1. Ciberataque: Cyber Kill Chain

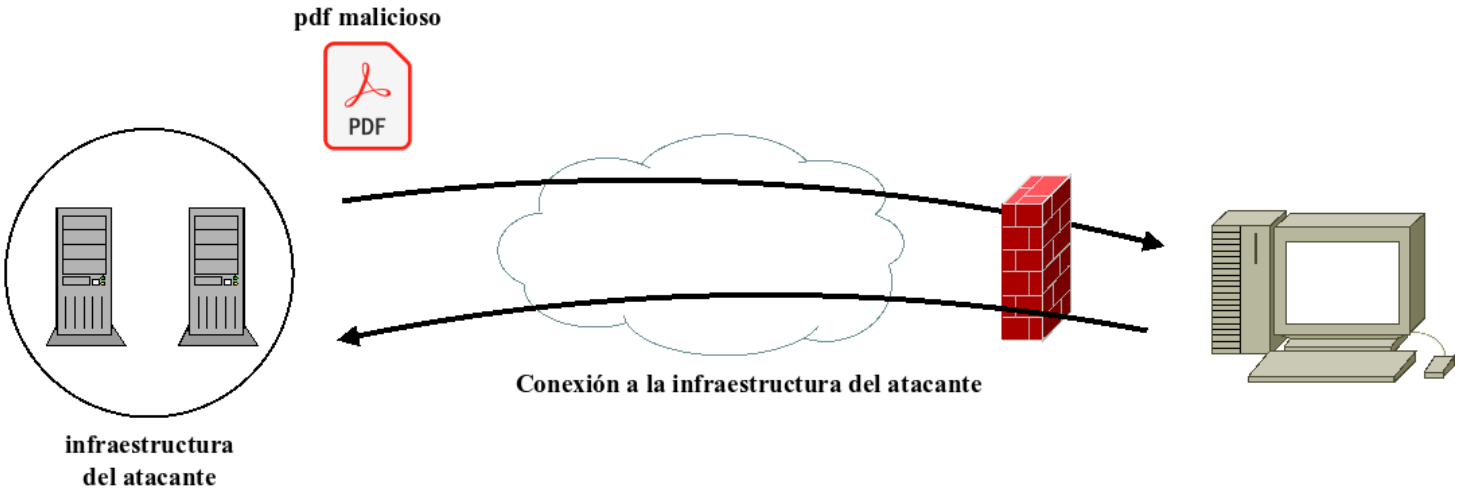
La *Cyber Kill Chain* es la adaptación hecha por Lockheed Martin Corporation al mundo de seguridad de la información del concepto de *Kill Chain* militar (identificación del objetivo, decisión y orden de ataque y finalmente destrucción del objetivo).

En ella se describen los pasos a seguir por un adversario o actor malicioso para lanzar un ciberataque a un objetivo y es especialmente buena para representar un escenario de ransomware o APT (Advanced Persistent Threats):

1. *Reconnaissance* (Reconocimiento)
   - Se recopila información sobre el objetivo usando fuentes abiertas (OSINT), whois, dns, network scanning, port scanning, enumeración de servicios, ...
   - En esta fase se busca obtener toda la información posible del objetivo como ubicaciones, presencia web (dominios, hosting, ...), empleados, direcciones de email, servidores (dns, web, correo, ftp, ...), topología de red, tecnologías empleadas, bloques de direcciones IP, ...
2. *Weaponization* (Preparación/Armamento)
   - En base al análisis de la información recopilada en la fase anterior, se prepara el ataque contra el objetivo.

- Dependiendo del tipo de objetivo se escogen las herramientas a usar, por ejemplo:
  - se puede crear un documento de Office con una macro maliciosa o VBA scripts para remitir por email a un determinado usuario
  - se puede crear un payload malicioso en un pendrive que luego se distribuirá.
  - se puede preparar un exploit para aprovechar una vulnerabilidad de un sistema como la MS17-010 que permite la ejecución remota de código.

