The Anatomy of a Threat Hunting Hypothesis

Introduction

- Director, Global Cyber Defense @ Marsh McLennan
- Done a lot of blue team work and led a lot of blue team work
- SecKC, BSidesKC CFP Board, #FUZZYSNUGGLYDUCK
- MS in Cybersecurity Policy @ Georgia Tech
- Trying to escape computers by running long distances in the woods

What’s on the agenda?

01

Introduction

*You are here

02

Hypothesis Diagramming

03

Impact Multipliers

04

Resources

A human-driven process to identify artifacts associated with a **previously undetected** intrusion or breach that was not identified by existing security controls.

–Joe Slowik

02

Hypothesis Diagramming

Welcome back to elementary school!

Building Better Hypotheses

- You deserve better hypotheses that work for you, not that you have to work for
- Bad inputs means bad outputs
- Too little freedom, bad time
- Too much freedom, bad time
- Find the four constant elements of a strong hypothesis:
    - Target
    - Technique
    - Payload/Action on Objective
    - Attacker Type (optional)

What Makes a Target?

- The system, application, person, or victim of malicious behavior
- Sets the tone of severity:
  - CEO’s inbox vs CISO’s inbox
  - Windows 7 host vs Windows 2016 server
  - Production finance application vs development web application
- Shortcut the scope of logs you should be searching

What Makes Technique?

- The malicious behavior you want to find
- Traditionally the hypothesis origin element
- MITRE ATT&CK provides cheat codes
    - T1570 - Lateral Tool Transfer
    - Moving malicious files between compromised hosts via SMB

MITRE | ATT&CK®

What Makes a Payload?

- AKA Action on Objective

- The big **WHY**

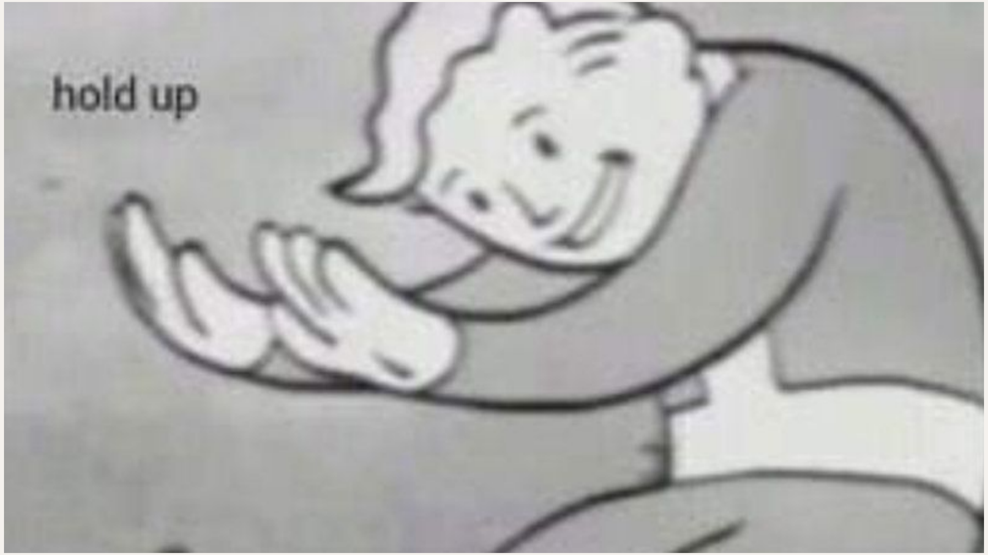
- Your management only cares about this because it means impact
  - Make them care

- Malware > Credential Theft
- Exfiltration > Data Extortion
- DDoS > Lost Business

- Highlight what success looks like

What About Attacker Type?

