The Most Dangerous Game
Hunting Adversaries Across the Internet
Scott J Roberts
ADVANCED PERSISTENT INCIDENT RESPONDER
@ GITHUB
How Kyle met Scott

or

How Scott met Kyle
If you are on the Twitter we’re @kylemaxwell & @sroberts #YOLOTHREAT
Intelligence Concepts

That everyone knows and already agrees on right...?
<table>
<thead>
<tr>
<th>Data</th>
<th>Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is a raw piece of information without context.</td>
<td>Intelligence has gone through the intelligence process.</td>
</tr>
</tbody>
</table>
Intelligence Cycle

Requirements

Feedback

Collection

Dissemination

Processing

Analysis
The Target
What is Targeting?

Making a plan for focusing threat research & investigation
Targeting Methodologies

Actor Centric

Target Centric

Technology Centric
Feeds

needles in haystacks
“MY 5.4 GAZILLION INDICATORS CAN BEAT UP YOUR THREAT INDICATORS. GARBAGE IN GARBAGE OUT #THREATINTEL”

~ RICK HOLLAND
Honeypots

BRINGING THE BAD GUYS TO YOU
## Low vs High Interaction

<table>
<thead>
<tr>
<th>Low Interaction</th>
<th>High Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeypots are an easy way to get low value intel on commodity threats</td>
<td>Honeypots are a risky &amp; complicated way to generate high quality intelligence</td>
</tr>
</tbody>
</table>
Software

**Old School:**
Honeynet Project

**New Hotness:**
Modern Honey Network
By Threat Stream
Vulnerability Information

Taking Care of Your Toys
“Structured vulnerability analysis is not threat intelligence. It is requirements gathering for threat intelligence.”

~ @SELIL
Personal Aside to Vendors

If you’re going to release a report, blog post, etc:

Do not break the Cut and Copy Actions
SHHH. MY COMMON SENSE IS TINGLING.
Review Your Own Incidents

Mine That Fancy Incident Management System...
Review Your Others Incidents

By sharing or news mining
What to Analyze

Technical Sources
What to Analyze: Hashes

Sources:
- VXShare
- VirusTotal
- Malwr.com

Reversing:
- C2 Info
- Developer Artifacts
What to Analyze: Passive DNS

- Single most useful tool for infrastructure research
- What resolved to what, and when?
- DNSDB (Farsight), PassiveTotal, VirusTotal
What to Analyze: Whois

- Tougher to Acquire
- Whodat Etc for Ongoing Tracking
What to Analyze

Actors
What to Analyze: Criminal

- PRIMARY WEAPON: GOOGLE
- SOCIAL MEDIA (TWITTER, FACEBOOK)
- UNDERGROUND FORUMS?
What to Analyze: Espionage

- This is hard
- Malware & System Artifacts
- Whois/Registrar Data
- Actions over Target
How to Keep Tracking
Threat Library

- CRITS is popular, MISP also
- Lighter solutions often work
- Market hasn't fully addressed this
Web Monitoring Systems

- Netflix Scumblr Meta Search
  (Works alongside Sketchy)
- Recorded Future
- Lots of custom development
Malware Monitoring

- **Virustotal is 👑
- Malware feeds with lots of custom internal solutions
- Maltrieve, Viper, & Cuckoo
Internal Logging

- Firewall, IDS, & Proxy
- Web, Mail, & DNS
- Authentication & Audit
The “Kill”
Incident Response

The entire goal... right?
The Imitation Game

Don’t let them know that you know that they know...
Attribution

Probably doesn't matter unless you can do this
Hand Cuffs or Cruise Missiles
KICK ‘EM OUT NOW!

SOMETIMES IT’S BETTER TO WATCH FOR A WHILE
Intel Driven Responses

DENY
DECEIVE
DEGRADE
DISRUPT
DESTROY
**Communication**

**Who can make use of this information?**

~

**Who might be able to provide additional intel?**
The Hunting Stories
Products

IOCS & RFIS

SHORT FORM PRODUCTS

LONG FORM PRODUCTS
Audience

Internal - Team
Internal - Organization
External - Peers
External - Wide
IOCs - Generalized

STIX & OPENIOC

same
"YOU PRETTY MUCH NEED A PHD IN XML TO UNDERSTAND EITHER STIX OR TAXII"

~ JEFF BRYNER
HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

**SITUATION:**
THERE ARE 14 COMPETING STANDARDS.

**14?! RIDICULOUS!**
WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.

**YEAH!**

**SOON:**

**SITUATION:**
THERE ARE 15 COMPETING STANDARDS.
IOCs - Specialized

**SNORT:**
Go to for network activity, comprehensive and well supported

**YARA:**
Malware centric AV signature style IOCS, getting more advanced
“OH: “YARA IS AN ANTIVIRUS THAT YOU UPDATE USING GIT PULL”

~ @TOMCHOP_
Requests For Intelligence

A Q/A requesting very specific intelligence

~

Shortest form possible

~

Fastest turn around
Short Form Products

Intermediate Products to Support Incident Response

Focus on Actionable Information
Comprehensive “All Source” Intelligence Products

Requires Considerable Time & A Well Rounded Team
The Surprise...
You Can’t Download a Threat Intelligence

Until now....
The Surprise

Coming out of stealth today, our new startup...

YoloThre.at
Announcement

YOLOTHTRE.AT HAS RUN OUT OF RUNWAY (WE USED UP OUR WHOLE STARBUCKS GIFT CARD)
SO WE’RE OPEN SOURCING EVERYTHING AND GOING BACK TO OUR OLD JOBS...
A COLLECTION OF OPEN SOURCE DOCKER CONTAINERS FOR THREAT INTEL
<table>
<thead>
<tr>
<th>Maltrieve</th>
<th>Malware Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combine</td>
<td>Threat Feed Aggregator</td>
</tr>
<tr>
<td>Scumblr</td>
<td>Social Network Collection</td>
</tr>
<tr>
<td>CRITS</td>
<td>Intel Collection System</td>
</tr>
<tr>
<td>MISP</td>
<td>Malware Analysis Hub</td>
</tr>
<tr>
<td>ELK</td>
<td>Log Analysis</td>
</tr>
<tr>
<td>Viper</td>
<td>Malware Zoo System</td>
</tr>
<tr>
<td>Thug</td>
<td>Website Collection Tool</td>
</tr>
<tr>
<td>Yara</td>
<td>Malware Identification</td>
</tr>
</tbody>
</table>
Review

The Target
The Hunt
The "Kill"
The Hunting Stories
Questions?