



.conf2015

Splunking the Endpoint

James Brodsky

Staff Engineer/Security SME, Splunk

brodsky@splunk.com



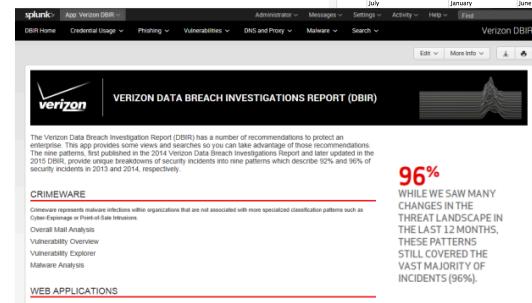
splunk®

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

About Me



Splunk and the SANS Top 20 Critical Security Controls

Mapping Splunk Software to the SANS Top 20 CSC Version 4.1

About Me

- And, I like infecting Windows Embedded POSReady systems running Splunk with RAM Scrapers for fun and profit!



That's an
endpoint!



.conf2015

Demo, Part I

splunk®

Do you know this man?



Ghosts of Sessions Past

“Finding Advanced Attacks & Malware with 6 Windows EventIDs you Configure and Monitor” – Michael Gough, Malware Archaeology

“Hunting known unknowns with DNS” – Kovar & Brant, Splunk

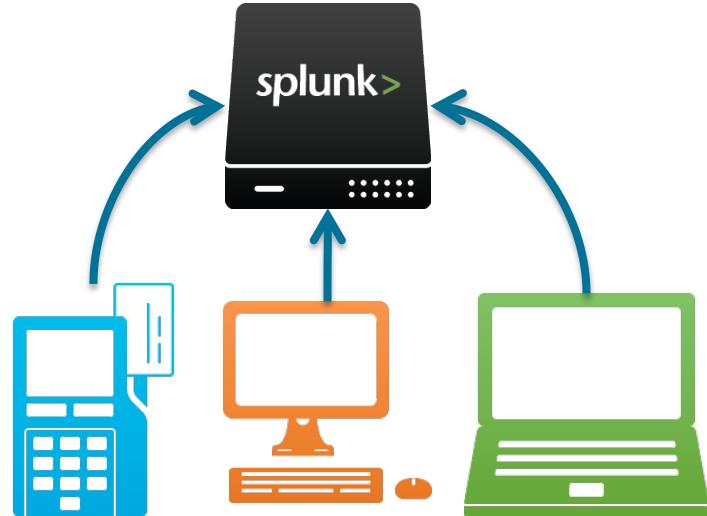
“Verifying Success of Key Mitigations” – Jim Ronayne, NSA

“Security Ninjutsu Part II” – David Veuve, Splunk

Check these
out!

Session Goals

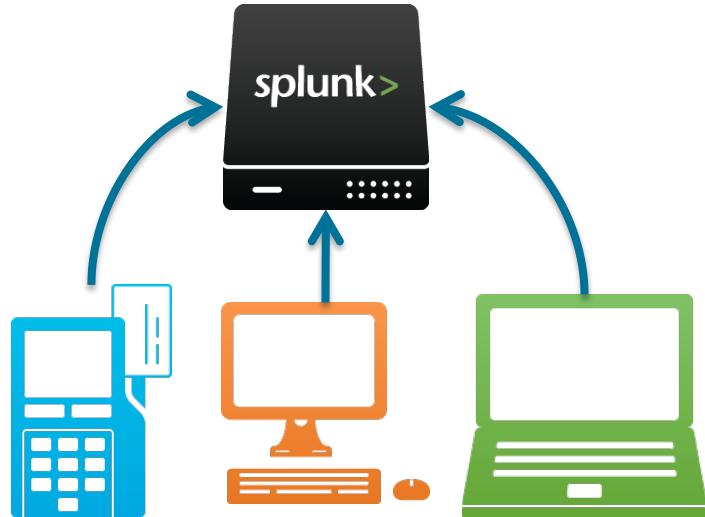
- Understand why you should Splunk the endpoint
- Believe that the Universal Forwarder is awesome
- Learn about customer success
- Get some artifacts you can use
- Bring home what you can do today



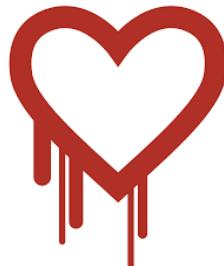
<https://splunk.box.com/splunking-the-endpoint>

WHY?

1. It is *relatively inexpensive* to Splunk your endpoints, and it will improve your security posture.
2. **VISIBILITY!** You will have *more complete information* in the case of breach.
3. The information from your endpoints *maps well to the CSC 20* and other security guidance.



You may have heard...



Endpoint/Server Vulnerabilities

Endpoint-Based Malware

Could we be more secure if we



splunk>

....the endpoints?

Endpoint/Server Vulnerabilities

Endpoint-Based Malware

Executive Summary:

YES!

(so do that)



.conf2015

THANK YOU

splunk®

The Endpoint is important!

Closest to humans

Underprotected



Versatile

Data-rich

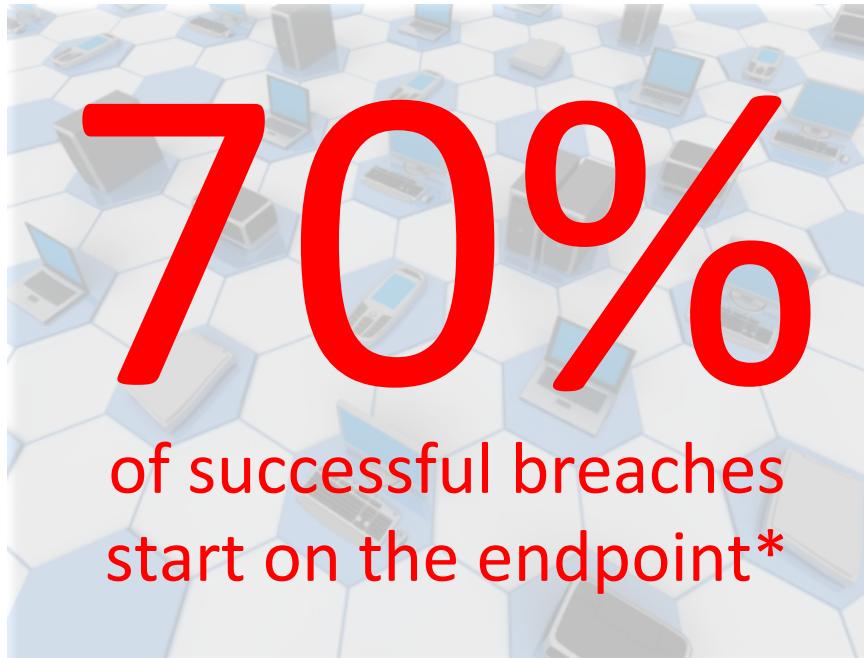
The Endpoint is important!

Closest to humans

Underprotected

Versatile

Data-rich



*IDC study 2014

The UE: It's more than you think

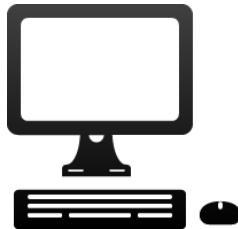
The Universal Forwarder allows

you to



....your endpoints.

The UF: It's more than you think



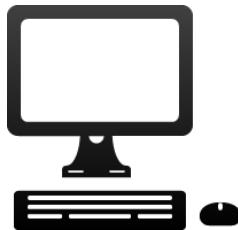
Logs

The UF: It's more than you think

Process/Apps/FIM

Registry

Scripts



Perfmon

Wire Data

Logs

Sysmon

Splunk Universal Forwarder for ETD*!

- “Free”
- Lightweight
- Secure
- Runs on many versions of Windows & *NIX & OSX
- Flexible
- Centrally configurable
- SCALE!

Splunk Universal Forwarder

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk Enterprise for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data with minimal impact on performance.

- ✓ Tagging of metadata (source, sourcetype and host)
- ✓ Configurable throttling and buffering
- ✓ Data compression
- ✓ SSL security
- ✓ Transport over any available network ports
- ✓ Local scripted inputs
- ✓ Centralized management

Choose Your Operating System to Start Download:



*Endpoint Threat Detection (Response?)

What about the “Response”?

VISIBILITY

reactivity

(for now)

What about the “Response”?

The screenshot shows two main sections of the Splunk Active Response Framework interface:

- Splunk setup:** A modal window titled "Active Response Framework" with options to "Save As" or "Close". Inside, there's a tree view with "Report", "Dashboard Panel", "Alert", and "Event type". Below the tree is a note: "Then, once an alert is triggered, according to the path and type of action chosen, a table is displayed with the actions to be taken. In order to really run the action, you need to select the appropriate alert".
- Actions:** A table listing actions. One row is selected: "action_type: block", "path: network.firewall.foorinet", and "status: activate". A note below says: "Once selected, you are sent to a confirmation dashboard".

Turning Splunk into a Systems Management Tool

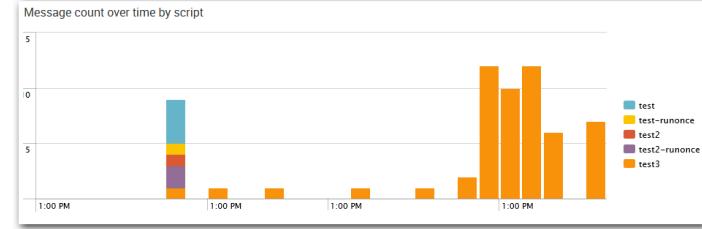
by Helge Klein on January 27, 2015 in Splunk

Despite its great power, Splunk is relatively static with regards to the data it processes. You cannot instruct it to simply run a script on all endpoints and index the results. The app *HK Systems Management* changes that. It turns Splunk into a kind of PsExec on steroids.

Background

Splunk is a fabulous tool for analysing all kinds of data, and there are many different ways of getting data into Splunk. But none of those are even close to being interactive, at least not if you want to collect data from thousands of machines.

Also, being a data analytics tools, Splunk data flow is one way only: from the endpoint to Splunk. There is no way back; at least, normally there is not.



There's stuff out
there. YMMV.

Come on. Is anyone using the Universal Forwarder in this way?

- “Free”
- Single Windows
- Secure
- Runs on Windows
- Flexible
- Centralized
- SCALABLE

Splunk Universal Forwarder

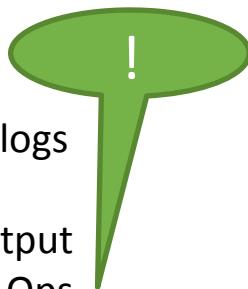
Universal forwarders play a valuable role in the Splunk architecture. They can forward the data to Splunk in real time or index it later for consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data with minimal impact on performance.

- ✓ Tagging of metadata (source, sourcetype and host)
- ✓ Configurable throttling and buffering

YES.

*Endpoint Threat Detection (Response?)

Use Case 1: Large Internet Company



config



install



search



*...x (Many
indexers)*

on prem



Int. forwarders

dmz



*UF
x10,000!*

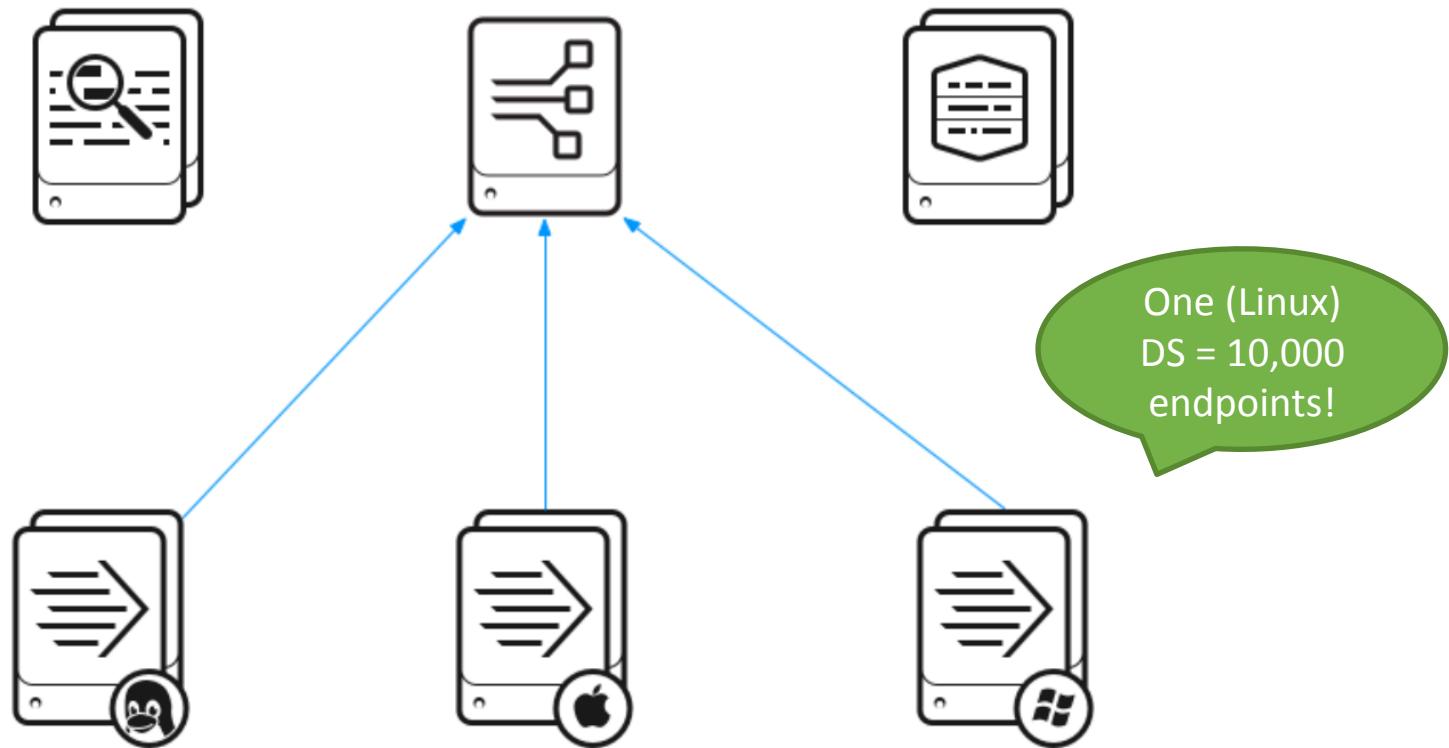
internet

- Windows event logs
- OSX /var/log/*
- Carbon Black output
- Crash logs for IT Ops
- Custom script for apps installed
- UNIX TA (upon request)
- Windows TA (upon request)
- Additional granularity for execs and their admins
- Moving to [Splunk Cloud](#)



