

**OST**  
Ostschweizer  
Fachhochschule

# Cyber Defense HS2024

## Mitre ATT&CK Framework

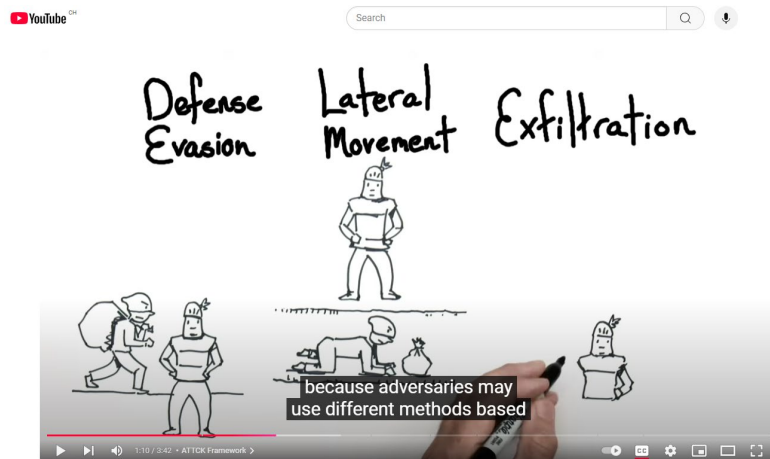
Ivan Bütler

12. November 2024

Abteilung Informatik, Rapperswil

# ATT&CK

- Acronym for “Adversarial Tactics, Techniques, & Common Knowledge”
- Framework to document common **tactics**, **techniques** and **procedures** (TTPs) that advanced persistent threats use against Windows enterprise networks
- Based on real-life observations (published reports) and attributions (mostly by vendors such as FireEye, Sophos, Kaspersky, ...)
- Useful for “blue” and “red” teams to understand an attack or a simulation



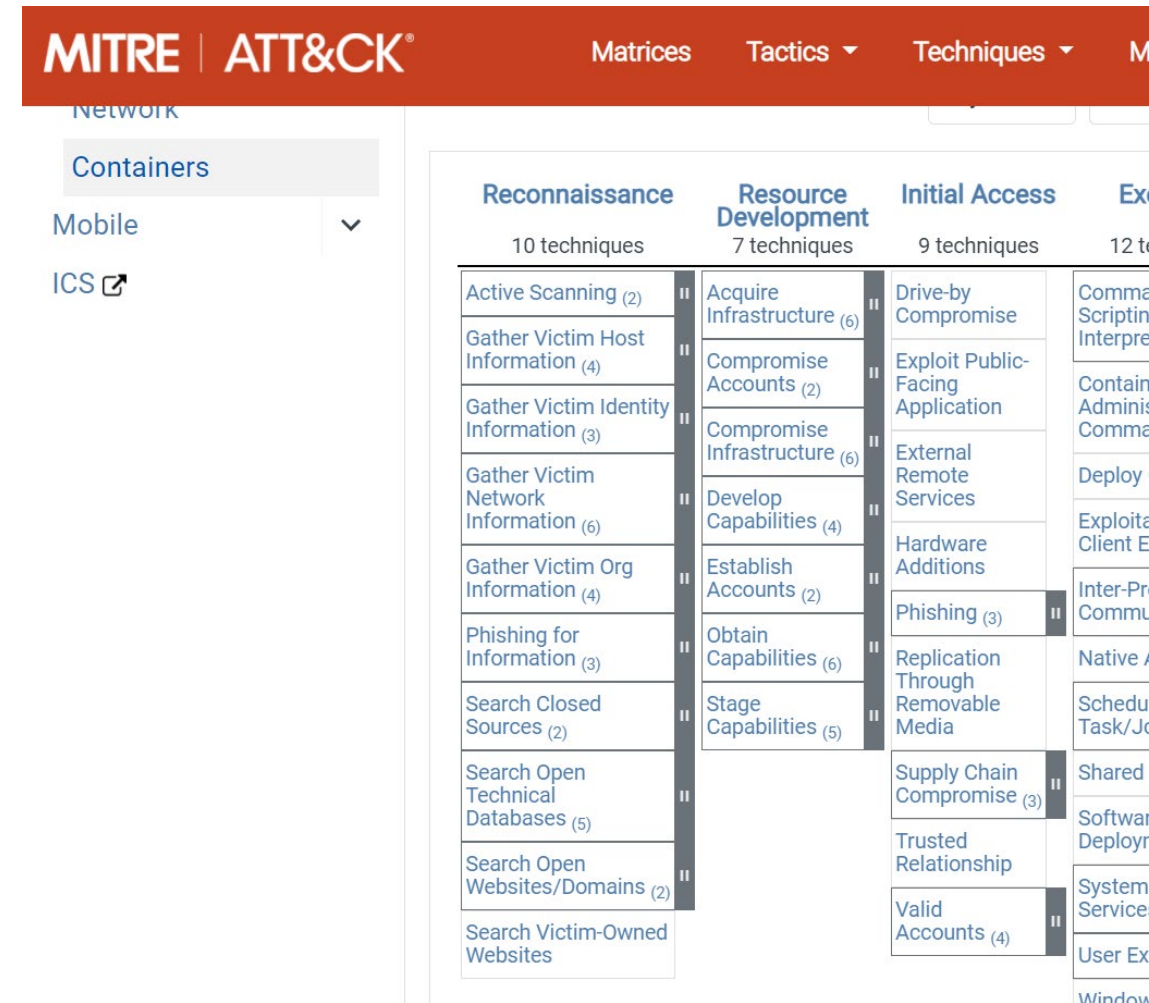
<https://www.youtube.com/watch?v=Yxv1suJYMI8>



# What is MITRE ATT&CK?

## What attacks do adversaries use?

- A knowledge base of adversary behavior
  - Based on real-world observations
  - Free, open, and globally accessible
  - A common language
  - Community-driven



The screenshot displays the MITRE ATT&CK framework interface. The top navigation bar includes the MITRE ATT&CK logo and links to Matrices, Tactics, and Techniques. A left sidebar shows a navigation menu with categories: Network, Containers, Mobile, and ICS. The main content area displays the 'Reconnaissance' matrix, which lists 10 techniques. The techniques are organized into columns: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), and Execution (12 techniques). The Reconnaissance column lists techniques such as Active Scanning, Gather Victim Host Information, Gather Victim Identity Information, Gather Victim Network Information, Gather Victim Org Information, Phishing for Information, Search Closed Sources, Search Open Technical Databases, Search Open Websites/Domains, and Search Victim-Owned Websites. The Resource Development column lists techniques such as Acquire Infrastructure, Compromise Accounts, Compromise Infrastructure, Develop Capabilities, Establish Accounts, Obtain Capabilities, and Stage Capabilities. The Initial Access column lists techniques such as Drive-by Compromise, Exploit Public-Facing Application, External Remote Services, Hardware Additions, Phishing, Replication Through Removable Media, Supply Chain Compromise, Trusted Relationship, and Valid Accounts. The Execution column lists techniques such as Command and Scripting Interpreter, Container Administration, Deployment, Exploitation of Client E, Inter-Process Communication, Native Application, Scheduling Task/Jobs, Shared Libraries, Software Deployment, System Services, and User Execution.

Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	12 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deployment
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation of Client E
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native Application
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduling Task/Jobs
Search Open Technical Databases (5)		Trusted Relationship	Shared Libraries
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment
Search Victim-Owned Websites			System Services
			User Execution

# Terminology

Terminology	Description	Example
Matrices	Container Name for Tactics & Techniques	<ul style="list-style-type: none"><li>• Enterprise</li><li>• Mobile</li><li>• ICS</li></ul>
Tactics	Tactics represent the " <b>why</b> " of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.	<ul style="list-style-type: none"><li>• TA0001 Initial Access</li><li>• TA0003 Persistence</li><li>• TA0008 Lateral Movement</li></ul>
Techniques	Techniques represent ' <b>how</b> ' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.	<ul style="list-style-type: none"><li>• TA0001 Initial Access<ul style="list-style-type: none"><li>• T1659 Content Injection</li><li>• T1189 Drive-by</li><li>• T1190 Exploit Public Apps</li></ul></li></ul>
Sub-techniques	Technique performed by known hacker groups	<ul style="list-style-type: none"><li>• APT19</li><li>• APT32</li><li>• APT37</li><li>• Bandook</li></ul>

