My Bro The ELK

Obtaining Security Context from Security Events

Travis Smith
tsmith@tripwire.com
Agenda

- What is the problem?
- Who is the Bro?
- What is an ELK?
- Beefing up the ELK
- Making Your Bro the ELK Intelligent
- Visualization w/ Kibana
- Introducing the TARDIS framework
<table>
<thead>
<tr>
<th>INPUTS</th>
<th>FILTERS</th>
<th>OUTPUTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>TCP/UDP</td>
<td>ElasticSearch</td>
</tr>
<tr>
<td></td>
<td>STDIN</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>40+ More</td>
<td>Email</td>
</tr>
<tr>
<td></td>
<td>GROK</td>
<td>STDOUT</td>
</tr>
<tr>
<td></td>
<td>GEOIP</td>
<td>50+ More</td>
</tr>
<tr>
<td></td>
<td>TRANSLATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TRANSLATE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>30+ More</td>
<td></td>
</tr>
</tbody>
</table>
INPUTS
- FILE
- TCP/UDP
- STDIN
- 40+ More

FILTERS
- GROK
- GEOIP
- TRANSLATE
- TRANSLATE
- 30+ More

OUTPUTS
- ElasticSearch
- Syslog
- Email
- STDOUT
- 50+ More
SECURITY DATA > BIG DATA
### Threat Intelligence Made Easy

<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uceprotect.net IP Blacklist</td>
<td>Conservative</td>
<td>Contains a list of IP addresses to blacklist for security purposes.</td>
</tr>
<tr>
<td>uceprotect.net IP Blacklist</td>
<td>Backscatterer</td>
<td>Similar to Conservative, but with a different focus on specific threats.</td>
</tr>
<tr>
<td>hosts-file.net Malware Domains</td>
<td></td>
<td>Tracks domains known to be associated with malware attacks.</td>
</tr>
<tr>
<td>PhishTank Intel Feed (Verified)</td>
<td></td>
<td>A validated list of phishing domains to help in the fight against phishing.</td>
</tr>
<tr>
<td>hosts-file.net Phishing Domains</td>
<td></td>
<td>Identifies domains used for phishing attacks.</td>
</tr>
<tr>
<td>blocklist.de IP Blocklist</td>
<td></td>
<td>Provides a list of IP addresses to blacklist.</td>
</tr>
<tr>
<td>hosts-file.net Fraud Domains</td>
<td></td>
<td>Monitors domains involved in fraudulent activities.</td>
</tr>
<tr>
<td>hosts-file.net Exploit Domains</td>
<td></td>
<td>Tracks domains used in exploiting vulnerabilities.</td>
</tr>
<tr>
<td>hosts-file.net Ad/Tracking Domains</td>
<td></td>
<td>Identifies domains used for advertising and tracking purposes.</td>
</tr>
<tr>
<td>sysctl.org Domain Blocklist (Ads)</td>
<td></td>
<td>Helps in blocking domains related to ads and tracking.</td>
</tr>
<tr>
<td>binarydefense.com IP Banlist</td>
<td></td>
<td>Bans IP addresses associated with malicious activity.</td>
</tr>
</tbody>
</table>

Each service provides a count of entries and a rating system to indicate the severity and reliability of the threats.
# Critical Stack Agent

