Understand Your Threat

A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted.
Let's build a million-dollar cluster to crack it.

NO GOOD! It's 4096-bit RSA!

BLAST! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:
His laptop's encrypted.
Drug him and hit him with this $5 wrench until he tells us the password.

GOT IT.
“If you’re good at security response, you will win all of the battles you fight.
If you’re great, you will know all of the battles you’re fighting”
CISOs finding it difficult to define security ROI to executives

*Short shelf life for CISOs*

Vastly expanding attack surface area

*Mobile, cloud, virtualization, global business operations*

Large protection investments and no good prioritization filter

*Who, why, when, how*

Operational chaos

*Too many alarms, not enough people, poor prioritization*

“Brain dead” security tools that rely on past events/signatures

*Verses extremely agile adversaries*

Severe breaches continue...
The Threat Intelligence Marketplace Challenge

- Most “intelligence” vendors delivering incident data without context or intent.
- Most solutions are U.S. focused and have superficial global insight.
- Most vendors delivering “intelligence” from historic breaches or events they are observing today.
- Most “intelligence” vendors don’t have the human expertise required to understand methods or affiliations.
How Can Cyber Threat Intelligence Help?

1. Be Proactive

2. Shrink the Problem

3. Improve Prioritization

4. Advance Executive Communications

CISO Recommendation:

“Use a commercial threat intelligence service to develop informed tactics for current threats, and plan for threats that may exist in the midterm future.”

Rob McMillan & Kelly Kavanagh
Technology Overview for Security Threat Intelligence Service Providers
Published: 16 October 2013
“Many vendors can provide raw information, but there are only a comparative few that provide true intelligence capabilities.”

Rob McMillan & Kelly Kavanagh
Technology Overview for Security Threat Intelligence Service Providers
Published: 16 October 2013

Actionable Intelligence is:
• Accurate
• Aligned with your intelligence requirements
• Integrated
• Predictive
• Relevant
• Tailored
• Timely

Rick Holland
Blog: Actionable Intelligence, Meet Terry Tate, Office Linebacker
Published: 11 February 2014
Intelligence from iSIGHT
iSIGHT Intelligence helps them determine which events pose the greatest risk to their unique organization.

Customer Side
People, process, and technology helps them determine possible risks.

Threat Sources
- Attack Surface
- Attack Alerts
- Correlated Events
- Incident Indicators
- Verified Threat Indicators
- Pre-Processed Analysis
- Raw Observations

Noise to Signal

VERIFIED THREAT INDICATORS
PRE-PROCESSED ANALYSIS
RAW OBSERVATIONS
Threat Sources

Shrink the problem
Changing the Cyber Security Discussion
Putting “Threat” Back Into the Risk Equation

Geek Speak

- Analyzed 1,452,134 logs
- Detected 423,132 viruses
- Blocked 2,028,438 connections
- Closed 3,095 Incident Tickets
- Patched 30,000 Systems

Business Impact

Prevented 2 Cyber-Crime Attacks
- Linked to ABC Criminal Organization
- Targeting POS Systems
- Prevented theft of 10M Customer Credit Cards
- Avoided $78M Loss:
  - Cleanup, Notification,
  - Brand Reputation & Revenue
  - Shareholder Lawsuit & Stock Drop
How Is Intelligence Led Security Defined?

- **Intelligence-led security isn’t:**
  - Just big-data technology integration
  - Just “dedicated” intelligence teams
  - Faster response times to security intelligence feeds

- **Our theory:**
  - A paradigm shift from technology-based decisions to threat-based decisions
  - Adding context and prioritization to technical environments and observations
  - Workflow changes from reactive to proactive
  - Connecting to the business
Cyber Threat Intelligence

WHO/WHAT?
- Actors
- Groups
- Government Sponsors

WHY/WHEN?
- Motivation
- Intent
- Capabilities

HOW?
- TTPs
- Methods
- Play Books

“Actionable Intelligence”
Multi-faceted, forward looking, validated, highly contextual analysis