# Matrix Overview

## Tactics

### Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
	Command-Line Interface		AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
External Remote Services	Compiled HTML File	Account Manipulation	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery		Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Internal Spearphishing	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
	Dynamic Data Exchange	Application Shimming	Code Signing	Compile After Delivery	Credentials in Registry	Network Share Discovery	Logon Scripts	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Attachment	Execution through API	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Credentials in Registry	Network Sniffing	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Link	Execution through Module Load	BITS Jobs	Dylib Hijacking	Component Firmware	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Elevated Execution with Prompt	Component Object Model Hijacking	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Emond	Connection Proxy	Hooking	Permission Groups Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Resource Hijacking
	InstallUtil	Change Default File Association	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Process Discovery	Remote Services	Man in the Browser	Fallback Channels	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Launchctl	Component Firmware	DCShadow	Deobfuscate/Decode Files or Information	Input Prompt	Query Registry	Replication Through Removable Media	Screen Capture	Multi-hop Proxy	Scheduled Transfer	Service Stop
Valid Accounts	Local Job Scheduling	Component Object Model Hijacking	Extra Window Memory Injection	Disabling Security Tools	Kerberoasting	Remote System Discovery	Shared Webroot	Video Capture	Multi-Stage Channels	Multiband Communication	Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	File System Permissions Weakness	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	SSH Hijacking	Multilayer Encryption	Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Hooking	DLL Side-Loading	Network Sniffing	Software Discovery	Taint Shared Content				
	Powercat	File Permissions	Process Hijacking	Execution Guardrails	Powercat	System Information					

# Tactics

ID	Name	Description
<a href="#">TA0043</a>	<b>Reconnaissance*</b>	The adversary is trying to gather information they can use to plan future operations.
<a href="#">TA0042</a>	<b>Resource Development*</b>	The adversary is trying to establish resources they can use to support operations.
<a href="#">TA0001</a>	<b>Initial Access</b>	The adversary is trying to get into your network.
<a href="#">TA0002</a>	<b>Execution</b>	The adversary is trying to run malicious code.
<a href="#">TA0003</a>	<b>Persistence</b>	The adversary is trying to maintain their foothold.
<a href="#">TA0004</a>	<b>Privilege Escalation</b>	The adversary is trying to gain higher-level permissions.
<a href="#">TA0005</a>	<b>Defense Evasion</b>	The adversary is trying to avoid being detected.
<a href="#">TA0006</a>	<b>Credential Access</b>	The adversary is trying to steal account names and passwords.
<a href="#">TA0007</a>	<b>Discovery</b>	The adversary is trying to figure out your environment.
<a href="#">TA0008</a>	<b>Lateral Movement</b>	The adversary is trying to move through your environment.
<a href="#">TA0009</a>	<b>Collection</b>	The adversary is trying to gather data of interest to their goal.
<a href="#">TA0011</a>	<b>Command and Control</b>	The adversary is trying to communicate with compromised systems to control them.
<a href="#">TA0010</a>	<b>Exfiltration</b>	The adversary is trying to steal data.
<a href="#">TA0040</a>	<b>Impact*</b>	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

# Mitre Att&ck Navigator

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Spearphishing Attachment	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Connection Proxy	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels	Stored Data Manipulation	Network Denial of Service
Spearphishing Link	InstallUtil	Component Firmware	Hooking	Control Panel Items	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	System Shutdown/Reboot	Resource Hijacking
Spearphishing via Service	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Kerberoasting	Process Discovery	Screen Capture	Multi-Stage Channels	Multiband Communication	Transmitted Data Manipulation	Runtime Data Manipulation
Supply Chain Compromise	Mshta	Create Account	DLL Search Order Hijacking	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Shared Webroot	Multilayer Encryption	Remote Access Tools		Service Stop
Trusted Relationship	PowerShell	DLL Search Order Hijacking	DLL Side-Loading	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Taint Shared Content	Third-party Software	Remote File Copy		Service Stop
Valid Accounts	Regsvcs/Regasm	External Remote Services	New Service	File System Permissions Weakness	Password Filter DLL	Software Discovery	Windows Admin Shares				Service Stop
	Regsvr32	File System Permissions Weakness	Parent PID Spoofing		Private Keys	System Information Discovery					Service Stop
	Rundll32		Path		Steal Web Session Cookie	System Network					Service Stop
	Scheduled Task										Service Stop



