Splunking The Endpoint III:

Hands-On with Boss of the SOC data!
(plus some other stuff)

James Brodsky | Sr. SE Manager / BOTS Scenario Owner

28 September 2017 | Washington, DC
whoami

- Sr. Sales Engineering Manager, Boulder CO of some of the hardest working SEs in Splunk
- Supports Major Accounts for Splunk in the West
- Splunk Security Architects Crazy Uncle
- Splunking the Endpoint! .conf2015, .conf2016
- BOTS 1.0, 2.0 BOTN 1.0
- CSC 20 Whitepaper, FFIEC Whitepaper (co-author), Tripwire apps, blogs, Sysmon contributions, etc, etc....
It’s a hands-on session. Eventually. But first slides. Lots of slides.
Even if you’re Shatner you still need to have brought a functional, modern computing device. And it needs to be on the Internet. And it needs a relatively modern browser.
roll d20 to determine your server!

left side of room=“a”

right side of room=“b”
roll d20 to determine your server!
left side of room=“a”
right side of room=“b”
prepend with “0” if single digit
alice/epsecurity

= https://conf17-bots-endpoint-14a.splunkoxygen.com

or

= https://conf17-bots-endpoint-14b.splunkoxygen.com

Depending on what side of the room you are on.
Welcome to the 3rd edition of our Endpoint breakout sessions, and the 2nd edition that includes a hands-on component. This year (2017) we'll showcase malware and ransomware investigation, data from non-Windows endpoints, and a brief tour through some of Ransomware's greatest hits of 2017. And, we'll mostly leverage data from Boss of the SOC (BOTS) v2.0 to do so.

This hands-on material was developed with awareness and consideration of the sessions that have come before it in 2015 and 2016, as well as a close collaboration with the BOTS team. Rather than publish all of the instructions and related resources for this session in an app, as was done in 2016, we have chosen to provide several bits of written collateral to help guide you through the BOTS (and some other ransomware) data.

How to Use This App

Simply download one or more of the companion PDFs linked below - whichever suits your learning style - and use the "Search" link above or here to run the searches and follow along with the session. Also download the encrypted JPG file from the last link. Once you get to the third major part of the session, visit the 'WannaCry/EternalRocks/NotPetya' app here.

Companion Material Downloads

- Detailed Companion Document with Screenshots and Short Explanations
- Abbreviated Companion Document with Just Searches
- Full Companion Document in Whitepaper Format

[encrypted image file for Ransomware Step 3]

Select additional content to view using the checkbox.
What we’ll cover
 Agenda
90 whirlwind minutes…

▶ Where have we been?
▶ What’s new over the past year or so?
  • Hands-on adventure #1
▶ Endpoints aren’t limited to Windows
  • Hands-on odyssey #2
▶ The part where we all have a group cry
  • Hands-on journey #3
▶ Q&A
We’re still talking about this…

…because frankly there’s something new to talk about every year.
• Windows focus
• Using the Universal Forwarder (UF) as an EDR
• Target Breach RAM Scraper Demonstration
• Example UF configurations (many of which have since been updated)
• First introduction to wonders of Sysmon
• No hands-on
Ransomware focus (Cerber) from BOTS v1 Data

• Detection, Prevention, Forensics
• Almost completely hands-on
• Updated information about UF configurations
• Many example searches provided
730 days later…still relevant.

The UF: More Than You Think!

*Including powershell!
Our new communications director has some updates to communicate about endpoint topics and Splunk. And then he has to leave.
Update: Sysmon Love Fest
Microsoft Sysmon: It keeps getting better.

