Security Attacks and Defenses

Brian A. LaMacchia
Software Architect
Microsoft Corporation

47th Meeting of IFIP WG 10.4
January 29, 2005

Agenda

- Kinds of attacks
  - Infrastructure threats
  - Monetizing attacks
  - Social engineering threats (phishing)
- Defensive techniques
  - Automatic patching
  - Development tools
  - Run-time techniques
  - Leveraging automated feedback from customers

Kinds of Attacks

- Infrastructure attacks
  - OS/local machine
  - Web server
  - Network protocols
- Some techniques becoming more prevalent
  - SQL injections, cross-site scripting
    - Rooted in poor development practices
  - Building hitlists from Google & other public sources
    - Better saturation of vulnerable hosts
- We’re *not* hearing about attacks on custom applications (if it’s happening it’s quiet)

Attack Goals Shifting

- We’ve seen a dramatic shift in the past 12-18 months in the goal of these attacks
  - Used to be malicious behavior
  - Now it’s financial
- Exploits are used to install Bots
  - Or the info is sold for $$$
- Networks of controlled exploited machines (BotNets) are then sold
  - Spammers
  - Organized crime

Terminology

- Bot
  - Application that performs action on behalf of a remote controller
  - Installed on a victim machine (zombie)
  - Most are open-source
  - Modular (plug in your functionality / exploit / payload)
- BotNet
  - Linkage of “owned” machines into centrally controlled armies
  - Literally, *roBOT NETworks*
- Control Channel
  - Method for communicating with an army
- Herder
  - a.k.a. Bot herder, controller, pimp
  - Owns control channel, commands BotNet army
  - Motivations – money, power

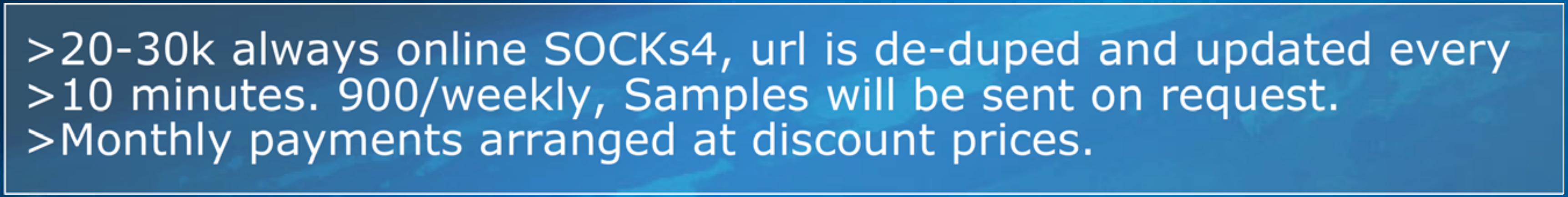
Bots & BotNets

- Bots are prolific
  - Earthlink claims 20% of machines have bots and/or spy-ware
  - May account for 1/3 of all email traffic from comcast.net
- Spam
  - Bots sent 66% of all SPAM traffic on the Internet
  - Bots are rented to spammers
  - Provide mass mailing and anonymity
- Identity theft
  - Some versions include scanners for SSNs and credit card information
- DDoS / Extortion
  - Used for sustained DDoS attacks
  - Used for online extortion against Internet merchants
- Infringement/License violations
  - Scanners for CD keys and content

