

# MITRE ATT&CK®: APT29 Techniques Mapped to Mitigations and Data Sources

## GET STARTED WITH ATT&CK

### Use ATT&CK for Cyber Threat Intelligence

Cyber threat intelligence comes from many sources, including knowledge of past incidents, commercial threat feeds, information-sharing groups, government threat-sharing programs, and more. ATT&CK gives analysts a common language to communicate across reports and organizations, providing a way to structure, compare, and analyze threat intelligence.

| Initial Access | Execution                         | Persistence       | Privilege Escalation | Defense Evasion              | Credential Access | Discovery        | Lateral Movement | Collection             | Command & Control | Exfiltration                             | Impact                       |
|----------------|-----------------------------------|-------------------|----------------------|------------------------------|-------------------|------------------|------------------|------------------------|-------------------|--|------------------------------|
| Remote Access  | Remote Management Instrumentation | Session Hijacking | Valid Accounts       | Multi-Authentication Process | Network Sniffing  | System Discovery | Remote Services  | Data File Local System | Data Observation  | Exfiltration Over Other Network Protocol | Data Exfiltration for Impact |
| Remote Access  | Remote Management Instrumentation | Session Hijacking | Valid Accounts       | Multi-Authentication Process | Network Sniffing  | System Discovery | Remote Services  | Data File Local System | Data Observation  | Exfiltration Over Other Network Protocol | Data Exfiltration for Impact |

Comparing APT28 to APT29

### Use ATT&CK to Build Your Defensive Platform

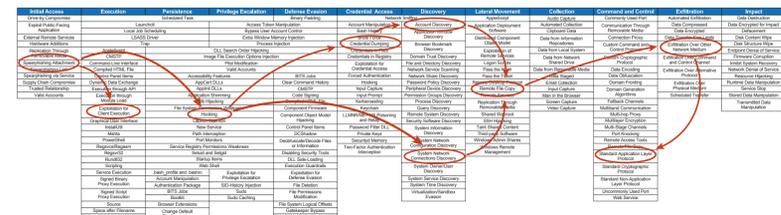
ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.

| Initial Access | Execution                         | Persistence       | Privilege Escalation | Defense Evasion              | Credential Access | Discovery        | Lateral Movement | Collection             | Command & Control | Exfiltration                             | Impact                       |
|----------------|-----------------------------------|-------------------|----------------------|------------------------------|-------------------|------------------|------------------|------------------------|-------------------|--|------------------------------|
| Remote Access  | Remote Management Instrumentation | Session Hijacking | Valid Accounts       | Multi-Authentication Process | Network Sniffing  | System Discovery | Remote Services  | Data File Local System | Data Observation  | Exfiltration Over Other Network Protocol | Data Exfiltration for Impact |

Finding Gaps in Defense

### Use ATT&CK for Adversary Emulation and Red Teaming

The best defense is a well-tested defense. ATT&CK provides a common adversary behavior framework based on threat intelligence that red teams can use to emulate specific threats. This helps cyber defenders find gaps in visibility, defensive tools, and processes—and then fix them.



