Information Security Summit 2007

Beyond Anti-Virus: Detecting and Suppressing Malicious Software

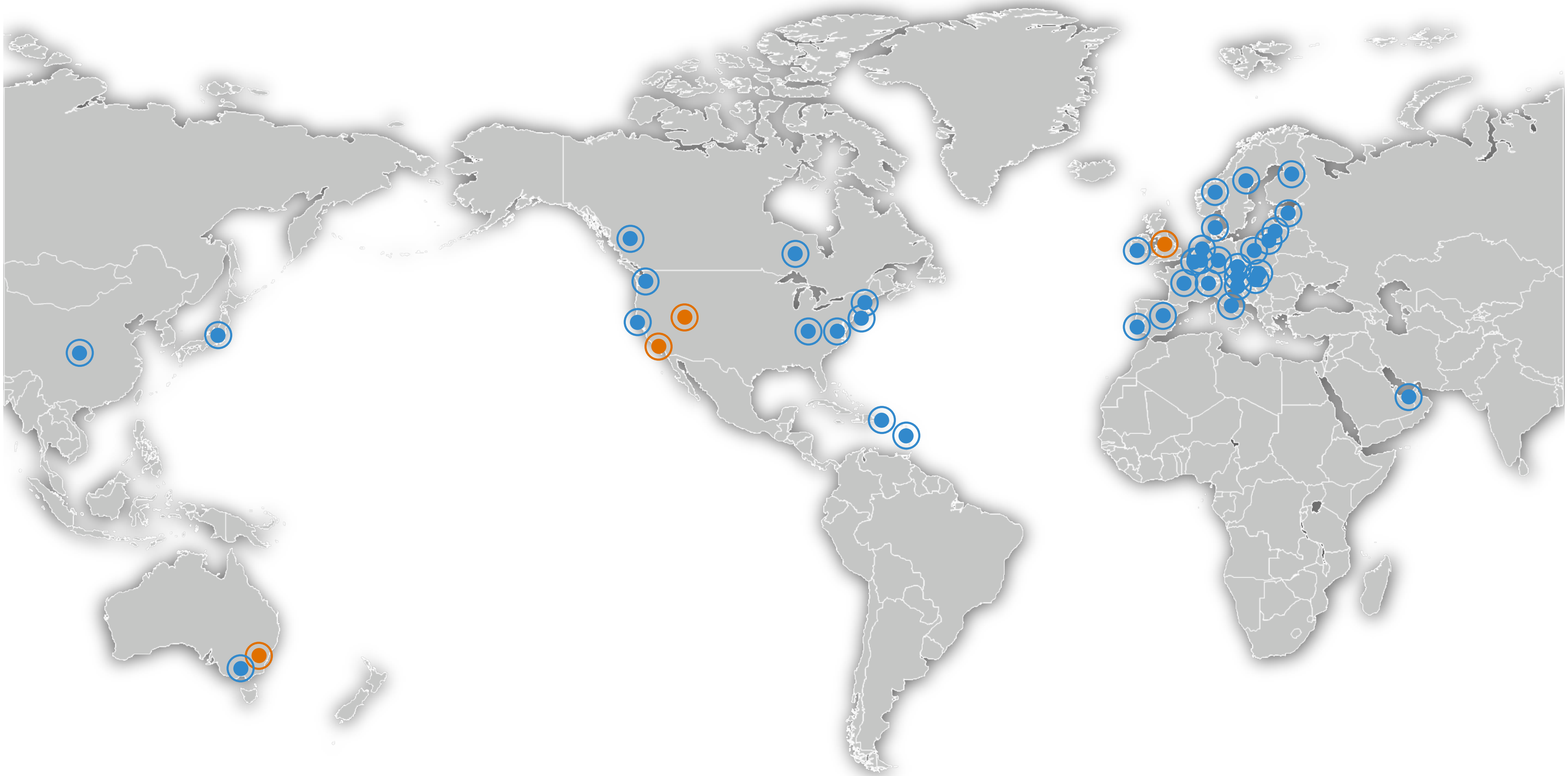
September 11th, 2007

Ron Dilley
Principal Information Security Architect
IS Security
Enterprise Architecture and Security

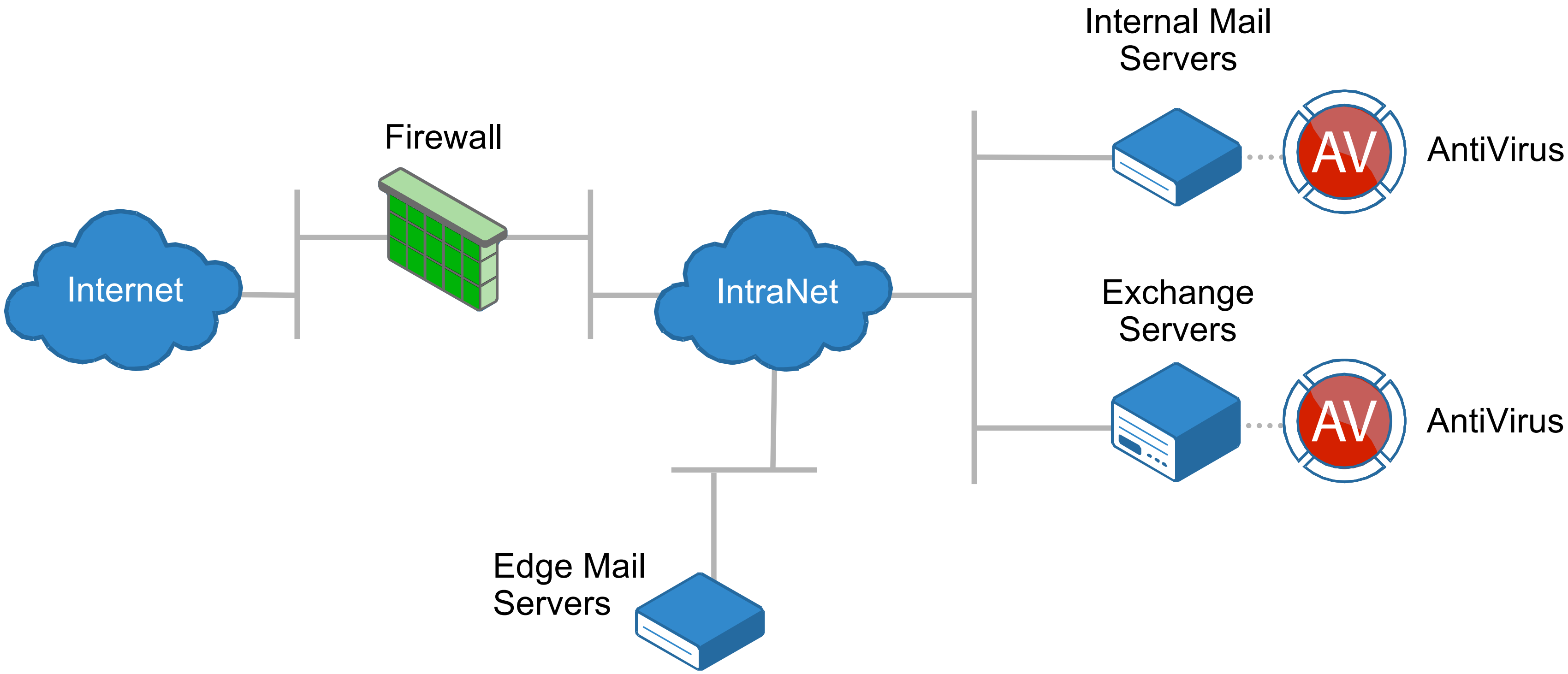
Si vis pacem, para bellum

"Let him who desires peace prepare for war."

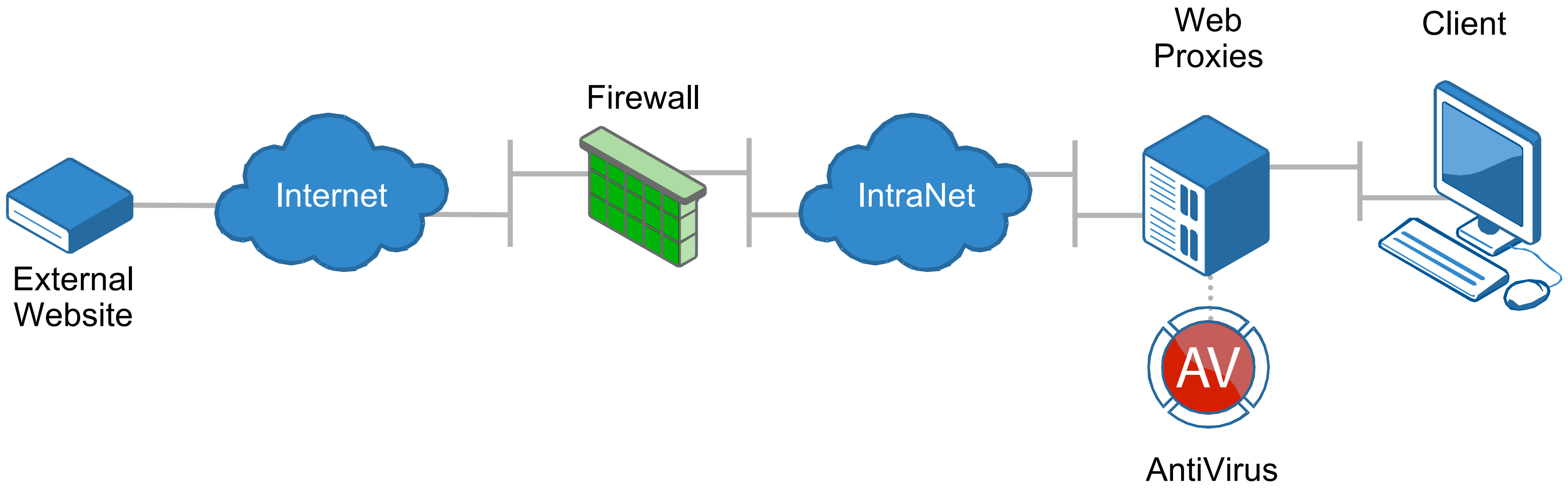
- Vegetius



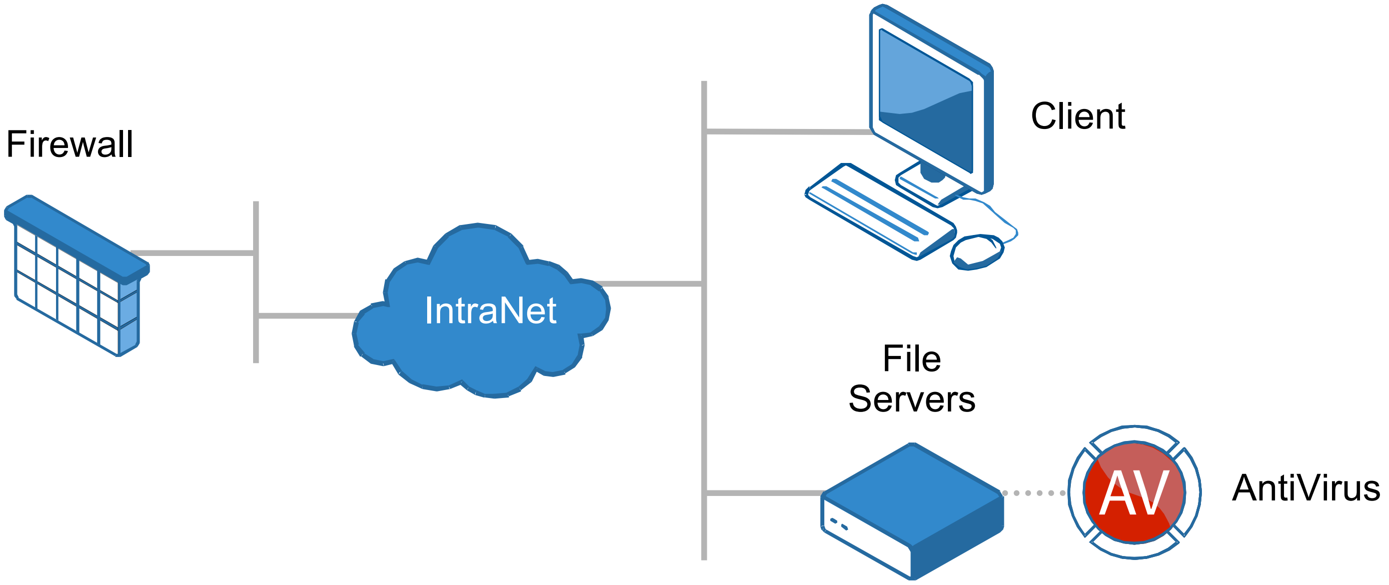
Infrastructure: E-mail AntiVirus



Infrastructure: Web AntiVirus



Infrastructure: File Server AntiVirus



Achilles Heal

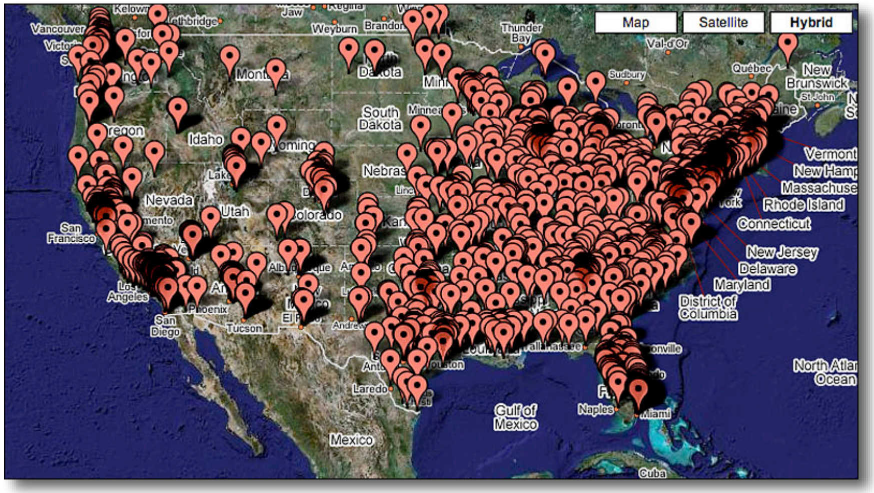
- Anti-Virus defends against known threats
- Zero-day malware gets through
- Custom malware gets through

Johann Heinrich Wilhelm Tischbein, 1751-1829: Achilles. Photo ©Maicar Förlag-GML

"Cyber-Criminals and Their Tools Getting Bolder, More Sophisticated" -Krebs The Washington Post

"Running some reverse lookups on the list of IPs produced more interesting results: Two of the machines were at biotech giant Amgen"

"The data was being compiled by a password-stealing virus that had infected many thousands of computers worldwide; the particular text file that I found included personal information on 3,221 victims scattered across all 50 U.S. states."



This is not an original idea

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."

- Sun Tzu, *544-496 BC*

Detection

- Users
- Intrusion Detection Systems (IDS)
- Tarpits
- Log Analysis
  - Overwatch

Users

- Majority of security incidents are detected by users
- Strange e-mails
- Odd system behavior
- System outages

Intrusion Detection Systems (IDS)

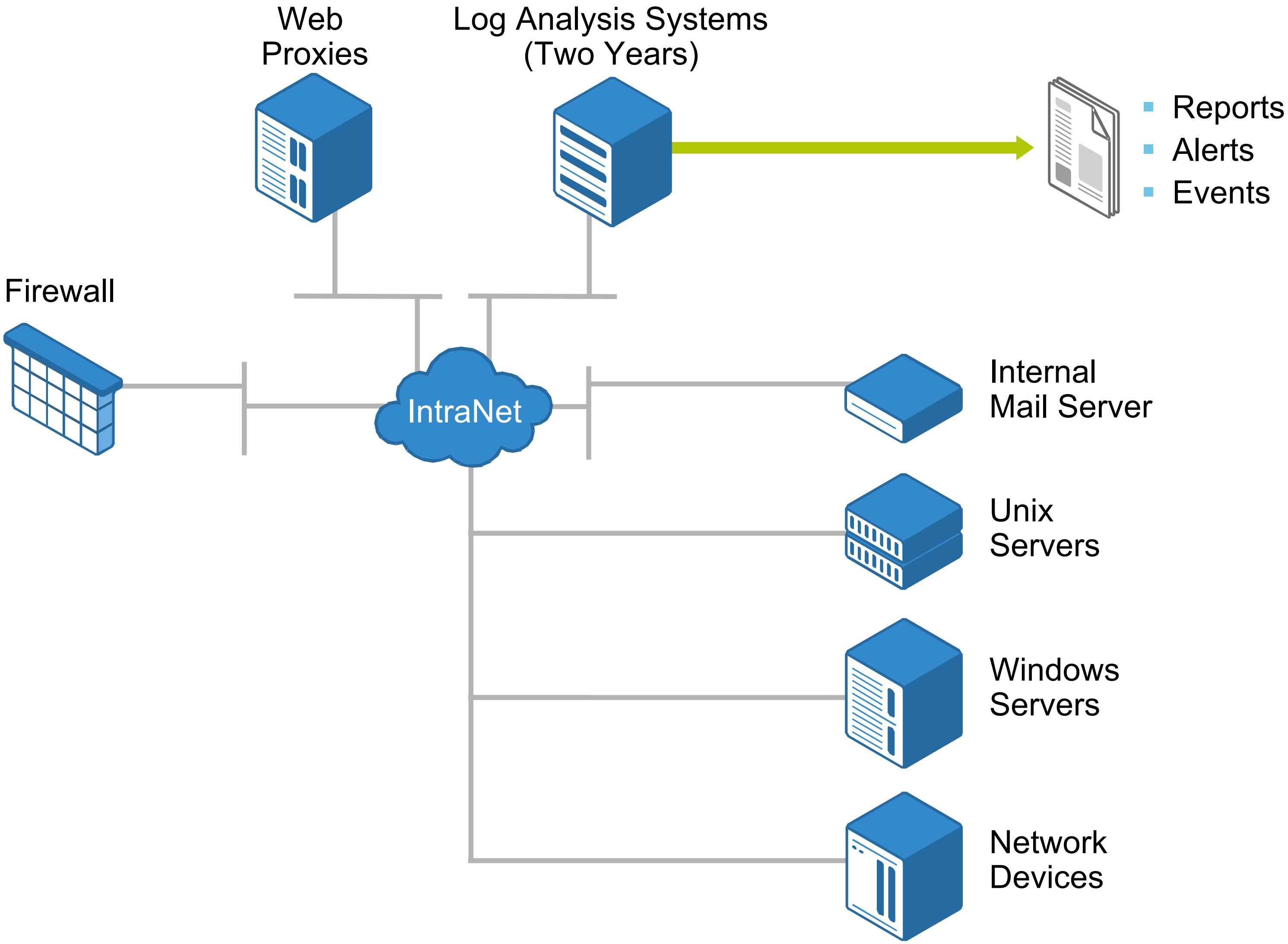
- Most effective at monitoring perimeter, Wide Area Network (WAN) and desktops
- Signature based with the same Achilles Heal as A/V
- Used mostly as a reactive measure

Tarpits

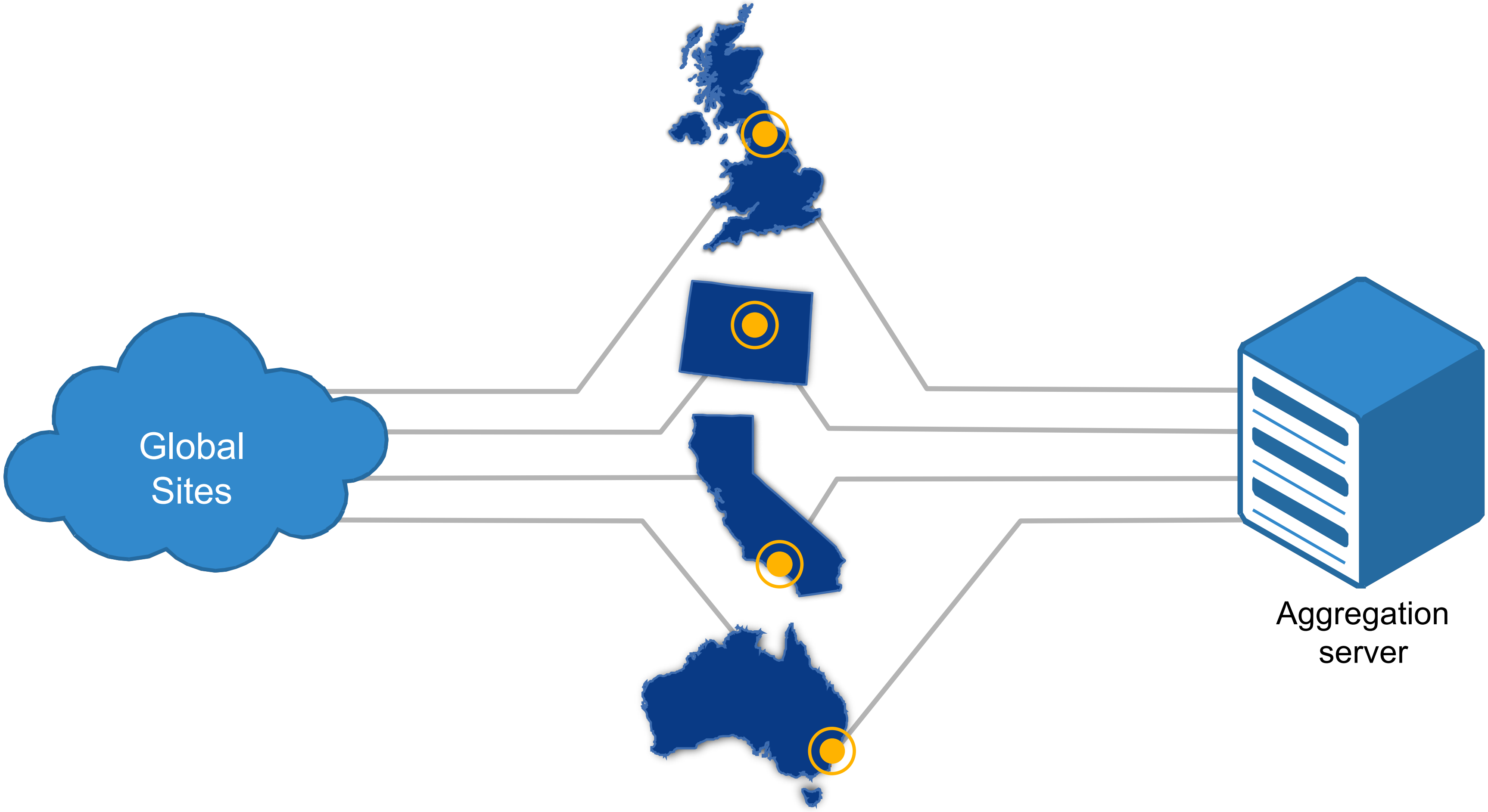
- LaBrea: A low interaction honey pot
  - *Written by Tom Liston (http://labrea.sourceforge.net)*
- When placed on an unused subnet, will respond to ping and TCP requests as though the subnet is fully populated

```
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.193 707 *
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.194 707
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35946 -> 10.22.9.193 110 *
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35946 -> 10.22.9.194 110
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.193 110 *
Sep  5 09:19:20 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.194 110
Sep  5 09:19:21 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35946 -> 10.22.9.193 9999 *
Sep  5 09:19:21 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35946 -> 10.22.9.194 9999
Sep  5 09:19:21 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.193 9999 *
Sep  5 09:19:21 labrea[20977]: Initial Connect - tarpitting: 10.10.10.38 35947 -> 10.22.9.194 9999
```

Logging


Web
Proxies
Log Analysis Systems
(Two Years)
Reports
Alerts
Events
Firewall
IntraNet
Internal
Mail Server
Unix
Servers
Windows
Servers
Network
Devices

Logs Are Collected at Each POP Site



Log Analysis

- Overwatch
  - Statistical analysis using matrices
  - Scoring based on traffic volume, bytes in/out, number of clients, key words, domain named, country of origin or destination, etc.
- Firewall logs
- Proxy logs
- DNS Activity

Firewall logs

- Contain all attributes related to each network connection
- Finding the BOTS:
  1. Calculate the ratio of bytes out over bytes in
  2. Summarize all connections based on source/destination IP address
  3. Sort by the ratio
  4. Remove known valid destination for data

```
16576004 10.10.10.10
        13080772 post.craigslist.org|443
        619852 www.plusone.com|443
        574766 63.240.253.71|443
        103280 v-208-42-157-76.mn.visi.com|443
        86940 64.23.32.13|443
        85037 www.invitrogen.com|443
        79966 miggins.aqhostdns.com|2082
        73957 198.140.180.213|443
        62292 147.21.176.18|443
        61512 159.53.64.173|443
        57494 63.240.110.201|443
… <snip> …
```

Proxy Logs

- Contain the transactions for all web (HTTP) traffic including the URI
- **Finding the BOTS:**
- Good URL’s have a few sub-domains and lots of sub-directories

http://**www.cnn.com**/video/#/video/world/2007/09/10/

- Bad URL’s have lots of sub-domains and few sub-directories

http://v-208-42-157-76.mn.visi.com/downloader.js

- Lets build a simple script to score each URL, add points for each sub-domain, subtract points for each directory . . .

A simple script

1. For each unique sub-domain, add 5 points
2. For each level of sub-domain, add 10 points
3. For each unique directory, subtract 1 point
4. For each level of sub-directories, subtract 3 points

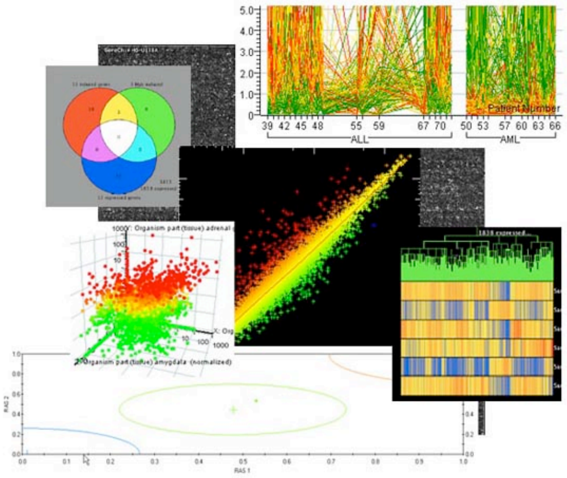
- The top scoring websites have no names, only IP addresses
- All URLs average score: **-0.5**
- Known bad URLs average score: **15**
- We can now use this data to find new URLs that are probably bad

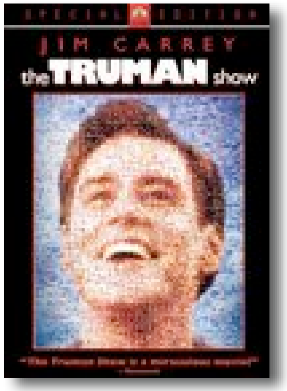
DNS

- The lowest common denominator for services that use the Internet
- Shutting down Malware that use IP addresses is much easier than if they use domain names
- Monitor DNS queries (passive DNS sniffer)
- Look for bad behavior:
  - DNS lookups that return non-routable addresses
  - Dynamic DNS domains
  - New domains that have never been seen before
  - DNS domains hosted by known malware ISPs
  - DNS domains pointing at Cable/DLS address ranges
  - Strange data in TEXT records
  - Low TTL on DNS records
  - DNS records with A records that change frequently

Analysis

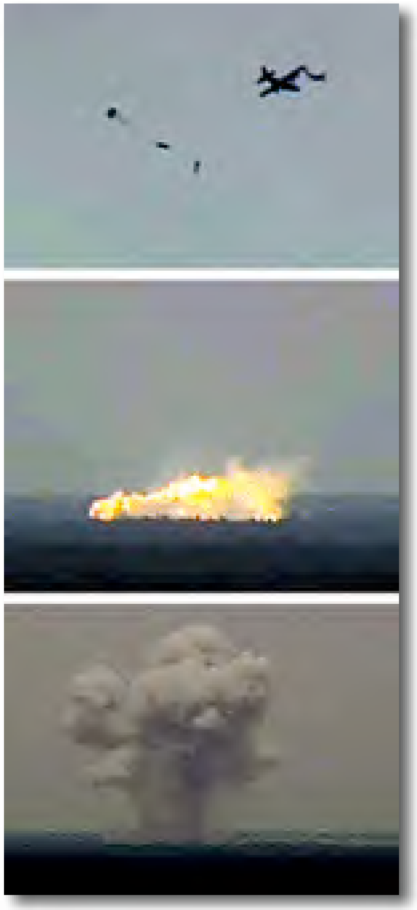
- VirusTotal
- Truman
- Spotfire
- Advisor Analyst Pro





Suppression

- Firewalls
  - Block command and control channels (C&C)
- Manual Cleaning
  - Find and remove the processes, files and registry entries
- Automated Cleaning
  - Mytobor.e



Mytobor.e

- BOT used Internet Relay Chat (IRC) for command and control, but the server had been shut down
- Of the many features in the BOT, one command forced the BOT to uninstall itself
- We hijacked the DNS name and pointed it to an internal system running a fake IRC server
- The fake IRC server (perl script) talked with the infected hosts and commanded it to uninstall the BOT
- All infected systems are cleaned in less than 5 minutes

In summary

“He is most free from danger, who, even when safe, is on his guard.”

- Publilius Syrus

Questions?