

# Protecting Your e-Commerce Website

Web Infections and Protections 2002

MnIPS Meeting  
Tuesday February 19, 2002

Copyright (c) 2002 Extratelligence

# Today's Presentation

- Based on Practitioners Perspective
- Assumptions and Infectious Agent Model
- Current Threat Levels and Incidents
- Action Plans

Copyright (c) 2002 Extratelligence

# Assumptions

- Living in a highly hostile computing environment with both individuals and groups actively seeking to impact the quality of the computing environment
- Not everyone will have security as a primary concern or have strong support available
- Continuing evolution of the Internet

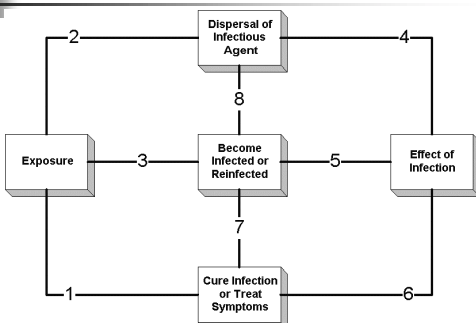
Copyright (c) 2002 Extratelligence

# References

- Based on previously published (IEEE) work on "Web Infections and Protections" between 1997 and 2001
- Previous IEEE Tutorials at IEEE CompSAC, IEEE LCN, and private sessions

Copyright (c) 2002 Extratelligence

# Infection Model



Copyright (c) 2002 Extratelligence

# Connections

1. Exposures can be treated after acquisition prior to effects occurring
2. Dispersal of infection can occur prior to effects
3. Exposure to infectious agents results in active infection
4. An effect of infection can be dispersal of infectious agents

Copyright (c) 2002 Extratelligence

## Connections (Continued)

5. Infections can result in damage or resource use
6. Cure can address cleaning out an infection or treating symptoms
7. Reinfection can result after treating only symptoms or after cure
8. Reinfection or infection can occur as part of active infection

Copyright (c) 2002 Extratelligence

## Current Threat Levels

- Threat to and from the Internet (DNS attacks)
- Attacks against local Networks (DoS)
- Attacks against local computing services (e-mail, web server, applications) (stealing service)
- Attacks against individual computing (desktop/laptop, PDA, telecomputing)

Copyright (c) 2002 Extratelligence

## Selected References

- Proceedings, IEEE Aerospace Conference, 1998, "Java, Agents, and Chronic Infections"
- Tutorial, IEEE Local Computer Networks Conference, 1998, "Web Infections and Protections"
- Panel Presentation, IEEE CompSAC, 2000
- Panel Presentation, IEEE CompSAC, 2001

Copyright (c) 2002 Extratelligence

## ILoveYou/Melissa and Outlook

- This still occurs due to unpatched versions of Microsoft Outlook.
- Versions have different levels of damage and dispersal.
- Updates are not common enough to eradicate any infection past 2M systems.

Copyright (c) 2002 Extratelligence

## Code Red/Code Red II

- On July 19 2001, the Code Red worm infected more than 250,000 systems in just 9 hours. (Source: Microsoft)
- Exploited IIS Index Server Flaw from Default Installation
- Estimates of Code Red II run to more than 1M Systems

Copyright (c) 2002 Extratelligence

## NIMDA Dispersal (CIAC)

- From client to client via email
- From client to client via open network shares
- From web server to client via browsing of compromised web sites
- From client to web server via active scanning for and exploitation of the "Microsoft IIS 4.0 / 5.0 directory traversal" vulnerability (VU #111677)
- From client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

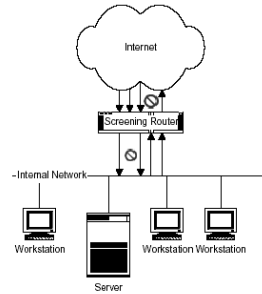
Copyright (c) 2002 Extratelligence

## Threats and the Internet

- Ideal mechanism to disperse infectious agents and attacks (Code Red)
- Geographic independence of attacker and those threatened (PTT incident)
- Final reservoir of infections and protections (NIMDA infection widespread within 12 hours of launch)