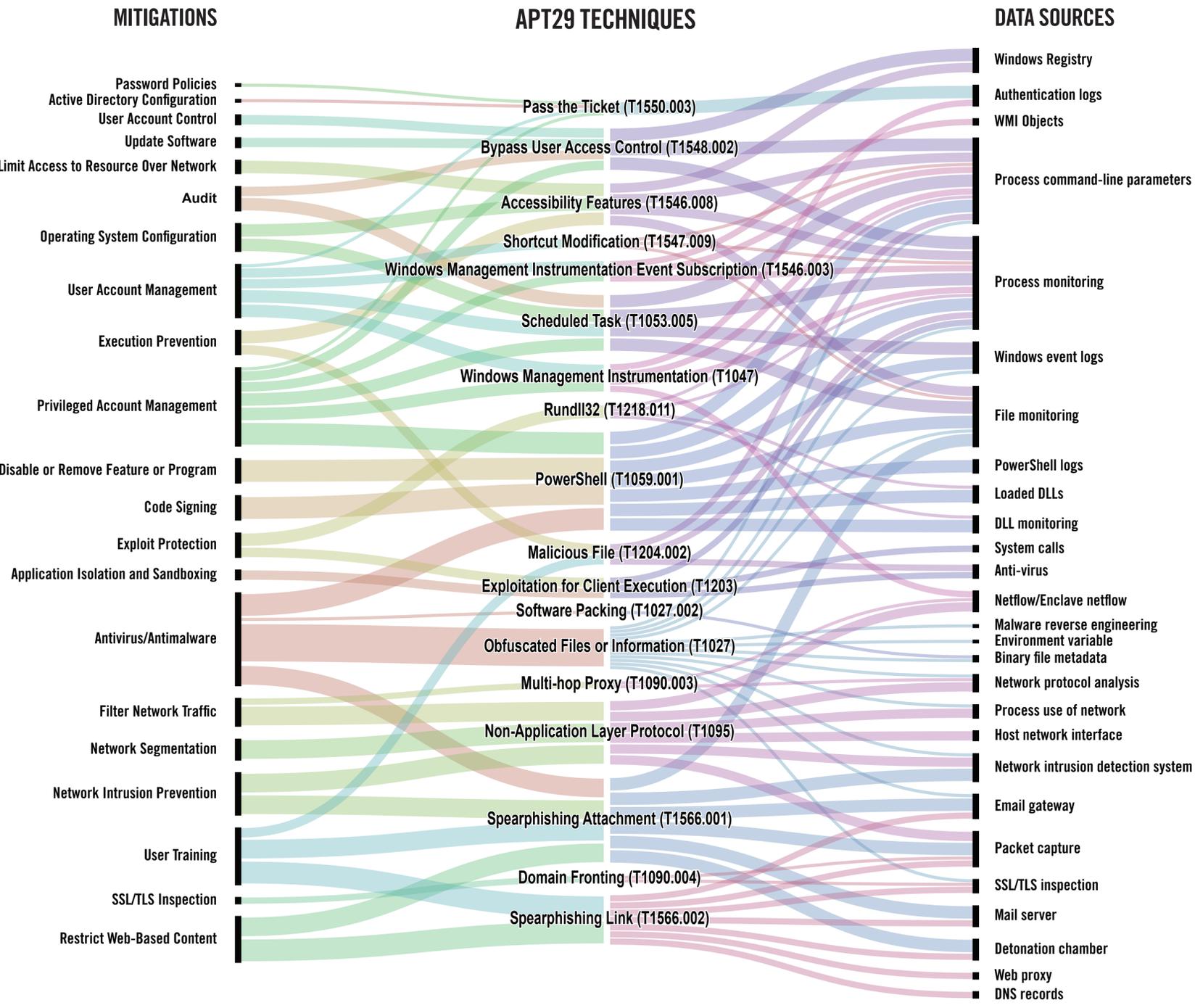
## ABOUT THIS DIAGRAM

### Aligning your Defenses to Adversaries with ATT&CK

ATT&CK provides a framework for defenders to enhance their posture against specific adversaries. To use ATT&CK in this way, find an adversary group you're interested in and identify the techniques that they are known to use. For each technique, pull up the technique page to see how that adversary uses the technique, as well as how you can potentially mitigate and detect it.

This chart helps visualize the results. Here, we have the techniques that APT29 is known to use in the middle column. We linked each technique on the left to potential means of mitigation and on the right to data sources that defenders can use to potentially detect the technique. Defenders can look at this chart either to see how their current mitigations and data sources stack up to APT29, or as a roadmap to plan how they can architect their defenses.

For more information, you can read about APT29, or other groups, on the ATT&CK website: [attack.mitre.org](https://attack.mitre.org).



Mitigate It!

Detect It!

To help cyber defenders gain a common understanding of the threats they face, MITRE developed the ATT&CK framework. It's a globally-accessible knowledge base of adversary tactics and techniques based on real world observations and open source research contributed by the cyber community.

Used by organizations around the world, ATT&CK provides a shared understanding of adversary tactics, techniques and procedures and how to detect, prevent, and/or mitigate them.

ATT&CK is open and available to any person or organization for use at no charge.

For more than 60 years, MITRE has worked in the public interest. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

