THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

Protecting Against Modern Advanced Persistent Threats

Darren Guarino

Information Security Director

Tyco International

What is APT ?

- Advanced persistent threat (APT) usually refers to a group, such as a foreign nation state government, with both the capability and the intent to persistently and effectively target a specific entity.
- The term is commonly used to refer to cyber threats, in particular that of Internet enabled espionage, but applies equally to other threats such as that of traditional espionage or attack.
- Attack vectors may include:
  - infected media, supply chain compromise, and social engineering.
- The term is almost always used in reference to a long-term pattern of targeted sophisticated hacking attacks aimed at governments, companies and political activists.

What’s Changed?

- COORDINATION, PERSISTENCE and FOCUS
- Ability to evade today’s detection technologies
- Ability to operate as trusted users
- Lack of standard recognizable patterns, well hidden
- Multiple avenues of infection
  - Social Media
  - Mobile technology
  - Outsourcing arrangements

What’s the Challenge

- Rethink “Old School” Security
  - Technology can’t provide the solution
  - The perimeter is dead – so are “trusted users”
- Rethink your reliance on preventative measures
- Shift from prevention to visibility and response

A New Mindset – A Place to Start

- Never confuse compliance with security, compliance is not good enough
- Network assets may not be "yours"
- Users may no longer be in control – you can't implicitly trust them
- Backwards compatibility on upgrades is not worth it
- Don't trust and Do verify
- **Start Your List Here…….**

Moving Forward

- Focus on prevention alone guarantees failure
- You must leverage industry partners, government agencies, and specific vendors for useful threat intelligence
- You must mature your organization to be able to rapidly detect and respond to threats
- Improvise, Adapt and Overcome

Thank You!

Darren Guarino

Information Security Director

Tyco International