Practical Cyber Threat Intelligence
Who Am I?

• Olivia Lomax – Junior in CS @ Mines
  • Cyber Threat Intelligence Intern @ Kaiser Permanente (8 mo.)
  • Participated in 2020 CCDC Qualifier
  • SANS Team Based Training Participant
What is Cyber Threat Intelligence? (CTI)

• Cyber Threat Intelligence is information that has been collected and analyzed by an organization to understand a threat actor’s motives, desires, tactics techniques and procedures (TTPs).

• CTI is very helpful when deciding how to defend your organization more efficiently.

• Nobody is ever fully protected 100% of the time. So, we must decide what TTPs are most important to defend against.
  • The data that is analyzed helps organizations decide whether it is more important to alert and detect different types of compromise. Whether that be data exfiltration, phishing, ransomware, etc.
How is Intel Collected & Used?

• Closed Source Intelligence
• Discovered/Internal Intelligence
• Open Source Intelligence
Closed Source Intelligence

• ISAC (Information Sharing and Analysis Center)
  • Member driven organizations that deliver physical and cyber threat information to help mitigate and assess potential threats to businesses and organizations

• Connections!
  • Gray Hat hackers

• Dark Web Forums / Marketplaces
Why is Closed Source Intel Important?

- Traffic Light Protocol (TLP)
  - TLP Red – Not for disclosure, restricted to participants only
  - TLP Amber – Limited disclosure, restricted to participants’ orgs
  - TLP Green – Limited disclosure, limited to the community
  - TLP White – Disclosure not limited
- Organization targeted intel
- Helpful for organizations with less mature Cyber Defense Programs
- Can sometimes be considered “snake oil”
Discovering Intel

• There is a wealth of information in your own network.
• Many organizations are compromised in some manner.
• When compromise is found the first step is to gather intel!
  • Take samples, find command and control servers, grab hashes
  • These samples will be the beginning of creating shareable intelligence

• Helpful Tools and Techniques:
  • Splunk
  • Reverse Engineering
  • VirusTotal
SIEMs

• Splunk, Graylog, etc.
• SIEM stands for Security Information and Event Management
• SIEMs let you throw tons of logs at them and allow you to correlate behavior you are seeing on your own network together
# Twistlock Incidents and Forensics

## Total Incidents in the last 7 days

<table>
<thead>
<tr>
<th>Image</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>infoslack/dwa:latest</td>
<td>5</td>
</tr>
<tr>
<td>registry-auth.twistlock.com/tw_crrwvcfeintl1v4e@yrzjks2mezah79/theconsole_19_83_317</td>
<td>24</td>
</tr>
<tr>
<td>serveethome/monero_cpu_minergate:latest</td>
<td>1</td>
</tr>
<tr>
<td>tl_demo/struts2_demo:2.3.12_build</td>
<td>1</td>
</tr>
<tr>
<td>ubuntu:16.04</td>
<td>1</td>
</tr>
</tbody>
</table>

## Total incidents in the last 30 days

<table>
<thead>
<tr>
<th>Host</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>demo-jeremy-p-twistlock-com</td>
<td>38</td>
</tr>
<tr>
<td>gke-jeremy-gke-remote-default-pool-7bd7c8d8f-dxnk</td>
<td>7</td>
</tr>
<tr>
<td>gke-jeremy-gke-remote-default-pool-7bd7c8d8f-f2gm9</td>
<td>7</td>
</tr>
<tr>
<td>demo-node-jeremy-p-twistlock-com</td>
<td>3</td>
</tr>
<tr>
<td>gke-jeremy-gke-docs-remote-default-pool-7f639b44-crmn</td>
<td>1</td>
</tr>
</tbody>
</table>

## Top 5 incident-prone images

- **cryptoMiner**
  - Host: demo-jeremy-p-twistlock-com

- **portScanning**
  - Host: demo-jeremy-p-twistlock-com

- **dataExfiltration**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

- **hijackedProcess**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

- **weakSettings**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

## Top 5 incident-prone hosts

- **cryptoMiner**
  - Host: demo-jeremy-p-twistlock-com

- **portScanning**
  - Host: demo-jeremy-p-twistlock-com

- **dataExfiltration**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

- **hijackedProcess**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

- **weakSettings**
  - Host: demo-jeremy-p-twistlock-com
  - Time: 2019-04-25T17:09:03Z

## Container incident details

<table>
<thead>
<tr>
<th>Time</th>
<th>Category</th>
<th>Host</th>
<th>Image</th>
<th>Container</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-04-25T18:20:48Z</td>
<td>cryptoMiner</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>serveethome/monero_cpu_minergate:latest</td>
<td>/nifty_volhard</td>
<td>5cc3599c8b7c9f72858b3b2e2</td>
</tr>
<tr>
<td>2019-04-25T18:21:12Z</td>
<td>portScanning</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>tl_demo/struts2_demo:2.3.12_build</td>
<td>/k8s.struts2server/struts2server-5769d498-d4ksx_struts-demo_ebb62577-6568-11e9-9733-42819a880002</td>
<td>5cc3599c8b7c9f72858b3b2e2</td>
</tr>
<tr>
<td>2019-04-25T17:09:03Z</td>
<td>dataExfiltration</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>tl_demo/struts2_demo:2.3.12_build</td>
<td>/k8s.struts2server/struts2server-5769d498-d4ksx_struts-demo_ebb62577-6568-11e9-9733-42819a880002</td>
<td>5cc3599c8b7c9f72858b3b2e2</td>
</tr>
<tr>
<td>2019-04-25T17:09:03Z</td>
<td>hijackedProcess</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>tl_demo/struts2_demo:2.3.12_build</td>
<td>/k8s.struts2server/struts2server-5769d498-d4ksx_struts-demo_ebb62577-6568-11e9-9733-42819a880002</td>
<td>5cc3599c8b7c9f72858b3b2e2</td>
</tr>
<tr>
<td>2019-04-25T17:09:03Z</td>
<td>weakSettings</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>infoslack/dwa:latest</td>
<td>/dwa</td>
<td>5cc4763a1875c/751932466aa</td>
</tr>
<tr>
<td>2019-04-25T17:09:03Z</td>
<td>weakSettings</td>
<td>demo-jeremy-p-twistlock-com</td>
<td>infoslack/dwa:latest</td>
<td>/dwa</td>
<td>5cc66991a875c/751932466aa</td>
</tr>
</tbody>
</table>
Reverse Engineering

• app.any.run is my favorite free sandbox
• You can also detonate in your own virtual machine and do packet capture analysis if you are very skilled in figuring out malware signatures and behaviors
PIVOT!

• Pivoting is taking found information and using it to “pivot” to extract more information to discover possible related malware or campaigns

• VirusTotal
Open Source Intelligence

- DNS records
- Social Media
- Github
- Public Records
GitGot Demo
Putting it All Together

• The power of cyber threat intelligence comes from collecting and analyzing information about indicators of past, current and future cyber threats, which enables an organization to take action to protect their assets, network and the entire organization

• Taking the various sources of intelligence we receive and discover ourselves lets us easily identify and attribute different attacks on our organization
Questions?

But pls don’t. It makes my job harder….