THREAT HUNTING: FROM PLATITUDES TO PRACTICAL APPLICATION

Neil “Grifter” Wyler
NEW PRESENTATION, WHO DIS?

SecTor 2018

@grifter801
What is it?

- Proactively searching through data in order to detect threats which have evaded traditional security measures.

Is it effective?

- It's often more effective than working incidents out of a queue. While traditional security programs are still important, hunting takes you to the next level.
Why hunt?

- Again, because it’s proactive.
  - Aren’t you tired of being purely reactive?

- It’s much harder to hide when someone is actively looking for you.

- It’s much harder to hide when someone knows their environment.

- By the way, you’ll know your environment better than you ever have before.

- It increases value to your organization.
WHERE DO WE BEGIN?

Log All the Things

- Collect logs from key areas
  - OS Event Logs
  - Application Logs
  - Know who is authenticating where, and at what level

- Don’t forget your network
  - Web Server logs
  - Proxy logs
  - Full … Packet … Capture

This can be an incredible amount of data

- Big Data is a part of your life now
  - Start small and grow your collection as you grow your program

SecTor 2018  @grifter801
WHERE DO WE BEGIN?

Situational Awareness

❑ Understand what normal looks like on your hosts and network.
  – Create a baseline that you can diff against

❑ Become intimately aware of what the norms are so that when an anomaly occurs, it sticks out like a sore thumb.

Leave preconceived notions at the door

❑ Don’t always start with an IOC. Start with a question.
  – If data was leaving my environment, where’s the most likely place it would leave?
HUNTING

Hosts

- Know which processes are running on your systems.
  - Process Names
  - Path to Executables
  - Parent Processes

- Look for process injection, hooking, and artifacts in shimcache.

Persistence

- Look beyond Run keys
- What Scheduled Tasks are configured on the system?
- Are there services that you didn’t create?
  - Typos or blank descriptions
  - Binary Path is not normal

SecTor 2018

@grifter801
Network

- What are your ingress and egress points?
  - Have they changed?
- Direct to IP Communication
- Communication to services using Dynamic DNS
- Tor traffic
- IRC traffic
- Look at HTTP traffic
  - POST activity with no referrer
  - User-Agent strings can be a red flag
- Traffic over non-standard ports

SecTor 2018  @grifter801
HUNTING MINDSET

Have a plan but be ready to adapt

- Know what you’re looking for and go try to find it.
  - But don’t be discouraged if/when you don’t

- Remain flexible
  - Sometimes what you started searching for will take you down a completely different path.

- Prepare for pivots, there will be many

- Find tools that help you make sense of the data you’ve collected

- Document everything you’re doing and what you’ve learned
  - Share it!
SO, WHAT NOW?
EXECUTING A HUNT

The Plan

❑ Provide Hunters \w Network Architecture / Diagrams

❑ Identify Potential Targets
  ❑ Tie IP Addresses to Assets
  ❑ Business Criticality

❑ Focus on Directionality
  ❑ Inbound
  ❑ Outbound
  ❑ Lateral Movement

❑ Determine Hunting Timeframe
  ❑ 24 hours on Average
  ❑ Expand timeframe for subjects/events of interest
EXECUTING A HUNT

- Service Analysis
  - Begin with the Smallest (IRC, VNC, BITTORRENT, RPC, RDP)
    - Allows for Quick Elimination
    - Continue to Work Backwards
    - Document Area that Each Analyst Covered (Analyst 1 – Outbound/RDP, Outbound/IRC, etc)

- Drill Down on Each Selected Service
  - Indicators of Compromise
  - Behaviors of Compromise
  - Enablers of Compromise

- Rinse and Repeat
EXECUTING A HUNT

Care and Feeding

- Investigate, Investigate, Eliminate

- Find the Signal in the Noise
  - Determine what traffic is causing false positives, and manage it.
  - As you tune and dial in your environment, actionable data will become increasingly apparent.

- Build reports and automate the pain away
SO, WHAT DO WE FIND?
CLEARTEXT OR ENCRYPTED?

- Percentage of traffic encrypted – NO decryption
Clear txt passwords going across the wire. Many are very complex, but this offers little protection if intercepted.
CLEARTEXT OR ENCRYPTED?

- Webcams
ALWAYS USE A VPN!

I DON'T ALWAYS TELL MY SECRETS,

BUT WHEN I DO, IT'S NOT VERY SECRETIVE.
THE RSAC DATING POOL

Harry, 17

About Harry:
Ginger fever. Very Famous. Must be into scars.

Mashable

SecTor 2018 @grifter801
ALL THINGS ARE NOT CONFIGURED EQUALLY
### Top 10 Websites / Concentrator

<table>
<thead>
<tr>
<th>Hostname Aliases</th>
<th>Total session size in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. au.download.windowsupdate.com</td>
<td>143.39 GB</td>
</tr>
<tr>
<td>2. au.b1.download.windowsupdate.com</td>
<td>79.81 GB</td>
</tr>
<tr>
<td>3. 2.tlu.dl.delivery.np.microsoft.com</td>
<td>77.75 GB</td>
</tr>
<tr>
<td>4. archive-2.kali.org</td>
<td>77.42 GB</td>
</tr>
<tr>
<td>5. download.windowsupdate.com</td>
<td>62.87 GB</td>
</tr>
<tr>
<td>6. iosapps.itunes.apple.com</td>
<td>57.03 GB</td>
</tr>
<tr>
<td>7. 3.tlu.dl.delivery.np.microsoft.com</td>
<td>46.54 GB</td>
</tr>
<tr>
<td>8. 7.tlu.dl.delivery.np.microsoft.com</td>
<td>44.52 GB</td>
</tr>
<tr>
<td>9. us.archiveubuntu.com</td>
<td>35.49 GB</td>
</tr>
<tr>
<td>10. officecdn.microsoft.com</td>
<td>25.15 GB</td>
</tr>
</tbody>
</table>
ZERO DAY, O-DAY OR SAME DAY?

BUSTED
Event Reconstruction

<table>
<thead>
<tr>
<th>Service</th>
<th>ID</th>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>First Packet Time</th>
</tr>
</thead>
</table>

Request & Response | Top To Bottom | View Text | Actions | Open Event In New Tab | Cancel |

**Request**

```
WHO #stufffedninja
```

**Response**

```
:tepper.freemode.net 352 LAM #stufffedninja -math seto upatiated/slatos tepper.freemode.net 352 H MG i0 New Nav Know Now
:tepper.freemode.net 352 LAM #stufffedninja -s7onghos pdkr/supportor/active/s7onghos7 sendok.freemode.net s7onghos7 H MG i0 s7onghos7
:tepper.freemode.net 352 LAM #stufffedninja 4242661 gateway/web/Freemode/1p.66.75.38.17 harbert.freemode.net pacificfrogturtle H MG i0 rpm.66.75.38.17 am.ress.run.com/66.75.36.17
:tepper.freemode.net 352 LAM #stufffedninja Chantary services. services. Chantary MG i0 Channel Services
:tepper.freemode.net 351 LAM #stufffedninja :End of /WHO list.
```

**Request**

```
PING :ALIVECHECK
```

**Response**

```
PONG :ALIVECHECK
```

**Request**

```
PRIMSG #stufffedninja :s7onghos7: do you still have that RF pager script?
PRIMSG #stufffedninja :routurer has a HackRF now as well
PRIMSG #stufffedninja :I'm thinking it might be worth trying it out at the luxor
```

14 packets loaded from cache | Show Reconstruction Log

---

SecTor 2018 @grifter801
“DEVICES”
Thanks

Neil “Grifter” Wyler
@grifter801