splunk>cloud

Central Control with Deployment Server



Additional ways to gather endpoint data

Proxy Logs



BLUE COAT websense®



Integrity Management



tripwire

OSSEC

NG Endpoint Protection



TANIUM™
ziften CYLANCE

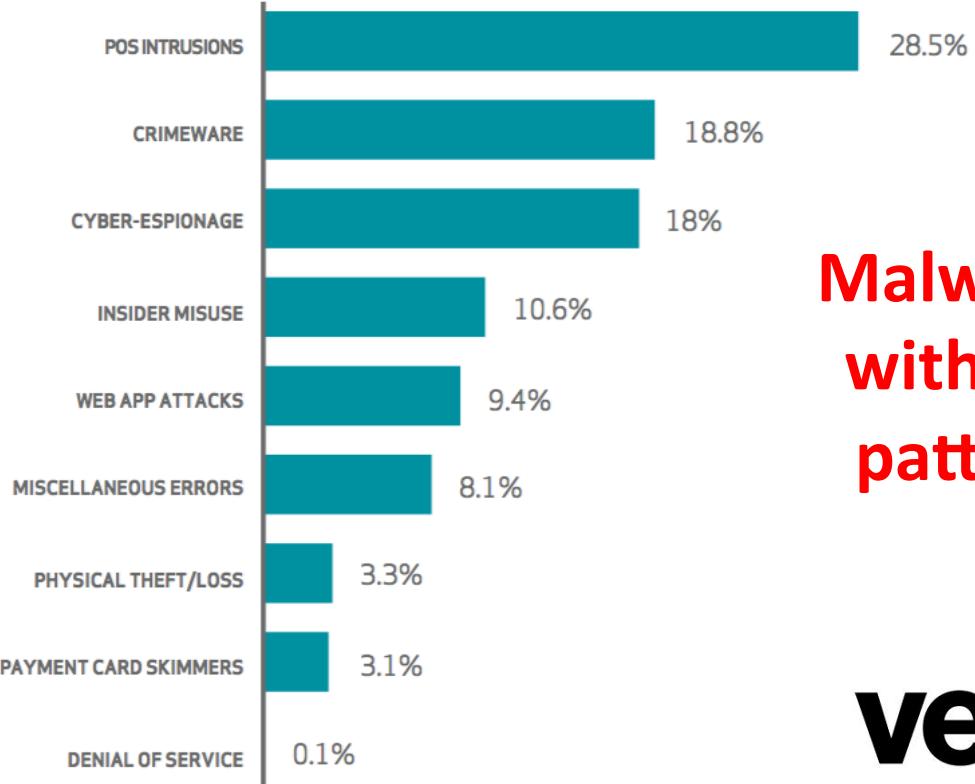
Whitelisting



splunk>

Look for apps
on
splunkbase!

Bit9



**Malware: involved
with top 3 attack
patterns in DBIR
2015**

verizon ✓

Obligatory
DBIR slide...

Back to these breaches...

Registry Entries

System Event Logs

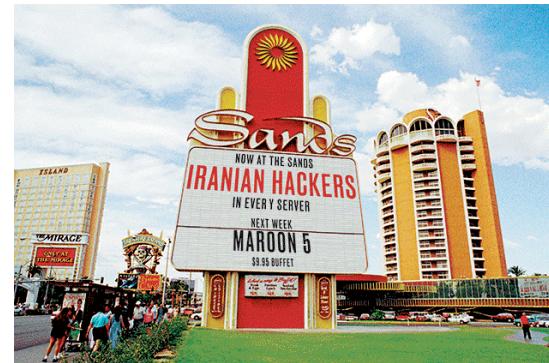
New Files

Security Event Logs

New Services

Comms/Running Proc

Known Vulns/Apps



Endpoint-Based Malware

Common malware leaves quite a trail...

Registry Entries

Security Event Logs

System Event Logs

New Files

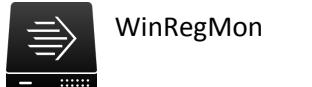
Known Vulns/Apps

New Services

Comms/Running Proc

We configure the forwarder to give us data of interest

Registry Entries



WinRegMon

System Event Logs



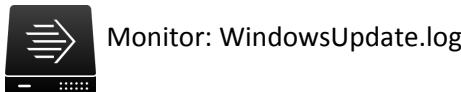
WinEventLog: System

Security Event Logs



WinEventLog: Security

Windows Update



Monitor: WindowsUpdate.log

New Files



WinEventLog: Security +
Auditing
Scripted Inputs

Known Vulns/Apps



Scripted Inputs or
WinHostMon

New Services



WinEventLog: System
and WinHostMon

Configuration
examples? See
demo & appendix

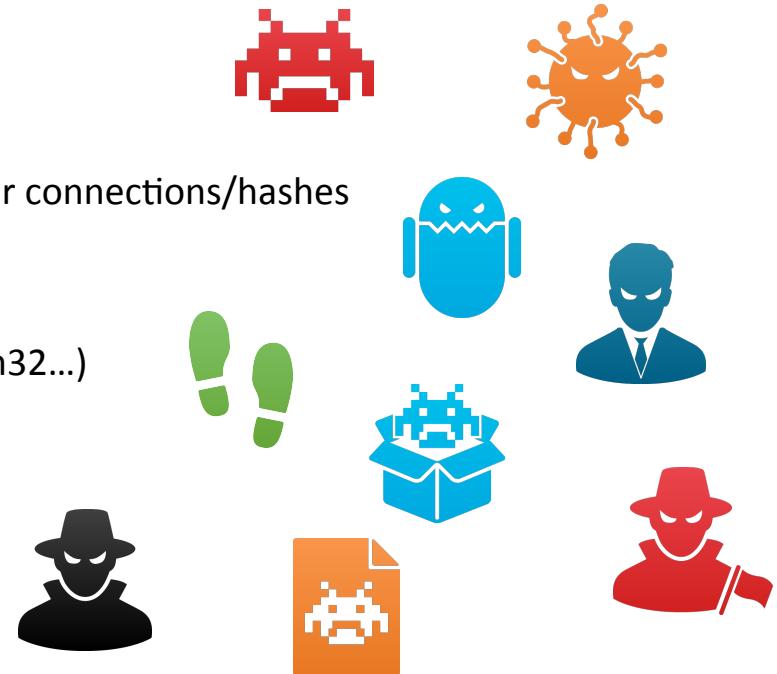
Comms/Running Proc



TA-Microsoft-Sysmon
Stream, WinHostMon

What could we look for?

- ANY new Windows services
- Registry being written to where it should not
- Users that shouldn't be used
- Unusual/unapproved processes being launched and their connections/hashes
- Unusual/unapproved ports/connections in use
- Unapproved USB devices being inserted
- New files in places they should not be (Windows\System32...)
- Files that look like one thing but are really another
- New drive letters being mapped
- Lack of recent Windows updates
- Versions of software known to be vulnerable
- ...and more



INSTANT, GRANULAR DATA ABOUT COMMON BEHAVIOR OF WINDOWS MALWARE!

Reconnaissance

Delivery

Installation

Actions on Objectives

Weaponization

Exploitation

Command & Control (C2)

Obligatory Kill
Chain slide...

Threat intelligence

Network
Activity/Security

Endpoint
Activity/Security

Auth - User Roles



115.29.46.99/32,zeus_c2s
61.155.30.0/24,cymru_http

Subject: new commission report breakdown
From: Jose Dave <jose.dave@buttercupgames.com>
To: <chris.gilbert@buttercupgames.com>
Content-type: multipart/mixed;
Content-type: application/pdf; name="Q2_commission.pdf"

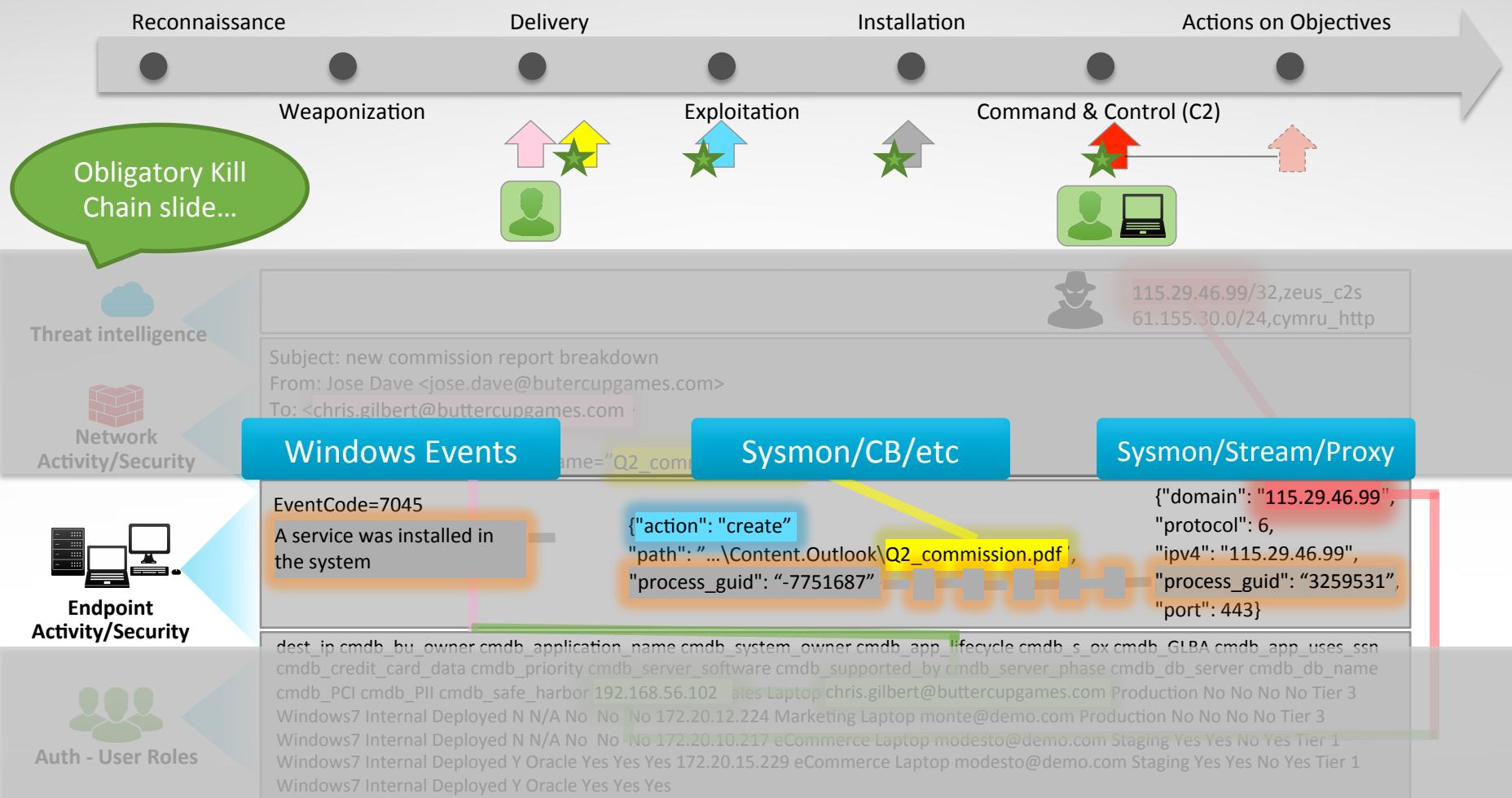
EventCode=7045

A service was installed in
the system

{"action": "create"
"path": "...\\Content.Outlook\\Q2_commission.pdf",
"process_guid": "-7751687"}

{"domain": "115.29.46.99",
"protocol": 6,
"ipv4": "115.29.46.99",
"process_guid": "3259531",
"port": 443}

dest_ip	cmdb_BU	cmdb_owner	cmdb_application_name	cmdb_system_owner	cmdb_app_lifecycle	cmdb_s_ox	cmdb_GLBA	cmdb_app_uses_ssl	cmdb_credit_card_data	cmdb_priority	cmdb_server_software	cmdb_supported_by	cmdb_server_phase	cmdb_db_name	cmdb_PCI	cmdb_PII	cmdb_safe_harbor	ales	Laptop	chris.gilbert@buttercupgames.com	Production	No	No	No	Tier 3
192.168.56.102	N	N/A	No	No	172.20.12.224	Marketing	Laptop	monte@demo.com	Production	No	No	No	No	No	Tier 3	Windows7	Internal	Deployed	N	N/A	No	No	Yes	Tier 1	
172.20.10.217	N	N/A	No	No	172.20.15.229	eCommerce	Laptop	modesto@demo.com	Staging	Yes	Yes	No	Yes	Yes	Tier 1	Windows7	Internal	Deployed	Y	Oracle	Yes	Yes	Yes	Tier 1	