Current Version: 6.10

Splunk

- Splunk enables collection and rich queries of Sysmon data
- Configuring Splunk for Sysmon:
  - https://github.com/splunk/TA-microsoft-sysmon
  - Install Splunk universal forwarder on Sysmon systems
  - Install Splunk Sysmon TA on search heads
  - Set Sysmon configuration to exclude Splunk binaries

```xml
<Image condition="contains">splunk</Image>
<Image condition="contains">streamfwd</Image>
..."
What’s new in Sysmon (past 2 years)?

• Event Code 11: File Creation
  • Poor mans FIM
  • Log when a file is created or over-written – monitor creation of things in autorun locations or with usually-suspicious extensions (.bat, .vbs, .ps1, .docm, .xlsm)

• Event Codes 12, 13, 14: Registry key creation and modification
  • More flexible/performant than registry monitoring built into UF
  • More persistent delivery than UF due to event log mechanism

• Event Code 15: Alternate Data Stream Creation
  • Tracks if/when files are created with ADS that have suspicious content (.bat, .vbs, .ps1, .cmd, etc…)
  • Browser Drops (Mark Of The Web)

• Event Code 10: Process Access
  • One process accessing the memory of other processes
  • Probably too noisy to use
And on 9/11/17, moar Sysmon...

- Event Codes 17 and 18: Pipe Events
  - Sometimes malware uses named pipes for interprocess communication

- Event Codes 19, 20, and 21: WMI Stuff
  - WMI event filter, event consumer, and event consumer to filter activity

For a good example of recent malware using BOTH of these techniques, research “Nyetya” derivative of Petya/NotPetya/Goldeneye.

http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

Sysmon TA has been updated in two places – we will see in 3.5 minutes…
You are a wonderful person that knows how useful Sysmon is.*

If you aren’t using SwiftOnSecurity’s Sysmon config, you should. Google “taytay swift sysmon” and you’ll find it.

And if you’d like some Splunky tweaks to it...those are on the next page.

*Not yet inclusive of latest 3 WMI Sysmon event codes.
Exclusions for EventCode 1

Exclusions for EventCode 2

Linked in the companion document
If you’re using a Sysmon configuration based on something other than TaySwifts…

...shake it off.
10,000 hosts, 7 days, ~130GB.

~19GB a day.

Or, about 2MB per endpoint, per day.

(Your Mileage May Vary.)
Yesterday, This Happened.
You should check out this talk from 9/27. Seriously.

Effectively Enhancing our SOC with Sysmon, PowerShell Logging and Machine Learning to Detect and Respond to Today’s Threats

Wednesday, September 27, 2017 | 2:15 PM-3:00 PM

Kent Farries, Sr. Systems Analyst, Security Intelligence & Analytics, TransAlta Corporation

Ikenna Nwafor, Sr Systems Analyst, Security Design, TransAlta

With today’s threats, TransAlta needed to improve its managed SOC with the goal of becoming a “pretty good SOC” in 2017. We had to look at how we are doing things today, what we should stop doing or automate and what we should be doing tomorrow. We decided that we needed to get better at hunting with limited resources, so we chose to leverage Sysmon, PowerShell logging and machine learning. This session will showcase how we used Splunk to efficiently collect and analyze the logs from thousands of endpoints to understand our security posture. We will also provide some insight from our lessons learned around deployment, tuning and capacity planning.

~1700 endpoints, ~10MB Per, Sysmon and Windows Events!
A cool community Sysmon app by HAGGIS!
Tayswift Config in Action

with network events

whut?

without network events
Clever network filtering *(the config is chock full of stuff like this)*

Late-Night BOTS scenario testing!
Recently Updated Splunkbase Sysmon TA. Why?

Add-on for Microsoft Sysmon

Overview

Provides a data input and CIM-compliant field extractions for Microsoft Sysmon. The Microsoft Sysmon utility provides data on process creation (including parent process ID), network connections, and much more.

Details

This add-on was originally created by Adrian Hui. We appreciate Adrian's contribution and his willingness to turn over control to the current team for ongoing maintenance and development.

Release Notes

Version 6.0.2 Sept. 6, 2017
### Additional Field Extractions

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[KbcEventLogging:Microsoft-Windows-Sysmon/Operational]</td>
</tr>
<tr>
<td>2</td>
