CASTING A BIG NET: Hunting At Scale
BIO – Paul Jaramillo (@DFIR_Janitor)
• Principal Consultant, CrowdStrike
• Previously Fortune 10, Government, Energy, Manufacturing, and Telecommunications industries
• Enjoys *sleep*, family time, craft beer, bourbon, college football, and fighting nation state adversaries
BIO – Reed Pochron (@rpochron)

- Senior Consultant, CrowdStrike
- Previously Ernst & Young
- Crossfit Flounder
- #PCMasterRace
Agenda
• Hunting Essentials
• Our Approach
• Collections with CrowdResponse
• Rapid Analysis with Splunk
• Demo
• Key Takeaways / Q&A
HUNTING: WHAT IT IS NOT

• Not a new concept
• Not alert driven
• Not a tool or product
• Not standardized
• Not a silver bullet

What Sales thinks hunting is

Image Credit: hxxps://www.pinterest.com/monsterstein1/army-guns/
HUNTING: WHAT IT IS

- The Ultimate DFIR Question
- Proactive
- Component of Active Defense
- Assumption of Breach
- Exploring your Ignorance*
  - Select data sources
  - Baseline behaviors
  - Identify anomalies
  - Learn > Apply > Detect > Repeat

What CISOs think hunting is

Image Credit: hxxps://www.northropgrumman.com/
HUNTING: HOW ITS DONE

• Approaches
  • Objective Driven
  • Intelligence Driven
  • Anomaly Driven
• Frequency
  • Ad-hoc> Project-based> Continuous
• Data analysis techniques
  • Rare – Least Frequency of Occurrence
  • Variance - Standard Deviation
  • New – 1st seen on Network/Host
  • Sampling – Data not normally collected
  • Temporal – Timing oddities

What hunting really is
## HUNTING: WHO & WHY

### Strengths (Who)
- Incident Response
- Network Visibility
- Host Visibility
- Centralized Logging

### Weaknesses (Why)
- Prevention
- Early Detection
- Limited Experience
- Budget

### Opportunities (Why)
- Loss Avoidance
- Risk Assurance
- Improve Detection & Response
- Job Enrichment

### Threats (Why)
- Organized eCrime
- Malicious Insiders
- Hactivists
- Nation State Adversaries
HUNTING: OUTPUTS

- Report & Debrief
- Increased Security Assurance
- Increased Business Intelligence
- Actionable Monitoring & Detections
- Loss Avoidance
- Staff Training & Enrichment
# HUNTING: THREAT DETECTION FRAMEWORK

**Tackling your "Knowns"**

| Use Case Library |

**Tackling your "Unknowns"**

- **Brainstorm or Goal Creation**
- **Mission Planning**
- **Collection**
- **Analysis**
- **Debrief**

* Found Something? * New Use Cases

Alert

Hunt

* Stuff we will talk about today

---

TDF at DFIRSummit by Austin Murphy

SANS #ThreatHuntingSummit 2016 #NOLA
HUNTING: EXAMPLE HUNT

**Goal Creation**
- What data are you currently collecting?
- What data can you collect?
- How much data will be manageable?

**Mission Planning**
- How are you going to collect data?
- What tools are needed to collect?
- How much data will collection take?

**Collection**
- Rubber meets the road
- Putting my toolset from to use

**Analysis**
- Is my analysis environment operating?
- Is my data coming in a format I can analyze?

**Debrief**
- Findings?
- Lessons Learned?
- Can this be tuned and turned into an alert?

**Goal Creation**
- What programs have established persistence in my environment?

**Mission Planning**
- PSEXEC, CrowdResponse, and an open share

**Collection**
- CAB & XML collection
- Splunk ingestion of processed CSV

**Analysis**
- Splunk queries for least frequency
- Analyst knowledge of other indicators

**Debrief**
- 10 binaries to analyze and follow up on
- 200 machines with commodity infections

SANS #ThreatHuntingSummit 2016 #NOLA
MISSION PLANNING: COLLECTING WITH CROWDRESPONSE

Author
• Robin Keir

Components
• CrowdResponse.exe - Windows Console Application
• CRConvert.exe - Output Parser

Output
• XML -> CSV, TSV, HTML, Plain Text

CrowdResponse Deployment
• Targeted Command Line
• External Config

Deployment Options
• Psexec
  • see SANS Blog on protecting your privileged credentials (IPC$ auth)
• Powershell
  • https://github.com/n3l5/irCRpull
• GPO
• SCCM

Collection/Analysis Platform
• Splunk preferred

WARNING: CrowdStrike is not responsible for your use (or misuse) of the tools listed.
MISSION PLANNING: COLLECTING THE CROWDSTRIKE WAY