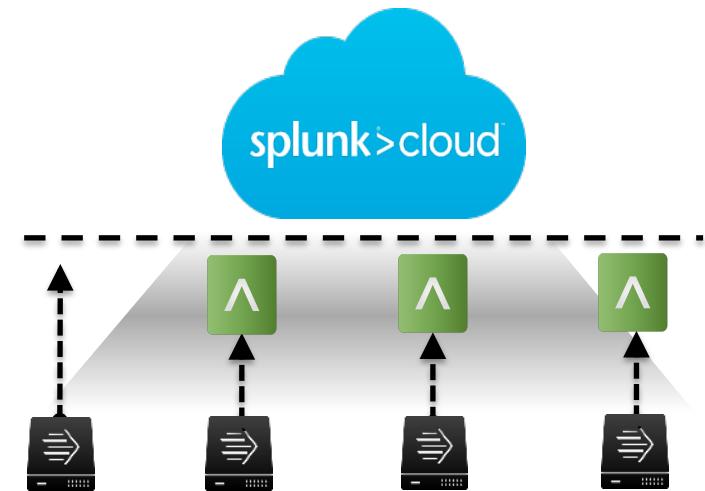
.conf2015

Demo, Part II

splunk®

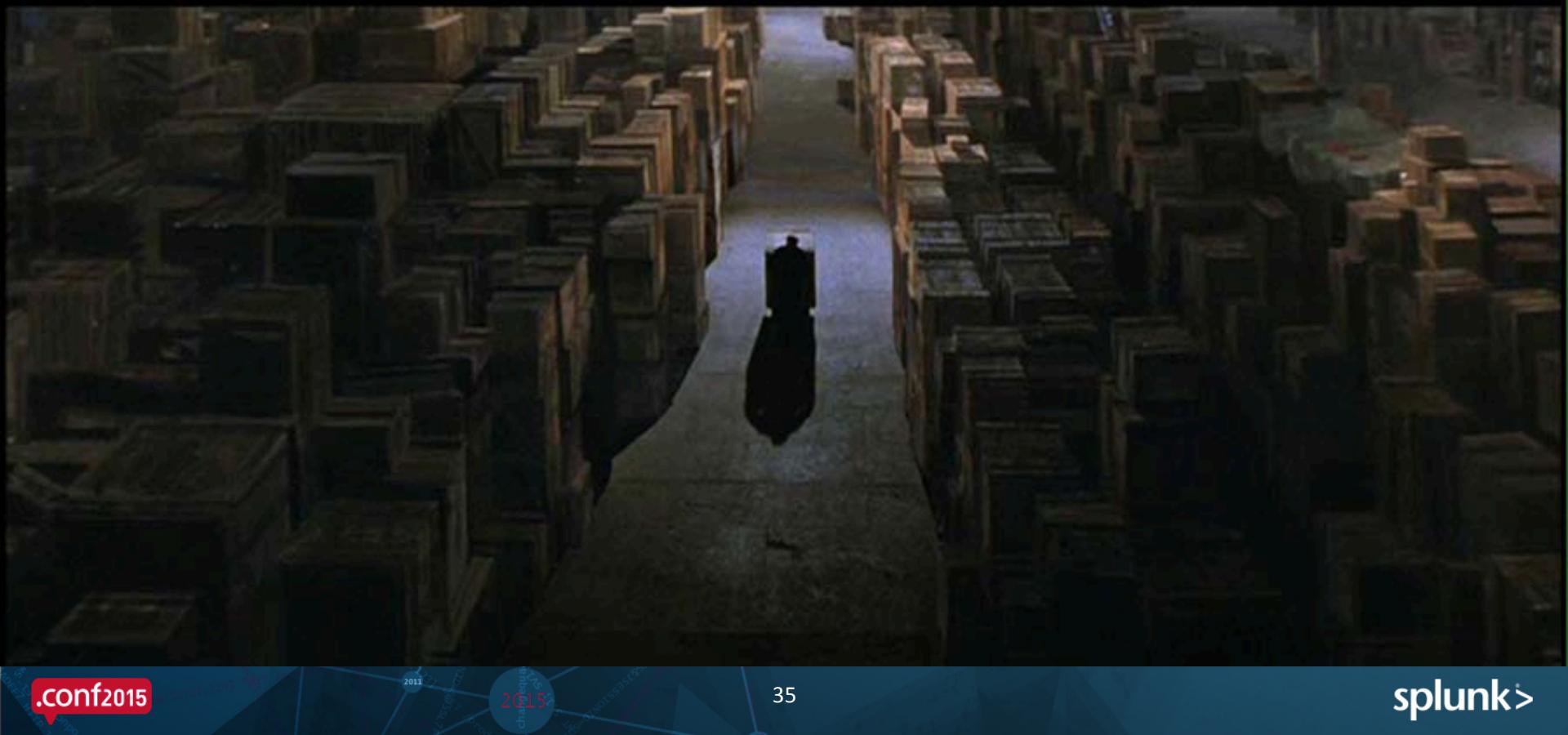
Use Case 2: UF for ATM Security + Fraud

- Bank uses ATMs that are Windows-based
- Each ATM has a UF installed, securely sending data to intermediate forwarder on prem and then up to Splunk Cloud
- Data retrieved from custom ATM logs – can understand what's going on within 1-2 seconds
- Customer reps can see what the problem is easily
- Understand baseline – when are ATMs popular? Handle the cash levels
- Understand fraud – has someone stolen a card + PIN and hitting ATMs in close clusters? “Superman” correlation
- Conversion Opp: know that a 3rd-party bank customer hits an bank ATM every Friday for \$200



Regional Bank in NE US

How about inventory + vulnerabilities?



How about inventory + vulnerabilities?



Two ways to get installed apps, there are more...

Search Pivot Reports Alerts Dashboards

New Search

```
index=main sourcetype=*sysmon* EventCode != 3 | dedup app | stats values(app) by host
```

84 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM)

Events Patterns Statistics (1) Visualization

100 Per Page Format Preview

Microsoft Sysmon

host values(app)

isengupta-T430s

```
C:\PROGRA~2\Symantec\SYMANT~1\121100~1.105\Bin\DWHWizrd.exe
C:\PROGRA~3\WebEx\WebEx1526\WebexStm\CiscoWebexVideoService.exe
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe
C:\Program Files (x86)\Common Files\AdobeARM\1.0\AdobeARM.exe
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE
C:\Program Files (x86)\Evernote\Evernote\Evernote.exe
C:\Program Files (x86)\Evernote\Evernote\EvernoteTray.exe
C:\Program Files (x86)\Google\Chrome\Application\44.0.2403.157\Installer\setup.exe
C:\Program Files (x86)\Google\Chrome\Application\45.0.2454.85\Installer\setup.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Update\1.3.28.13\GoogleCrashHandler.exe
C:\Program Files (x86)\Google\Update\1.3.28.13\GoogleCrashHandler64.exe
C:\Program Files (x86)\Google\Update\1.3.28.13\GoogleUpdateOnDemand.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Program Files (x86)\Google\Update\Install\{28A0F4A6-439E-43B9-BC7B-5026D9055161}\45.0.2454.85_44.0.24
C:\Program Files (x86)\Lenovo\Access Connections\AcHelper4.exe
C:\Program Files (x86)\Lenovo\Access Connections\AcWin7Hpr.exe
C:\Program Files (x86)\Lenovo\Access Connections\SvcGuiHpr.exe
C:\Program Files (x86)\Lenovo\Customer Feedback Program\Lenovo.TVT.CustomerFeedback.Agent.exe
C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE
C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE
C:\Program Files (x86)\Microsoft Office\Office14\POWERPNT.EXE
C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
C:\Program Files (x86)\Mozilla Firefox\firefox.exe
C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe
C:\Program Files (x86)\Skype\Phone\Skype.exe
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.1000.157.105\Bin\SavUI.exe
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.1000.157.105\Bin\ccSvchst.exe
C:\Program Files (x86)\Windows Media Player\wmplayer.exe
C:\Program Files\Lenovo\Lenovo Solution Center\app\LSCService.exe
C:\Program Files\Lenovo\Lenovo Solution Center\ann\SCTaskService.exe
```

Search Pivot Reports Alerts Dashboards

New Search

```
index=* sourcetype="Script:InstalledApps" | eval nameversion=Publisher.".".DisplayName.".".DisplayVersion | stats list(nameversion) by host
```

121 events (9/6/15 11:00:00.000 PM to 9/7/15 11:00:50.000 PM)

Events Patterns Statistics (3) Visualization

20 Per Page Format Preview

host list(nameversion)

barnstorming

```
SplunkUniversalForwarder:6.2.3.264376
NVIDIA:NVIDIA:1.10.8
NVIDIA:NVIDIA:2.1002.109.706
NVIDIA:NVIDIA:1.10.8
NVIDIA:NVIDIA:307.83
NVIDIA:NVIDIA:307.83
Microsoft:Microsoft:2.0.50728
AVG:AVG:15.0.6086
Microsoft:Microsoft:4.5.50938
AVG:Visual:14.0.0.1
Microsoft:Microsoft:5.1.40728.0
Microsoft:Microsoft:4.5.50938
ActiveState:ActivePerf:5.16.1601
Microsoft:Microsoft:9.0.30729.5.161
Microsoft:Microsoft:9.0.30729.4148
AVG:AVG:15.0.4397
Gadwin:Gadwin:5.3.1.0
Igor:7-Zip:9.20.0.0
VMware:VMWare:3.5.2
Piriform:Recuva:1.51
AVG:AVG:2015.0.6086
```

choppercommand

```
Microsoft:Microsoft:4.0.30319
Intel:Intel:1.24.388.1
Microsoft:Microsoft:4.5.0216.0
Microsoft:PlayReady:1.3.0
Fresco:Fresco:3.5.93.0
Microsoft:Microsoft:4.0.30319
Oracle:Oracle:4.3.14
Microsoft:Microsoft:5.1.30514.0
Apple:Bonjour:3.0.0.10
SplunkUniversal:5.0.4.172409
Apple:Apple:6.1.0.13
Igor:7-Zip:9.20.0.0
Microsoft:Microsoft:10.0.40219
Apple:iTunes:11.0.2.26
Microsoft:Microsoft:4.5.216.0
Microsoft:Microsoft:4.0.30319
Microsoft:Microsoft:4.0.30319
```

Scripted Input from Windows TA or
WinHostMon

What versions of what exist on my network?

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search

Save As ▾ Close

index=* sourcetype="Script:InstalledApps" | rex ".*DisplayName=(?<dnname>.*)" | eval nameversion=Publisher.".":dnname.".":DisplayVersion | stats dc(host) by nameversion

Last 24 hours ▾

121 events (9/6/15 11:00:00.000 PM to 9/7/15 11:04:52.000 PM)

Job ▾ II ■ ▶ ↴ ↴ ⚡ Fast Mode ▾

Events Patterns Statistics (67) Visualization

Scripted Input from Windows TA or WinHostMon

20 Per Page ▾ Format ▾ Preview ▾

nameversion ▾

	dc(host) ▾
Igor:7-Zip 9.20 (x64 edition):9.20.00.0	3
Microsoft:Microsoft .NET Framework 4.5.1:4.5.50938	2
Microsoft:Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148:9.0.30729.4148	2
Microsoft:Microsoft Visual J# 2.0 Redistributable Package - SE (x64):2.0.50728	2
AMD:AMD Steady Video Plug-In:2.06.0000	1
AVG:AVG 2015:15.0.4392	1
AVG:AVG 2015:15.0.6086	1
AVG:AVG 2015:2015.0.6086	1
AVG:Visual Studio 2012 x64 Redistributables:14.0.0.1	1
ActiveState:ActivePerl 5.16.1 Build 1601 (64-bit):5.16.1601	1
Adobe:Adobe Anchor Service x64 CS4:2.0	1
Adobe:Adobe CMaps x64 CS4:2.0	1
Adobe:Adobe CSI CS4 x64:1	1
Adobe:Adobe Drive CS4 x64:1	1
Adobe:Adobe Fonts All x64:2.0	1
Adobe:Adobe InDesign CS4 Icon Handler x64:6.0	1
Adobe:Adobe Linguistics CS4 x64:4.0.0	1
Adobe:Adobe PDF Library Files x64 CS4:9.0	1
Adobe:Adobe Photoshop CS4 (64 Bit):11.0	1
Adobe:Adobe Photoshop Lightroom 5.2 64-bit:5.2.1	1

Do I have known vulnerable software on endpoints?

Do I have known
vulnerable
software on
endpoints?

Hash data from apps

The screenshot shows the Splunk App Search & Reporting interface. The search bar contains the command: `index=main host="isengupta-T430s" Image!="svchost.exe" Image!="splunk*" | rex mode=sed field=Hashes "s/SHA1//g" | stats dc(Hashes) as numhashes,values(Hashes) as SHA1 by Image | where numhashes>0 | sort -numhashes`. The search results show 62,851 events from 9/1/15 to 9/2/15. The results table includes columns for Image, numhashes, and SHA1. Two entries for 'chrome.exe' are highlighted with red boxes: one with SHA1 `A8AF113914CD161FF6B33B8968DB31A427E66C4DD09A3AD4D958075F5E2A42DA01A64917E6BCC543` and another with `A4288CD5600C8670ED666F623702F76550C5DAD4`. A pink arrow points to the second hash. A green speech bubble on the right says 'Correlate hash with threat intel'. The interface also features tabs for Events, Patterns, Statistics (87), and Visualization.

