Embracing the Uncertainty of Advanced Attacks using Big Data Analytics

Eddie Schwartz
CISO, RSA
ANONYMOUS
We are Legion. We do not Forgive. We do not Forget.
<table>
<thead>
<tr>
<th>Last</th>
<th>First</th>
<th>AB</th>
<th>R</th>
<th>H</th>
<th>2B</th>
<th>3B</th>
<th>HR</th>
<th>RBI</th>
<th>BB</th>
<th>SO</th>
<th>SB</th>
<th>BA</th>
<th>OBP</th>
<th>SLG</th>
<th>OPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ortiz</td>
<td>David</td>
<td>560</td>
<td>113</td>
<td>162</td>
<td>37</td>
<td>1</td>
<td>41</td>
<td>130</td>
<td>109</td>
<td>129</td>
<td>0</td>
<td>.289</td>
<td>.406</td>
<td>.577</td>
<td>.983</td>
</tr>
<tr>
<td>Ramirez</td>
<td>Manny</td>
<td>486</td>
<td>93</td>
<td>144</td>
<td>32</td>
<td>1</td>
<td>33</td>
<td>105</td>
<td>84</td>
<td>111</td>
<td>0</td>
<td>.297</td>
<td>.400</td>
<td>.567</td>
<td>.967</td>
</tr>
<tr>
<td>Pena</td>
<td>Wily Mo</td>
<td>378</td>
<td>55</td>
<td>104</td>
<td>23</td>
<td>1</td>
<td>20</td>
<td>66</td>
<td>30</td>
<td>111</td>
<td>3</td>
<td>.276</td>
<td>.336</td>
<td>.504</td>
<td>.840</td>
</tr>
<tr>
<td>Youkilis</td>
<td>Kevin</td>
<td>523</td>
<td>90</td>
<td>142</td>
<td>37</td>
<td>2</td>
<td>18</td>
<td>76</td>
<td>84</td>
<td>106</td>
<td>4</td>
<td>.271</td>
<td>.376</td>
<td>.456</td>
<td>.832</td>
</tr>
<tr>
<td>Crisp</td>
<td>Coco</td>
<td>509</td>
<td>84</td>
<td>158</td>
<td>27</td>
<td>3</td>
<td>13</td>
<td>63</td>
<td>40</td>
<td>75</td>
<td>2</td>
<td>.310</td>
<td>.358</td>
<td>.524</td>
<td>.884</td>
</tr>
<tr>
<td>Pedroia</td>
<td>Dustin</td>
<td>451</td>
<td>114</td>
<td>93</td>
<td>18</td>
<td>2</td>
<td>10</td>
<td>41</td>
<td>30</td>
<td>69</td>
<td>5</td>
<td>.263</td>
<td>.336</td>
<td>.446</td>
<td>.753</td>
</tr>
<tr>
<td>Hinske</td>
<td>Eric</td>
<td>279</td>
<td>41</td>
<td>73</td>
<td>18</td>
<td>2</td>
<td>10</td>
<td>41</td>
<td>30</td>
<td>69</td>
<td>5</td>
<td>.263</td>
<td>.336</td>
<td>.446</td>
<td>.753</td>
</tr>
<tr>
<td>Lowell</td>
<td>Mike</td>
<td>482</td>
<td>64</td>
<td>131</td>
<td>33</td>
<td>1</td>
<td>15</td>
<td>74</td>
<td>42</td>
<td>59</td>
<td>2</td>
<td>.273</td>
<td>.333</td>
<td>.441</td>
<td>.774</td>
</tr>
<tr>
<td>Lugo</td>
<td>Julio</td>
<td>473</td>
<td>74</td>
<td>134</td>
<td>29</td>
<td>3</td>
<td>8</td>
<td>51</td>
<td>44</td>
<td>74</td>
<td>19</td>
<td>.284</td>
<td>.347</td>
<td>.406</td>
<td>.753</td>
</tr>
<tr>
<td>Mirabelli</td>
<td>Doug</td>
<td>124</td>
<td>13</td>
<td>27</td>
<td>7</td>
<td>0</td>
<td>5</td>
<td>17</td>
<td>12</td>
<td>38</td>
<td>0</td>
<td>.218</td>
<td>.294</td>
<td>.386</td>
<td>.680</td>
</tr>
<tr>
<td>Cora</td>
<td>Alex</td>
<td>212</td>
<td>26</td>
<td>54</td>
<td>8</td>
<td>2</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>27</td>
<td>5</td>
<td>.254</td>
<td>.313</td>
<td>.333</td>
<td>.646</td>
</tr>
<tr>
<td>Giambi</td>
<td>Jason</td>
<td>395</td>
<td>84</td>
<td>100</td>
<td>18</td>
<td>0</td>
<td>29</td>
<td>81</td>
<td>92</td>
<td>102</td>
<td>2</td>
<td>.252</td>
<td>.413</td>
<td>.518</td>
<td>.930</td>
</tr>
<tr>
<td>Rodriguez</td>
<td>Alex</td>
<td>555</td>
<td>128</td>
<td>102</td>
<td>24</td>
<td>1</td>
<td>20</td>
<td>64</td>
<td>47</td>
<td>92</td>
<td>3</td>
<td>.277</td>
<td>.389</td>
<td>.447</td>
<td>.835</td>
</tr>
<tr>
<td>Jeter</td>
<td>Derek</td>
<td>585</td>
<td>110</td>
<td>189</td>
<td>32</td>
<td>4</td>
<td>12</td>
<td>71</td>
<td>59</td>
<td>93</td>
<td>23</td>
<td>.322</td>
<td>.390</td>
<td>.452</td>
<td>.843</td>
</tr>
<tr>
<td>Abreu</td>
<td>Bobby</td>
<td>474</td>
<td>95</td>
<td>131</td>
<td>28</td>
<td>2</td>
<td>16</td>
<td>65</td>
<td>86</td>
<td>107</td>
<td>22</td>
<td>.289</td>
<td>.383</td>
<td>.447</td>
<td>.835</td>
</tr>
<tr>
<td>Damon</td>
<td>Johnny</td>
<td>548</td>
<td>94</td>
<td>158</td>
<td>30</td>
<td>4</td>
<td>18</td>
<td>73</td>
<td>62</td>
<td>76</td>
<td>14</td>
<td>.289</td>
<td>.362</td>
<td>.485</td>
<td>.821</td>
</tr>
<tr>
<td>Posada</td>
<td>Jorge</td>
<td>405</td>
<td>65</td>
<td>105</td>
<td>21</td>
<td>1</td>
<td>24</td>
<td>65</td>
<td>84</td>
<td>131</td>
<td>102</td>
<td>.259</td>
<td>.365</td>
<td>.443</td>
<td>.808</td>
</tr>
<tr>
<td>Cano</td>
<td>Robinson</td>
<td>533</td>
<td>76</td>
<td>164</td>
<td>36</td>
<td>3</td>
<td>16</td>
<td>80</td>
<td>30</td>
<td>65</td>
<td>5</td>
<td>.308</td>
<td>.345</td>
<td>.472</td>
<td>.817</td>
</tr>
<tr>
<td>Posada</td>
<td>Jorge</td>
<td>405</td>
<td>65</td>
<td>105</td>
<td>21</td>
<td>1</td>
<td>24</td>
<td>65</td>
<td>84</td>
<td>131</td>
<td>102</td>
<td>.259</td>
<td>.365</td>
<td>.443</td>
<td>.808</td>
</tr>
<tr>
<td>Phillips</td>
<td>Andy</td>
<td>286</td>
<td>37</td>
<td>74</td>
<td>15</td>
<td>2</td>
<td>11</td>
<td>45</td>
<td>21</td>
<td>60</td>
<td>0</td>
<td>.259</td>
<td>.313</td>
<td>.441</td>
<td>.754</td>
</tr>
<tr>
<td>Cabrera</td>
<td>Melky</td>
<td>514</td>
<td>74</td>
<td>145</td>
<td>27</td>
<td>3</td>
<td>10</td>
<td>59</td>
<td>45</td>
<td>65</td>
<td>10</td>
<td>.282</td>
<td>.341</td>
<td>.408</td>
<td>.749</td>
</tr>
<tr>
<td>Mientkiewicz</td>
<td>Doug</td>
<td>232</td>
<td>29</td>
<td>58</td>
<td>13</td>
<td>1</td>
<td>5</td>
<td>30</td>
<td>26</td>
<td>38</td>
<td>1</td>
<td>.251</td>
<td>.328</td>
<td>.382</td>
<td>.710</td>
</tr>
<tr>
<td>Cairo</td>
<td>Miguel</td>
<td>179</td>
<td>22</td>
<td>46</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>16</td>
<td>9</td>
<td>23</td>
<td>8</td>
<td>.258</td>
<td>.300</td>
<td>.343</td>
<td>.643</td>
</tr>
<tr>
<td>Fasano</td>
<td>Sal</td>
<td>130</td>
<td>10</td>
<td>29</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>16</td>
<td>1</td>
<td>37</td>
<td>0</td>
<td>.256</td>
<td>.290</td>
<td>.352</td>
<td>.612</td>
</tr>
</tbody>
</table>
Audit Checklist

- Audit Satisfactory
- Nonconformances Found
- Observations Made
Just a question on signatures...

Does the signature team not do Zeus/ZBot configuration files? We have submitted a number (20+) of ".bin" files over the last 6-8 weeks but have yet to see these files detected using "Official" signatures. Should we not submit these files?

Tom
Caesar recognized the omens, he just didn’t think they applied to HIM.” - Nate Silver
The signal is the truth. The noise is what distracts us from the truth. This is a book about the signal and the noise.
APT 2:
Exposing one China’s most
BIZARRE cyber espionage units
What level of resources belongs RIGHT HERE??

APT Attack Progression

- Prepare
  - Reconnaissance
  - Weaponization
- Infect
  - Delivery
  - Detonation
- Interact
  - Command and Control
  - Escalation & Lateral Movement
- Exploit
  - Entrenchment
  - Data Exfiltration

Cost to remediate

Defense Solutions

What is the universe of data that is useful here?

Attacker’s exposure

Cost to attacker

High detection potential

Source: Greg Hogland
Prevention: 80%
Monitoring: 15%
Response: 5%

Prevention: 33%
Monitoring: 33%
Response: 33%
The Rise of Big Data
I don't always like uncertainty

But when I do, I want BIG DATA Analytics
BIG DATA
TRANSFORMS
SECURITY
• Comprehensive Visibility
• Actionable Intelligence
• Agile Analytics
• Centralized Incident Management
<table>
<thead>
<tr>
<th></th>
<th>SOC</th>
<th>CIRC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tasks</strong></td>
<td>• Tool Administration</td>
<td>• Incident Investigation</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability Scanning</td>
<td>• Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td>• Tier 1 Event Support</td>
<td>• Malware Analytics</td>
</tr>
<tr>
<td></td>
<td>• Break-Fix</td>
<td>• Response Coordination</td>
</tr>
<tr>
<td><strong>Skill set required</strong></td>
<td>• Intermediate security knowledge</td>
<td>• Deep threat knowledge</td>
</tr>
<tr>
<td></td>
<td>• Good tool &amp; process knowledge</td>
<td>• Advanced technical capability</td>
</tr>
<tr>
<td></td>
<td>• Generic company knowledge</td>
<td>• Investigative experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deep company knowledge</td>
</tr>
<tr>
<td><strong>Role of a service provider</strong></td>
<td>• Can successfully be outsourced to an MSSP</td>
<td>Tough to outsource as a standalone function</td>
</tr>
<tr>
<td><strong>Bottom Line</strong></td>
<td>• Waiting for a smack on the head</td>
<td>Hunting bad guys</td>
</tr>
</tbody>
</table>
I get Dark Reading RSS Feeds...

