Smart People Solving Hard Problems

CSN31: Writing Threat Intelligence Content for Today's Threats

John DiFederico

Security Engineer

B.S. CIS, GCIH, ASCA

SAIC®
From Science to Solutions

Importing Threat Intelligence Is Not Enough

Import

Filter

Correlate

Elevate

SAIC
From Science to Solutions

Basic Content Will Net Basic Results

Threat Intelligence Content Methodology

- What threat is it tracking?
- How would a host affected by this threat behave?
- Is this feed tracking attackers or destinations?
- Are hits to this intelligence simply suspicious or confirmed malicious?

Repeat Offender Content

- Trojans and other data-siphoning malware check into their botnet controllers over many intervals.
- You need content that separates bursts of traffic from interval traffic.
- Monitor these repeat offender events in a dashboard or query viewer sorted by highest count.

Bytes Out Tracker

- Malware check-ins are normally around the same packet size. If you don’t have content monitoring your trends, you’ll never find the deviations.

- A large data monitor will give you a good idea of what your trends are and easily spot deviating traffic. This is great for detecting worm or trojan outbreaks.

DNS Tracker

- Malware commonly hijacks users' Domain Name Service (DNS) settings in an attempt to phish data or install additional malware.
- Rules detecting port 53 traffic to threat intelligence is not enough.
- Use a data monitor to track DNS traffic to public address space.

High and Low Port Rules

- Event volume to uncommon ports will be low, but high in relevance.
- Common use cases satisfied with this content are SMB transfers to suspicious Internet providers, unauthorized RDP sessions, FTP data siphoning, and IRC bots.

SMB - Service Message Block Protocol RDP= remote desktop FTP = File Transfer Protocol IRC = Internet relay chat

File Extension Correlation

- Some of the most critical threat intelligence matches are those that request files that can contain binaries. Separate these events with additional content.

- Correlate all of your threat intelligence against file names and URLs that end in .exe, .pdf, .swf, .bin, .jar and other files that commonly contain executable code.

URL = Uniform Resource Locator

IDPS Correlation

- Breathe new life into old signatures with threat intelligence correlation.
- Example “GEN:ZEUS-USER-AGENT matches Web Traffic to RBN”.
- Example “GEN:UPX-PACKED-BINARY after Web Traffic to RBN”.

IDPS = Intrusion Detection and Prevention System RBN = Russian Business Network

SAIC® From Science to Solutions

Domain Parking Lots

- Domain parking lot Internet Protocol (IP) addresses are often added to threat intelligence feeds even when only one of 100,000 domains hosted there are suspicious.

- Domain parking lot threat intelligence traffic made up over 50 percent of our total threat intelligence traffic and was almost entirely false positives.

- Discover which domain on that IP Address is considered suspicious, add it to a domain-based Active List of threat intelligence, and wait for events that explicitly match.

SAIC
From Science to Solutions

Dashboards, Query Viewers, and Reports vs. Active Channels

- While Active Channels remain a common tool for investigations, it is not always the best tool to prioritize and triage investigations.
- Threat intelligence is often waiting for a trend or pattern to be established before an investigation is warranted.
- Dashboards can display multiple data monitors like this and keep the most suspicious hosts in easy view.

Lessons Learned

- If you're not learning from your investigations, you're not reaching your full potential.
- Document false positive domains and IPs.
- Track newly acquired intelligence.
- These domains, IP Addresses, and user-agents should be added to new Active Lists with descriptions and correlated against.

IP = Internet Protocol

SAIC
From Science to Solutions

Summary

- Importing threat intelligence feeds is half the battle.

- Without content geared to specific threat behavior, you will be searching for a needle in a haystack.

- Using the best tools in ArcSight to view your events is as important as the filters.

- Lessons learned from your investigations will lead you beyond pre-compiled intelligence feeds.

SAIC®
From Science to Solutions