



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

The MITRE ATT&CK logo is displayed within a solid red rectangular box. The word "MITRE" is in a bold, white, sans-serif font. To its right is a vertical white line, followed by the text "ATT&CK" in the same bold, white, sans-serif font. A registered trademark symbol (®) is located at the top right of the "K".

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

Technique

Target

Payload

Diagram It - Better Hypothesis

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

Target

Technique & Payload

Technique

Payload

Diagram It - Best Hypothesis

Technique

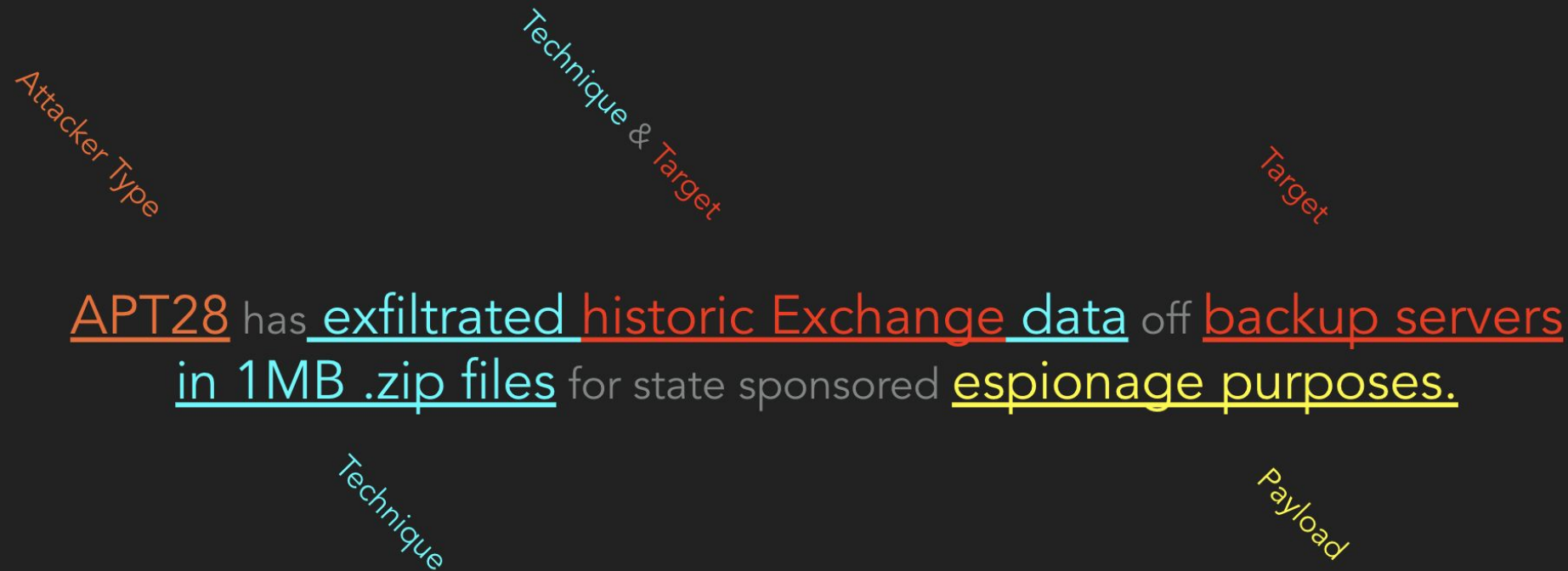
Payload

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.

Target

Diagram It - Best² Hypothesis

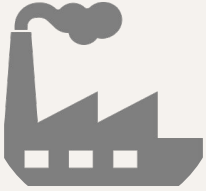




03

Impact Multipliers

Make It Matter



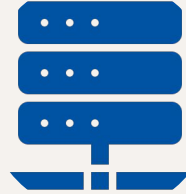
Industry

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



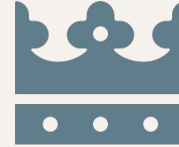
Geolocation

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 was 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



Psexec.exe is being used for lateral movement post compromise

Q New Search

Close

```
(ParentBaseFileName="cmd.exe" OR ParentBaseFileName="powershell.exe") AND FileName="psexec.exe" AND (CommandLine="*-accepteula*") AND CommandLine="*\\*"
| rex field=CommandLine "{7<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

|| ■ 📄 ⬇️ Schedule Search

🗨️ Verbose Mode

Events (291) Patterns Statistics (25) Visualization

Line Chart Format



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

Powershell is being used for second stage downloads

Q New Search

Close

```
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
```

Last 3 days ▾



✓ 16 events (9/27/22 11:00:00.000 PM to 9/30/22 11:59:09.000 PM) No Event Sampling ▾

⏏ ⌵ ⚙ ⬇ Schedule Search

🗨 Verbose Mode ▾

Events (16)

Patterns

Statistics (5)

Visualization

100 Per Page ▾ /Format ▾ Preview ▾

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 Content



The
ThreatHunting
Project



ThreatHunting
Open Threat Research



Questions?



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



<https://laurenproehl.com>



<https://twitter.com/jotunvillur>