Security Operations Use Cases: 'Cause Bears, Pandas, and Sandworms

Ryan Chapman & Lisa Tawfall

Bechtel Corporation

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.

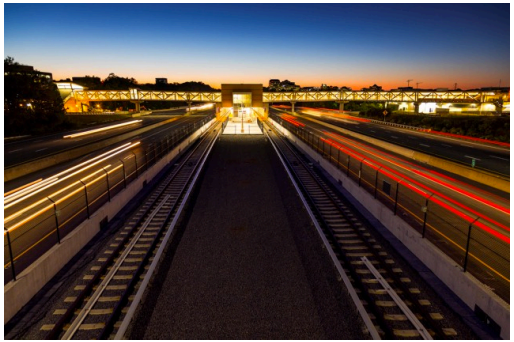
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the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

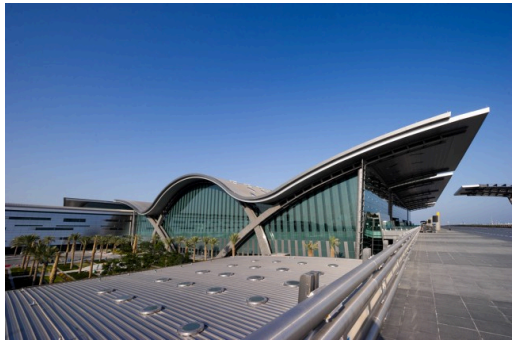
Agenda

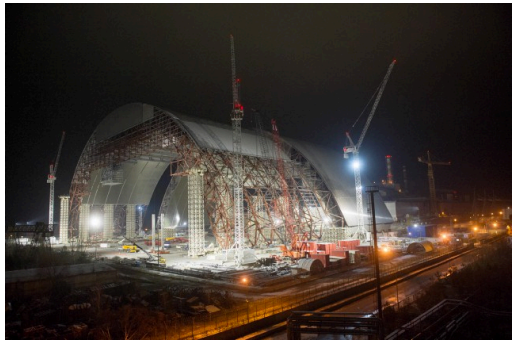
- Who Are We?
- Overview of Security @ Bechtel
- Why Splunk
- Use Cases

Bechtel Corporation

Bechtel Corporation is the largest construction and civil engineering company in the U.S., making the company a target rich environment. Since 2011, Bechtel has set out to build a world-class Security Operations Center, which relies heavily on Splunk.







Ryan Chapman

@rj_chap

- Network Security Monitoring Analyst
- Incident Handler
- CIRT / SOC Liaison
- “Did You Check Splunk?” Guy
- No Really. Did You Check Splunk?

Lisa Tawfall

@ltawfall

- Security Unicorn (Yes, really)
- Lead for the team that manages security infrastructure at Bechtel
- Splunk Administrator
- Breaker of Splunk
- Fixer of Splunk

