Splunking the Endpoint

James Brodsky

Staff Engineer/Security SME, Splunk

brodsky@splunk.com

splunk>

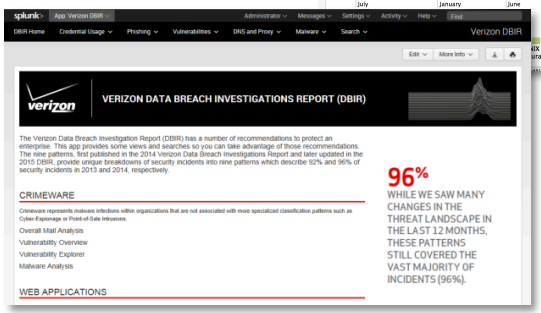
Disclaimer

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 the 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> 2 Years+



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!

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

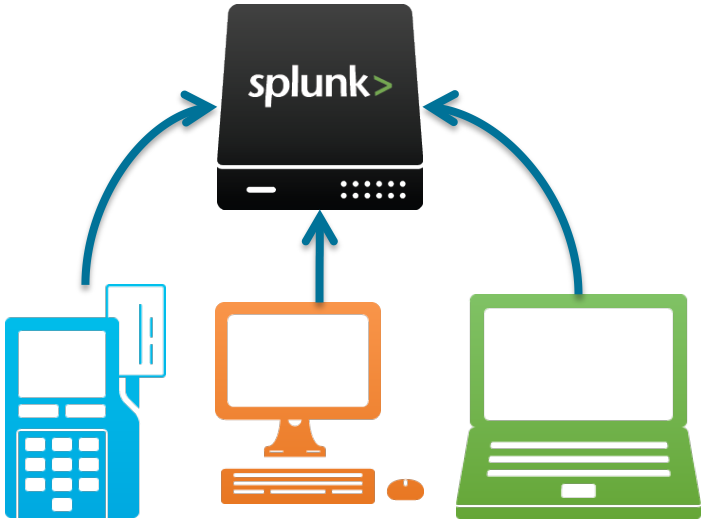
"Hunting known unknowns with DNS" – Kovar & Brant, Splunk

"Verifying Success of Key Mitigations" – Jim Ronayne, NSA

"Security Ninjutsu Part II" – David Veuve, Splunk

Session Goals

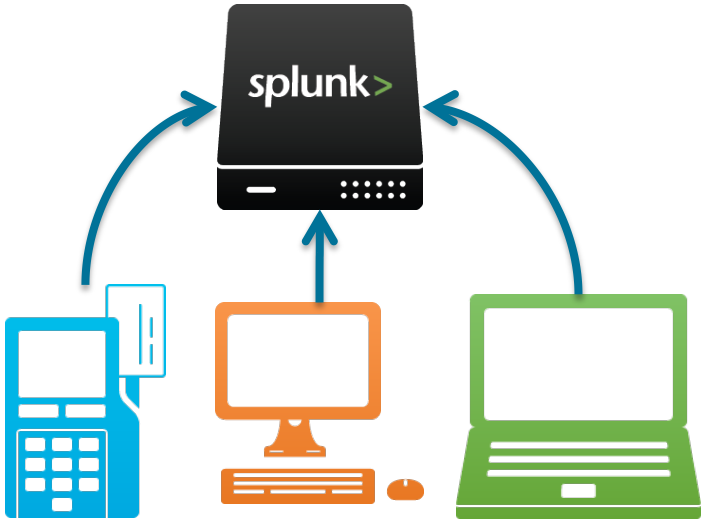
- Understand why you should Splunk the endpoint
- Believe that the Universal Forwarder is awesome
- Learn about customer success
- Get some artifacts you can use
- Bring home what you can do today



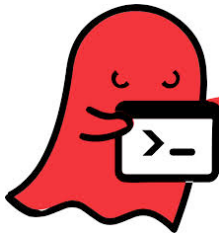
https://splunk.box.com/splunking-the-endpoint

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…

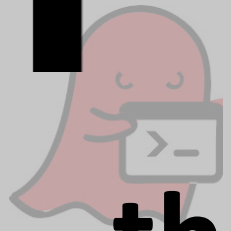


Endpoint/Server Vulnerabilities

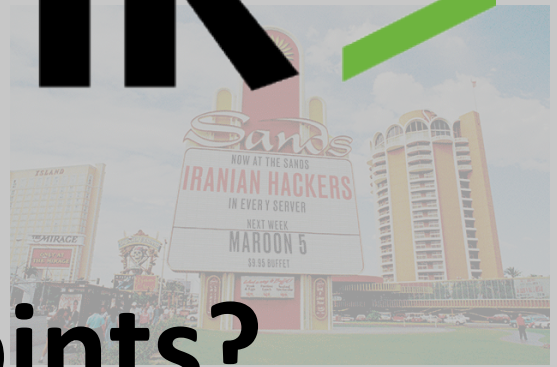
Endpoint-Based Malware

So these happened in 2014/2015...

Could we be more secure if we



splunk>



….the endpoints?

Endpoint/Server Vulnerabilities

Endpoint-Based Malware

Executive Summary:

YES!

(so do that)

THANK YOU

splunk>

The Endpoint is important!

Closest to humans

Underprotected

Versatile

Data-rich

The Endpoint is important!

Closest to humans

Underprotected

Versatile

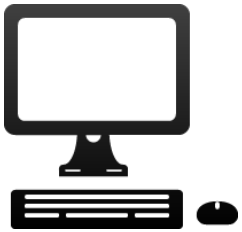
Data-rich

*IDC study 2014

The 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

Perfmon

Registry

Wire Data

Scripts

Logs

Sysmon

Splunk Universal Forwarder for ETD*!

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

*Endpoint Threat Detection (Response?)

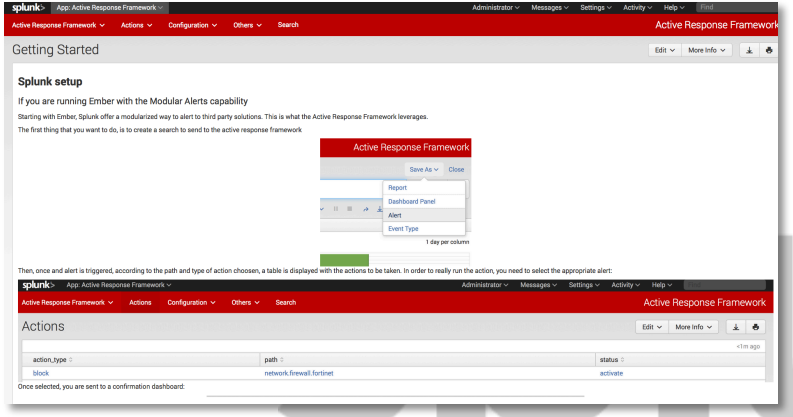
What about the “Response”?

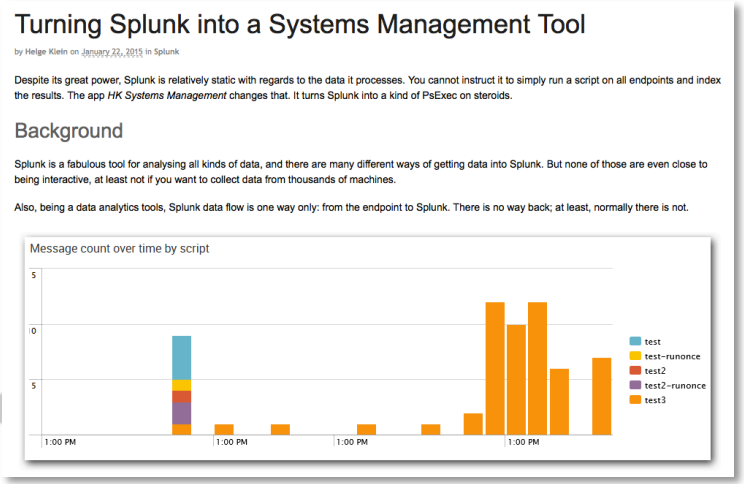
VISIBILITY

reactivity

(for now)

What about the “Response”?





ziften

There’s stuff out there. YMMV.

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

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

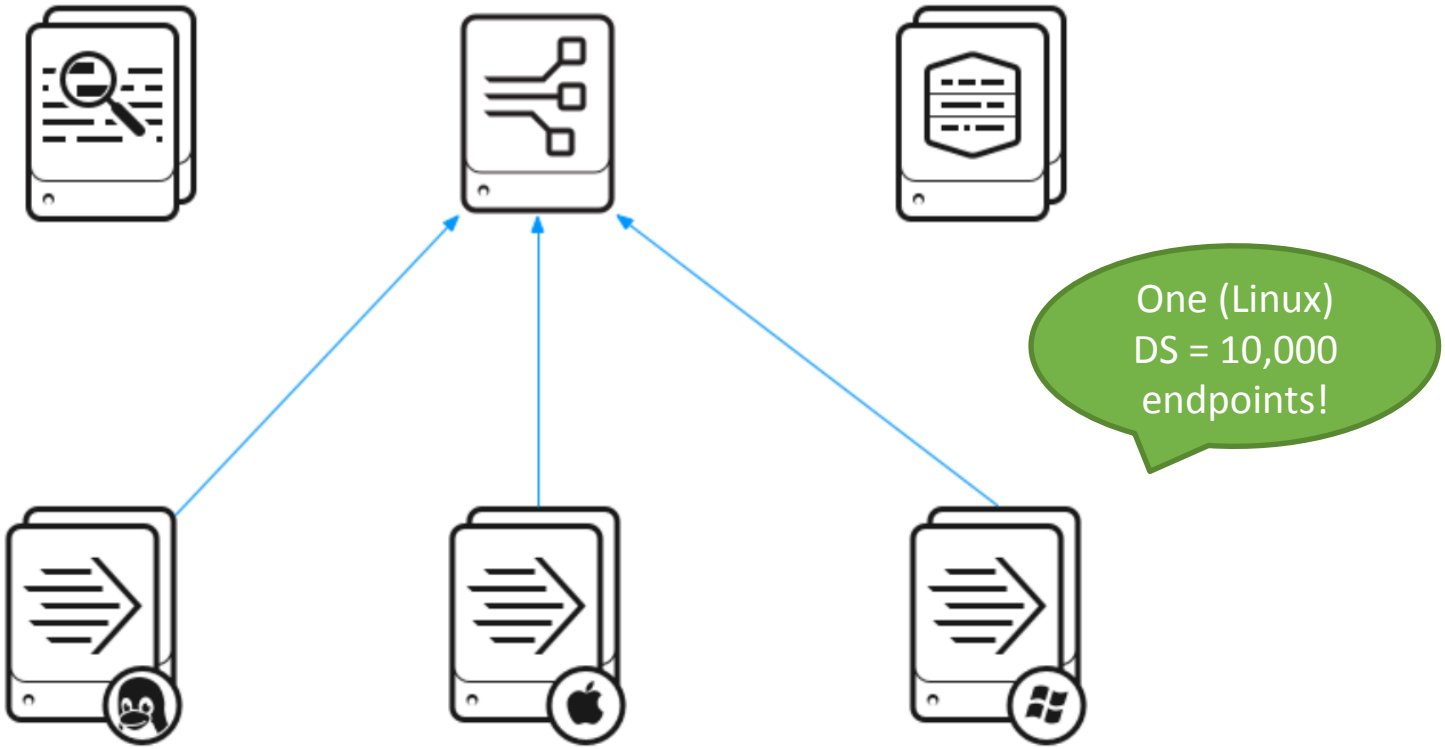
- Windows event logs
- OSX /var/log/*
- Carbon Black output
- Crash logs for IT Ops
- Custom script for apps installed
- UNIX TA (upon request)
- Windows TA (upon request)
- Additional granularity for execs and their admins
- Moving to Splunk Cloud

