

[www.TrustedCS.com](http://www.TrustedCS.com)

## ***Identifying Botnet Activity by Analyzing Network Behavior***

*Richard Cullingford  
Senior Software Engineer*

*March 23, 2010*



# Trusted Computer Solutions (TCS)



- Founded in 1994
- Experience building security products that meet the most stringent security requirements mandated by the Intelligence Community & Federal government.
- Products Accredited and in Operational use today protecting our nation's most valuable digital assets.
- Solutions include:
  - Cross Domain Solutions for DoD, Intelligence Community and Civilian Government
  - An automated Operating System lock down tool - Security Blanket
  - A Network Security solution - CounterStorm

# CounterStorm - A Distinguished Pedigree



- CounterStorm emerged from Columbia University research funded by grants from the Department of Homeland Security (DHS) and the Defense Advanced Research Projects Agency (DARPA).
- The technology was based upon extensive research on the viability of machine learning as a potentially effective tool to protect computer networks from non-signature based, unknown attacks, also referred to as zero-day attacks.
- As a leader in cyber security solutions that automate the process of making organizations more secure and facilitate rapid compliance with security requirements, CounterStorm is an excellent addition to TCS' portfolio of solutions.



# Agenda



- ❑ Botnets: What They Are and the Threats They Pose
- ❑ Botnet Examples and Lifecycle
- ❑ Detecting Botnet Activities through Their Network Behavior
- ❑ The CounterStorm Approach

# Botnets, Bots & Bot-Masters



- A **Botnet** is a loosely-coupled distributed computing system composed of individual hosts called **bots** (software robots), controlled from a single host called the **Bot-Master**.
- Bots intended for malicious activity run on compromised hosts called **zombies**. The zombies typically run identical copies of a package of malware including multiple exploits, attack vectors, obfuscation code, etc.
- Bot-Masters often rent out subsets of a botnet to mount coordinated attacks on third-party hosts.
- A botnet established in a corporate or government enclave is a particular threat because **targeted attacks** become possible. Botnet Command and Control (C&C) arrangements provide a **backdoor** (via botnet takeover) to attacks by other malware.
- Botnets are **hard to detect** because their network behavior is low-level, sporadic and hard to see in the volume of ordinary traffic.

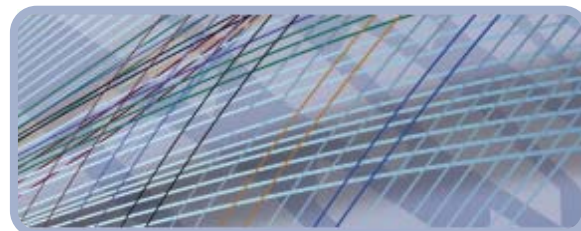
# Botnet Threats



- Stealthy Implantation
  - Social engineering exploits using infected email attachments or drive-by browsing injection techniques
  - Targeted attacks (spear-phishing)
  - Social Networking sites (Facebook, et. al.)
- Distributed Denial of Service (DDoS)
- Click fraud
- Spambots & Spamdexing
  - Bogus email agent or relay
  - Spam may attempt to affect search engine rankings



# Botnet Threats (continued)



- Keylogging & Theft of Credentials
  - Polymorphic attacks - malware that modifies itself to evade detection
  
- Exfiltration of Sensitive Data



*A recent report claims that more than half of Fortune 100 corporate networks were found to be infected by the Mariposa botnet in 2009.*

*An insidious problem with such infestations is that the bots are susceptible to take-over by other botnets. No separate incursion is required.*

Ref: [blogs.pcmag.com/securitywatch/2009/09/botnet\\_reported\\_loose\\_in\\_fortu.php](http://blogs.pcmag.com/securitywatch/2009/09/botnet_reported_loose_in_fortu.php)

# Botnet Lifecycle



- **Setup:** Bot-Master determines bot parameters such as infection vectors, exploit payloads and Command and Control (C&C) details.
- **Incursion:** Bot-Master launches (e.g., via network worm) or seeds (e.g., by a social-engineering exploit) new bots into an enclave.
- **Spread:** Bot attempts to compromise other machines in the enclave (e.g., by scanning-worm attacks).
- **Synchronization:** Bot uses pre-assigned C&C parameters to contact the Bot-Master.
- **Attack Modalities:** Bot-Master assigns a bot to a team that engages in a coordinated activity of some sort.
- **Bot upgrade:** Bot periodically contacts the master for upgrades to spread techniques, attack vectors, or (more rarely) changes in C&C arrangements.
- **Shutdown/Co-Optation:** Occasionally, bots are taken out by system administrators or security researchers; or taken over by competing botnets.

