

ShmooCon 2007

March 24th 2007

Designing and Responding to Targeted Network Attacks Against the Enterprise

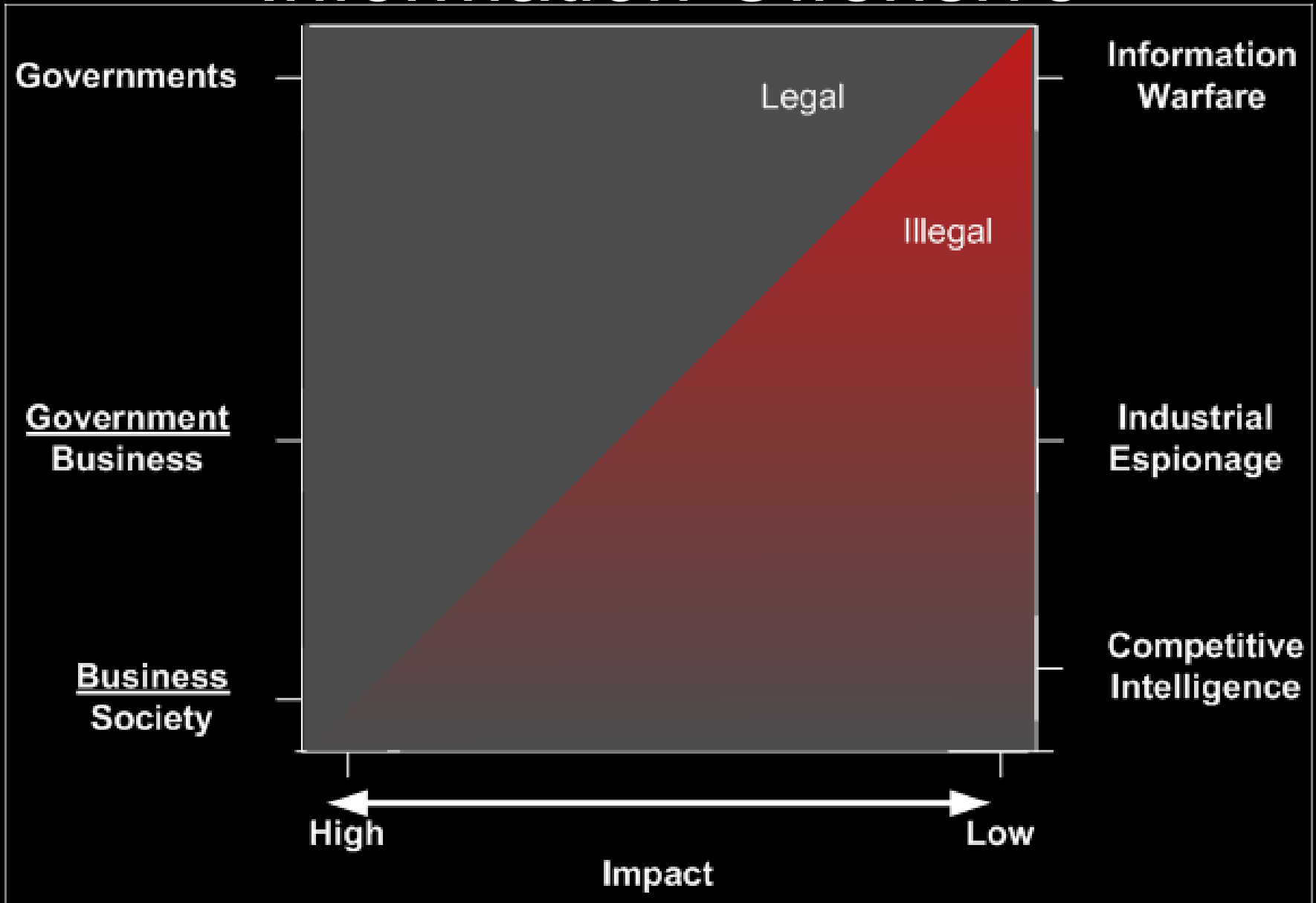
Michael Murphy, CISSP

Cygnus

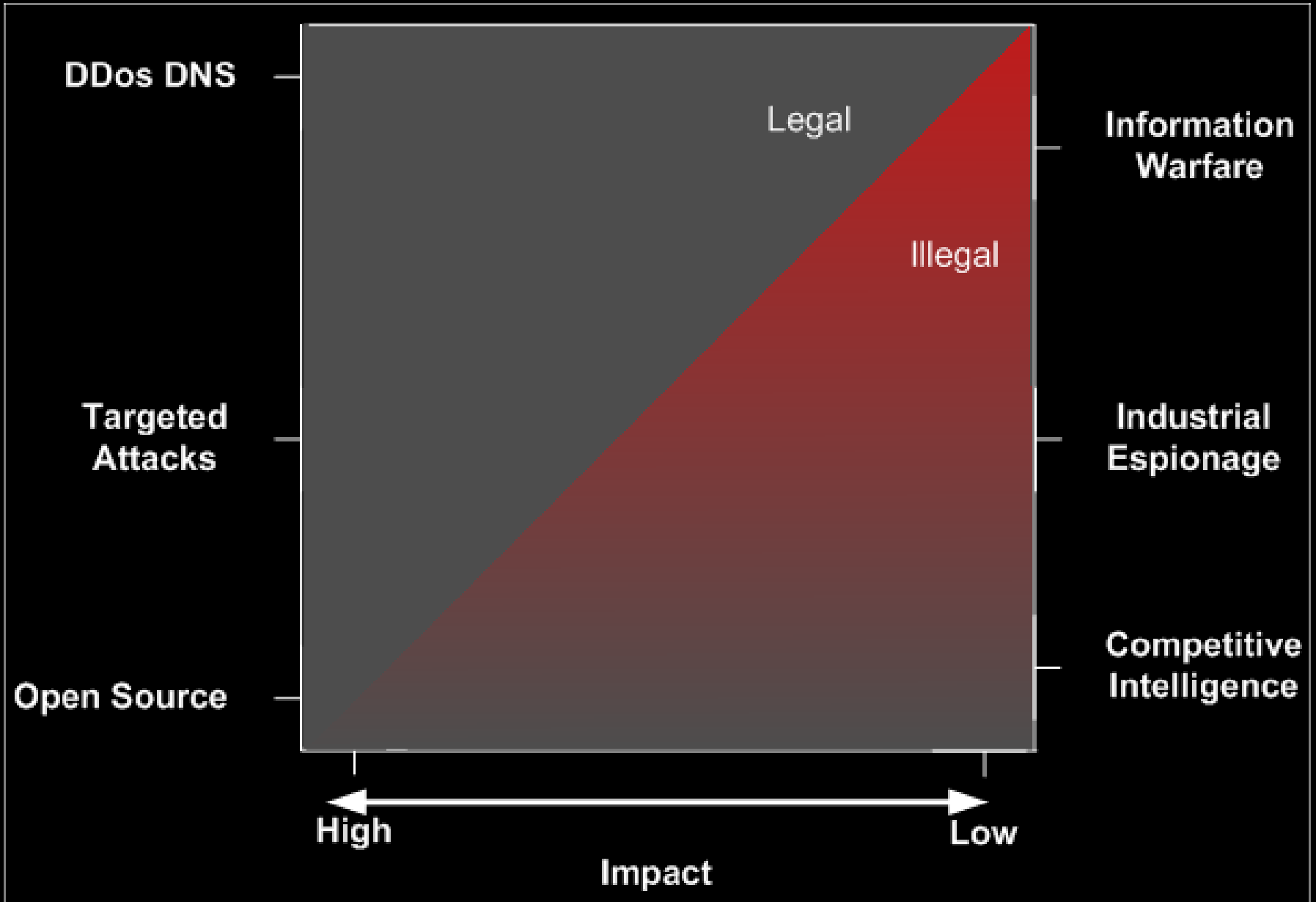
Agenda

- Context
- Reconnaissance and Design
- Attack
- Defense / Response
- Questions

Information Offensive



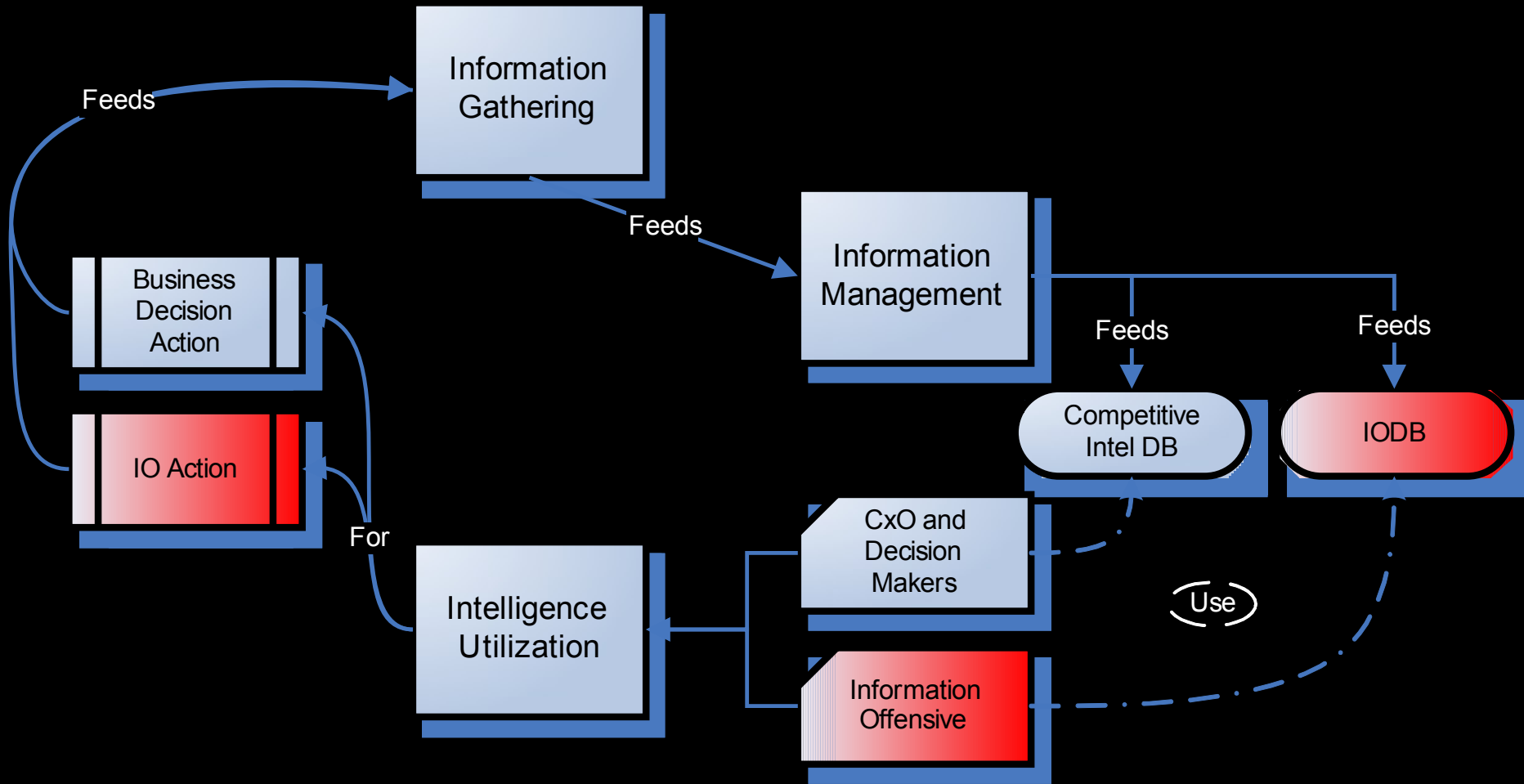
Network Related Offensive Actions



Context

- Attacker motivation?
- Automated security works but there is human interaction
- Traditional goals of an attack
- The goal is not to attack the network but the enterprise as a whole through its people.
- To control or influence a decision maker's actions.

IO Place in the organization



Net Attack Info Gathering

- Open Source
 - Web
 - Company Web
 - FCC
 - Patents
 - Legal filings
- Past/Current employees
- Industry knowledge
 - Trade shows
 - Publications
- Internal knowledge
- Suppliers
- Information systems
 - Software and system providers
 - Network mapping
 - Attacks

NetOpp IE Planning

- Defining a goal and targets
- Determine if sufficient intelligence exists for success
- Network attack example
 - Primary
 - Trade Secrets
 - Secondary
 - Business information
 - Foothold for future attacks

Attack Design

- Who / What are you attacking
 - What networks and systems do they own
 - What address space do they reside in
 - IP ranges, Domains
 - Types of people who work there
 - Types of software those people use
 - Something specific to the industry that can be exploited?
 - Servers, Client OS, Browsers

Recon

(Build a target model)

- Find the targets network surface area
 - IP ranges, domains, and the providers of the target's and their business partners infrastructure
 - Whois, ARAN lookup, news
 - Enumerate all services
 - typical scanning but intelligently
 - Banners, web apps, bad security
- Know the business relationships intimately
 - Learn how their network makes their business flow.

Recon

(continued)

- Discover primary applications for each business unit
 - When singling out business units use exploits designed for those applications
- Data mine the target and business partners public website
- Is the target already compromised?
 - Who?
- Goal is to build a model for all points of entry. NOT to exploit the first or easiest security hole.

Social Recon

- Conferences/expos; Local Bar; Etc and so forth
- Build organizational chart
- Publication search
- Presentation search
- Help wanted?
- Media

Attack Recon

- Email recon
 - Legit correspondence with target users for email cribs
 - Benign attacks to determine network security
 - Disguised as Spam and Phishing
 - Track successful methods
 - Gullibility of target users
 - List of legit users vulnerable to attack

Attack Recon

(continued)

- Network routing and timing
 - Determine network layout and security devices
 - IT blogs, news groups, expert sites
- Web apps
 - Check browser version and user agents
 - Find out what plugs are supported
 - Check the IP space they browse from
 - Do all go through one proxy?

The Attack

“The attacks are also very well researched, Shipp said. One targeted Trojan was sent to five employees at one company--every single person was a member of the firm's research and development team.”

<http://www.securityfocus.com/news/11418/1>

The Email Attack

- Who do you target?
 - Marketing/Sales People
 - Distribute contact info at events
 - Product information
 - Engineers
 - Product Experts
 - Limited customer contact
 - Mid to High level execs
 - They have access
 - Admin Assistants
 - Under paid, over worked

Send and Receive...

- Email with attachment
 - Ask the recipient to review the contents of the attachment
 - Use a real document so the person isn't tipped off
 - Use a vulnerability to drop an executable
 - Exe installs itself
 - Exe beacons to site you control
 - DNS, HTTPS, HTTP
- Phishing email
 - Spoofed from person A to person B with the correct signature block
 - Email contains a link to a site which you control
 - Steal the client IP and the account it was sent to

Quote

“During the 12 months studied by Shipp, the majority of the Trojan horse programs, almost 70 percent, used a malicious Word document as the vehicle for the attack. That's already changing, with PowerPoint and Excel documents now becoming popular, he said.”

<http://www.securityfocus.com/news/11418/2>

Web Site Attack

- Limit the victim list
 - Know the IP range of the network you're after
- Different pages for different intended victims
 - New Product Announcement
 - Trojaned Document
 - Media presentation
 - “requires” a plugin ;)
 - Financial info
 - Quarterly results contain exploit
 - Audio file of quarterly stock holders meeting requires a “special” player

The Backdoor: Hiding it

- Rootkit isn't necessary
 - Have it blend in
 - Make sure AV doesn't detect it
 - Build it specifically for your target
 - Its only going to be seen by the targeted company
 - Change time stamps
 - Hook other critical processes
 - Explorer
 - Scvhost

The Backdoor: Communication

- Make its communication blend in
 - Https, HTTP, DNS, Mail Headers
 - Use info you have already gathered from traffic to your site and emails sent from them
 - Use existing programs
 - Email
 - IE / Firefox
 - Encrypt the traffic
 - 443 (SSL or Custom)

Backdoor: Protection

- Virtual Machine detection
 - Offensive Computing
 - <http://www.offensivecomputing.net/?q=node/172>
 - Forces it to be run on a real box
 - See talk on Sandnets by Joe Stewart
- Anti-reversing Techniques
 - Junk code
 - PE Header Modifications
 - Custom packer

Control of the Backdoor

- To be safe all communication is initiated from inside the network
 - Beaconing
 - DNS
 - HTTP/HTTPS
 - Email
 - P2P / TOR
 - Depends heavily on the level of security found on the network
 - Highly anonymous and hard to track
 - Reverse shell over 443 and encrypted

Beaconing

- HTTP
 - Make sure the User Agent is the same you captured when they visited the site
 - Be aware of proxies
 - Traffic not going through the proxy is very easy to spot
- HTTPS
 - Ensure it blends in well with other traffic
 - Remember people don't log into their email when they aren't at work

Beaconing

- DNS
 - Use internal DNS servers
 - Do not make direct DNS request to a machine you control
 - Keep it RFC compliant
- Email
 - Internal
 - Headers and or email content
 - Webmail
 - Hotmail, Gmail, Yahoo...

Email Beacons

- Use external email
 - Trojan logs into a webmail account and “reads” email for commands
 - Benefits
 - Encrypted (IDS won’t see it)
 - No trace on the company mail servers
 - Blends right in with other web mail traffic
 - Can send attachments with corporate data back
 - Gmail could be the next IRC

Automated Functions

- Complete listing of files found on the drive
- Steals address book
- Steal the SAM file
- Capture security settings
- Capture network information
 - IP, DNS Servers, Gateway,
 - Network Shares Available
 - ARP Cache

Automated Continued

- String searches inside files
 - Passwords
 - Company data
 - Product data
- Attack last 3 OS remote vulns on local LAN
- Attempt dictionary attack against admin account

Reverse Shell

- New tools can be installed and uploaded
- Lateral attacks and information gathering
- Use the current pc as a platform for more social engineering attacks
 - Email link to a doc on the file server that is trojanized to other coworkers
 - No one expects file on the local fileserver to be bad

Defense and Clean Up

"Your problem is no longer how do I avoid being attacked, but how do I find where I've been compromised."

Defense

- Your defenses will only make it more difficult for the attacker, not impossible
 - IDS/IPS/Firewalls/Filtering Devices
 - Critical but can only do so much
 - Assume the attacker will get in
 - Limit his ability to hurt you
 - Design the network to not have a soft core
 - Have an incident response team
 - Documented Procedures
 - Experience

Train Your Users

- The easiest way in is your users
 - Teach them the dangers of acting on a link or file
 - Train users to spot and report suspicious emails
 - Train users to report when an office application crashes after opening an emailed document

Protect your Email

- Digitally Sign internal emails
 - Validate all internal email
 - Employee spoofing can't happen
- Consider disallowing HTML email
 - Spoofed links will be easy to see
- Deny email that is spoofed
 - IP != Domain its “coming” from
 - Not always accurate / DNS is broken
 - RBL's
- AV / Spam filtering

Web Surfing is dangerous

- Good content filtering is a must
 - Filter files which contain known viruses
 - Consider disallowing regular users the ability to download packed exe's
 - Some proxies / content filtering devices are capable of examining office documents
 - IPS products may also recognize exploit code

Detecting the compromise

- Real Time
 - Are signatures going to detect a targeted attack?
 - Anomaly detection won't work on traffic that is created to blend in
 - IPS don't block unknown exploits
 - If you have multiples IDS/IPS is the data being properly correlated
- Historical
 - Log Files are Critical
 - DNS
 - DHCP
 - IDS / IPS / Firewall
 - VPN
 - Mail Server logs
 - SQL / Web server logs
 - Proxy Logs

Dumb Luck

- Users
 - Report their machine crashed
 - Report they can't seem to get a office document to open
 - Report their browser keeps crashing when they try to visit a link
 - Account mysteriously locked out

Clean Up

- Corporate Incident Response Team
 - CIRT procedures should be well defined
 - Experience counts
 - Time until detection is critical
 - Talented attackers may only be on your network for a matter of hours or days
 - Data exfiltration will start immediately after the compromise

Procedures

- Authority must be delegated to the CIRT to take actions to protect the network
 - Pulling a business critical machine offline has consequences
 - Do you leave it online for a short bit to gather more information?
 - Do you leave it online to start up a backup machine?
 - Law Enforcement
 - What situations are handled internally, what situations require law enforcement involvement?
 - If law enforcement is called how is evidence handled so that it is valid in court?

Locate Compromised Machines

- Find a compromised machine
 - Locate the backdoor and associated files
 - Determine the method of communication
 - Run it in a lab environment
 - Reverse Engineer it
 - IDS / Firewall Log analysis
 - Find the other machines communicating with the attacker
 - Hash the malware
 - Search for those files across the enterprise

Recovery

- Block IP's
 - Attacker
 - Point of infection
 - Website / Email
- Black Hole Domain Names
- Develop IPS signatures to block future traffic
- AV sigs for the malware
- Patch for the exploit used

Conclusions

- Attacks like these are very difficult to detect and prevent
 - 0Day not necessary but can be helpful
 - Users are socially engineered
- Detection and prevention tools are not up to the challenge and will fail
- User training is critical
- A good CIRT can limit the damage of an attack
- Organizations are targeted in a holistic manner