MITRE TryHackMe Write-up

Posted on January 11, 2021 by Jon Jepma

This is a Write up for the MITRE Room Created by heavenraiza

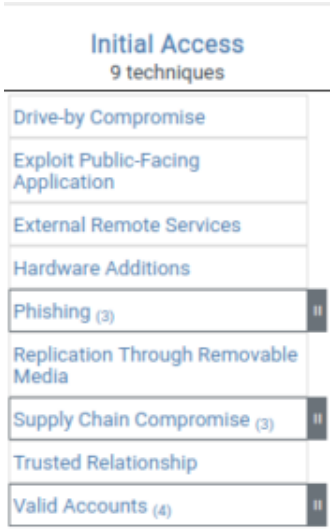
TASK 1 & 2 are simple click and complete tasks

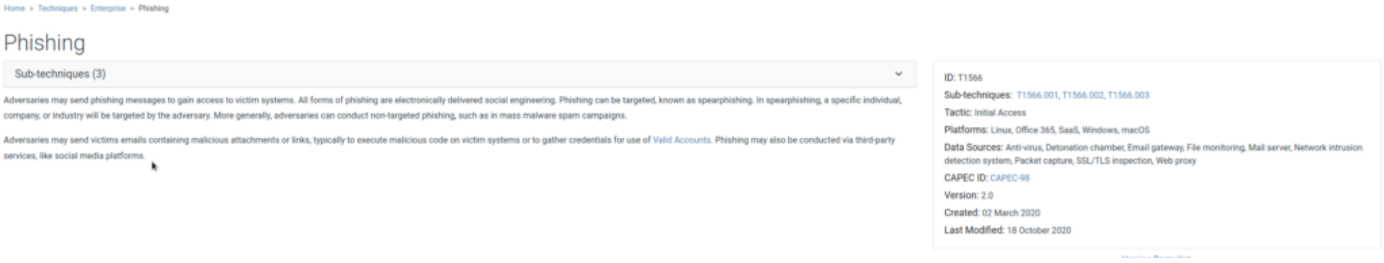
TASK 3

Question 1: Only blue teamers will use the ATT&CK Matrix? (Yay/Nay)

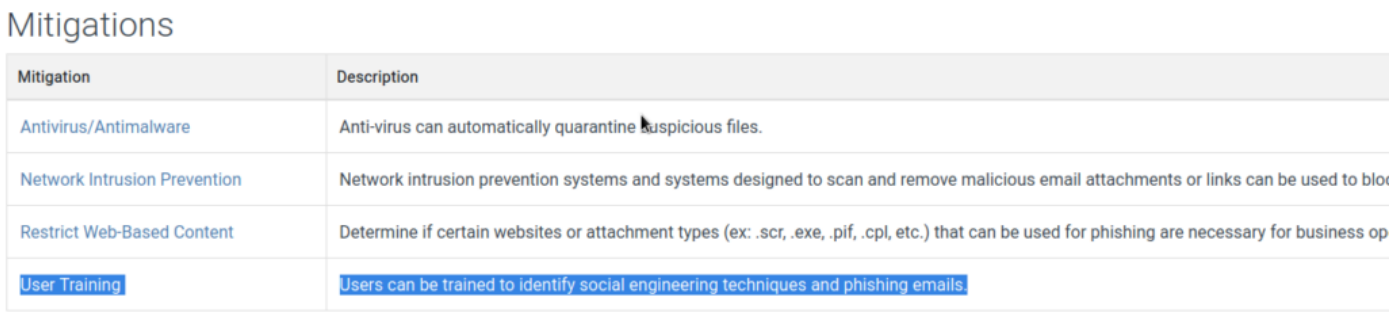
Question 2: we need to head over to https://attack.mitre.org/

*Keep in mind it mentions to start your research on the Phishing page





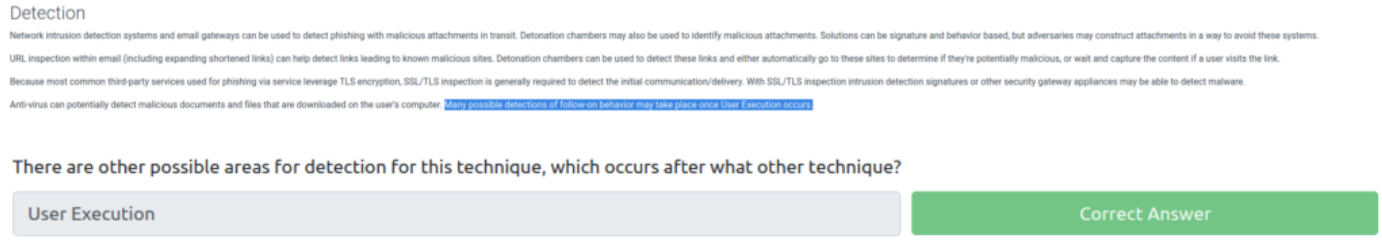
Question 3: is found under the Mitigations section on the Phishing page



Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to bloc
Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business op
User Training	Users can be trained to identify social engineering techniques and phishing emails.

