Matriz Mitre ATT&CK® for Enterprise V12

Tácticas, técnicas y conocimiento común de adversarios (11/2022)



¿QUÉ ES MITRE ATT&CK?

Se trata de una base de conocimiento en el que se muestran las tácticas y técnicas que forman parte del ciclo de vida de un ciberataque.

Utilizada por los equipos Red Team (ofensivos) para modelar ataques, y equipos Blue Team (defensivo) para mitigaciones.



TÉCNICAS ENTERPRISE En la actualidad la matriz está conformada por 14 técnicas.

ID	Nombre	Descripción
TA0043	Reconocimiento	El adversario está tratando de recopilar información que pueda usar para planificar operaciones futuras.
TA0042	Desarrollo de recursos	El adversario está tratando de establecer recursos que puedan usar para apoyar las operaciones.
TA0001	Acceso incial	El adversario está tratando de entrar en su red.



TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0002	Ejecución	El adversario está tratando de ejecutar un código malicioso.
TA0003	Persistencia	El adversario está tratando de mantener su punto de apoyo.
TA0004	Elevación de privilegios	El adversario está tratando de obtener permisos de nivel superior.
TA0005	Evasión de defensa	El adversario está tratando de evitar ser detectado.



TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0006	Acceso a credenciales	El adversario está tratando de robar nombres de cuenta y contraseñas.
TA0007	Descubrimiento	El adversario está tratando de averiguar su entorno.
TA0008	Movimiento lateral	El adversario está tratando de moverse a través de su entorno.
TA0009	Recopilación	El adversario está tratando de recopilar datos de interés para su objetivo.



TÉCNICAS ENTERPRISE

ID	Nombre	Descripción
TA0011	Command & Control	El adversario está tratando de comunicarse con los sistemas comprometidos para controlarlos.
TA0010	Exfiltración	El adversario está tratando de robar datos.
TA0040	Impacto	El adversario está tratando de manipular, interrumpir o destruir sus sistemas y datos.



TÁCTICAS ENTERPRISE

Cada una de las técnicas esta compuesta por una serie de **TÁCTICAS**.

ID	Nombre	Tácticas
TA0043	Reconocimiento	10
TA0042	Desarrollo de recursos	7
TA0001	Acceso incial	9
TA0002	Ejecución	13
TA0003	Persistencia	19



TÁCTICAS ENTERPRISE

ID	Nombre	Tácticas
TA0004	Elevación de privilegios	13
TA0005	Evasión de defensa	42
TA0006	Acceso a credenciales	17
TA0007	Descubrimiento	30
TA0008	Movimiento lateral	9
TA0009	Recopilación	17



TÁCTICAS ENTERPRISE

ID	Nombre	Tácticas
TA0011	Command & Control	16
TA0010	Exfiltración	9
TA0040	Impacto	13
	TOTAL	224



FASES DEL CIBERATAQUE

PREPARACIÓN

INTRUSIÓN

BRECHA ACTIVA

TA0043

Reconocimiento

TA0001

Acceso inicial

TA0004

Escalada de privilegios

TA0005

Evasión de defensas

TA0042

Desarrollo de recursos

TA0002

TA0003

Ejecución

Persistencia

TA0006

Acceso a credenciales

TA0007

Descubrimiento

8000AT

Movimiento lateral

TA0009

Recopilación

TA0011

Command & Control

TA0010

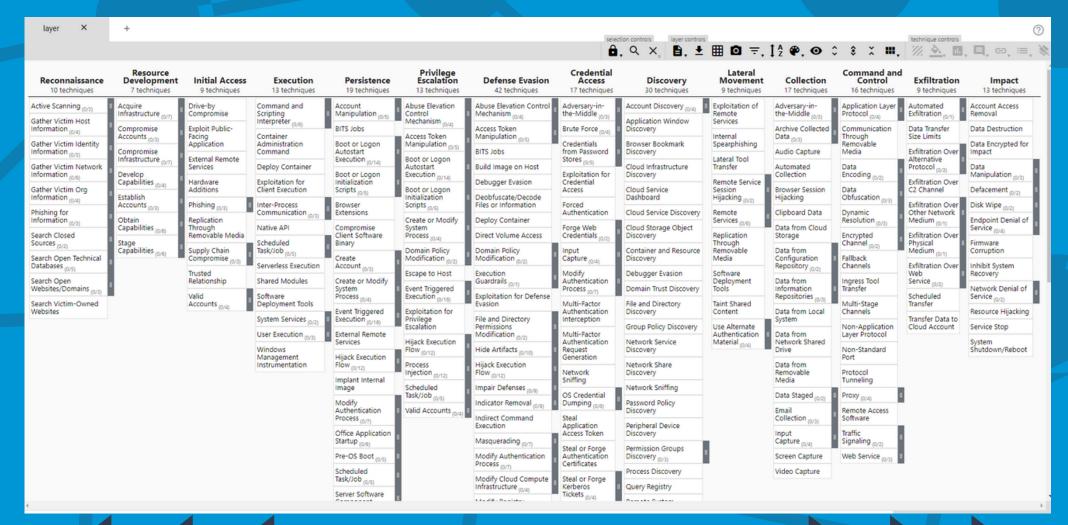
Exfiltración

TA0040

Impacto

Mitre ATT&CK Navigator Disponible versión web totalmente funcional y gratuita.

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





¿PARA QUÉ USAR MITRE ATT&CK?

- Mapeo de controles defensivos
- Búsqueda de amenazas
- Actores de referencia (APT)
- Modelado de ataques (Red Team)

ENLACES Y RECURSOS

Web oficial. Toda la información y acceso a los recursos disponibles de sus base de conocimiento

https://attack.mitre.org/

MITRE ATT&CK"	Matrices Ta	actics * Techniques *	Data Sources	Mitigations *	Groups	Software Ca	ampaigns f	Resources *	Blog ♂	Contribute	Search Q
		ATT&CK v12 is no	ow live! Check out to	he updates here							
	MITRE ATT&CK® is a globally-accessible tactics and techniques based on real-with knowledge base is used as a foundation threat models and methodologies in the plant of the cybersecurity product and service of the cybersecurity product and service of the cybersecurity product and service of the cybersecurity, ATT&CK, MITRE is problems for a safer world — by bringing more effective cybersecurity, ATT&CK is of organization for use at no charge. Getting Started Contribute	rorld observations. The All for the development of significant of the development	TT&CK pecific nt, and solve evelop	Tweets by MITR	Eattack						
	FAQ	Random Page 🔻									
		ATT&CK № layout: side • show		Enterprise							
Reconnaissance Resource Initial A	ccess Execution Persistence	Privilege Defens Escalation	se Evasion Cr	edential Access	Discovery	Lateral Movement	Collection	Command Control	and Exfilt	tration	Impact



ENLACES Y RECURSOS

MITRE ATT&CK Navigator. Aplicación web que nos permite el diseño de matrices personalizadas, exportación y otras posibilidades

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

	MITRE ATT&CK® Navigator	
It can	ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices, in be used to visualize defensive coverage, red/blue team planning, the frequency of cted techniques, and more. help changelog theme •	
Create New Layer	Create a new empty layer	,
Open Existing Layer	Load a layer from your computer or a URL	
Create Layer from other layers	Choose layers to inherit properties from	





Gracias por tu tiempo!

¿Conocías MITRE ATT&CK?

Comparte, comenta o etiqueta a quién pueda serle de interés