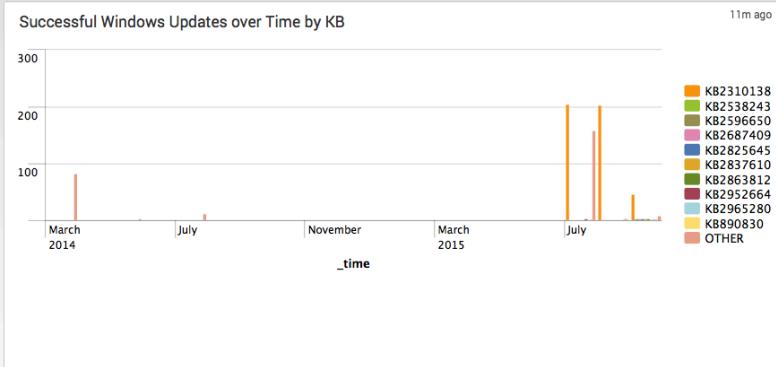
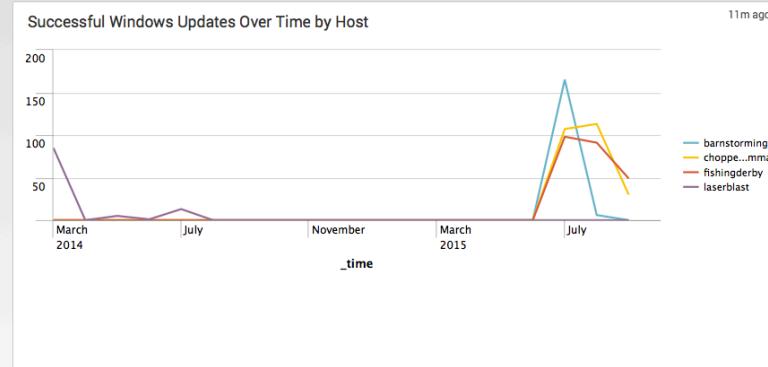
Image	numhashes	SHA1
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2	A8AF113914CD161FF6B33B8968DB31A427E66C4DD09A3AD4D958075F5E2A42DA01A64917E6BCC543
C:\PROGRA~2\Symantec\SYMANTE~1\121100~1.105\Bin\DWHWizrd.exe	1	A4288CD5600C8670ED666F623702F76550C5DAD4
C:\PROGRA~3\WebEx\WebEx\1526\WebexStm\CiscoWebexVideoService.exe	1	328D2AC05833A7C24A075E081E48732C2D46FE28
C:\PROGRA~3\WebEx\WebEx\1526\atshell.exe	1	FBFA1D5A8023E6C69258B2B6C27A054384D0012D
C:\Program Files (x86)\Adobe\Adobe Creative Cloud\HEX\Adobe CEF Helper.exe	1	CD1DE24DB4000A94028E84F6C8A2705390D2682B
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe	1	5EA3B6B57EADC1A8DBD6BF60AB4CAD40
C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe	1	9B5C1DD5C2F7C30A6A303C03640
C:\Program Files (x86)\Atlassian\HipChat\hipchat.exe	1	A637C3B4AC793E3456C1F6C1
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	1	E9E1551426148EE9D7A6CD4
C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\AAM Updates Notifier.exe	1	A304928311BF24C9123D381
C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\updatestartuputility.exe	1	E056DDDC15C841CC06B5
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe	1	F147BB4A573E5F
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\distnoted.exe	1	BD893147AC95BCEA1C1CCEBA54661C477
C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceHelper.exe	1	EBB62A866F7DFDA5467694E23DBD74E52721EC36
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	1	835E982347DB919A681BA12F3891F62152E50F0D
C:\Program Files (x86)\Evernote\Evernote\Evernote.exe	1	A51C893266D85FF171629C137C63BEFB291A5565
C:\Program Files (x86)\Evernote\Evernote\EvernoteTray.exe	1	D00C5236000A3D00A4A569F61FAB1770C1C40672

Windows Update data

CIP 007-R2 Patch Management

Display Windows Update and RHN Status

Edit More Info



Successful Windows Updates by Host

11m ago

host	Trend	count
choppercommand		250
fishingderby		238
barnstorming		171
laserblast		104

Update Lag

11m ago

host	Last Update Time	Days Since Last Update
laserblast	03/08/14 03:02:09	549
barnstorming	08/13/15 03:08:16	26
fishingderby	09/04/15 00:19:27	4
choppercommand	09/04/15 00:40:51	4

Successful Windows Updates by KB Name

11m ago

package_title	host	_time	Trend	count
Security Update for Microsoft Office Visio 2007 suites (KB2965280)	fishingderby	2015-09-08 14:11:59		2
Security Update for Microsoft Office Visio 2007 suites (KB2965280)	fishingderby	2015-09-08 14:11:59		1
Security Update for Microsoft Office 2007 suites (KB2825645)	fishingderby	2015-09-08 14:11:50		2
Security Update for Microsoft Office 2007 suites (KB2825645)	fishingderby	2015-09-08 14:11:50		1
Security Update for Microsoft Office 2007 suites (KB2596650)	fishingderby	2015-09-08 14:08:33		2
Security Update for Microsoft Office 2007 suites (KB2596650)	fishingderby	2015-09-08 14:08:33		1
Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	fishingderby	2015-09-08 14:08:28		2
Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	fishingderby	2015-09-08 14:08:28		1
Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB2863812)	fishingderby	2015-09-08 14:05:14		2
Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB2863812)	fishingderby	2015-09-08 14:05:14		1

< prev 1 2 3 4 5 6 7 8 9 10 next >

Windows Update Data (two sourcetypes)

The screenshot shows a Splunk search interface. The search bar contains the query: `eventtype="Update_Successful" package=* host="" sourcetype="WinEventLog:System" | rex fie`. Below the search bar, a message indicates `✓ 2 events (1/9/10 8:02:25.000 PM to 9/8/15 2:16:31.000 PM)`. The interface includes tabs for Events (2), Patterns, Statistics, and Visualization. Below these tabs are buttons for Format Timeline, Zoom Out, Zoom to Selection, and Deselect. The main area displays the title "Monitor: WinEventLog:System" in red. The results table has columns for Hide Fields, All Fields, Time, and Event. The first event listed is from 09/08/2015 at 02:08:28 PM, with details including LogName=System, SourceName=Microsoft-Windows-WindowsUpdate, EventCode=19, EventType=4, Type=Information, ComputerName=fishingderby, User=SYSTEM, Sid=S-1-5-18, and SidType=1. It also mentions TaskCategory=Windows Update Agent, OpCode=Installation, RecordNumber=83349, Keywords=Installation, Success, and Message=Installation Successful: Windows distributable Package (KB2538243). A "Collapse" link is present at the bottom of this event row. The second event is partially visible. On the left, there are sections for Selected Fields (host, source, sourcetype) and Interesting Fields (ComputerName, dest, dvc, dvc_nt_host, event_id, EventCode, eventtype, EventType). The "List" and "Format" dropdowns are set to List, and the "20 Per Page" dropdown is set to 20.

Windows Port Data

New Search

index=main sourcetype="Script:ListeningPorts" host=* | eval porttrans=dest_port.".".transport | regex dest_port="^\d+\$" | stats dc(host) as numhosts,values(host) by porttrans

1,391 events (9/7/15 9:00:00.000 PM to 9/8/15 9:12:11.000 PM)

Events Patterns Statistics (35) Visualization

20 Per Page ▾ Format ▾ Preview ▾

porttrans ▾ numhosts ▾ values(host) ▾

porttrans	numhosts	values(host)
135:TCP	4	barnstorming choppercommand fishingshockey laserblast
139:TCP	4	barnstorming choppercommand fishingshockey laserblast
445:TCP	4	barnstorming choppercommand fishingshockey laserblast
49152:TCP	4	barnstorming choppercommand fishingshockey laserblast
49153:TCP	4	barnstorming choppercommand fishingshockey laserblast
49154:TCP	4	barnstorming choppercommand fishingshockey laserblast
5357:TCP	4	barnstorming choppercommand fishingshockey laserblast
8089:TCP	4	barnstorming choppercommand fishingshockey laserblast
49155:TCP	3	barnstorming fishingshockey laserblast
3389:TCP	2	choppercommand fishingshockey

Scripted input from Windows TA or WinHostMon

Windows Port Data

Time	Event
> 9/8/15 9:00:56.000 PM	09/08/2015 21:00:56 transport=TCP dest_ip=[::] dest_port=3389 pid=1144 host = choppercommand index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 9:00:56.000 PM	09/08/2015 21:00:56 transport=TCP dest_ip=0.0.0.0 dest_port=3389 pid=1144 host = choppercommand index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 8:24:22.000 PM	09/08/2015 20:24:22 transport=TCP dest_ip=[::] dest_port=3389 pid=1556 host = fishingderby index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 8:24:22.000 PM	09/08/2015 20:24:22 transport=TCP dest_ip=0.0.0.0 dest_port=3389 pid=1556 host = fishingderby index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 8:00:56.000 PM	09/08/2015 20:00:56 transport=TCP dest_ip=[::] dest_port=3389 pid=1144 host = choppercommand index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 8:00:56.000 PM	09/08/2015 20:00:56 transport=TCP dest_ip=0.0.0.0 dest_port=3389 pid=1144 host = choppercommand index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 7:24:22.000 PM	09/08/2015 19:24:22 transport=TCP dest_ip=[::] dest_port=3389 pid=1556 host = fishingderby index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 7:24:22.000 PM	09/08/2015 19:24:22 transport=TCP dest_ip=0.0.0.0 dest_port=3389 pid=1556 host = fishingderby index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts
> 9/8/15 7:08:56.000 PM	09/08/2015 19:08:56 transport=TCP dest_ip=[::] dest_port=3389 pid=1144 host = choppercommand index = main linecount = 1 source = C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listeni... sourcetype = Script:ListeningPorts

PID data=easy correlation to process responsible

Or use sysmon...

Endpoint info critical to CSC (SANS) 20

- 1 & 2: Log hardware info, running procs/svcs
- 3: Scripted inputs to check for config issues
- 4: Evaluate processes/services for vulns
- 5: Look for malicious new services/processes
- 11: Look for malicious ports/protocols
- 12: Look for local use of priv accounts
- 14: Gather windows events/*NIX logs
- 16: Evaluate use of screensaver locks
- 17: Identify lapses in local encryption

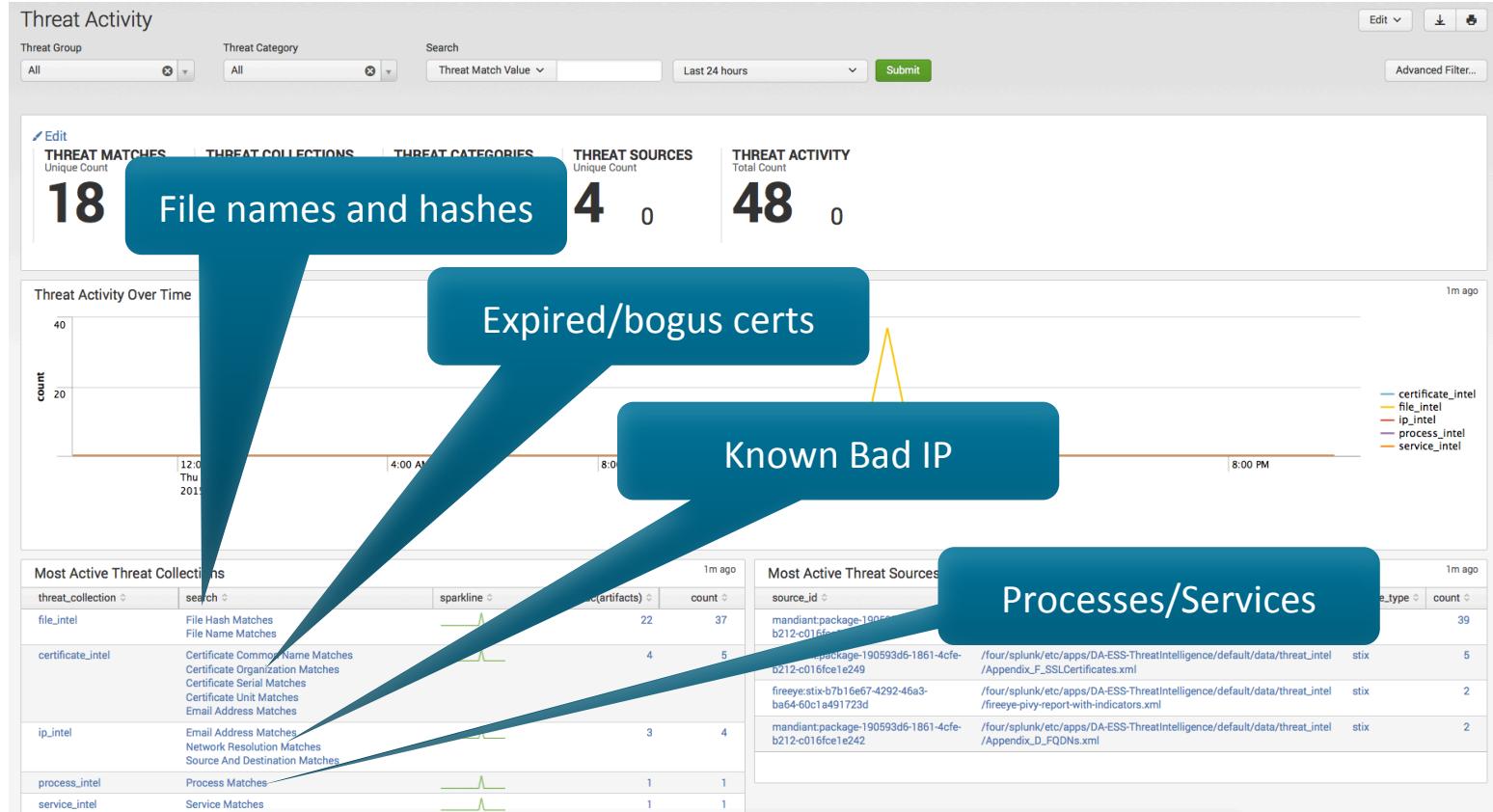
You could do **all** of that with the Universal Forwarder.

- 1 Inventory of Authorized & Unauthorized Devices
- 2 Inventory of Authorized & Unauthorized Software
- 3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- 4 Continuous Vulnerability Assessment & Remediation
- 5 Malware Defenses
- 6 Application Software Security
- 7 Wireless Access Control
- 8 Data Recovery Capability
- 9 Network Configuration Assessment & Configuration to Fill Gaps such as firewalls, Routers, and Switches
- 11 Limitation and Control of Network Ports, Protocols and Services
- 12 Controlled Use of Administration Privileges
- 13 Boundary Defense
- 14 Maintenance, Monitoring & Analysis of Audit Logs
- 15 Controlled Access Based on the Need to Know
- 16 Account Monitoring & Control
- 17 Data Protection
- 18 Incident Response and Management
- 19 Secure Network Engineering
- 20 Penetration Tests and Red Team Exercises

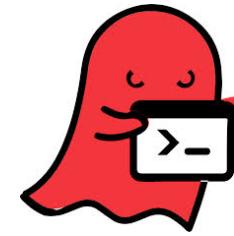
Obligatory
SANS 20
slide...



Threat Intelligence, you say?



Endpoint vulns can be found if you google what to look for...



A checker (site and tool) for CVE-2014-0160.

Public site at <https://filippo.io/Heartbleed/>

Tool usage:

```
Heartbleed [-service="service_name"] example.com[:443]
Heartbleed service_name://example.com[:443]
```

```
$: 0 - SAFE; 1 - VULNERABLE; 2 - ERROR. (recently changed)
```

Online FAQ for an explanation of error messages including TIMEOUT and BROKEN PIPE.

If a name is specified besides https , the tool checks the specified service using STARTTLS.
It will need to specify the correct port.

To check for the CVE-2014-6271 vulnerability

```
env x="() ( ); echo vulnerable` bash -c "echo this is a test"
```

It should NOT echo back the word vulnerable.

To check for the CVE-2014-7169 vulnerability

(warning: if yours fails it will make or overwrite a file called /tmp/echo that you can delete after, and need to delete before testing again)

```
cd /tmp; env X="() { (a)>>` bash -c <echo date>; cat echo
```

It should say the word date then complain with a message like cat: echo: No such file or directory. If instead it tells you what the current datetime is then your system is vulnerable.

SSLv3 Test Using cURL

```
:1 -v3 -X HEAD https://www.example.com
```

Check the output, you want to see something similar

```
* SSL peer handshake failed
```

Rather than something like this:

```
* SSL 3.0 connection using SSL NULL WITH NULL NULL
```

```
#!/bin/bash
#version 3
echo "Installed glibc version(s)"
rver0
for glibc_nvr in $( rpm -q --qf '%{name}-%{version}-%{release}.%{arch}\n' glibc ); do
    glibc_ver=$( echo "$glibc_nvr" | awk '{print $2}' )
    glibc_ma=$( echo "$glibc_ver" | awk '{ print $1 }' )
    glibc_mi=$( echo "$glibc_ver" | awk '{ print $2 }' )
    echo -n " $glibc_nvr: "
    if [ "$glibc_ma" -gt 2 ] || ( [ "$glibc_ma" -eq 2 ] &amp; [ "$glibc_mi" -ge 19 ] ); then
        # fixed upstream version
        echo "not vulnerable"
    else
        # all RHEL updates include CVE in rpm changelog
        if rpm -q --changelog "$glibc_nvr" | grep -q 'CVE-2015-0235'; then
            echo "not vulnerable"
        else
            echo "vulnerable"
            rv=1
        fi
    done
    if [ $rv -ne 0 ]; then
        cat <>202
    fi
done
exit $rv
```

This system is vulnerable to CVE-2015-0235. <<https://access.redhat.com/security/cve/CVE-2015-0235>>

Please refer to <<https://access.redhat.com/articles/133213>> for remediation steps

EOP

fi

Remember this?

shellshock



- Publicly announced on **9/24/2014**.
- One Vulnerability Management vendor had a plugin on **9/25**. That's pretty good!
- Others followed on **9/26** and **9/29** – not so good.
- These **require authenticated** scans.

Google shellshock vulnerability detection

Web News Videos Images Shopping More Search tools

About 78,600 results (0.40 seconds)

Scholarly articles for **shellshock vulnerability detection**
Review: Screening for vulnerability to psychological ... - Jones - Cited by 65

How to Detect the ShellShock Bash Bug on Your Internal ...
www.tripwire.com › Home › Featured Articles › Tripwire › Sep 26, 2014 - As you're probably aware, a new vulnerability (CVE-2014-6271) was recently disclosed that affects Bash—a common shell used by most ...

Shellshock BASH Vulnerability Tester
<https://shellshocker.net/> ▾ Shellshock BASH Vulnerability tester. Are you vulnerable to #shellshock? (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, ...)

Shellshock: Prevent, Detect and Respond
<https://securityintelligence.com/shellshock-prevent-detect-and-respond/> ▾ To help organizations address this vulnerability, IBM provides security solutions that can help prevent, detect and respond to the Shellshock threat.

Shellshock | Tenable Network Security
www.tenable.com/shellshock ▾ Tenable Network Security ▾ CVE 2014-6271 and CVE-2014-7169, known as "Shellshock" in the media, affects Linux, ... via SSH via an authenticated scan, and to test for the vulnerability via HTTP(s). ... Tenable Issues Shellshock Detection Plugins, Wizard, Dashboard ...

Tenable Issues Shellshock Detection Plugins, Wizard ...
<https://www.tenable.com/.../tenable-issues-shell...> ▾ Tenable Network Security ▾ Sep 25, 2014 - As many of you know, a major vulnerability was discovered yesterday, CVE 2014-6271 and CVE 2014-7169, known as "Shellshock" in the ...

Custom Option Profile To Detect Bash Shellshock - Hide the ...
<https://community.qualys.com/.../custom-option-profile-to-detect...> ▾ Qualys ▾ Oct 9, 2014 - A new option profile in the Qualys Vulnerability Management (VM) Option Profile library can be used to detect instances of the Shellshock ...

Qualys Releases Detection for Bash Shellshock Vulnerability
www.qualys.com/.../Newsroom/News Releases/USA/2014/Qualys/... ▾ Qualys ▾ Sep 29, 2014 - Critical Vulnerability Detected via Qualys Vulnerability Management Cloud offering and Qualys FreeScan Service.

Remember this? Could



shellshock splunk

- Publicly announced on **9/24/2014**.
- One Vulnerability Management vendor had a plugin on **9/25**. That's pretty good!
- Others followed on **9/26** and **9/29** – not so good.
- These require **authenticated** scans

make this process more timely?

Google shellshock vulnerability detection

Web News Videos Images Shopping More Search tools

About 78,600 results (0.40 seconds)

scholarly articles for shells(R) vulnerability detection

Screening for vulnerability to psychological ... - Jones - Cited by 65

How to Detect the ShellShock Bug on Your Internal ...

What you're probably aware, a new vulnerability (CVE-2014-6271) was disclosed that affects Bash—a common shell used ...

Shellshock Bash Vulnerability Tester

https://securityintelligence.com/shellshock-prevent-detect-and-respond/

To help organizations address this vulnerability, IBM provides security solutions that can help prevent, detect and respond to the Shellshock threat.

Shellshock | Tenable Network Security

www.tenable.com/shellshock ▾ Tenable Network Security ▾ CVE 2014-6271 and CVE-2014-7189, known as "Shellshock" in the media, affects Linux, ... via SSH via an authenticated scan, and to test for the vulnerability via HTTP(s). ... Tenable Issues Shellshock Detection Plugins, Wizard, Dashboard ...

Tenable Issues Shellshock Detection Plugins, Wizard ...

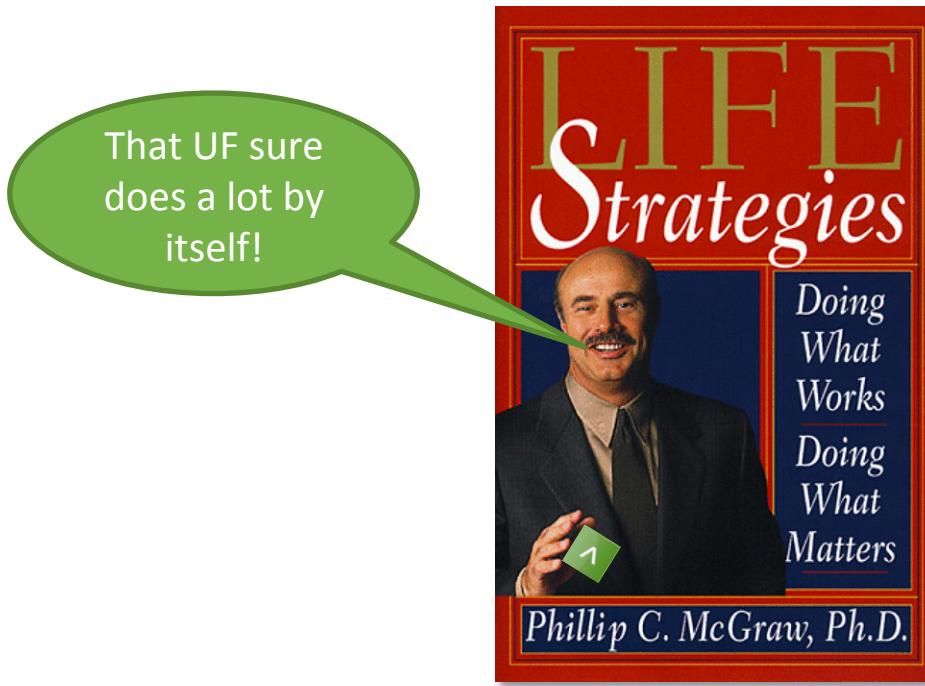
https://www.tenable.com/...enable-issues-shell... ▾ Tenable Network Security

Sep 25, 2014 - As many of you know, a major vulnerability was discovered yesterday, CVE-2014-6271, commonly known as "Shellshock". ...

Qualys Releases Detection for Bash Shellshock Vulnerability

www.qualys.com/.../Newsroom/News Releases/USA/2014/... Qualys ▾ Sep 29, 2014 - Critical Vulnerability Detected via Qualys Vulnerability Management Cloud offering and Qualys FreeScan Service.

The Universal Forwarder as self-help guru

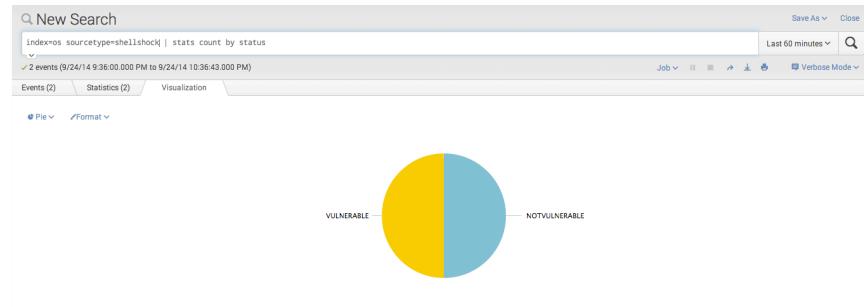


That UF sure
does a lot by
itself!

The Universal Forwarder as self-help guru



- If you had the Splunk UF on all of your production *NIX servers...
- You could **very quickly** program them to find shellshock (or ghost, or poodle, or heartbleed).
- You avoid Vulnerability Management Vendor Lag
- You could then report on remediation efforts over time.
- **And** the data ingest would be very small.



5 Step Vulnerability Tracking Strategy

1. On day one, become aware of vulnerability
2. Google “how to detect <vulnerability>”
3. Adopt code via script (shell, batch, etc) and place into your Splunk deployment server
4. Forwarders run code and deliver results into Splunk indexers
5. Report on the results

A good step by step

Google search results for "splunk shellshock". The first result is a Splunk blog post titled "Finding shellshock (CVE-2014-6271, 7169, 7186, 7187 ...)". A green speech bubble points to this result with the text "A good step by step".

splunk shellshock

Web News Videos Images Shopping

About 7,630 results (0.35 seconds)

Splunk® IT Data Engine - splunk.com
Ad www.splunk.com/ ▾
Get Operational Intelligence from your IT Data with Splunk. More Info
You've visited splunk.com many times. Last visit: today
Free Download Product Company Solutions

Finding shellshock (CVE-2014-6271, 7169, 7186, 7187 ...)
blogs.splunk.com/.../finding-shellshock-cve-2014-6271-with-splu... ▾ Splunk ▾
Sep 24, 2014 · The second shellshock vulnerability, CVE-2014-7169, requires a different test. ... And basically – stop reading Splunk blogs and go patch bash.
You've visited this page 4 times. Last visit: 9/6/15

Splunk response to "shellshock" vulnerabilities | Splunk
www.splunk.com/view/SP-CAAANJN ▾ Splunk ▾
Sep 29, 2014 · Vulnerability Descriptions and Ratings. • Splunk Enterprise response to Bash "shellshock" parsing attack (CVE-2014-6271, CVE-2014-7169).

splunk>blogs

Blogs: Security

Finding shellshock (CVE-2014-6271, 7169, 7186, 7187) with Splunk forwarders

UPDATE 9/24/14 (evening): I changed the script a little bit to include platform information in the output by using the uname command and bash version information in the output with --version. This should work on Linux and OSX.

UPDATE 9/25/14: The first script below is specific to find the original shellshock: [CVE-2014-6271](#). The second shellshock vulnerability, [CVE-2014-7169](#), requires a different test. See the script later in the post to cover this.

UPDATE 9/26/14: A whole bunch of useful comments have been added to this post. I have added information at the end of the post in response. I have further updated the scripts. Also, I should point out – if you are looking for information about how Splunk products are affected (or not) by this vulnerability, the official source is, and will always be, our [Product Security Portal](#).