Question 4: can be found under the Detection section of this same page



Detection

Network intrusion detection systems and email gateways can be used to detect phishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

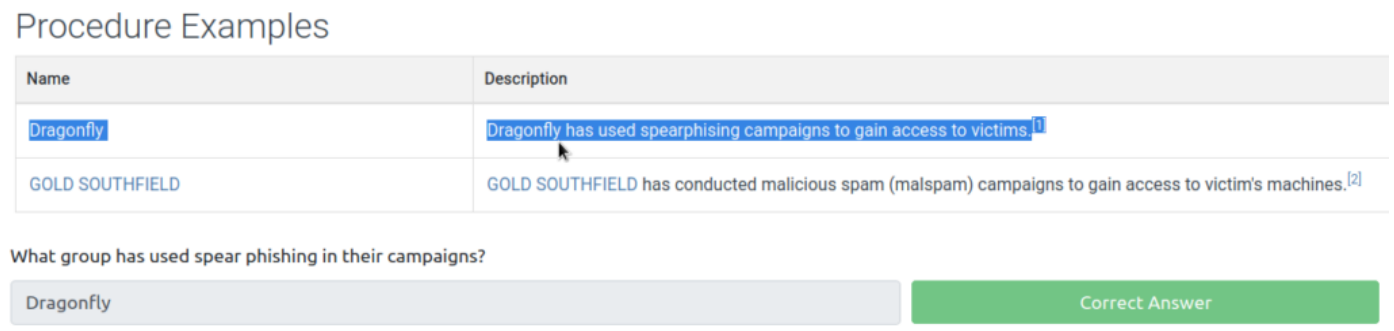
Because most common third-party services used for phishing via service leverage TLS encryption, SSL/TLS inspection is generally required to detect the initial communication/delivery. With SSL/TLS inspection intrusion detection signatures or other security gateway appliances may be able to detect malware.

Anti-virus can potentially detect malicious documents and files that are downloaded on the user's computer. Many possible detections of follow-on behavior may take place once User Execution occurs

There are other possible areas for detection for this technique, which occurs after what other technique?

User Execution — Correct Answer

Question 5: Is located on the same page near the top



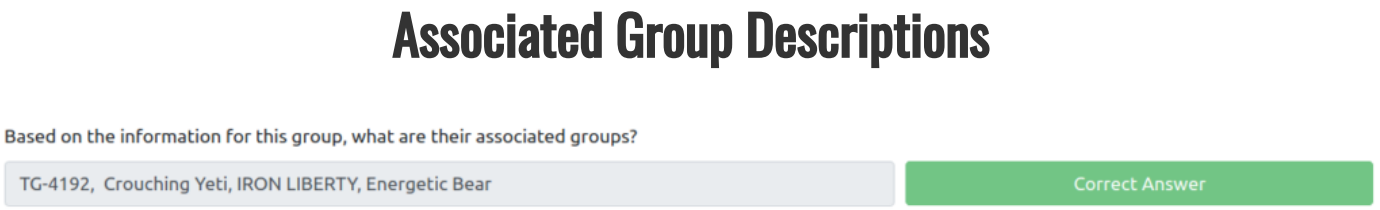
Procedure Examples

Name	Description
Dragonfly	Dragonfly has used spearphising campaigns to gain access to victims.[1]
GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines.[2]

