

# 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.

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

Home > Groups > APT29

## APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).<sup>[1][2]</sup> They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.<sup>[3][4][5][6]</sup>

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.<sup>[7][8]</sup> Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.<sup>[9]</sup>  
[10][11][12]

ID: G0016  
① Associated Groups: Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke  
Contributors: Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary  
Version: 2.0  
Created: 31 May 2017  
Last Modified: 30 April 2021

Version Permalink

GROUPS

Overview

admin@338

Ajax Security Team

APT-C-36

APT1

APT12

APT16

APT17

APT18

APT19

APT28

- Skim through APT29's TTPs; study APT29 [Initial Access](#) and [Execution](#) TTPs in particular. Examine how APT29 has executed phishing TTPs.

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1548	.002 Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC. <sup>[16]</sup>
Enterprise	T1087	Account Discovery	APT29 obtained a list of users and their roles from an Exchange server using <code>Get-ManagementRoleAssignment</code> . <sup>[12]</sup>
Enterprise	T1098	.001 Account Manipulation: Additional Cloud Credentials	APT29 has added credentials to OAuth Applications and Service Principals. <sup>[17]</sup>
		.002 Account Manipulation: Exchange Email Delegate Permissions	APT29 added their own devices as allowed IDs for active sync using <code>Set-CASMailbox</code> , allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals. <sup>[12][17]</sup>
Enterprise	T1583	.001 Acquire Infrastructure: Domains	APT29 has acquired C2 domains through resellers. <sup>[10][18]</sup>
		.006 Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERTOSS. <sup>[19]</sup>
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	APT29 has used HTTP for C2 and data exfiltration. <sup>[12]</sup>
Enterprise	T1560	.001 Archive Collected Data: Archive via Utility	APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfiltration. <sup>[12][20]</sup>
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT29 added Registry Run keys to establish persistence. <sup>[16]</sup>
		.009 Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution. <sup>[21]</sup>

Carbanak

Chimera

Cleaver

Cobalt Group

CopyKittens

Dark Caracal

Darkhotel

DarkHydus

DarkVishnya

Deep Panda

Dragonfly

Dragonfly 2.0

DragonOK

Dust Storm

Elderwood

Equation

Evilnum

FIN10

FIN4

FIN5

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

MITRE | ATT&CK<sup>®</sup>

Matrices   Tactics   Techniques   Mitigations   Groups   Software   Resources   Blog   Contribute   Search Q

Techniques Used

Click Here → ATT&CK<sup>®</sup> Navigator Layers

Enterprise Layer  
download  
view ?

Domain	ID	Name	Use
Enterprise	T1548 .002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC. <sup>[16]</sup>
Enterprise	T1087	Account Discovery	APT29 obtained a list of users and their roles from an Exchange server using <code>Get-ManagementRoleAssignment</code> . <sup>[7]</sup>
Enterprise	T1098 .001	Account Manipulation: Additional Cloud Credentials	APT29 has added credentials to OAuth Applications and Service Principals. <sup>[17]</sup>
	.002	Account Manipulation: Exchange Email Delegate Permissions	APT29 added their own devices as allowed IDs for active sync using <code>Set-CASMailbox</code> , allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals. <sup>[18][19]</sup>
Enterprise	T1583 .001	Acquire Infrastructure: Domains	APT29 has acquired C2 domains through resellers. <sup>[10][14]</sup>
	.006	Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as <code>HAMMERTOSS</code> . <sup>[11]</sup>
Enterprise	T1071	Application Layer Protocol: Web Protocols	APT29 has used HTTP for C2 and data exfiltration. <sup>[12]</sup>
Enterprise	T1560	Archive Collected Data: Archive via Utility	APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfiltration. <sup>[12][20]</sup>
Enterprise	T1547 .001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT29 added Registry Run keys to establish persistence. <sup>[16]</sup>
	.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution. <sup>[21]</sup>