Microsoft

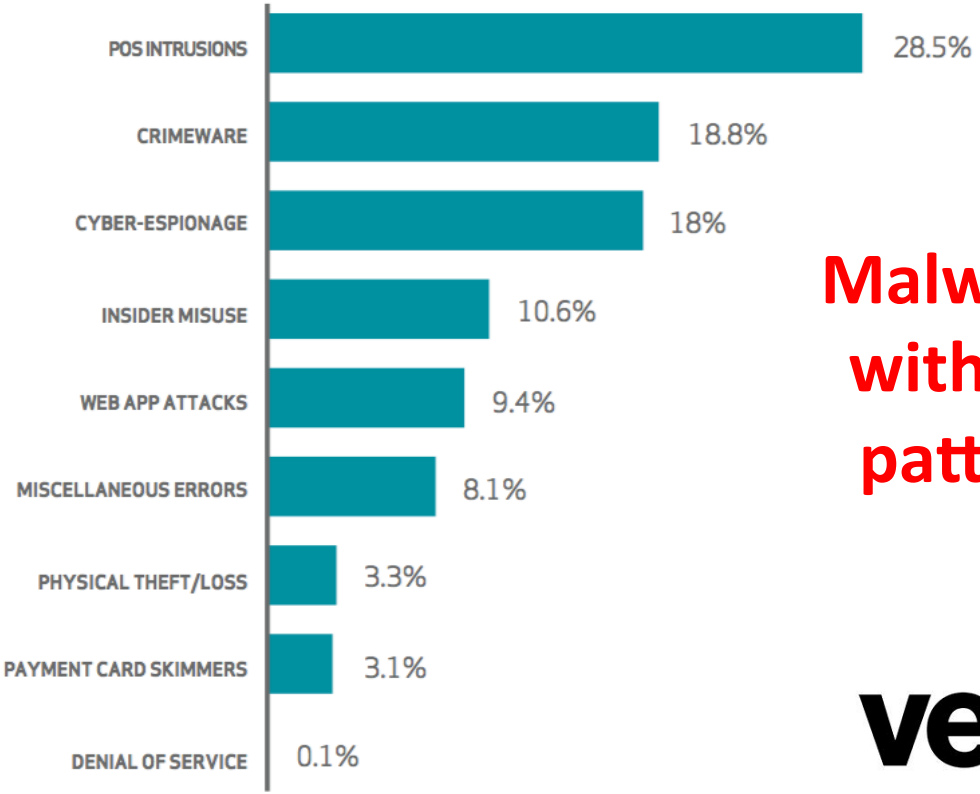
Bit9 + CARBON BLACK

splunk>cloud

Central Control with Deployment Server



Additional ways to gather endpoint data



Obligatory DBIR slide…

Malware: involved with top 3 attack patterns in DBIR 2015

verizon

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

Known Vulns/Apps

New Files

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

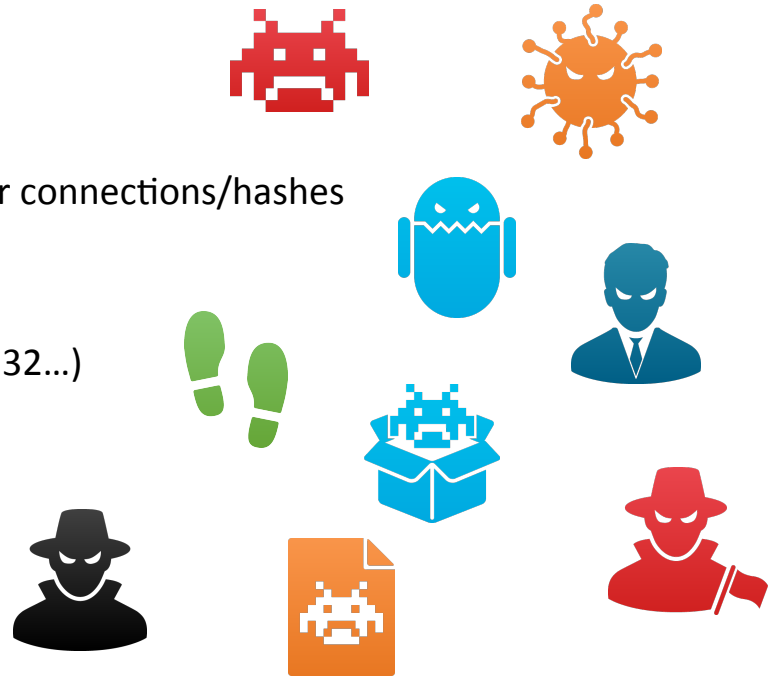
Configuration examples? See demo & appendix

Comms/Running Proc

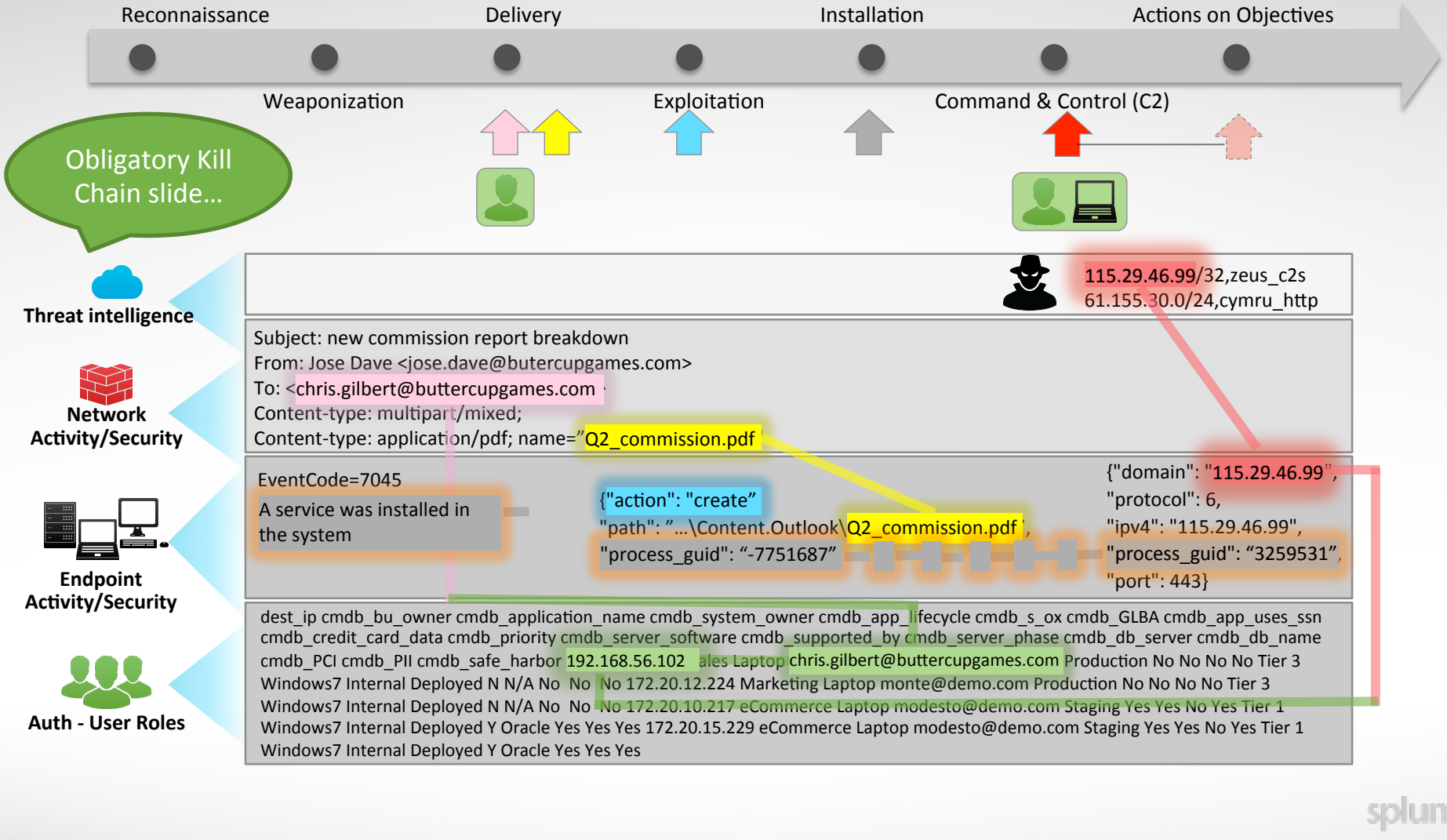
TA-Microsoft-Sysmon Stream, WinHostMon

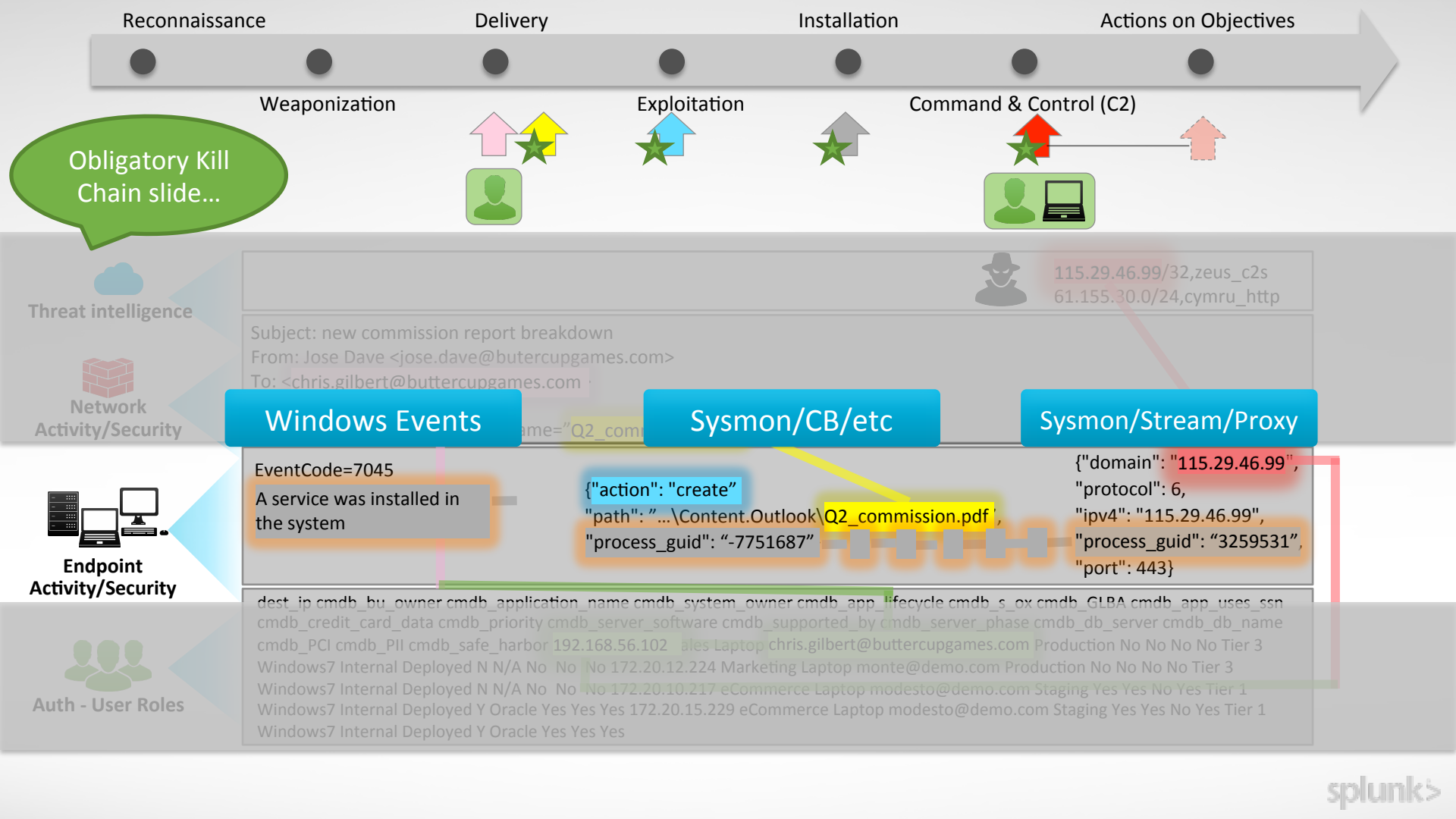
What could we look for?

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

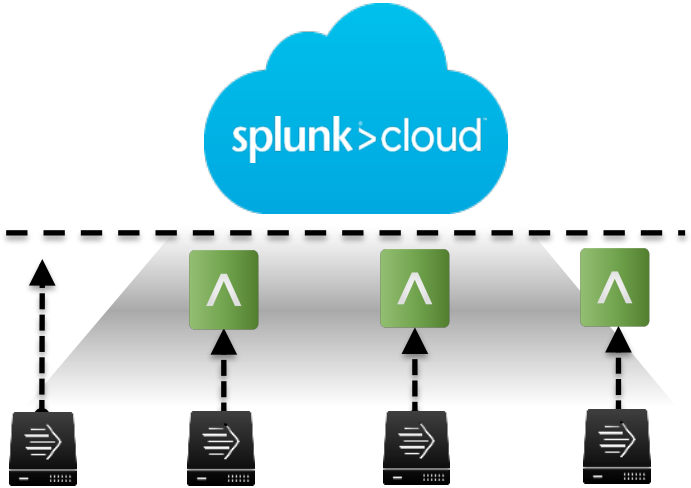

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control (C2)
Actions on Objectives
Obligatory Kill Chain slide…
Threat intelligence
115.29.46.99/32,zeus_c2s
61.155.30.0/24,cymru_http
Network Activity/Security
Subject: new commission report breakdown
From: Jose Dave <jose.dave@butercupgames.com>
To: <chris.gilbert@buttercupgames.com
Windows Events
Sysmon/CB/etc
Sysmon/Stream/Proxy
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}
Endpoint Activity/Security
Auth - User Roles
dest_ip cmdb_bu_owner cmdb_application_name cmdb_system_owner cmdb_app_lifecycle cmdb_s_ox cmdb_GLBA cmdb_app_uses_ssn
cmdb_credit_card_data cmdb_priority cmdb_server_software cmdb_supported_by cmdb_server_phase cmdb_db_server cmdb_db_name
cmdb_PCI cmdb_PII cmdb_safe_harbor 192.168.56.102 ales Laptop chris.gilbert@buttercupgames.com Production No No No No Tier 3
Windows7 Internal Deployed N N/A No No 172.20.12.224 Marketing Laptop monte@demo.com Production No No No No Tier 3
Windows7 Internal Deployed N N/A No No 172.20.10.217 eCommerce Laptop modesto@demo.com Staging Yes Yes No Yes Tier 1
Windows7 Internal Deployed Y Oracle Yes Yes Yes 172.20.15.229 eCommerce Laptop modesto@demo.com Staging Yes Yes No Yes Tier 1
Windows7 Internal Deployed Y Oracle Yes Yes Yes

