Cyber Kill Chain Ataque y Defensa

Arévalo Cuevas, Edwin Javier
edwin-arevalo1@upc.edu.co
Universidad Piloto de Colombia

Resumen **- Las actuales formas de ataques cibernéticos sofisticados y dirigidos pretenden evadir los sistemas de detección de intrusos, lo que resulta en uno de los mayores desafíos que enfrentan los profesionales de la seguridad. La Cyber Kill Chain es un concepto diseñado para entender y combatir las amenazas cibernéticas de manera efectiva. Fue desarrollado como una forma de estructurar y visualizar el proceso que los atacantes siguen para comprometer un sistema o red. En términos simples es una cadena de ataque, el camino que toma un intruso para penetrar los sistemas de información a lo largo del tiempo y ejecutar un ataque contra el objetivo. Pero al mostrar las fases ofensivas también se pretende desarrollar capacidades de respuesta y análisis de incidentes. Este documento describe las metodologías, técnicas y herramientas involucradas en los ataques cibernéticos y sus opciones de defensa.**

Índice de Términos **– Ataque, defensa, ciberseguridad, Cyber Kill Chain, metodología.**

Abstract **- Current forms of sophisticated and targeted cyberattacks attempt to evade intrusion detection systems, resulting in one of the biggest challenges facing security professionals. The Cyber Kill Chain is a concept developed to understand and combat cyber threats effectively. It was developed as a way to structure and visualize the process attackers follow to compromise a system or network. In simple terms it is an attack chain, the path an intruder takes to penetrate information systems over time to execute an attack against the target. But by showing the offensive phases it is also intended to develop incident response and analysis capabilities. This document describes the methodologies, techniques and tools involved in cyber attacks and some defense options.**

Key Words **– Attack, defense, cybersecurity, Cyber Kill Chain, methodology.**

I. INTRODUCCIÓN

En la era digital en la que vivimos, la seguridad cibernética se ha convertido en una preocupación siempre presente. Las organizaciones, ya sean empresas o gobiernos, se enfrentan a amenazas cada vez más sofisticadas que buscan comprometer su infraestructura, robar información valiosa y causar estragos en sus operaciones. Ante este panorama, los profesionales y en general los encargados de la seguridad de la información deben conocer los diversos marcos y metodologías desarrolladas que permiten comprender cómo funciona el proceso del ataque cibernético lo cual resulta fundamental para poder defendernos de manera efectiva.

Es aquí donde entra en juego la Cyber Kill Chain, uno de los enfoques más reconocidos y utilizados en la industria de la seguridad informática. Esta metodología, desarrollada por Lockheed Martin, proporciona una visión detallada de las etapas que un ciberataque suele seguir, desde la etapa inicial de reconocimiento hasta la fase final de extracción o secuestro de datos sensibles o la interrupción de servicios. El desglosar el proceso en pasos claramente definidos, permite a los expertos en ciberseguridad identificar las vulnerabilidades y contrarrestar los ataques en cada una de estas etapas. Cada fase de la cadena de ataque cibernético representa un paso crucial en la ejecución exitosa de un ciberataque [1].

En este artículo, exploraremos en profundidad la Cyber Kill Chain y analizaremos cada una de sus fases. Desde el primer paso de reconocimiento hasta la fase de acción final, examinaremos cómo los actores maliciosos aprovechan las debilidades de seguridad y despliegan tácticas ingeniosas para infiltrarse en el sistema objetivo. Al comprender el modus operandi de los ciberdelincuentes, podremos fortalecer nuestras defensas y mitigar los riesgos asociados a los ataques cibernéticos.

A lo largo del texto, también abordaremos las mejores prácticas de defensa y las contramedidas recomendadas que pueden ayudar a las organizaciones a protegerse contra este tipo de ataques de seguridad en cada una de sus fases. Desde la implementación de firewalls y sistemas de detección de intrusiones hasta la concienciación del personal y la adopción de políticas de seguridad sólidas, examinaremos las medidas clave que deben tomarse para salvaguardar la integridad de los sistemas y la información sensible.

En última instancia, el objetivo es proporcionar una visión clara y completa de este modelo, destacando su importancia en la lucha contra las amenazas cibernéticas y proporcionando a los lectores las herramientas necesarias para fortalecer su postura en materia de seguridad. Al estar preparados y comprender cómo se desarrollan los ataques cibernéticos, podremos estar un paso adelante de los ciberdelincuentes, proteger nuestros activos digitales y navegar con confianza en el siempre cambiante paisaje de la seguridad cibernética.