# Botnet Architectures



- Have become more elaborate over time, as Bot-Masters attempt to protect their creations
- Star: Master host at the “hub” with a dedicated IRC channel for C&C
- Multi-Server: Control is devolved onto a collection of closely coupled sub-master hosts. Use of HTTP for C&C.
- Hierarchical: Multiple layers of controllers are provided, yielding some fault tolerance.
- Random: All bots are also control nodes; communication is via Peer-to-Peer (P2P).

# Botnet Examples



- **MafiaBoy Botnet** (February 2000): Canadian teenage hacker mounts DDoS attacks that brought down the websites of Amazon.com, Ebay.com, Dell.com, etc. Used a botnet he apparently stumbled across.
- **Clickbot.A** (May 2006): an early botnet (up to 100,000 hosts) that specialized in “low-noise click fraud against search engines.” Google was eventually able to identify the fraud, effectively shutting the botnet down.
- **Storm** (January 2007): 100,000+ host botnet spread by email spam. Botnet actively defends itself against attackers. Controllers appear to be decentralizing the botnet into subnets that can be individually deployed.
- **Waledac** (Fall 2009): a “pseudo-clone” of Storm apparently built using a botnet toolkit. Shut down in February 2010 after analysis by Microsoft Digital Crimes Unit.

## Botnet Examples (continued)



- **Srzibi** (March 2007): a 450,000+ host botnet specializing in spam (responsible in 2008 for at least 40% of all spam on the Internet)
- **Conficker** (Nov 2008): extensive botnet (8 million hosts in 100 countries) distinguished by large number of attack exploits. At least five variants have been deployed, each with more advanced capabilities.
- **Mariposa** (Summer 2009): global botnet (bots in 190 countries) with an estimated 13 million hosts. Shut down in Feb 2010.

# Network-Visible Botnet Behaviors



- Incursion: Very unlikely to be detected
- Spread: If network worm techniques are used, scanning activity may be visible. Odd payloads may flow into infected hosts.
- Spread: As botnet forms inside the enclave, surges of DNS activity on a “strange” domain may occur.
- Synchronization & Attack: Surges in SMTP traffic may occur (Spambot). Odd network services may appear in the enclave, and probes to peculiar services on external machines (e.g., via HTTP) may happen. Odd protocols (e.g., peer-to-peer) may come into use.
- Exfiltration: “Unusual” payloads may be observed moving out of the enclave (use of encryption is suspicious).