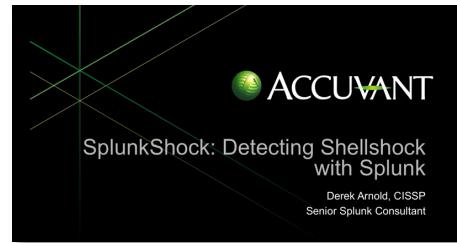
CATEGORIES

CATEGORY	POSTS
TIPS & TRICKS	950
SECURITY	176
LIFE AT SPLUNK	244
DEV	304
UI & DESIGN	43
CUSTOMERS	265
CIO BLOG	21
.CONF SPEAKERS	83
SPLUNKNEWS	100

Use Case 3: UF for Shellshock Tracking

(Large payment processing company)

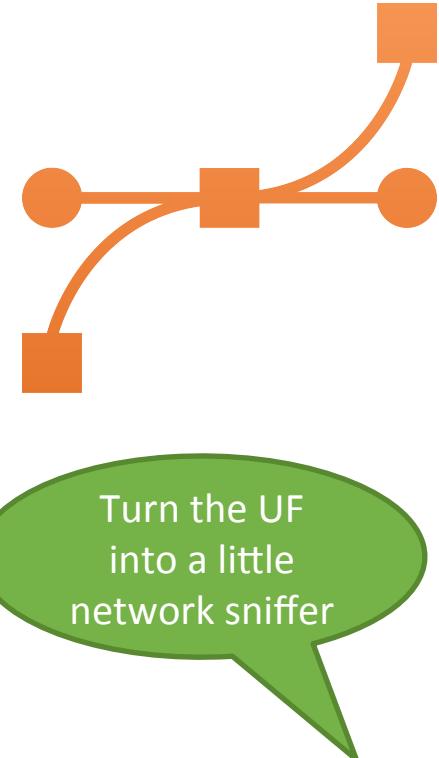
Shellshock on 20,000 Linux, Solaris, AIX servers tracked in Splunk



“We wrote it on the same day and ran it – it is really fundamental to our defense.” – Mark Graff, NASDAQ

How about wire data?

- Technology Add-on or TA (Splunk_TA_stream)
- Provides a new Data Input called “Wire Data”
 - passively captures traffic using a modular input
 - C++ executable called “Stream Forwarder” (streamfwd)
- Captures application layer (level 7) attributes
- Automatically decrypts SSL/TLS traffic using RSA keys



Stream Protocols/Platforms Supported

- UDP
- TCP
- HTTP
- FTP
- SMB
- NFS
- POP3
- SMTP
- LDAP/AD
- SIP
- XMPP
- AMQP
- MAPI
- IRC
- DNS
- DHCP
- RADIUS
- Diameter
- BitTorrent
- SMPP
- IMAP
- MySQL (login/cmd/query)
- Oracle (TNS)
- PostgreSQL
- Sybase/SQL Server (TDS)

Supports Windows 7 (64-bit), Windows 2008 R2 (64 bit), Linux (32-bit/64-bit) and Mac OSX (64-bit)

Nice try, Brodsky.



"a typical day at
the office..."

▼ Date Range

Between 09/01/2015 and 09/01/2015
00:00:00 24:00:00



TA-microsoft-sysmon



Splunk_TA_windows

All this endpoint Splunking will
blow up my license...

How much data?


Windows Sysinternals
TA-microsoft-sysmon


Microsoft
Splunk_TA_windows



“a typical day at the office...”

Date Range

Between and 00:00:00 24:00:00

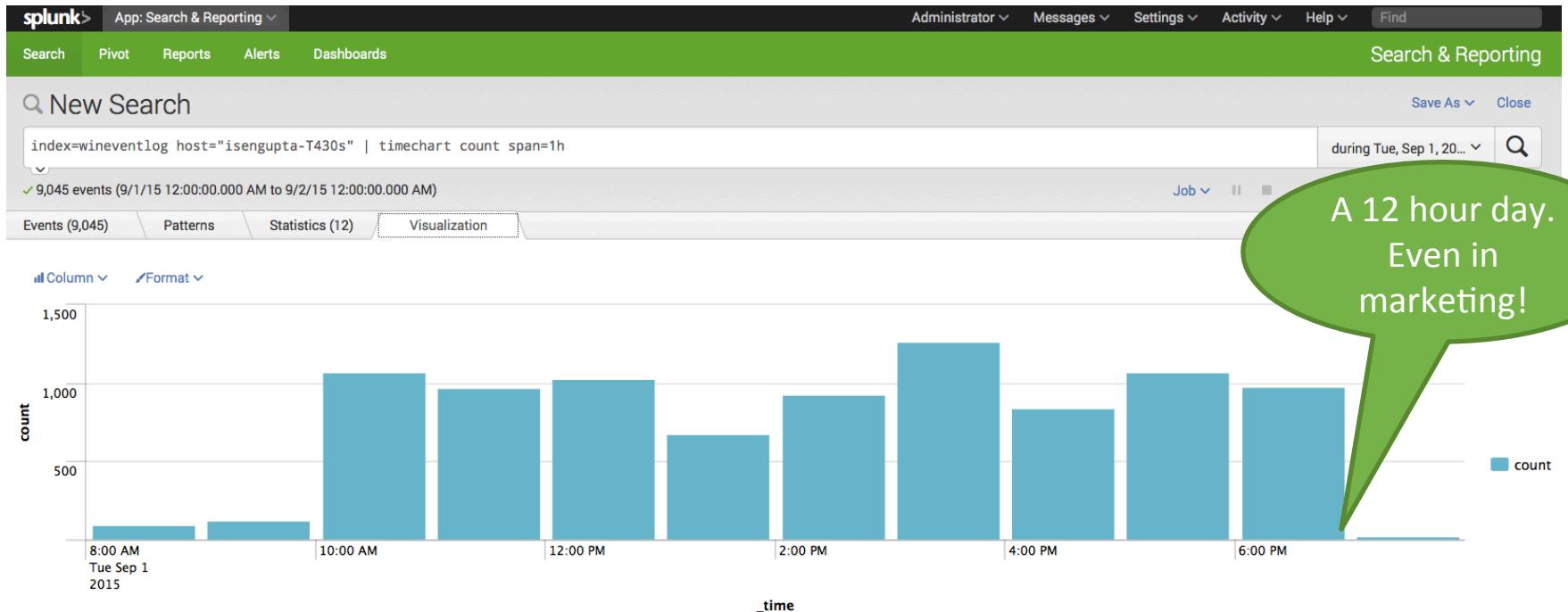
Apply


Ishaan Sengupta
Sr. Online Marketing Specialist at Splunk
San Francisco Bay Area | Internet

Current: Splunk
Previous: Reply.com, AnchorFree, Apollo Group
Education: University of California, Santa Cruz

[Connect](#) [Send Ishaan InMall](#) ▾ 183 connections

How much data?



How much data?

The screenshot shows the Splunk interface with a search query and its results. The search query is:

```
index=wineventlog host="isengupta-T430s" | eval length_in_bytes=len(_raw) | stats sum(length_in_bytes) as bytes by sourcetype | eval mbytes=(bytes/1024/1024) | eval mbytes=round(mbytes,2) | addcoltotals | fields - bytes
```

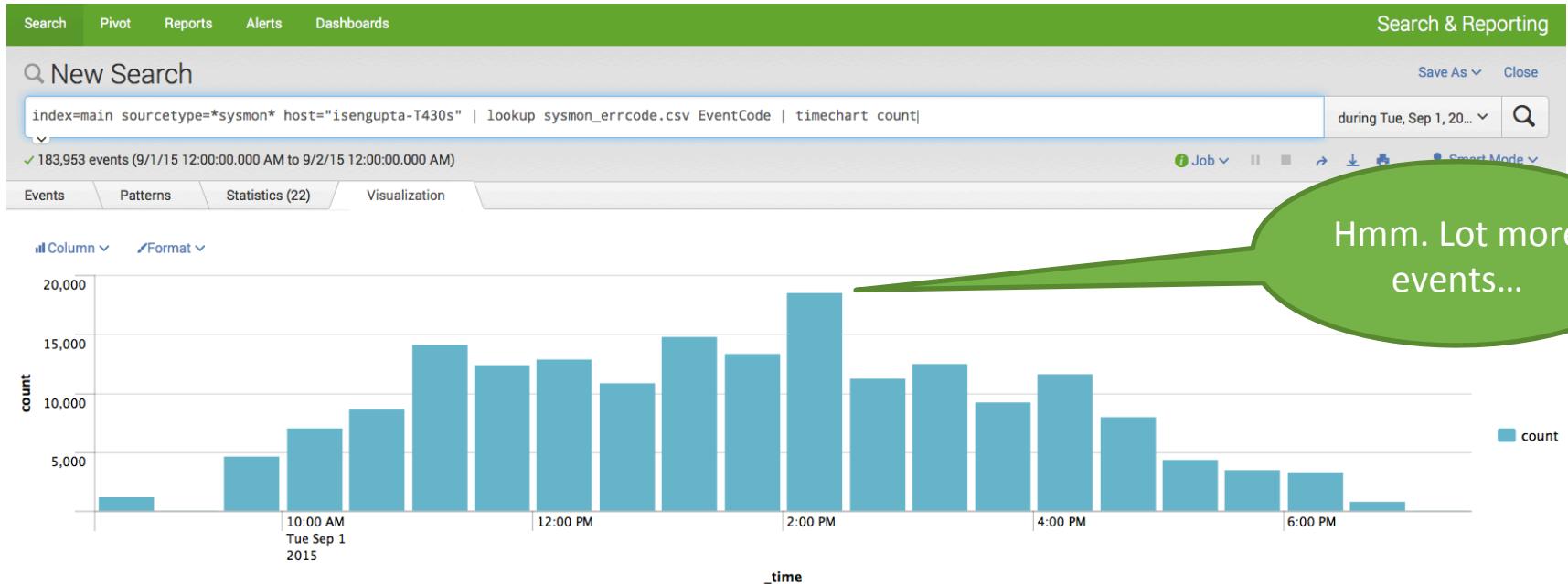
The results show 9,045 events from September 1, 2015, to September 2, 2015. The Statistics tab is selected, displaying the following data:

sourcetype	mbytes
WinEventLog:Application	0.04
WinEventLog:Security	5.38
WinEventLog:System	0.11
	5.53

A red box highlights the value '5.53' in the last row.

12 hours of standard event logs = 5.5 MB. Nice!

How much data?



How much data?

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ Close

```
index=main sourcetype=*sysmon* host="isengupta-T430s" | eval length_in_bytes=len(_raw) | lookup sysmon_errcode.csv EventCode| stats sum(length_in_bytes) as bytes by EventDescription | eval mbytes=(bytes/1024/1024) | addcoltotals | eval mbytes=round(mbytes,2)
```

183,953 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM) Job ▾ Smart Mode ▾

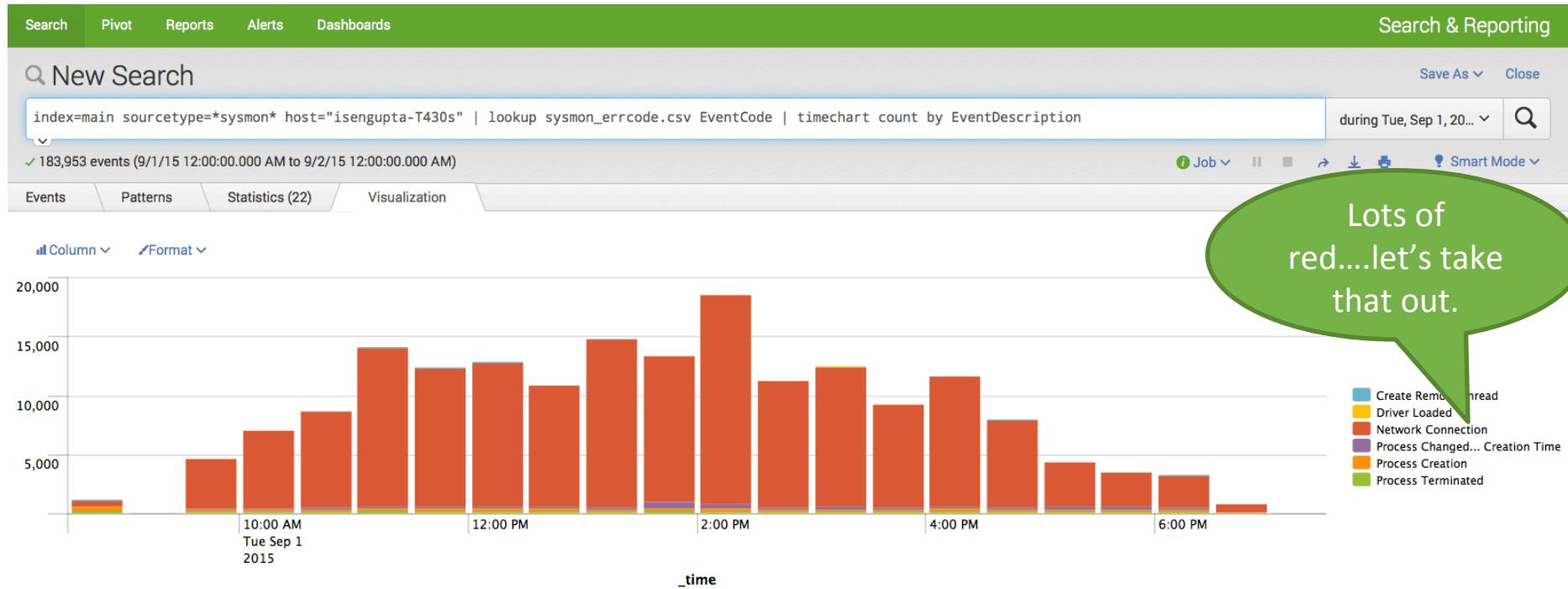
Events Patterns Statistics (7) Visualization

100 Per Page ▾ Format ▾ Preview ▾

EventDescription	bytes	mbytes
Create Remote Thread	601311	0.57
Driver Loaded	26490	0.03
Network Connection	236119819	225.18
Process Changed File Creation Time	4439548	4.23
Process Creation	7630200	7.28
Process Terminated	3764731	3.59
	252582099	240.88

12 hours of Sysmon logs = 241 MB. Oh crap. There goes my .conf talk...

How much data?



Lots of
red....let's take
that out.

How much data?

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ Close

```
index=main sourcetype=sysmon* host="isengupta-T430s" EventCode != 3| eval length_in_bytes=len(_raw) | lookup sysmon_errcode.csv EventCode| stats sum(length_in_bytes) as bytes by EventDescription | eval mbytes=(bytes/1024/1024) | addcoltotals | eval mbytes=round(mbytes,2)
```

13,291 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM) Job ▾ Smart Mode ▾

Events Patterns Statistics (6) Visualization

100 Per Page ▾ Format ▾ Preview ▾

EventDescription	bytes	mbytes
Create Remote Thread	601311	0.57
Driver Loaded	26490	0.03
Process Changed File Creation Time	4439548	4.23
Process Creation	7630200	7.28
Process Terminated	3764731	3.59
	16462280	15.70

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.

