MITRE ENGENUITY | Center for Threat Informed Defense

Lab 4.1: Planning TTP Implementations

Introduction

Over the next four labs, you are going to implement a selection of TTPs attributed to a sophisticated threat actor, APT29.

You will begin this process by researching an APT29 CTI article. From this article, you will identify and understand several APT29 TTPs observed during a phishing campaign.

Once you understand the CTI article contents, you will plan how you will emulate APT29 TTPs. In the next lab, you will put this plan to use by implementing APT29 TTPs.

Objectives

1. Utilize ATT&CK to understand APT29 targets and TTPs.
2. Describe APT29 TTPs from a 2018 phishing campaign reported by Mandiant.
3. List APT29 initial access payload components and behaviors.

Estimated Completion Time

a) 30 minutes to 1 hour

Requirements

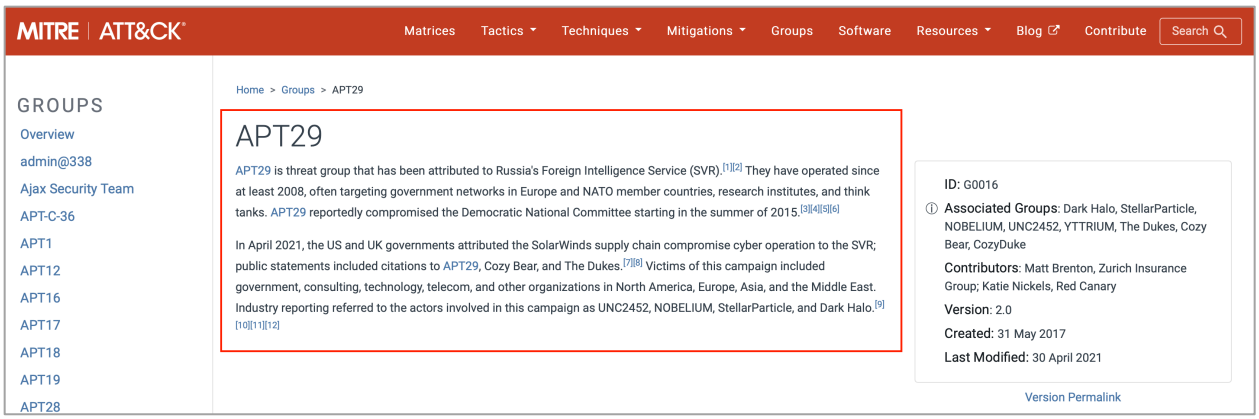
1. Internet access
2. Web browser

Walkthrough

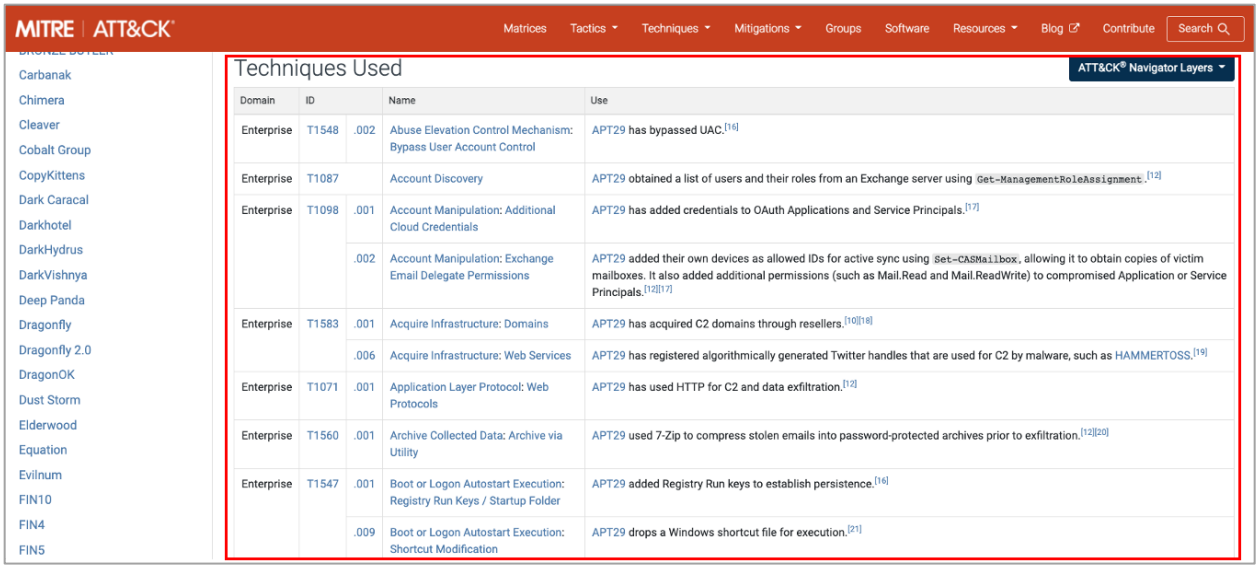
Step 1: Understanding APT29 Targets and TTPs