# “Odd” Behaviors as Anomalies

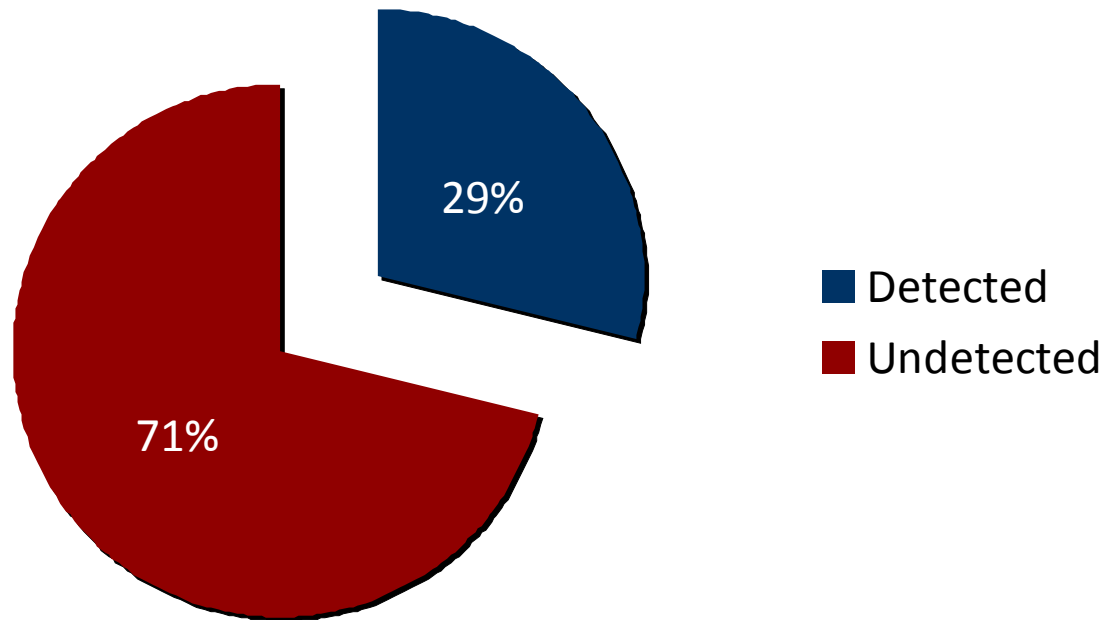


*Can we interpret anomalous behaviors as malicious?*

# What You Don't Know



## Malware Detected by Anti-Virus



Source: Cyveillance <http://tinyurl.com/malware-detection>

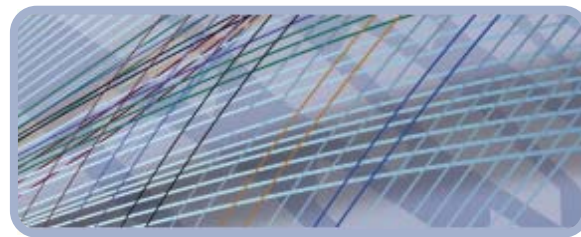
# Anomaly Detection



- People use anomaly detection intuitively.
- People have a mental model for what is normal in a given environment.
- Abnormal behavior stands out.
- Some things are obvious red flags on most networks:
  - Outbound IRC traffic
  - Unusual Windows processes
- Manual anomaly detection has shortcomings
  - Networks are complicated. “Normal” might be surprising.
  - Data overload



# An Assist From Automation



## ➤ Automated anomaly detection

- Not a replacement for signature-based IDS or anti-virus.
- Filters for the most anomalous, or more interesting, events.
- Provides a safety net for advanced threats that bypass other defenses.
- Increases network analysts' effectiveness.

# Types of Anomaly Detection: Behavioral Anomaly Detection



## ➤ Behavioral (Heuristic) Anomaly Detection

- Rules-based
- A static model of “anomalous”, but more general than traditional signatures.
- How must malware behave differently from normal traffic in order to accomplish its mission?

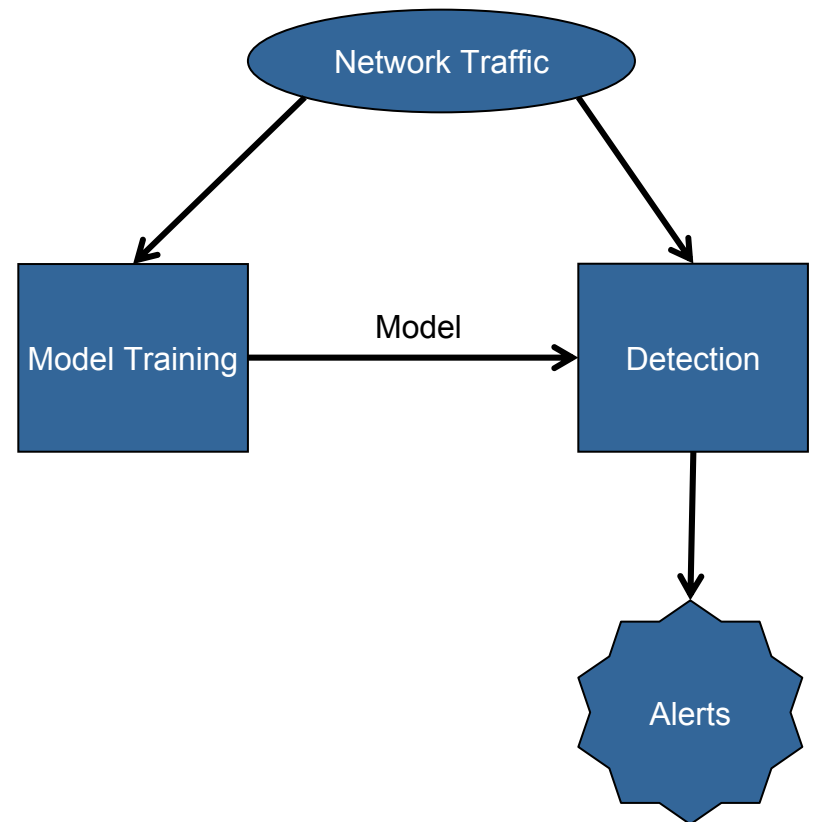
## ➤ Examples:

- Scanning
- Connections to common command and control ports

# Types of Anomaly Detection: Statistical Anomaly Detection



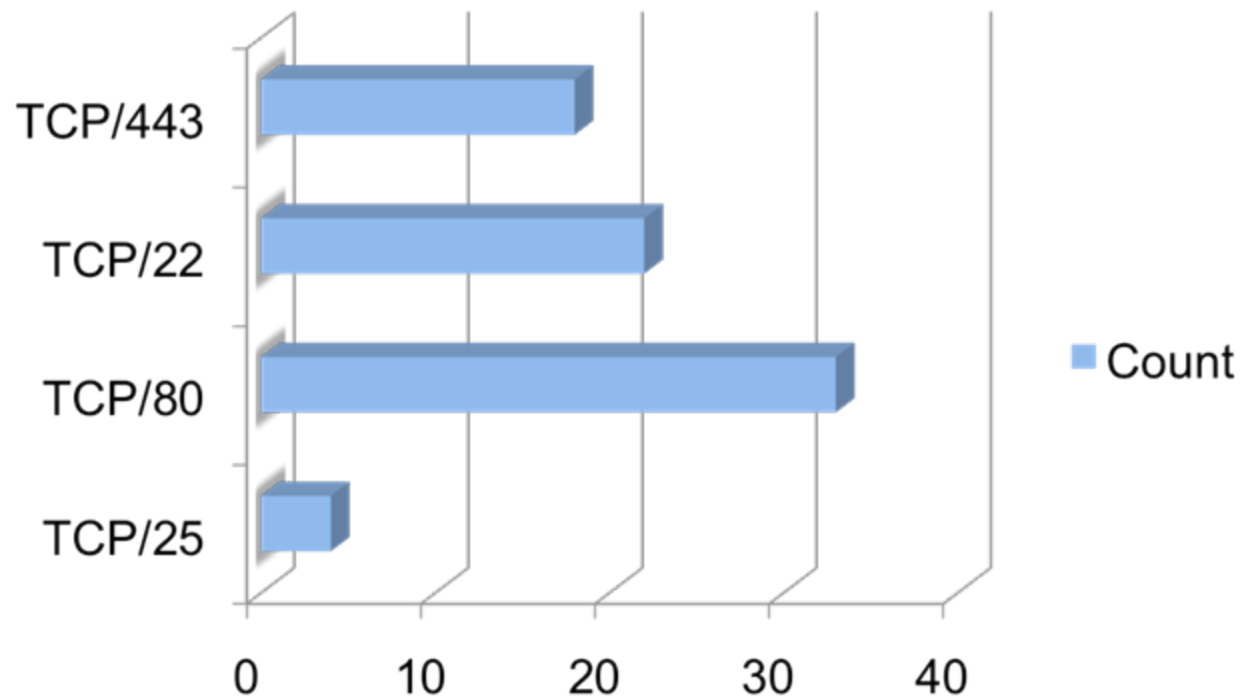
- Dynamic, learned, model of “normal”.
- Types
  - Flow-based discrete models
  - Flow-based continuous models
  - Payload analysis
- Models are specific to each site.
- Models can be continuously trained.
- Supervised vs. unsupervised



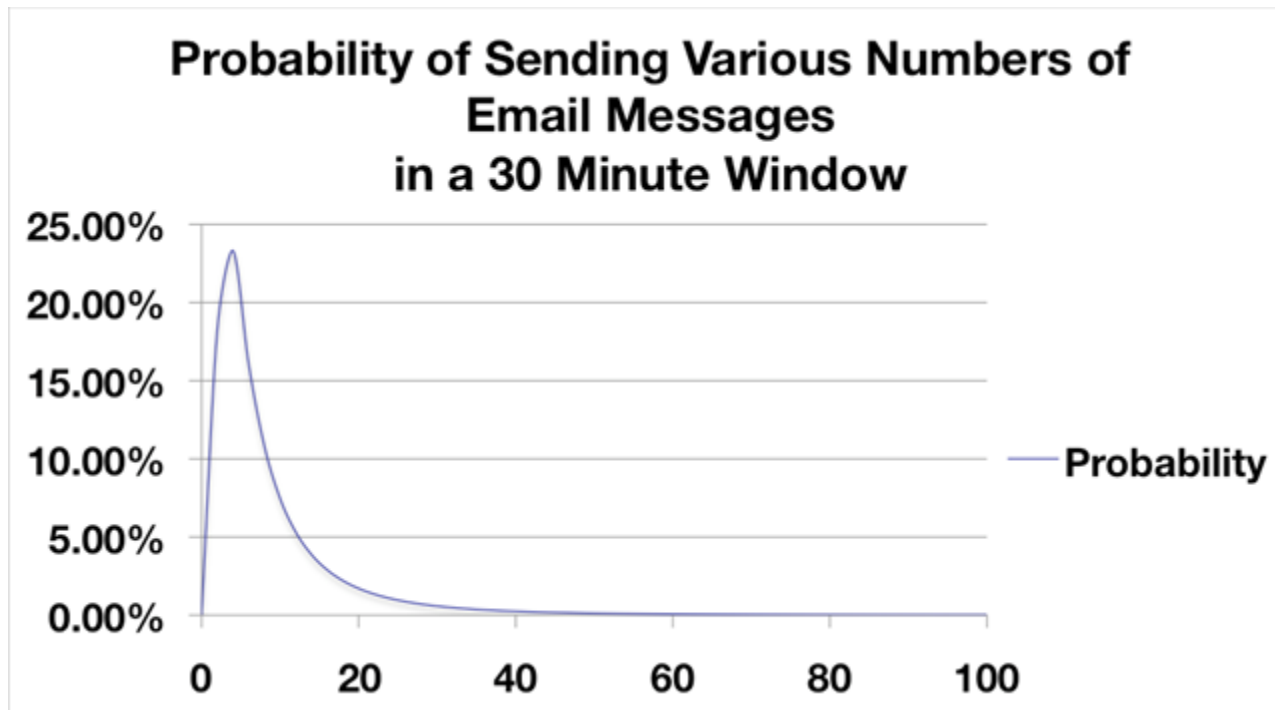
# Statistical Anomaly Detection: Discrete Models



## Connections by Service Port



# Statistical Anomaly Detection: Continuous Models



# Statistical Anomaly Detection: Payload Analysis



- Does the traffic on this port look like the traffic seen during the model training period, or is somebody sending a new or different protocol over this port?
- Can model undocumented, non-standard, and proprietary protocols.
- Natural language version
  - All human beings are born free and equal in dignity and rights.
  - Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti.
- Network traffic version
  - GET /en\_us/blogs/gumblar-continues-spread HTTP/1.1
  - GET /scripts/../../winnt/system32/cmd.exe?/c+dir HTTP/1.1

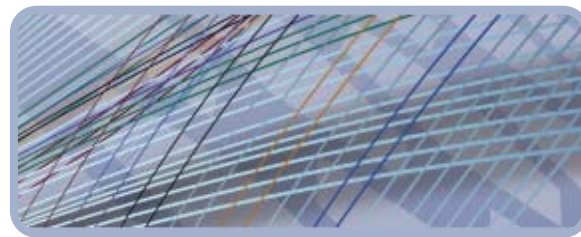
# CounterStorm: An IDS with Multiple Detection Engines



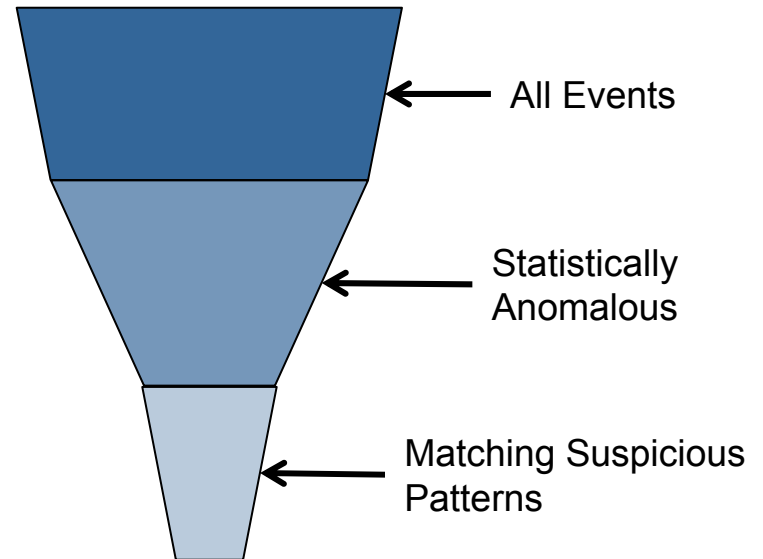
- Uses behavioral Anomaly Detection (AD) to detect several important kinds of surveillance activities (Scan Detection)
- Uses several kinds of statistical AD to infer malicious behavior
  - Volumetric: Surges in infrastructure usage
  - Rogue: Appearance of peculiar services and hosts
  - Statistical Payload Analysis (SPA): Anomalous payloads in network dataflows



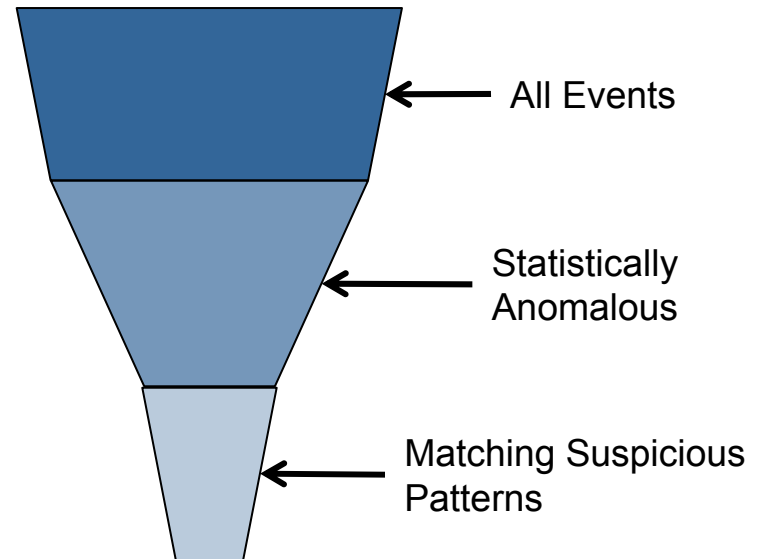
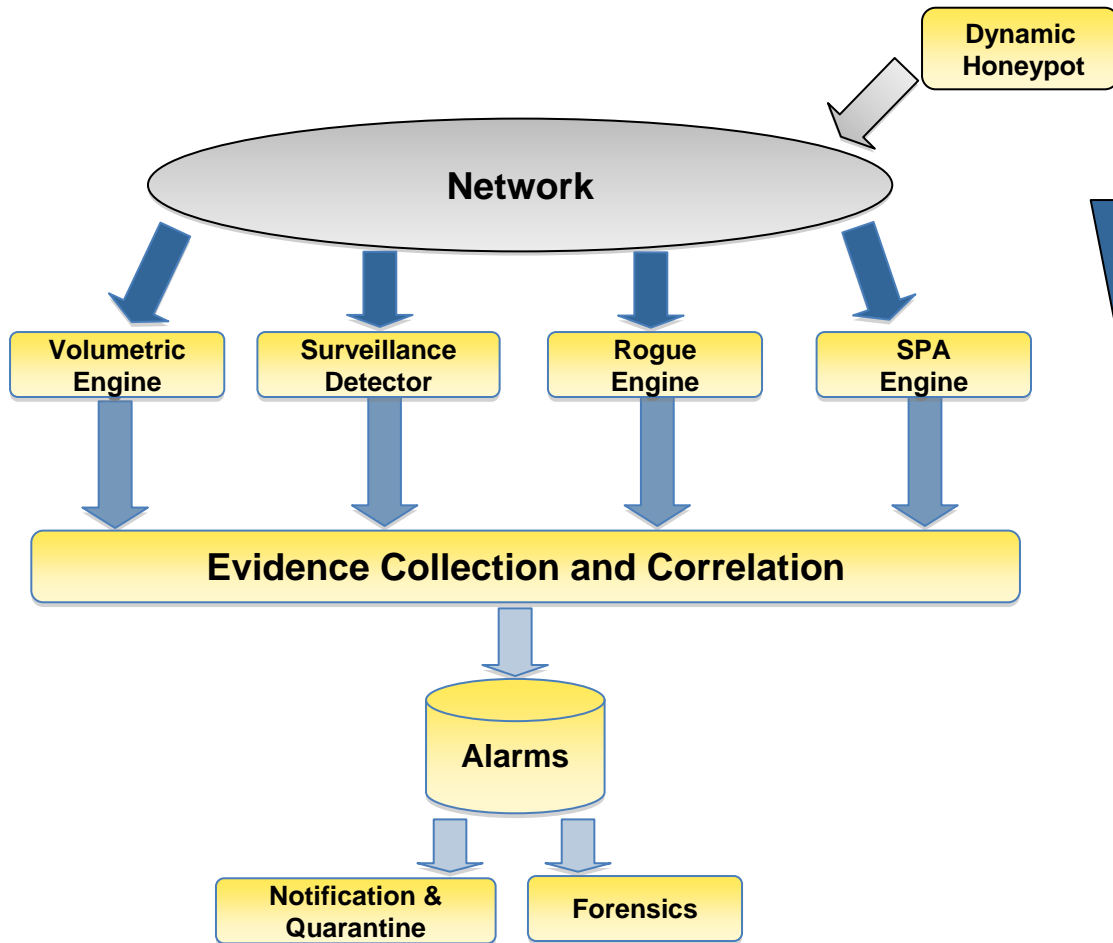
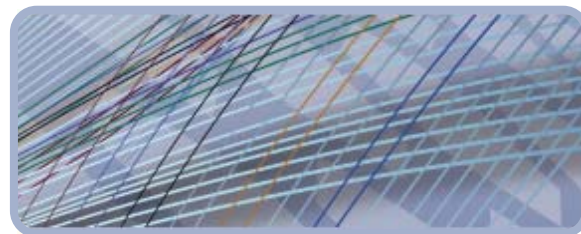
# The CounterStorm Approach