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\WebEx\1526\WebexStm\CiscoWebexVideoService.exe C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe C:\Program Files (x86)\Common Files\Adobe\ARM\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\AcHelper64.exe C:\Program Files (x86)\Lenovo\Access Connections\AcWin7Hlpr.exe C:\Program Files (x86)\Lenovo\Access Connections\SvcGuiHlpr.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\App\LSCTaskService.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)

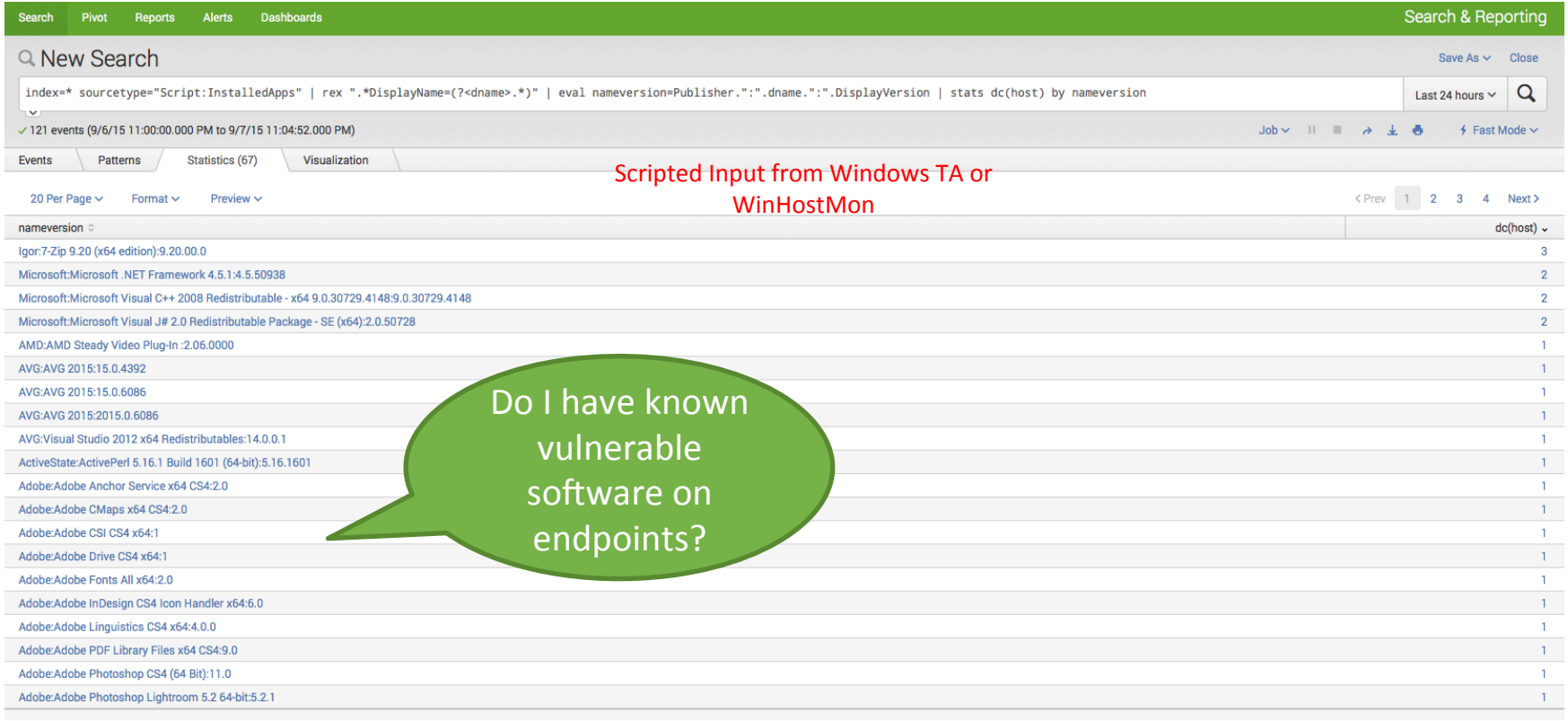
Events | Patterns | Statistics (3) | Visualization

Scripted Input from Windows TA or WinHostMon

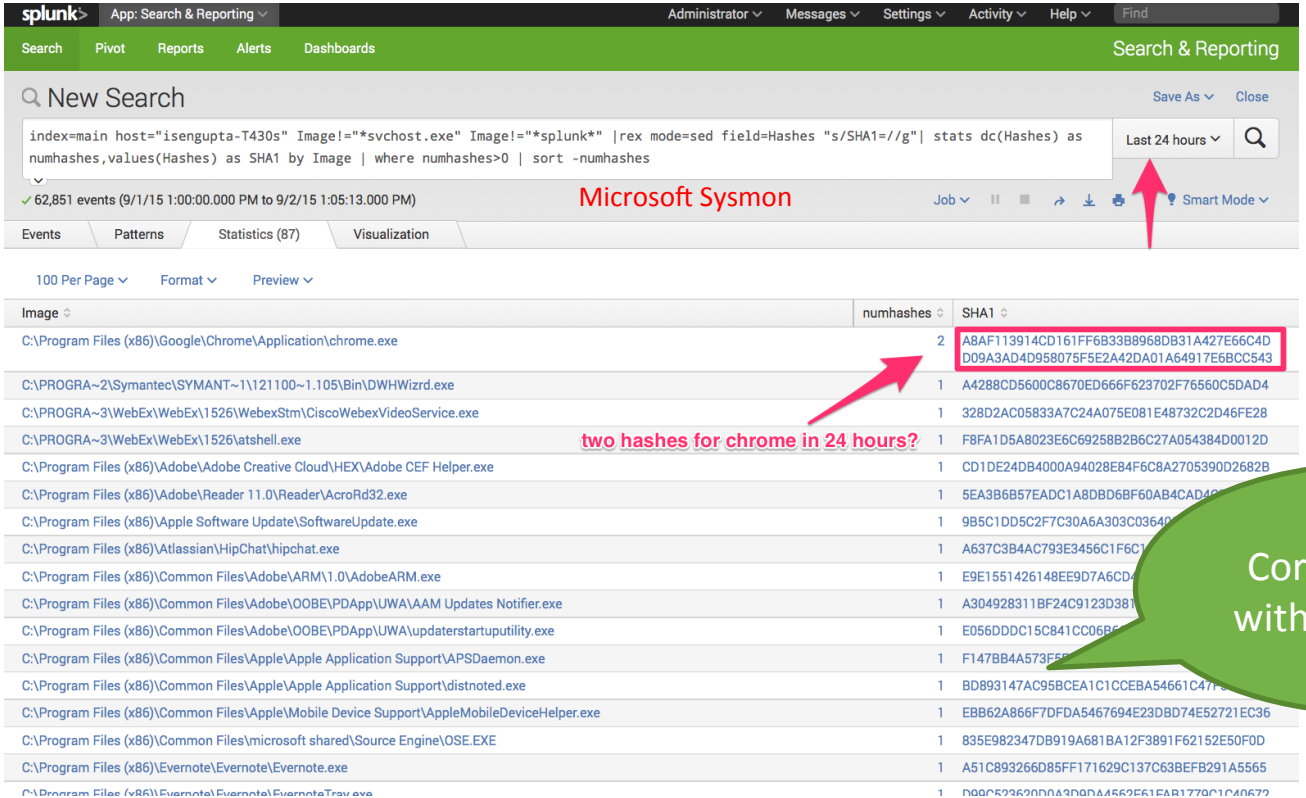
20 Per Page | Format | Preview

host	list(nameversion)
barnstorming	Splunk:UniversalForwarder: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:ActivePerl:5.16.1601 Microsoft:Microsoft:9.0.30729.6161 Microsoft:Microsoft:9.0.30729.4148 AVG:AVG:15.0.4392 Gadwin:Gadwin:5.3.1.0 Igor:7-Zip:9.20.00.0 VMware:VMware:3.5.2 Piriform:Recuva:1.51 AVG:AVG:2015.0.6086
choppercommand	Microsoft:Microsoft:4.0.30319 Intel:Intelr: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 Splunk:Universal:5.0.4.172409 Apple:Apple:6.1.0.13 Igor:7-Zip:9.20.00.0 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

What versions of what exist on my network?



Hash data from apps



Windows Update data

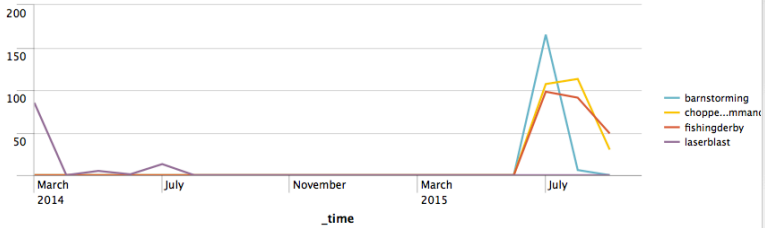
CIP 007-R2 Patch Management

Display Windows Update and RHN Status

Edit | More Info

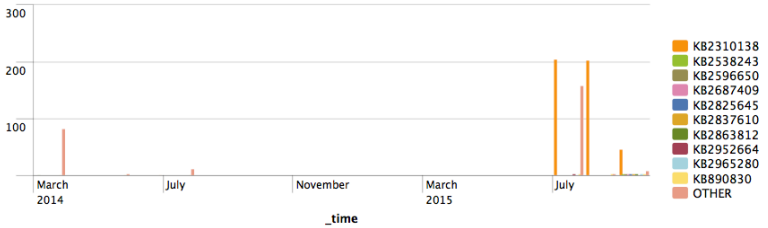
Successful Windows Updates Over Time by Host