# MITRE ATT&CK Navigator

MITRE | ATT&CK®

Matrices

Tactics ▾

Techniques ▾

Mitigations ▾

Groups

Software

Resources ▾

Blog ↗

Contribute

Search 🔍

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Data Obfuscation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	User Execution (2)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Fallback Channels	Exfiltration Over Physical Medium (1)	Inhibit System Recovery	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	Group Policy Modification	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Windows Management Instrumentation	Event Triggered Execution (15)	Hijack Execution Flow (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
Search Victim-Owned Websites				External Remote Services	Process Injection (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		System Shutdown/Reboot
				Implant Container Image	Valid Accounts (4)	Indicator Removal on Host (6)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		
				Office Application Startup (6)		Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Masquerading (6)	Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Modify Authentication Process (4)		Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Cloud Compute Infrastructure (4)		Query Registry		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Registry		Remote System Discovery		Video Capture			
				Valid		Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (5)		System Network Configuration Discovery					
								System Network Connections Discovery					



# MITRE ATT&CK Framework

- Threat Actors (Groups)
  - Tracking activities of 100+ threat actors (groups)
  - Collection from real attacks
  - Structured observations
  - Technical details, guidance and examples
  - Open source intelligence only

**MITRE | ATT&CK®**

MatricesTactics ▾Techniques ▾Mitigations ▾GroupsSoftwareResources ▾Blog ↗ContributeSearch 🔍

APT18APT19APT28APT29APT3APT30APT32APT33APT37

analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 109

Name	Associated Groups	Description
<a href="#">admin@338</a>		<a href="#">admin@338</a> is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as <a href="#">PoisonIvy</a> , as well as some non-public backdoors.
<a href="#">APT-C-36</a>	Blind Eagle	<a href="#">APT-C-36</a> is a suspected South America espionage group that has been active since at least 2018. The group mainly

# Mögliche Prüfungsfrage

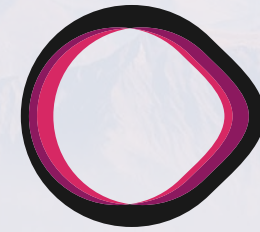
- Was ist nicht Teil des MITRE ATT&CK Frameworks:
  1. Steckbriefe von Threat Actor Gruppen
  2. Anwendungsbeispiele für Malware/Tools
  3. Online-Navigationstool zur Erstellung von personalisierten Matrixen/Tabellen
  4. Liste mit Standard-Passwörtern für Firewalls
  5. Hunting-Queries für VirusTotal
  6. Technique, das Phishing beschreibt

>> 4 und 5 sind nicht enthalten

# Mögliche Prüfungsfrage

- Nennen Sie 2 MITRE ATT&CK Kategorien mit hohem Potential um Hunts zu schreiben. Erläutern Sie warum (viele Log Quellen etc.)?

Kategorie	Beschreibung
<b><u>Execution</u></b>	<ul style="list-style-type: none"><li>• Generiert viele Logs</li><li>• Kann vom AV erkannt werden</li><li>• Viele Artefakte</li></ul>
<b><u>Persistence</u></b>	<ul style="list-style-type: none"><li>• Generiert viele Logs</li><li>• Kann vom AV erkannt werden</li><li>• Viele Artefakte</li></ul>
<b>Defense Evasion</b>	<ul style="list-style-type: none"><li>• Generiert viele Logs</li><li>• Kann vom AV erkannt werden</li><li>• Viele Artefakte</li></ul>



**OST**  
Ostschweizer  
Fachhochschule

# **Attack Simulation**

## **Red Team, Blue Team Tools**

Ivan Bütler

12. November 2024

Abteilung Informatik, Rapperswil



VECTR documentation can be found here: <https://docs.vectr.io>

- VECTR is a tool that facilitates tracking of your red and blue team testing activities to measure detection and prevention capabilities across different attack scenarios. VECTR provides the ability to create assessment groups, which consist of a collection of Campaigns and supporting Test Cases to simulate adversary threats. Campaigns can be broad and span activity across the kill chain, from initial compromise to privilege escalation and lateral movement and so on, or can be a narrow in scope to focus on specific detection layers, tools, and infrastructure. VECTR is designed to promote full transparency between offense and defense, encourage training between team members, and improve detection & prevention success rate across the environment.

