CounterStorm™

Deploying Statistical Anomaly Detection to Improve Cyber Security

Dr. Greg Shannon
Chief Scientist

shannon@counterstorm.com

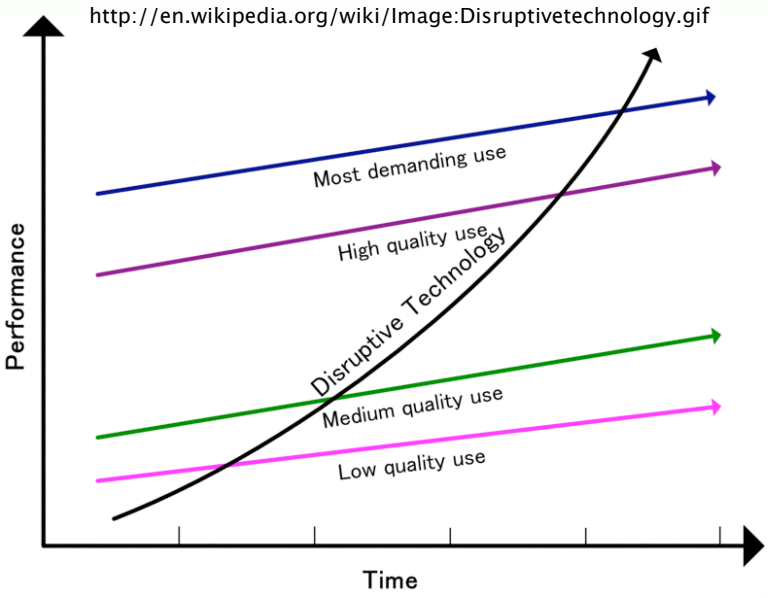
May 14, 2007

CounterStorm

Comments on Disruptive Technologies

- The DT usually has new / unique capabilities
- The DT often is invented by or at least known by the incumbents
- The DT always has an initial niche area of REAL application

http://en.wikipedia.org/wiki/Image:Disruptivetechnology.gif

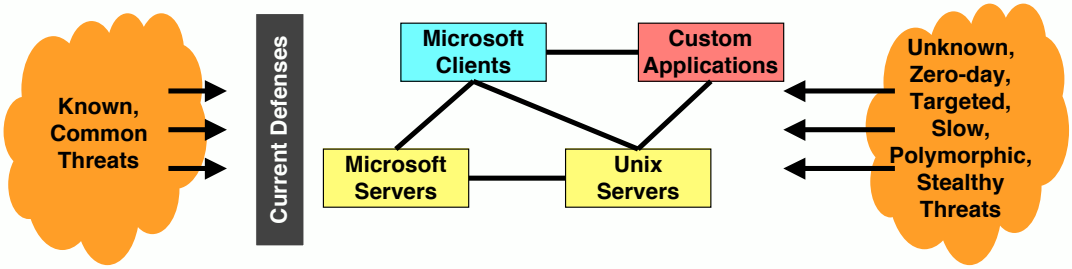


Copyright 2007, CounterStorm, Inc.

Serious Cyber Threats

How do we protect mission-critical networks and applications against the growing volume of sophisticated cyber attacks?

- Attacks are designed to avoid detection
- Protection is needed BEFORE attacks start



Copyright 2007, CounterStorm, Inc.

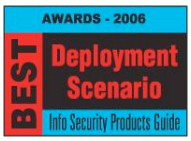
Thesis

- **Statistical Anomaly Detection is a disruptive technology to the incumbents of signatures, policies and rules for detecting the most serious threats to information systems and networks**
- **Statistical Anomaly Detection now has a niche in improving federal cyber security where incumbent solutions are significantly inadequate**
- **Statistical Anomaly Detection needs R&D investments to improve the demonstratable scope of threats detected, understanding alerts and threat scalability**

Copyright 2007, CounterStorm, Inc.