- Check your program maturity first
- Focus on techniques and scale
- Threat actors can garner rapid support from leadership
  - But it can also result in false findings and goose chases



Good Hypothesis

PowerShell is being leveraged on endpoints to execute malware in memory

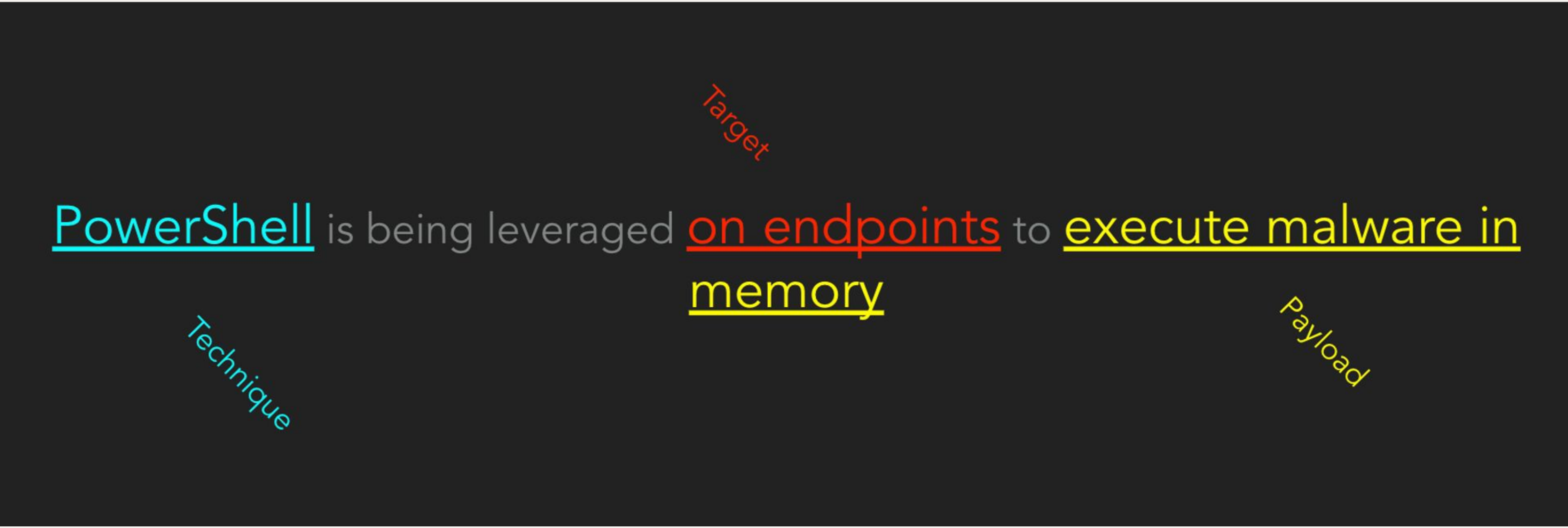
Better Hypothesis

Attackers are compiling exploits locally on servers/clients to use, and using basic naming schema, like “exploit.exe.”

Best Hypothesis

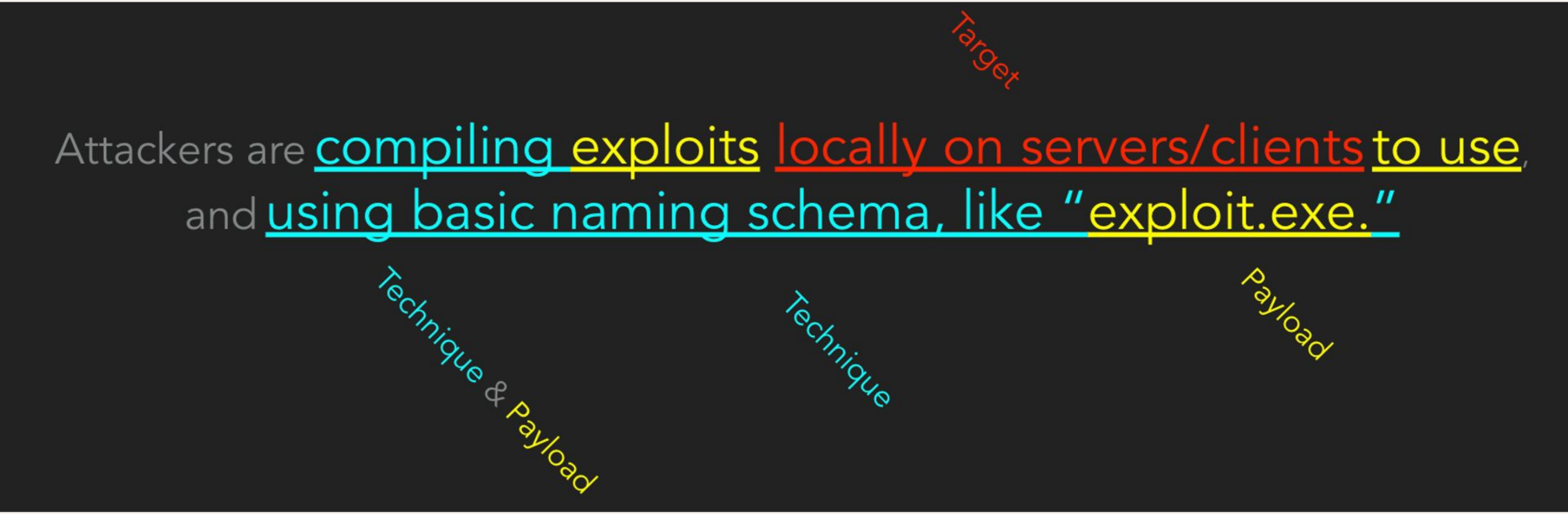
WSL (the Windows Subsystem for Linux) is being used for malicious scripting purposes and cross compatibility malware execution by malicious insiders.

