Security Camp Conference
Fine Art of Balancing Security & Privacy

Kim Bilderback
AT&T Director GovEd Cybersecurity Services
kb7459@att.com
August 21, 2014
Cybersecurity - The Threats Increase

**Ten-Fold**
Increase in DDOS attacks in the last 2 years

**614%**
Mobile malware increase March ’12 to March ’13
Juniper Networks Mobile Threats Report 2013

**BotNets**
Infection rate = 18 computers per second = 500 million annually
Director of FBI’s cyber division, Joseph Demarest, 07/15/14

**Recent Breaches**
St. Louis, CHS, Shaw’s, CyberVor, eBay, & People’s Liberation Army

![AT&T DDoS Mitigations](chart)

Cost of managing cyber security breach: ranges from $1.4 million to $46 million/year (56 businesses studied)

[http://www.youtube.com/watch?v=eOSRQ-c1XW0](http://www.youtube.com/watch?v=eOSRQ-c1XW0)
Cybersecurity – Defense Spending (In Billions)
Cybersecurity - Verizon 2014 Data Breach Investigations Report

Number of breaches per threat action category over time

http://www.verizonenterprise.com/DBIR/2014/
What’s Going On?

The likelihood approaches certainty that something unknown is in your network.

“…There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don’t know we don't know.” - US DoD Press Conf. 02/02

THE WALL STREET JOURNAL.

“APTs are the cutting edge of cyber attacks, and even the most hardened security pros say they are almost impossible to prevent. "There isn't a corporation in the nation today that can't be penetrated, not one,“

April 2, 2012
Anti-virus Scanning Effectiveness - Myth of the Known Knowns

Virus Bulletin – VB100 RAP Test Results

- Reactive & Predictive Test
- Effectiveness detecting 100% malware samples listed as 'In the Wild' by the WildList Organization
- Generate no false positives when scanning an extensive test set of clean samples
- All this done with default, out-of-the-box settings in the VB lab environment.
Malicious Software – The Rise of The Unknown Unknowns

Unknown Unknowns

Anti-virus Scanning Effectiveness – The Challenge of the Unknown Unknowns

Lastline Labs AV Scan Effectiveness Analysis

• Tested new malware daily for year against the 47 Virus Total service A/V scanners

• 51% Detected New Malware Zero Day

• Avg. 2 days for at least one AV scanner to detect when not found Zero Day

• Over 365 days no single AV scanner had a perfect day

• After a year, there are samples that 10% of the scanners still do not detect

http://securityaffairs.co/wordpress/25385/malware/zero-day-malware-detection.html
What To Do?

**Signature Based Detection Not Enough**
- Polymorphic malware characteristics now common avoid signature detection through obfuscation techniques
- Explosion of zero-day malware variants unknown to signature developers. Time delay to recognize, develop & implement signatures causes vulnerability
- Exponential growth in malware causing exponential size increase for signature databases. Complex to support, maintain, update & causes process difficulties
- Intrusive Yet More “Private”

**Behavioral Based Detection Needed Too**
- Baseline normal network traffic behavior or characteristics using Big Data analytics
- Anomalies or deviations to normal trigger timely alerts causing detailed analysis
- Timely analysis yields faster knowledge of a breach & quicker time to mitigation
- Behavior based detection systems:
  1. SIEM
  2. RSA Silvertail
  3. DDoS Detection – Arbor Networks
- Non-intrusive Yet Less “Private”
Behavioral Analysis (SIEM) – Effectiveness

Comparison of APT and No-APT by SIEM and non-SIEM sub-samples

Ponemon Institute

Behavioral & Signature Based Monitoring System – AT&T Example

Threat Alert & Response
“Single Pane of Glass”

Behavioral Based Detection
(Zero Day and Advanced Persistent Threats)

Signature Based Detection
(traditional)

Manage Signal-to-Noise Ratios

Behavior Based Detection
Sign Based Detection
Behavioral & Signature Based Monitoring System – RSA Silvertail Example

Manage Signal-to-Noise Ratios
Behavioral & Signature Based Monitoring System – Arbor DDoS Example

Manage Signal-to-Noise Ratios
Adaptive Security Architecture – Gartner Model

- Secure Infrastructure
  - Firewalls
  - IAM
- Vulnerability Scans
- Pen Testing
- SIEM Baselining
- Incidence Response
- SIEM Alerting
- DDoS Mitigation
- Log Analysis
- Packet Capturing
- Intrusion Detection
- Email Filtering
- A/V Scanning
- SIEM Detection
Cybersecurity threat landscape consists of “known knowns” & “unknown unknowns” – the latter is the greater threat.

Yet most organizations invest majority of time & money defending against the “known knowns” using ineffective “signature based” technology.

An improved defensive posture is achieved augmenting “signature based” technology with “behavioral based” technology shown to be more effective detecting “unknown unknowns”.

Privacy concerns may increase as more “behavioral based” technology deployed, but that is offset by increased defensive posture and can be balanced by governance.

Effective cybersecurity is not about finding the best technology and turning it on, but in deploying a range of defensive measures, monitoring and managing them.

Vigilance – “Alert & Persistent Watchfulness”
More On The Subject

att.com/threattraq

kb7459@att.com
Thank you.