

Technology Showcase Presentation

June 19, 2013



Active Threat Deception



Why

There is a need to protect customers from Advanced Persistent Threats (APTs) that may already be in the network

What is the safety net IF all else fails?

How

- Proven technology deployments for DoD, Navy, NSA, etc.
- Software-Defined Networking (SDN) and
 - Network Virtualization technologies

What

- “Shadow Networks” that
- *Detect* APTs already in customer environment
 - *Hide* critical resources
 - *Dynamically quarantine* threats for observation and forensic analysis

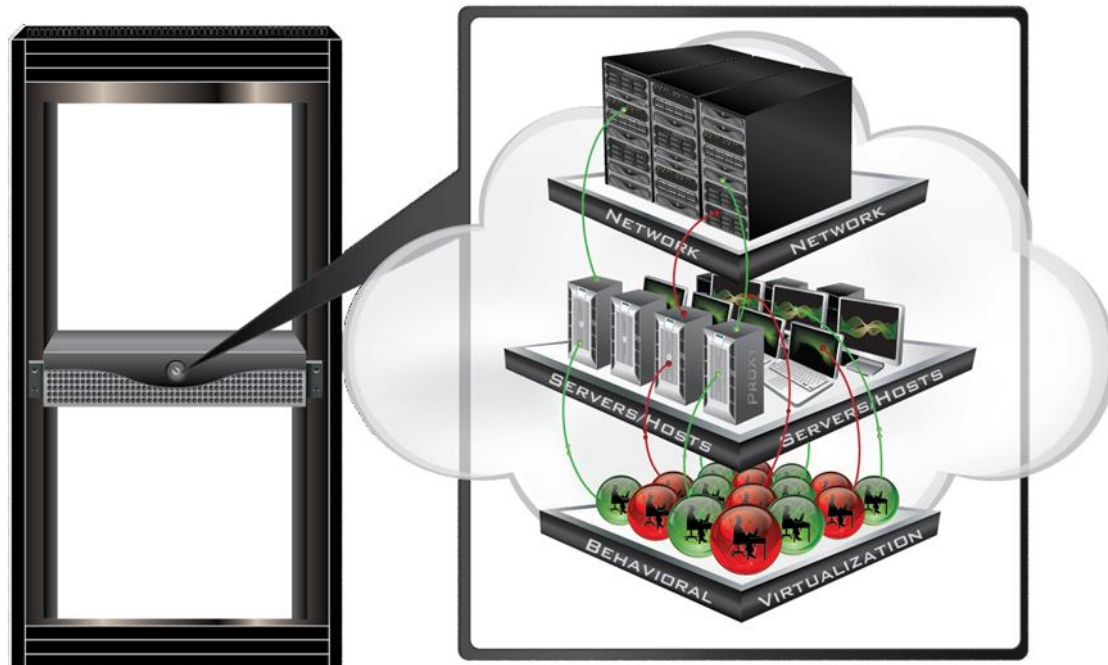
Background on ZanttZ



Patented Technology in use by US Government



- Cyber warfare training
- Cyber network emulation
- Cyber security



ZanttZ Proprietary and Confidential

Market Opportunity: Advanced Persistent Threats



Millions
of Attacks

1000

250

100

50

1990

1995

2000

2005

2010

Source: FBI, Symantec, McAfee, Kaspersky, Mandiant

Advanced Persistent Threats



- 760 networks “calling home” to C&C
- Most Fortune 500s recently breached at some level
- Only 37% of companies detect APTs internally, the rest were notified externally

Critical Infrastructure: Increasing Sophistication and Impact



NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”

U.S. companies lose about \$250 billion per year through intellectual property theft, with another \$114 billion lost due to cyber crime, a number that rises to \$338 billion when the costs of down time due to crime are taken into account.

- General Keith Alexander, July 9, 2012

Aramco Says Cyberattack Was Aimed at Production

Aramco, said on Sunday that a cyber attack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia, the biggest exporter in the Organization of the Petroleum Exporting Countries.

- Reuters, Dec 9 2012

Cyberattack leaves natural gas pipelines vulnerable to sabotage

A government report says a cyber attack against 23 natural gas pipeline operators stole crucial information that could compromise security. ... The stolen information could give an adversary all the insider knowledge necessary to blow up not just a few compressor stations but perhaps many of them simultaneously, effectively holding the nation's gas infrastructure hostage.