II. QUÉ ES CYBER KILL CHAIN

Cyber Kill Chain es un concepto utilizado en seguridad informática para describir las etapas de un ataque cibernético. Fue desarrollado por Lockheed Martin en el 2011 como parte de su programa de defensa cibernética y se utiliza ampliamente en la industria.para comprender y contrarrestar las amenazas cibernéticas de manera efectiva.

El término "Kill Chain" se deriva de la jerga militar y se refiere a una secuencia de pasos que llevan al éxito de una misión o a la "muerte" del objetivo. En el contexto de la ciberseguridad, la Cyber Kill Chain describe las etapas que un atacante típicamente atraviesa para llevar a cabo un ataque exitoso. El modelo identifica lo que los adversarios deben completar para lograr su objetivo, detenerlos en cualquier etapa rompe la cadena de ataque [2].

Comprender estas etapas es fundamental para la ciberseguridad, ya que permite a los equipos de defensa anticiparse a las acciones de los atacantes y tomar medidas para prevenir, detectar o mitigar los ataques en cada etapa. Al comprender cómo funciona la Cyber Kill Chain, las organizaciones pueden implementar medidas de seguridad en cada fase para fortalecer su postura defensiva y mitigar los riesgos asociados con los ataques cibernéticos. Los adversarios deben progresar completamente a través de todas las fases para tener éxito.

Y visto desde los atacantes, una nueva clase de amenaza aparece, denominada apropiadamente como "Amenaza persistente avanzada" APT, la cual presenta adversarios capacitados y con recursos suficientes que llevan a cabo campañas de intrusión de largo tiempo dirigidas a información económica, de propiedad o de seguridad altamente confidencial. Estos adversarios logran sus objetivos utilizando herramientas y técnicas avanzadas diseñadas para derrotar a la mayoría de los mecanismos de defensa de redes informáticas convencionales [3].

Pero las técnicas de defensa de la red que aprovechan el conocimiento sobre estos adversarios pueden crear un ciclo de retroalimentación de inteligencia, lo que permite a los defensores bien preparados establecer un estado de superioridad sobre la información y esto disminuye la probabilidad de éxito del adversario con cada intento de intrusión posterior.

El modelo de la Cyber Kill Chain es una herramienta valiosa para comprender las tácticas utilizadas por los ciberdelincuentes y desarrollar estrategias de seguridad efectivas.

III. EL MODELO

El modelo de Cyber Kill Chain está compuesto por las siguientes siete etapas:

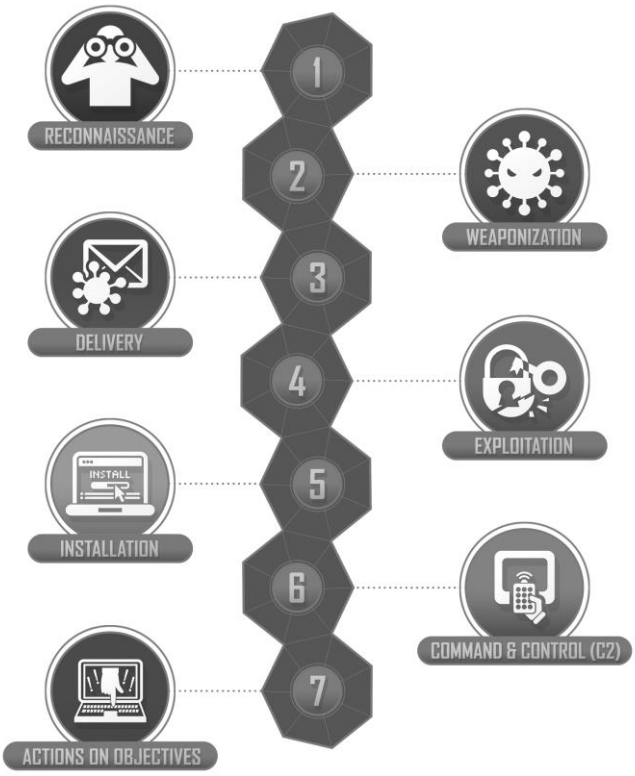

Fig.1 Modelo Cyber Kill Chain.
Fuente Lockheed Martin

A. Reconocimiento

Ataque

En esta fase, los atacantes recopilan información sobre su objetivo, buscan identificar posibles vulnerabilidades y puntos débiles en los sistemas de la organización objetivo. Durante la fase de reconocimiento, los atacantes pueden llevar a cabo varias actividades, como la recopilación de información pública, la exploración de redes sociales y la búsqueda de información sobre empleados y socios comerciales [4]. El objetivo es obtener la mayor cantidad de información posible sobre la organización objetivo, incluyendo detalles sobre su infraestructura, empleados, proveedores, socios y sistemas técnicos. Algunas técnicas comunes utilizadas en esta fase incluyen:

1. Búsqueda de información pública: Los atacantes pueden utilizar motores de búsqueda y herramientas de recopilación de información para buscar detalles sobre la

organización objetivo, como direcciones de correo electrónico, números de teléfono, nombres de empleados y detalles de contacto.
2. Escaneo de puertos y servicios: Los atacantes pueden utilizar herramientas de escaneo de puertos para identificar los servicios y sistemas expuestos en la infraestructura de la organización objetivo. Esto les permite tener una idea de qué servicios están disponibles y pueden ser atacados.
3. Enumeración de sistemas: Los atacantes pueden utilizar técnicas de enumeración para recopilar información adicional sobre los sistemas de la organización objetivo, como nombres de hosts, direcciones IP y nombres de dominio.
4. Sondeo de redes sociales: Los atacantes pueden buscar perfiles en redes sociales para obtener información sobre empleados y socios comerciales. Esta información puede ser utilizada para realizar ataques de ingeniería social más adelante en la cadena de ataque.
5. Recopilación de información de infraestructura: Los atacantes pueden buscar información sobre los proveedores de servicios de la organización objetivo, como registros DNS y datos WHOIS, para comprender mejor la arquitectura de la red y buscar posibles puntos de entrada.

Defensa

Detectar el reconocimiento en el momento en que sucede puede ser muy difícil, pero cuando los defensores descubren el reconocimiento, incluso mucho después del hecho, puede revelar la intención de los adversarios. Es esencial implementar medidas de seguridad adecuadas para detectar y prevenir actividades de reconocimiento. Algunas prácticas recomendadas incluyen:

1. Educación y concienciación: Los empleados deben recibir capacitación regular sobre las amenazas de seguridad esto incluye, técnicas de ingeniería social, cómo reconocer correos electrónicos de phishing, cómo manejar archivos adjuntos y enlaces sospechosos y cómo informar actividades inusuales. Lo que se busca es reducir la posibilidad de que se realicen acciones maliciosas. que faciliten la ejecución de herramientas en fases posteriores.
2. Monitoreo de red: Utilizar sistemas de detección y prevención de intrusiones (IDS/IPS) y soluciones de monitoreo de seguridad para identificar actividades de escaneo y enumeración en la red.
3. Actualizaciones y parches: Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas, esto ayuda a prevenir el uso de exploits y reduce la superficie de ataque.
4. Control de acceso: Implementar políticas de acceso sólidas y autenticación multifactorial para proteger los sistemas y datos sensibles.
5. Seguridad en capas: Es recomendable utilizar soluciones de seguridad en múltiples capas para aumentar las defensas. Esto incluye el uso de antivirus/antimalware, firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de anomalías, sistemas de protección de correo electrónico y filtrado de contenido web. Estas soluciones pueden ayudar a detectar y bloquear el malware antes de que se ejecute en los sistemas para proteger la infraestructura de la organización.

Es importante destacar que la fase de reconocimiento no implica necesariamente una intrusión en los sistemas de la organización objetivo. Su objetivo principal es recopilar información para las etapas posteriores de la cadena de ataque. Sin embargo, esta información recopilada durante el reconocimiento puede ser utilizada para diseñar y llevar a cabo ataques más efectivos en etapas posteriores. La detección temprana de actividades de reconocimiento puede ayudar a prevenir ataques más avanzados en las etapas posteriores de la cadena del ataque cibernético.

B. Armamento

Ataque

La fase de armamento se refiere al proceso en el que se desarrollan y preparan los elementos necesarios para crear y distribuir una carga útil (payload) maliciosa. Durante esta fase, los atacantes pueden utilizar diferentes técnicas para diseñar y construir el malware o la herramienta maliciosa que se utilizará para comprometer el sistema objetivo. Esto puede incluir la creación de exploits, la manipulación de archivos o documentos, el desarrollo de código malicioso o la modificación de herramientas existentes. Un armador "weaponizer" combina malware y exploit en una carga útil entregable.