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>LAST UPDATED</th>
<th>INDICATOR COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mastm-RotNet-(Master-Feed)</td>
<td>04/03/15-10:23:01-am</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>USLE-IP-List</td>
<td>04/18/15-06:38:01-am</td>
<td>124</td>
</tr>
<tr>
<td>3</td>
<td>CryptoGuard-(Master-Feed)</td>
<td>04/14/15-03:18:01-pm</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>Root-Tracker-Drop-Zones-(Master-Feed)</td>
<td>03/26/15-02:12:01-pm</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>TinyTracker-/Tinno-(Master-Feed)</td>
<td>03/26/15-02:12:01-pm</td>
<td>132</td>
</tr>
<tr>
<td>6</td>
<td>PushDo-Malware-(Master-Feed)</td>
<td>03/29/15-02:12:01-pm</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>Known-Tor-Exit-Nodes</td>
<td>04/16/15-11:16:01-am</td>
<td>5567</td>
</tr>
<tr>
<td>8</td>
<td>iCyber-Urine-Tracker</td>
<td>04/17/15-02:38:01-pm</td>
<td>3163</td>
</tr>
<tr>
<td>9</td>
<td>Zeus-Tracker-Confite</td>
<td>03/26/15-02:14:01-pm</td>
<td>58</td>
</tr>
<tr>
<td>10</td>
<td>Zeus-Tracker-Drop-Zones</td>
<td>03/26/15-02:14:01-pm</td>
<td>24</td>
</tr>
<tr>
<td>11</td>
<td>Zeus-Tracker-Binkies</td>
<td>04/16/15-11:35:01-am</td>
<td>59</td>
</tr>
<tr>
<td>12</td>
<td>SSL-Blacklist-(SSL)</td>
<td>03/26/15-02:12:01-pm</td>
<td>541</td>
</tr>
<tr>
<td>13</td>
<td>Pakcrol-Domain-Block-List</td>
<td>04/07/15-11:30:01-am</td>
<td>45</td>
</tr>
<tr>
<td>14</td>
<td>Pakcrol-IP-Block-List</td>
<td>03/20/15-02:13:01-pm</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>Zeus-Tracker-Domain-Block-List</td>
<td>03/30/15-01:23:01-pm</td>
<td>509</td>
</tr>
<tr>
<td>16</td>
<td>SpyEye-IP-Black-List</td>
<td>02/19/15-01:24:01-pm</td>
<td>5</td>
</tr>
<tr>
<td>17</td>
<td>SpyEye-Domain-Black-List</td>
<td>02/18/15-03:57:01-am</td>
<td>127</td>
</tr>
<tr>
<td>18</td>
<td>WinRaid-Intel-Feed-(Verified)</td>
<td>04/16/15-04:57:01-am</td>
<td>2733</td>
</tr>
<tr>
<td>19</td>
<td>Abuse-Reporting-and-Blacklisting</td>
<td>04/16/15-11:27:01-am</td>
<td>7666</td>
</tr>
<tr>
<td>20</td>
<td>UShield-Domain-List-(Low-Sav)</td>
<td>03/26/15-02:12:01-pm</td>
<td>400</td>
</tr>
<tr>
<td>21</td>
<td>UShield-Domain-List-(High-Sav)</td>
<td>04/17/15-01:17:01-pm</td>
<td>4039</td>
</tr>
<tr>
<td>22</td>
<td>UShield-Domain-List-(Medium-Sav)</td>
<td>03/26/15-02:12:01-pm</td>
<td>1221</td>
</tr>
<tr>
<td>23</td>
<td>Malware-Update</td>
<td>04/17/15-01:16:01-am</td>
<td>11659</td>
</tr>
<tr>
<td>24</td>
<td>Scam-Doamins-(Fake/Malware/Or ya-Ry)</td>
<td>04/16/15-11:27:01-am</td>
<td>4653</td>
</tr>
<tr>
<td>25</td>
<td>ET-Known-Compromised-Hosts</td>
<td>04/16/15-03:28:01-am</td>
<td>1888</td>
</tr>
<tr>
<td>26</td>
<td>USLE-Domain</td>
<td>04/15/15-08:38:01-am</td>
<td>473</td>
</tr>
<tr>
<td>27</td>
<td>IP-Bad-Suspction-(Mail)</td>
<td>04/14/15-06:42:01-pm</td>
<td>101</td>
</tr>
<tr>
<td>28</td>
<td>IP-Bad-Suspction-(HTTP/HTTPS)</td>
<td>03/25/15-04:19:01-pm</td>
<td>57</td>
</tr>
<tr>
<td>29</td>
<td>IP-Bad-Suspction-(Scan)</td>
<td>04/01/15-04:34:01-pm</td>
<td>412</td>
</tr>
<tr>
<td>30</td>
<td>Parnovics-Malware-Doamins</td>
<td>03/26/15-02:12:01-pm</td>
<td>12</td>
</tr>
<tr>
<td>31</td>
<td>Parnovics-Malware-IPs</td>
<td>03/26/15-02:12:01-pm</td>
<td>31</td>
</tr>
<tr>
<td>32</td>
<td>Parnovics-Boxnet-IPs</td>
<td>04/15/15-03:57:01-pm</td>
<td>6</td>
</tr>
<tr>
<td>33</td>
<td>FTA-Suspicous-(dnsdomain-(All))</td>
<td>03/17/15-07:43:01-am</td>
<td>129</td>
</tr>
<tr>
<td>34</td>
<td>Beeloh-Doamin List</td>
<td>03/22/15-09:32:01-am</td>
<td>7</td>
</tr>
<tr>
<td>35</td>
<td>Beeloh-Doamin List</td>
<td>03/26/15-02:12:01-pm</td>
<td>17</td>
</tr>
</tbody>
</table>