APT29 (08816)					selection controls									
Techniques Used					layer controls									
Techniques Used					technique controls									
Reconnaissance	Resource Development	Initial Access	Execution	Persistence										
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques										
Active Scanning (0/2)	Botnet	Drive-by Compromise	AppleScript	Add Office 365 Global Administrator										
Gather Victim Host Information (0/4)	DNS Server	Exploit Public-Facing Application	JavaScript	Additional Cloud Credentials										
Gather Victim Identity Information (0/3)	Acquire Infrastructure (2/6)	External Remote Services	Network Device CLI	Exchange Email Delegate Permission										
Gather Victim Network Information (0/6)	Server	Hardware Additions	PowerShell	SSH Authorized Keys										
Gather Victim Org Information (0/4)	Virtual Private Server		Python	BITS Jobs										
Phishing for Information (0/3)	Compromise Accounts (0/2)	Phishing (2/3)	Unix Shell	Active Setup										
Search Closed Sources (0/2)	Botnet		Visual Basic	Authentication Package										
Search Open Technical Databases (0/5)	DNS Server	Replication Through Removable Media	Windows Command Shell	Kernel Modules and Extensions										
Search Open Websites/Domains (0/2)	Domains	Supply Chain Compromise (1/3)	Container Administration Command	LSASS Driver										
Search Victim-Owned Websites	Server	Compromise Hardware Supply Chain	Deploy Container	Plist Modification										
	Virtual Private Server	Compromise Software Dependencies and Development Tools	Exploitation for Client Execution	Port Monitors										
	Web Services	Compromise Software Supply Chain	Inter-Process Communication (0/2)	Print Processors										
	Code Signing Certificates		Native API	Re-opened Applications										
				Registry Run Keys / Startup Folder										
				Security Support Provider										

## Learning Check

- Choose all that apply: according to ATT&CK, which entities has APT29 targeted previously?
  - government networks in Europe and NATO member countries
  - research institutes
  - financial services organizations
  - think tanks
- Which of the following describes APT29's use of Phishing: Spearphishing Link?
  - APT29 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites.
  - 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.

Tactics ▾ Techniques ▾ Data Sources Mitigations ▾ Groups Software Resources ▾ Blog ↗ Contribute Search 🔍

### Identify TTPs mapped to this article

#### References

1. White House. (2021, April 15). Imposing Costs for Harmful Foreign Activities by the Russian Government. Retrieved April 16, 2021.
2. UK Gov. (2021, April 15). UK and US expose global campaign of malign activity by Russian intelligence services. Retrieved April 16, 2021.
3. F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.
4. Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017.
5. Alperovitch, D. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.
6. UK Gov. (2021, April 15). UK exposes Russian involvement in SolarWinds cyber compromise. Retrieved April 16, 2021.
7. NSA, FBI, DHS. (2021, April 15). Russian SVR Targets U.S. and Allied Networks. Retrieved April 16, 2021.
8. UK NCSC. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved April 16, 2021.
9. FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved January 4, 2021.
10. Nafisi, R., Lelli, A. (2021, March 4). GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved March 8, 2021.
21. Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.
22. MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved December 30, 2020.
23. Smith, L., Leathery, J., Read, B. (2021, March 4). New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452. Retrieved March 12, 2021.
24. FireEye Labs. (2015, July). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Retrieved September 17, 2015.
25. MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop. Retrieved January 22, 2021.
26. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018.
27. MSTIC. (2020, December 18). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers. Retrieved January 5, 2021.
28. Symantec Security Response. (2015, July 13). "Forkmeiamfamous": Seaduke, latest weapon in the Duke armory. Retrieved July 22, 2015.
29. MSRC Team. (2021, February 18). Microsoft Internal Solorigate Investigation – Final Update. Retrieved May 14, 2021.

1 of 10 matches Begins with 🔍 [26] Done

		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution. <sup>[26]</sup>
Enterprise	T1110	.003	Brute Force: Password Spraying	APT29 has conducted brute force password spray attacks. <sup>[17]</sup>
Enterprise	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. <sup>[12][27][28][21][26]</sup>
		.003	Command and Scripting Interpreter: Windows Command Shell	APT29 used <code>cmd.exe</code> to execute commands on remote machines. <sup>[12][27]</sup>

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