11m ago



Successful Windows Updates over Time by KB

11m ago



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

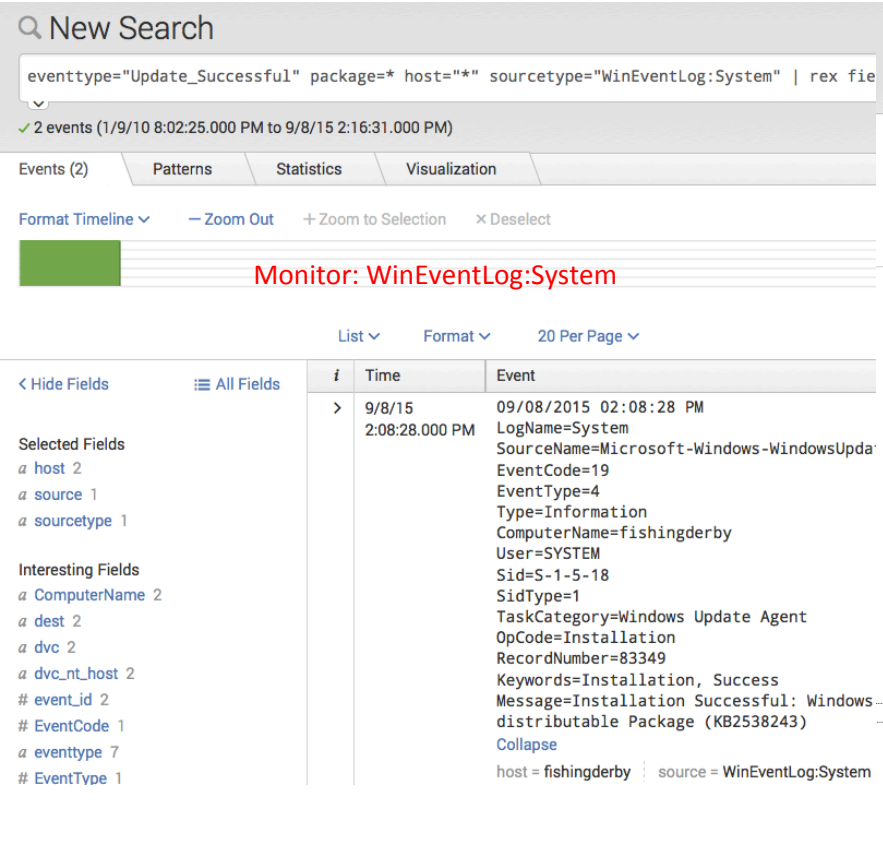
Successful Windows Updates by KB Name

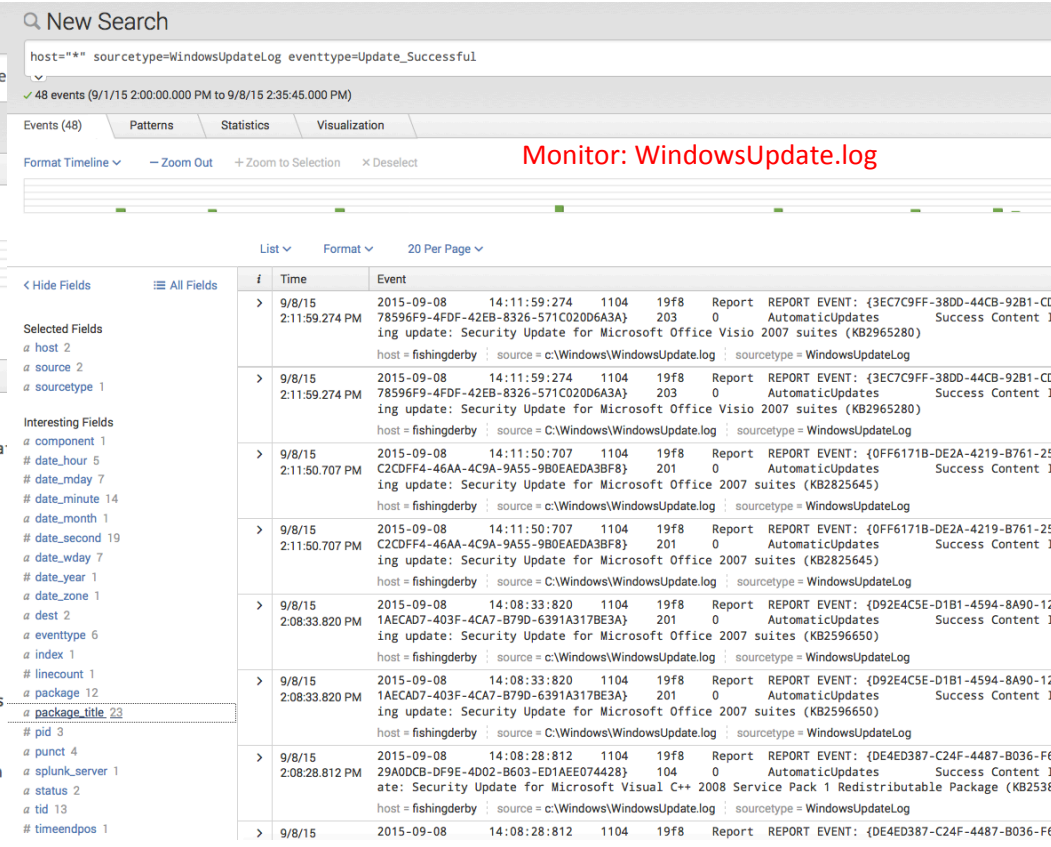
11m ago

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

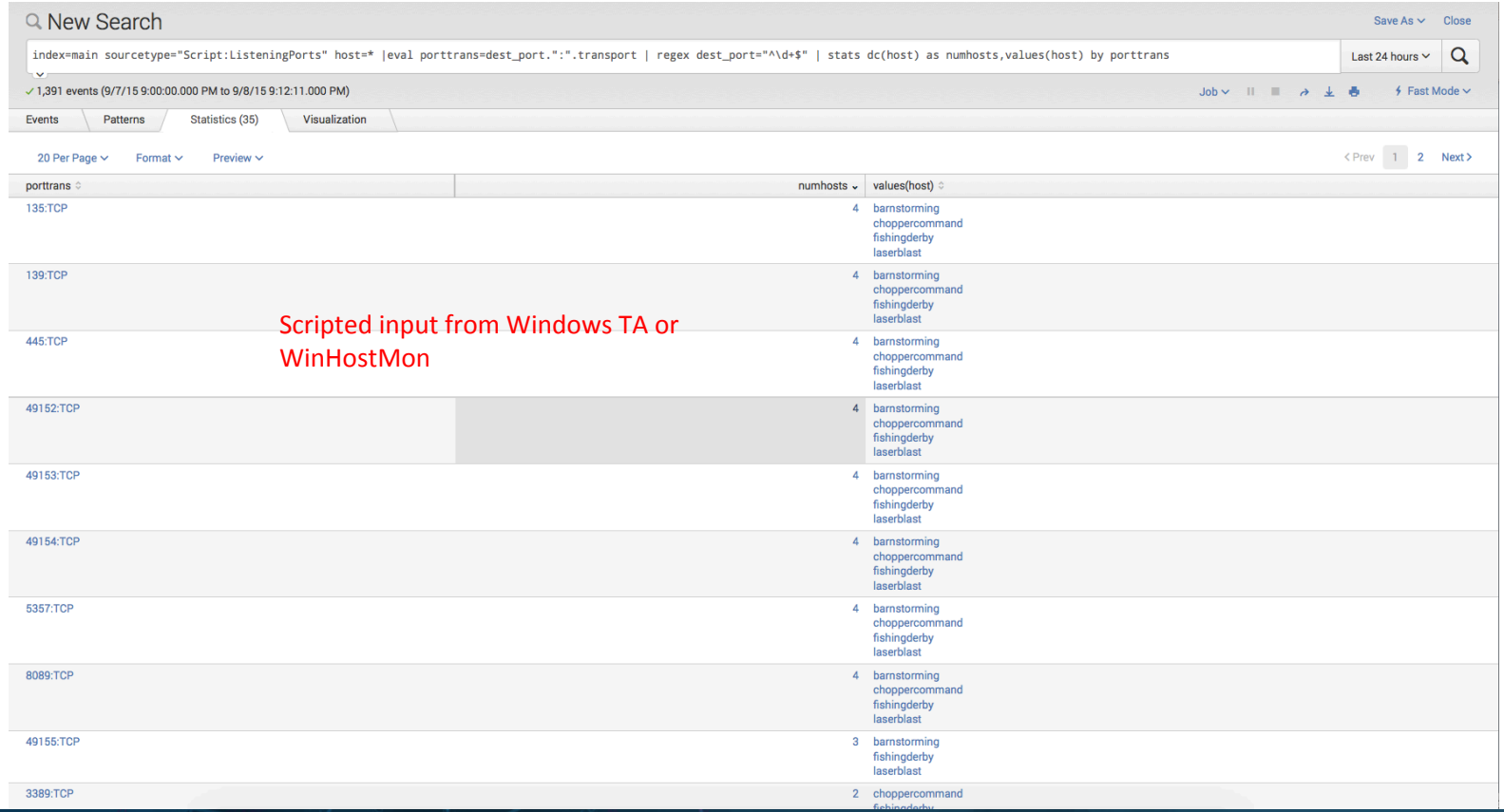
« prev 1 2 3 4 5 6 7 8 9 10 next »

Windows Update Data (two sourcetypes)





Windows Port Data



Windows Port Data

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

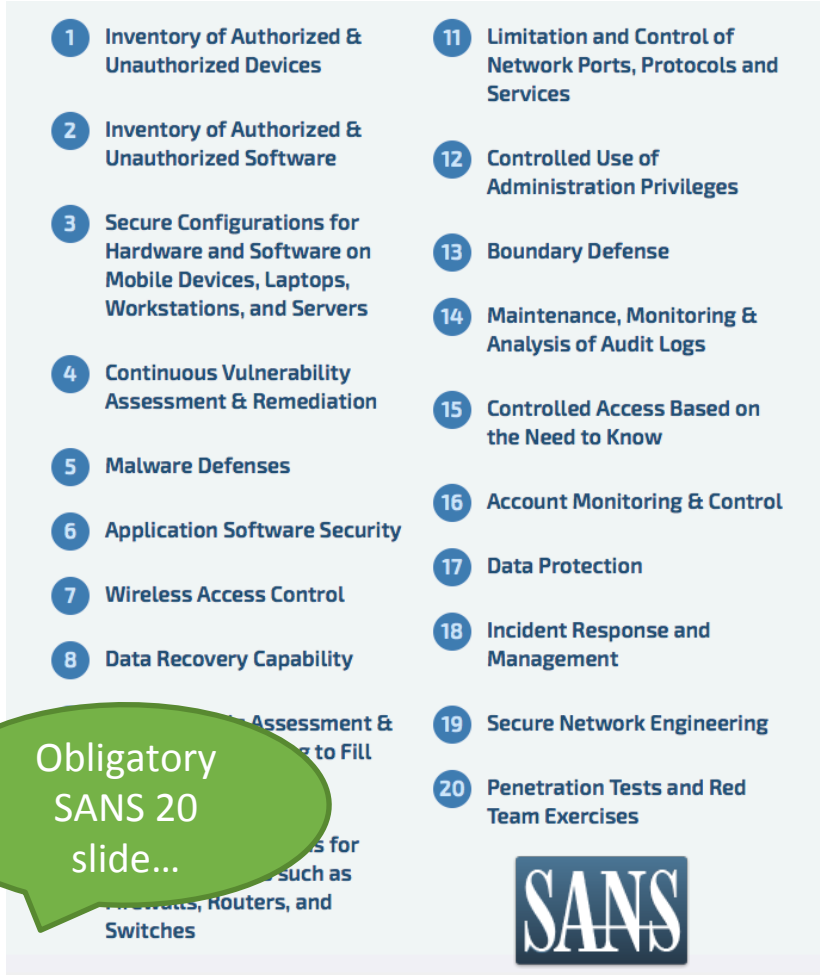
12: Look for local use of priv accounts

14: Gather windows events/*NIX logs

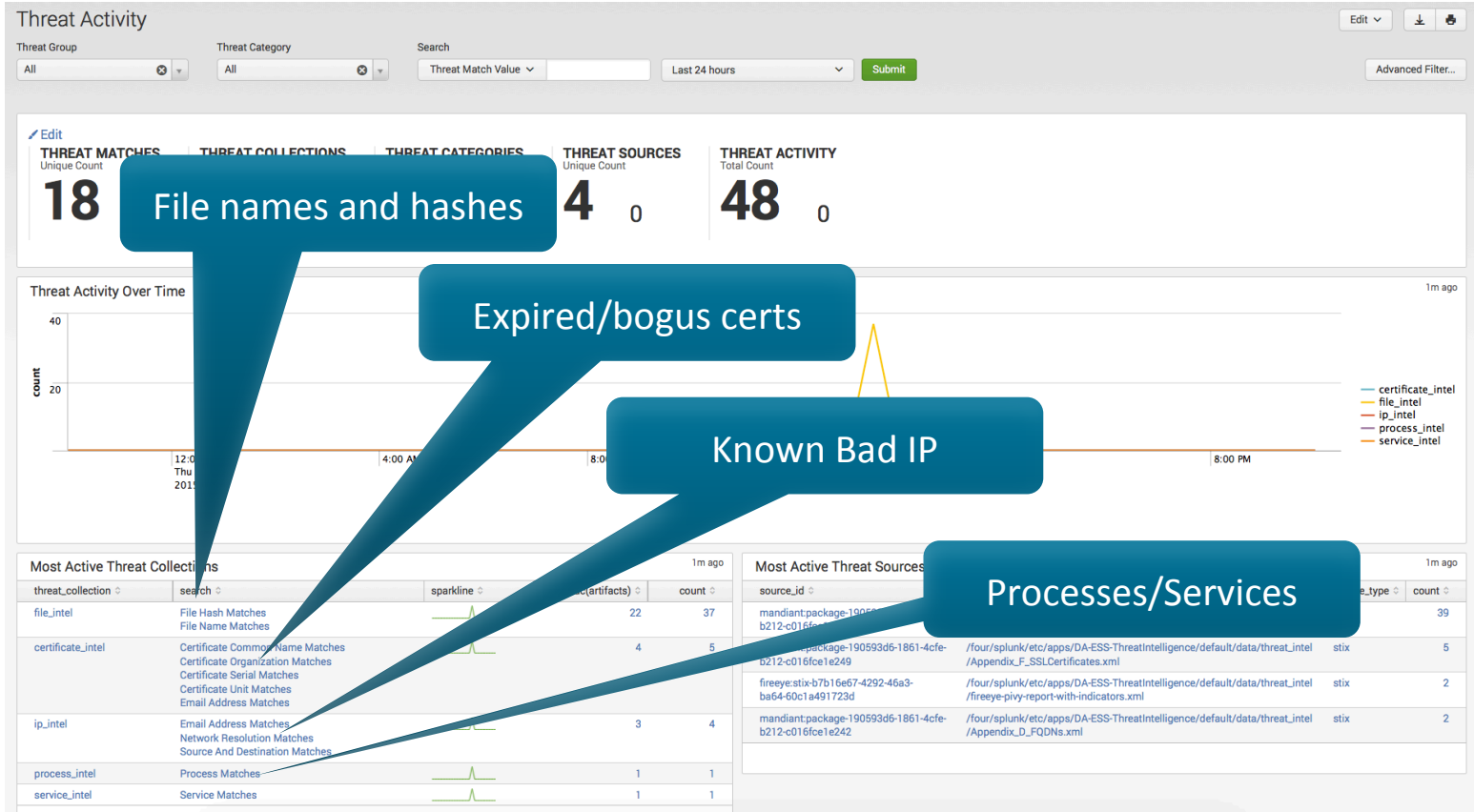
16: Evaluate use of screensaver locks

17: Identify lapses in local encryption

You could do all of that with the Universal Forwarder.



Threat Intelligence, you say?



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

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.

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

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

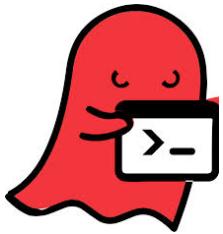
Tool usage:

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

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

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

e name is specified besides `https`, the tool checks the specified service using STARTTLS.
ill need to specify the correct port.