CounterStorm Background

- **Protecting against politically and criminally motivated attacks**
  - Handle the next generation of threats
  - CounterStorm-1 appliance for internal threat protection
  - Software subsystems
- **Founded in 2001**
  - Headquartered in NYC
  - Started with research at Columbia funded by DARPA since the mid-90s
- **Enterprise proven, government supported**
  - Enterprise customers in healthcare, media and finance
  - Two Department of Homeland Security SBIR phase II grants
  - Used in DoD programs



Copyright 2007, CounterStorm, Inc.

What is Statistical Anomaly Detection?

- **Anomalies reflect important observable behavior**
  - Bad ⇒ Anomaly … Finding Lose Threads
- **Statistical Anomaly Detection:**
  - A machine-learning technique for detecting when observed behavior statistically deviates from a base-line behavior profile
  - E.g., The probability of observing this value/event is .001%
    - A packet of all K's on port 80
    - 100 SMTP connections in 10 seconds
  - Anomaly Detection leverages the inherent complexity of networked systems to detect the growing variety of threats, especially evasive zero-day threats
- **It is NOT:**
  - Detecting protocol violations (protocol anomaly detection)
  - Setting value thresholds (network behavior analysis, NBAD)
  - Drawing graphs for operators to "see" unusual behavior

Copyright 2007, CounterStorm, Inc.

Problem Space – Detecting Cyber Threats

- **Problem**
  - Detect cyber threats in a timely manner
- **Status Quo**
  - Signatures, rules and policies
  - Based on past or anticipated threats
- **Key Detection Properties**
  - Coverage of known threats
  - Installability
  - Alert understandability
  - Coverage of evasive and new threats
  - Scalability to threat volume, velocity and variety
  - Accuracy

Copyright 2007, CounterStorm, Inc.

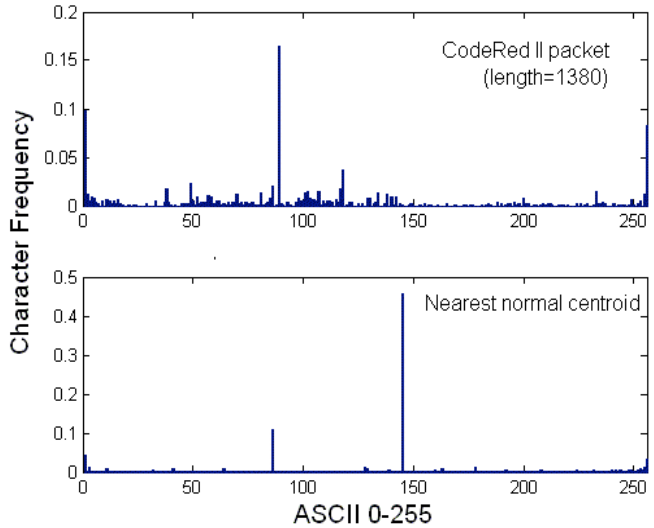
Status Quo v. Anomaly Detection

	Statu Quo	Anomaly Detection
Known Threats	Excellent	Fair
Installation	Excellent	Poor
Understanding Alerts	Excellent	Poor
Evasive & New Threats	Poor	Good
Threat Scalability	Poor	Good
Accuracy	Fair	Fair

Copyright 2007, CounterStorm, Inc.

What Can Statistical Payload Analysis (SPA) Do?

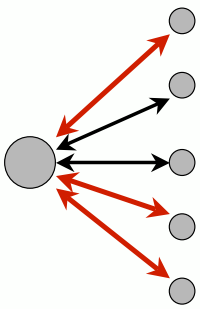
CR II Distribution v. Normal-Packets Distribution



Copyright 2007, CounterStorm, Inc.