Diagram It - Good Hypothesis



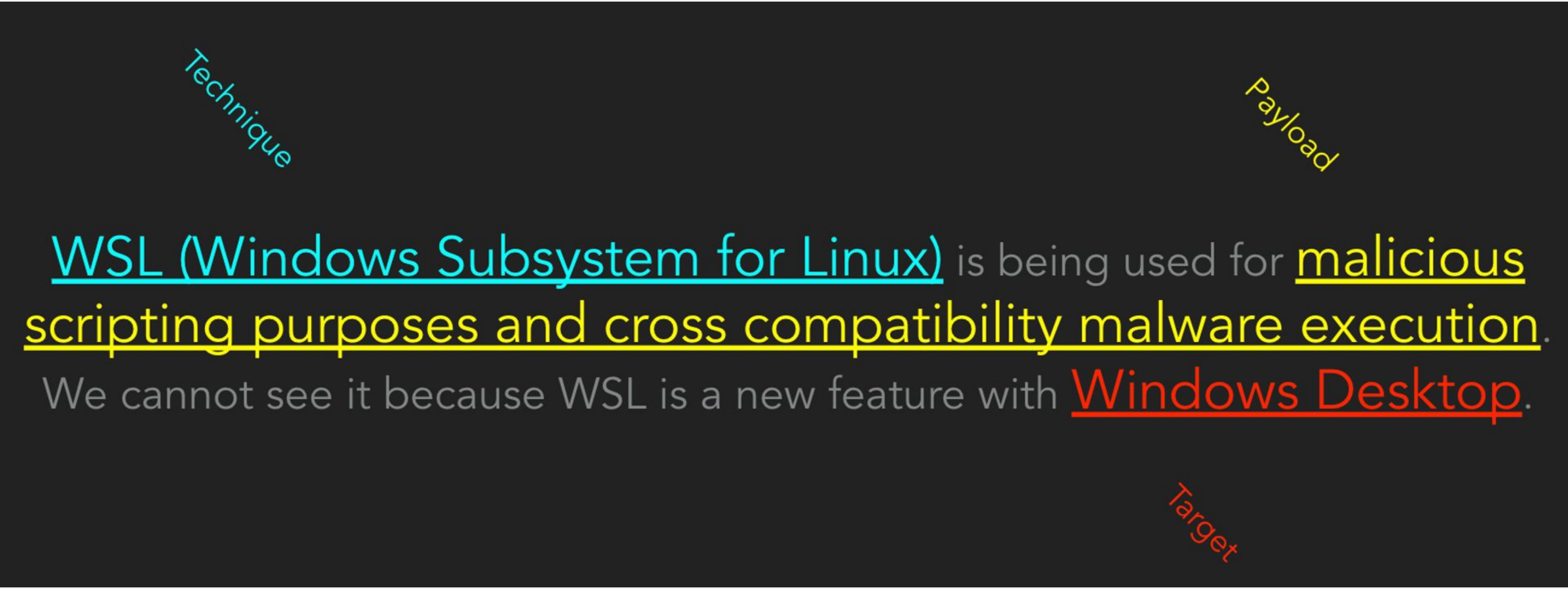
PowerShell is being leveraged on endpoints to execute malware in memory

Diagram It - Better Hypothesis



Attackers are compiling exploits locally on servers/clients to use, and using basic naming schema, like "exploit.exe."