SLv3 Test Using cURL

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

eck the output, you want to see something similar

```
* SSL peer handshake failed
```

Rather than something like this:

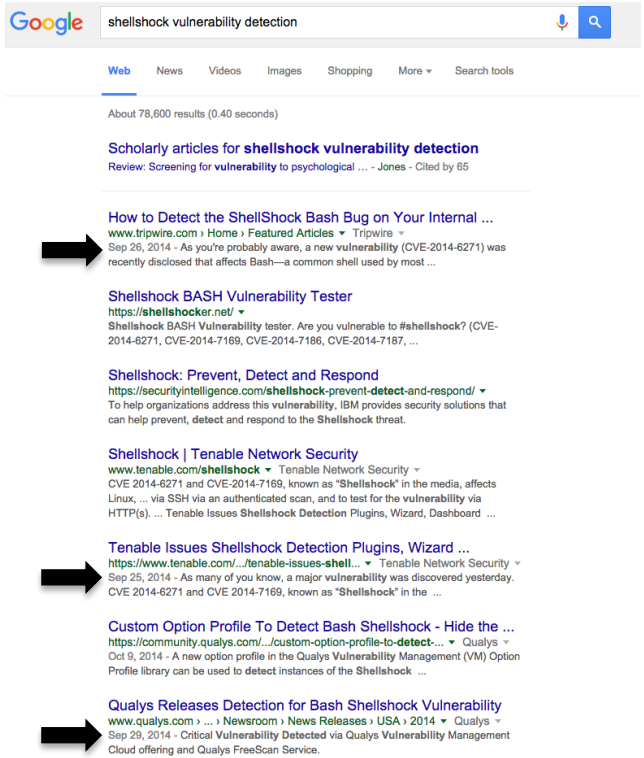
```
* SSL 3.0 connection using SSL_NULL_WITH_NULL_NULL
```

```
#!/bin/bash
#Version 3

echo "Installed glibc version(s)"

rv=0
for glibc_nvr in $( rpm -q --qf '%{name}-%{version}-%{release}.%{arch}\n' glibc ); do
    glibc_ver=$( echo "$glibc_nvr"  | awk -F- '{ print $2 }' )
    glibc_maj=$( echo "$glibc_ver"  | awk -F. '{ print $1 }')
    glibc_min=$( echo "$glibc_ver"  | awk -F. '{ print $2 }')

    echo -n "- $glibc_nvr:  "
    if [ "$glibc_maj" -gt 2  -o  \
         \( "$glibc_maj" -eq 2  -a  "$glibc_min" -ge 18 \) ]; 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
    fi
done

if [ $rv -ne 0 ]; then
    cat <<EOF

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/1332213> for remediation steps
EOF
fi

exit $rv
```

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.



Remember this?

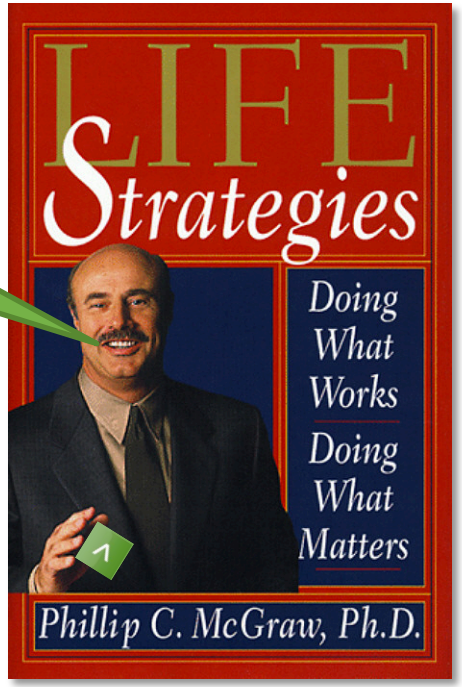
shellshock

- 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.

Could splunk> make this process more timely?

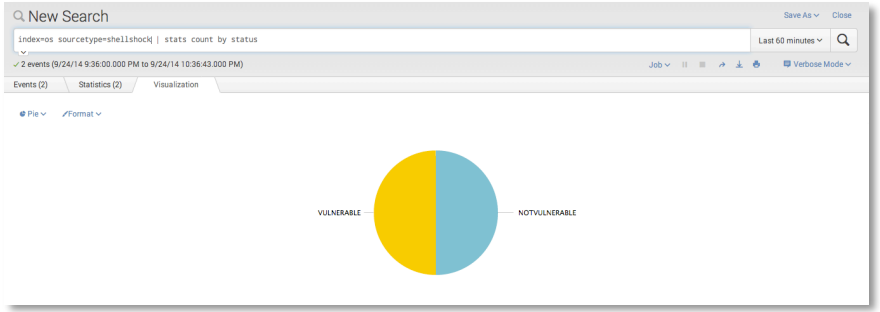
The Universal Forwarder as self-help guru

That UF sure does a lot by itself!



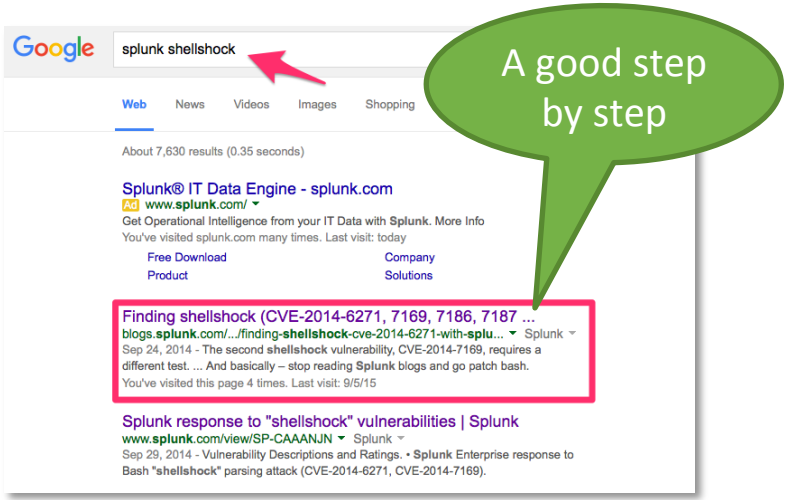
The Universal Forwarder as self-help guru

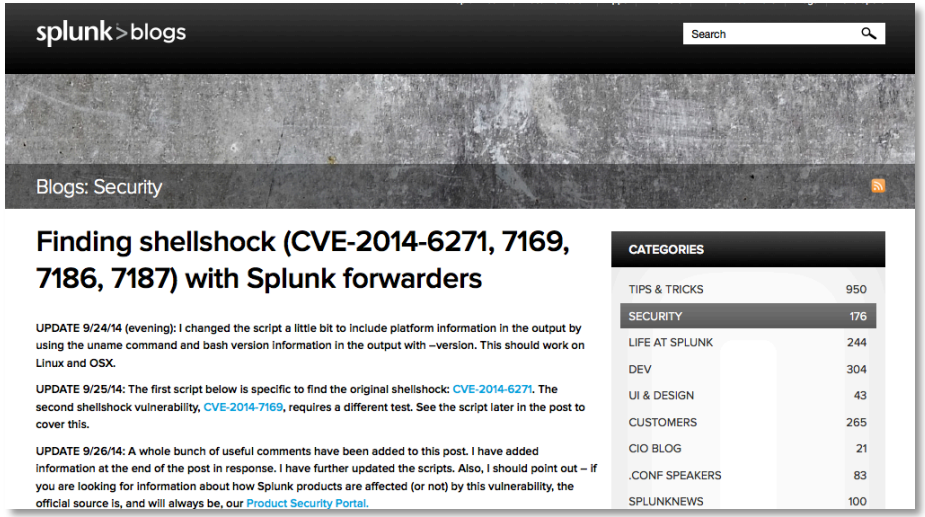
- If you had the Splunk UF on all of your production *NIX servers…
- You could **very quickly** program them to find shellshock (or ghost, or poodle, or heartbleed).
- You avoid Vulnerability Management Vendor Lag
- You could then report on remediation efforts over time.
- **And** the data ingest would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



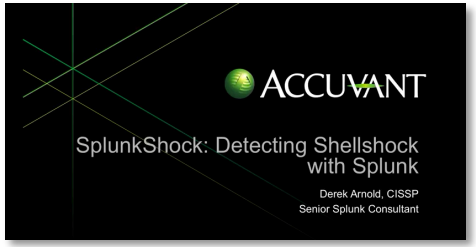


Use Case 3: UF for Shellshock Tracking

(Large payment processing company)

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

OPTIV

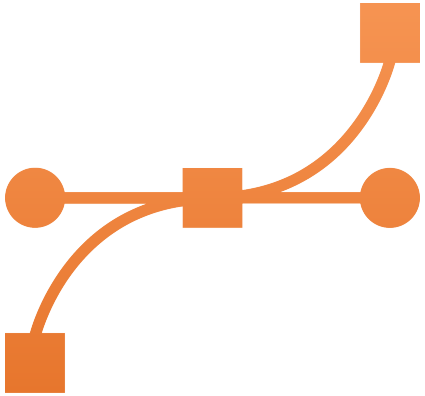


NASDAQ®

"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…"

Windows Sysinternals

TA-microsoft-sysmon

Microsoft

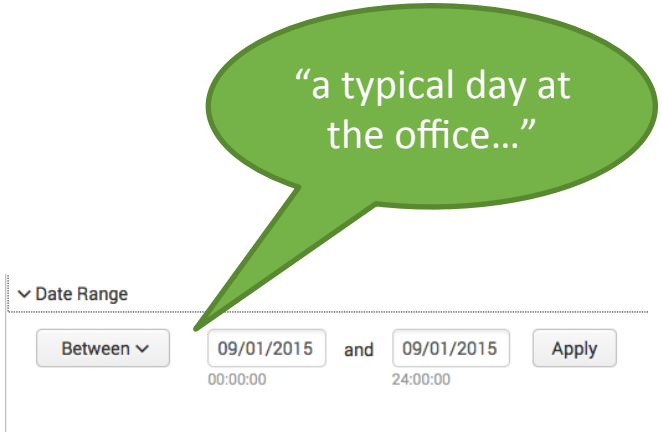
Splunk_TA_windows

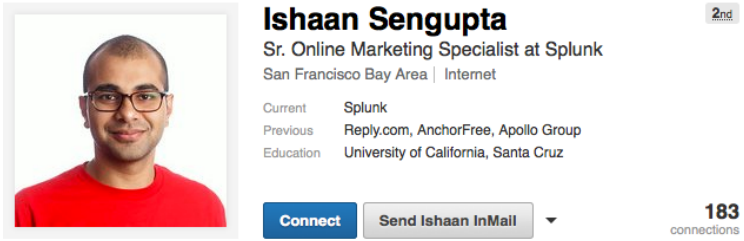
All this endpoint Splunking will blow up my license…

How much data?