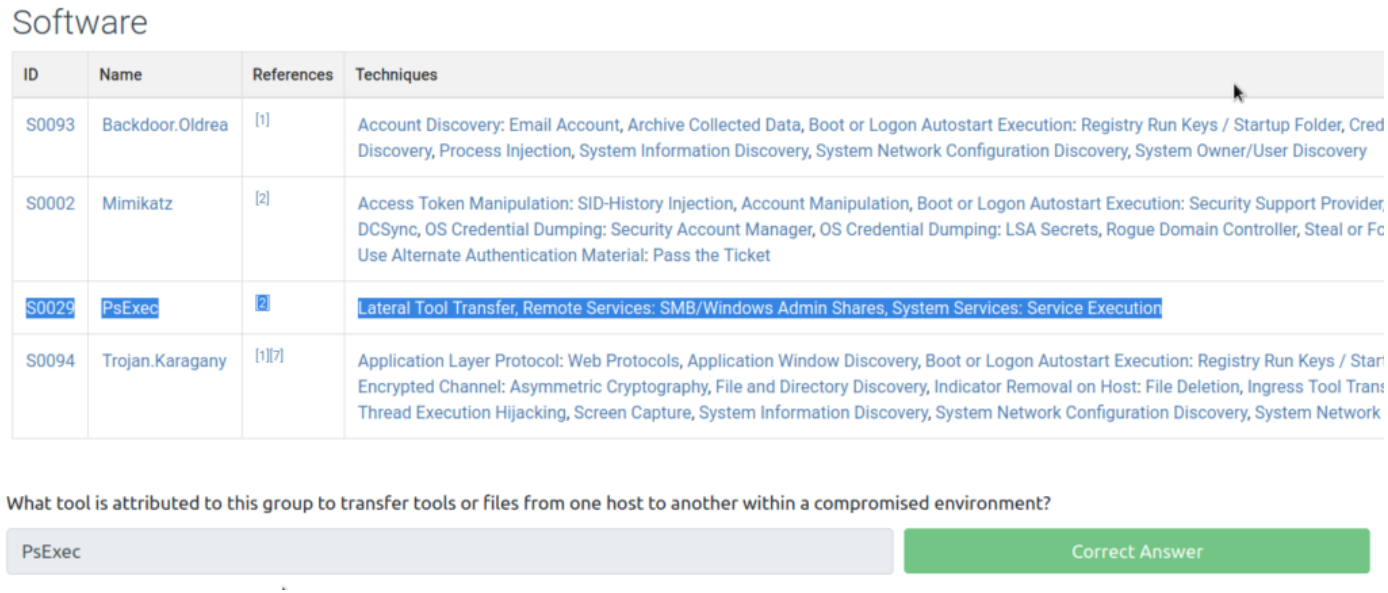
What group has used spear phishing in their campaigns?

Dragonfly — Correct Answer

Question 6: click on the Groups link to learn more about them and the information is located under



Question 7: is located under the Software Section



Question 8: is found when we click the hyperlink for PsExec we are led to a page about the tool and who has been known to use it and this will help us answer this question.

Based on the information about this tool, what group used a customized version of it?

FIN5 | Correct Answer

Question 9: Click on the FIN5 Group hyperlink to be taken to their page to find the next answers

FIN5

FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. [1] [2] [3]

This group has been active since what year?

2008 | Correct Answer

Question 10: This located under the software section where we learn that the Windows Credential Editor is used by FIN5

Software

ID	Name	References	Techniques
S0173	FLIPSIDE	[2]	Protocol Tunneling
S0029	PsExec	FIN5 uses a customized version of PsExec.[2]	Lateral Tool Transfer, Remote Services: SMB/Win
S0006	pwdump	[2]	OS Credential Dumping: Security Account Manag
S0169	RawPOS	[3][2]	Archive Collected Data: Archive via Custom Meth
S0195	SDelete	[2]	Data Destruction, Indicator Removal on Host: File
S0005	Windows Credential Editor	[3][2]	OS Credential Dumping: LSASS Memory

Instead of Mimikatz, what OS Credential Dumping tool is does this group use?

Windows Credential Editor — Correct Answer

And here is our TASK 3 Recap

Only blue teamers will use the ATT&CK Matrix? (Yay/Nay)

Nay — Correct Answer

What is the ID for this technique?

T1566 — Correct Answer — Hint

Based on this technique, what mitigation covers identifying social engineering techniques?

User Training — Correct Answer

There are other possible areas for detection for this technique, which occurs after what other technique?

User Execution — Correct Answer

What group has used spear phishing in their campaigns?

Dragonfly — Correct Answer

Based on the information for this group, what are their associated groups?

TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear — Correct Answer

What tool is attributed to this group to transfer tools or files from one host to another within a compromised environment?

PsExec — Correct Answer

Based on the information about this tool, what group used a customized version of it?

FIN5 — Correct Answer

This group has been active since what year?