You'll begin by using ATT&CK and the ATT&CK Navigator to gain a general understanding of APT29 targets and TTPs.

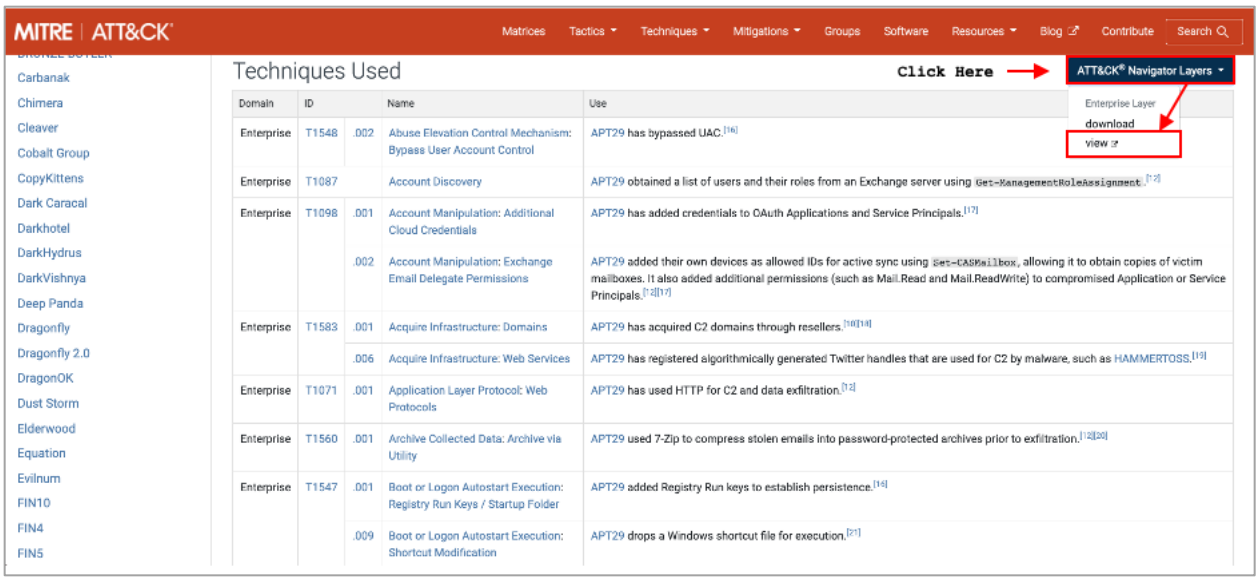
1. Read the APT29 actor summary on ATT&CK: https://attack.mitre.org/groups/G0016/. Identify organizations APT29 has targeted previously.