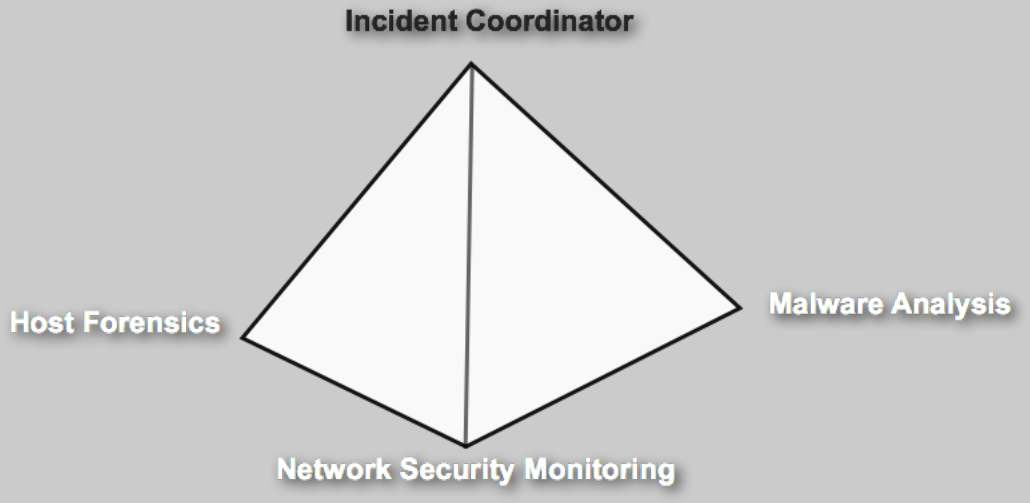
Security @ Bechtel

splunk>

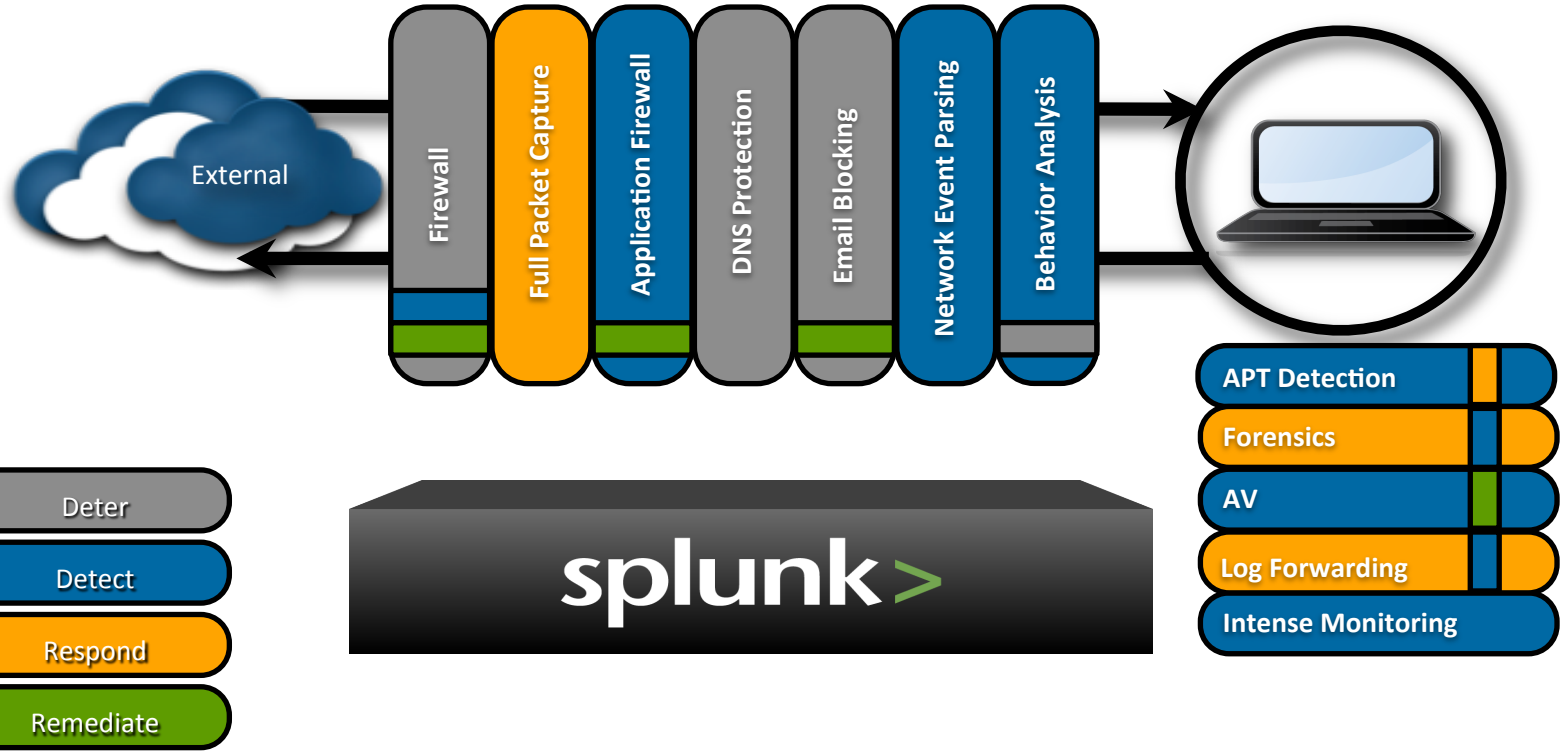
Background

- How were you doing it before **Splunk?**
- How much **time** would it take you?
- Why wasn't it **working?**

Post Remediation Structure



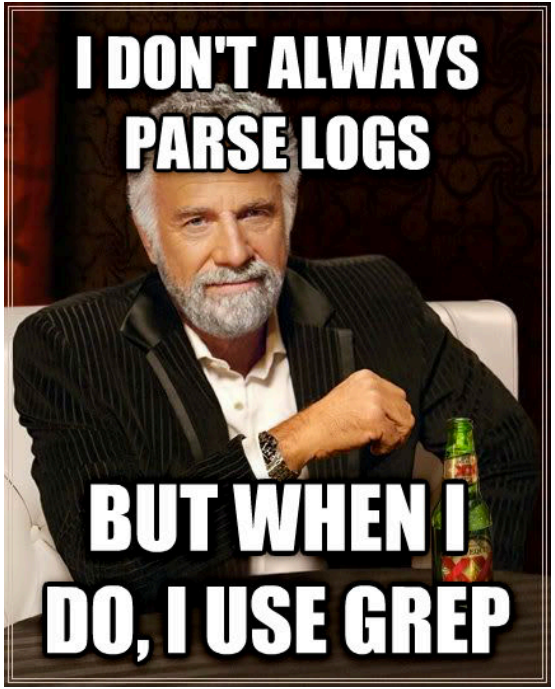
The Security Stack



Why Splunk?

Because it's awesome!

- Better than GREP?
- Parsing Individual Logs?
  - 2.35TB/day License
- Primary uses:
  - Alert generation
  - Response!
    - The "5 W's"



Why Splunk?

Bechtel is target rich!