Based On Multiple Collection Methods

Threat Data Feeds

- One dimensional data
- Narrow collection focus
- No or limited validation and analysis
- High signal-to-noise = many false positives
- Increased alerts = wasted effort
- Little/no prioritization context
Rich Threat Context VS Minimal Analysis

Cyber Threat Intelligence
- Bad IP Address
- Actor Group
- Motivation
- Primary Targets
- Ability to Execute
- Additional IPs, Domains
- Malware Used
- Lures
- Vulnerabilities Targeted
- Historic Campaigns
- Successful Compromises

Threat Data Feed
- Bad IP Address
- Ranking
- Last Hop Geo Location

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved. www.isightpartners.com
Categorical Application of Intelligence

- **Strategic**
  - Future Oriented
  - Utilize emerging trends and patterns to make long-term decisions
  - Understand current and planned controls with respect to their application to countering the threat

- **Operational**
  - Prioritize Resources for the “Real vs. the Perceived”
  - Consider affiliations and historical capabilities of actors
  - Factor business outcomes of threats into detection, mitigation strategies and priorities

- **Tactical**
  - Interactive analysis and information flow from partners, internal tools and threat environment
  - Prioritize technical threat analysis vs. mitigation resources “as it happens”
  - Factor business outcomes of the threats into mitigation actions
Objectives

Provide understanding of identified and credible threats, correlated to business impact

Enable formulation of approaches to dealing with threats

Provide understanding of how to mitigate threats directly

Strategic

Operational

Tactical

Executives

Managers & Analysts

Security Operators
Intelligence Integration Across the IS Environment

INTELLIGENCE SOURCES
- Cyber Threat Intelligence
- Informal Networks of Peers
- Social Media Indications & Warnings
- Academia
- Vendor Studies
- Data Feeds
- Reputable Web Sources
- Public/Private Sharing
- Internal/Subject Matter Experts

INTEL ANALYSIS
- Intelligence Analyst Workbench
- Intelligence Data Repository

SENSOR ENRICHMENT
- Intrusion Detection System/Intrusion Prevention System
- Inline Malware Analysis
- Firewalls
- Web Application Firewall/DDoS Migration
- DLP/Endpoint Protection

SECURITY ANALYTICS
- Security Operations Center (SOC) 
- Security Information and Event Management Tools
- Proxies
- NetFlow

HIGH FIDELITY RESPONSE
- Incident Response Team
- Incident Case Management Tool
- Incident Partners – Business unit
- Security
- Legal
- Communications
- External parties, Law enforcement, If engaged

External Info Sharing
- With industry peers,
- Critical Infrastructure partners, public/private
- Documentation, e.g., PR-IRAC

Fraud, Business Unit owners, event sponsorship teams, e.g., Olympics, World Cup
ecosystem partners, i.e., suppliers-manufacturers-merchants, Supply Chain,
Executive Management, Physical security teams, emerging technology/products,
teams, Mergers & Acquisitions

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved www.isightpartners.com
Threat Intelligence Operations

**Intelligence enabled Detection:**
- Assess requirements and plan integrated technology platform with intelligence capabilities
- Route high impact threat information quickly through the value chain through tagging

**Intelligence enabled Analysis:**
- Ensure end-to-end link between technical artifacts produced by tools and business context
- Fuse Threat, Technical and Campaign Intelligence

**Intelligence enabled Response:**
- Continue information and context gathering during incident response
- Understanding adversary guides response actions

**Intel to business**
- Strategic, Operational and Tactical intelligence
- Adversary and Actor Information

**Incidents**
- Aggregation and Correlation Platform
- Workflow Automation
- Vulnerability and Impact Assessment

**Indicators**
- Malware, Technical & Campaign Intelligence
- Link Analysis

**Observables**
- Threat Detection Platform
- Technical and Non-Technical Events
- Identification Training
- Discovery Planning and Requirements Management

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved
www.isightpartners.com
### Cyber Threat Intelligence Case Study

