U Mad Bro?

Enfranchising Your Analysts Using Bro

Jason Batchelor
Intelligence & Response
dbatchelor@emerson.com

Dan Nieters
Enablement
dnieters@emerson.com
Outline

- Maturity
  - Philosophy
  - Strategic direction

- Current Implementation
  - High level overview
  - Traffic taxonomy
  - Challenges

- Extending Bro
  - Custom sauce
  - Integration
  - Future state
Maturity
Paradigm Shift

Old School

New School

Capabilities Analysis

Analysis Capabilities
Path to Custom Solutions...

- Best in class COTS capabilities
  - Capabilities team had adopted were ‘black box’ solutions
  - Not as extendable as we’d like
  - Gaps in capabilities identified, desire to innovate past them
  - Alerting and detections not shared, creating confusion

- Seeking validation
  - Are we really seeing traffic we expect?
  - What other data points can I pivot on?
  - I noticed something interesting about this attack, can I add a custom signature?

- Sitting in the drivers seat... forging understanding and continuity
  - Engage infrastructure team, hash out a tapping infrastructure that makes sense
    - Lots of learning on both sides
      - “That's not supposed to work that way?”
    - Establish a common language and overview of what we want and how it looks
      - Create and apply a template to our major internet points of presence
    - Building relationships with other organizations
      - It’s not always technical!
Current Implementation
Custom sensor and file scanning platform made by, for, and maintained by Emerson incident response analysts

Hardware: Dell PowerEdge R720
- Intel XEON E5-2670, 32 cores @ 2.60GHz, 128G RAM, 24TB SAS storage @ RAID10
- 1 x 1Gb Management interface, 1 x 10Gb Tapping interface

Minimal CentOS 6.5 for OS baseline

Bro v2.4 as the network analysis framework
- 1 manager, 2 proxies, 8 worker members per proxy
- Currently set to generate all common logs

PF RING v6 for software-based load balancing

Custom built client module for file scanning and disposition
- Files matching specified MIME types are sent off for heavy lifting to separate hardware file scanners
4 major hubs worldwide, with one or more sensors

Each sensor is assigned a 10Gb tap port on a local Gigamon appliance
- Gigamons are network visibility tools in their own right
- Used to replicate and send off flow data from certain places on the network

Sensor types
- **Internal CIRT Sensor (ICS):** Monitors bidirectional traffic inside Emerson's managed IP space
- **External CIRT Sensor (ECS):** Monitors bidirectional traffic outside Emerson's managed IP space
- **Hybrid CIRT Sensor (HCS):** Monitors both types
- **File Scanning Framework (FSF):** Receives certain file types from regional sensor to scan
Software & Scalability: Challenges & Solutions

- So why the large amount of packet discards?
  - 10-12% per hour drop rate peak
  - Plenty of bandwidth overhead (2.2Gbps on 10Gb)
  - Number of concurrent connections was excessive

- Load balancing on Gigamon for ICS feed
  - Horizontally scale with ICS-1 and ICS-2
  - 10-12% down to <1% drop rate

- Kernel upgrades and PF RING
- CPU pinning and worker nodes
Sensor Load & Bandwidth Utilization

2 ICS sensors in main hub
- Plus 1 ECS sensor and 1 FSF scanner
- Highest loads are seen on this hub’s ICS sensors
- All other hubs and sites can handle ingress and egress traffic on a single HCS (hybrid) sensor on-site

Sample from 1 ICS sensor (0900 – 2400 UTC)
- Average capture interface traffic peaks at 2.2 Gbps
- Interface utilization peaks at 21% on average
- CPU Load average peaks at around 11 out of 32 total cores
Extending Capabilities
Querydb

- Makes Bro data queryable
  - KISS Principle
  - Command line based
  - Vast volumes of data, difficult to search through
  - Increased queriability equals increased utility

- Aim at quickly answering common questions for IP addresses and domains
  - Have I seen this indicator? If so, where, and when...?
  - Pivot for more information

- Keeps analysts on the Linux command line
  - Consistent with strategic direction for analyst development
Querydb

- Components
  - Aggregator - Runs on each sensor and gets all unique IP addresses and domains for each rotation interval
  - Database - Two MongoDB collections for connections and domains
    - TTL index
  - Frontend - Small python script that pulls sources based on query
Querydb

Check for communication to domains and sub domains between dates, show only results from specific appliance...

Query each http log for domain and fetch results

Domain | Appliance | Date | Log File
---|---|---|---


Domain

Appliance

Date

Log File
File Scanning Framework

- Extract various file types we are interested in off the wire
- Recursively scan object and sub objects of files
  - Get more file metadata
  - Increase utility of custom Yara signatures
    - Scan files with signatures we develop through our own research
    - Let Yara detection drive some action by a module on the file
- Increase the value of malware reverse engineering efforts
  - Make the adversary pay for every byte they send us
  - Make it more expensive for the adversary to succeed
    - Cyber Kill Chain® approach
- Increase the value of threat intelligence sources that share malware
- Enable the analyst to define what is actionable cyber intelligence
  - Opportunity for more advanced and creative threat detections
File Scanning Framework
File Scanning Framework

- Demo...

Recursively process objects, extract metadata and enrich intelligence...
File Scanning Framework

- **LaikaBOSS**
  - [https://github.com/lmco/laikaboss](https://github.com/lmco/laikaboss)
  - [http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LaikaBOSS%20Whitepaper.pdf](http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LaikaBOSS%20Whitepaper.pdf)

- **MITRE Multiscanner**
  - [https://github.com/MITRECND/multiscanner](https://github.com/MITRECND/multiscanner)

- **Viper**
  - [http://viper.li/](http://viper.li/)
  - [https://github.com/viper-framework/viper](https://github.com/viper-framework/viper)
Key Takeaways

● Relying solely on COTS only solutions Isn’t the best idea
  – Relying on the opportunity to solve the problem for themselves
  – May find yourself handcuffed to a capability that doesn’t meet your needs
  – Enable yourself to solve world class problems

● Adopting Bro as a Network Analysis Framework has been a key enabler
  – Gain visibility into network traffic
  – Augment standalone analysis
  – Extend team capabilities, put analyst in drivers seat

● Introducing… Emerson GitHub!
  – We’ve done a lot to extend capabilities of Bro
  – We’ve written standalone tools of our own
  – [https://github.com/EmersonElectricCo](https://github.com/EmersonElectricCo)
Questions?

- Thanks for your kind attention!