Obligatory Splunk Quote

"We wouldn't be able to do our jobs without Splunk"

Use Case One

splunk>

Use Case 1

"These computers are infected"

- Project site contacts the SOC
  - "Symantec is not catching infections."
  - "OK. what's going on?"
  - "Infections."
- Additional info requested
  - 5 Hostnames provided
  - Multiple occurrences of ".Trashes"

Initial Analysis

It's Splunk time, baby

- Symantec Enterprise Protection (SEP)
  - Is SEP leaving as-is?
- Initial focus: action taken
  - Looking for "**left alone**"

Symantec Enterprise Protection (SEP) Logs

Left alone?

earliest=02/01/2015:00:00:00
latest=04/01/2015:00:00:00 **index=sep**
sourcetype="sep12:risk" OR
sourcetype="sep12:proactive" OR
sourcetype="sep12:ids"
(src="[REDACTED]" OR src="[REDACTED]" OR
src="[REDACTED]" OR src="[REDACTED]" OR
src="[REDACTED]")
action="Left Alone"
| table event_time, src, hash_value,
scan_type, action, actual_action

SEP Logs cont'd

Are we getting logs?

- Try to avoid false negatives!

src	hash_value	scan_type	action	actual_action
[redacted]	D84A[redacted]	Scheduled Scan	blocked blocked	Quarantined
[redacted]	29DB[redacted]	DefWatch	blocked blocked	Quarantined
[redacted]	87C2[redacted]	Scheduled Scan	blocked	Cleaned by deletion
[redacted]	87C2[redacted]	Real Time Scan	blocked	Cleaned by deletion

- Yes, we have logs
- action = "blocked"
  - *actual_action != "Left Alone"*

Windows Logging Service (WLS)

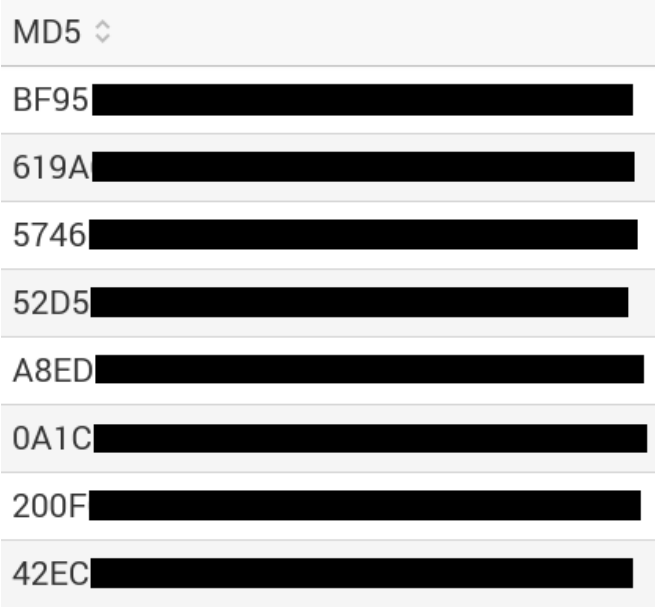
Give me your tired, your weak, **YOUR HASHES**

earliest=03/01/2015:00:00:00
latest=03/03/2015:00:00:00

index=wls EventID="4688"

(Computer="[REDACTED]"
OR Computer="[REDACTED]"
OR Computer="[REDACTED]"
OR Computer="[REDACTED]"
OR Computer="[REDACTED]")

| **stats count by MD5** | sort 0 -count



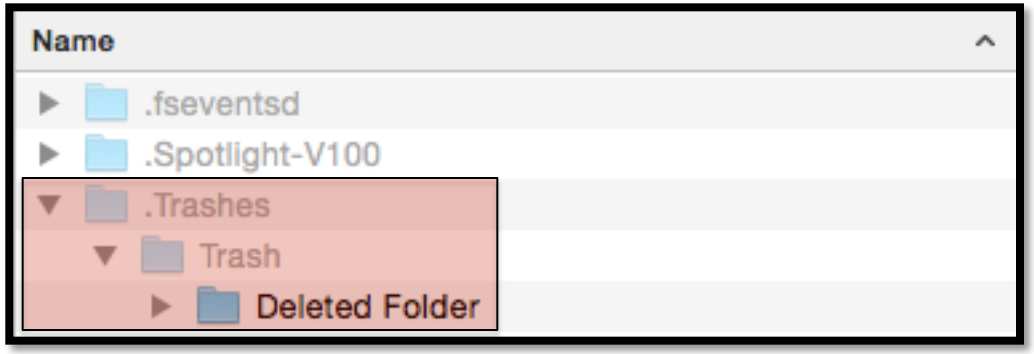
Hash Analysis

We Haz tools

```
nfworkshop:bacon ryanchapman$ ./bacon.py -i input.txt

Using the following OUTPUT files:
TXT output file: ./20150824_032558-bacon_results.txt
CSV output file: ./20150824_032558-bacon_results.csv

***************** Hash *****************
BF95[redacted]
****************************************

querying virustotal...
checking for known bad stuff...
checking for related isight reports...

[*] Processed indicator #1

***************** Hash *****************
619A[redacted]
****************************************

querying virustotal...
```

Indicator	Hits	Mal_Hits
5746[redacted]	0	None
52D5	0	None
A8ED	1	Hash found at ThreatExpert: 2 December 2014, 00:15:39
619A	0	None
42EC	0	None
0A1C	0	None
BF95	0	None
EC7B	1	VT Ratio 11 / 54 (!!)