Monetizing BotNets

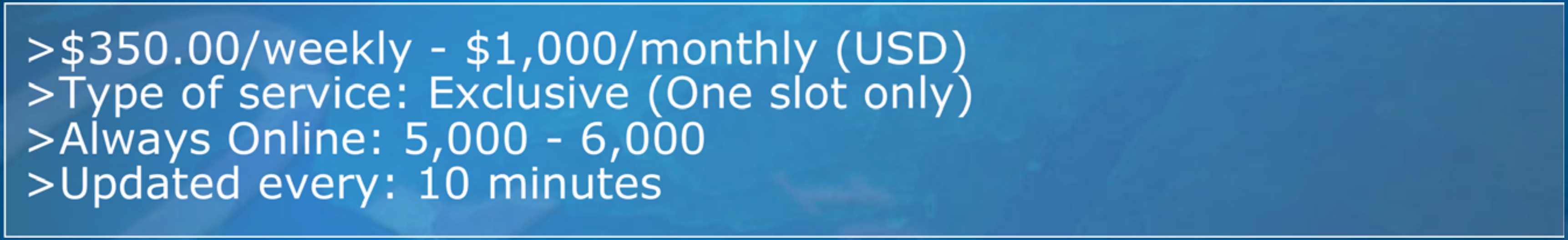
- First large-scale monetization done with MyDoom.A
  - Eight days after MyDoom.A hit the Internet, somebody scanned millions of IP addresses looking for the back door left by the worm
  - The attackers searched for systems with a Trojan horse called Mitglieder installed
  - Then used those systems as their spam engines
  - Millions of computers across the Internet were now for sale to the underground spam community

BotNet Spammer Rental Rates



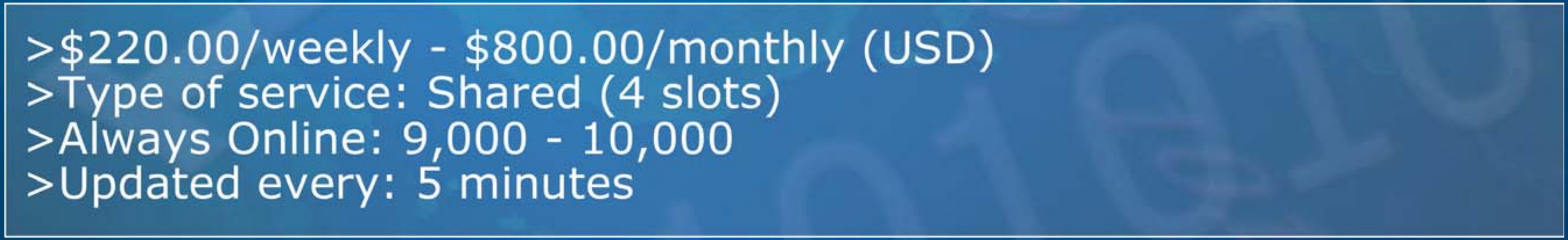
>20-30k always online SOCKs4, url is de-duped and updated every
>10 minutes. 900/weekly, Samples will be sent on request.
>Monthly payments arranged at discount prices.

- **3.6 cents per Bot week**



>$350.00/weekly - $1,000/monthly (USD)
>Type of service: Exclusive (One slot only)
>Always Online: 5,000 - 6,000
>Updated every: 10 minutes

- **6 cents per Bot week**



>$220.00/weekly - $800.00/monthly (USD)
>Type of service: Shared (4 slots)
>Always Online: 9,000 - 10,000
>Updated every: 5 minutes

- **2.5 cents per Bot week**

September 2004 postings to SpecialHam.com, Spamforum.biz

Current situation

- BotNets themselves unseen; uses are noticed
  - Spam relays
  - Identity theft, credit cards, keystrokes, other PII
  - DDoS attacks
- Ease of writing, deploying Bots is increasing
  - GUIs driven by script kiddies (13 year olds)
  - Many don’t know how to program – “personalized” bots
  - Automatic scanning for vulnerable machines
- Threat is escalating
  - Low profile (vs. Slammer / MyDoom / phishing, etc.)
  - Financial opportunity driving activity
  - Model is maturing into tiers – herders, service providers
  - Numbers are increasing
  - Bot technologies are getting better

Bot Pedigree

- Relatively few “families” of Bots
  - Based on open source Bot collaboration efforts
  - Berbew, Gaobot, …
- Custom variants abound
  - Typically see 3 to 5 new variants per week
  - Have seen as many as 50 per day

BotNet use: Data Theft

Bots often have built-in functionality to steal

- Documents or data from an infected computer
- Computer passwords, IRC passwords
- Bank account numbers and passwords
- PayPal account info
- Credit card data
- Keystroke loggers

http://www.lurhq.com/phatbot.html

Botnet use: Extortion

Small-scale: Even small BotNets (a few hundred machines) can extort online businesses for money.