# 800,000+ Indicators

98 Threat Feeds
Logstash Filtering

• Utilizing Custom Patterns
• GROK Message Filtering
• Adding Custom Fields
• Adding Geo IP Data
• Date Match
• Using Translations for Threat Intel
Logstash Configuration

```ruby
filter {
  grok {
    match => {
      "message" => "${IP:client} ${WORD:method} ${URIPATHPARAM:request} ${NUMBER:bytes} ${NUMBER:duration}"
    }
  }
}
```
Utilize Custom Patterns

```ruby
filter {
  grok {
    patterns_dir => "/opt/logstash/custom_patterns"
    match => {
      message => "\{291001\}"
    }
  }
}

/opt/logstash/custom_patterns/bro.rule
291001 (\<start_time>\d{10}\d{6}\t\<evt_srcip>\d+.\+\t\<evt_dstip>\d+.\+\t\<evt_srcport>\d+\t..."
Message Filtering

```
filter {
  if [message] =~ /^((\d{10}\.\d{6})\t([\d.]+)([\d.]+)\t([\d.]+)\t([\d.]+)\t([\w.]+))/ {
    grok {
      patterns_dir => "/opt/logstash/custom_patterns"
      match => {
        message => "\{291001\}"
      }
    }
  }
}
```
Add Custom Fields

filter {
  if [message] =~ /\d{10}\d{6}\d{10}\d{6}\d{10}\d{6}\w+/ {
    grok {
      patterns_dir => "/opt/logstash/custom_patterns"
      match => {
        message => "%{291001}"
      }
      add_field => [ "rule_id", "291001" ]
      add_field => [ "Device Type", "IPSIDSDevice" ]
      add_field => [ "Object", "NetworkTraffic" ]
      add_field => [ "Action", "General" ]
      add_field => [ "Status", "Informational" ]
    }
  }
}
}
Geo IP

filter {
.....all normalization code above here....

geoip {
    source => "evt_dstip"
    target => "geoip_dst"

database => "/etc/logstash/conf.d/GeoLiteCity.dat"

add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][longitude]}" ]
add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][latitude]}" ]
add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][city\_name]}" ]
add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][continent\_code]}" ]
add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][country\_name]}" ]
add_field => [ "[geoip_dst][coordinates]", "%{[geoip_dst][postal\_code]}" ]

mutate {
    convert => [ "[geoip_dst][coordinates]", "float" ]
}
}
GeoIP Template Update

curl -XGET localhost:9200/_template/logstash
{"logstash":{
   "order":0,
   "template":"logstash-*",
   "settings":{
       "index.refresh_interval":"5s"
   },
   "mappings":{
       "properties":{
           "geoip":{
               "dynamic":true,
               "properties":{
                   "location":{
                       "type":"geo_point"
                   }
               },
               "type":"object"
           },
           "type":"object"
       }
   }
}

curl -XPUT localhost:9200/_template/logstash -d ‘....’
Date Match

filter {
    ....all normalization code above here....
    ....all GeoIP code here....
    date {
        match => [ "start_time", "UNIX" ]
    }
}
filter {
    ....all normalization code above here....
    ....all GeoIP code here....
    translate {
        field => "evt_dstip"
        destination => "tor_exit_IP"
        dictionary_path => '/etc/logstash/conf.d/torexit.yaml'
    }
}

- Run Scripts to update the YAML files on a regular basis
- Logstash will check the YAML for updates every 300 seconds
  - Configurable by adding refresh_interval => numSeconds
Custom Fields:

- "Device Type" => "IPSIDSDevice"
- "Object" => "HTTP"
- "Action" => "General"
- "Status" => "Informational"

Threat Intel Translations:

- "tor_exit_IP" => "YES"
- "malicious_IP" => "YES"

Geo IP Data:

- "country_code2" => "RU"
- "country_code3" => "RUS"
- "country_name" => "Russian Federation"
- "continent_code" => "EU"
- "city_name" => "Moscow"
- "postal_code" => "121087"
- "latitude" => 55.75219999999999
- "longitude" => 37.6156
- "timezone" => "Europe/Moscow"
The TARDIS Framework

- Threat Analysis, Reconnaissance, & Data Intelligence System
- Historical exploit/IOC detection
- Time Lord of forensic log data
- Available at [https://github.com/tripwire/tardis](https://github.com/tripwire/tardis)
- Demo at Arsenal Thursday @ 12:45
TARDIS

Import

Search

10.10.10.10 - [06/Aug/2015:05:38:38] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - [06/Aug/2015:05:39:39] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - [06/Aug/2015:05:40:40] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - [06/Aug/2015:05:41:41] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - [06/Aug/2015:05:42:42] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
10.10.10.10 - [06/Aug/2015:05:43:43] "GET /cgi-bin/test.cgi HTTP/1.1 200 525 """" [ text; ]echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd"
Sound Bytes

- Use NSM With Log
- Security Tools Are Better With Intelligence
- Take Integrations to the Next Level With TARDIS
Thank You

Travis Smith
tsmith@tripwire.com

https://github.com/Tripwire/tardis
https://github.com/TravisFSmith/MyBroElk