The Rise of Threat Detection and Response

Lucas Zaichkowsky
lucas@accessdata.com
Twitter: @LucasErratus
Is Prevention Futile?
Security Economics
Tit for Tat
A product to stop advanced attacks?

Detection by Deception
Slow down and prevent automated and human attacks with no false positives.
1. Perform footprinting and reconnaissance
2. Gain initial entry. Common methods…
   a) SQLi
   b) Phishing
   c) Buying backdoor access on black market
   d) Compromise a 3rd party with access
3. System and network enumeration
4. Privilege escalation
5. Lateral movement to establish a beachhead
   a) Drop a diverse set of backdoors
   b) Steal user passwords, target domain controllers and file servers
6. Find pivot points to access restricted network segments
7. Copy sensitive data to another compromised system using valid credentials
8. Exfiltrate undetected through obfuscation and “blending in” with internet traffic
What really works? Defense in depth.
Intelligence-driven defense creates a defenders advantage

**Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**, Lockheed Martin

**Intrusion Attempts 1, 2, and 3 Indicators**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Intrusion 1</th>
<th>Intrusion 2</th>
<th>Intrusion 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weaponization</td>
<td>Trivial encryption algorithm</td>
<td>Key 1</td>
<td>Key 2</td>
</tr>
<tr>
<td>Delivery</td>
<td>[Email subject]</td>
<td>[Email subject]</td>
<td>[Email subject]</td>
</tr>
<tr>
<td></td>
<td>[Email body]</td>
<td>[Email body]</td>
<td>[Email body]</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:dnt...etot@yahoo.com">dnt...etot@yahoo.com</a></td>
<td><a href="mailto:ginette...e...@yahoo.com">ginette...e...@yahoo.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>00.abc.xyz.215</td>
<td>216.abc.xyz.76</td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td>CVE-2009-0658 [shellcode]</td>
<td>[PPT 0-day] [shellcode]</td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>C1...Vsexm32.exe</td>
<td>C1...VSEXUpd.exe</td>
<td>C1...VEXPLORE.exe</td>
</tr>
<tr>
<td>C2</td>
<td>202.abc.xyz.7 [vTTP request]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Courses of Action Matrix**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Web analytics</td>
<td>Firewall ACL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weaponization</td>
<td>NIDS</td>
<td>NIPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>Vigilant user</td>
<td>Proxy filter</td>
<td>In-line AV</td>
<td>Queueing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td>HIDS</td>
<td>Patch</td>
<td>DEP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>HIDS</td>
<td>&quot;chroot&quot; jail</td>
<td>AV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>NIDS</td>
<td>Firewall ACL</td>
<td>NIPS</td>
<td>Tarpir</td>
<td>DNS redirect</td>
<td></td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td>Audit log</td>
<td>Quality of Service</td>
<td>Honeypot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Moving Beyond Prevention
Detection and response on the rise

The Fatal Mistake:
85% of security budgets currently go here

Progress:
Companies are now investing here

And Then:
Companies are forced to invest here

By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2013 (Gartner)
Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

“… it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn’t publicly revealed: Poring over computer logs, Target found FireEye’s alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware.”

– Bloomberg BusinessWeek

FireEye Alert: “malware.binary”

“This event represents detection of one or more binaries being transferred over the wire and detected by the FireEye appliance as malicious.”

http://www.reuters.com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313

“The experts said that they believed it was likely that Target’s security team received hundreds of such alerts on a daily basis, which would have made it tough to have singled out that threat as being particularly malicious.”

Only 31% of companies discover breaches through their own monitoring…

For retailers, it’s only 5%.

– Verizon Enterprise Solutions 3-Year Study
Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data…

“The hackers moved unnoticed in the company’s computers for more than eight months, sometimes tripping hundreds of alerts daily…”

-- Bloomberg BusinessWeek

“These 60,000 entries, which occurred over a three-and-a-half month period, would have been on average around 1 percent or less of the daily entries on these endpoint protection logs, which have tens of thousands of entries every day,”

-- Neiman Marcus Spokesperson
Too many alerts, not enough analysts

Key Metrics:
- Mean Time to Detect
- Mean Time to Validate
- Mean Time to Contain
- Mean Time to Resolution

400,000,000 events received per day
5,714 alerts generated and evaluated per day
157 incidents investigated per day
The slower the response, the greater the exposure

- 66% Of Breaches Took Months or Even Years to Discover
- 60% Of Breaches Have Data Exfiltrated in First 24 Hours
- 60,000 Number of Alerts Hackers Set Off at Neiman Markus
- 229 Median Number of Days Advanced Attackers Present Before Detection
- 33% Of Organizations Discover Breaches Through Their Own Monitoring

How long to investigate alerts?