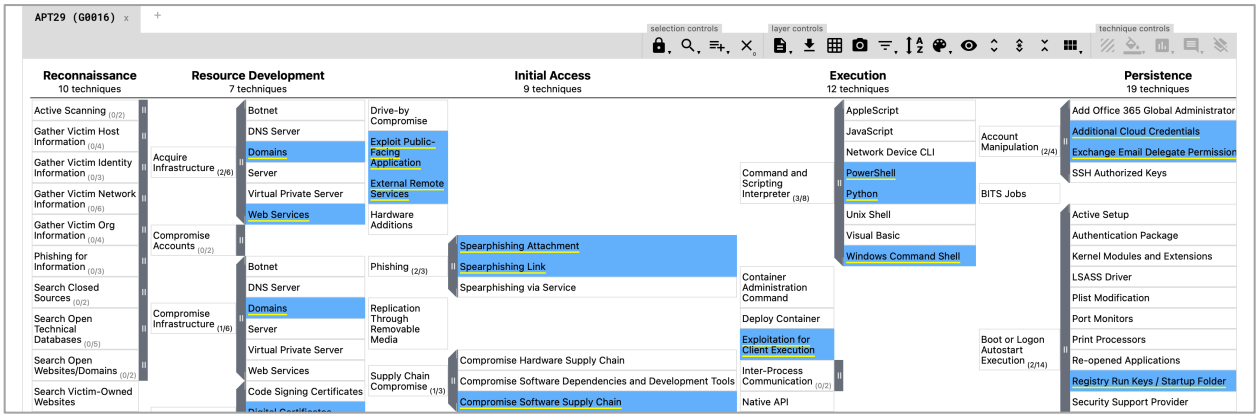


2. Skim through APT29's TTPs; study APT29 Initial Access and Execution TTPs in particular. Examine how APT29 has executed phishing TTPs.



3. Use the ATT&CK Navigator to more easily see APT29's use of Initial Access and Execution TTPs.





Learning Check

1. *Choose all that apply: according to ATT&CK, which entities has APT29 targeted previously?*
   a. government networks in Europe and NATO member countries
   b. research institutes
   c. financial services organizations
   d. think tanks

2. *Which of the following describes APT29's use of [Phishing: Spearphishing Link]?*

   a) APT29 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
   b) APT29 has sent spearphishing emails containing links to .hta files.

c) APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files.
d) APT29 has used the legitimate mailing service Constant Contact to send phishing e-mails.

Step 2: Understanding APT29 TTP Implementations

You've decided you would like to implement APT29 TTPs from a 2018 spearphishing campaign reported by Mandiant. You will utilize Mandiant's CTI report and ATT&CK to understand how APT29 implemented the TTPs used in this campaign.

1. Read the following CTI report by Mandiant. Understand how APT29 sent phishing payloads to targets, and how the payloads were constructed.

https://www.mandiant.com/resources/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign

Learning Check

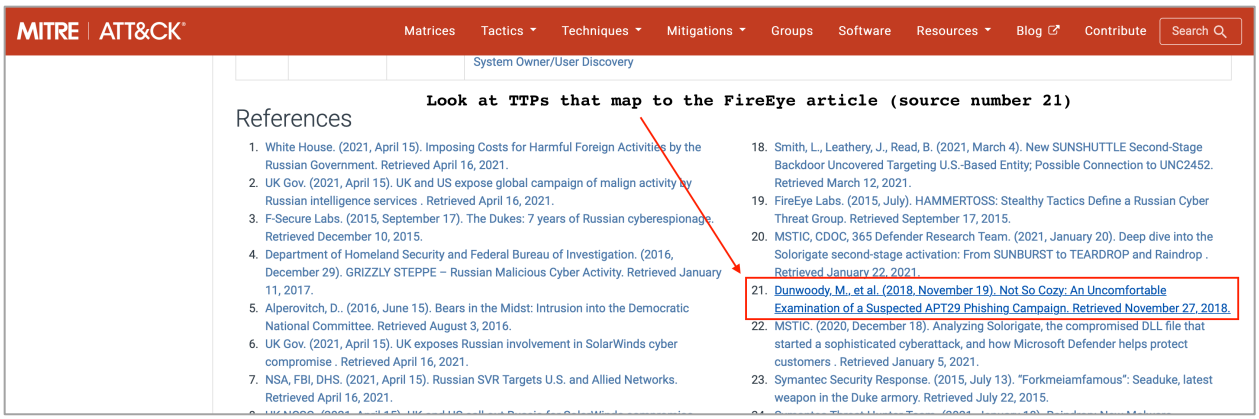
1. *The Mandiant report describes how APT29 sent phishing emails with hyperlinks to a zip file. What type of payload was contained in the zip files??*
   a) Windows Executable
   b) Windows DLL
   c) PowerShell Stager
   d) Windows Shortcut File

