Threat Intelligence

What Makes It Smart

Presented by:

C. Thomas "Space Rogue"
Threat Intelligence Manager

Who Am I

- C. Thomas aka "Space Rogue"
  - Member of L0pht Heavy Industries
  - Creator of the Whacked Mac Archives
  - Testified to Congress on "Weak Computer Security in Government"
  - Defcon, SOURCE, HOPE – MTV, ABC News, CNN
  - Editor in Chief of The Hacker News Network
  - Threat Intelligence Manager for Trustwave SpiderLabs

cthomas@trustwave.com @spacerog

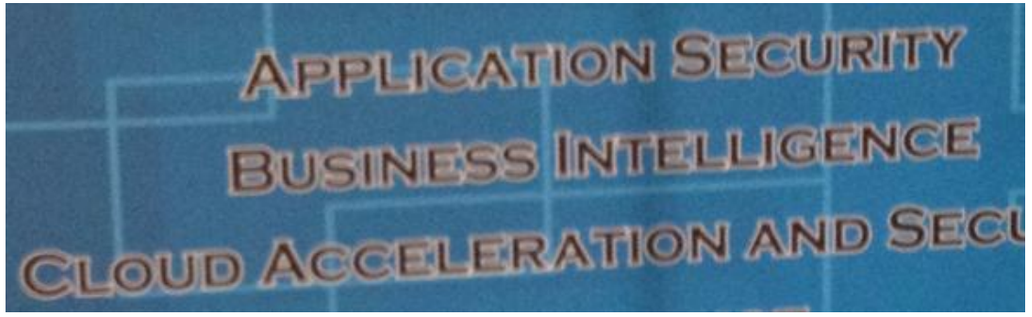
What is Threat Intelligence?

threat [thret] *noun* 1. a declaration of an intention or determination to inflict punishment, injury, etc., in retaliation for, or conditionally upon, some action or course; menace *2. an indication or warning of probable trouble* 3. a person or thing that threatens.

intelligence [in-tel-li-juhns] *noun* 1. capacity for learning, reasoning, understanding, and similar forms of mental activity; aptitude in grasping truths, relationships, facts, meanings, etc. 2. manifestation of a high mental capacity 3. the faculty of understanding. *4. knowledge of an event, circumstance, etc., received or imparted; news; information. 5. the gathering or distribution of information, especially secret information.*

What is Threat Intelligence?

- **Market Definitions:**



What is Threat Intelligence?

- Types of InfoSec Threat Intelligence
  - New Malware Attacks
  - Phishing exploits in the wild
  - Known Vulnerabilities
  - Who are the Bad Guys (and their motivations)
  - New Patches
  - Industry specific attacks

What is Threat Intelligence?

- Types of InfoSec Threat Intelligence
  - New Malware Attacks
  - Phishing exploits in the wild
  - Known Vulnerabilities
  - Who are the Bad Guys (and their motivations)
  - New Patches
  - Industry specific attacks

- More than just a SIEM or SOC service can provide

What is Threat Intelligence?

- **Market Definitions:**
  - SIEM (Security Information and Event Management)
    - Automated Log Analyses
    - Actively attacking your network right now
      - Lot of false positives
    - Many are Malware Centric
      - Signature based
    - Alerts often have no context or *analysis*

Intelligence Gathering

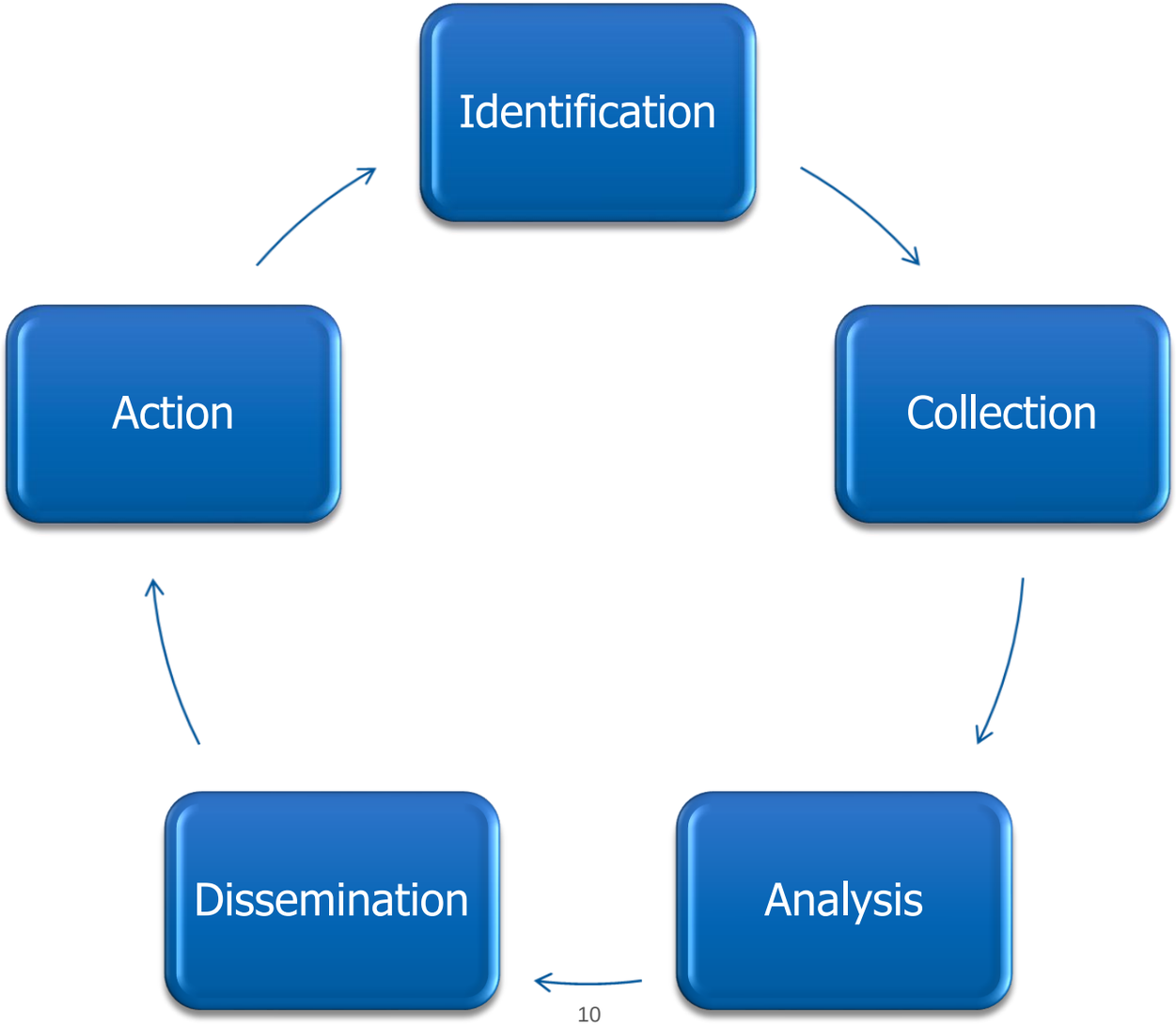
Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge. —Sun Tzu, The Art of War