HFS/HFS+ & “.Trashes”



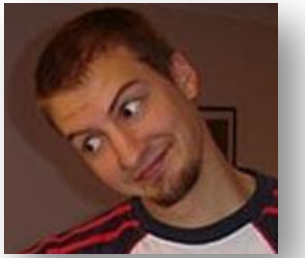

```
nfworkshop:501 ryanchapman$ cd /Volumes/BSLV15EK/.Trashes/501/
nfworkshop:501 ryanchapman$ ls -la
total 96
drwxrwxrwx@ 1 ryanchapman  staff  16384 Aug 27 14:22 .
drwxrwxrwx@ 1 ryanchapman  staff  16384 Aug 27 14:22 ..
drwxrwxrwx  1 ryanchapman  staff  16384 Aug 27 14:21 Deleted Folder
nfworkshop:501 ryanchapman$ id -u
501
```

Rummaging Through the .Trashes

These sites don't use Macs…

```
earliest=03/01/2015:00:00:00
latest=03/15/2015:00:00:00
index=wls EventID=4688
CommandLine="*.Trashes*"
| rex field=Computer
  "(?<site_code>[A-Za-z]{3})"
| eval site_code = upper(site_code)
| stats count by site_code
| sort 0 -count
```

site_code	count
[redacted]	4637
[redacted]	99
[redacted]	35
[redacted]	3
[redacted]	1
[redacted]	1



Process Execution

Event code 4688

earliest=02/01/2015:00:00:00
latest=04/01/2015:00:00:00

index=wls EventID=4688 CommandLine="*.Trashes*"

| table _time, Computer, SubjectDomainName, SubjectUserName, **BaseFileName**, **CommandLine**, CompanyName, CreatorProcessName, NewProcessName, FileDescription, FileVersion, MD5

BaseFileName	CommandLine
wscript.exe	wscript '.Trashes\902\pmeuu.js'
wscript.exe	wscript '.Trashes\451\wjsdim.js'
wscript.exe	wscript '.Trashes\602\seaqe.js'
wscript.exe	wscript '.Trashes\749\vyhvewx.js'
wscript.exe	wscript '.Trashes\749\vyhvewx.js'
wscript.exe	wscript '.Trashes\520\aynxlohw.js'
wscript.exe	wscript '.Trashes\520\aynxlohw.js'
wscript.exe	wscript '.Trashes\517\ikfue.js'
wscript.exe	wscript '.Trashes\517\ikfue.js'

JS.Proslikefan.B

Similar to: JS.Bondat

- Google to the rescue!
- Symantec write-up
  - **Sample not yet detected**
  - **Eventually set to →**
- Windows scripting host
  - WScript.exe
  - Runs .vbs and **.js** Scripts

Discovered: October 31, 2014
Updated: November 3, 2014 10:54:59 PM
Type: Trojan, Worm
Infection Length: 43,287 KB
Systems Affected: Windows 7, Windows Vista

The worm may be spread through USB drives.

When the worm is executed, it may copy itself to the following locations:

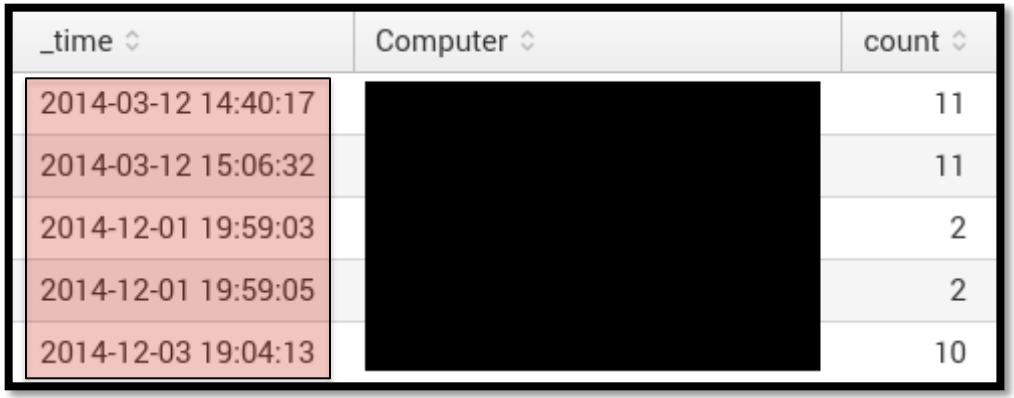
- %Driveletter%:\.Trashes\[CALCULATED VALUE]\[CALCULATED VALUE].js
- %UserProfile%\Local Settings\Temp\[CALCULATED VALUE].js
- %UserProfile%\[CALCULATED VALUE].js
- %UserProfile%\AppData\Roaming\[CALCULATED VALUE].js

(Symantec, 2014)

Identifying Infected Hosts

Initial host(s)?

earliest=01/01/2014:00:00:00
latest=04/01/2015:00:00:00
index=wls EventID=4688
CommandLine="*.Trashes*"
| regex CommandLine="Trashes\\\[0-9]{3}\\\[A-Za-z]{4,8}\\.js"
| fields _time, Computer
| eventstats count by Computer
| dedup Computer | sort 0 _time
| table _time, Computer, count



_time	Computer	count
2014-03-12 14:40:17	[redacted]	11
2014-03-12 15:06:32		11
2014-12-01 19:59:03		2
2014-12-01 19:59:05		2
2014-12-03 19:04:13		10

Now What?

