.conf Ransomware Hands-on: What’s your Birth Day?

https://conf-sec-seho-<2 digit number that is your birthday>.splunkoxygen.com/

EXAMPLE if I was born on July 31st:

EXAMPLE if I was born on August 4th:
https://conf-sec-seho-04.splunkoxygen.com/

Username: conf2016     Password: security
Splunking the Endpoint: “Hands on!”
Ransomware Edition

James Brodsky
Guy with beard | Splunk

Dimitri McKay
Guy with larger beard | Splunk

.conf2016
Disclaimer

During the course of this presentation, we may make ridiculous statements regarding Splunk features that may or may not be true. This is not reflective of Splunk as a company. We caution you that such statements reflect our own personal lack of intelligence and you should lower your expectations based on the fact that we’re not all that bright. By we, we mean Dimitri. Actual features or functions and their explanation of which may differ from reality. For Splunk Search Language questions, Dimitri’s answers will probably not be the truth, as such, actual results will differ greatly from those contained in Splunk documentation. If you record this presentation, you are giving up your right to vote, right to bare arms (i.e. no tank tops), and rights to your first born male child. The forward-looking statements made in this presentation are being made up as we go along. If reviewed after its live presentation, this content may not contain current or factual information. Please do not assume any legal obligation to our comments or statements as frankly, if you tattle, we will deny everything. In addition, information in this presentation is subject to change at any time without notice based on how much trouble we could potentially be in. This presentation is for educational informational entertainment purposes only. Do not hold Splunk accountable for anything that we might say or do, as frankly, the biased opinions and poor decisions we are about to make here are our own. Thanks, and enjoy the show.
Brodsky

SE Manager SW Majors
Security Practice Fanboy

3 Years+

SPLUNK® AND THE CIS CRITICAL SECURITY CONTROLS
Mapping Splunk Software to the CIS 20 CSC Version 6.0
Dimitri McKay | Senior Security Architect | CISSP | CCSK | LOLZ | WTF

- 20 years of net/system security experience.
- 2nd place, 2016 Defcon Beard Competition
- Former pentester, corporate security slacker for a search engine and plus sized hand model.
- Enjoys making poor decisions, breaking things and disappointing my parents.
- Current role on the Security Practice team focuses on security strategy for the fortune 50, evangelism and asking dumb questions.
- Currently interested in machine learning for home home automation products which will eventually become self aware and kill us all.

Minster of Swagger @dimitrimckay
Dimitri McKay | Senior Security Architect | CISSP | CCSK | LOLZ | WTF

- 20 years of net/system security experience.
- 2nd place, 2016 Defcon Beard Competition
- Former pentester, corporate security slacker for a search engine and plus sized hand model.
- Enjoys making poor decisions, breaking things and disappointing my parents.
- Current role on the Security Practice team focuses on security strategy for the fortune 50, evangelism and asking dumb questions.
- Currently interested in machine learning for home home automation products which will eventually become self aware and kill us all.

Minster of Swagger @dimitrimckay
04 MINUTES 00 SECONDS
Agenda

• Really short ransomware overview
• What’d we talk about last year and errata
• How do we log in?
• Hands-On: Detection by watching the endpoints
• Hands-On: A diversion over to forensics
• Hands-On: Ideas for prevention
• Collapse on stage
Intentionally Left Blank
So... what’s the problem, Dimitri?
ransomware

(n.) when cyber criminals screw you over for money
Ransomware Evolution

- RANSOMLOCK
- URAUSY
- CRYPTOLOCKER
- CRYPTODEFENSE
- CRYPTOWALL
- REVETON
- LOCKDROID
- VIRLOCK
- TESLACRYPT
- CTB-LOCKER
- LOCKSCREEN
- TOX
- TESLACRYPT 2.0
- TORRENTLOCKER
- DMALOCK
- CHIMERA
- 73V3N
- LOCKY
- SAMSAM
- KERANGER
- POWERWARE
- PETYA
- TESLACRYPT 3 & 4
- CERBER
- JIGSAW
- ROKKU
- HYDRACRYPT

2013
2014
2015
2016
2
So, wait, how bad is it, Dimitri?
2016 Verizon breach report

- C2: 175
- Ransomware: 148
- Spyware/keylogger: 42
- Backdoor: 21
- Export data: 19

Incident count
DO YOU WANT TO GET RANSOMWARE?

BECAUSE THAT'S HOW YOU GET RANSOMWARE.
Mind visualizing that to the kill chain, Dimitri?
Ransomware Kill Chain

Criminal Syndicate → Ransomware → Watering Hole /Exploit Kit → Malicious Email (Link/Attachment) → Victim

Stages:
- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control (C2)
- Actions on Objectives
Switch to James
But before we continue...
Let’s go back in time...
To exactly 1 year ago
Poor decisions were made.
The UF: It’s more than you think

Logs
The UF: It’s more than you think

- Process/Apps/FIM
- Registry
- Scripts
- Logs
- Perfmon
- Wire Data
- Sysmon
Ransomware Exercises: from the UF

- Process/Apps/FIM
- Registry
- Logs
- Wire Data
- Sysmon
And we will add from non UF sources:

- Process/Apps/FIM
- Vulnerabilities
- Firewall
- Registry
- Wire Data
- Forensics
- Logs
- Sysmon
How much data?

That’s more like it. 16MB of Sysmon, 5.5MB of Windows events = 21.5MB per endpoint.

Coverage for 1,000 Windows endpoints? 21.5GB ingest, per day.
What went wrong last year?
Let's go back in time...

no one is perfect...
Mistakes were made...