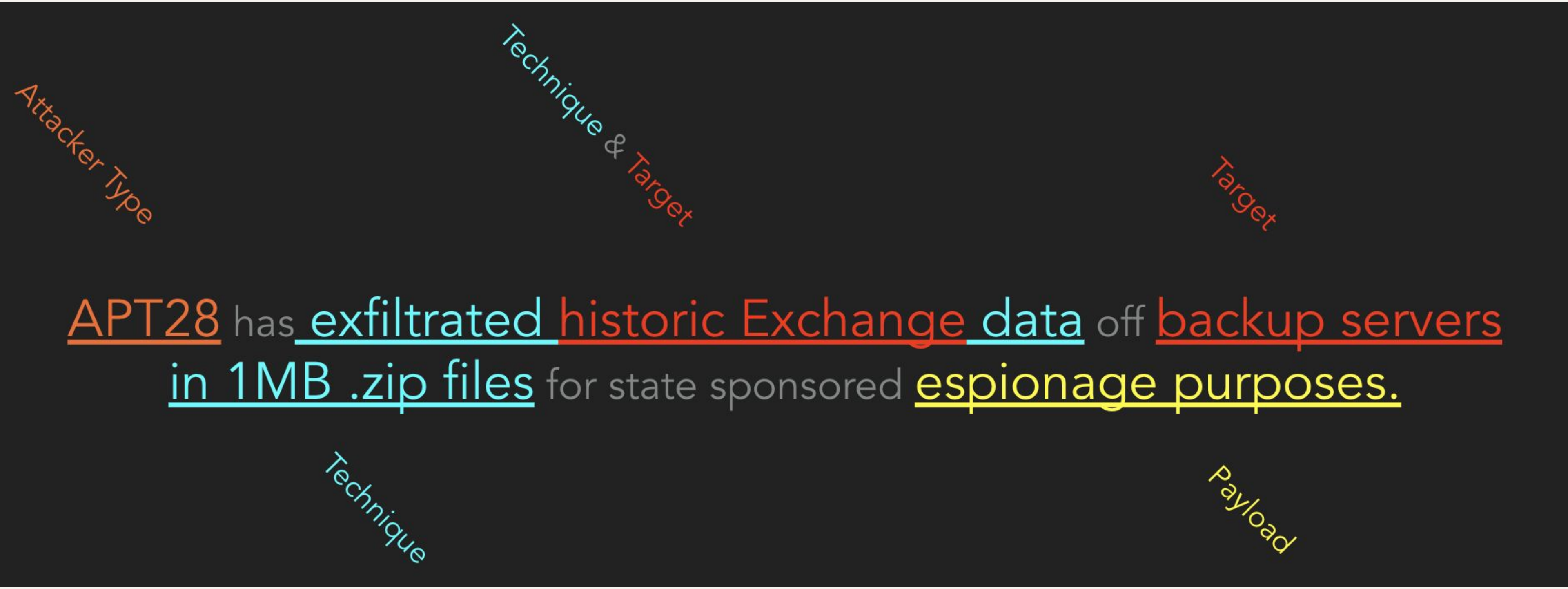
Diagram It - Best Hypothesis



WSL (Windows Subsystem for Linux) is being used for malicious scripting purposes and cross compatibility malware execution. We cannot see it because WSL is a new feature with Windows Desktop.

Technique
Payload
Target

Diagram It - Best^2 Hypothesis



APT28 has exfiltrated historic Exchange data off backup servers in 1MB .zip files for state sponsored espionage purposes.