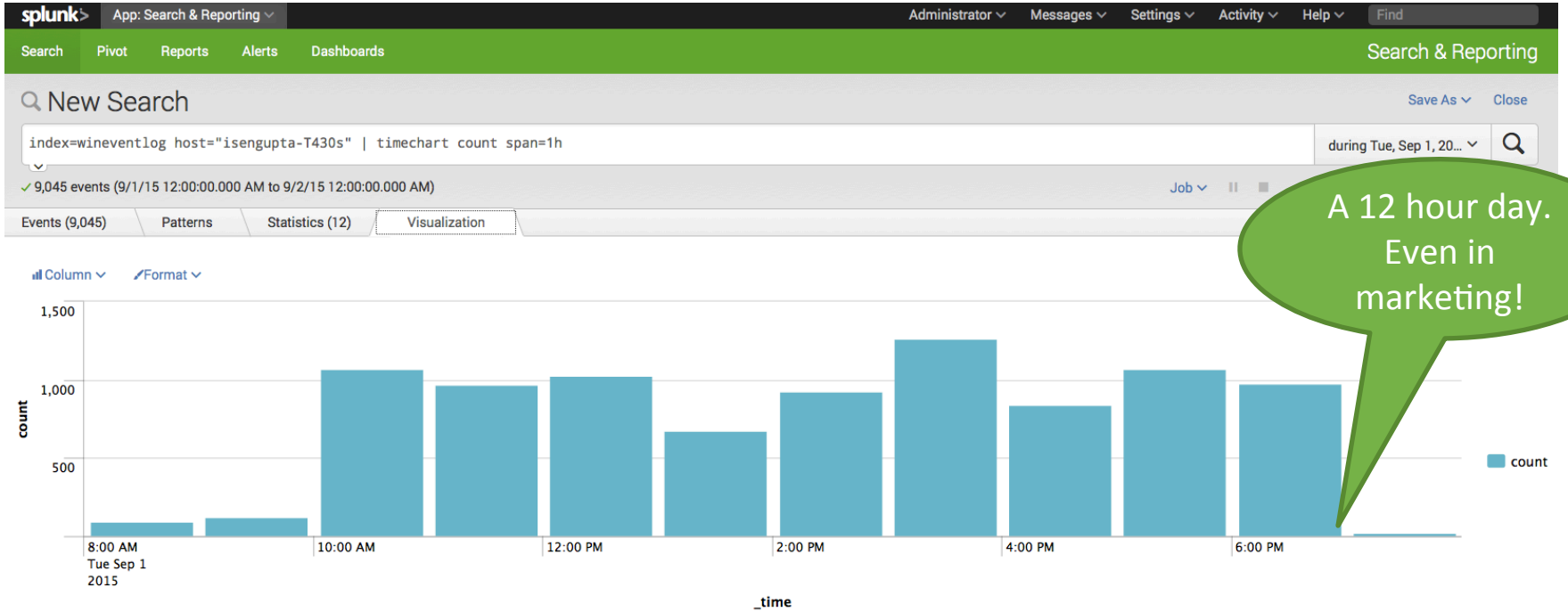
TA-microsoft-sysmon

Splunk_TA_windows

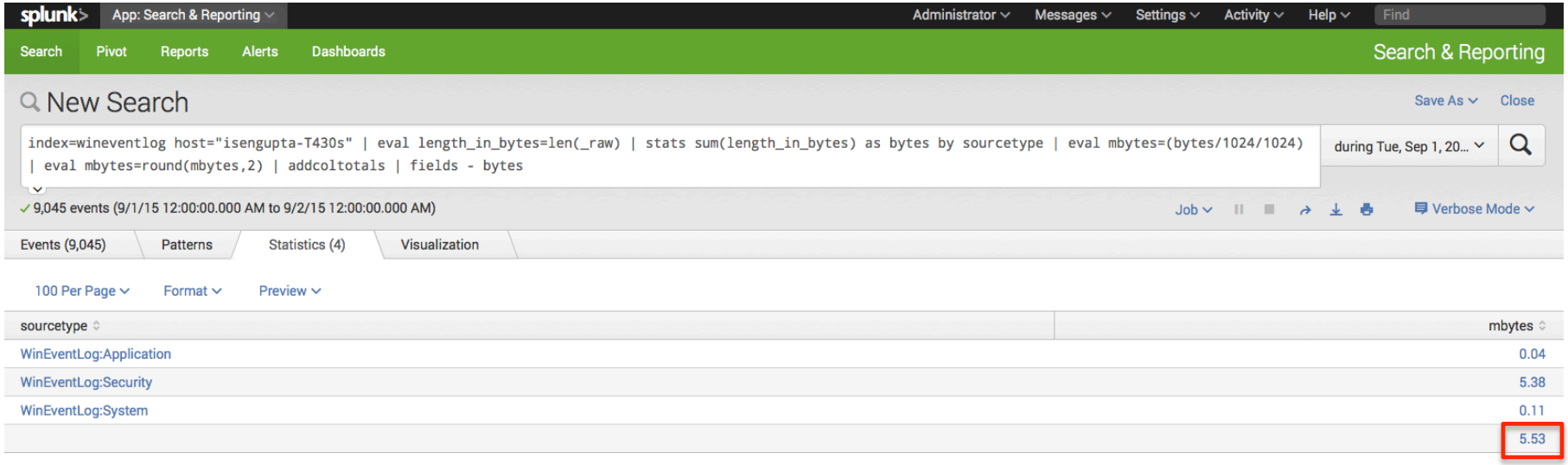




How much data?

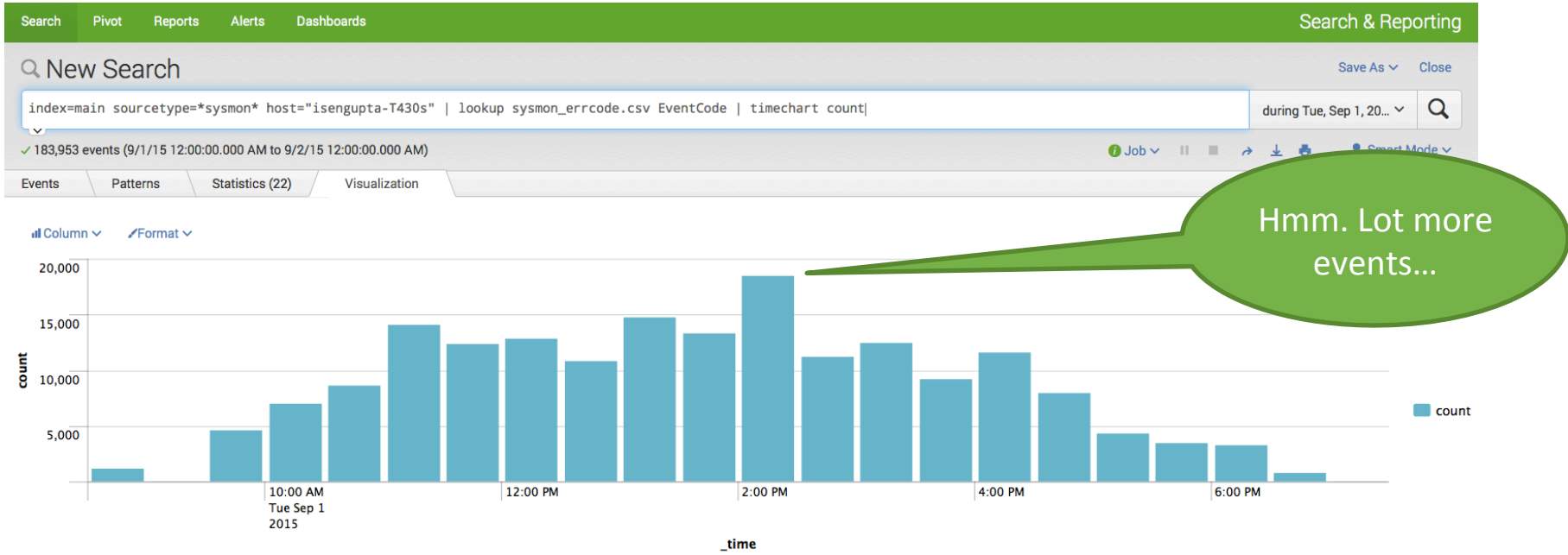


How much data?

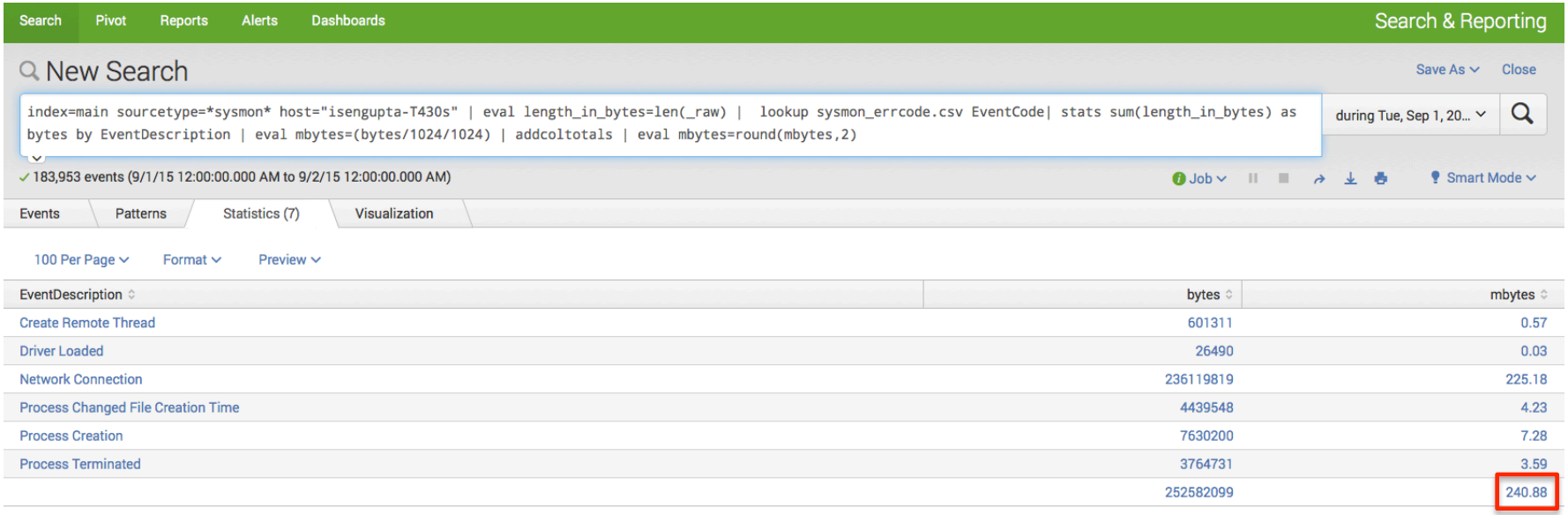


12 hours of standard event logs = 5.5 MB. Nice!

How much data?



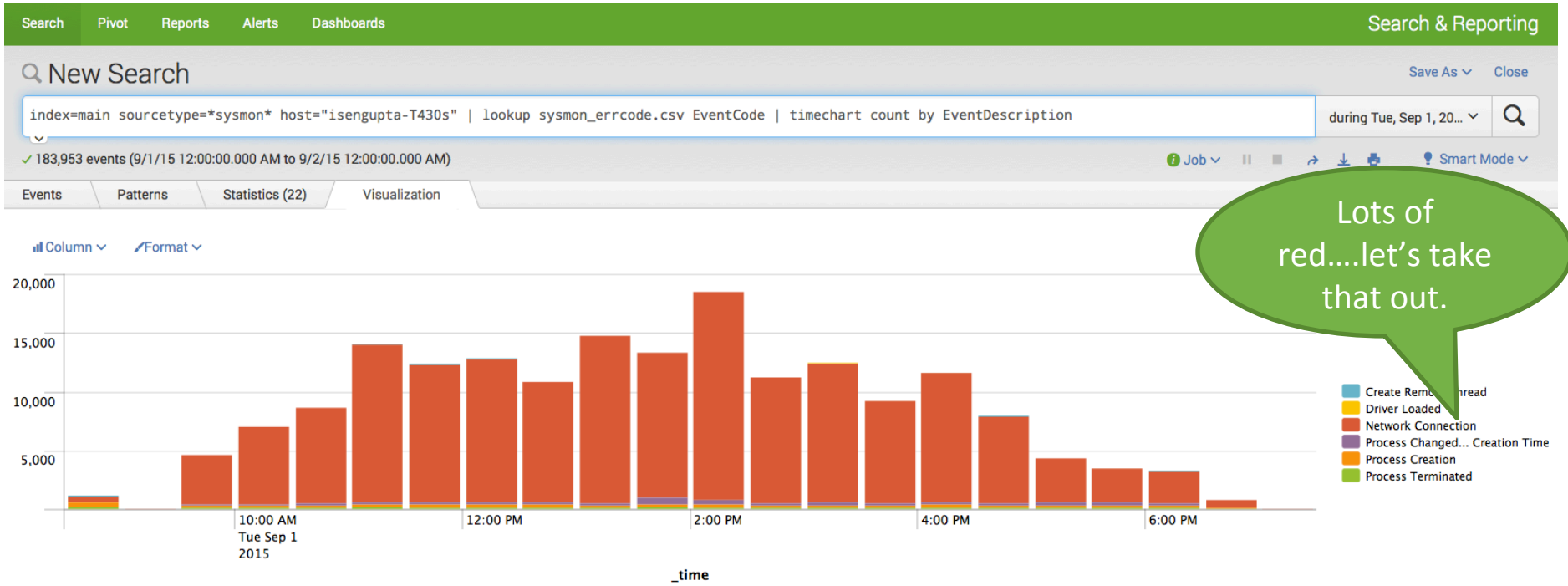
How much data?



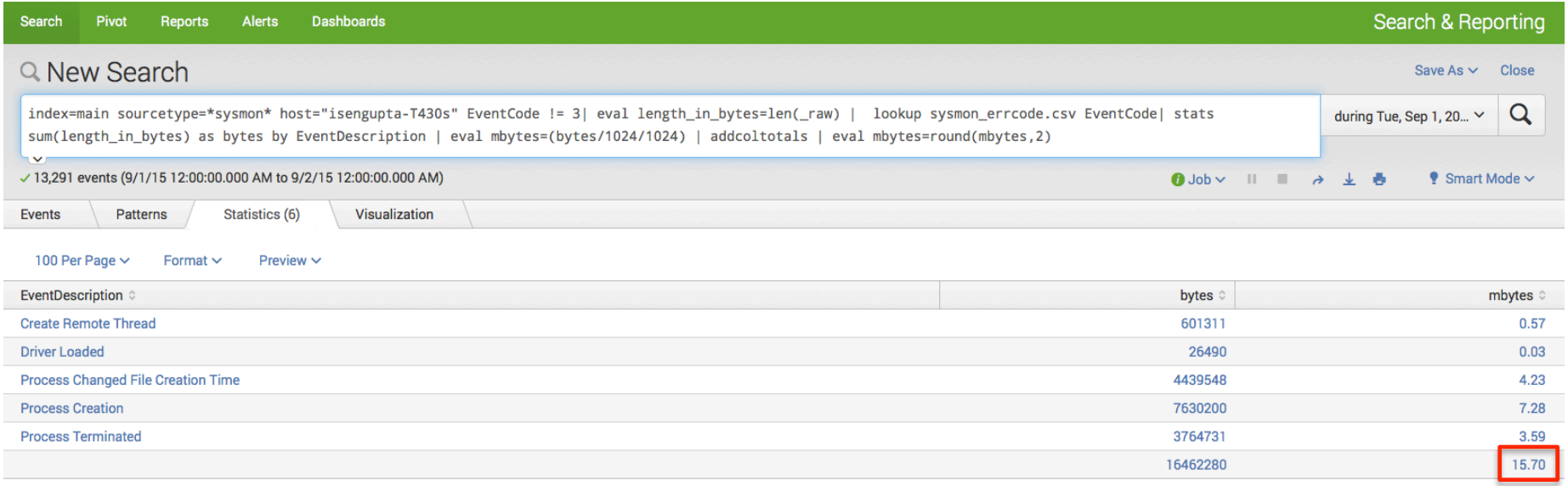
EventDescription	bytes	mbytes
Create Remote Thread	601311	0.57
Driver Loaded	26490	0.03
Network Connection	236119819	225.18
Process Changed File Creation Time	4439548	4.23
Process Creation	7630200	7.28
Process Terminated	3764731	3.59
	252582099	240.88

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

How much data?