2008 — Correct Answer

Instead of Mimikatz, what OS Credential Dumping tool is does this group use?

Windows Credential Editor — Correct Answer

Task 4

Question 1: Splunk search is pseudo

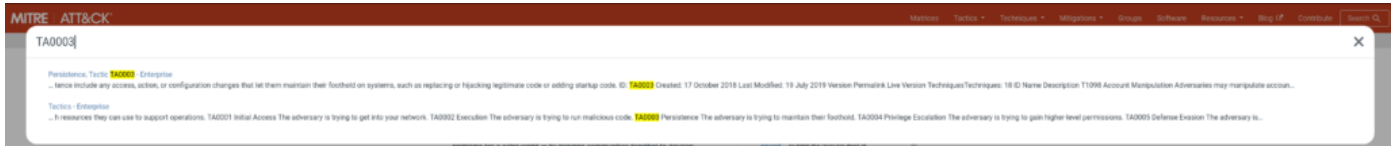
We're also provided with Pseudocode and a query on how to search for this specific analytic within Splunk. A pseudocode is a plain, human-readable way to describe a set of instructions or algorithms that a program or system will perform.

Splunk search - Windows task file creation (Splunk, Sysmon native)

This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\
*" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

Question 2: Head to https://attack.mitre.org/ and click on the search icon on the top right and enter TA0003, if we click on the first link we are then taken to What type of Tactic this is.



What tactic has an ID of TA0003?

Persistence | Correct Answer | Hint

Question 3: Head to https://car.mitre.org/ and I searched for Zeek

Analytic Source Code Libraries

Some analytics are built as source code for specific products. In these cases, code might support a broad set of detections in a way that makes it hard to describe a set of distinct analytics. For these types of analytics, rather than integrating them into the main CAR site, we've collected them under a library of implementations. Currently, the only library is BZAR, a collection of Zeek (Bro) scripts looking primarily at SMB and RPC traffic.

Question 4: Head to https://car.mitre.org/analytics/ and I searched for hash (only 3 results)

CAR-2013-05-009: Running executables with same hash and different names	• Masquerading	Dnif, Sigma, Splunk	Windows, Linux, macOS

What is the name of the technique for running executables with the same hash and different names?

Masquerading | Correct Answer | Hint

Question 5: There is a section for Test Cases located on the same page

Unit Tests

Test Case 1

Configurations: Windows 7

- From an admin account, open Windows command prompt (right click, run as administrator).
- Execute "at 10:00 calc.exe," substituting a time in the near future for 10:00.
- The program should respond with "Added a new job with job ID = 1" where the job ID is dependent on what tasks are scheduled.
- The program should execute at the time specified. This is what the analytic should fire on.
- To remove the scheduled task, execute "at 1 /delete" where you replace "1" with the job ID output in step 2a above.

```
at 10:00 calc.exe // returns a job number X
at X /delete
```

TASK 4 Recap

Examine CAR-2013-05-004, what additional information is provided to analysts to ensure coverage for this technique?

Unit Tests | Correct Answer | Hint

For the above analytic, what is the pseudocode a representation of?

Splunk Search — Correct Answer

What tactic has an ID of TA0003?

Persistence — Correct Answer — Hint

What is the name of the library that is a collection of Zeek (BRO) scripts?

BZAR — Correct Answer — Hint

What is the name of the technique for running executables with the same hash and different names?

Masquerading — Correct Answer — Hint

Examine CAR-2013-05-004, what additional information is provided to analysts to ensure coverage for this technique?

Unit Tests — Correct Answer — Hint

TASK 5

Question 1 & 2: we need to go tohttps://shield.mitre.org/ > Matrix > this lists all the techniques and we see that Detect has the most.

Which Shield tactic has the most techniques?

Detect — Correct Answer

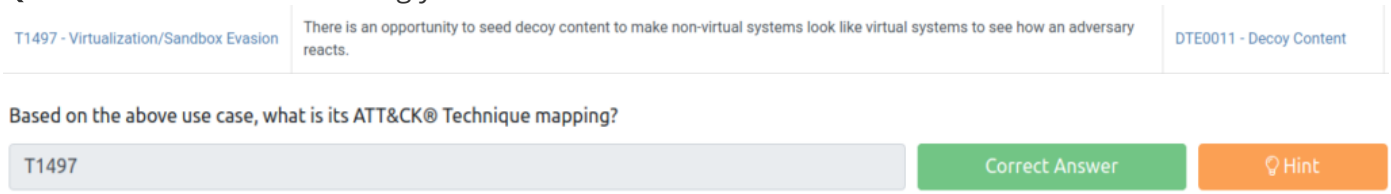
Is the technique 'Decoy Credentials' listed under the tactic from question #1? (Yay/Nay)