- ✓ The most common complaint about anomaly detection is the false positive rate.
- ✓ This reputation stems largely from attempts to use the fire hose of statistical anomaly detection alerts directly.
- ✓ Simply increasing thresholds creates an unnecessarily large blind spot.
- ✓ CounterStorm's hybrid approach combines detection techniques in series to provide only the most interesting alarms to the user.



# The CounterStorm Approach (cont.)



# Covering Your Bases: A Botnet Example



Activity	Detected by
Infection by known malware	Anti-virus and traditional IDS
Worm-like propagation	CounterStorm's Surveillance Detection
Spam dissemination	CounterStorm's Volumetric Engine
C&C connections to unusual ports, like IRC	Firewall Rules CounterStorm's Rogue Engine
C&C connections to normal ports, like HTTP	CounterStorm's Statistical Payload Analysis Engine
Connections to normal ports on unusual servers or from unusual clients (e.g., HTTP to a database server)	CounterStorm's Rogue Engine
Data Exfiltration	CounterStorm's Rogue Engine

# CounterStorm Benefits



- Provides actionable intelligence so that network analysts can focus on the most important activity.
- Discovers malware before signatures are available.
- Finds zero-day, targeted, and advanced persistent threats.
- Can be configured to automatically quarantine devices until suspicious activity can be investigated.
- Passively monitors, so network performance is not degraded.
- Provides multiple means of detecting subtle behaviors, such as botnet activity

# Summary



- Botnets are a serious, stealthy threat to enterprise and government networks.
- Signature- and rule-based Intrusion Detection Systems (IDSs) attempting to provide “border” defense are inadequate.
- IDSs based on Anomaly Detection (AD) provide multiple opportunities to detect botnet activity across their complete lifecycle.
- CounterStorm, a network IDS deployed inside the enclave

# Contact Information



For more information or to purchase CounterStorm, contact:

**[CSSales@TrustedCS.com](mailto:CSSales@TrustedCS.com)**  
**866.230.1307**

**[www.TrustedCS.com/CounterStorm](http://www.TrustedCS.com/CounterStorm)**

# Questions



*Questions?*



*[www.TrustedCS.com](http://www.TrustedCS.com)*