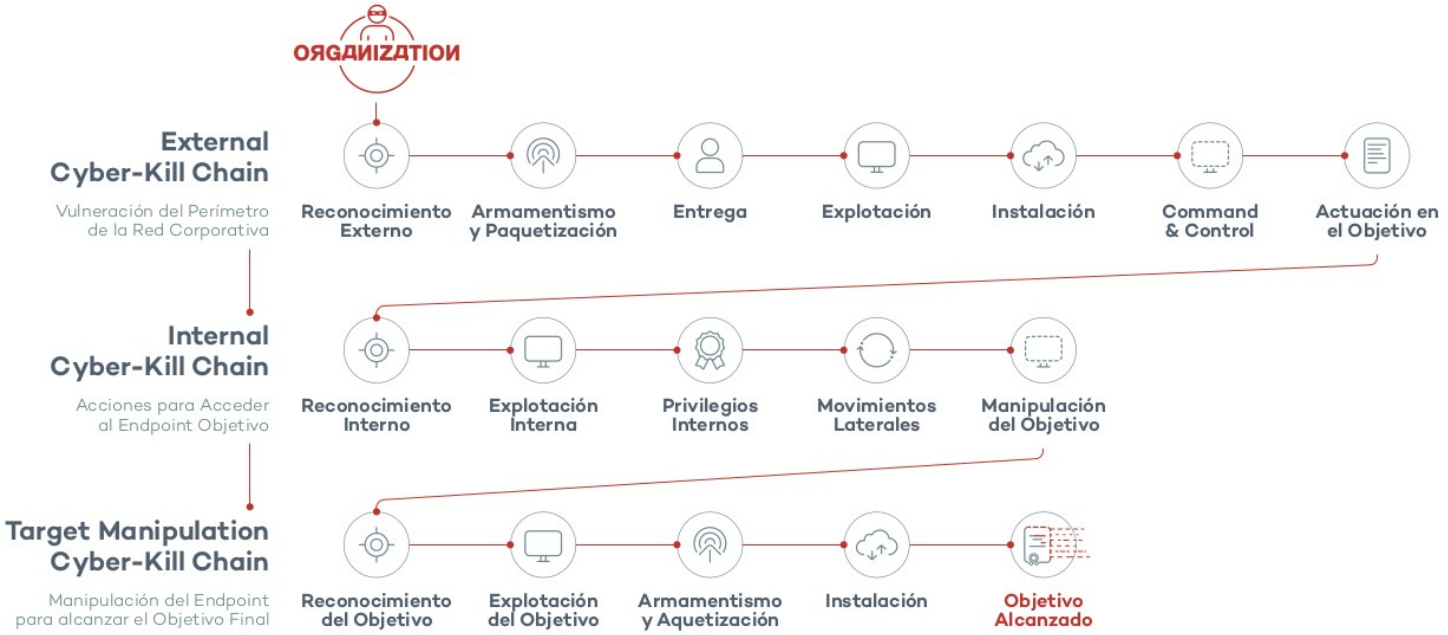
3. *Delivery* (Distribución/Entrega)
   - Se produce la transmisión del ataque; por ejemplo creando y enviando un email con el documento malicioso adjunto o con un enlace al documento para que el destinatario pinche en él y lo descargue.
   - Ejemplos:
     - phishing emails.
     - distribución de pendrives infectados.
     - *watering hole attack* donde se compromete un sitio web que visitan habitulamente los objetivos y cuando lo visitan se les redirige a un sitio malicioso controlado por el atacante.
4. *Exploitation* (Explotación)
   - Es el momento en el que se aprovecha una vulnerabilidad del sistema objetivo para asaltarlo. El resultado puede ser por ejemplo que se envía una *shell* a un equipo del atacante, desde la que podrá ejecutar comandos.



5. *Installation* (Instalación)
   - En esta fase se busca la permanencia en el equipo atacado vía registro, tareas programadas, ..., para garantizar acceso futuros. Se suben/instalan más herramientas para tener vías alternativas de acceso y parar continuar el proceso.
   - Ejemplos para conseguir la persistencia:
     - instalación de *web shells*.
     - instalación de puertas traseras (*backdoors*).
     - creación/modificación de servicios Windows.
     - añadir entradas en el registro de Windows o en las carpetas de arranque.
     - crear cuentas de usuario.
6. *Command & Control* (C2, C&C, Mando y control)
   - A través de canales C2 se controlan los sistemas atacados y en función del objetivo perseguido se les puede dar instrucciones para llevar acciones como ataques DoS o exfiltración de documentos.
   - Mediante canales dns (*dns tunneling*), icmp, sitios web, redes sociales, ..., se envían órdenes al equipo comprometido para indicarle qué hacer.
7. *Actions on objectives* (Acciones sobre objetivos)
   - En función de los objetivos del atacante se puede exfiltrar información, dañar activos, identificar nuevos objetivos internos de la organización y expandirse, ...

Una vez alcanzado el último paso y afectado un equipo dentro de la organización, el proceso se puede repetir para con más reconocimientos y movimientos laterales en el interior de la organización. Aunque la Cyber Kill Chain se representa como una línea hay que verla como un **proceso cíclico**.