Algunas de las técnicas comunes utilizadas durante esta fase son las siguientes:

1. Desarrollo de malware: Los atacantes pueden utilizar diferentes lenguajes de programación para desarrollar malware personalizado que se adapte a sus objetivos específicos. Esto implica la creación de código malicioso que pueda ser ejecutado en el sistema objetivo y realizar las acciones deseadas, como robar información, tomar el control del sistema, etc.
2. Ofuscación y encriptación: Para evitar la detección por parte de los sistemas de seguridad, los atacantes pueden utilizar técnicas de ofuscación y encriptación para ocultar el malware. Estas técnicas pueden incluir el uso de herramientas específicas que alteran el código del malware de tal manera que sea más difícil de detectar, como el empaquetamiento, ocultamiento del código fuente o la encriptación de la carga útil.
3. Ingeniería social: La ingeniería social es una técnica

comúnmente utilizada en la fase de armamento, donde los atacantes intentan manipular a los usuarios para que realicen acciones que faciliten la ejecución del malware. Esto puede incluir el envío de correos electrónicos de phishing convincentes, la creación de sitios web falsos o la explotación de la confianza de los usuarios para engañarlos y hacer que descarguen o ejecuten el malware.
4. Exploits y vulnerabilidades: Los atacantes también pueden aprovechar vulnerabilidades conocidas en el software o el sistema operativo objetivo para desarrollar exploits. Estos exploits permiten aprovechar las debilidades del sistema y ejecutar el malware de forma remota o local. Los atacantes pueden descubrir o adquirir exploits existentes o incluso desarrollar sus propios exploits personalizados para atacar vulnerabilidades específicas.

Una vez que se ha creado la carga útil maliciosa, el atacante buscará métodos para ocultarla y asegurarse de que pase desapercibida por los sistemas de seguridad y las defensas del objetivo como antivirus y otros sistemas de seguridad.

Defensa

Esta es una fase esencial que los defensores deben entender. Aunque no pueden detectar el uso de armas en el momento en que ocurre, pueden inferir mediante el análisis de artefactos de malware. Adicional a las descritas en la primera fase, se pueden implementar las siguientes medidas de seguridad:

1. Filtrado y control de contenido web: Implementar soluciones de filtrado y control de contenido web puede ayudar a prevenir la descarga de malware o acceso a sitios web maliciosos. Estas soluciones bloquean el acceso a dominios conocidos por ser maliciosos o sospechosos y pueden ayudar a evitar que los usuarios accedan involuntariamente a fuentes de infección.
2. Análisis de archivos adjuntos y enlaces: Se deben implementar soluciones de análisis de seguridad para escanear y analizar los archivos adjuntos de correo electrónico y los enlaces en busca de amenazas conocidas. Esto puede ayudar a identificar archivos o enlaces maliciosos antes de que se abran o hagan clic, evitando así la ejecución de malware.
3. Supervisión de tráfico de red: Monitorear el tráfico de red y utilizar soluciones de detección de intrusiones (IDS) e inteligencia de amenazas puede ayudar a identificar actividades sospechosas y comportamientos maliciosos. Esto permite detectar y bloquear posibles intentos de infiltración y distribución de malware.
4. Análisis de comportamiento y anomalías: Implementar soluciones de detección de anomalías y análisis de comportamiento puede ayudar a identificar patrones de actividad maliciosa en los sistemas. Estas soluciones utilizan modelos y algoritmos avanzados para detectar comportamientos inusuales o anómalos en tiempo real, lo que puede indicar una posible actividad de armamento.
5. Control de aplicaciones y privilegios: Implementar políticas de control de aplicaciones y privilegios para limitar la capacidad de los atacantes para ejecutar software no autorizado o malicioso en los sistemas. Restringir los privilegios de los usuarios y emplear mecanismos de autenticación sólidos también puede dificultar la ejecución exitosa de malware en esta fase.

Las defensas eficaces contra el armamento requieren una combinación de medidas técnicas y de concienciación para identificar y mitigar las amenazas antes de que se materialicen.

C. Entrega

Ataque

Se refiere al proceso mediante el cual un atacante introduce un malware o una carga útil maliciosa en el sistema objetivo. Durante esta fase, el atacante utiliza diversas técnicas para entregar el malware al sistema objetivo. Algunas de las técnicas comunes utilizadas en esta etapa son:

1. Phishing: El atacante puede enviar correos electrónicos fraudulentos que parecen legítimos y engañan a los usuarios para que abran adjuntos maliciosos o hagan clic en enlaces que descargan el malware.
2. Descargas maliciosas: Los atacantes pueden aprovechar vulnerabilidades en sitios web legítimos o comprometerlos para entregar malware a los visitantes sin su conocimiento.
3. Dispositivos de almacenamiento extraíbles: Los atacantes pueden utilizar dispositivos USB u otros medios extraíbles para entregar malware a través de la conexión física con el sistema objetivo.
4. Exploits y kits de explotación: Los atacantes pueden utilizar exploits de vulnerabilidades conocidas en el software o sistemas operativos para entregar malware.
5. Ingeniería social: El atacante puede utilizar tácticas de manipulación psicológica para convencer a los usuarios de que descarguen o ejecuten el malware de forma voluntaria.