How much data?



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…

Search | Pivot | Reports | Alerts | Dashboards — Search & Reporting

New Search — Save As — Close

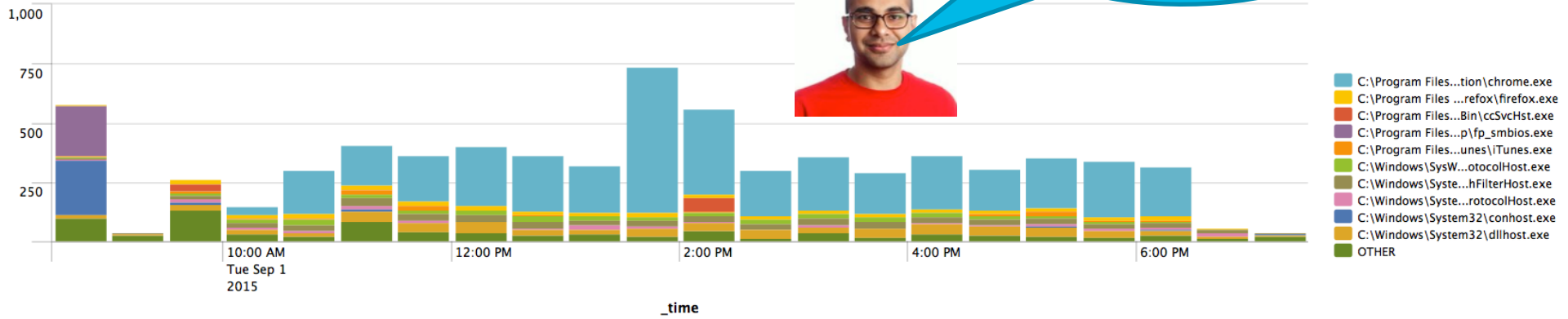
```
index=main sourcetype=*sysmon* host="isengupta-T430s" EventCode != 3 app!=*splunk* | timechart count by app
```

Tue, Sep 1, 20…

✓ 7,214 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM) — Smart Mode

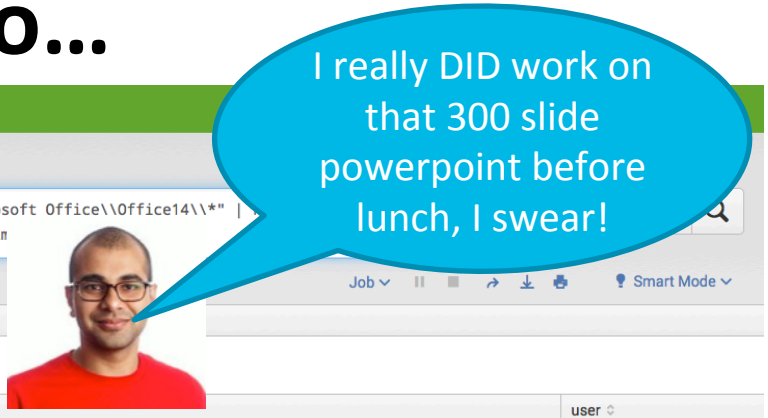
Events | Patterns | Statistics (22) | Visualization

Column — Format



I surfed a whole lot in Chrome today… listened to some tunes, too!

And also…



Search | Pivot | Reports | Alerts | Dashboards

New Search

```
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 +_tim
```

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

Job | Smart Mode

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

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.

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

THANK YOU

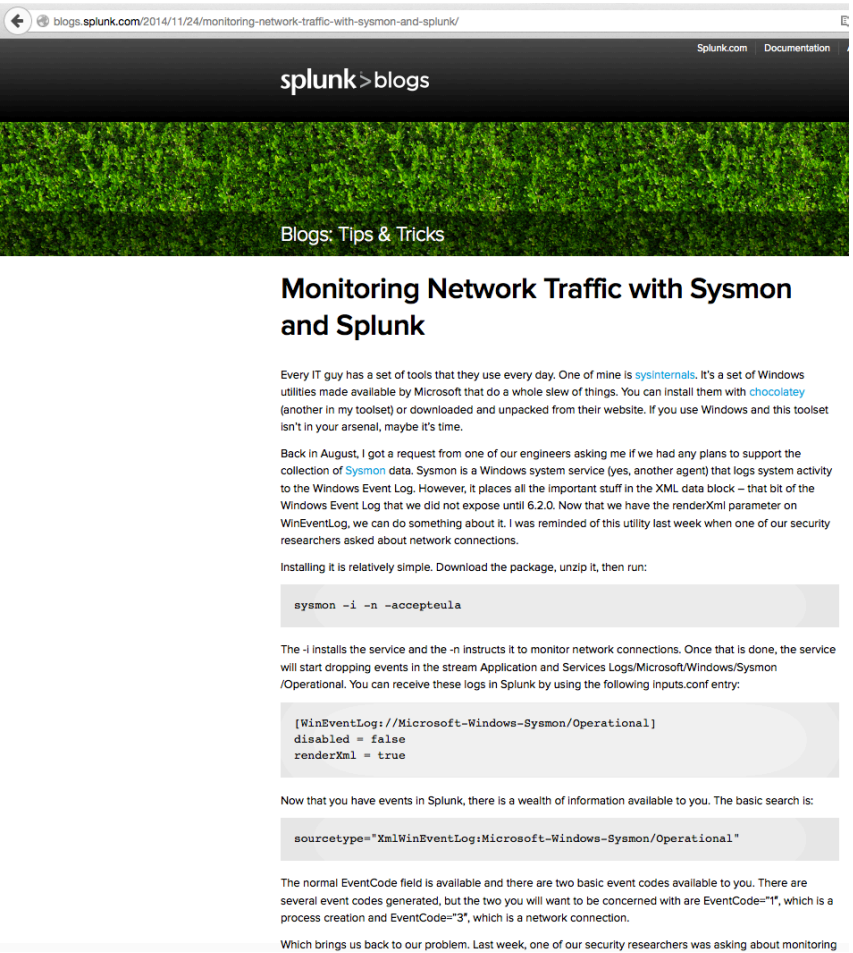
splunk>

Appendix

splunk>

Sysmon Details

splunk>



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

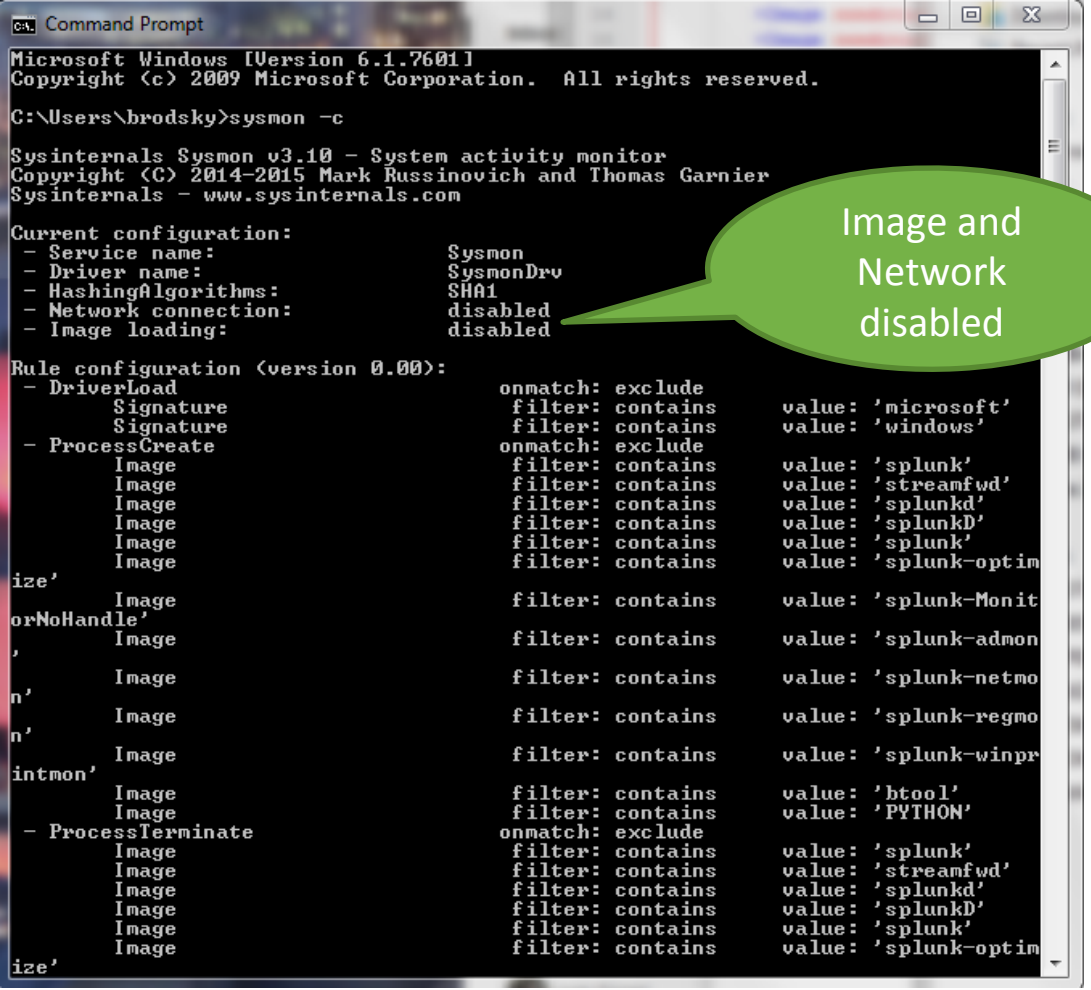
```
<Sysmon schemaversion="2.0">
  <HashAlgorithms>SHA1</HashAlgorithms>
  <EventFiltering>
      <!-- Log all drivers except if the signature -->
      <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
        <Signature condition="contains">microsoft</Signature>
        <Signature condition="contains">windows</Signature>
    </DriverLoad>
      <!-- Exclude certain processes that cause high event volumes -->
    <ProcessCreate default="include">
      <Image condition="contains">splunk</Image>
      <Image condition="contains">streamfwd</Image>
      <Image condition="contains">splunkd</Image>
      <Image condition="contains">splunkD</Image>
      <Image condition="contains">splunk</Image>
      <Image condition="contains">splunk-optimize</Image>
      <Image condition="contains">splunk-MonitorNoHandle</Image>
      <Image condition="contains">splunk-admon</Image>
      <Image condition="contains">splunk-netmon</Image>
      <Image condition="contains">splunk-regmon</Image>
      <Image condition="contains">splunk-winprintmon</Image>
      <Image condition="contains">btool</Image>
      <Image condition="contains">PYTHON</Image>
    </ProcessCreate>
    <ProcessTerminate default="include">
      <Image condition="contains">splunk</Image>
      <Image condition="contains">streamfwd</Image>
      <Image condition="contains">splunkd</Image>
      <Image condition="contains">splunkD</Image>
      <Image condition="contains">splunk</Image>
      <Image condition="contains">splunk-optimize</Image>
      <Image condition="contains">splunk-MonitorNoHandle</Image>
      <Image condition="contains">splunk-admon</Image>
      <Image condition="contains">splunk-netmon</Image>
      <Image condition="contains">splunk-regmon</Image>
      <Image condition="contains">splunk-winprintmon</Image>
      <Image condition="contains">btool</Image>
      <Image condition="contains">PYTHON</Image>
    </ProcessTerminate>
    <FileCreateTime default="include">
      <Image condition="contains">splunk</Image>
      <Image condition="contains">streamfwd</Image>
      <Image condition="contains">splunkd</Image>
      <Image condition="contains">splunkD</Image>
      <Image condition="contains">splunk</Image>
      <Image condition="contains">splunk-optimize</Image>
      <Image condition="contains">splunk-MonitorNoHandle</Image>
      <Image condition="contains">splunk-admon</Image>
      <Image condition="contains">splunk-netmon</Image>
      <Image condition="contains">splunk-regmon</Image>
      <Image condition="contains">splunk-winprintmon</Image>
      <Image condition="contains">btool</Image>
      <Image condition="contains">PYTHON</Image>
      </FileCreateTime>
  </EventFiltering>
```