- Small site in Kentucky taken down for a week because they refused to pay $10k

http://www.courier-journal.com/business/news2004/05/10/F1-scam10-8568.html

Large-scale: Crime rings extorting business for "protection monies“.

- A number of UK gambling sites have been offered protection for $50k/year

http://www.rense.com/general44/hack.htm

Attack Trends

- From isolated to networked
  - Attacker is on the “outside”
- From programs to services
  - Unconstrained input
- From multi-user to single user to multi-user
  - “User as admin” problem
- From asynchronous to mass malware
  - Asymmetry favors attacker
- From vandalism to for profit
  - More dedicated attackers
- From specific to general to specific
  - Value will draw more sophisticated adversaries

Phishing Attacks

- Much more than a nuisance
  - Hotmail is blocking ~3B pieces of spam per day, much of it phishing attacks
- Most people (>60% of the American public) have inadvertently visited a fake or spoofed site.
- Over 15% of respondents admit to having provided personal data to a spoofed site.
- Trending upward: more fake e-mails, spoofed Web sites and phishing scams.
- Most vulnerable targets: banks, credit card companies, Web retailers, online auctions (E-bay) and mortgage companies.

Losses from Phishing

- Estimated economic losses:
  - Small number of people (slightly more than 2%) affected, with an average cost of $115 dollars/victim.
  - Extrapolating to the entire U.S. population, economic impact of fraud close to $500M.

Defensive Techniques

- Automated patching
- Development tools
- Run-time techniques
- Leveraging automated feedback from customers