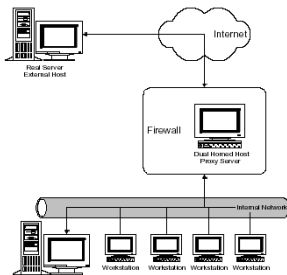
Copyright (c) 2002 Extratelligence

## Screening Router



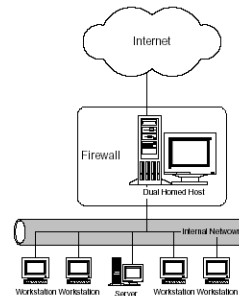
Copyright (c) 2002 Extratelligence

## Proxy Server with dual homed host

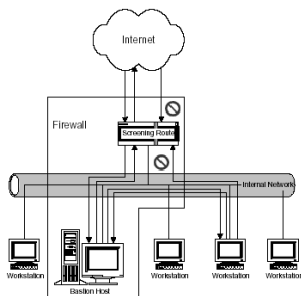


Copyright (c) 2002 Extratelligence

## Dual Homed Host

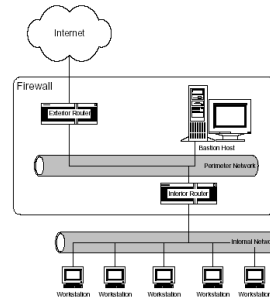


## Screened Host



Copyright (c) 2002 Extratelligence

## Screened Subnet

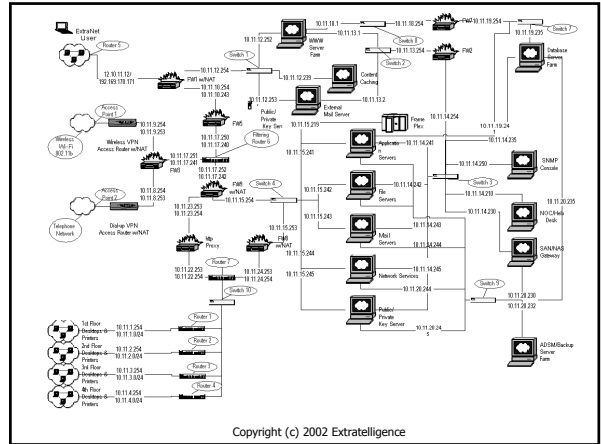


Copyright (c) 2002 Extratelligence

## Double Hosted Firewall Designs

- Protect against outside world in conjunction with router configurations.
- Can handle multiple network routings.
- Provide highly configured barrier against intrusion.
- Protect inside world with proxy services and filtering.
- Provide services to inside world such as IP address translation.
- Provide filtering opportunity for internal traffic.
- Requires interlocking router and server configuration.
- Frequent updating required.

Copyright (c) 2002 Extratelligence



## Local Threats

- Local threats against both the local network (LAN, PVN, etc.) and services (e-mail, webs, servers, telephones, applications).
- Denial of Service (DoS), breach of security, or service stealing
- Detection and identification are difficult
- All threat management costs money

Copyright (c) 2002 Extratelligence

## Threats to Individuals

- Individual computing is becoming pervasive (roaming on multiple machines, PDAs, wireless, and node computing)
- Threats affect gigantic numbers of machines
- Any connected machine is threatened

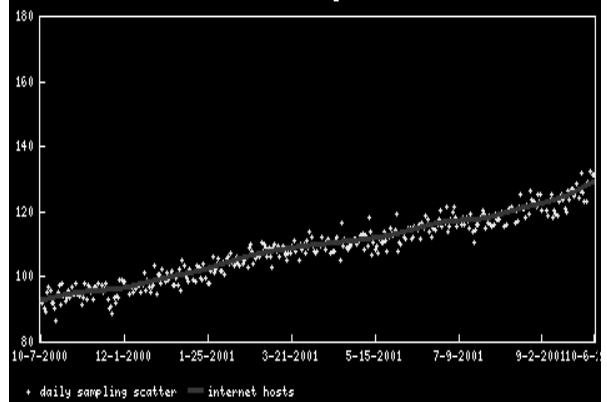
Copyright (c) 2002 Extratelligence

## Why care?

- Stolen identities nearing critical levels
- Anonymity (different by culture) is threatened (e911, 3G, PDAs)
- Invasion into work and personal life

Copyright (c) 2002 Extratelligence

Growth of the Internet During the Year From 10-7-2000



## ILoveYou, Melissa, and more

- Rapid spread of infection affected systems worldwide across multiple OS (Microsoft based scripting)
- Java viruses already known
- Internet worms already have resulted in prison time for inventors (KM)
- LA Times Recommendation

