anonymization tactics
  - Numerous command and control structures
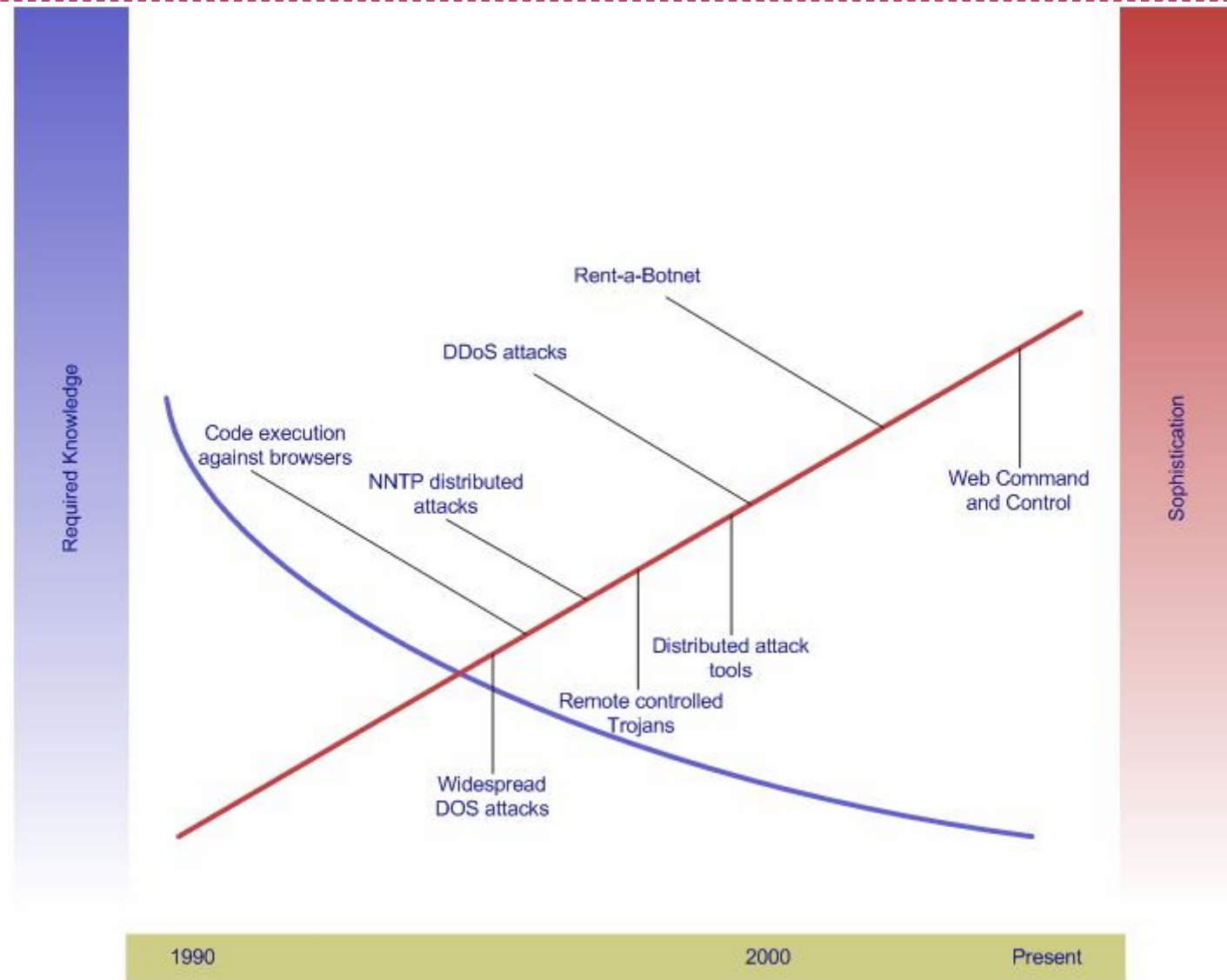
iDEFENSE
A VeriSign Company

Presently Known Characteristics

+ Measurements vary widely
  - 1,000-8,000 attacks per day

+ Vast majority of attacks last less than 25 minutes

+ Nearly all attacks utilize massive botnets

+ Largest attacks exceed 10 Gbps

Attack Motivations

+ Experiments or challenges

  ▪ Script-Kiddies and rival hacking groups

  ▪ Profuse, but are often low-intensity and of short duration

  ▪ In the aggregate, a significant concern

+ Principle-Driven attacks

  ▪ Political, religious or ideological motivation

  ▪ Special interest groups

  ▪ Revenge

+ Sabotage and extortion

  ▪ Pure economic motivation

  ▪ Longer, stronger and often conducted by the best

  ▪ Paying up does not guarantee cessation

Attack Tools and Methods

+ Methods
  - Bandwidth Depletion
    - ICMP flood attacks (Ping of Death)
    - Reflection attacks (Smurf and Fraggle)
    - UDP flooding
    - Amplification attacks
  - Resource Depletion
    - TCP SYN attacks (Synflood)
    - PUSH and ACK attacks
    - Recursive HTTP flood (Spidering)
    - Teardrop, Land, and Naptha

+ Major tools
  - TCP SYN Attacks (Synflood)
  - Trinoo
  - Tribe Flood Network (TFN)
  - Stacheldraht (German for 'Barbed Wire')
  - Trinity
  - Shaft

iDEFENSE
A VeriSign Company

DDoS via DNS Recursion

+ Process
  - Attacker queries for a large, typically altered, DNS record
  - Large response is sent to the target

+ 75-80 percent of DNS servers allow recursive requests

+ Amplification of more than 70x

+ Mitigation requires collective action
  - Packet filtering by ISPs
  - Disable recursive DNS