Filter out all the Splunk activity

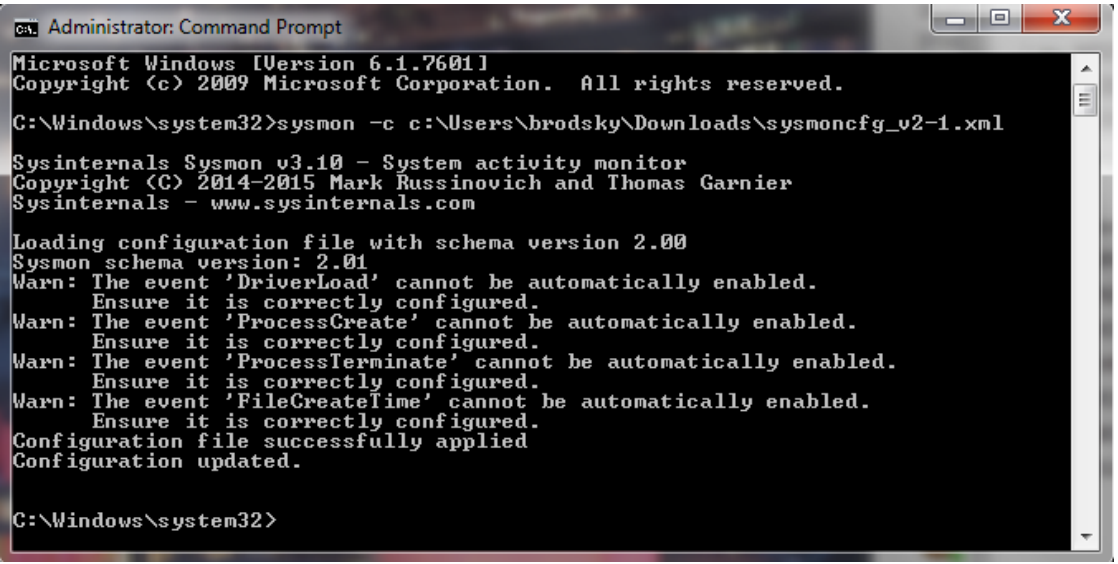
- This works for Sysmon 3.1+
- Add what you need
- If you actually want Image and Network data, add those stanzas
- Email brodsky@splunk.com for links to example files!

Sysmon Config List

- sysmon –c with no filename will dump config



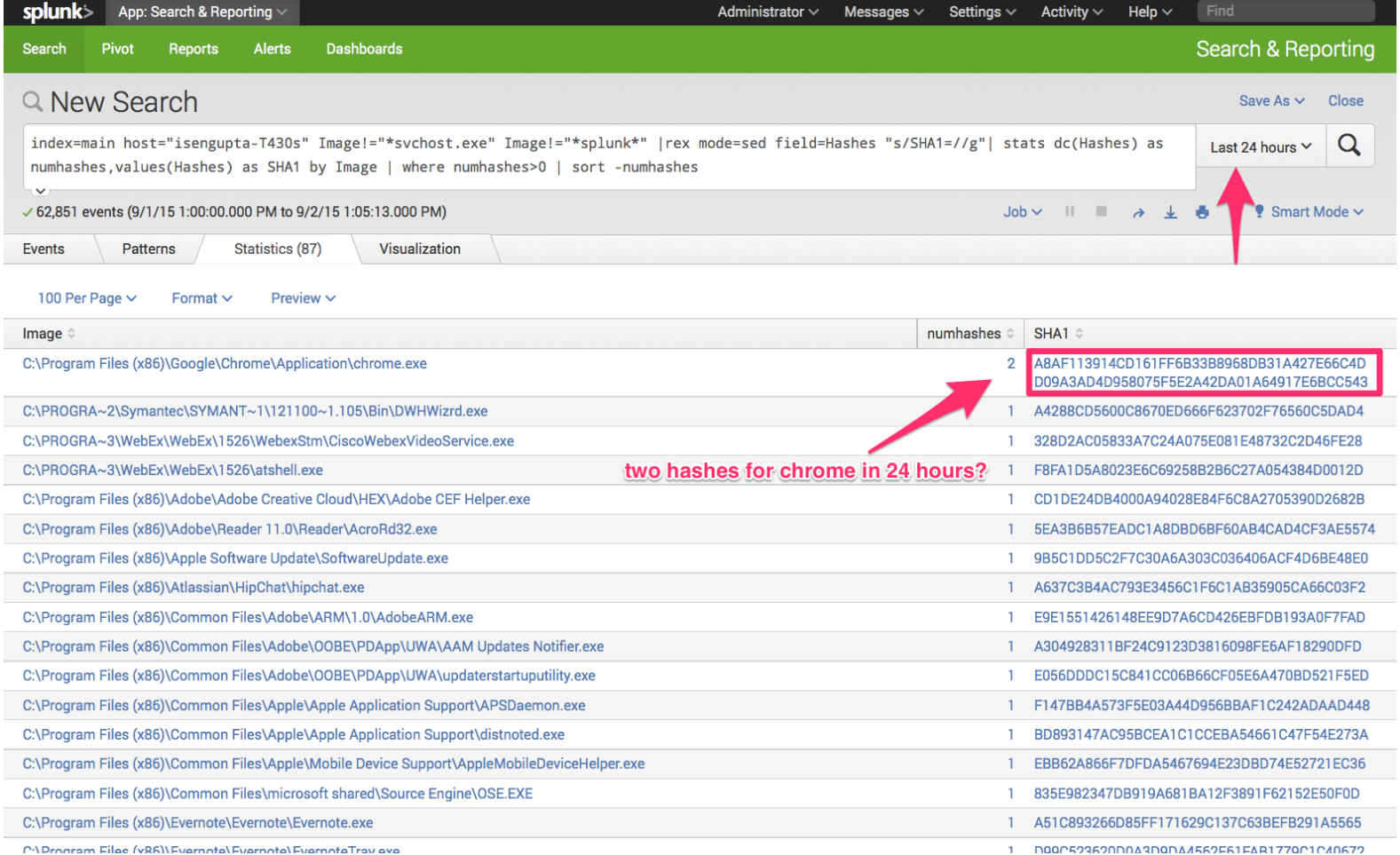
Sysmon Config Load



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

Hash Analysis with Sysmon

splunk>


splunk> App: Search & Reporting
Administrator Messages Settings Activity Help Find
Search Pivot Reports Alerts Dashboards
Search & Reporting
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 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 D09A3AD4D958075F5E2A42DA01A64917E6BCC543
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
two hashes for chrome in 24 hours?
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 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\updaterstartuputility.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\distnoted.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

virustotal

SHA256: 76fa85ad2ca9eadedb5b018d6432fd7d6d90a0893e9b1676c3b686001ab9eff1

File name: chrome.exe

Detection ratio: 0 / 56 — not malicious

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

20 14

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

virustotal

SHA256: f9b8b1efcf5c0d12fc444ee1d910ce5342814bea83f9e221f8931e0f28aae569

File name: chrome.exe

Detection ratio: 0 / 56 — not malicious either

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

0 0

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 — a new Chrome version!
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

virustotal

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.

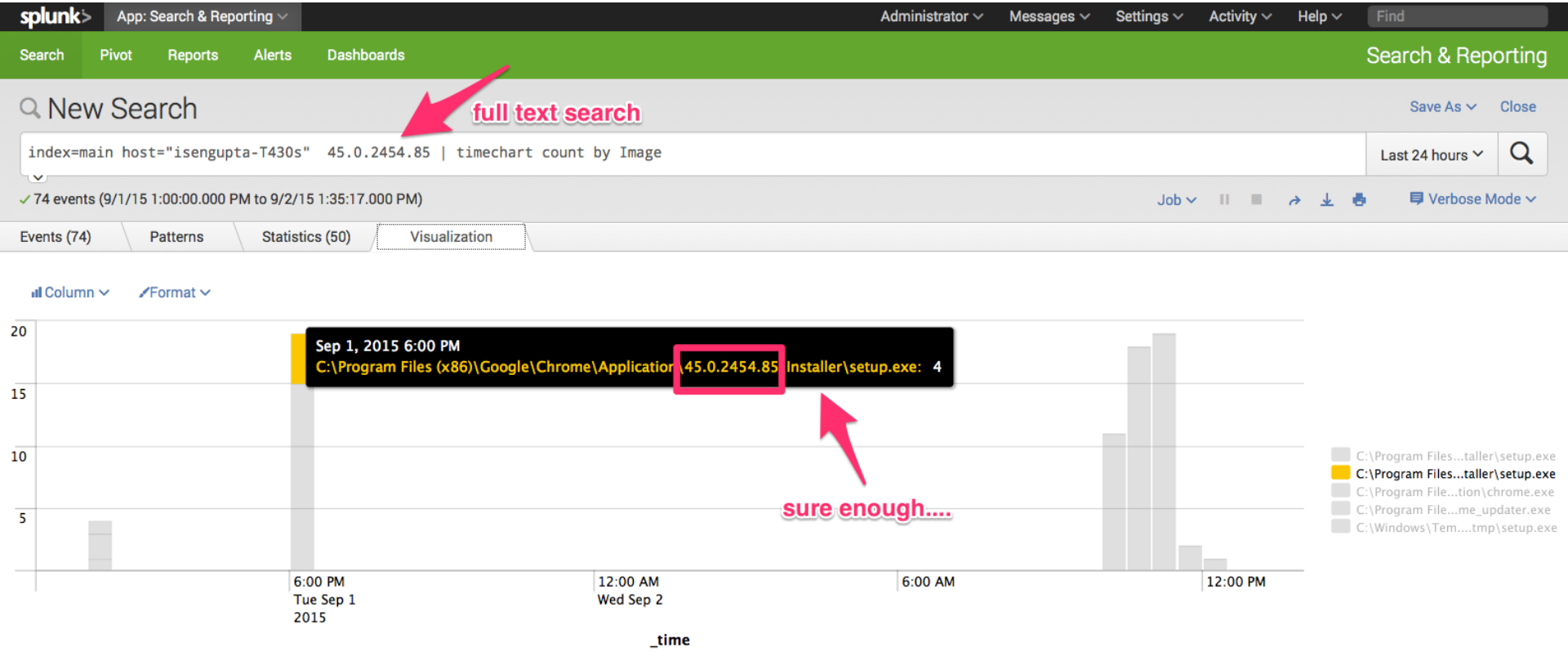
Analysis | File detail | Relationships | Additional information | Comments 0 | Votes

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


splunk> App: Search & Reporting
Administrator Messages Settings Activity Help Find
Search Pivot Reports Alerts Dashboards
Search & Reporting
New Search
full text search
Save As Close
index=main host="isengupta-T430s" 45.0.2454.85 | timechart count by Image
Last 24 hours
74 events (9/1/15 1:00:00.000 PM to 9/2/15 1:35:17.000 PM)
Job Verbose Mode
Events (74) Patterns Statistics (50) Visualization
Column Format
20
15
10
5
Sep 1, 2015 6:00 PM
C:\Program Files (x86)\Google\Chrome\Application\45.0.2454.85 Installer\setup.exe: 4
sure enough....
6:00 PM
Tue Sep 1
2015
12:00 AM
Wed Sep 2
6:00 AM
12:00 PM
_time
C:\Program Files...taller\setup.exe
C:\Program Files...taller\setup.exe
C:\Program File...tion\chrome.exe
C:\Program File...me_updater.exe
C:\Windows\Tem....tmp\setup.exe

Windows Registry Monitoring

splunk>

Registry Monitoring config

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

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

[WinRegMon://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

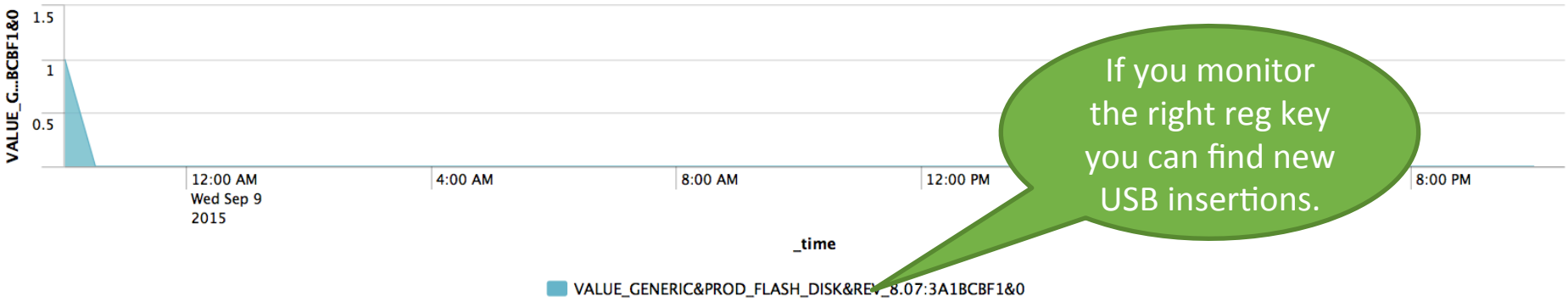
Edit | More Info

Select a POS

Last 24 hours | DAL-TX-POS2

New USB Disk Insertions

<1m ago



If you monitor the right reg key you can find new USB insertions.

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	cou
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

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 ever 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