



SCADA Honeynets

Dale Peterson, Digital Bond

peterson@digitalbond.com

See our SCADA Security Blog & SCADApedia

www.digitalbond.com



Thanks to the UK Government CPNI
for funding the initial phase of
Digital Bond's SCADA Honeynet Project



What is a Honeynet?

◆ Honeywall

- Capture attack data
- Control the attacker
- Manage the honeynet
- Not visible to an attacker

◆ Honeypot / Target

- Real or virtual (simulated)
- High interaction
- Provides responses to keep attacker going



Why Honeynets?

- ◆ Learn about the threat
 - What is the frequency (likelihood) of attack?
 - How will a control system be attacked?
 - How far will an attacker take the attack?
- ◆ Early warning sensors for attacks
 - Honeynets in a production environment should never be attacked
 - Any activity on a production honeynet should be investigated



SCADA Honeynet

- ◆ Looks and acts like a very popular PLC
 - High interaction
 - Will fool a sophisticated attacker for a long time
 - MODBUS TCP
 - Points list and changes from large utility
 - Management
 - Web, ftp, telnet and SNMP interfaces
 - Looks exactly like the PLC



Honeynet Results

- ◆ Caveat – limited time and limited honeynets deployed.
- ◆ Honeynets were exposed to the Internet as well as in less exposed environments
- ◆ No activity on SCADA ports
 - Modbus TCP port 502
 - Very important finding, dispels some FUD
 - No intelligent attacks on management protocols



Honeynet Results

- ◆ Robust, automated attacks on http and ftp management ports
 - Rigorous password cracking attacks from lists
 - Web server and ftp server attacks
- ◆ Why do we say automated attacks?
 - Web & ftp management had default credentials
 - Attacker could simply Google the vendor / equipment and discover credentials
 - This never happened



Prediction

Control system default credentials
will be added to hacking tools
within two years!

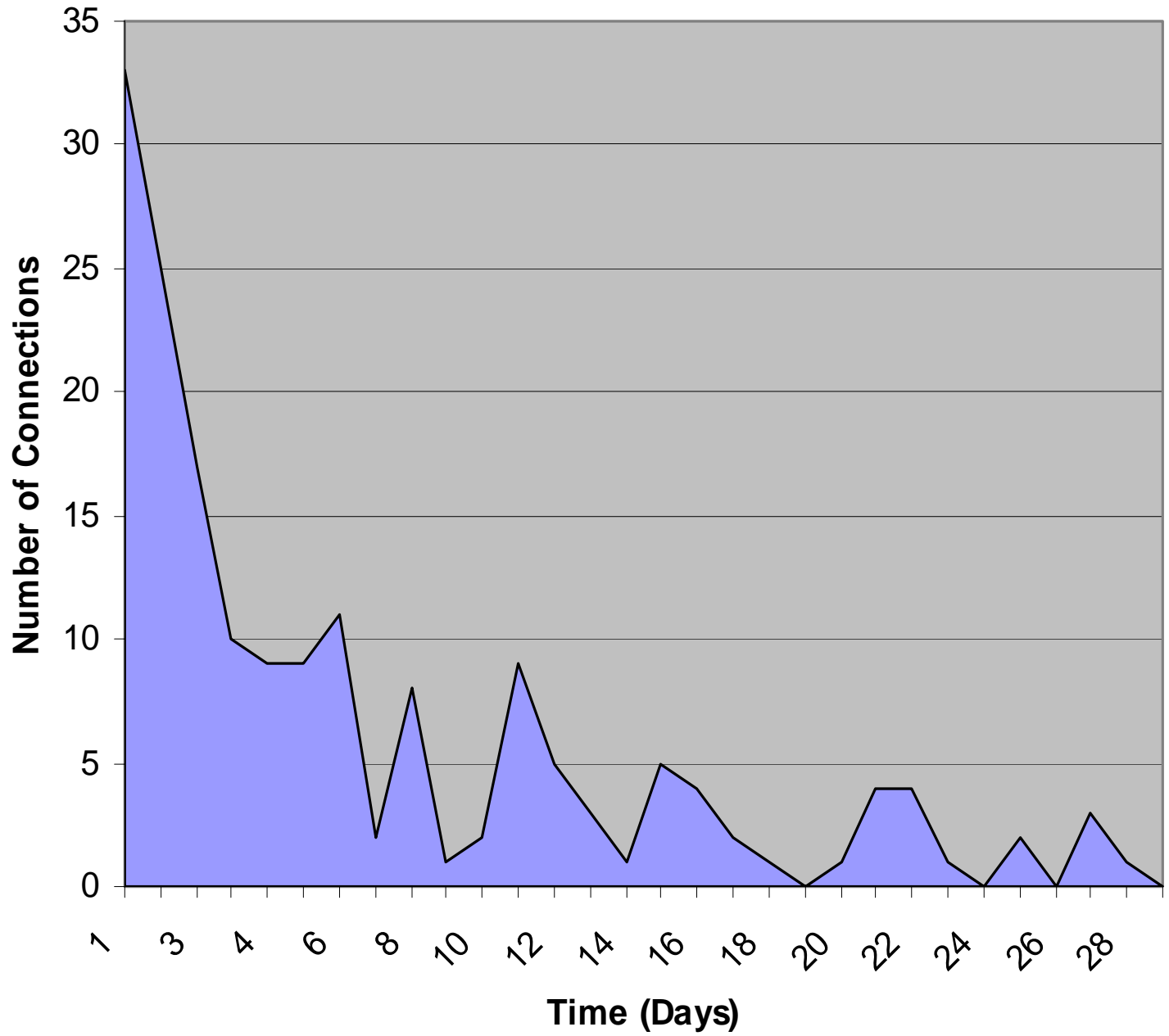
Honeynets could help identify this important shift



Substation WLAN Exposed

- ◆ Located in an electric substation
 - Low income, apartment buildings nearby
- ◆ 802.11 b/g access point
- ◆ Many connection attempts in the 1st day
- ◆ Many infected systems

No Room For Error





WLAN Results

- ◆ Where were they trying to go?
- ◆ Traffic analyzed by DNS queries
- ◆ Majority looking for pirated software (Gnutella, Limewire, Morpheus, etc)
- ◆ Large amount was spyware/malware “phoning home”
- ◆ Rest resulted in email checking or automated software updates



WLAN Lessons Learned

- ◆ Wireless while providing great savings and conveniences, must be deployed securely
- ◆ No grace period
 - Imagine if just one access point is deployed insecurely
- ◆ People notice when a new network appears and they're not afraid to use it
- ◆ Utility or contract workers bringing in an access point to surf while on the job?
 - Easier than requesting network access



Contact Information

Dale Peterson

peterson@digitalbond.com

954-315-4633

Presentation available at:

www.digitalbond.com/resources/presentations