1. Retrieve live response data to validate alerts
2. Classify the incident by searching for reputation, history, and context
3. Collect and analyze:
   • Data from disk
   • Memory
   • Netflow data and network sessions
   • Logged events
4. Timeline attack activity
   • Collect and analyze more data as required
5. Create and execute a remediation plan
   • Remove malware
   • Undo changes to web sites
   • Reset all potentially compromised passwords
Achieving Rapid Detection and Response
Talent shortage?
What about point product fatigue?
Consolidate capabilities needed by security teams

- Endpoint forensics
- Endpoint network packet capture
- Mobile endpoint support
- Endpoint threat detection
- Endpoint activity recording and replay
- Malware analysis
- Memory analysis
- Removable media monitoring
- Network packet capture and forensics
- Network threat detection
- Threat intelligence
- Enterprise remediation
Integrate into existing products, services, and threat intelligence sources

- SIEMs
- Malware analysis products and services
- Next-Generation threat detection products
- Commercial and free threat intelligence feeds
- Machine readable threat intelligence (STIX, OpenIOC, YARA, delimited files, XML, etc.)
Automate workflows and standard operating procedures

1. Analyst Reviews Alert
2. IR Triage of the Target System and Review Results
3. System is Potentially Compromised, Perform Network Isolation
4. Search and Determine if Any Suspicious Processes are Running
5. Perform Memory Dump and Analyze
6. Perform Deeper Incident Response - Review Key Artifacts (events logs/internet history)
7. Gain Context and Understand the Threat
8. Manual Remediation or Reimage of the System
IDT Corp Automation Case Study

### Savings per security alert

- **Rapid detection and response halts attack progression, thereby reducing risk.** Automation reduced the 30 minute response time to 30 seconds.

- **Lost IT technician productivity went from a half day to zero**

- **Lost productivity for each affected employee went from a full workday to 2.5 hours**

- **Manual forensic analysis can be up to $25,000 and take several days.** Automation reduced roughly 80% of that.

<table>
<thead>
<tr>
<th>Current Manual Approach to Incident Response</th>
<th>RI Platform Approach to Incident Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="SIEM Alert" /></td>
<td><img src="image" alt="SIEM Alert" /></td>
</tr>
<tr>
<td><strong>LEADING SIEM</strong></td>
<td><strong>LEADING SIEM</strong></td>
</tr>
<tr>
<td>Manual Information Security</td>
<td><strong>ResolutionOne™ Platform</strong></td>
</tr>
<tr>
<td><img src="image" alt="30 min." /></td>
<td><img src="image" alt="30 sec." /></td>
</tr>
<tr>
<td>Manual System Isolation</td>
<td>Automated System Isolation</td>
</tr>
<tr>
<td><img src="image" alt="1.5 hrs." /></td>
<td><img src="image" alt="1.5 hrs." /></td>
</tr>
<tr>
<td>Manual Forensic Imaging (Memory and Disk)</td>
<td>Automated Live Forensic Analysis and Imaging (Memory and Disk)</td>
</tr>
<tr>
<td><img src="image" alt="6 hrs." /></td>
<td><img src="image" alt="Instantly" /></td>
</tr>
<tr>
<td>Manual Re-imaging from Gold Master + Patching</td>
<td>Automated Malware Analysis</td>
</tr>
<tr>
<td><img src="image" alt="4 hrs." /></td>
<td><img src="image" alt="1 hr." /></td>
</tr>
<tr>
<td>Manual Return to User</td>
<td>Automated Re-imaging and Return to User</td>
</tr>
</tbody>
</table>

**Total Time:**
- Automated: 2.5 hrs.
ResolutionOne™ CyberSecurity: Consolidate, integrate, automate
Questions?

Lucas Zaichkowsky
lucas@accessdata.com
Twitter: @LucasErratus