yay — Correct Answer

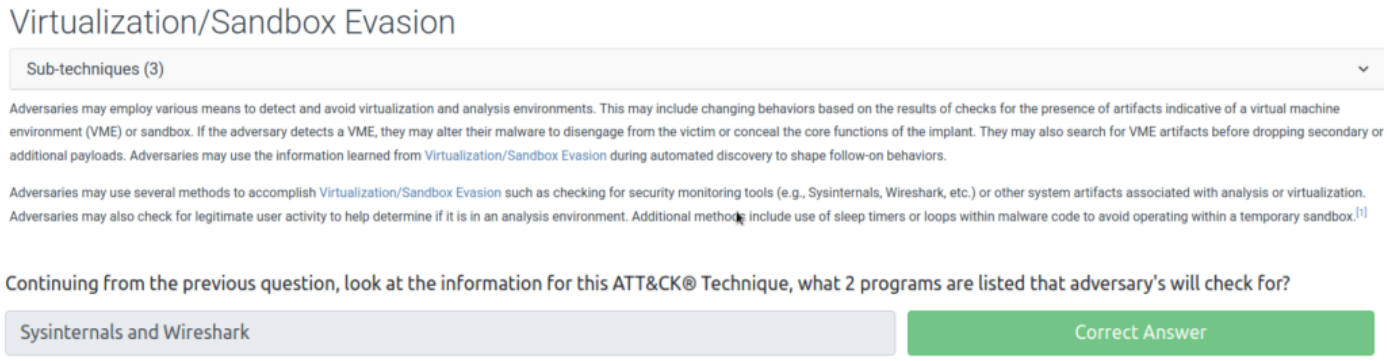
Question 3: all we need to do is a quick search from the search bar shows that DTE0011 is Decoy Content >

DUC0234	A defender can plant files, registry entries, software, processes, etc. to make a system look like a VM when it is not.

Question 4: involves continuing your search from the DTE0011



Question 5: https://shield.mitre.org/attack_mapping/mapping_all > get here by using the navigation bar and clicking Att&ck Mapping > Overview > then a few lines down there is a hyperlink for the complete mapping.



Task 5 Recap

Which Shield tactic has the most techniques?

Detect — Correct Answer

Is the technique 'Decoy Credentials' listed under the tactic from question #1? (Yay/Nay)

yay — Correct Answer

Explore DTE0011, what is the ID for the use case where a defender can plant artifacts on a system to make it look like a virtual machine to the adversary?

DUC0234 — Correct Answer

Based on the above use case, what is its ATT&CK® Technique mapping?