<td>#SECOD-pw_rule1 = s/\w+/\w+/ <strong>MA$$</strong>//g</td>
</tr>
<tr>
<td>4</td>
<td>EVAL-src_ip = SourceIp</td>
</tr>
<tr>
<td>5</td>
<td>EVAL-src_host = SourceHostName</td>
</tr>
<tr>
<td>6</td>
<td>EVAL-src = if(!isnotnull(SourceHostName), SourceHostName, SourceIp)</td>
</tr>
<tr>
<td>7</td>
<td>-21.6 -21.9</td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>EVAL-user = User</td>
</tr>
<tr>
<td>10</td>
<td>EVAL-vendor_product = &quot;Microsoft Sysmon&quot;</td>
</tr>
<tr>
<td>12</td>
<td>+EVAL-cmdline = CommandLine</td>
</tr>
<tr>
<td>13</td>
<td>+EVAL-parent_process_id = ParentProcessId</td>
</tr>
<tr>
<td>14</td>
<td>+EVAL-parent_process = ParentProcess</td>
</tr>
<tr>
<td>15</td>
<td>LOOKUP-eventcode = eventcode EventDescription EventDescription AS signature</td>
</tr>
<tr>
<td>16</td>
<td>FIELDLAVIS-signature_id = EventCode AS signature_id</td>
</tr>
<tr>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

**better extractions for hashes, commandline data**
Better support for Change Analysis DM

Filesystem Changes

<table>
<thead>
<tr>
<th>file_name</th>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the file that is the object of the event (without location information related to local file or directory structure).</td>
<td></td>
</tr>
</tbody>
</table>

All Changes

<table>
<thead>
<tr>
<th>object</th>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the affected object on the resource (such as a router interface, user account, or server volume).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>object_attrs</th>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>The attributes that were updated on the updated object.</td>
<td></td>
</tr>
</tbody>
</table>
It’s still not perfect.
We need a real, standard Common Information Model for endpoint process data.

There is progress being made. Thank you, Security Research team.
Recently Updated Github Version of Sysmon TA
Update: Many Other New Things
In looking into compromised systems, often what is needed by incident responders and investigators is not enabled or configured when it comes to logging. To help get system logs properly Enabled and Configured, below are some cheat sheets to help you do logging well and so the needed data we all need is there when we look.

Cheat Sheets to help you in configuring your systems:

- The Windows Logging Cheat Sheet  
  Updated Oct 2016

- The Windows Splunk Logging Cheat Sheet  
  Updated Mar 2017

- The Windows File Auditing Logging Cheat Sheet  
  Updated Oct 2016

- The Windows Registry Auditing Logging Cheat Sheet  
  Updated Oct 2016

- The Windows PowerShell Logging Cheat Sheet  
  Updated July 2016

- The Windows Sysmon Logging Cheat Sheet  
  Coming soon
Our old friend, URL Toolbox...

Great for URL manipulation and string analysis!

URL Toolbox

Overview

UTBox is a set of building blocks for Splunk specially created for URL manipulation.

UTBox has been created to be modular, easy to use and easy to deploy in any Splunk environments. It only needs to be deployed on Splunk Search Heads and the bundles will automatically be sent to your Splunk Indexers.

One of the core feature of UTBox is to correctly parse URLs and complicated TLDs (Top Level Domain) using the Mozilla Suffix List. Other functions like shannon entropy, counting, suites, meaning ratio, bayesian analysis, etc. are also available.

UTBox has firstly been created for security analysts but may fit other needs as it's a set of building blocks. Enterprise Security users will need to modify the import statement to use UTBox.

You should also take a look at URL Parser for efficient URL parsing; https://splunkbase.splunk.com/app/3396/

Release Notes

Version 1.6  April 10, 2016

Community Supported App

Details

755 3,061
Installs Downloads

LOGIN TO DOWNLOAD

VERSION

16+

BUILT BY

Cedric Le Roux

CATEGORY & CONTENTS

Categories: Security, Fraud & Compliance, Utilities

App Type: App

COMPATIBILITY

Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, 6.0, 5.0
Platform: Platform Independent
...has a new friend, “JellyFisher.”

Also written by Cedric Le Roux
Leverages Python “jellyfish” Library for approximate and phonetic string matches.
URLParser is a custom search command designed to parse URLs. Because it relies on the new chunked protocol, URLParser is compatible starting with Splunk 6.4.0 and above.

```
... | urlparser [field=fieldname] [listname="*|iana|mozilla|...''] [mode=simple|extended]
```

URLParser is a community supported app and compared to UTBox, URLParser is faster, extract more fields and is easier to use.

**Extracted fields**

- url_domain
- url_domain_without_tid
- url_fragment
- url_hostname
- url_netloc
- url_params
- url_password
- url_path
- url_port
URLParser: URL/domain manipulation portions of URL Toolbox in "turbo mode" 3x-4x faster...

search url!=- url=* | head 200000 | urlparser listname="mozilla|iana"

This search has completed and has returned 5,123 results by scanning 204,129 events in 26.91 seconds

As a reference point for comparison, here are the results with UTBox:

search url!=- url=* | head 200000 | eval list="*" | lookup ut_parse_extended_lookup url list

This search has completed and has returned 5,123 results by scanning 204,129 events in 83.123 seconds

Extracted fields

URLParser will extract the following fields from the submitted URLs:
- url_domain
- url_domain_without_tid
- url_fragment
- url_hostname
- url_netloc
- url_password
- url_params
- url_path
- url_port

Cedric Le Roux

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance, Utilities
App Type: App

COMPATIBILITY
Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4
Platform: Platform Independent
David Veuve is My SPL Patronus

...and he will be yours too after you review his stuff.
BUT WHAT ABOUT MACHINE LEARNING?
Practical Endpoint ML Example #1
DGA Analysis using MLTK – released this week!
“Collect all my DNS (or Netflow) data? Nope. Splunk is too expensive.”
New Pricing for DNS or Netflow data is 33% of what you will pay for a normal Enterprise Term license.

- 500GB minimum
- Term, not permanent
- License tied to those two sourcetypes
- Call your Splunk account team
Everyone Can Build a Security App!
Tuesday, September 26, 2017 | 12:05 PM-12:50 PM
Tuesday, September 26, 2017 | 1:10 PM-1:55 PM
GOOD FOR ALL SKILL LEVELS

Young Cho, Technical Marketing Manager, Security, Splunk
Jae Lee, Product Marketing Director, Splunk
Anthony Tellez, Lead, Business Analytics & IoT, Splunk

Attend this guided, hands-on session to learn security best practices related to building a Splunk App – specifically, key aspects of operationalizing security searches, visualizations and workflow. We’ll cover a range of topics, including: - Overall methodology: when and how building an app can help with security challenges and how to design an app to extract key insights from common data sources. - Foundational concepts: TA application, data validation, CIM, summarization, data enrichment, analysis techniques, visualizations, rules definition and more. - More advanced: including modeling, applying data science techniques, forming hypotheses and process considerations. You’ll learn first-hand by iteratively developing an app that you can then take home and continue to use as a learning or testing tool. Alternatively, you can customize and/or deploy or even rebuild it using your security or compliance framework of choice. The app includes the security-rich dataset used in last year’s (conf2016*)’s Boss of the SOC competition. You can get great, useful info and techniques from this session regardless of your skill level with Splunk or whether your current primary use case is security, IT operations or something else. Laptops are required to participate.

https://splunk.box.com/v/Buildingasecurityapp