- CS Monitor, Feb 26, 2013

ZanttZ' Approach: Active Threat Deception

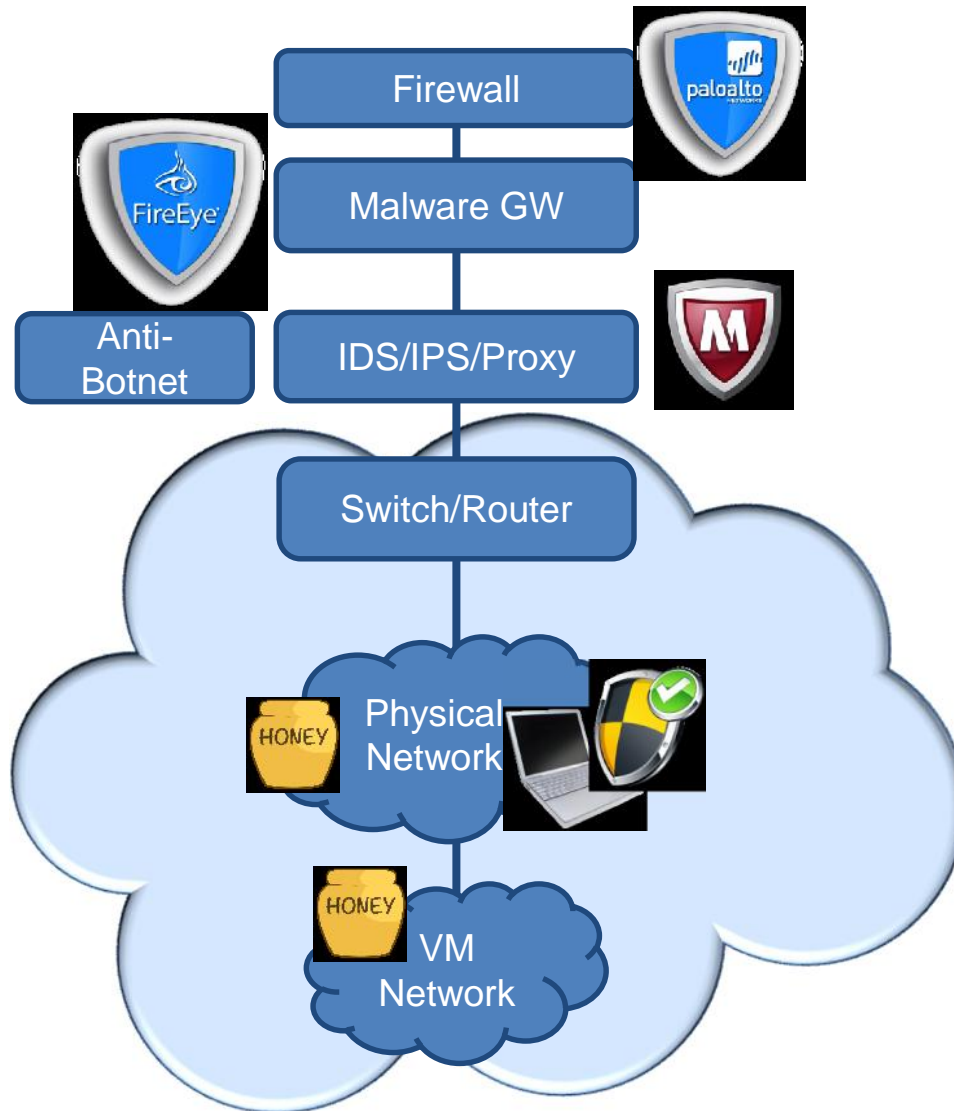


- 1 Create operationally realistic “network neighborhood” to **Bait and Detect** APTs already operating in the network
- 2 Software Defined Networking allows cost-effective scale to **Hide and Protect** actual network resources
- 3 Dynamic quarantine to **Contain and Inspect** threats to determine intent and provide deep forensics

“Moving Target Defenses (systems that continuously blur the lines between what is real and what is virtual)...will gather momentum rapidly, especially as it converges with new developments in SDN”

Accenture Technology Vision 2013

Complements Existing Solutions (For Threats “Already Inside Network”)



Today's security best practices involve a multi-vendor defense-in-depth “shield” approach

- ShadowBox™ complements security best practices today
- Targets threats already operating inside networks

Investment History and Exit Potential



Network Security



IPO ~\$1.5B valuation
>10x Revenue



\$80M acquisition
>25x Revenue

Software Defined Networking



\$1.26B acquisition
>100x Revenue

Financing

- 2011 \$2M Seed round (led by Crosslink Capital)
- 2012 \$8M A round planned for Fall
 - \$3M+ Convertible Note (Oversubscribed)
 - \$5M planned for Fall (\$3M already committed)
- Use of funds
 - Complete 1.0 MVP (available July 2013)
 - Public launch 2.0 and 3.0 solutions in 2014

Thank You!



www.zanttz.com