The screenshot displays the MITRE ATT&CK Assessment Heatmap tool interface. At the top, the campaign is identified as "Atomic Red (MITRE) Assessment - 2018" with the status "ALL SELECTED". The heatmap itself is a grid where rows represent specific attack techniques and columns represent different stages of an attack (e.g., Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command and Control). Each cell in the grid is color-coded based on its severity or coverage, with a legend at the top indicating a scale from "No Coverage" (grey) to "Strong" (green). A detailed tooltip for the technique "T1223 - Compiled HTML Help Remote Payload" is open, showing its description, execution details, and evasion techniques. The tooltip also includes a "No Coverage" label and a "Weakness" indicator.

Status: Completed



Attack Start

07/01/2020 09:54:20  
status changed to  
InProgress

Attack Stop

07/01/2020 09:54:21  
status changed to  
Completed

Source IPs

Linux VM

Red Team Details

Name

Extract Logonpasswords via Dumpert

Description

Use dumpert to extract credentials from LSASS process memory

Technique

Credential Dumping

Phase

Credential Access

Operator Guidance

beacon>  
dumpert

References



Attacker Tools

Dumpert  
Cobalt Strike

Target Assets

Target Laptop

Blue Team Details

Outcome

☐ TBD ☒ Blocked ☐ Detected ☐ NotDetected

Detecting Blue Tool(s):

EDR platform

Was an alert triggered?

☒ Yes ☐ TBD ☐ No

Outcome Notes

Ran dumpert on target workstation, successfully blocked by EDR/NGAV agent and alerted via SIEM.

Tags

High Priority RE-TEST

Rules

Detection

1) Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs



Prevention

1) Suspicious process execution is blocked by EDR or other endpoint security tool

Detection Time

07/01/2020 09:55:48  
outcome changed to  
Blocked

Expected

Detection Layers

SIEM

EDR

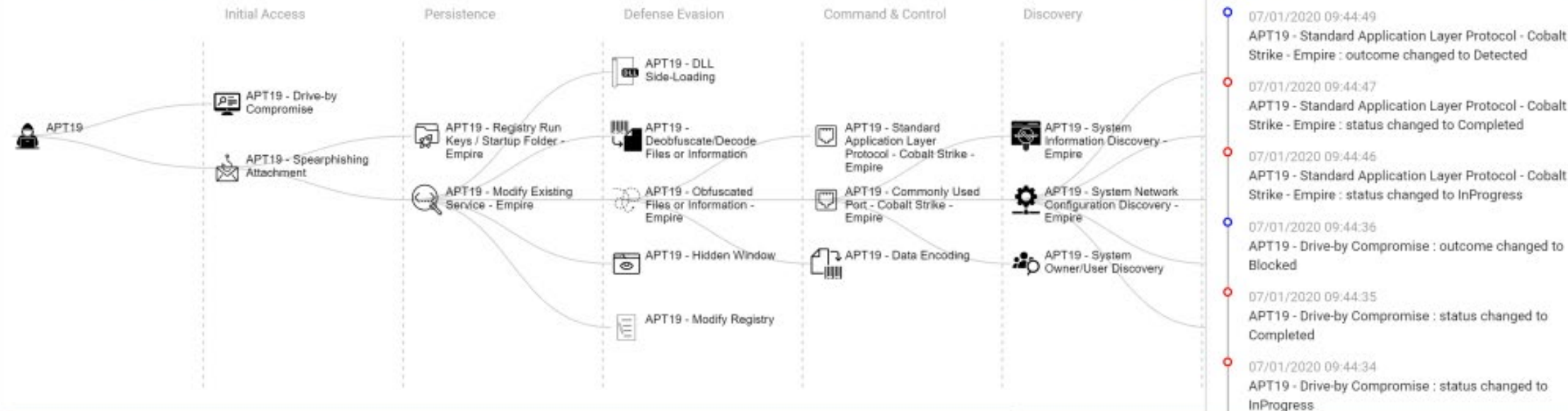
Endpoint Protection

Screenshot from <https://docs.vectr.io/>

## APT19: Escalation Path

PNG

## Timeline



## Test Cases

NEW

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Discovery	System Information Discovery	APT19 - System Information Discovery - Empire	Completed	Not Detected	High Priority	
Persistence	Registry Run Keys / Startup Folder	APT19 - Registry Run Keys / Startup Folder - Empire	Completed	Blocked		
Defense Evasion	DLL Side-Loading	APT19 - DLL Side-Loading	Completed	Not Detected	Medium Priority	
Execution	Regsvr32	APT19 - Regsvr32	Completed	Detected		
Initial Access	Drive-by Compromise	APT19 - Drive-by Compromise	Completed	Blocked		
Command & Control	Standard Application Layer Protocol	APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire	Completed	Detected		

