¿Los ataques modernos son secuenciales?

Por: Xenia Vasquez

Contenido

Resumen

¿Los ataques siguen realmente una receta lineal?

Existen marcos como MITRE ATT&CK o Cyber Kill Chain que describen tácticas, técnicas y etapas utilizadas por actores maliciosos. Sin embargo, en un entorno operativo los ataques rara vez ocurren de forma rígida o cronológica.

La realidad es mucho más dinámica: los atacantes cambian de estrategia, regresan a etapas anteriores, aprovechan errores humanos y adaptan sus movimientos según las respuestas defensivas del entorno.

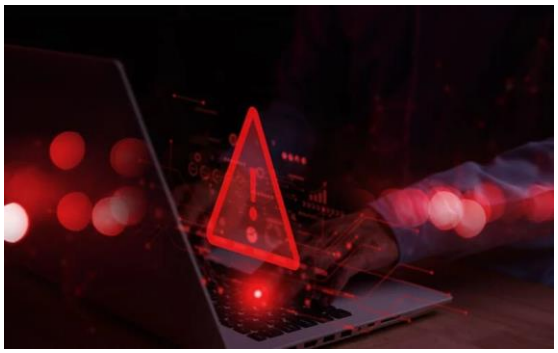
En este artículo abordaremos cómo se comportan realmente los ataques desde una perspectiva operativa, por qué el factor humano continúa siendo uno de los vectores más explotados y por qué los incidentes rara vez siguen una línea recta.

Introducción: La contradicción de la linealidad

En muchos entrenamientos de ciberseguridad, los ataques se presentan como procesos lineales y ordenados. Frameworks como MITRE ATT&CK o Cyber Kill Chain ayudan a estructurar el entendimiento de los ataques, pero generan una percepción errónea: que los actores maliciosos siguen rutas predecibles y lineales.

Sin embargo, la realidad operativa es distinta. Los ataques reales son caóticos, adaptativos, disruptivos y frecuentemente no lineales.

Por eso evitar sesgos de linealidad resulta fundamental para detectar y contener ataques antes de que alcancen etapas críticas.



Partimos entonces de una premisa fundamental: si un actor malicioso busca evitar la detección, ¿por qué seguiría un proceso estrictamente lineal que podría delatar su comportamiento de forma inmediata?

Los frameworks modelan comportamiento, no cronologías

Mitre ATT&CK

¿Qué es en realidad Mitre att&ck? De forma estricta es una base de conocimiento que cataloga TTPs (Tácticas, Técnicas y Procedimientos), que utilizan delincuentes cibernéticos durante la vida de un ciberataque, las tácticas van desde reconocimiento hasta impactó y de ahí se desprenden múltiples técnicas como: obtener credenciales, fuerza bruta, exfiltración automatizada, entre otras; esta herramienta de uso libre nos permite comprender un poco más sobre cómo actúan los atacantes, podemos ver de diferentes forma la página: lineal, por departamento, mostrando u ocultando la subtecnica, eso puede generar la siguiente duda: ¿Los atacantes deben seguir el orden descrito en la base de conocimiento?

La respuesta corta es no.

MITRE ATT&CK como vimos no fue diseñado como una línea temporal estricta ni como un flujo obligatorio de ejecución. Su propósito principal es catalogar y organizar comportamientos observados en ataques reales para facilitar el análisis, la detección y la comprensión de las TTPs.

Cyber Kill Chain

Este frameworks se trata de una serie de pasos que pueden seguir los ciberdelincuentes para ejecutar un ataque; a diferencia de Mitre ATT&CK este marco si nos muestra los pasos en serie que puede seguir un ataque, este modelos nos dice que un ataque no es un evento aislado sino pasos conectados; este modelo se compone de siete pasos:

1. Reconocimiento: Recopilación de información sobre el objetivo de ataque.

2. Armado: Preparación de malware, a menudo vinculando exploits a archivos o enlaces maliciosos.

3. Entrega: Envío de la carga útil, normalmente se dispersa por phishing de correos electrónicos o descargas drive-by.

4. Explotación: El código malicioso se ejecuta en el sistema de destino.

5. Instalación: El malware establece persistencia.

6. Comando y control (C2): Los atacantes se comunican con el sistema comprometido para emitir comandos.

7. Acciones sobre objetivos: Logran su objetivo, ya sea robando datos, cifrando archivos o interrumpiendo servicios. (Clay, 2026)

Al descomponer un ataque en tácticas y etapas, este tipo de marcos permite comprender mejor el comportamiento adversario e identificar en qué punto puede intervenir un equipo defensivo.

Sin embargo, es importante entender que frameworks como MITRE ATT&CK y Cyber Kill Chain no representan una secuencia rígida de ejecución. Con la evolución de las tecnologías, la automatización y las técnicas de evasión, los ataques modernos han dejado de comportarse como procesos estrictamente lineales.

Estos modelos deben entenderse como una base conceptual para analizar intrusiones, no como una receta exacta que un atacante seguirá paso a paso.