Defensa

Crucial para prevenir un ataque exitoso, esta es la primera y más importante oportunidad para que los defensores bloqueen la operación. Una medida clave de la eficacia es la fracción de intentos de intrusión que se bloquean en la etapa de entrega. Aquí hay algunas medidas de defensa que se pueden implementar en esta fase:

1. Concienciación sobre la seguridad: Comprender los servidores de destino y personas, sus roles y responsabilidades, qué información está disponible. Los empleados y usuarios deben recibir educación sobre las

técnicas de entrega de malware, el reconocimiento de correos electrónicos de phishing, la descarga de archivos de fuentes no confiables y otras prácticas seguras. Esto ayuda a prevenir que el malware sea entregado en primer lugar.
2. Filtrado de contenido y correos electrónicos: Implementar soluciones de filtrado de contenido y correos electrónicos puede ayudar a identificar y bloquear correos electrónicos maliciosos o sitios web comprometidos que podrían entregar malware. Estas soluciones pueden detectar y bloquear enlaces, archivos adjuntos y contenido malicioso conocido.
3. Actualizaciones y parches de software: Mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad ayuda a mitigar las vulnerabilidades conocidas que los atacantes podrían aprovechar para entregar malware.
4. Recopile registros web y de correo electrónico para reconstrucción forense. Incluso si una intrusión se detecta tarde, los defensores deben poder determinar cuándo y cómo comenzó la entrega.
5. Análisis de comportamiento y reputación: Utilizar soluciones de seguridad que empleen análisis de comportamiento y reputación puede ayudar a detectar y bloquear actividades maliciosas en tiempo real. Estas soluciones analizan el comportamiento de los archivos y las actividades de red para identificar posibles amenazas.
6. Control de dispositivos y políticas de seguridad: Establecer políticas de seguridad y control de dispositivos puede ayudar a prevenir la entrega de malware a través de medios extraíbles, como unidades USB. Limitar o controlar el acceso a dispositivos externos puede reducir el riesgo de infección.

D. Explotación

Ataque

Implica el uso de una vulnerabilidad o debilidad descubierta en el sistema objetivo para ejecutar código malicioso o tomar control del sistema. El atacante aprovecha las vulnerabilidades encontradas en el sistema para lograr sus objetivos. Algunos ejemplos de técnicas de explotación comunes incluyen:

1. Explotación de vulnerabilidades conocidas: Los atacantes pueden utilizar vulnerabilidades previamente identificadas y documentadas en sistemas, aplicaciones o software para obtener acceso no autorizado. Estas vulnerabilidades pueden ser causadas por errores de programación, configuraciones incorrectas o falta de actualizaciones de seguridad.
2. Explotación de día cero: En algunos casos, los atacantes pueden aprovechar vulnerabilidades desconocidas o recién descubiertas en sistemas que aún no se han parcheado. Estas vulnerabilidades son llamadas "día cero" y pueden ser especialmente peligrosas, ya que no hay una solución o parche disponible en el momento del ataque.
3. Inyección de código: Los atacantes pueden aprovechar vulnerabilidades como la inyección de SQL o la inyección de comandos para insertar código malicioso en sistemas o aplicaciones. Esto les permite ejecutar comandos y manipular el comportamiento del sistema según sus intenciones.
4. Explotación de debilidades en la autenticación: Los atacantes pueden utilizar técnicas como el "password cracking" (romper contraseñas), el "brute-forcing" (fuerza bruta) o el robo de credenciales para obtener acceso no autorizado a sistemas protegidos por autenticación.
5. Elevación de privilegios: Si un atacante ha obtenido acceso inicial con privilegios limitados, la fase de explotación puede implicar la búsqueda de formas de elevar los privilegios para obtener un mayor control sobre el sistema comprometido.

Defensa

En términos de defensa, esta fase es crucial para implementar medidas que puedan mitigar los intentos de explotación y reducir el impacto de un ataque. Aquí, las medidas de refuerzo tradicionales agregan resiliencia, pero las capacidades personalizadas son necesarias para detener las vulnerabilidades de día cero. Algunas estrategias y medidas de defensa que se pueden implementar son:

1. Mantener los sistemas actualizados: Es fundamental mantener el software, sistemas operativos y aplicaciones al día con los últimos parches de seguridad. Las actualizaciones suelen incluir correcciones para vulnerabilidades conocidas, lo que reduce la posibilidad de que un atacante pueda aprovecharlas.
2. Aplicar configuraciones seguras: Configurar los sistemas y las aplicaciones con medidas de seguridad adecuadas puede ayudar a prevenir o dificultar la explotación. Esto puede incluir el uso de contraseñas seguras, la limitación de privilegios de usuario y la implementación de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS).
3. Utilizar soluciones de seguridad avanzadas: Implementar soluciones de seguridad, como antivirus, antimalware, soluciones de gestión de vulnerabilidades y sistemas de detección de intrusos, puede ayudar a identificar y bloquear intentos de explotación.
4. Realizar pruebas de penetración: Las pruebas de penetración, o pen tests, son evaluaciones controladas de la seguridad de los sistemas. Estas pruebas simulan los métodos y técnicas que un atacante podría utilizar, identificando las vulnerabilidades y debilidades que necesitan ser corregidas.
5. Monitoreo y análisis de registros de seguridad: El monitoreo constante de los registros de seguridad puede ayudar a identificar actividades sospechosas o intentos de explotación. El análisis de estos registros puede ayudar a detectar patrones o anomalías que puedan indicar una

intrusión en curso.
6. Implementar segmentación de red: Dividir la red en segmentos más pequeños y restringir el tráfico entre ellos puede ayudar a limitar el movimiento lateral de un atacante en caso de una explotación exitosa.

E. Instalación

Ataque

En esta fase el atacante implanta y configura el malware o software malicioso en el sistema comprometido, por lo general, los adversarios instalan una puerta trasera persistente o un implante en el entorno de la víctima para mantener el acceso durante un período de tiempo prolongado. Durante la fase de instalación, se puede llevar a cabo una serie de acciones, tales como:

1. Descarga o inyección de malware: El atacante puede descargar archivos maliciosos desde una ubicación externa e introducirlos en el sistema comprometido. También puede inyectar código malicioso en aplicaciones o sistemas existentes.
2. Ejecución de archivos maliciosos: El atacante ejecuta los archivos maliciosos en el sistema comprometido para iniciar el proceso de infección. Estos archivos pueden incluir troyanos, ransomware, keyloggers u otros tipos de malware.
3. Configuración de puertas traseras (backdoors): El atacante puede crear puertas traseras en el sistema comprometido, lo que le permite mantener acceso remoto al sistema en el futuro, incluso si se toman medidas para mitigar el ataque inicial.
4. Manipulación de configuraciones: El atacante puede modificar la configuración del sistema comprometido para permitir el acceso no autorizado o alterar su funcionamiento normal. Esto puede incluir la creación de nuevas cuentas de usuario, la modificación de permisos o la desactivación de controles de seguridad para asegurar persistencia en el sistema.

Defensa

Implica implementar medidas para detectar y prevenir la instalación exitosa de malware u otros componentes maliciosos en el sistema objetivo. La idea es interrumpir o dificultar el avance del atacante en el ciclo de ataque. Algunas estrategias y prácticas defensivas que se pueden emplear son:

1. Seguridad del perímetro: Implementar soluciones de seguridad perimetral, como firewalls y sistemas de prevención de intrusiones (IPS), para bloquear o monitorear el tráfico de red sospechoso y prevenir que el malware ingrese a la red o se propague.
2. Filtros de contenido: Utilizar filtros de contenido web y de correo electrónico para bloquear mensajes o sitios web maliciosos, reduciendo la posibilidad de que los usuarios interactúen con enlaces o archivos que puedan conducir a la instalación de malware.
3. Actualizaciones y parches: Mantener los sistemas y aplicaciones actualizados con los últimos parches y actualizaciones de seguridad para mitigar las vulnerabilidades conocidas que podrían ser aprovechadas por los atacantes durante la fase de instalación.
4. Soluciones de seguridad en endpoints: Utilizar software de seguridad en los endpoints, como soluciones antivirus, antimalware y de detección y respuesta de endpoints (EDR), para bloquear la ejecución de archivos o programas maliciosos en los sistemas de usuario.
5. Supervisión y detección de anomalías: Implementar sistemas de monitorización y análisis de logs que permitan detectar comportamientos anómalos en el tráfico de red, actividades de usuarios y eventos del sistema, lo cual puede indicar la presencia de actividades de instalación de malware.
6. Segmentación de red: Dividir la red en segmentos aislados, utilizando firewalls y políticas de acceso adecuadas, para limitar la propagación del malware en caso de una intrusión exitosa.

F. Comando y Control C2

Ataque

Durante la fase de C2, el atacante busca establecer una infraestructura de comunicación encubierta para poder enviar comandos, recibir datos e interactuar con los sistemas comprometidos sin ser detectado. El objetivo principal de esta fase es permitir al atacante mantener un control constante sobre los sistemas comprometidos, y poder realizar acciones maliciosas adicionales, como extraer datos, distribuir malware adicional o llevar a cabo actividades de espionaje cibernético. Algunas de las técnicas comunes utilizadas en la fase de C2:

1. Uso de servidores de comando y control (C&C): El atacante puede utilizar servidores comprometidos o controlados por ellos para establecer una comunicación encubierta con los sistemas comprometidos. Estos servidores actúan como intermediarios para enviar comandos y recibir datos de los sistemas infectados.
2. Uso de protocolos no estándar: En lugar de utilizar los protocolos de red estándar, el atacante puede emplear protocolos personalizados o poco comunes para establecer comunicación con los sistemas comprometidos. Esto dificulta la detección y el bloqueo de las comunicaciones maliciosas.
3. Técnicas de encriptación: El atacante puede utilizar técnicas de encriptación para ocultar las comunicaciones y evitar su detección. La encriptación puede aplicarse tanto a los comandos enviados como a los datos recibidos de los sistemas comprometidos.
4. Uso de proxy y túneles: Se pueden utilizar para redirigir y

enmascarar las comunicaciones entre el atacante y los sistemas comprometidos. Estas técnicas ayudan a ocultar la verdadera ubicación del atacante y dificultan la identificación y bloqueo de las comunicaciones maliciosas.
5. Uso de DNS (Domain Name System): El atacante puede utilizar consultas DNS para establecer comunicación y enviar comandos a los sistemas comprometidos. Esto puede implicar el uso de nombres de dominio registrados por el atacante o la manipulación del sistema DNS de la víctima.
6. Uso de canales encubiertos: Se pueden utilizar técnicas de ocultamiento, como el uso de archivos de imágenes o archivos de audio, para ocultar comandos y datos dentro de archivos aparentemente benignos. Estos canales encubiertos permiten al atacante evadir la detección y mantener la comunicación con los sistemas comprometidos.
7. Uso de malware persistente: El atacante puede utilizar malware persistente, como rootkits o troyanos de acceso remoto (RAT), para mantener un control constante sobre los sistemas comprometidos. Estos tipos de malware permiten al atacante establecer una conexión remota y enviar comandos de forma continua.

Defensa

La última mejor oportunidad del defensor para bloquear la operación es obstruyendo el canal C2. Si los adversarios no pueden dar órdenes, los defensores pueden evitar el impacto. Algunas técnicas comunes de defensa utilizadas para contrarrestar la fase de C2:

1. Monitorización del tráfico de red: Se puede implementar un monitoreo constante del tráfico de red para identificar patrones y comunicaciones sospechosas. Esto implica el uso de herramientas de análisis de tráfico y la creación de perfiles de comportamiento de red normal para detectar anomalías.
2. Análisis de comportamiento de sistemas: El análisis del comportamiento de los sistemas puede ayudar a identificar actividades anómalas o maliciosas. Se pueden implementar soluciones de seguridad que supervisen y alerten sobre comportamientos inusuales, como cambios en los archivos del sistema, modificaciones de registros o actividades de red no autorizadas.
3. Lista de control de acceso (ACL): Las ACL permiten controlar y filtrar el tráfico de red permitido y bloquear conexiones a dominios o direcciones IP conocidos de servidores de comando y control (C&C). Esto ayuda a prevenir la comunicación con fuentes maliciosas y a bloquear el acceso a infraestructuras de C&C conocidas.
4. Análisis de reputación de IP y dominios: Se pueden utilizar servicios y bases de datos de reputación de IP y dominios para evaluar la confiabilidad y la reputación de las comunicaciones. Esto ayuda a identificar conexiones a fuentes maliciosas conocidas y a bloquear o restringir el acceso a esas fuentes.
5. Implementación de detección de amenazas: Utilizar soluciones de detección de amenazas basadas en firmas, heurísticas y técnicas de análisis de comportamiento puede ayudar a identificar y bloquear actividades maliciosas en la fase de C2. Estas soluciones pueden identificar patrones y comportamientos asociados con ataques de C&C.
6. Compartir información y colaboración: La colaboración con otras organizaciones de seguridad y la participación en grupos de intercambio de información sobre amenazas pueden ayudar a obtener inteligencia sobre nuevas técnicas y herramientas utilizadas en la fase de C2. Esto permite una respuesta más rápida y efectiva ante los ataques.
7. Actualizaciones y parches: Mantener los sistemas actualizados con los últimos parches y actualizaciones de seguridad ayuda a cerrar posibles brechas de seguridad utilizadas por los atacantes en la fase de C2. Esto reduce las oportunidades para que los atacantes establezcan comunicaciones y control sobre los sistemas.