Exercise 1: Sysmon in BOTS - APT and Ransomware Scenarios
roll d20 to determine your server!

left side of room=“a”

right side of room=“b”

prepend with “0” if single digit

alice/epsecurity

= https://conf17-bots-endpoint-14a.splunkoxygen.com

or

= https://conf17-bots-endpoint-14b.splunkoxygen.com

Depending on what side of the room you are on.
Get ready to cheat learn.
Did you play?

Let’s recap the first scenario...
Theme: How to go from finding an unusual process executing on an endpoint to full-blown exfiltration of corporate secrets via DNS in 12 easy searches.
How to go from finding an unusual process executing on an endpoint to full-blown exfiltration of corporate secrets via DNS in 12 easy searches.

Please log into your Splunk systems.
Something like this

index=bots-apt sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 | eval allcommand=CommandLine+"":"+ParentCommandLine | eval set="@base64@" | `ut_countset(_raw,set)` | spath input=ut_countset | rename ut_countset.sum AS base64charcount | dedup allcommand | eval totallen=len(_raw) | eval commandlen=len(allcommand) | eval ratio = base64charcount/totallen | stats values(allcommand) by ratio,totallen,base64charcount,commandlen | where ratio>.90 | sort -ratio
Additional .conf2017 Content Worth Looking At!

Review these talks when you are able

Security Ninjutsu Part Four: Attackers Be Gone in 45 Minutes of Epic SPL
Wednesday, September 27, 2017 | 2:15 PM-3:00 PM
David Veuve, Principal Security Strategist, Splunk Inc.

My favorite part of any spy movie is the gadgets. You see a spy in normal attire, without knowing that the jacket is bulletproof and the watch shoots amnesia darts. That spy i...

Quickly Advance Your Security Posture With Splunk Security Essentials
Tuesday, September 26, 2017 | 1:10 PM-1:55 PM
David Veuve, Principal Security Strategist, Splunk Inc.

Whether you’re looking to reduce breaches, set up monitoring to anticipate attacks, or build more predictive capabilities, you will learn to apply the power of Splunk’s search...

Searching FAST: How to Start Using tstats and Other Acceleration Techniques
Wednesday, September 27, 2017 | 12:05 PM-12:50 PM
David Veuve, Principal Security Strategist, Splunk Inc.

You know the use cases, you understand stats. You might strug through the halls of .conf events as an advanced SPLer. But you’ve heard a whisper on the wind, a next-level appr...

Hunting the Known Unknowns: Finding Evil With SSL Traffic
Tuesday, September 26, 2017 | 12:05 PM-12:50 PM
Steve Brant, Senior Security Strategist, Splunk Inc.
Ryan Kovar, Staff Security Strategist, Splunk Inc.

This year’s “Hunting” session will describe how to find malicious adversaries using SSL. The talk will cover new ways to log SSL/TLS certificates and how to find malware in yo...
Not Everyone Runs Windows
Browsing Yelp reviews of all avocado toast food trucks within 500 yards. NOT worried about malware, amirite?
You most likely have some Macs.

(2016 JAMF “Managing Apple Devices in the Enterprise”)
Total Mac OS Malware

(2017 McAfee)
You could, and should, have a traditional endpoint A/V solution on your corporate Macbooks.

But what could you do with Splunk?
Here’s what we said about Windows...

The UF: More Than You Think!
The UF: More Than You Think!

UF + nix TA + Stream + osquery!
osquery allows you to easily ask questions about your Linux, Windows, and macOS infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company.

Read the deployment guide or start contributing!