Remediation issues

- Cannot remediate without addressing USB drives

- Steps to remediate:
  - **1) Identify infected drives**
    - Provide list to project IT
  - 2) Project IT burns USB drives
  - 3) Implement new USB policy
  - 4) Rebuild hosts
  - *5) Cross fingers*

USB Drive Identification

via WLS Logs

```
earliest=03/01/2015:00:00:00
latest=03/03/2015:00:00:00
index=wls* EventID="20001"
(Computer="[REDACTED]" OR
 Computer="[REDACTED]" OR
 Computer="[REDACTED]" OR
 Computer="[REDACTED]" OR
 Computer="[REDACTED]")
| table _time, Computer, SetupClass,
DriverDescription, DeviceInstanceID,
DriverName
```

DriverDescription	DeviceInstanceID
WPD FileSystem Volume Driver	WPDBUSENUMROOT\UMB\2&3
Generic volume	STORAGE\VOLUME_??_USBST
Disk drive	USBSTOR\DISK&VEN_SANDISK
USB Mass Storage Device	USB\VID_0781&PID_556B\2004
WPD FileSystem Volume Driver	WPDBUSENUMROOT\UMB\2&3
Generic volume	STORAGE\VOLUME_??_USBST
Disk drive	USBSTOR\DISK&VEN_SMI&PRO
USB Mass Storage Device	USB\VID_090C&PID_1000\6&29

USB Drive Identification cont'd

via SEP Logs

earliest=03/01/2015:00:00:00
latest=03/03/2015:00:00:00

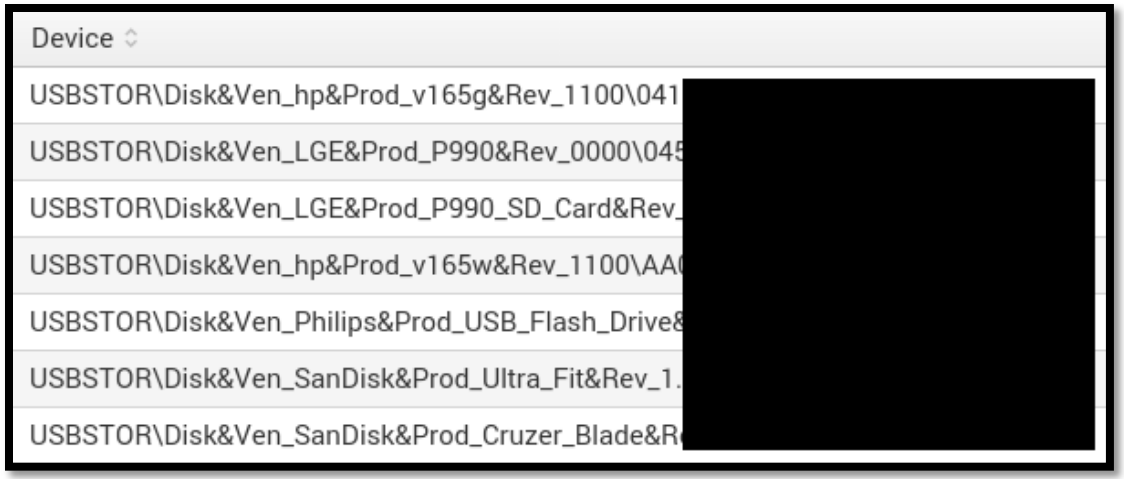
index=sep eventtype=nix_usb

([REDACTED – Hostnames Here])

| dedup dest_nt_host, device_id

| sort 0 dest_nt_host

| table dest_nt_host, device_id



USB Drive Identification cont'd

Parsing USB device descriptor

```
| dedup dest_nt_host, device_id
| rex field=device_id "USBSTOR\\\
(?<type>.*)&Ven_
(?<vendor>.*)&Prod_
(?<product>.*)&Rev_
(?<revision>.*$)"
| sort 0 dest_nt_host
| table dest_nt_host, type, vendor,
product, revision
```

vendor	product	revision
hp	v165g	1100\041
hp	v165w	1100\AA
LGE	P990	0000\045
LGE	P990_SD_Card	0000\045
hp	v165g	1100\041
hp	v165w	1100\AA
Philips	USB_Flash_Drive	PMAP\07
SanDisk	Cruzer_Blade	1.26\200
SanDisk	Ultra_Fit	1.00\4C5
SanDisk	Cruzer_Blade	1.26\200