Sysmon with network/image filtering?

You still get...

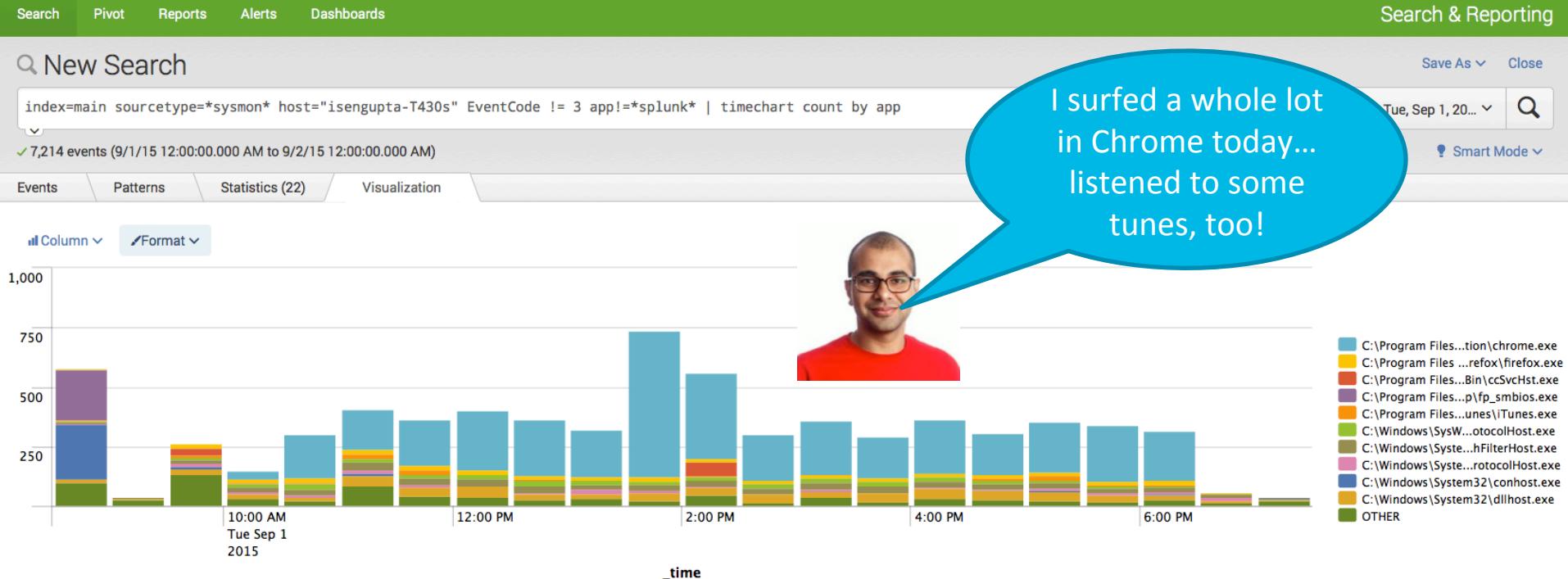
- Start/Stop of all processes
- Process names & full command line args
- Parent/child relationships (GUIDs) between processes
- Session IDs
- Hash and user data for all processes
- Filenames that have their create times updated
- Driver/DLL loads with hash data

You retain far more function than you lose.

You lose...

- Network communication per process (TCP and UDP) including IP address, size, port data
- Ability to map communication back to process GUID and session ID

So you can still do...



And also...

Splunk interface showing search results for Microsoft Office usage.

Search bar: index=main sourcetype=*sysmon* host="isengupta-T430s" EventCode != 3 app="C:\\Program Files (x86)\\Microsoft Office\\Office14*" | ".*\\"(?<filename>.*.(pptx|docx|oft))\" | dedup filename| table _time,app,filename,user | sort +_time

15 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM)

Events Patterns Statistics (15) Visualization

100 Per Page Format Preview

_time	app	filename	user
2015-09-01 09:42:06	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template-4.oft	SPLUNK\isengupta
2015-09-01 09:47:14	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template-5.oft	SPLUNK\isengupta
2015-09-01 09:48:11	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template-6.oft	SPLUNK\isengupta
2015-09-01 09:48:30	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	Splunk Monthly External Newsletter - Word Doc.docx	SPLUNK\isengupta
2015-09-01 09:50:11	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template-7.oft	SPLUNK\isengupta
2015-09-01 09:55:02	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	Splunk Monthly External Newsletter - Word Doc Mac Only.docx	SPLUNK\isengupta
2015-09-01 09:57:38	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	Monthly External Newsletter Mac September 2015.docx	SPLUNK\isengupta
2015-09-01 10:52:47	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template Windows Only.oft	SPLUNK\isengupta
2015-09-01 10:52:57	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template Windows Only-1.oft	SPLUNK\isengupta
2015-09-01 10:53:12	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly Newsletter September 2015.oft	SPLUNK\isengupta
2015-09-01 10:53:30	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template Windows Only-2.oft	SPLUNK\isengupta
2015-09-01 10:53:53	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	Splunk Monthly External Newsletter - Outlook Template Windows Only-3.oft	SPLUNK\isengupta
2015-09-01 11:40:45	C:\Program Files (x86)\Microsoft Office\Office14\POWERPNT.EXE	GettingStartedWithSplunk-Sept3rd_2015.pptx	SPLUNK\isengupta
2015-09-01 14:25:39	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	Trial Product Interstitial Landing Page.docx	SPLUNK\isengupta
2015-09-01 14:28:04	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	Try Splunk Light for Free Interstitial_MI_DR9-1-2015.docx	SPLUNK\isengupta

A blue speech bubble points to the file "GettingStartedWithSplunk-Sept3rd_2015.pptx" in the search results. Inside the bubble, a young man with glasses and a red shirt is smiling. The text in the bubble reads: "I really DID work on that 300 slide powerpoint before lunch, I swear!"

In Sum

1. If you're not Splunking the data from your various endpoints today, you should be.
2. The Splunk Universal Forwarder is a super-powerful tool to use on your endpoints, free to install, scales well, can be centrally configured, and data volumes are quite reasonable.
3. For Windows, event data is critical. Sysmon data is great too, and free to install.
4. Other customers from many verticals are having continued success with the data they can gather from endpoints.



.conf2015

Final Questions?

splunk®

Ghosts of Sessions Past and Future

“Finding Advanced Attacks & Malware with 6 Windows EventIDs you Configure and Monitor” – Michael Gough, Malware Archaeology

“Hunting known unknowns with the Splunk App for Enterprise Security” – Kovar & Brant, Splunk

“Splunk Assessment of Mitigation Implementations” – Jim Ronayne, NSA

Check these out!

.conf2015

THANK YOU

splunk®

.conf2015

Appendix

splunk®

.conf2015

2015

Sysmon Details

splunk®

The screenshot shows a blog post on the Splunk website. The URL is blogs.splunk.com/2014/11/24/monitoring-network-traffic-with-sysmon-and-splunk/. The page title is "splunk > blogs". Below the title is a green grass background image. A sidebar on the left says "Blogs: Tips & Tricks". The main content is titled "Monitoring Network Traffic with Sysmon and Splunk". It discusses the use of Sysmon to log system activity and how to install it on Windows using Chocolatey. It also covers how to configure Splunk to receive Sysmon logs via Forwarder 6.2+ and how to search for events. A code block shows the configuration for inputs.conf and a basic search in Splunk. The post concludes with a note about EventCode values.

Blogs: Tips & Tricks

Monitoring Network Traffic with Sysmon and Splunk

Every IT guy has a set of tools that they use every day. One of mine is [sysinternals](#). It's a set of Windows utilities made available by Microsoft that do a whole slew of things. You can install them with [chocolatey](#) (another in my toolset) or downloaded and unpacked from their website. If you use Windows and this toolset isn't in your arsenal, maybe it's time.

Back in August, I got a request from one of our engineers asking me if we had any plans to support the collection of [Sysmon](#) data. Sysmon is a Windows system service (yes, another agent) that logs system activity to the Windows Event Log. However, it places all the important stuff in the XML data block – that bit of the Windows Event Log that we did not expose until 6.2.0. Now that we have the `renderXml` parameter on `WinEventLog`, we can do something about it. I was reminded of this utility last week when one of our security researchers asked about network connections.

Installing it is relatively simple. Download the package, unzip it, then run:

```
sysmon -i -n -accepteula
```

The `-i` installs the service and the `-n` instructs it to monitor network connections. Once that is done, the service will start dropping events in the stream Application and Services Logs/Microsoft/Windows/Sysmon/Operational. You can receive these logs in Splunk by using the following inputs.conf entry:

```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
```

Now that you have events in Splunk, there is a wealth of information available to you. The basic search is:

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
```

The normal `EventCode` field is available and there are two basic event codes available to you. There are several event codes generated, but the two you will want to be concerned with are `EventCode="1"`, which is a process creation and `EventCode="3"`, which is a network connection.

Which brings us back to our problem. Last week, one of our security researchers was asking about monitoring

.conf2015

Sysmon Info

- Blog post from November, 2014
- App available on Splunkbase, works with current (3.1) version of Sysmon:
- Forwarder 6.2+ needed to get XML formatted Sysmon data (a good idea, cuts down on size)

Sysmon Filters

Filter out all the
Splunk activity

```
1 <Sysmon schemaversion="2.0">
2   <HashAlgorithms>SHA1</HashAlgorithms>
3   <EventFiltering>
4     <!-- Log all drivers except if the signature -->
5     <!-- contains Microsoft or Windows -->
6     <DriverLoad onmatch="exclude">
7       <Signature condition="contains">microsoft</Signature>
8       <Signature condition="contains">windows</Signature>
9     </DriverLoad>
10    <!-- Exclude certain processes that cause high event volumes -->
11    <ProcessCreate default="include">
12      <Image condition="contains">splunk</Image>
13      <Image condition="contains">streamfd</Image>
14      <Image condition="contains">splunkd</Image>
15      <Image condition="contains">splunkd</Image>
16      <Image condition="contains">splunk</Image>
17      <Image condition="contains">splunk-optimize</Image>
18      <Image condition="contains">splunk-MonitorIoHandle</Image>
19      <Image condition="contains">splunk-admin</Image>
20      <Image condition="contains">splunk-netmon</Image>
21      <Image condition="contains">splunk-regmon</Image>
22      <Image condition="contains">splunk-winprintmon</Image>
23      <Image condition="contains">btool</Image>
24      <Image condition="contains">PYTHON</Image>
25    </ProcessCreate>
26    <ProcessTerminate default="include">
27      <Image condition="contains">splunk</Image>
28      <Image condition="contains">streamfd</Image>
29      <Image condition="contains">splunkd</Image>
30      <Image condition="contains">splunkd</Image>
31      <Image condition="contains">splunk</Image>
32      <Image condition="contains">splunk-optimize</Image>
33      <Image condition="contains">splunk-MonitorIoHandle</Image>
34      <Image condition="contains">splunk-admin</Image>
35      <Image condition="contains">splunk-netmon</Image>
36      <Image condition="contains">splunk-regmon</Image>
37      <Image condition="contains">splunk-winprintmon</Image>
38      <Image condition="contains">btool</Image>
39      <Image condition="contains">PYTHON</Image>
40    </ProcessTerminate>
41    <FileCreateTime default="include">
42      <Image condition="contains">splunk</Image>
43      <Image condition="contains">streamfd</Image>
44      <Image condition="contains">splunkd</Image>
45      <Image condition="contains">splunkd</Image>
46      <Image condition="contains">splunk</Image>
47      <Image condition="contains">splunk-optimize</Image>
48      <Image condition="contains">splunk-MonitorIoHandle</Image>
49      <Image condition="contains">splunk-admin</Image>
50      <Image condition="contains">splunk-netmon</Image>
51      <Image condition="contains">splunk-regmon</Image>
52      <Image condition="contains">splunk-winprintmon</Image>
53      <Image condition="contains">btool</Image>
54      <Image condition="contains">PYTHON</Image>
55    </FileCreateTime>
56  </EventFiltering>
```

- This works for Sysmon 3.1+
- Add what you need
- If you actually want Image and Network data, add those stanzas
- Email brodsky@splunk.com for links to example files!

cn Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\brodsky>sysmon -c

Sysinternals Sysmon v3.10 - System activity monitor
Copyright <C> 2014-2015 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
- Service name: Sysmon
- Driver name: SysmonDrv
- HashingAlgorithms: SHA1
- Network connection: disabled
- Image loading: disabled

Rule configuration (version 0.00):
- DriverLoad
  Signature onmatch: exclude
  Signature filter: contains value: 'microsoft'
- ProcessCreate
  Image onmatch: exclude
  Image filter: contains value: 'windows'
  Image filter: contains value: 'splunk'
  Image filter: contains value: 'streamfwd'
  Image filter: contains value: 'splunkd'
  Image filter: contains value: 'splunkD'
  Image filter: contains value: 'splunk'
  Image filter: contains value: 'splunk-optim
ize'
  Image filter: contains value: 'splunk-Monit
orNoHandle'
  Image filter: contains value: 'splunk-admon
',
  Image filter: contains value: 'splunk-netmo
n'
  Image filter: contains value: 'splunk-regmo
n'
  Image filter: contains value: 'splunk-winpr
intmon'
  Image filter: contains value: 'btool'
  Image filter: contains value: 'PYTHON'
- ProcessTerminate
  Image onmatch: exclude
  Image filter: contains value: 'splunk'
  Image filter: contains value: 'streamfwd'
  Image filter: contains value: 'splunkd'
  Image filter: contains value: 'splunkD'
  Image filter: contains value: 'splunk'
  Image filter: contains value: 'splunk-optim
ize'
```

Image and
Network
disabled

Sysmon Config List

- sysmon -c with no filename will dump config

Sysmon Config Load

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sysmon -c c:\Users\brodsky\Downloads\sysmoncfg_v2-1.xml

Sysinternals Sysmon v3.10 - System activity monitor
Copyright (C) 2014-2015 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 2.00
Sysmon schema version: 2.01
Warn: The event 'DriverLoad' cannot be automatically enabled.
    Ensure it is correctly configured.
Warn: The event 'ProcessCreate' cannot be automatically enabled.
    Ensure it is correctly configured.
Warn: The event 'ProcessTerminate' cannot be automatically enabled.
    Ensure it is correctly configured.
Warn: The event 'FileCreateTime' cannot be automatically enabled.
    Ensure it is correctly configured.
Configuration file successfully applied
Configuration updated.