Finding Botnets with Statistical Payload Analysis (SPA)
DHS Funded

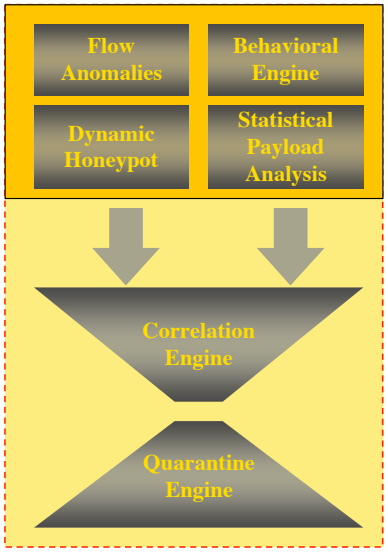
- **Detects anomalous payloads**
  - Compared with previously seen traffic on that network
  - Correlate anomalies by source or destination
- **Anomalous payloads are common in botnets**
  - Asking hosts to behave differently
  - Difficult for any botnet to avoid detection
- **Creation**
  - Exploits – known and zero-day
- **Command & Control**
  - Tunneled traffic (IRC over HTTP)
  - Unexpected encrypted/compressed traffic
- **Action**
  - Data exfiltration



Copyright 2007, CounterStorm, Inc.