03

Impact Multipliers

Make It Matter

Industry

The type of business you do, the customers your serve, the suppliers you rely on

Geolocation

Global, national, regional

Technology Stack

What make your business go

Crown Jewels

Very important people, assets, applications, or processes

Trends

What you are seeing from a detection and response perspective

You’re Not Alone

- Consider the threats facing your industry
  - Learn from other people’s incidents
- Consider your key partnerships
- Consider your key clients
- Supply chain is real and should inform your hunts

Where's Waldo?

- Physical location matters as much as workforce distribution
- An organization solely operating in Illinois doesn't need to look at threats only impacting Ukrainian organizations
  - Be aware, but don't overcommit

What’s Inside?

- Hunt against things you have
- If you have GSuite, don’t focus on Exchange exploit outputs
- Partner with the business to highlight key strategy items
    - Moving to cloud? Would be a shame if someone found how bad everything really way and provided ample evidence

King of the Castle

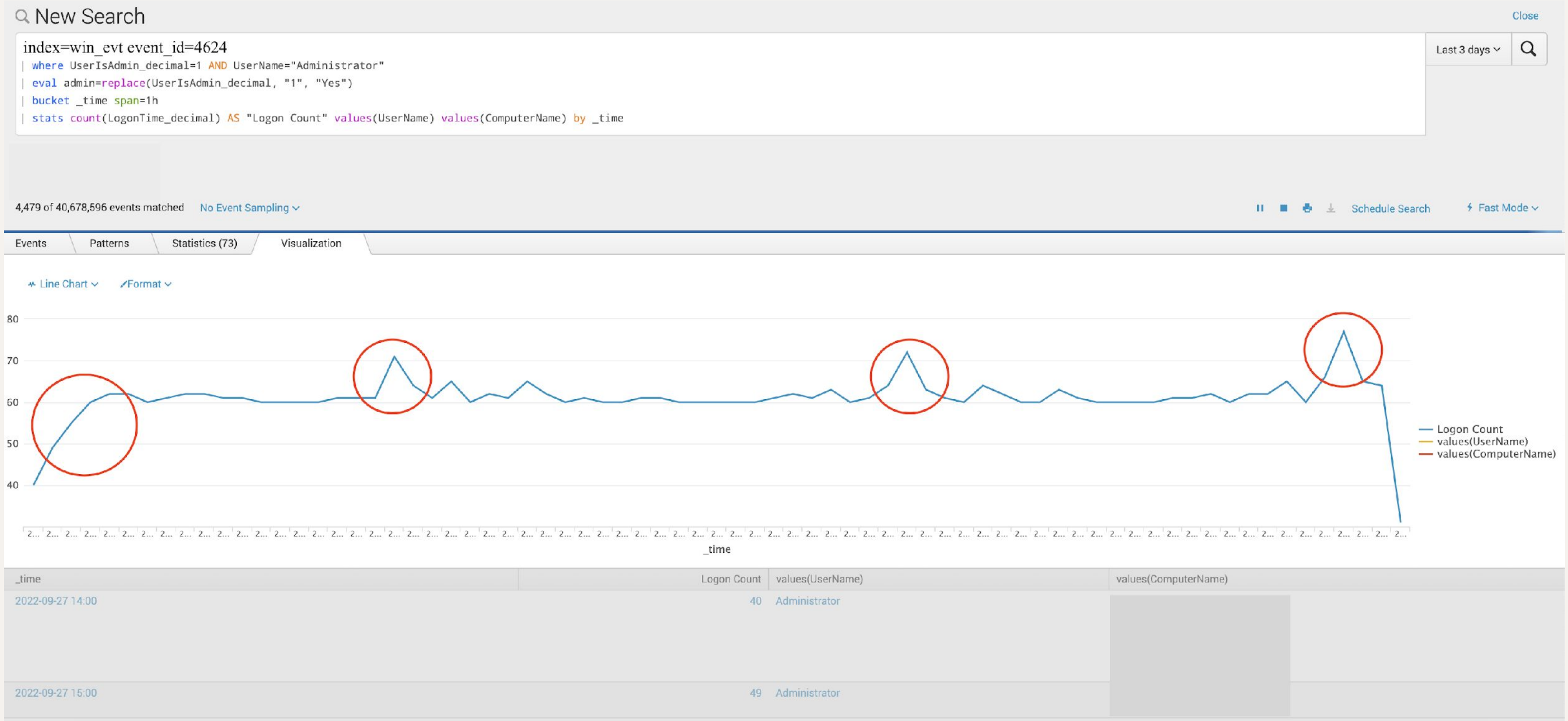
- Known your high risk, high value items
  - People
  - Assets
  - Applications
  - Data
  - Processes