I am an ISAC member

I apply threat and IOC data to my SIEM

I write rules and synthesize data

The AV companies rely on me for data

One does not simply walk into intelligence-driven security
<table>
<thead>
<tr>
<th>Monitoring and Detection</th>
<th>Incident Response</th>
<th>Threat Intelligence</th>
<th>Systems &amp; Analytics</th>
<th>Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawl</td>
<td>N/A (Reactive)</td>
<td>Responding to business impacts only</td>
<td>Basic IoC Register</td>
<td>Network Egress Key End Points</td>
</tr>
<tr>
<td>Walk</td>
<td>All major PoPs Remote Access</td>
<td>Continued discovery &amp; prioritization of compromises</td>
<td>Trending / Profiling Kill Chain Analysis</td>
<td>Forensic Evidence Repository &gt; 50% End Points</td>
</tr>
<tr>
<td>Run</td>
<td>Dedicated FTEs 75% delivery detection</td>
<td>Planned Containment &amp; Eradications</td>
<td>External Intel Sources Sharing Groups</td>
<td>&gt; 90% End Point Analysis Lab</td>
</tr>
<tr>
<td>Advanced</td>
<td>&gt; 90% NW and End Point Visibility</td>
<td>&lt; 5% Business Impact Dedicated FTEs</td>
<td>Detailed Campaign Analysis</td>
<td>Advanced Analysis Dedicated FTEs</td>
</tr>
<tr>
<td>World Class</td>
<td>Subsidiaries, M&amp;As, B2B links</td>
<td>Training &amp; Rotation Delegation &amp; Liaisons</td>
<td>Federated Intel Sharing</td>
<td>Resident RE Mobile &amp; Emerging Tech</td>
</tr>
</tbody>
</table>
Critical Incident Response Center

Cyber Threat Intelligence
- Open/All Source Actor Attribution
- Attack Sensing & Warning
- Social Media
- High Value Target (HVT)

Advanced Tools, Tactics & Analysis
- Reverse Malware Engineering
- Host & Network Forensic
- Cause & Origin Determination
- Email operations

Critical Incident Response Team
- Eyes-on-Glass
- End User Intake
- Event Triage
- Incident Containment
- 24x7 Coverage

Advanced Specialists
- Integration & Content Development
- Strategic Planning
THE ANALYTICS

- Reporting and Alerting
- Investigation
- Malware Analytics
- Administration
- Complex Event Processing
- Free Text Speech
- Correlation
- Metadata Tagging

REAL-TIME

LIVE INTELLIGENCE

- Threat Intelligence
- Rules
- Parsers
- Alerts
- Feeds
- Apps
- Directory Services
- Reports and Custom Actions

FLEXIBLE INTEGRATION (API)

Incident Management

Asset Criticality

Compliance

DISTRIBUTED COLLECTION

- Europe
- North America
- Asia

WAREHOUSE

MONTHS/YEARS

LONG-TERM
All Network Traffic & Logs

Downloads of executables

Type does not match extension

Terabytes of data - 100% of total

Thousands of data points – 5% of total

Hundreds of data points – 0.2% of total

Create alerts to/from critical assets
A few dozen alerts
• Named Pipes -> OS Construct for Inter-process Communication.
• Can be used as an endpoint for IPC across the network (e.g. \PIPE\ATSVC)
• Process that owns the Named Pipe must have NT AUTHORITY\NETWORK
• OS interrogates the caller’s security context
• Widely used; enumerate Named Pipes with Mark Russinovich’s Pipelist:

```
C:\Documents and Settings\user\Desktop>pipelist
PipeList v1.01
by Mark Russinovich
http://www.sysinternals.com

<table>
<thead>
<tr>
<th>Pipe Name</th>
<th>Instances</th>
<th>Max Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>TerminalServer\AutoReconnect</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>InitShutdown</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>lsass</td>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>protected_storage</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>ntsvcs</td>
<td>4</td>
<td>-1</td>
</tr>
<tr>
<td>scerp</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>SfcApi</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>net\NtControlPipe1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Winsock2\CatalogChangeListener-3d8-0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>net\NtControlPipe7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>atsvc</td>
<td>2</td>
<td>-1</td>
</tr>
</tbody>
</table>
```
<match name="pipe">
  <if name="state" equal="1">
    <!-- move back past the \PIPE\ string and two length bytes -->
    <move value="-8" />

    <!-- read LSB of PIPE length ; assume max pipe length of 255 (FF)--> 
    <read name="pipe_name_len" length="1" />

    <!-- move past second len byte -->
    <move value="1" />

    <!-- decrement the pipe length to account for null byte--> 
    <decrement name="pipe_name_len" value="1" />

    <!-- read the full pipe name without null byte -->
    <read name="full_pipe_name" length="$pipe_name_len" />

    <!-- read next byte--> 
    <read name="check_byte" length="1"/>

    <!-- this is the "sanity checking" part. if the byte read is the null byte, we have more assurance we just read a complete string, probably for a pipe length -->
    <if name="check_byte" equal="&\0:"> 
      <register name="alert" value="$full_pipe_name" />
    </if>
  </if>
</match>
PIPE
0c 00 \PIPE\n
6 + 2 = 8 Bytes
0c 00 \PIPE\atsvc | 2 Bytes 12 - 1 = 11 Bytes
0c 00 \PIPE\atsvc 001