Copyright (c) 2002 Extratelligence

## Code Red/Code Red II

- Limited to NT IIS Web Server Attacks
- Extremely high distribution of vulnerability means extremely high rates of dispersal and infection – active agent
- More infectious on more network bandwidth (any IP)
- GG Recommendation based on TCO impacts

Copyright (c) 2002 Extratelligence

## NIMDA

- Worst characteristics of Code Red and other prior infections
- Multiple vectors of dispersal
- Intel-CPU based infection

Copyright (c) 2002 Extratelligence

## SNMP Vulnerability

- Cross Vendor warning from the SANS Institute warning (CA-2002-03)
- Preliminary testing showed every piece of equipment is vulnerable, including servers, routers, switches, etc.

Copyright (c) 2002 Extratelligence

## 10 Emerging Threats: 1998

1. Cable Modems (and other high speed links) that enable Windows specific vulnerabilities for large populations
2. AOL Password stealing via Infected E-mails
3. MS Outlook/Exchange Script-based Vulnerabilities (server and client based)
4. Server agent based breaches (Lotus Notes, Exchange, SendMail, others)
5. Wireless Exposed Vulnerabilities (wireless data, CDPD data, GSM data)
6. Personal Appliance Replication on networks (Palm, Windows CE)
7. Converging Technologies (digital wiretapping, game consoles, set tops)
8. Version-'itis' of software (Win 2K, NetScape, others)
9. 'Free Software' (Linux, StarOffice, others)
10. 'Instant' messaging breaches

Copyright (c) 2002 Extratelligence

## Emerging Threats: 2001

1. Continued threat to the installed base of systems means that 'dormant' viruses will be huge threats (CodeRed, Nimda (?), others)
2. Emergent cell-networks will produce newer even more widespread problems
3. Application-based attacks will emerge
4. Denial-of-Service attacks will become the most common
5. Anonymous attacks by proxy machines will become normal
6. Infowar incidents will be the catalyst for major attacks
7. Infrastructure attacks will become known (electrical utilities, public utilities, transportation)
8. Governments will become major participants in countermeasures
9. Cost of Ownership levels will inhibit innovation
10. Attacks with social engineering will increase combined with attacks on privacy and identity

Copyright (c) 2002 Extratelligence

## 10 Countermeasures

1. Rapidly updated rule based firewall automation services (ISS BlackICE, TrendMicro)
2. Security servicing via out-tasking (Subscription and managed services)
3. AI network active monitoring (Symantec)
4. Agent based behavior pattern recognition (AdAware)
5. Hardware based authentication (SecureID)
6. 'Over the shoulder' active agents (ZoneAlarm, TCP Wrappers)
7. Role frameworks in task security management (PICS)
8. Risk driven activity profiling (safewall at work based on job task eeds)
9. Software integrated personal authentication for applications (Passport)
10. Software designed for better security (Secure Linux)

Copyright (c) 2002 Extratelligence

## 11 Basic Things to Do

1. If you have high speed access, then use a double bastion firewall and proxy. Access modems should use NAT.
2. If you have a web site check it regularly to see it hasn't been hacked.
3. Keep browsers up to date. (IEUpdate, SmartUpdate)
4. Do multi-generation backup and archiving regularly. Use RAID for servers.
5. Guard privacy. Never give out passwords or financial profiling.
6. Minimize network protocols. (Turn off NetBEUI, IPX/SPX) Use WEP.
7. Use active anti-virus software updated regularly.
8. Use encryption locally and on protocol transport.
9. Review audit trails and logs frequently.
10. Observe netiquette. Avoid sites who violate it.
11. Avoid the use of wireless networks.

Copyright (c) 2002 Extratelligence

## What Me Worry?

- You don't have to pay attention. The problem will come to find you.
- You don't have to change your state-of-practice. The start-of-the-art will change faster than you do.
- You don't have to change your process. The rest of the world will change without you.

Copyright (c) 2002 Extratelligence

## Further Discussion

- Bruce Healton  
[bruce.healton@extratelligence.com](mailto:bruce.healton@extratelligence.com)
- Arnold Kwong  
[arnold.kwong@extratelligence.com](mailto:arnold.kwong@extratelligence.com)
- Rodney Lancaster  
[rodney.lancaster@extratelligence.com](mailto:rodney.lancaster@extratelligence.com)

Copyright (c) 2002 Extratelligence