- Nothing gets you more resources like saying you identified a targeted attack against the CFO

Page Six, Get This

- Where there is smoke, there is fire
- Talk to your reactive teams more
- Improve the posture of the firm one hunt at a time
  - Also maybe help your fellow SOC and IR folks get some sleep and generate some good karma

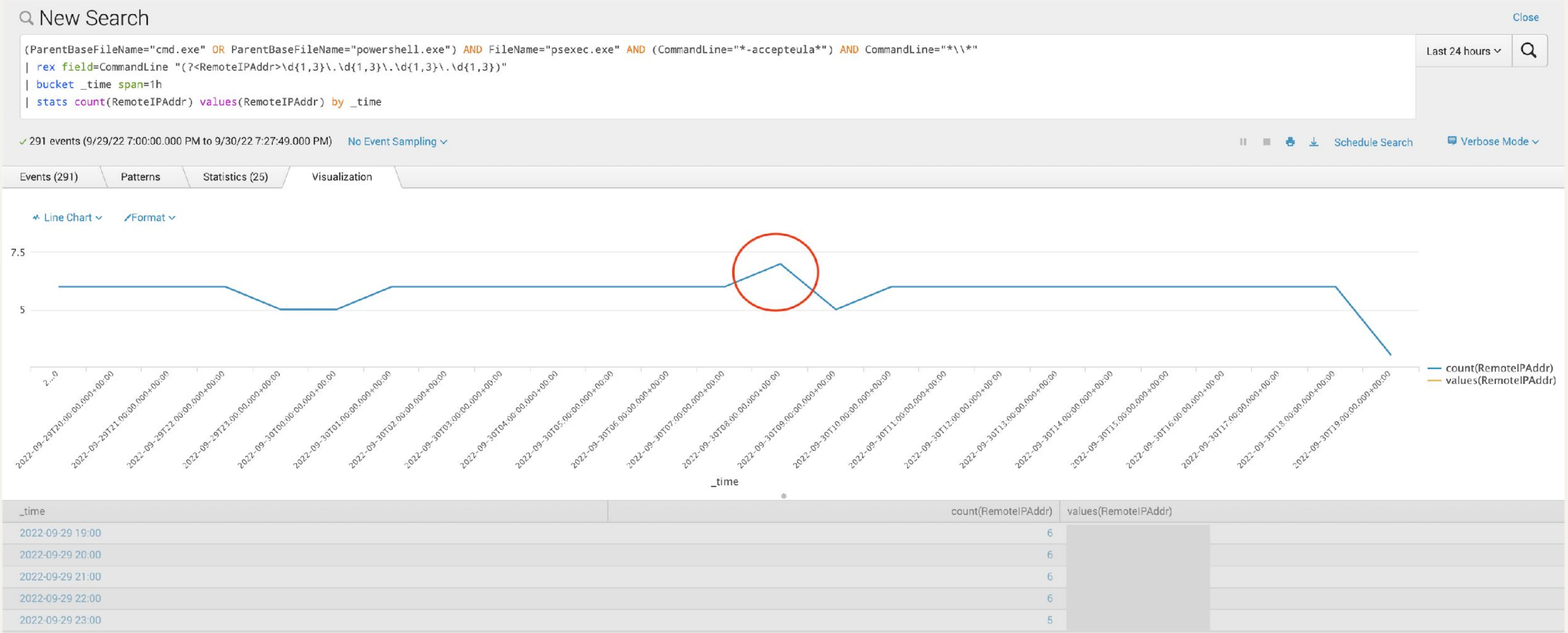
Someone created a local admin account on an endpoint



```
index=win_evt event_id=4624
| where UserIsAdmin_decimal=1 AND UserName="Administrator"
| eval admin=replace(UserIsAdmin_decimal, "1", "Yes")
| bucket _time span=1h
| stats count(LogonTime_decimal) AS "Logon Count" values(UserName) values(ComputerName) by _time
```