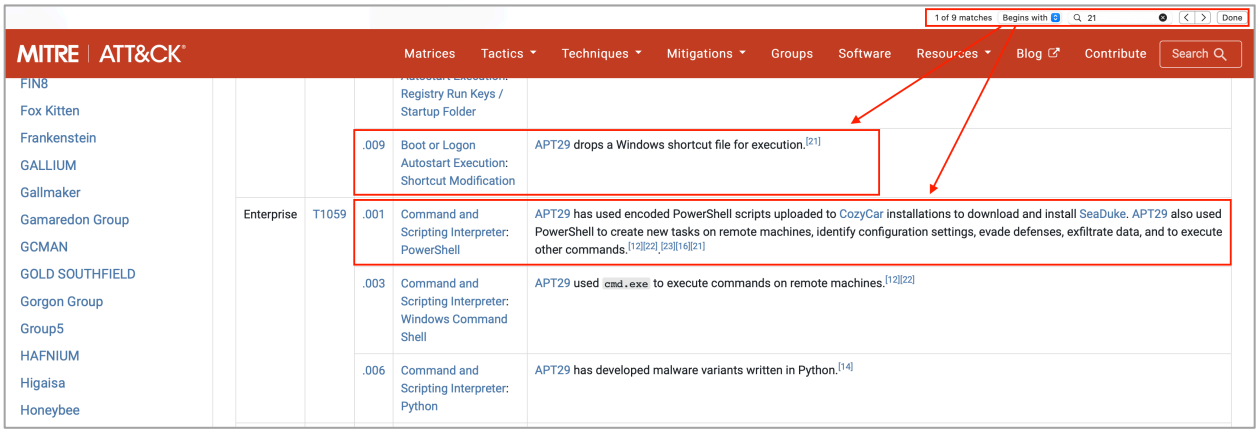
2. *The Mandiant report describes an APT29 initial access payload, ds7002.lnk. Select all of the payload components contained in ds7002.lnk:*
   a) PowerShell Loader
   b) PowerShell Empire Stager
   c) Embedded Cobalt Strike Beacon DLL
   d) Decoy Executable
   e) Decoy PDF
   f) Visual Basic Discovery Script

Step 3: List APT29 TTPs

Now that you have a general understanding of APT29 TTPs, you will plan out your implementation. We'll start by listing all of the specific TTPs we will implement.

1. Use ATT&CK to identify all of the TTPs described in the Mandiant article. We will implement these TTPs in the next lab.





The following table contains all of the TTPs from the Mandiant article.

Technique ID	Sub-technique ID	Name	Use
T1547	.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution.[21]
T1059	.001	Command and Scripting Interpreter: PowerShell	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell to create new tasks on remote machines, identify configuration settings, evade defenses, exfiltrate data, and to execute other commands.[12][22][23][16][21]
T1095	N/A	Non-Application Layer Protocol	APT29 has used TCP for C2 communications.[21]

T1027	N/A	Obfuscated Files or Information	APT29 has used encoded PowerShell commands.[21]
T1218	.011	Signed Binary Proxy Execution: Rundll32	APT29 has used Rundll32.exe to execute payloads.[17][20][21]
T1204	.001	User Execution: Malicious Link	APT29 has used various forms of spearphishing attempting to get a user to click on a malicious link.[21][14]
T1204	.002	User Execution: Malicious File	APT29 has used various forms of spearphishing attempting to get a user to open attachments, including, but not limited to, malicious Microsoft Word documents, .pdf, and .lnk files. [3][21][14]

Thinks about how you would implement these TTPs:

- How would you go about implementing the TTP?
- What resources do you need?
- How long would it take you to implement these TTPs?
- What are your options if you don't have access to a particular tool (for example, Cobalt Strike)?

Summary

In this lab, you have used ATT&CK to understand APT29 targets and TTPs.

You also used a CTI article to understand the components and behaviors of an APT29 payload.

In the next lab, you will put this information to use by implementing your own trusted .LNK payload based on the Mandiant article.

Learning Check Answer Key

1. *Choose all that apply: according to ATT&CK, which entities has APT29 targeted previously?*
   a) government networks in Europe and NATO member countries
   b) research institutes
   c) financial services organizations
   d) think tanks

2. *Which of the following describes APT29's use of Spearphishing Link?*

   a) APT29 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
   b) APT29 has sent spearphishing emails containing links to .hta files.
   c) APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files.
   d) APT29 has used the legitimate mailing service Constant Contact to send phishing e-mails.

3. *The Mandiant report describes how APT29 sent phishing emails with hyperlinks to a zip file. What type of payload was contained in the zip files??*
   e) Windows Executable
   f) Windows DLL
   g) PowerShell Stager
   h) Windows Shortcut File

4. *The Mandiant report describes an APT29 initial access payload, ds7002.lnk. Select all of the payload components contained in ds7002.lnk:*
   g) PowerShell Loader
   h) PowerShell Empire Stager
   i) Embedded Cobalt Strike Beacon DLL
   j) Decoy Executable
   k) Decoy PDF
   l) Visual Basic Discovery Script