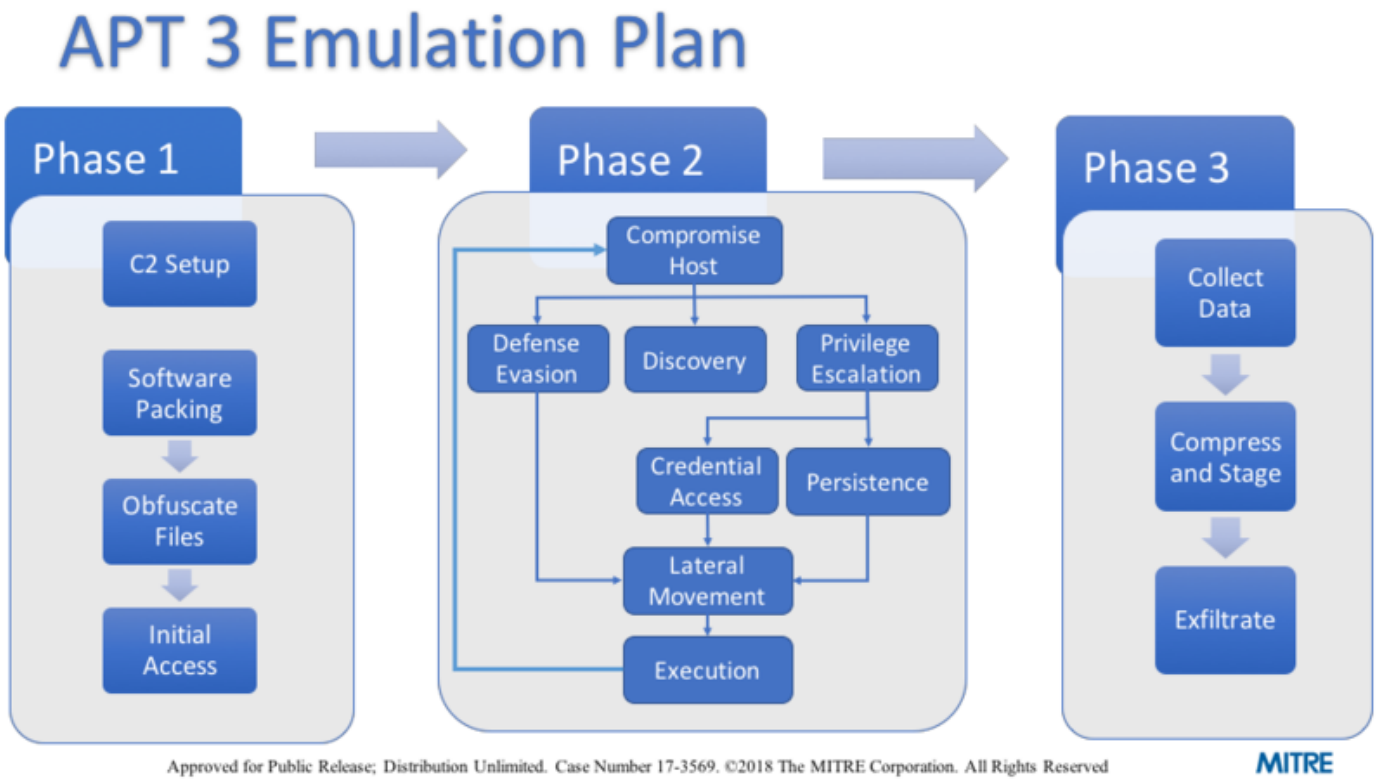
T1497 — Correct Answer — Hint

Continuing from the previous question, look at the information for this ATT&CK® Technique, what 2 programs are listed that adversary's will check for?

Sysinternals and Wireshark — Correct Answer

TASK 6

Question 1: Click the APT3 hyperlink they provided in the room to find this answer



Question 2: This can be located viahttps://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf > Phase 2 > Persistence | utilize the table of contents to find this easily!

3.2.1.3 Persistence

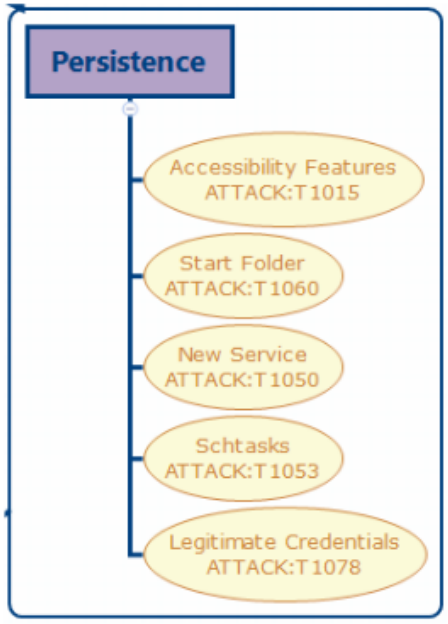


Figure 5 APT3 Persistence ATT&CK Techniques

APT3 has used multiple methods for persistence: creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and also by placing scripts in the Startup Folder [7] [T1060 - Registry Run Keys/Start Folder].

APT3 has replaced the Sticky Keys binary (`C:\Windows\System32\sethc.exe`) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 – Remote Desktop Protocol]. This specific Persistence technique has an added benefit of allowing an operator to open a command prompt when connected over RDP without having to provide valid credentials [23].

APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 – Create Account]. Presumably this is done for easier future access.