| Initial Access<br>9 techniques      | Execution<br>10 techniques         | Persistence<br>18 techniques         | Privilege Escalation<br>12 techniques | Defense Evasion<br>34 techniques            | Credential Access<br>14 techniques   | Discovery<br>24 techniques            | Lateral Movement<br>9 techniques | Collection<br>16 techniques        | Command and Control<br>16 techniques | Exfiltration<br>9 techniques           | Impact<br>13 techniques   |
|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|---|--------------------------------------|---------------------------------------|----------------------------------|------------------------------------|--------------------------------------|--|---------------------------|
| Valid Accounts                      | Scheduled Task/Job                 |                                      | Modify Authentication Process         |   | System Service Discovery             |                                       | Remote Services                  | Data from Local System             | Data Obfuscation                     | Exfiltration Over Other                | Data Destruction          |
| Replication Through Removable Media | Windows Management Instrumentation | Valid Accounts                       |                                       | Network Sniffing                            |                                      | Software Deployment                   | Tools                            | Data from Removable Media          | Fallback Channels                    | Network Medium                         | Data Encrypted for Impact |
| Trusted Relationship                | Software Deployment                | Hijack Execution Flow                |                                       | OS Credential Dumping                       | Application Window Discovery         | Replication Through Removable Media   | Input Capture                    | Media                              | Application Layer Protocol           | Scheduled Transfer                     | Service Stop              |
| Supply Chain Compromise             | Tools                              | Boot or Logon Initialization Scripts | Direct Volume Access                  | Input Capture                               | Discovery                            | Internal Spearphishing                | Screen Capture                   | Proxy                              | Proxy                                | Data Transfer Size Limits              | Inhibit System Recovery   |
| Hardware Additions                  | Shared Modules                     | Event Triggered Execution            | Obfuscated Files or Information       | Two-Factor Authentication Interception      | System Owner/User Discovery          | Use Alternate Authentication Material | Email Collection                 | Web Service                        | Web Service                          | Exfiltration Over C2 Channel           | Defacement                |
| Exploit Public-Facing Application   | User Execution                     | Boot or Logon Autostart Execution    |                                       | Information                                 | System Owner/User Discovery          | Lateral Tool Transfer                 | Clipboard Data                   | Multi-Stage Channels               | Ingress Tool Transfer                | Exfiltration Over Physical Medium      | Resource Hijacking        |
| Phishing                            | Exploitation for Client Execution  | Account Manipulation                 | Process Injection                     | Exploitation for Credential Access          | System Network Connections Discovery | Taint Shared Content                  | Automated Collection             | Dynamic Resolution                 | Dynamic Resolution                   | Exfiltration Over Web Service          | Network Denial of Service |
| External Remote Services            | System Services                    | Office Application Startup           | Group Policy Modification             | Steal Web Session Cookie                    | Permission Groups                    | Exploitation of Remote Services       | Audio Capture                    | Traffic Signaling                  | Traffic Signaling                    | Automated Exfiltration                 | System Shutdown/Reboot    |
| Drive-by Compromise                 | Command and Scripting Interpreter  | Create Account                       | Abuse Elevation Control Mechanism     | Unsecured Credentials                       | Credentials from Password Stores     | Remote Service Session Hijacking      | Video Capture                    | Man in the Browser                 | Remote Access Software               | Exfiltration Over Alternative Protocol | Account Access Removal    |
|                                     | Native API                         | Browser Extensions                   | Exploitation for Privilege Escalation | Indicator Removal on Host                   | Credentials from Password Stores     | File and Directory Discovery          | Man in the Browser               | Data from Information Repositories | Dynamic Resolution                   | Exfiltration Over Alternative Protocol | Disk Wipe                 |
|                                     | Inter-Process Communication        | Traffic Signaling                    |                                       | Modify Registry                             | Steal or Forge Kerberos Tickets      | Peripheral Device Discovery           | Repositories                     | Man-in-the-Middle                  | Non-Standard Port                    | Transfer Data to Cloud Account         | Data Manipulation         |
|                                     |                                    | BITS Jobs                            |                                       | Trusted Developer Utilities Proxy Execution | Forced Authentication                | Network Share Discovery               | Man-in-the-Middle                | Protocol Tunneling                 | Encrypted Channel                    |  |                           |
|                                     |                                    | Server Software Component            |                                       | Traffic Signaling                           | Steal Application Access Token       | Password Policy Discovery             | Archive Collected Data           | Non-Application Layer Protocol     |                                      |  |                           |
|                                     |                                    | Pre-OS Boot                          |                                       | Signed Script Proxy Execution               | Man-in-the-Middle                    | Browser Bookmark Discovery            | Data from Network Shared Drive   |                                    |                                      |  |                           |
|                                     |                                    | Compromise Client Software Binary    |                                       | Rogue Domain Controller                     |                                      | Virtualization/Sandbox Evasion        | Data from Cloud Storage Object   |                                    |                                      |  |                           |
|                                     |                                    | Implant Container Image              |                                       | Indirect Command Execution                  |                                      | Cloud Service Dashboard               |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | BITS Jobs                                   |                                      | Software Discovery                    |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | XSL Script Processing                       |                                      | Query Registry                        |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Template Injection                          |                                      | Remote System Discovery               |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | File and Directory Permissions Modification |                                      | Network Service Scanning              |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Virtualization/Sandbox Evasion              |                                      | Process Discovery                     |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Unused/Unsupported Cloud Regions            |                                      | System Information Discovery          |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Use Alternate Authentication Material       |                                      | Account Discovery                     |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Impair Defenses                             |                                      | System Time Discovery                 |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Hide Artifacts                              |                                      | Domain Trust Discovery                |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Masquerading                                |                                      | Cloud Service Discovery               |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Deobfuscate/Decode Files or Information     |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Signed Binary Proxy Execution               |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Exploitation for Defense Evasion            |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Execution Guardrails                        |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Modify Cloud Compute Infrastructure         |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Pre-OS Boot                                 |                                      |                                       |                                  |                                    |                                      |  |                           |
|                                     |                                    |                                      |                                       | Subvert Trust Controls                      |                                      |                                       |                                  |                                    |                                      |  |                           |

≡ Has sub-techniques

# MITRE ATT&CK<sup>®</sup> Enterprise Framework

attack.mitre.org