NULL Byte?
Success.
Named Pipes on the Wire.
Named Pipes on the Wire.
Named Pipes on the Wire:

```
pipe\lsass (1342) - pipe\browser (113) - pipe\srvsvc (13) - pipe\winreg (9) - pipe\ntsvcs (4) - pipe\hello (3) -
pipe\atsvc (2) - pipe\wkssvc (1)
```

OH HAI DERE!
Next Steps:

- Whitelists (lsass, samr, netlogon, browser, spoolss, wkssvc, winreg, srvsvc, atsvc, netlogon, sql\query)
- External intel joins (IOCs, etc.)
- What else can we learn from other standard Named Pipes, i.e. detect services configuration.
- UUID & SecondaryAddr mismatch?
- Anonymous Pipes, Other RPC Connection Modalities
Even MORE Big Data Inside

URGENT
Visibility

Intelligence

Control

Governance
Fraud Prevention

Criminals Look Different than Others..

- Velocity
- Page Sequence
- Origin
- Contextual Information
Threat Modeling

Velocity
Behavior
Parameter
Injection
Man in the Middle
Man in the Browser

Anomaly Identification
Asset Intelligence
Event Capture
Investigations
Threat Intelligence
Asset Intelligence
Analyst Prioritizations
Event Capture
Investigations
Threat Intelligence
Big Data

IT Info
- Asset List
- Device Type
- Device Content
- CMDBs
- Vuln. Scans

Biz Context
- Device Owner
- Business Owner
- Business Unit
- Biz Process
- RPO / RTO

Criticality Rating

Big Data
- Asset Criticality Intelligence
  - IP Address
  - Criticality Rating
  - Business Unit
  - Facility
IGNORANCE
Sometimes it's best just not to know.
BIG DATA FUELS INTELLIGENCE-DRIVEN SECURITY

Rapid growth in security information creates new capabilities to defend against the unknown

AUTHORS
Sam Carry, Chief Technology Officer, Identity and Data Protection business unit; Chief Technologist, RSA, The Security Division of EMC
Engin Kirda, Sy and Laurie Stemberg Associate Professor of Information Assurance, Northeastern University
Eddie Schwartz, Vice President and CSIO, RSA, The Security Division of EMC
William H. Stewart, Senior Vice President, Bocx Allen Hamilton
Avi Yaron, General Manager, Security Management and Compliance business unit; Senior Vice President, RSA, The Security Division of EMC

January 2013

WHAT IS BIG DATA?
Big data describes datasets that are too large, too unrefined or too fast-changing for analysis using relational or multidimensional database techniques. Analyzing big data can require dozens, hundreds or even thousands of servers running massively parallel software. What truly distinguishes big data, aside from its volume and variety, is the potential to analyze it to uncover new insights to optimize decision-making.

KEY POINTS
- The dissolution of traditional defensive perimeters coupled with attackers’ abilities to circumvent traditional security systems requires organizations to adopt an intelligence-driven security model that is more risk-aware, contextual, and agile.
- Intelligence-driven security relies on big data analytics. Big data encompasses both the breadth of sources and the information depth needed for programs to assess risks accurately and to defend against illicit activity and advanced cyber threats.
- Within the next two years, we predict big data analytics will disrupt the status quo in most information security product segments, including SIEM, network monitoring; user authentication and authorization; identity management; fraud detection; and governance, risk & compliance.
- In the next three to five years, we predict data analytics tools will further evolve to enable a range of advanced predictive capabilities and automated real-time controls.
- Integrating big data analytics into business risk management and security operations will require organizations to rethink how information security programs are developed and executed. Six recommendations are presented in the session titled Building a Big Data Security Program.
- Security teams need analysts who combine data science with a deep understanding of business risks and cyber attack techniques. Personnel with these skill sets are scarce, and they will remain in high demand. As a result, many organizations are likely to turn to outside partners to supplement internal security analytics capabilities.

Thank you!

eddie.schwartz@rsa.com
http://www.linkedin.com/in/eddieschwartz/