"I was almost as well advised of the strength of the hostile army in my front as its commander." – General Pierre Gustave Toutant Beauregard, CSA – Battle of Bull Run

Intelligence Gathering

- Basics Still Apply
  - Identification
    - Identify topics – What information is wanted
  - Collection
    - Acquisition of raw information
  - Analysis
    - Organization – filtering – formatting – correlation – reducing to facts
  - Distribution
    - Email – dashboard – white paper
  - Action

Intelligence Cycle



Threat Intelligence Sources

- Open Source Intelligence (OSINT)
  - Social Networking (Facebook, Twitter, etc…)
  - Traditional Media (NY Times, CNN, Al Jazeera, etc…)
  - Underground (IRC, Forums, etc…)
  - Mailing Lists (ISN, Full Disclosure, BugTraq, etc…)

Threat Intelligence Sources

- Open Source Intelligence (OSINT)
  - Social Networking (Facebook, Twitter, etc…)
  - Traditional Media (NY Times, CNN, Al Jazeera, etc…)
  - Underground (IRC, Forums, etc…)
  - Mailing Lists (ISN, Full Disclosure, BugTraq, etc…)
- Private
  - Mailing Lists (Dragon Newsbytes, DailyDave, FiRST)
  - Corp and Edu Research Labs
  - Mil and Gov

Threat Intelligence Sources

- Can not rely on traditional media alone
  - Slow / Rush to Publish
  - Large amounts of content (impossible to keep up)
  - Trying to be Social Media = Fail
  - Inaccurate – Failure to Verify
    - Mitnick broke into NORAD
    - Brazil Blackout was a cyber attack
    - IL Water Plant pump failure
    - NW Railroad 'slowdown'
  - No Analysis

Threat Intelligence Providers

- Are they reputable?
  - Bias?
  - Influenced? (Advertising?)
  - Easily trolled?
  - Parrots?
- Are they regurgitating Google searches?
  - Sexy headlines and buzzwords
- "algorithmically aggregated news" – Rob Malda, Editor Washington Post (Slashdot)

Threat Intelligence Providers

- Are feeds too targeted (not enough info)
- Are feeds too broad (too much info)(duplicates)
- Can you customize what you are paying for?

- Are you getting the right analysis?
  - Does it matter to me?
  - Is it sales babble? Or real news?
  - Do they have the Threat Level right? (Hype)
    - Crying wolf is bad.
    - Being wrong about a real threat is not fun, either.

Trustwave SpiderLabs Threat Intelligence

Trustwave SpiderLabs

Trustwave

SpiderLabs – Threat Intelligence

- What do you get?
  - Targeted email feed
    - Dashboard/portal planned
  - Quarterly Reports
    - 4 Focus Areas (Mobile, Malware, Infrastructure, Cloud)
  - Access to SpiderLabs Team
    - Product Analysis, Custom Research, Advice

SpiderLabs – Threat Intelligence

- Feed
  - Targeted
    - 4 Focus Areas (Mobile, Malware, Infrastructure, Cloud, +)
  - Multiple sources
    - (Traditional Media, Mailing Lists, RSS Feeds, Twitter, Forums, IRC, Trustwave SOC, SpiderLabs Team)
  - Each item manually reviewed
  - Expert Analysis and Commentary
  - Dedicated Team – NOT Algorithmically Aggregated
  - No Hype

SpiderLabs – Threat Intelligence

- Quarterly Reports
  - 4 Focus Areas (Mobile, Malware, Infrastructure, Cloud)
  - Aggregates news items from the quarter
  - Identifies Trends
  - Unique Insight

SpiderLabs – Threat Intelligence

- Access to the SpiderLabs Team
  - Advice
  - Product Analysis
  - Custom Research
  - Trusted Advisor

SpiderLabs – Threat Intelligence

- What do you get?
  - Targeted email feed
    - Dashboard/portal planned
  - Quarterly Reports
    - 4 Focus Areas (Mobile, Malware, Infrastructure, Cloud)
  - Access to SpiderLabs Team
    - Product Analysis, Custom Research, Advice

Threat Intelligence

Overview

Presented by:

C. Thomas "Space Rogue"
Threat Intelligence Manager