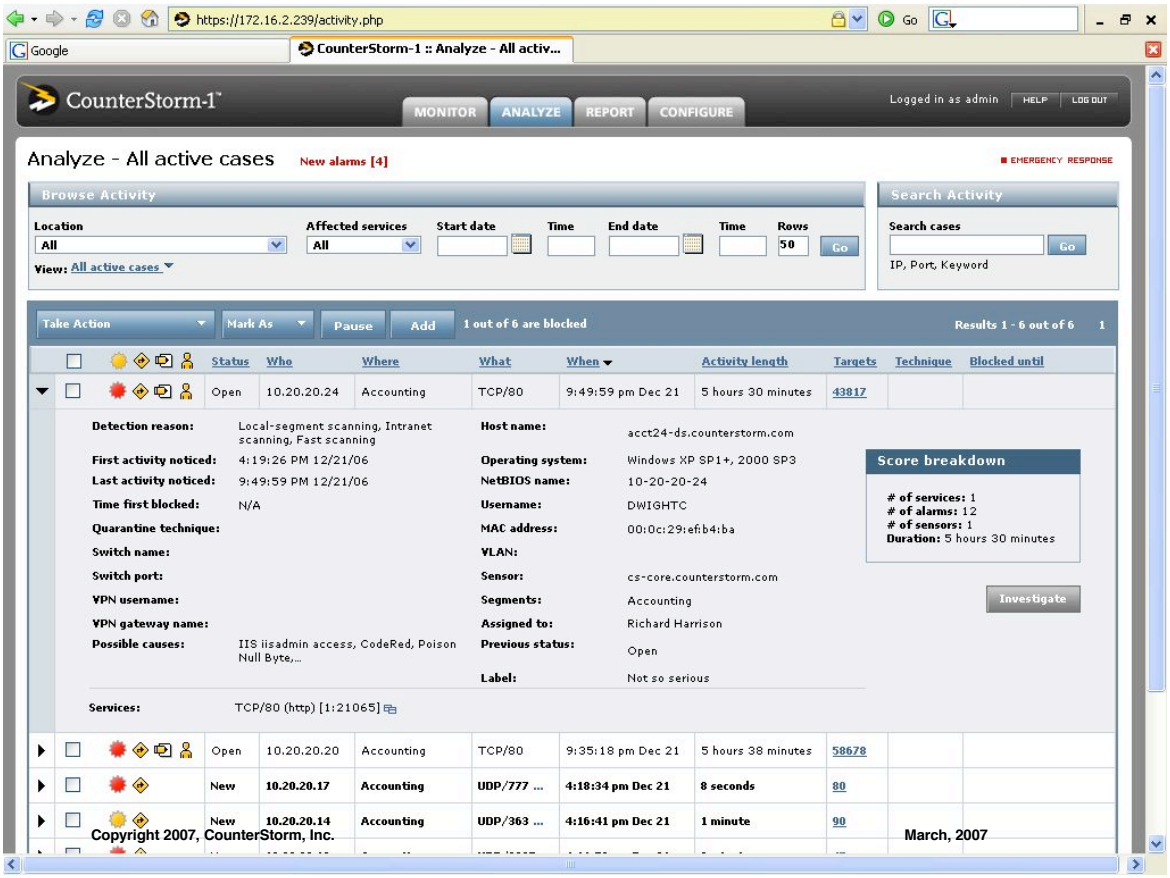
CounterStorm

CounterStorm-1 Appliance: How It Works



- **Multiple advanced detection engines** **Sense**
  - Statistical payload analysis (SPA)
    - Recognizes exploits at layer 7 without signatures
  - Behavioral attack recognition
    - Recognizes initial attack propagation patterns
    - Requires no signatures or protocol rules
  - Flow anomaly detection
    - Dynamically baselines network traffic to detect anomalous activity
  - Dynamic honeypot
    - Detects attacks on unused network addresses
- **Dynamic real-time correlation** **Infer**
  - Processes evidence from multiple sensor engines
  - Eliminates false positives
- **Quarantine engine** **Act**
  - Applies flexible response policy to stop attacks

Copyright 2007, CounterStorm, Inc.



Copyright 2007, CounterStorm, Inc.

Healthcare Case Study

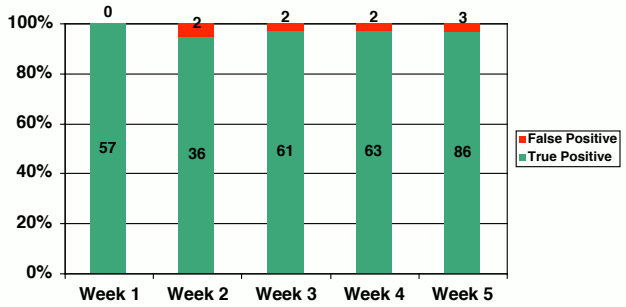
The customer:

- East coast community hospital system
- 7 centrally managed hospital facilities with 2 data centers
- 2,700 bed facility, 23,000 employees, 4,600 physicians
- Diverse user community

CounterStorm Detected:

- Zero-day attacks
- Botnets
- Root-kits
- P2P
- Worms

97% accuracy over 6 months



Copyright 2007, CounterStorm, Inc.

R&D to Strengthen Anomaly Detection's Advantages

- **Evasive and new threats**
  - Training on dirty data
  - Anit-mimicry via combinatorics
- **Scalability to threat volume, velocity and variety**
  - Scalable use of signaures
  - Account for new attack modes
    - Web 2.0/user content
    - IPv6
    - Virtualization
  - Continuous pressure from Moore's Law
- **Accuracy Improvements**
  - T/F positives, false negatives
  - Protocol/modality-specific
  - Correlation/inference techniques

Copyright 2007, CounterStorm, Inc.

CounterStorm

R&D to Make Anomaly Detect Competitive

- **Coverage of known threats**
  - Update test methodologies to account for training
  - Available / relevant zoos
  - Communicate results
- **Alert understandability**
  - What's an anomaly mean?
  - What do correlated anomalies mean?
  - How can we provide autonomic explanations?
  - How to "pull the lose thread?"
- **Installation**
  - Plug and play
  - Environment drift

Copyright 2007, CounterStorm, Inc.

CounterStorm

Recap

- **Statistical Anomaly Detection is a disruptive technology to the incumbents of signatures, policies and rules for detecting the most serious threats to information systems and networks**

- **Statistical Anomaly Detection now has a niche in improving federal cyber security where incumbent solutions are significantly inadequate**

- **Statistical Anomaly Detection needs R&D investments to improve the demonstratable scope of threats detected, understanding alerts and threat scalability**

Copyright 2007, CounterStorm, Inc.