C:\Windows\system32>
```

- sysmon -c with filename will load config
- No restart needed
- Ignore errors
- Run as admin (or script as admin)

.conf2015

2015

Hash Analysis with Sysmon

splunk®

New Search

Save As ▾ Close

```
index=main host="isengupta-T430s" Image!="svchost.exe" Image!="splunk*" | rex mode=sed field=Hashes "s/SHA1=/g" | stats dc(Hashes) as numhashes,values(Hashes) as SHA1 by Image | where numhashes>0 | sort -numhashes
```

Last 24 hours



62,851 events (9/1/15 1:00:00.000 PM to 9/2/15 1:05:13.000 PM)

Job ▾ II ■ ↻ ↴ ⌂ Smart Mode ▾

Events Patterns Statistics (87) Visualization

100 Per Page ▾ Format ▾ Preview ▾

Image	numhashes	SHA1
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	2	A8AF113914CD161FF6B33B8968DB31A427E66C4D D09A3AD4D958075F5E2A42DA01A64917E6BC543
C:\PROGRA~2\Symantec\SYMANT~1\121100~1.105\Bin\DWHWizrd.exe	1	A4288CD5600C8670ED666F623702F76560C5DAD4
C:\PROGRA~3\WebEx\WebEx\1526\WebexStm\CiscoWebexVideoService.exe	1	328D2AC05833A7C24A075E081E48732C2D46FE28
C:\PROGRA~3\WebEx\WebEx\1526\atshell.exe	1	F8FA1D5A8023E6C69258B2B6C27A054384D0012D
C:\Program Files (x86)\Adobe\Adobe Creative Cloud\HEX\Adobe CEF Helper.exe	1	CD1E24DB4000A94028E84F6C8A2705390D2682B
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe	1	5EA3B6B57EADC1A8DBD6BF60AB4CAD4CF3AE5574
C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe	1	9B5C1DD5C2F7C30A6A303C036406ACF4D6BE48E0
C:\Program Files (x86)\Atlassian\HipChat\hipchat.exe	1	A637C3B4AC793E3456C1F6C1AB35905CA66C03F2
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	1	E9E1551426148EE9D7A6CD426EBFDB193A0F7FAD
C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\AAM Updates Notifier.exe	1	A304928311BF24C9123D3816098FE6AF18290DFD
C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\updatestartutility.exe	1	E056DDDC15C841CC06B66CF05E6A470BD521F5ED
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe	1	F147BB4A573F5E03A44D956BBAF1C242ADAAD448
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\dinstored.exe	1	BD893147AC95BCEA1C1CCEBA54661C47F54E273A
C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceHelper.exe	1	EBB62A866F7DFDA5467694E23DBD74E52721EC36
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	1	835E982347DB919A681BA12F3891F62152E50F0D
C:\Program Files (x86)\Evernote\Evernote\Evernote.exe	1	A51C893266D85FF171629C137C63BEFB291A5565
C:\Program Files (x86)\Evernote\Evernote\EvernoteTray.exe	1	000C52362000A3D00A1562F61EAR1770C1C0672

two hashes for chrome in 24 hours?

SHA256: 76fa85ad2ca9eadedb5b018d6432fd7d6d90a0893e9b1676c3b686001ab9eff1

File name: chrome.exe

Detection ratio: 0 / 56

not malicious



Analysis date: 2015-09-02 19:46:59 UTC (23 minutes ago)

@ Probably harmless! There are strong indicators suggesting that this file is safe to use.

[Analysis](#)[File detail](#)[Relationships](#)[Additional information](#)[Comments 1](#)[Votes](#)

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

Authenticode signature block and FileVersionInfo properties

Copyright Copyright 2012 Google Inc. All rights reserved.

Publisher Google Inc

Product Google Chrome

Original name chrome.exe

Internal name chrome_exe

File version 44.0.2403.157

Description Google Chrome

Signature verification Signed file, verified signature

Signing date 6:24 AM 8/18/2015

Signers [+]
[+] Google Inc
[+] VeriSign Class 3 Code Signing 2010 CA
[+] VeriSignCounter signers [+]
[+] Symantec Time Stamping Services Signer - G4
[+] Symantec Time Stamping Services CA - G2
[+] Thawte Timestamping CA

SHA256: f9b8b1fcf5c0d12fc444ee1d910ce5342814bea8319e221fb931e0f28aae569

File name: chrome.exe

Detection ratio: 0 / 56

not malicious either



Analysis date: 2015-09-02 19:46:20 UTC (27 minutes ago)

@ Probably harmless! There are strong indicators suggesting that this file is safe to use.

[Analysis](#)[File detail](#)[Relationships](#)[Additional information](#)[Comments 0](#)[Votes](#)

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

Authenticode signature block and FileVersionInfo properties

Copyright Copyright 2012 Google Inc. All rights reserved.

Publisher Google Inc

Product Google Chrome

Original name chrome.exe

Internal name chrome_exe

File version 45.0.2454.85

Description Google Chrome

Signature verification Signed file, verified signature

Signing date 1:17 AM 8/28/2015

Signers [+]
[+] Google Inc
[+] VeriSign Class 3 Code Signing 2010 CA
[+] VeriSignCounter signers [+]
[+] Symantec Time Stamping Services Signer - G4
[+] Symantec Time Stamping Services CA - G2
[+] Thawte Timestamping CA

a new Chrome version!

SHA256: f9b8b1efcf5c0d12fc444ee1d910ce5342814bea83f9e221f8931e0f28aae569

File name: chrome.exe

Detection ratio: 0 / 56

Analysis date: 2015-09-02 19:46:20 UTC (27 minutes ago)



ⓘ Probably harmless! There are strong indicators suggesting that this file is safe to use.

Analysis

File detail

Relationships

Additional information

Comments 0

Votes

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

Authenticode signature block and FileVersionInfo properties

Copyright Copyright 2012 Google Inc. All rights reserved.

Publisher Google Inc

Product Google Chrome

Original name chrome.exe

Internal name chrome_exe

File version 45.0.2454.85

Description Google Chrome

Signature verification ✅ Signed file, verified signature

Signing date 1:17 AM 8/28/2015

Signers [+] Google Inc
[+] VeriSign Class 3 Code Signing 2010 CA
[+] VeriSign

Counter signers [+] Symantec Time Stamping Services Signer - G4
[+] Symantec Time Stamping Services CA - G2
[+] Thawte Timestamping CA

that's the new version



New Search

full text search

```
index=main host="isengupta-T430s" 45.0.2454.85 | timechart count by Image
```

Save As ▾ Close

Last 24 hours ▾



✓ 74 events (9/1/15 1:00:00.000 PM to 9/2/15 1:35:17.000 PM)

Job ▾ II ■ ↗ ↓ ↖ ↙ Verbose Mode ▾

Events (74)

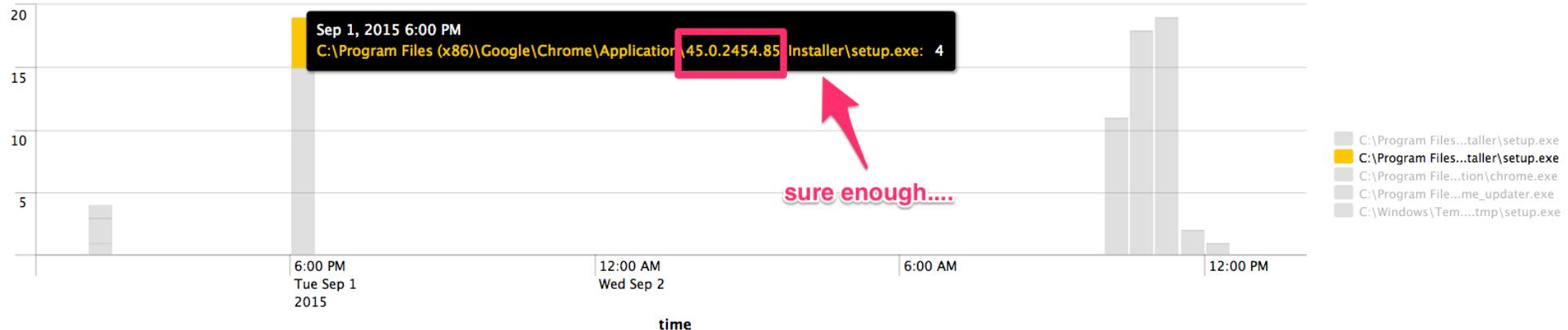
Patterns

Statistics (50)

Visualization

Column ▾

Format ▾





.conf2015

Windows Registry Monitoring

splunk®

Registry Monitoring config

```
[WinReqMon://hkcu_run]
disabled = 0
hive = \\REGISTRY\\USER\\.*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\.*
proc = .*
type = set|create|delete|rename

[WinReqMon://hklm_run]
disabled = 0
hive = \\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\.*
proc = .*
type = set|create|delete|rename

[WinReqMon://hklm_services]
disabled = 0
hive = \\REGISTRY\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\.*
proc = .*
type = set|create|delete|rename
```

- Simple examples shown here
- Email
brodsky@splunk.com
for an extensive registry monitoring config based on Autoruns

USB Activity

KC 3

[Edit ▾](#)
[More Info ▾](#)


Select a POS

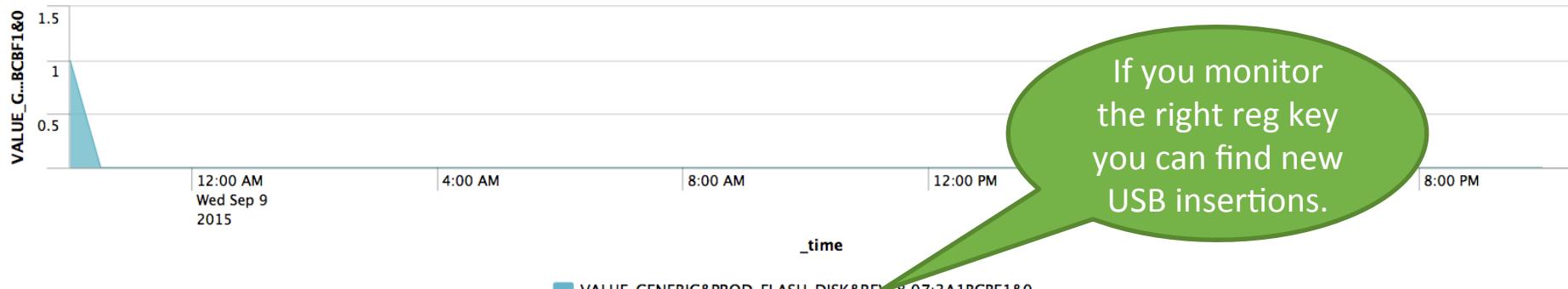
Last 24 hours

DAL-TX-POS2



New USB Disk Insertions

<1m ago



USB Disk Insertions

<1m ago

_time	host	USBDiskID	USBDiskSerial
2015-09-08 22:18:34	DAL-TX-POS2	_Generic&Prod_Flash_Disk&Rev_8.07	3A1BCBF1&0

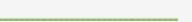
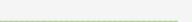
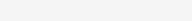
Drive Letters

<1m ago

_time	host	DriveLetter
2015-09-08 22:18:34	DAL-TX-POS2	e:

Recent Registry Changes

1m ago

host	key_path	process_image	data	sparkline	count
DAL-TX-POS2	HKLM\system\controlset001\services\disk\displayname	c:\Windows\System32\services.exe	Disk Driver		
DAL-TX-POS2	HKLM\system\controlset001\services\poswds\displayname	c:\Windows\System32\services.exe	POSWDS		
DAL-TX-POS2	HKLM\system\controlset001\services\poswds\imagepath	c:\Windows\System32\services.exe	E:\black-pos.exe		
DAL-TX-POS2	HKLM\system\controlset001\services\poswds\objectname	c:\Windows\System32\services.exe	LocalSystem		
DAL-TX-POS2	HKLM\system\controlset001\services\usbstor\displayname	c:\Windows\System32\services.exe	USB Mass Storage Driver		
DAL-TX-POS2	HKLM\system\controlset001\services\volsnap\displayname	c:\Windows\System32\services.exe	Storage volumes		

Registry Results

- USB inserted with BlackPOS malware
- Malware executed – these are the registry changes logged



.conf2015

WinHostMon

splunk®

```

# Queries computer information.
[WinHostMon://computer]
type = Computer
interval = 300

# Queries OS information.
# 'interval' set to a negative number tells Splunk Enterprise to
# run the input once only.
[WinHostMon://os]
type = operatingSystem
interval = -1

# Queries processor information.
[WinHostMon://processor]
type = processor
interval = -1

# Queries hard disk information.
[WinHostMon://disk]
type = disk
interval = -1

# Queries network adapter information.
[WinHostMon://network]
type = networkAdapter
interval = -1

# Queries service information.
# This example runs the input every 5 minutes.
[WinHostMon://service]
type = service
interval = 300

# Queries information on running processes.
# This example runs the input every 5 minutes.
[WinHostMon://process]
type = process
interval = 300

# Queries information on installed applications.
# This example runs the input every 5 minutes.
[WinHostMon://application]
type = application
interval = 300

```

WinHostMon

- Get hardware details, services, processes, apps, etc...
- Built right into the forwarder, no scripts needed