#### Combatting the Threat with Intelligence

<table>
<thead>
<tr>
<th>Executive</th>
<th>Operational</th>
<th>Tactical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness to consider applicability of threat and susceptibility to threat.</td>
<td>Control tuning and adversary focused assessment.</td>
<td>Detect and mitigate and rapid response.</td>
</tr>
<tr>
<td>Process reviews and asset inventory.</td>
<td>Monitoring and mitigation of egress.</td>
<td>Proactively applied intelligence.</td>
</tr>
<tr>
<td>Control audits and resource planning.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Strategic
- **April 8, 2013**
  - Analysis of “Dump Memory Grabber” POS Malware

#### Operational
- **April 11, 2013**
  - Attribution of Russian Actor ‘Ree[4]’
- **May 1, 2013**
  - Russian Actor ‘Ree[4]’ Seeks to Expand Sales of Credit Card RAM Memory Grabber
- **August 6, 2013**
  - Source Code for BlackPOS Sold in the Underground
- **October 15, 2013**
  - Command and Control Infrastructure Used for POS Malware
- **Dec 20, 2013**
  - Trojan POSRAM Malware and stolen card sales
- **Jan 14, 2014**
  - Kaptoxa Point-of-Sale Compromise
- **Jan 29, 2014**
  - Overview of Point-of-Sale Malware
- **March 17, 2014**
  - POSRAM related to other malware families

#### Tactical
- **2013**
  - **2014**

---

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved www.isightpartners.com
## Cyber Threat Intelligence Case Study

### Combatting the Threat **without** Intelligence

<table>
<thead>
<tr>
<th>Strategic</th>
<th>Operational</th>
<th>Tactical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive awareness to consider applicability of threat and susceptibility to threat.</td>
<td><strong>Operational</strong> teams gain increased awareness of threat as proliferation is now eminent.</td>
<td><strong>Tactical</strong> monitoring for specific indicators of compromise and fraud activity.</td>
</tr>
<tr>
<td>▪ Rumors</td>
<td>▪ Ingress focused detection</td>
<td>▪ Unlinked FireEye alerts</td>
</tr>
<tr>
<td>▪ PCI Attestation</td>
<td></td>
<td>▪ Respond to law enforcement enquiries</td>
</tr>
</tbody>
</table>

### Awareness of an emerging threat | Barrier to entry removed | Active victim exploitation | Evolution and proliferation

- April 8, 2013: Analysis of ‘Dump Memory Grabber’ POS Malware
- April 11, 2013: Attribution of Russian Actor ‘Ree[4]’
- May 1, 2013: Russian Actor ‘Ree[4]’ Seeks to Expand Sales of Credit Card RAM Memory Grabber
- August 6, 2013: Source Code for BlackPOS’ Sold in the Underground
- October 15, 2013: Command and Control Infrastructure Used for POS Malware
- Dec 20, 2013: Trojan.POSRAM Malware and stolen card sales
- Jan 14, 2014: Kaptoxa Point-of-Sale Compromise
- Jan 29, 2014: Overview of Point-of-Sale Malware
- March 17, 2014: POSRAM related to other malware families

---

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved  www.isightpartners.com
### 2014 Ponemon Study – Reasons for participating in Threat Intelligence Sharing

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improves the security posture of my organization</td>
<td>71%</td>
</tr>
<tr>
<td>Improves the security posture of the nation’s critical infrastructure</td>
<td>64%</td>
</tr>
<tr>
<td>Improves situational awareness</td>
<td>54%</td>
</tr>
<tr>
<td>Fosters collaboration among peers and industry groups</td>
<td>51%</td>
</tr>
<tr>
<td>Makes threat data more actionable</td>
<td>24%</td>
</tr>
<tr>
<td>Reduces the cost of detecting and preventing cyber attacks</td>
<td>21%</td>
</tr>
<tr>
<td>Enhances the timeliness of threat data</td>
<td>16%</td>
</tr>
</tbody>
</table>
2014 Ponemon Study – Reasons for not participating in Threat Intelligence Sharing