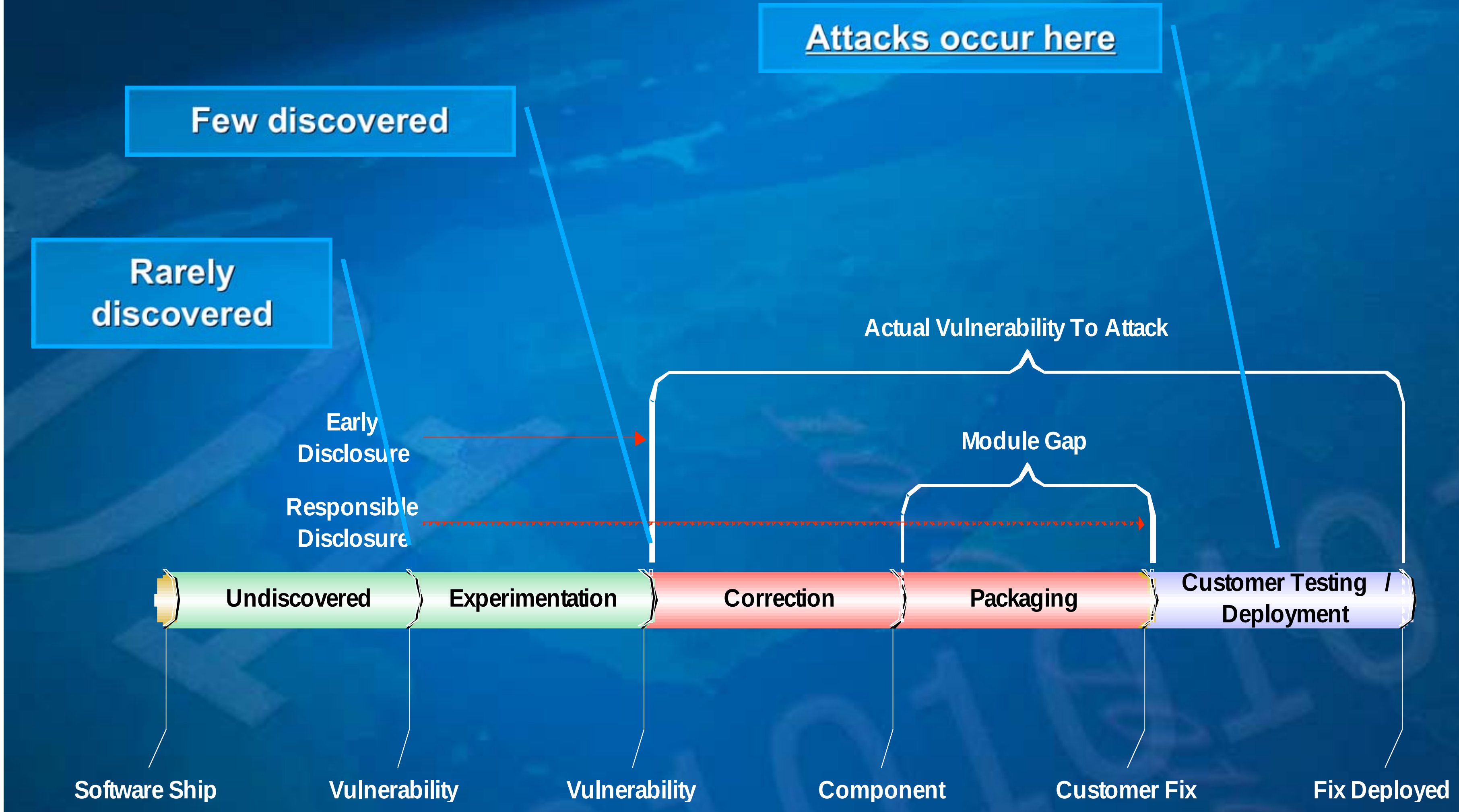
First, Some Numbers

- 656.5M PCs run Windows Client worldwide
  - OEMs shipped 115.4M Windows PCs in 2004
- MS Malicious Software Removal Tool
  - Released 1/11/05 – targets 8 families of malware
  - As of 1/27/2005
    - Run over 104M times
    - Over 177K infected hosts cleaned
- MS Anti-Spyware Beta
  - Over 3M downloads in <2 weeks

Automatic Patching

- Windows Update services 190M PCs
- 140M PCs use Automatic Updates to stay current with patches
- Time to update 95% of XP PCs with a patch via Automatic Update
  - <14 days

