ThreatQ/Reservoir Labs: Maximizing Value of Threat Intelligence at the Sensor Level

Ryan Trost, Co-Founder & CTO
Ryan.Trost@threatq.com
ThreatQuotient

ThreatQ was built by a SOC team of security, intelligence, malware, and signature analysts to structure, centralize and ‘man-handle’ intelligence through:

- Indicator Management
- Attack Tracker (i.e. spearphish)
- Adversary Profile
- Signature Repository

...and the Threat Intelligence Platform (TIP) technology was born!
Threat Intelligence is critical because...

Fact:
- threat intelligence can REDUCE adversary dwell time!
- threat intelligence is reaching critical mass and analysts are swimming in data pools (i.e. ‘paralysis by analysis’)
- collecting threat intelligence is 1/2 the battle because unless organizations can deploy it...it’s pretty USELESS!!

...this is where ThreatQ and R-Scope fit perfectly!!
How does it work?

THREATQUOTIENT
Battle Rhythm Workflow

1. Automatically ingest, normalize, and structure indicators from malware tools and/or external intelligence sources. API, STIX/TAXII, XML, JSON, CSV, crontab, parse, analysts’ muscle

2. Perform a “rear-view mirror” search to identify prior successful attempts and determine indicator’s false positive probability.

3. Distribute indicators/signatures to appropriate sensor grid.

4. Deploy single/group of IOCs to a SIEM for advanced correlation. Provide indicator attribution to SIEM to prioritize incoming alerts.

5. Collect incident details from ticket system to calculate indicator, threat intelligence, and source metrics.

6. Collect event details from SIEM to calculate indicator, threat intelligence, and source metrics.

7. Easily export intelligence for sharing.

USER LEGEND

- Security Analyst
- Signature Engineer
- Malware Analyst
- Intel/Fusion Analyst
- SOC/CIRT Manager

Reservoir Labs

Reservoir Labs
### Use Case Example - CryptoJoker Ransomware

<table>
<thead>
<tr>
<th>Reconnaissance</th>
<th>Weaponization</th>
<th>Delivery</th>
<th>Exploitation</th>
<th>Installation</th>
<th>C2</th>
<th>Mission</th>
</tr>
</thead>
</table>

#### SOURCE #1
- .pdf document
  - 2015:12:31 09:22:01-05:00
- MD5: bca6c1fa9b9a8bf60eeceb91e08d1323
  - file987[at]sigaint[dot]org
  - file987[at]openmail[dot]cc
  - <shell code>
- %TEMP%\imgdesktop.exe; \windefrag.exe;
  - daapv[dot]de/wp-content/.../statistics.exe
  - server6[dot]hcservers.com/~advavast/...
  - SSL S/N: 0x00c4679a049741ef47

#### SOURCE #2
- .pdf document
  - 2015:12:30 11:31:32-05:00
- MD5: ec434e23f7568ceb961253fe6abef71
  - file987[at]sigaint[dot]org
- file987[at]tutanota[dot]com
  - <shell code>
- %TEMP%\ drvpci.exe; windrv.exe; winpnp.exe
  - daapv[dot]de/wp-content/.../statistics.exe
  - svcrec[dot]org/offline.php
  - argentcourt[dot]com/offline.php

#### SOURCE #3
- .pdf document
  - 2015:12:24 15:14:33-05:00
- MD5: 904b0888bfa02d200091fa8ad014d016
  - file9876[at]openmail[dot]cc
- <shell code>
  - SSL S/N: 0x00c4679a049741ef47

#### DISPARATE THREAT INTELLIGENCE

...based on real data
...let’s see how the sausage is made!
Step 1: Threat Intelligence is collected, normalized, and de-duplicated
Step 2: What the data looks like within ThreatQ
Step 3: ThreatQ exports the intelligence into BRO Policies

module $Spearphish;
export {
    # We'll generate a new notice when we see this. Let's add that to the known notice types.
    redef Notice::Type += { CryptoJoker_Spearphisher_Found);
}
event SMTP::log_smtp(rec: SMTP::Info) {
    if ( rec$from == "file987@sigaint.org" ) {
        # We have a match on the email sender, now let's check if our known domain is in the transmission chain for this message
        for ( i in rec$path ) {
            if ( rec$path[i] == daapv.de/wp-content/…/stapspcs.exe ) {
                NOTICE([$note=CryptoJoker_Spearphisher_Found, $msg=fmt("Spearphisher found, sending e-mail with subject %s., rec$subject), $uid=rec$uid, $id=rec$id]);
                # To associate a particular connection with this notice.
                return;
            } # end path if
        } # end for
    } # end from if
} # end log_smtp event
Step 4: R-Scope monitors for the malicious activity and creates “notices”