El hecho de estar dentro de una organización hace que los privilegios y las posibilidades de acceso a los recursos sea diferente que desde el exterior, por lo que el atacante puede usar nuevas técnicas y procedimientos. Esto ha hecho que algunas organización trabajen con versiones ampliadas de la Cyber Kill Chain:



2. Mitre ATT&CK

MITRE presentó en 2013 ATT&CK (*Adversarial Tactics, Techniques and Common Knowledge*) que viene siendo una base de datos con información sobre tácticas y técnicas conocidas que usan los grupos de atacantes cuando están perpetrando una intrusión contra plataformas concretas (p.e. windows, linux, ...).

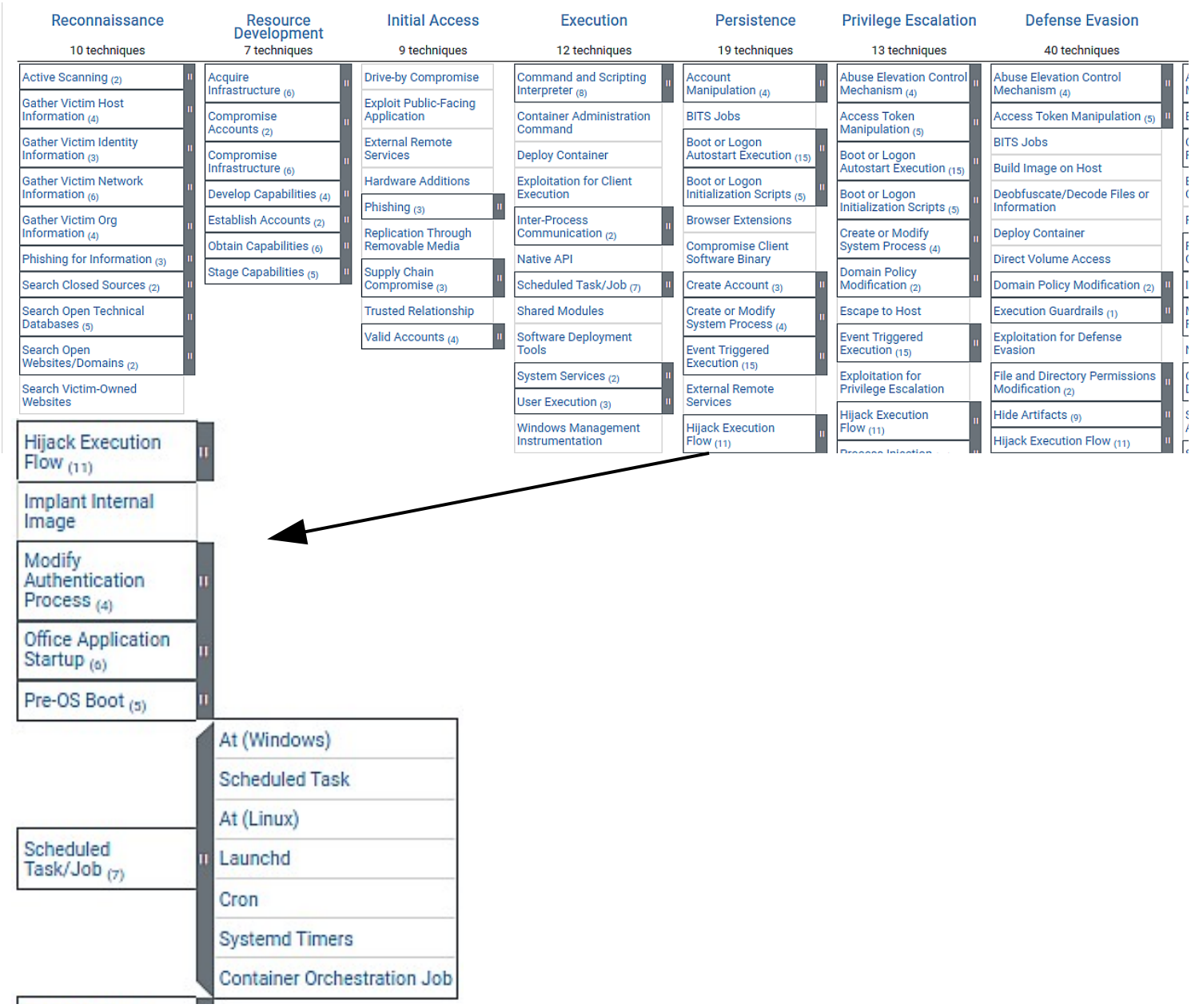
ATT&CK tiene algunos aspectos que lo hacen muy interesante y cada vez más presente en la industria:

- **Comportamiento del adversario**: se centra en tácticas y técnicas usadas por los atacantes y no en indicadores como direcciones IP, nombres de archivo, herramientas, ..., que pueden cambiar fácilmente.
- **Aplicable a entornos reales**: las tácticas, técnicas y procedimientos (TTP) que recoge ATT&CK están basadas en incidentes observados y medibles.
- **Taxonomía común**: las TTP deben ser comparables entre diferentes tipos de grupos de adversarios utilizando la misma terminología.

Para ATT&CK:

- Las **tácticas** son *el qué* está tratando de conseguir un adversario en un momento dado de la intrusión. Es el objetivo del atacante para desarrollar una acción; por ejemplo, lograr la persistencia en un equipo.
- Las **técnicas** son *el cómo* se logra el objetivo. Por ejemplo, para lograr la persistencia se aprovecha la funcionalidad del sistema operativo de tareas programas.

Cómo hay muchas formas (técnicas) de que el atacante logre sus objetivos tácticos, hay múltiples técnicas en cada categoría táctica. Por ejemplo, bajo la táctica Persistencia (*Persistence*) aparecen 19 técnicas que a su vez pueden tener subcategorías:



Para facilitar el uso de todo esta información MITRE ha creado tres matrices:

- ATT&CK Enterprise: centrada en el comportamiento de los adversario en entornos Windows, Linux, Mac, Cloud (Office 365, Azure, ...) y entornos de red..
- ATT&CK Mobile: para entornos Android e IOS.
- ATT&CK ICS (Indutrial Control Systems): para entornos industriales.

En la ATT&CK Enterprise se han definido las siguientes categorías (*tácticas*):

1. *Reconnaissance*: trata de recopilar información sobre la organización para futuras acciones.

2. *Resource Development*: preparación de recursos para dar soporte a las operaciones, como comprar de dominios, alquiler de VPS, ...

3. *Initial Access*: el adversario trata de entrar en la red, por ejemplo usando *spear phishing*, cuentas predeterminadas, ...

4. *Execution:* trata de ejecutar código malicioso, por ejemplo comandos o scripts linux o powershell, ...

5. *Persistence*: trata de mantenerse en el sistemas, por ejemplo con tareas programadas, creando cuentas de usuario, ...

6. *Privilege Escalation*: trata de obtener más privilegios en el sistema, por ejemplo aprovechando malas configuraciones o vulnerabilidades.

7. *Defense Evasion*: intenta evitar ser detectado, por ejemplo desactivando software de seguridad, ofuscando ficheros, ...

8. *Credential Access*: trata de robar credenciales como usuario/contraseña, por ejemplo mediante keylogging o sniffing.

9. *Discovery*: trata de descubrir el entorno, por ejemplo analizando los recursos compartidos, sniffing, ...

10. *Lateral Movement*: el adversario trata de moverse a través de tu organización, por ejemplo usando credenciales legítimas para acceder a otros sistemas, ...

11. *Collection*: recopilar información que le pueda servir para sus intereses, por ejemplo accediendo a audios, vídeos, emails, ...

12. *Command and Control*: trata de comunicarse con los sistemas comprometidos para controlarlos, por ejemplo usando túneles ICMP, ...

13. *Exfiltration*: trata de robar información, por ejemplo subiéndola a una cuenta en la nube, ...

14. *Impact*: trata de manipular, interrumpir o destruir sistemas e información, por ejemplo modificando la página web de la empresa (*defacement*), cifrando la información (ransomware), ..

Además podremos acceder a información sobre mecanismos de mitigación y detección así como a datos de los grupos de adversarios (APT29, APT37, ...).

Hay dos diferencias fundamentales entre Mitre ATT&CK y la Cyber Kill Chain de Lockheed Martin:

- ATT&CK profundiza en cómo se desarrolla cada etapa del ataque especificando tácticas y técnicas.
- ATT&CK se actualiza regularmente en base a los nuevos incidentes informados desde las empresas, de forma que los defensores pueden conocer las últimas tácticas/técnicas y herramientas empleadas por los adversarios. Esta actualización es especialmente relevante en sectores no contemplados originalmente por la Cyber Kill Chain como los entornos Cloud (donde acciones como el envío de malware no es tan relevante y que es uno de los pilares de la Cyber Kill Chain).