Use Case 1 Wrap-Up

Remediation details

- **287 Hosts Rebuilt** Initially
  - + ~40 Hosts over time
  - 3 Sites affected heavily
- USB drive policy changes
  - We found 1,000s in use
    - **Some hosts > 20 a day!**
  - Project IT in charge of drives
  - Greater focus on USB dangers
- **Ongoing alert via saved search**

Use Case Two

splunk>

Use Case 2

Vetting threat intel

- Intel, Intel, Intel – It's every where
- Paid feeds, open source, blogs, twitter, that guy you worked wit two companies ago…
- How do you process all those Indicators of Compromise (IOCs)

Vetting Threat Intel

The Naikon APT

Tracking Down Geo-Political Intelligen One Nation at a Time

By Kurt Baumgartner, Maxim Golovkin on May 14, 2015. 3:00 am

PUBLICATIONS

APT | CYBER ESPIONAGE | SOCIAL ENGINEERING | TARGETED ATTACKS | VULNERABILITIES AN

Our recent report, "The Chronicles of the Hellsing APT: the Empir to the Naikon APT, describing it as "One of the most active APTs Sea". Naikon was mentioned because of its role in what turned ou payback. It was a Naikon attack on a Hellsing-related organizatio Considering the volume of Naikon activity observed and its relent confrontation was worth looking into, so we did.

Tweet

The #NaikonAPT group wa an actor we now call "Hells

The Naikon APT aligns with the actor our colleagues at FireEye r haven't discovered any exact matches. It is hardly surprising that both actors have for years mined victims in the South China Sea intelligence.

WHAT'S NEXT IN MALWARE AFTER KULUOZ?

POSTED BY: Ryan Olson on August 10, 2015 4:00 AM

FILED IN: Malware, Unit 42
TAGGED: Asprox, AutoFocus, CryptoWall, Dyre, kuluoz, Threat Landscape Review, Trojan, Upatre, WildFire

Regular readers of this blog have heard all about the infamous Kuluoz malware. This family was the latest evolution of the Asprox malware and at its peak in 2014 it accounted for 80% of all malware sessions we observed in WildFire. When the team published our Threat Landscape Review in December of last year, we highlighted this family as a scourge that impacted nearly every company Palo Alto Networks protected in 2014. Kuluoz was primarily distributed through e-mail, which means we saw large numbers of SMTP sessions, but also downloads over a variety of webmail clients.

Even if you didn't read our blogs, you probably dealt with Kuluoz. Throughout 2014, most of the waves of spam e-mails carrying fake court notices, voicemail messages and package delivery alerts carried a Kuluoz attachment. If you opened these attachments you quickly became part of the botnet, sending copies of the malware to other victims while the botmaster silently installed additional malicious software on your system.

Given all of this activity, we were quite surprised when the malware all but disappeared at the end of December 2014.

Contact Us:
(877) 347-3393

Worldwide

tions | Mandiant Consulting | Current Threats

Threat Research

0097 Exploited in the Wild

eep Singh, Kenneth Hsu | Exploits, Threat Research

In March 2015, Microsoft patched a remote code execution (RCE) vulnerability (CVE-2015-0097) in Microsoft Office. In July 2015, Eduardo Prado released a Proof of Concept (PoC) exploit for this vulnerability here. It did not take long for attackers to repackage this PoC and use it in attacks in the wild. We observed a few variants of attacks exploiting CVE-2015-0097 that are using the same PoC to create a .doc exploit. This vulnerability could also be exploited using other Office file formats.

he vulnerability, it does not require common exploitation techniques like a ain to gain code execution on a machine. In this blog, we describe how this exploited in the wild and the details of the malicious binaries it drops post

etails

RCE vulnerability that Mitre describes as a "Microsoft Word Local Zone Remote erability" [1]. Unlike memory corruption vulnerabilities, this vulnerability results crosoft Office applications. Office can open documents as HTML files via the tControl.1 control. If the document contains valid HTML (in this case, appended ument), the HTML is launched in the Local Security Zone. Scripts embedded ent then write to disk with the ADODB.Recordset Active X Control. By writing tartup directory as shown in Figure 1, the attacker's scripts achieve full RCE and

Automate All the Things


WHAT'S NEXT IN MALWARE AFTER KULUOZ?

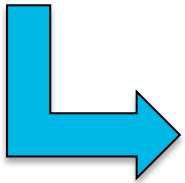
POSTED BY: Ryan Olson on August 10, 2015 4:00 AM

FILED IN: Malware, Unit 42
TAGGED: Asprox, AutoFocus, CryptoWall, Dyre, kuluoz, Threat Landscape Review, Trojan, Upatre, WildFire

Regular readers of this blog have heard all about the infamous Kuluoz malware. This family was the latest evolution of the Asprox malware and at its peak in 2014 it accounted for 80% of all malware sessions we observed in WildFire. When the team published our Threat Landscape Review in December of last year, we highlighted this family as a scourge that impacted nearly every company Palo Alto Networks protected in 2014. Kuluoz was primarily distributed through e-mail, which means we saw large numbers of SMTP sessions, but also downloads over a variety of webmail clients.