- No perceived benefit to my organization: 65%
- Lack of trust in the sources of intelligence: 53%
- Potential liability of sharing: 50%
- Lack of resources: 42%
- Anti-competitive concerns: 26%
- Cost: 25%
- Slow, manual sharing processes: 24%
- Lack of incentives: 15%
### 2014 Ponemon Study – Main Sources of Threat Intelligence

<table>
<thead>
<tr>
<th>Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peers in other companies</td>
<td>58%</td>
</tr>
<tr>
<td>IT security vendors</td>
<td>55%</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>33%</td>
</tr>
<tr>
<td>Industry associations</td>
<td>26%</td>
</tr>
<tr>
<td>Government officials</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>
2014 Ponemon Study – How Threat Intelligence is Shared

- Data feeds: 57%
- Peer group discussion via phone, email or in-person: 54%
- Threat advisories: 49%
- Intelligence briefs: 33%
- Other: 4%
2014 Ponemon Study – What Threat Intelligence is Shared

- Threat indicators such as suspicious phishing or malware IP addresses: 55%
- Software vulnerability patch updates: 48%
- Incident response information: 36%
- Results of cybercrime investigations and prosecutions: 22%
- Other: 3%
2014 Ponemon Study – Ways to Share Threat Intelligence

- Trusted intermediary that shares with other organizations: 34%
- Threat intelligence exchange service: 25%
- Industry organization that distributes to others: 19%
- Government entity that shares with other organizations: 9%
- Directly with other organizations: 8%
- No preference: 5%
Lessons Learned - Consortiums

- Establish strong information sharing protocols
- Drive Public/Private Partnership
- Enable a culture of (Information) Security
- Change the conversation to include business context
- Employ basic information security hygiene
- Continuously seek to understand the evolving threat
- Recognize that you are not unique
- Understand third party connections
- Agree on standards and support them as a community
Cybercrime actors have a very high interest in targeting personal and financial data that can be monetized.

Cybercrime actors launch malware campaigns on a constant basis, and like to use what works.

Capable cybercrime actors are constantly seeking holes in web applications in order to harvest consumer data.

Cybercrime actors may use DDoS attacks to mask other malicious activity.

Hardware/Supply Chain exploitation is less likely from cybercrime activity.

Cybercrime actors face low barriers to entry.

<table>
<thead>
<tr>
<th>Likelihood of Impact</th>
<th>Malware Campaigns</th>
<th>Web Application Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate Threat</td>
<td>Distributed Denial-of-Service (DDoS)</td>
<td></td>
</tr>
<tr>
<td>Low Threat</td>
<td>Hardware / Supply Chain Exploitation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope of Impact</th>
<th>Narrow / Low</th>
<th>Partial / Moderate</th>
<th>Broad / High</th>
<th>Universal / Very High</th>
</tr>
</thead>
</table>
**State-Sponsored Threats**

State-sponsored actors are typically well-resourced and sophisticated.

**State-Sponsored activities** may also involve acquiescence and or public/private partnership.

**Targeted information typically** includes data that can be used to gain some sort of strategic advantage.

**State-sponsored espionage activity** can also take the form of hacktivism.

**Cyber espionage activity** is often facilitated by malware campaigns using specially-crafted lures to deliver payloads such as RATs.

**Watering hole attacks** are also frequently leveraged in targeted intrusion activity.

<table>
<thead>
<tr>
<th>Likelihood of Impact</th>
<th>Web Application Attacks</th>
<th>Malware Campaigns</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate Threat</td>
<td></td>
<td>Hardware / Supply Chain Exploitation</td>
</tr>
<tr>
<td>Low Threat</td>
<td>Distributed Denial-of-Service (DDoS)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope of Impact</th>
<th>Narrow / Low</th>
<th>Partial / Moderate</th>
<th>Broad / High</th>
<th>Universal / Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Convergence of Threats