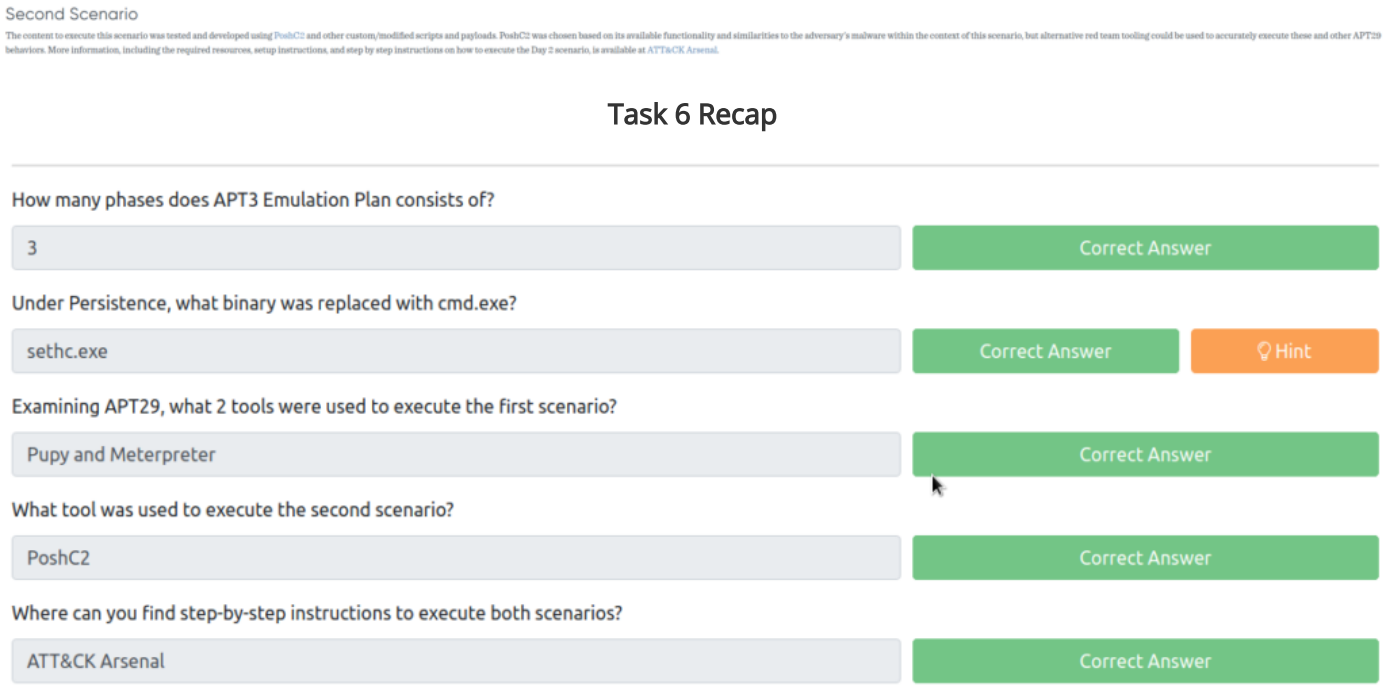
Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.

Question 3: This can be found by reading the First Scenario section via https://attackevals.mitre-engenuity.org/APT29/operational-flow


First Scenario

The content to execute this scenario was tested and developed using Pupy, Meterpreter, and other custom/modified scripts and payloads. Pupy and Meterpreter were chosen based on their available functionality and similarities to the adversary's malware within the context of this scenario, but alternative red team tooling could be used to accurately execute these and other APT29 behaviors. More information, including the required resources, setup instructions, and step by step instructions on how to execute the Day 1 scenario, is available at ATT&CK Arsenal.

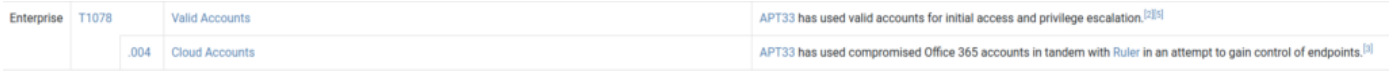
Question 4: This can be found by reading the Second Scenario section via https://attackevals.mitre-engenuity.org/APT29/operational-flow