Report Type

Assessments

Campaigns

Outcomes

Statuses

Heat Map - Enterprise Purple - 2018 Q1 + 3 more - Register Phishing Domains + 88 more -

ALL SELECTED - Completed + 3 more -

## Assessment Heat Map

Map Type

Display Mode

Latest

Allow Repeats

MITRE FILTERS

VECTR FILTERS

EXPORT LAYER

STATS

PNG

?

Test Cases: 282

Unique Test Cases: 244

Techniques: 79

Unique Techniques: 63

Blocked: 50

Detected: 52

Not Detected: 31

No Test Coverage

Outcome TBD

Weakest

Minimal

Lower

Moderate

Strong

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application 3	Component Object Model and Distributed COM 2	Create Account 2	Exploitation for Privilege Escalation 2	DCShadow	Brute Force 6	Account Discovery 3	Component Object Model 2	Data from Local System 2	Commonly Used Port 9	Automated Exfiltration 7	Data Encrypted for Impact
External Remote Services 2	Dynamic Data Exchange	External Remote Services 2	New Service	Disabling Security Tools 4	Credential Dumping 8	Enterprise Purple - 2020 Q1 T1003 • Logged: No			Custom Command and Control Protocol 7	Data Compressed	
Hardware Additions 5	Execution through API	Local Job Scheduling 2	Parent PID Spoofing	Indicator Blocking	Kerberoasting 2	Enterprise Purple - 2020 Q1 T1003 • Logged: No			Multi-hop Proxy	Data Encrypted	
Replication Through Removable Media 3	Exploitation for Client Execution 12	Modify Existing Service	Valid Accounts 4	Masquerading 8	LLMNR/NBT-NS 3	Enterprise Purple - 2020 Q1 T1003 • Logged: No				Exfiltration Over Alternative Protocol 7	
Spearphishing Attachment 31	Local Job Scheduling 2	New Service		Mahta 2	Poisoning and Relay 3	Enterprise Purple - 2020 Q1 T1003 • Logged: No				Exfiltration Over Command and Control Channel 3	
Spearphishing Lateral 33	Mahta 2	Registry Run Key/Startup Folder 2		Obfuscated Files and Information 2	Network Sniffing 3	Enterprise Purple - 2020 Q1 T1003 • Logged: No				Exfiltration Over Other Network Medium 2	
Trusted Relationship 2	PowerShell 4	Valid Accounts 4		Parent PID Spoofing		Enterprise Purple - 2020 Q1 T1003 • Logged: No				Exfiltration Over Physical Medium 5	
Valid Accounts 4	Regsvr32 2	Windows Management Instrumentation Event Subscription		Regsvr32 2		Enterprise Purple - 2020 Q1 T1003 • Logged: No					
	Scripting 5			Scripting 5		Enterprise Purple - 2020 Q1 T1003 • Logged: No					
	Signed Binary Proxy Execution			Signed Binary Proxy Execution		Enterprise Purple - 2020 Q1 T1003 • Logged: No					
	Trusted Developer Utilities			Template Injection		Enterprise Purple - 2020 Q1 T1003 • Logged: No					
	User Execution 5			Trusted Developer Utilities		Enterprise Purple - 2020 Q1 T1003 • Logged: No					
				Valid Accounts 4		Enterprise Purple - 2020 Q1 T1003 • Logged: No					





Report Type

Assessments

Campaigns

Metrics

TED

ALL SELECTED

Test Case Drilldown

Historical Trending

Heat Map

Toolset Drilldown

Campaigns Aggregated

105

Test Cases Completed:

765

Test Cases Passed:

361

 Detected:

174

 Blocked:

187

Test Cases Failed:

404

 Not Detected:

404

Test Cases Not Completed:

0

 To Be Determined:

0

Overall Score

Average