Vulnerability Timeline



Attacks occur here

Few discovered

Rarely discovered

Actual Vulnerability To Attack

Early Disclosure

Module Gap

Responsible Disclosure

Undiscovered

Experimentation

Correction

Packaging

Customer Testing / Deployment

Software Ship

Vulnerability

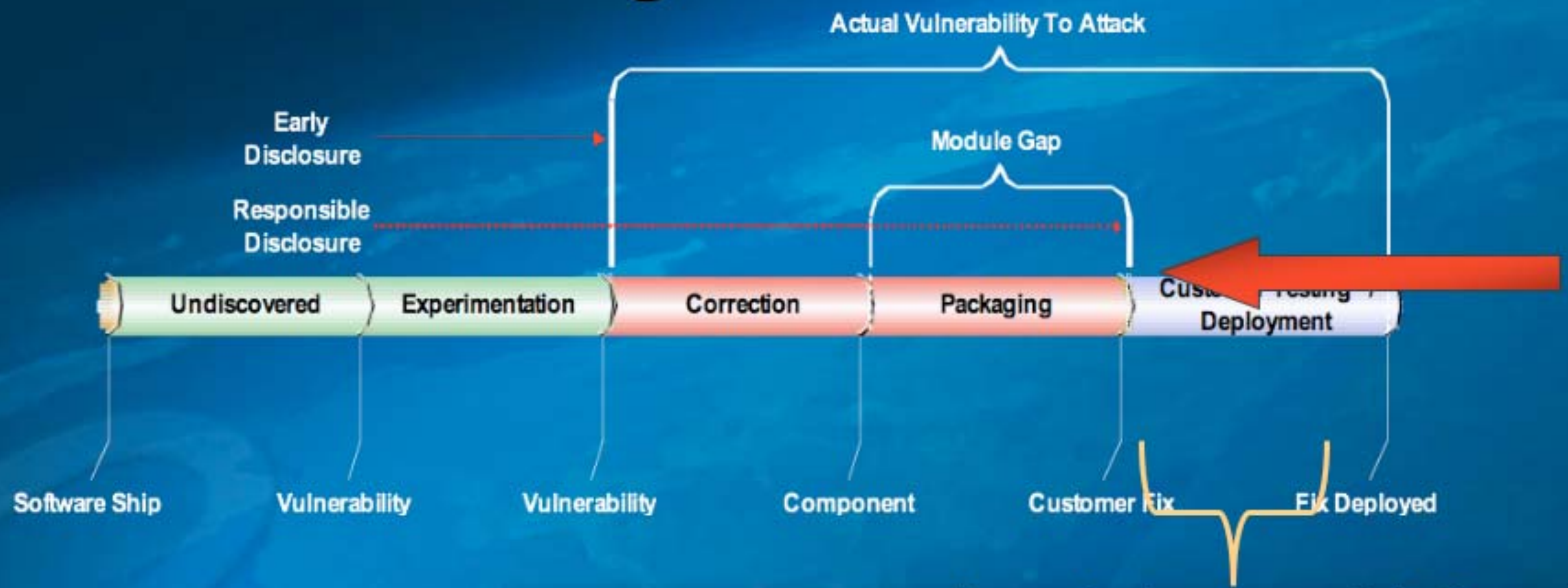
Vulnerability

Component

Customer Fix

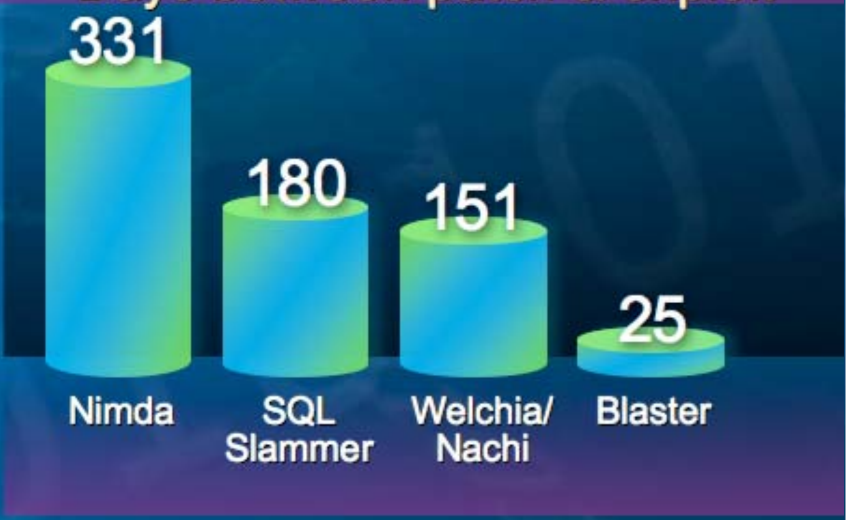
Fix Deployed

Vulnerability Timeline



- Days From Patch To Exploit
  - Have decreased so that patching is not a defense in large organizations
  - Average 9 days for patch to be reverse engineered to identify vulnerability

Days between patch & exploit



Development Tools

- Source code defect detection tools
  - PREfix & PREfast (C/C++)
    - Detects defects like bounds violations, resource exhaustion, memory management errors, format string errors, etc.
  - FXCop (MSIL -- .NET managed code)
    - Detects defects in these categories: Library design, Localization, Naming conventions, Performance, Security
- Developers run versions of these tools before checking code into a product tree.
  - We also integrate the tools directly into the build process for automatic scans & bug reporting

Run-time Techniques

- Dynamic input scanning
  - Ex: URL filtering
- Middleware-based isolation
  - JVM, CLR, other host-based VMs
- OS virtualization
  - VMWare/Virtual PC/Xen
  - Hypervisors (IBM sHype, Intel VT)

Leveraging Customer Feedback

- MS Online Crash Analysis
  - Mechanism for reporting errors back to Microsoft, along with some debugging & tracing information (“minidumps”)
  - OCA reports are bucketed by application/module offset information
  - Minidump analysis identifies likely buffer overruns & other issues
  - Potential code defects automatically flagged for developer review

Summary

- Attack frequency ↑
- Spyware ↑
- Vandalism → monetary objectives
- Patch reverse engineering time ↓

Blatant Workshop Plug

- DIMACS Workshop on Security of Web Services & E-Commerce
  - May 5-6, 2005
  - DIMACS Center, Rutgers Univ. Piscataway, NJ
  - CFP deadline: February 11, 2005

http://dimacs.rutgers.edu/Workshops/Commerce/

Questions?