Even if you didn't read our blogs, you probably dealt with Kuluoz. Throughout 2014, most of the waves of spam e-mails carrying fake court notices, voicemail messages and package delivery alerts carried a Kuluoz attachment. If you opened these attachments you quickly became part of the botnet, sending copies of the malware to other victims while the botmaster silently installed additional malicious software on your system.

Given all of this activity, we were quite surprised when the malware all but disappeared at the end of December 2014.



Changed on 06/29/15 at 07:41:17 by script_utils

comment:1

Reply Edit

Generated by Scrypture at 2015-06-29T07:41:17.002408
WARNING! This is an automated triage tool. IOCs may be extracted incorrectly or not at all.
See a bug? Please create an Issue on GitHub.

Auto-Extracted Indicators

domain

```
e[redacted]o.com
m[redacted]rg
h[redacted]nfo
```

url

```
hu[redacted]]info/common[.]php
eh[redacted]p[.]com/common[.]php
m:[redacted]]org/common[.]php
```

md5

```
021[redacted]1F71
9F0[redacted]CD60
C03[redacted]CBFE
C04[redacted]ED65
577[redacted]D785
D3E[redacted]B696
12E[redacted]E6E9
880[redacted]476D
4AA[redacted]9A7F
F5C[redacted]F97E
FAE[redacted]C510
675[redacted]A6DD
A14[redacted]28B0
D5E[redacted]BF5A
D3E[redacted]7CB1
67D[redacted]2C67
```

IOC Triage (IOCSaw, WAM, Trac)

INDICATOR	#	LAST	FIRST	BLKD	COMMENT	CATEGORY	CREATED	UPDATED	RELEASE	TRAC
bad.site.cc				1	Ticket#27565, OSINT. (India Breach)	Targeted	2013-03-14T 01:37:15	2013-03-14T 01:37:15	3/14/13	#54728
palace.malware.net				1	More dynamic dns blocks	Dynamic DNS	2013-09-03T 20:19:09	2013-09-03T 20:19:09	9/3/13	#78508 ,#53939
totally.legit.net				1	INT: [DIB] Weekly Round Up IOCs 02/10	Targeted	2013-08-29T 14:30:06	2013-08-29T 14:30:06	8/29/13	#41152
test-user123.crime.com				1	Ticket#27565, OSINT. (India Breach)	Targeted	2013-03-14T 01:37:15	2013-03-14T 01:37:15	3/14/13	#54728
securelist.com	223	07/14/2015:21:46:03	07/16/2014:22:53:45							32 matched tickets

Hash Triage (NSRL* lookup and Trac)

HASH	NSRL_FNAME	NSRL_MFG	NSRL_PROD	TRAC
7D7D7D7D7D7D7D7D7D7D7D7D7D22				
E9A87BB87BB87BB6DC053238B0A87B				#83349, #83030, #83021, #82915
EDCD313791506EDCD318A2A88B9EDC				
72EDCD31A7AAD3102C5AA7758EEDCD				#84507
AAA62D5F0E348F0E8AAAAAADDDDDDE				
4DFDF00000000000474B8F431B6E07				
21C46A95329F3F1688888888800000				
0B3D7D7D7D7D7D8887BB1D32FFFFFF				
2020202020289393939D7D7D7D7D				
5A22E5AEE4DA2FE363B77F1A22E5AE				#83532
5A22E5AEE4DAA22E5AEE4DAA22E5AE				
F8A22E5AEE4DA488BA22E5AEE4DA44				#82887