Botnet Command and Control

+ Agent-Handler attacks
  - No longer widely used
  - Not scaleable

+ IRC
  - Massive increase in IRC bots began in 2004, continues today
  - Limited to tens of thousands of nodes
  - Customized IRC servers and commands
  - Driven by diverse, elegant source code development and modularity
  - Major families
    – AgoBot
    – PhatBot
    – Rbot
    – SDbot
    – Spybot

Botnet Command and Control (cont.)
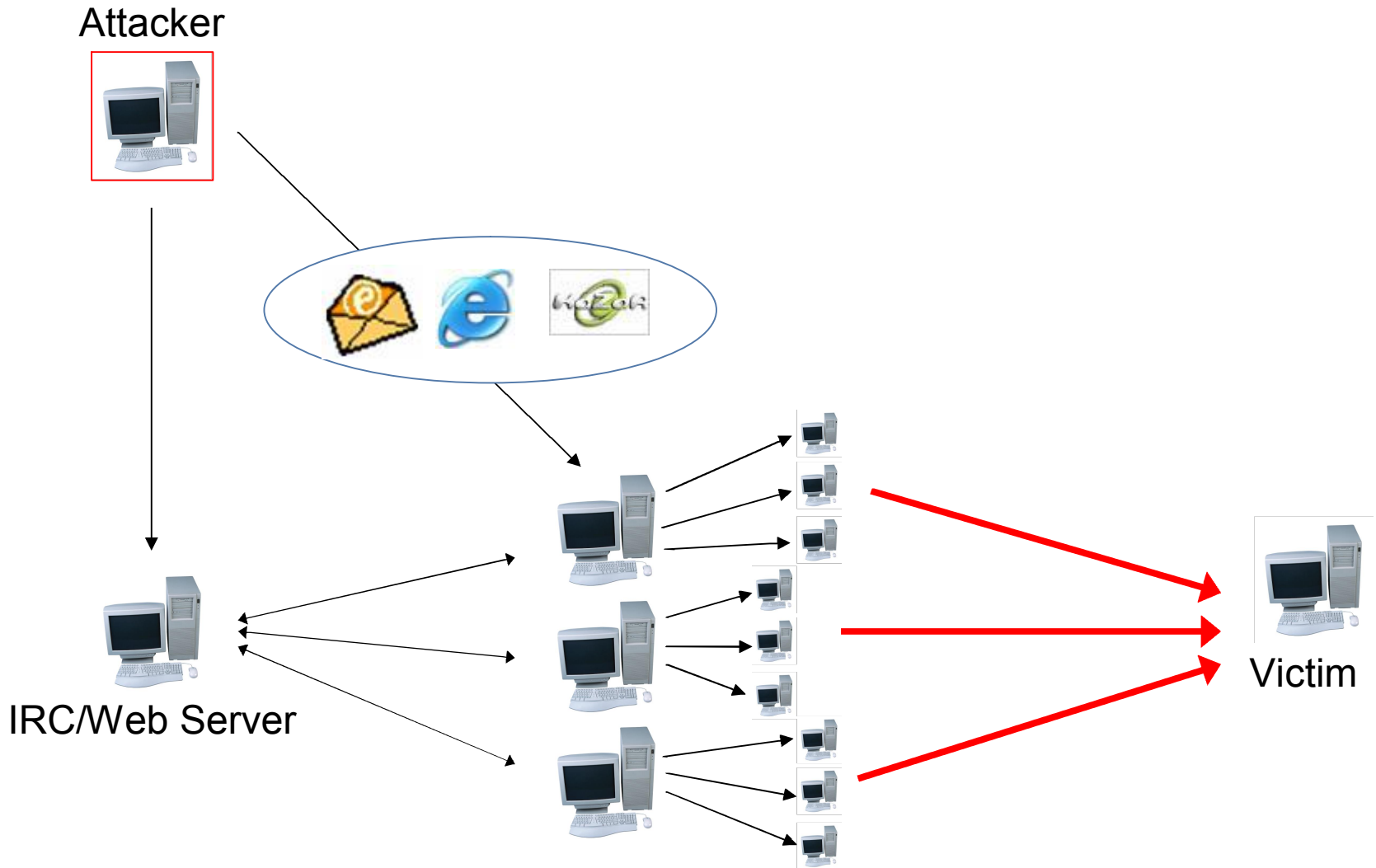
+ Web-based
  - Easy to deploy
  - More scaleable, allowing larger botnets
  - Communication over port 80
  - Easier to use - Easier to sell

+ VoIP
  - Use is speculative
  - Highly anonymous

Structure of a Botnet

Attacker

IRC/Web Server

Victim

Defenses

+ Deck is stacked in favor of the attacker

+ Prevention and mitigation

+ Internal approaches
  - Overprovisioning
    - Bandwidth
    - Hardware
  - Key resources:
    - Trained Staff
    - DDoS-specific appliances
  - Can grow enormously expensive

+ External approaches
  - Independent network analysis
  - Traffic filtering services
  - Emergency response services

Case Study: US Financial Services Firm

+ Began in March 2004, and lasted nearly one year

+ 2,000-4,000 request intensity: 5-6 MB bandwidth consumption

+ Worm spread from Middle East— source never identified
  - Code analysis points to venerable attacker sympathetic to Al Qaeda
  - Coder is not highly skilled, but is well connected to underground

+ Mitigation
  - Syslog appliance
  - Trip wire set at 50,000 requests per eight hour period
  - Suspicious request origins were blacklisted
  - Redirect implementation
  - Law enforcement contacted— hardware seized in the US and Canada

+ The attack continues today, but is insignificant

Q&A

Eli Jellenc and Josh Lincoln

Threat Intelligence Team

iDefense, a VeriSign Company

Where it all comes together.

Thank You