<table>
<thead>
<tr>
<th></th>
<th>Pre-2007</th>
<th>2007-2010</th>
<th>2010-current</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeting</strong></td>
<td>Public Sector</td>
<td>Private Sector</td>
<td>Public Sector</td>
</tr>
<tr>
<td><strong>Adversary</strong></td>
<td>CC (Individuals)</td>
<td>CE (Hacktivist Groups)</td>
<td>CC (Cyber Espionage)</td>
</tr>
<tr>
<td><strong>Methodologies</strong></td>
<td>CC (Web defacement)</td>
<td>CE (Direct Exploitation Modified Crime tools)</td>
<td>CC (Spear Phishing/Spam)</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>CC (Individually operated)</td>
<td>CE (Botnet rentals)</td>
<td>CC (Cybercrime)</td>
</tr>
</tbody>
</table>

Proprietary and Confidential Information. © Copyright 2014, iSIGHT Partners, Inc. All Rights Reserved. www.isightpartners.com
IE 0-Day Exploitation

VWF Compromise
- Watering hole attack hosted on Veterans of Foreign Wars website
- Leveraged IE 10 0-day vulnerability (later assigned CVE-2014-0322)
- Attributed to group targeting a specific population, most likely for strategically-valuable data

Other Use
- Leveraged the same 0-day over the same timeframe
- Involves multiple sites redirecting to exploit site
- All compromised sites resolve to the same IP; thus, the adversary may have compromised a VPS server, suggesting indiscriminate targeting and an attack less opportunistic in nature than the VWF compromise

Some Overlap in Tactics, Techniques and Procedures
University of Washington website compromised, served DarkComet RAT

- Evidence for cybercrime attribution
  - Obfuscation techniques used typically associated with cybercrime activity
  - DarkComet often associated with cyber espionage, but is freely available online
- Possible evidence for cyber espionage attribution
  - Decoded data from malicious binary included a string possibly indicating targeting victims related to a government entity

Overlap in Malware, TTPs, Targets
Campaigns Exploiting CVE-2013-3906

Hangover Campaign
- Attribution
  - State-sponsored actors
- Targets
  - Individuals in high-profile organizations primarily in South Asia

Campaign Leveraging Citadel, Solarbot, other interactive malware
- Attribution
  - Financially-motivated actors
- Targets
  - Financial institutions in SE Asia and the Middle East
- Potential targeted intrusion model

Dual use nature of exploits, shared underground resources and use of targeted intrusion tactics by financially-motivated actors
In Feb. 2014, Colombian law enforcement dismantled a cyber crime group with alleged ties to a paramilitary group.

The group reportedly caused $14.7 million USD in losses to Colombian banking customers.

Allegedly used Xtreme RAT, which has various functionality:
- Keylogging to capture victims' online banking credentials
- Searching victims' computers for personal information to impersonate them
- Identification of high-value accounts
Russian-Language Underground

- Russian-language actor “Eshkinkot” active in cybercrime forums tied to cyber espionage campaign (2012)
  - Sought assistance using exploits, decryption and data exfiltration malware
  - Claimed to have installed an unidentified Trojan on a corporate network

- Implication: the cybercrime underground enables espionage activity
  - Provides a marketplace for tools, knowledge and skilled actors willing to act on behalf of interested parties

Shared Network of Underground Channels and Resources
Crossover Campaigns: Global evolution of threats

• iSIGHT Partners has observed sophisticated espionage activity campaigns and TTPs transcending boundaries and sectors with common TTPs since 2009.

• Observed attacks on Tibet's government-in-exile and global Tibetan activists overlap with campaigns perpetrated against high-value assets elsewhere.

• Tibetan cyber espionage campaigns contain leading and trailing indicators that will be used against government, defense and civilian industry targets.

• GhostNet, ShadowNet and LuckyCat Campaigns
  • The LuckyCat Campaign
  • Poison Ivy Trojan
  • Lurid Trojan
  • Protux
  • Dojack
  • NetTravler Trojan