*National Software Reference Library

Macros are Awesome

Hashes - give us all your hashes

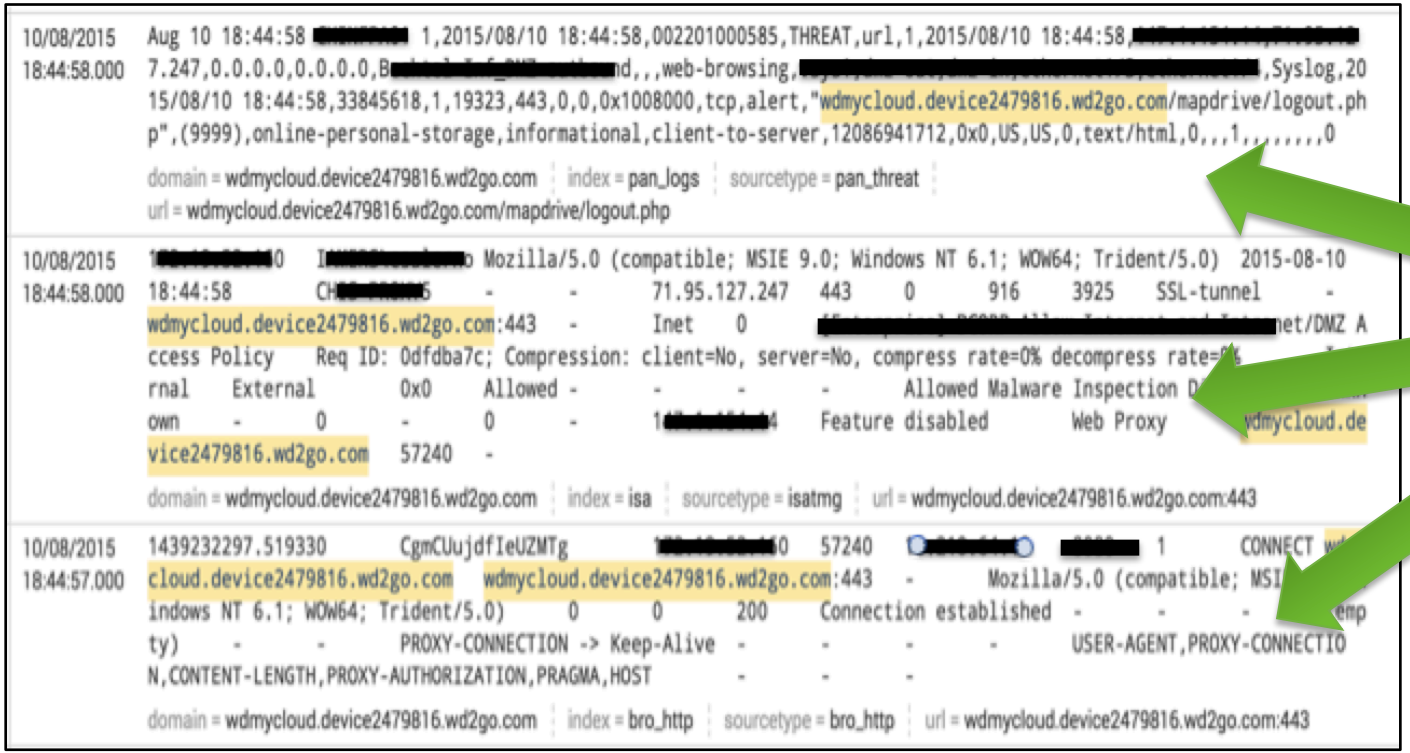
- `hash_indices` Macro:

(index=wls* OR index=bro_http OR index=bro_notice OR index=bro_smtp_entities OR index=fe OR index=fireeye OR index=bro_files OR sourcetype="sep12:risk" OR sourcetype=sep12:proactive OR sourcetype=sep12:behavior) AND file_hash!="-"

earliest=-24h `hash_indexes` file_hash="B9A4DAC2192FD78CDA097BFA79F6E7B2" OR file_hash="E7B2ED6FF40DAB2F235000B0299E7B2" OR file_hash="E7B2B87136E2DC22F8D2740F3E6EE7B2"

Aug 27 06:50:06 [redacted] Security: LogType="WLS", BaseFileName="net.exe", Cached="True", Channel="Security", CompanyName="Microsoft Corporation", Computer="[redacted]", CreatorProcessName="cmd", EventID="4688", EventRecordID="5610374", ExecutionProcessID="4", ExecutionThreadID="104", FileDescription="Net Command", FileVersion="6.1.7600.16385 (win7_rtm.090713-1255)", InternalName="net.exe", Keywords="0x8020000000000000", Language="English (United States)", Length="46080", Level="0", MD5="B9A4DAC2192FD78CDA097BFA79F6E7B2", NewProcessId="0x5c8", NewProcessName="C:\Windows\System32\net.exe", Opcode="0", ProcessId="0x1530", ProductVersion="6.1.7600.16385", ProviderGuid="{54849625-5478-4994-A5BA-3E3B0328C30D}", ProviderName="Microsoft-Windows-Security-Auditing", SHA1="9A544E2094273741AA2D3E7EA0AF303AF2B587EA", Signed="Catalog", SSDeep="768:ybyAXHGTQ8xm8ZiOXCFIIHHyXIf4/TBNrt6pDHmIkRx6HFxLpcn5mlq:eyAXivhJyLHSXuyTBN2Hc6zpc5mY", SubjectDomainName="[redacted]", SubjectLogonId="0xaec58", SubjectUserName="r[redacted]", SubjectUserSid="S-1-5-21-1960408961-1844823847-1417001333-1014054", Task="13312", TokenElevationType="TokenElevationTypeLimited (3)", ValidSignatureDate="False", Version="1", Zone="0"

Another Useful Macro



- Palo Alto
- ISA Proxy
- BRO

Splice

Splice of life is IOCs

- We have lots of indicators of compromise…
- We had MIR…
- We have Splice Now

- https://splunkbase.splunk.com/app/2637/
- This functionality is now available in Splunk Enterprise Security 3.3

Recap of 5 Takeaways

‘Member these things

- **Saved Searches** are you friend
  - **25.33%** Percent of our tickets
- **Macros** are your friend
- **CIM** is your friend
- Avoid false negatives: always check for log activity!
- Remember to check Splunk, the **answers** could already be there
- Troll **answers.splunk.com**, **splunk blog,** and **splunk base**

@rj_chap **@ltawfall**

Questions?

THANK YOU

splunk>