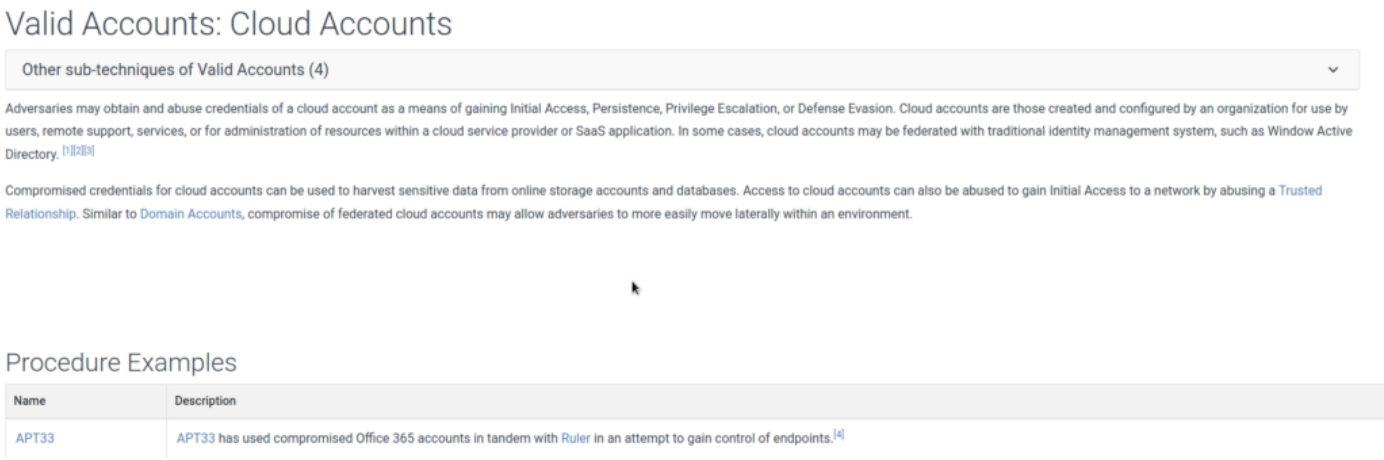
TASK7

Question 1 & 2: We need to head back to MITRE and use the navigation bar to search groups (or here is a link https://attack.mitre.org/groups/) a search on the page for Aviation reveals that APT33 is the group who may target us in this scenario

Question 3: Go to the APT33 Group page https://attack.mitre.org/groups/G0064/ > scroll to software



Question 4: If we Take a look at what Techniques they use under T1078.004 we find the information below to help us find this answer



Valid Accounts: Cloud Accounts

Other sub-techniques of Valid Accounts (4)

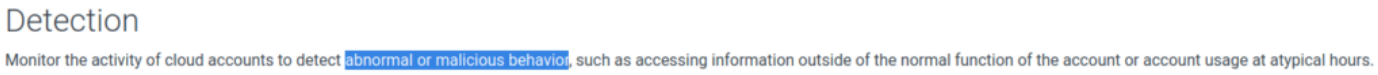
Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management system, such as Window Active Directory. [1][2][3]

Compromised credentials for cloud accounts can be used to harvest sensitive data from online storage accounts and databases. Access to cloud accounts can also be abused to gain Initial Access to a network by abusing a Trusted Relationship. Similar to Domain Accounts, compromise of federated cloud accounts may allow adversaries to more easily move laterally within an environment.

Procedure Examples

Name	Description
APT33	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints.[4]

Question 5: Further on this page we have a Detection writeup that we can use.



Detection

Monitor the activity of cloud accounts to detect abnormal or malicious behavior, such as accessing information outside of the normal function of the account or account usage at atypical hours.

Question 6: On the top right of the page we will find the ID information to finish up this room!

ID: T1078.004

Sub-technique of: T1078

Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Platforms: AWS, Azure, Azure AD, GCP, Office 365, SaaS

Permissions Required: Administrator, User

Data Sources: AWS CloudTrail logs, Authentication logs, Azure activity logs, Stackdriver logs

Version: 1.1

Created: 13 March 2020

Last Modified: 19 October 2020

Task 7 Recap

What is a group that targets your sector who has been in operation since at least 2013?

APT33 — Correct Answer

Does this group use Stuxnet? (Yay/Nay)

Nay — Correct Answer

As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?

Cloud Accounts — Correct Answer

What tool is associated with this technique?

Ruler — Correct Answer

Per the detection tip, what should you be detecting?

abnormal or malicious behavior — Correct Answer

What platforms does this affect?

AWS, Azure, Azure AD, GCP, Office 365, SaaS — Correct Answer

Thanks for stopping by and I hope this is able to help you complete any tasks/questions that were proving difficult to find!

Posted in CTF Write-ups

← CISSP Domain 1 Study notes and Resources

Leave a Reply

Your email address will not be published. Required fields are marked *

Start typing...

You may use these HTML tags and attributes:

<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike>

Name *

Email *

Website

Post Comment

Search ...

Recent Posts

MITRE TryHackMe Write-up

CISSP Domain 1 Study notes and Resources

Archives

January 2021

Categories

Cissp

CTF Write-ups