El atacante en un entorno real

En entornos reales, un ciberatacante rara vez opera siguiendo una secuencia rígida o exacta. Sus acciones y decisiones normalmente dependen del contexto y brechas que puedan encontrar durante su ejecución.

Sus ataques tienden a adaptarse continuamente para evitar ser detectados y maximizar su probabilidad de éxito.

Podemos observar incidentes reales dentro de organizaciones que aparentan estar seguras.

Por ejemplo, un proveedor de servicios de atención al cliente de una gran corporación, con controles de seguridad limitados y poca capacitación al personal recibe un correo aparentemente legítimo, proveniente de un proveedor con el que interactúa cotidianamente.

Un empleado abre el mensaje, interactúa con el enlace y, en cuestión de segundos, su cuenta corporativa queda comprometida. A partir de ese momento, el atacante comienza a enviar cientos de correos internos desde una identidad legítima, propagándose rápidamente hacia líderes, áreas administrativas y otros usuarios de confianza dentro de la organización.

Desde una perspectiva teórica, podríamos intentar mapear el incidente dentro de un framework lineal: reconocimiento, entrega, explotación, persistencia, movimiento lateral y acciones sobre el objetivo. Sin embargo, en la práctica, muchas de estas etapas ocurren de forma simultánea, implícita o incluso imperceptible para el equipo defensivo.

El ataque aparenta “saltar” directamente desde la entrega inicial hasta la propagación y el impacto operativo. Entonces surge una pregunta importante: ¿qué ocurrió con el resto de las etapas?

La respuesta es que no desaparecieron; simplemente ocurrieron de manera dinámica, automatizada o empalmadas entre sí. El atacante no necesita respetar una secuencia visible para alcanzar sus objetivos.

El riesgo de la linealidad

Asumir que todos los ataques siguen una secuencia ordenada y predecible puede generar sesgos operativos dentro de los equipos. Cuando los analistas esperan observar un flujo “correcto” de etapas, existe el riesgo de ignorar comportamientos que no encajan dentro de esa narrativa lineal.

En un entorno real, los atacantes no necesariamente avanzan paso a paso. Pueden repetir técnicas, cambiar de estrategia, abandonar tácticas, volver a fases de reconocimiento o ejecutar múltiples acciones simultáneamente. Sin embargo, muchos procesos de detección continúan construidos bajo la expectativa de progresiones lineales y rígidas.

Por ejemplo, un posible Command and Control (C2) podría ser descartado porque previamente no se detectó reconocimiento, explotación o acceso inicial. Bajo una lógica lineal, el analista espera observar una secuencia completa antes de validar el incidente.

Sin embargo, como hemos mencionado en entornos reales, la ausencia de evidencia no representa necesariamente ausencia de compromiso.

El acceso inicial pudo ocurrir días antes, fuera del alcance de monitoreo, mediante credenciales válidas, dispositivos no supervisados o técnicas que lograron evadir los controles defensivos. Aun así, el comportamiento observado en etapas posteriores puede continuar siendo legítimamente malicioso.

Finalmente el problema no es utilizar frameworks como MITRE ATT&CK, sino convertirlos inconscientemente en expectativas cronológicas rígidas que sólo acrecientan el riesgo de descartar señales críticas simplemente porque no encajan dentro de la narrativa esperada del ataque.

Conclusión

Los ataques modernos no deben entenderse como una secuencia rígida de eventos, sino como un proceso adaptativo y dinámico. Cada decisión tomada por un atacante depende del entorno comprometido, de las oportunidades descubiertas durante la intrusión y demás contextos.

Frameworks como MITRE ATT&CK y Cyber Kill Chain continúan siendo herramientas fundamentales para comprender y clasificar comportamientos de adversarios. Sin embargo, su verdadero valor no radica en describir una

cronología exacta del ataque, sino en proporcionar una estructura común para analizar tácticas y técnicas observadas en incidentes reales.

El problema aparece cuando estos modelos son interpretados como rutas estrictamente secuenciales. En entornos operativos, los ataques pueden acelerarse, retroceder, mutar o ejecutar múltiples acciones simultáneamente. Bajo esta realidad, los sesgos de linealidad pueden convertirse en puntos ciegos defensivos que afectan la capacidad de detección y respuesta de los equipos de seguridad.

Comprender que un ataque no necesita “verse completo y lineal” para ser real es fundamental para construir una defensa más crítica, flexible y alineada con la naturaleza cambiante de las amenazas modernas.

Bibliografía

1. ¿Qué es el marco MITRE ATT&CK? (2026, febrero 19). Ibm.com. https://www.ibm.com/mx-es/think/topics/mitre-attack
2. MITRE ATT&CK®. (s/f). Mitre.org. Recuperado el 14 de mayo de 2026, de https://attack.mitre.org/
3. ¿Qué es la Cyber Kill Chain? (s/f). Trend Micro. Recuperado el 15 de mayo de 2026, de https://www.trendmicro.com/es_es/what-is/cyber-attack/cyber-kill-chain.html
4. What is the cyber kill chain? (s/f). Microsoft.com. Recuperado el 15 de mayo de 2026, de https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain