Defending Against Advanced Threats

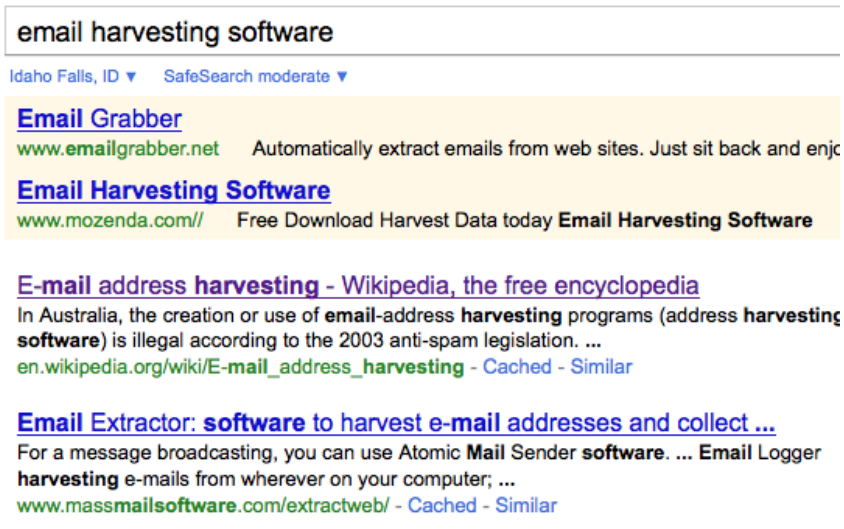
Sans Process Control and SCADA Security Summit

Robert Huber

How are the threats getting in?

- 99% is via targeted email/spear phishing – attachments, or links to web sites

(Google email harvesting, find likely targets yourself)



- Driveby Downloads

Traditional Defense in Depth and Why They Fail Against APT

Network	Firewalls – IPs change constantly DNS – new domains all the time
IDS/IPS	No signatures for 0 Days AND can't decode emails and links on the fly - base 64, embedded EXEs, XORed EXEs in emails
Virus Protection	No signatures for 0 Days
Server Hardening	Attacks are against the application layer
Application & Data	Availability & functionality always win

Critical Intelligence

Intellectual Armor for Critical Infrastructure

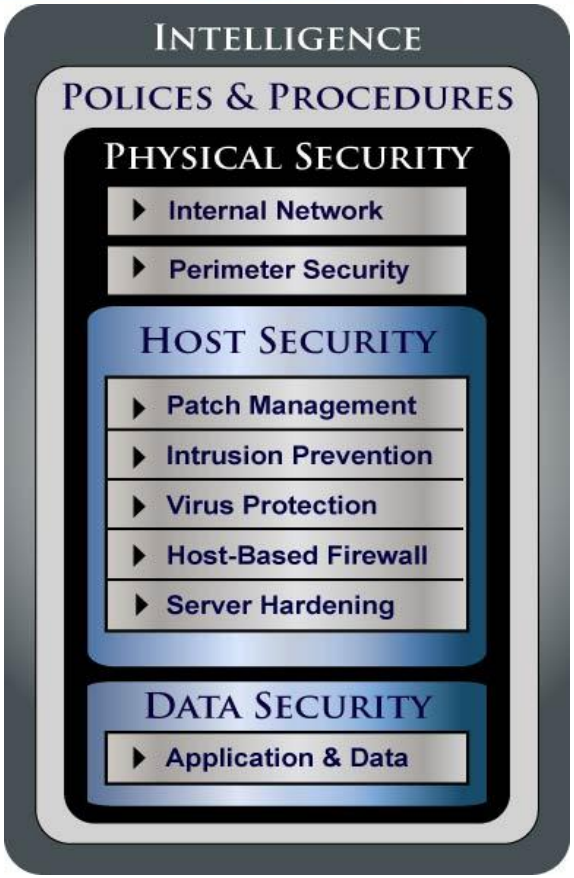
Firewall Fail - Changing IPs

IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2005-03-05	New	-none-	XXX.172.95.125
2007-07-15	Change	XXX.172.95.125	XXX.180.245.252
2007-10-21	Not Resolvable	XXX.180.245.252	-none-
2008-01-06	Change	XXX.180.245.252	XXX.172.95.124
2008-01-13	Change	XXX.172.95.124	XXX.180.245.239
2008-03-16	Change	XXX.180.245.239	XXX.180.245.140
2008-03-23	Change	XXX.180.245.140	XXX.180.245.239
2008-07-13	Change	XXX.180.245.239	XXX.180.245.249
2008-07-27	Change	XXX.180.245.249	XXX.180.245.23
2008-08-31	Change	XXX.180.245.23	XXX.180.245.239
2008-09-21	Change	XXX.180.245.239	XXX.180.245.23
2008-09-28	Change	XXX.180.245.23	XXX.180.245.239
2008-10-26	Change	XXX.180.245.239	XXX.172.95.103
2009-01-26	Change	XXX.172.95.103	XXX.172.95.104
2009-02-16	Change	XXX.172.95.104	XXX.172.95.118
2009-05-04	Change	XXX.172.95.118	XXX.172.95.104
2009-05-11	Change	XXX.172.95.104	XXX.172.95.118
2009-06-15	Change	XXX.172.95.118	XXX.172.95.104
2009-06-22	Change	XXX.172.95.104	XXX.88.127.157
2009-08-10	Change	XXX.88.127.157	XXX.88.127.228
2009-08-25	Change	XXX.88.127.228	XXX.155.212.88
2009-09-05	Change	XXX.155.212.88	XXX.155.212.81
2009-10-24	Change	XXX.155.212.81	XXX.155.212.88
2009-11-03	Change	XXX.155.212.88	XXX.155.212.81
2009-11-23	Change	XXX.155.212.81	XXX.155.235.203
2010-01-13	Change	XXX.155.235.203	XXX.155.235.196

Information from domaintools.com

How do we stop the threat from getting in?



Intel

- US-CERT/Government Partners, ISACs, InfraGuard, Security Threat Intelligence Providers, Security Community (Sans, EnergySec etc.)
- Best source of intel, your own data!
  - Antivirus blocks a piece of malware, your organization stops there
  - Create your own intelligence - analyze the malware, pull indicators
    - C2 IPs and hostnames, file metadata (creator tool, author, timezone, timestamp), mutex names, username/passwords, other unique strings
- Intel feeds all defensive layers (HIPS, IDS/IPS, firewall, message filtering, DNS, proxy blocks etc.)

Other Means

- Antivirus - on the SMTP servers and desktop

(hopefully these are different products)

- Message Filtering
  - use a solution that implements IP white/black/graylisting and IP reputation scoring via a feed
- User Security Education and Awareness
  - run simulated phishing exercises that relate to your business, and target executives, assistants, and others that have publicly available information

User Clicked! Now what?

How do we stop execution/C2/exfiltration?

- Host – HIPS or similar, to prevent file drops, system changes, file execution
- Antivirus to detect malware – probably not, but eventually
- Malware will need to communicate at some point
  - Malware uses hard coded C2 IPs – firewall block, proxy server block
  - Malware uses DNS - DNS blackhole the entire domain, the DNS servers for the domain, or that specific host, RBLDNS – get feeds (if you were getting feeds from malwaredomains.com, some of the Aurora domains would have been blocked a long time ago)
  - Malware may or may not use proxy
    - Force all web traffic through a proxy, this will stop some malware (not proxy aware)
    - Proxy block of C2 indicators (hostnames, URIs, User Agents, unique strings)
    - Configure your proxies to block all category none, or unknown requests (this helps with new C2 sites that have not been categorized)

Critical Intelligence

Intellectual Armor for Critical Infrastructure

Things you can do today

- Get Intel from somewhere – generate your own
- Feed the Intel into your current solution sets
- Implement central web proxy solutions, limit your outbound web traffic to your proxies, and BLOCK uncategorized or sites not rated

Intelligence is of the essence in warfare. It is what the Armies depend upon in their every move. - *Sun Tzu*