Our Lessons Learned:

• Frictionless deployment & collection
• Persistence vs Self Cleaning
• Establish a centralized intake server to receive files
• Intake server decompresses and converts data into Splunk accessible directory
• Large collections can create havoc, be prepared to adjust if needed
• Multiple indexes can separate hunts
• Scripts to handle duplicates
• IOPS reign supreme
• Temporary open share for ad-hoc collections
**Artifact Refresh:**

Filesystem Metadata about files

$MFT or FAT

MACE/MACB timestamps

**Example:**

Directory listing and all sub-directories looking for executables (exe)

```
@DirList "%windir%" -s -f *.exe
```
CROWDRESPONSE: REGISTRY

Artifact Refresh:
- Data files called “HIVES”
- Key and Value Pairs
- Multiple Hives for User/System

Windows Reg HIVES are a treasure trove of data
- UserAssist
- MRU
- ShimCache
- Services
- And much more!

@RegDump [-dstT] [-r <remote>] <reg key>
- d - Nested output format
- r <remote> - Connect to remote registry at [remote]
- s - Recursive dump
- T - Output additional wide character text version of binary data
- t - Output additional ASCII text version of binary data
<reg key> - Registry key to start dump from

@RegFile [-chmqrst] [-z <size>] <reg key>
- c - Verify and display digital signature information
- h - Do SHA256 hashes
- m - Do MD5 hashes
- q - Perform "quick" hash of only the 1st 512 bytes of the file
- r - Display application resource information
- s - Recursive dump
- t - Display file create, modified and accessed times
- z <size> - Don't hash files greater than this size in megabytes
<reg key> - Registry key to start dump from
Introducing: CrowdResponse Tasks

• Available after #ThreatHuntingSummit on www.crowdstrike.com/resources

New module to collect Windows Scheduled Tasks information

• Processes Task Scheduler 1.0 and 1.2 (vista+)
• Task name
• Application
• Parameters
• Working Directory
• And more!
Artifact Refresh:
Another persistence method and possibly privilege escalation leveraging the Windows Task Scheduler

Can be found in:
- C:\Windows\Tasks\ (XP - Windows Job Format)
- C:\Windows\System32\Tasks\ (Win7+ - XML)
- C:\Windows\SysWow64\Tasks\ (Win7+ - XML)

C: \> schtasks
C: \> at

...yes that’s it
The new CrowdResponse also features updates to your favorite modules!

- @Mal now includes option to detect DLL Hijacking
  - Checks for DLL name conflicts found in $PATH
  - Checks for DLL name conflicts NOT found in $PATH
  - Checks svchost.exe processes for same DLL name loaded in different path
- Additional bug fixes and improved processing with CRConvert

WARNING: errors can occur if using old CRConvert to parse new collections
Collection is mostly solved...but some problems remain

- Unsupported Operating System (*NIX, OS X, iOS, Android, ChromeOS, etc)
- Offline hosts
- Network bandwidth (Memory, Disk Images, etc)
- Legal (EU, Works Councils, etc)

Establishing a reliable analysis platform is a much bigger challenge initially

- Easy to scale
- Fast, repeatable searches
- Automatic data ingestion
- Automatic field parsing
- Easy data manipulation and statistical functions
- Timelining
Splunk vs ELK vs Other
• Not traditional SIEM-like data ingestion
• Live Response Centric

Splunk applications
• Versioning - 6.x
• Advanced XML or HTML, CSS, Javascript

Application goals
• Faster searching
• Repeatable workflow
• Easy Pivoting
ANALYSIS: RAPID ANALYSIS W/ SPLUNK

Module-based hunting
ANALYSIS: RAPID ANALYSIS W/ SPLUNK

Methodology-based hunting
ANALYSIS:
RAPID ANALYSIS W/ SPLUNK

Indicator Management Lite
DEMO:
HUNTING W/ CROWDRESPONSE
Let's recap what we observed:

• Indicator hits for DEEPPANDA SAKULA malware and credential dumper
• Persistence for a netcat listener
• ”At” Scheduled Tasks for a batch file
• Sticky keys debugger set to cmd.exe for the On-Screen Keyboard (osk.exe)
• ShimCache evidence of possible reconnaissance and exfiltration preparation

Not client data but all TTPs seen in CrowdStrike IRs
HUNTING: KEY TAKEAWAYS

PLAN
Business & Threat Aligned Use Cases

Gain approval, organize resources, and EXECUTE

DELIVER tangible outputs to stakeholders

PROFIT from increased Security Assurance and Loss Avoidance

SANS #ThreatHuntingSummit 2016 #NOLA
QUESTIONS?
Possibly Answers