```
osquery> SELECT uid, name FROM listening_ports l, processes p WHERE l.pid=p.pid;
```

osquery gives you the ability to query and log things like running processes, logged in users, password changes, USB devices, firewall exceptions, listening ports, and more. You can perform ad-hoc queries or schedule them, optionally enable file integrity monitoring and process accounting too. More details can be found here.

- **Enterprise Ready**: CentOS, Ubuntu LTS, Windows, and macOS, and almost every Linux OS released since 2011 are supported with no dependencies. osquery powers some of the most demanding companies, including Facebook.
- **Differential Changes**: Know when critical objects are added, modified or deleted from a system. Use a combination of event streams and polling with set differentials.
- **Feature Velocity**: You control the roadmap. Developed in the open, by the community, for the community on Github.

Linux, macOS, Windows, etc... Open source.
Ad-Hoc or Scheduled.

JSON output gathered by UF.

Highly scalable (started by Facebook)

FIM!

Community App written by Thomas Przelomiec (Splunk)
Introduction to osquery for Threat Detection & DFIR

What is osquery?

osquery is an open source tool created by Facebook for querying various information about the state of your machines. This includes information like:

- Running processes
- Kernel modules loaded
- Active user accounts
- Active network connections

And much more!
Don’t forget about the *NIX TA
Exercise 2: osquery, Stream, *NIX TA in BOTs Ransomware Scenario
Theme: Let’s save the day by using osquery to find ransomware that royally messed up some critical marketing files, and then decrypt them!
The malwarewolf

One day, my blog will have something to say about this.

Friday, February 26, 2016

OSQuery, Splunk and PCI

A couple of years ago over at Facebook, OSQuery was open sourced. This tool allows you to make SQL-Lite queries against tables containing information about a running Linux or OSX host. One massive advantage of this is a wide range of system attributes can be queried using a universal syntax; just imagine building (and maintaining!) even a modest sized bank of queries using native Linux tools, as well as trying to get their collective outputs into a universal format.

You can check out the tables available here: https://osquery.io/docs/tables/ and you’ll notice the file_events table, which if you are faced with PCI requirement 11.5, you’ll probably find your interest starting to get piqued...
You may have heard. Ransomware is still a thing.
’member this?
*Don't Panic!*- Scene from Airplane
Most malware/ransomware behaves in predictable ways.

Assuming you instrument your environment appropriately (with the UF, or other) you should be searching for certain things.

Searches that we’ve been talking about for the past two years would have helped with:

- WannaCry
- NotPetya
- EternalRocks
- …and whatever comes down the pike next.
This is a pike.
THE BOSS CAN DO AS HE LIKES

Yes, also a pike.
Indeed, a pike.
Indeed, a pike.

Pipes.
Believe it or not, the original term is “pike.”

- **Canadian Oxford Dictionary, 2nd Edition:**
  
  *come down the pike* N Amer. appear on the scene; come to notice. [Abbreviation of TURNPIKE]

- **The American Heritage College Dictionary, 4th Edition:**
  
  **Idiom:** *come down the pike* Slang To become prominent. [Short for TURNPIKE.]

- **The American Heritage Dictionary of the English Language, 5th Edition:**
  
  **Idiom:** *come down the pike* Slang To come into prominence: “a policy . . . allowing for little flexibility if an important new singer comes down the pike” (Christian Science Monitor). [Short for TURNPIKE.]

...and now you can say you learned something at .conf. Tell your manager!
What were we talking about, again?
Don't Pay Ransomware

Splunk Insights for Ransomware provides smaller organizations with an additional layer of security to help combat ransomware. By enabling a broader analytics-driven approach to security, Splunk Insights for Ransomware enables understaffed IT and security shops to gain end-to-end visibility into potential ransomware activity across the IT environment.

Assess security posture, investigate and verify efficiently, and remediate quickly and appropriately – from critical infrastructure to deprecated operating systems, Splunk Insights for Ransomware helps you get better at staying on top of security hygiene to combat persistent and emerging ransomware threats, so you can maintain business continuity in the face of mutations – even global, fast-propagating attacks like WannaCry.

- Central visibility and analysis of ransomware: Use relevant data – endpoint, network, etc. – to identify and assess potential ransomware activity
- Faster, streamlined investigation of ransomware activity: Pivot easily between technologies to find evidence of ransomware threats, across security and IT
User-based Pricing (up to 1000 users) (not stackable)
Let’s revisit Ransomware’s Greatest Hits.
Exercise 3: WannaCry, EternalRocks, and NotPetya
Theme: Yes, Ms. Chief of Information Security. This expensive solution called Splunk that we bought can help us detect and defend against WannaCry/NotPetya/TheFlavorOfTheWeek.
Ransomware, Schmansomware
Early detection, prevention...

Analyze Endpoint Activity
Find malware infections before damage is caused to business operations
- Validate the method and source of infection by analyzing endpoint behavior
- Scope the broader impact of the malware or ransomware infection
- Understand how to prevent similar infections in the future

Ransomware Wrangling with Splunk
Tuesday, September 27, 2016  |  11:35 AM-12:20 PM


Speakers
Kenneth Westin, Security Market Specialist, Splunk

Recording
Thank You

Don't forget to rate this session in the .conf2017 mobile app

...or there won’t be a Splunking the Endpoint IV!

splunk> .conf2017