Let’s go back in time...
There were... inaccuracies...
These didn’t always work. Have been updated/fixed.

https://splunk.box.com/splunking-the-endpoint

Thank you, Jeff Walzer and Mike Sangray!
.conf Ransomware Hands-on: What’s your Birth Day?

https://conf-sec-seho-<2 digit number that is your birthday>.splunkoxygen.com/

EXAMPLE if I was born on July 31st:

EXAMPLE if I was born on August 4th:
https://conf-sec-seho-04.splunkoxygen.com/

Username: conf2016 Password: security
While you’re getting logged in...

An interlude to talk about your priorities, people. Dimitri?
Switch to Dimitri
"Only the dead have seen the end of cyberwar."

-Taylor Swift
Please log into your server now.

U: conf2016 P: security

Raise your hand if you are finding this difficult.
You might need help!
Follow along with the narration in the app, at least for the first few examples.
Find statistically significantly long command executions

```
index:myevents | sourcetype:plainfileventing:mscorrel-events |Microsoft-Windows-System-Operational| EventCode:1
| eval cmdLine=replace(CommandLine, '\n', '')
| stats stdev(CommandLine) as stdev, count(cmdLine) as count, avg(cmdLine) as avg by host
| stats max(cmdLine) as maxLine, values(avg) as avgdev, values(stdev) as stdevhost, values(avg) as avghost by host
| where maxLine=4(stdevhost)
```

**Line by Line**

1. **What**: Pull in our Sysmon events. We could also use Windows Security events if we wanted as we saw earlier.
2. **Eval**: Eval how long each command line is per event. Then calculate the standard deviation and the average command line length, per host, for the whole dataset.
3. **Stats**: Display the maximum, stdev, and average values of commandline length per host.
4. **Why**: This will allow us to determine commandline lengths that deviate from their norms.
5. **What**: Filter out 'normal' commandline lengths.

**If the command line seen more than four standard deviations away from the normal, then show just these. Four standard deviations may be a bit too long — but see what a reasonable threshold is for your organization. You might also say that critical endpoints have a lower threshold than non-critical.**
You’ve got this! Copy and paste the example searches into the “search bar” in the “SplunkLive Security 2016” app.
Ninja Path

Find statistically significantly long command executions

```bash
index=wayne "sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1
| eval cmdlen=len(CommandLine)
| eventstats stdev(cmdlen) as stdev, avg(cmdlen) as avg by host
| stats max(cmdlen) as maxlen, values(stdev) as stddevhost, values(avg) as avgperhost by host,CommandLine
| where maxlen>4*(stdevperhost+avgperhost)
```
Ninja Path

stay within app context

paste search here
What have we here?

Our learning environment consists of:

- 31 publically-accessible single-instance Splunk servers
- Each with ~700K events, from real environment.
What do you think my lab looks like...
What's the lab environment look like? This? What you think my lab looks like is the reality.
attribution.
Get ready to cheat learn.
Hi. We’re blackhats.
Hi! I’m an endpoint!
USB Drive with Malicious Word Macro Doc

miranda_tate_unveiled.dotm (via USB drive)
Communication to Download Cryptor Code

we8106desk

LAN

webackupsvr1  WE9041SRV

wenessus1  192.168.2.50

suricata-ids

Fortigate NG Firewall
192.168.250.1

Internet

OD-FM-CONF-NA (AWS)

webackupsvr1  WE9041SRV

wenessus1  192.168.2.50

suricata-ids

Fortigate NG Firewall
192.168.250.1

Internet

OD-FM-CONF-NA (AWS)
Local File Encryption

we8106desk

webackupsvr1

WE9041SRV 192.168.2.50

wenessus1

Fortigate NG Firewall 192.168.250.1

suricata-ids

OD-FM-CONF-NA (AWS)

Internet

wenessus1

LAN

splunk-02

STM

WESIFTSVR1 WESTOQSVR1

Local File Encryption

69
Lateral Move to Fileshare
Abandon Hope
Sourcetypes We Have

- WinEventLog: System
- WinEventLog: Application
- WinEventLog: Security
- Microsoft-Windows-Sysmon/Operational
- WinRegistry
- netbackup_logs
- nessus:plugin
- nessus:scan
- log2timeline
- stoq:*
DETECTION: Windows events, stream, sysmon, registry, firewall....
DETECTION - We learned that:

- Many ways to detect unusual endpoint behavior that could indicate ransomware infection.
- Make your searches look for general, abnormal behavior – not “specific” or you’ll never keep up.
- You don’t have to turn on everything we showed to get some value – but the more you have the more confident you can be. Windows events are a bare minimum!
- The earlier you detect, the better chance you have at stopping the spread.
FORENSICS: A dive into a disk image
Forensics: What did we learn?

- Don’t use suspicious USB drives containing macro-enabled Word docs. 😊
- While lots of good commercial forensic analysis tools exist, there’s a lot you can do with programs from the open-source community.
- Log2timeline/Plaso has been around for a LONG time and can be enhanced via extensive plugins. Cost = $0. Lots of training!
- You could gather disk images from infected systems and use Splunk to sift through the extensive amounts of data.
- In smaller shops, this is a good use for a copy of FREE SPLUNK on your laptop.
Prevention: What did we learn?

- Do what you can about implementing policy to harden your endpoints.
- Back everything up always and verify.
- Scan your systems, patch your systems, use asset and identity info.
- Perform automated analysis to know when bad stuff’s arriving.
- Leverage infection lag built into ransomware variants to “take action” before the darkness.
- Ken Westin’s talk from Tuesday!
Adaptive Response.
Dimitri’s Magical and Timely AR Slide
THANK YOU

https://splunk.box.com/splunking-the-endpoint