_time	Logon Count	values(UserName)	values(ComputerName)
2022-09-27 14:00	40	Administrator	[redacted]
2022-09-27 15:00	49	Administrator	[redacted]

Psexec.exe is being used for lateral movement post compromise



New Search

```
(ParentBaseFileName="cmd.exe" OR ParentBaseFileName="powershell.exe") AND FileName="psexec.exe" AND (CommandLine="*-accepteula*") AND CommandLine="*\\*"
| rex field=CommandLine "(?<RemoteIPAddr>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| bucket _time span=1h
| stats count(RemoteIPAddr) values(RemoteIPAddr) by _time
```

Last 24 hours

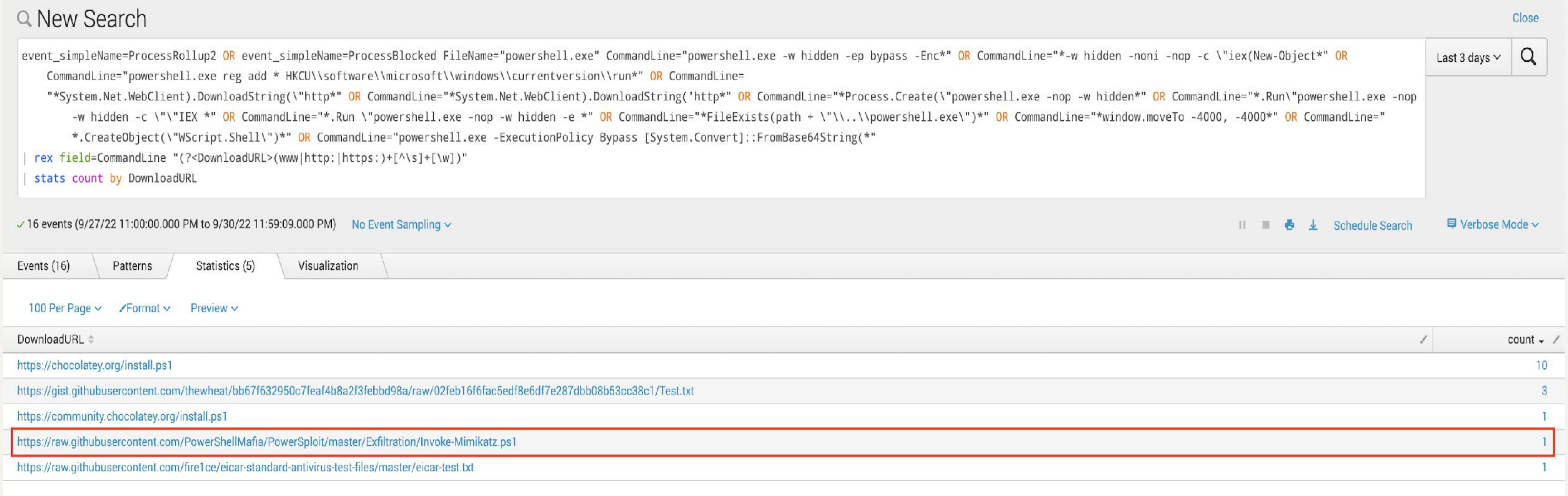
✓ 291 events (9/29/22 7:00:00.000 PM to 9/30/22 7:27:49.000 PM)   No Event Sampling