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>ts</td>
<td>uid</td>
<td>id.orig_h</td>
<td>id.resp_h</td>
<td>method</td>
<td>host</td>
<td>uri</td>
<td>referer</td>
<td>resp_mime_types</td>
</tr>
<tr>
<td>1451561468</td>
<td>OctKHes5Gq8pA6e</td>
<td>109.237.132.12</td>
<td>GET</td>
<td>dascv.de</td>
<td>/mime/蛉t/蛉nt/蛉nt/蛉nt/statistic.exe</td>
<td>-</td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561470</td>
<td>COB9q63K553W52Dh</td>
<td>143.233.204.80</td>
<td>POST</td>
<td>career.aga.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?90=14&amp;dl=1</td>
<td>-</td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561471</td>
<td>OD826Z2W4Z2FIFwR5</td>
<td>143.233.204.80</td>
<td>GET</td>
<td>career.aga.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?90=14&amp;dl=3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561474</td>
<td>QAe1qQWq5Kw6B6T9k</td>
<td>148.146.61.138</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru/">http://in-adler.ru/</a></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561475</td>
<td>Co57C13K48S5P7K7</td>
<td>143.233.204.80</td>
<td>GET</td>
<td>career.aga.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?90=14&amp;dl=5</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561476</td>
<td>QAIur48usQc7V26</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;4f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561477</td>
<td>CoZv7Ygi6Zq7TiYh</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561478</td>
<td>OAI23P4QW6Zp7YFA</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru">http://in-adler.ru</a></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561503</td>
<td>CZmJ5Mc38Q7TioW</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;4f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561517</td>
<td>Co6FakwMh94n414</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru">http://in-adler.ru</a></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561528</td>
<td>CJ35OG3EEYVLYL6p9</td>
<td>82.146.61.138</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru">http://in-adler.ru</a></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561531</td>
<td>CTkX4Z2B5m8Z7V</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561545</td>
<td>CynXn41U8LbH9bZy5</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561555</td>
<td>OEv9w20ZU0N7PQJh</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru">http://in-adler.ru</a></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1451561558</td>
<td>CTP4l8ggy6O4AC</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;4f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561572</td>
<td>CJF65jUQ3KM3W5GFG</td>
<td>211.119.245.213</td>
<td>GET</td>
<td>kbconst.co.kr</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=4899=1&amp;4f=1 &amp;sleey3.dll</td>
<td><a href="http://kbconst.co.kr">http://kbconst.co.kr</a></td>
<td>text/plain</td>
<td>-</td>
</tr>
<tr>
<td>1451561580</td>
<td>Co3TCY1CfTrkX6Xh</td>
<td>82.146.61.138</td>
<td>GET</td>
<td>in-adler.ru</td>
<td>/mime/蛉t/蛉nt/蛉nt/php &amp;?100=2&amp;99=14&amp;file=sleey32.dll</td>
<td><a href="http://in-adler.ru">http://in-adler.ru</a></td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J</th>
<th>K</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>1451561468</td>
<td>109.237.132.12</td>
</tr>
<tr>
<td>24</td>
<td>1451561470</td>
<td>172.16.72.243</td>
</tr>
<tr>
<td>25</td>
<td>1451561470</td>
<td>143.233.204.80</td>
</tr>
<tr>
<td>26</td>
<td>1451561470</td>
<td>143.233.204.80</td>
</tr>
<tr>
<td>27</td>
<td>1451561474</td>
<td>172.16.76.243</td>
</tr>
<tr>
<td>28</td>
<td>1451561474</td>
<td>82.146.61.136</td>
</tr>
<tr>
<td>29</td>
<td>1451561474</td>
<td>82.146.61.136</td>
</tr>
<tr>
<td>30</td>
<td>1451561475</td>
<td>211.119.245.213</td>
</tr>
<tr>
<td>31</td>
<td>1451561475</td>
<td>211.119.245.213</td>
</tr>
</tbody>
</table>
Conclusion

Threat intelligence is valuable due to the contextual data used to jumpstart an investigation and exponentially more valuable if deployed seamlessly!!

Threat intelligence platforms are a relatively “newer” technology used to centralize and man-handle information to maximize collaboration, context, and deployment.
Questions?

ryan.trost@threatq.com