No Event Sampling ⌄   Verbose Mode ⌄

Close
Schedule Search
Events (291)
Patterns
Statistics (25)
Visualization
Line Chart
Format
7.5
5
2...0
2022-09-29T20:00:00.000+00:00
2022-09-29T21:00:00.000+00:00
2022-09-29T22:00:00.000+00:00
2022-09-29T23:00:00.000+00:00
2022-09-30T00:00:00.000+00:00
2022-09-30T01:00:00.000+00:00
2022-09-30T02:00:00.000+00:00
2022-09-30T03:00:00.000+00:00
2022-09-30T04:00:00.000+00:00
2022-09-30T05:00:00.000+00:00
2022-09-30T06:00:00.000+00:00
2022-09-30T07:00:00.000+00:00
2022-09-30T08:00:00.000+00:00
2022-09-30T09:00:00.000+00:00
2022-09-30T10:00:00.000+00:00
2022-09-30T11:00:00.000+00:00
2022-09-30T12:00:00.000+00:00
2022-09-30T13:00:00.000+00:00
2022-09-30T14:00:00.000+00:00
2022-09-30T15:00:00.000+00:00
2022-09-30T16:00:00.000+00:00
2022-09-30T17:00:00.000+00:00
2022-09-30T18:00:00.000+00:00
2022-09-30T19:00:00.000+00:00
_time
count(RemoteIPAddr)
values(RemoteIPAddr)

_time	count(RemoteIPAddr)	values(RemoteIPAddr)
2022-09-29 19:00	6	[redacted]
2022-09-29 20:00	6	[redacted]
2022-09-29 21:00	6	[redacted]
2022-09-29 22:00	6	[redacted]
2022-09-29 23:00	5	[redacted]

Powershell is being used for second stage downloads



```
event_simpleName=ProcessRollup2 OR event_simpleName=ProcessBlocked FileName="powershell.exe" CommandLine="powershell.exe -w hidden -ep bypass -Enc*" OR CommandLine="*-w hidden -noni -nop -c \"iex(New-Object*" OR
    CommandLine="powershell.exe reg add * HKCU\\software\\microsoft\\windows\\currentversion\\run*" OR CommandLine=
    "*System.Net.WebClient).DownloadString(\"http*" OR CommandLine="*System.Net.WebClient).DownloadString('http*" OR CommandLine="*Process.Create(\"powershell.exe -nop -w hidden*" OR CommandLine="*.Run\"powershell.exe -nop
        -w hidden -c \"\"IEX *" OR CommandLine="*.Run \"powershell.exe -nop -w hidden -e *" OR CommandLine="*FileExists(path + \"\\..\\powershell.exe\")*" OR CommandLine="*window.moveTo -4000, -4000*" OR CommandLine="
        *.CreateObject(\"WScript.Shell\")*" OR CommandLine="powershell.exe -ExecutionPolicy Bypass [System.Convert]::FromBase64String(*"
| rex field=CommandLine "(?<DownloadURL>(www|http:|https:)+[^\s]+[\w])"
| stats count by DownloadURL
```

✓ 16 events (9/27/22 11:00:00.000 PM to 9/30/22 11:59:09.000 PM)

DownloadURL	count
https://chocolatey.org/install.ps1	10
https://gist.githubusercontent.com/thewheat/bb67f632950c7feaf4b8a2f3febbd98a/raw/02feb16f6fac5edf8e6df7e287dbb08b53cc38c1/Test.txt	3
https://community.chocolatey.org/install.ps1	1
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1	1
https://raw.githubusercontent.com/fire1ce/eicar-standard-antivirus-test-files/master/eicar-test.txt	1

03

Resources

Other Hunt Ideas

- **Exfiltration:** Employees have committed sensitive information, including API keys, to public code repositories or forums and put internal data at risk
- **Defense Evasion:** Attackers have disabled Windows Defender, Windows Firewall, and cleared Windows Events to avoid detection
- **Privilege Escalation:** Employees are practicing hacking activities and/or researching hacking methods on enterprise networks
- **Impact:** Managed hosts have been infected with ransomware and have not alerted through existing security detections due to new decryption notification files in use.
- **Initial Access:** Attackers are using simple, text-only emails to avoid setting off detection signatures and social engineer finance or HR employees
- **Lateral Movement:** Attackers are attempting to compromise third-party vendors in order to gain a foothold in your enterprise network
- **Execution:** OS X endpoints may be targeted for attacks due to their high-level users and differing security controls. Attacks that no longer easily work on Windows could work on Macs.

Other Hunt Content

MITRE
ATT&CK™

The ThreatHunting Project

ThreatHunting
Open Threat Research

Questions?

https://github.com/triw0lf/anatomy-of-a-threat-hunt

https://laurenproehl.com

https://twitter.com/jotunvillur