G. *Acciones sobre objetivos*

Ataque

La fase de acciones sobre objetivos, también conocida como la última fase de la cadena de ataque cibernético (Cyber Kill Chain), es donde el atacante logra su objetivo final, que puede variar según el tipo de ataque y los motivos del atacante. Esta fase se produce después de que el atacante ha atravesado todas las etapas anteriores de la cadena, desde la identificación del objetivo hasta la explotación de vulnerabilidades y el acceso a sistemas o datos sensibles. El atacante busca alcanzar los resultados deseados mediante una serie de acciones. Estas acciones pueden incluir:

1. Recopilación de datos: El atacante puede recopilar más información sobre el objetivo, como datos personales, credenciales de acceso, información financiera o cualquier otro dato relevante para su objetivo final.
2. Extracción o secuestro de datos: El atacante puede intentar extraer o encriptar información o datos sensibles de los sistemas comprometidos. Esto puede implicar la transferencia de datos a servidores controlados por el atacante o el uso de técnicas encubiertas para enviar datos fuera de la red comprometida.
3. Manipulación de datos: En algunos casos, el atacante puede modificar o manipular datos dentro de los sistemas comprometidos para lograr su objetivo. Esto podría implicar alterar registros, cambiar configuraciones o realizar cambios sutiles que puedan tener un impacto significativo.
4. Destrucción de datos: En ciertos ataques, el objetivo del atacante puede ser eliminar o dañar permanentemente datos o sistemas. Esto puede hacerse mediante la

eliminación de archivos críticos, la corrupción de bases de datos o la interrupción de servicios esenciales.

5. Persistencia: El atacante puede tomar medidas para mantener el acceso a los sistemas comprometidos incluso después de que se haya detectado y mitigado la amenaza inicial. Esto puede incluir la creación de puertas traseras, la instalación de malware persistente o la explotación de otras vulnerabilidades desconocidas.

Defensa

Todas las acciones que se toman para detener y mitigar el ataque en curso. Esto implica una respuesta rápida y coordinada, que incluye la interrupción de la comunicación con el atacante, el aislamiento de sistemas comprometidos y la eliminación del malware. Los equipos de respuesta a incidentes deben estar preparados y contar con planes de acción claros para minimizar el tiempo de respuesta. Algunas acciones de respuesta a las acciones sobre objetivos son:

1. Respuesta a incidentes: Establezca un equipo de respuesta a incidentes de seguridad (CSIRT) dedicado y bien entrenado para abordar los incidentes de seguridad en tiempo real. El equipo debe tener planes de acción claros y predefinidos para responder rápidamente a los ataques en curso, incluida la contención del incidente, la eliminación del malware y la restauración de los sistemas afectados.
2. Aislamiento de sistemas comprometidos: Si se detecta una intrusión, es importante aislar los sistemas comprometidos de la red principal para evitar que el atacante se propague y cause más daño. Esto se puede lograr desconectando los sistemas comprometidos de la red o utilizando tecnologías de aislamiento como segmentación de red o contenedores.
3. Limpieza de sistemas afectados mediante el escaneo y eliminación de malware, actualización de software y parches de seguridad, y restauración desde copias de seguridad confiables.
4. Captura de paquetes de red para recrear la actividad, realizar evaluación de daños con expertos, detectar exfiltración de datos, usos de credenciales y movimientos no autorizados.
5. Análisis de registros y registros de auditoría: Realice un análisis detallado de los registros de eventos y registros de auditoría generados por los sistemas y aplicaciones de la organización. Esto puede ayudar a identificar actividades maliciosas, patrones de tráfico sospechosos y anomalías en el comportamiento del sistema.
6. Análisis forense: Realice un análisis forense exhaustivo para determinar el alcance del compromiso, identificar la causa raíz y recopilar pruebas para futuras acciones legales. El análisis forense puede ayudar a comprender las tácticas, técnicas y procedimientos utilizados por el atacante, así como a fortalecer las defensas de seguridad para evitar futuros ataques similares.

IV. CONCLUSIONES

El modelo de la Cyber Kill Chain proporciona una estructura útil para comprender las etapas de un ataque y desarrollar estrategias de prevención y detección temprana. Al comprender cómo los atacantes operan, las organizaciones pueden implementar medidas de seguridad más efectivas para evitar que los ataques tengan éxito o detectarlos rápidamente cuando ocurren.

Se destaca la importancia de tomar medidas proactivas para defenderse contra los ciberataques. En lugar de centrarse únicamente en la respuesta a incidentes después de que un ataque haya ocurrido, las organizaciones pueden utilizar el modelo para anticiparse a las etapas del ataque y tomar medidas para prevenirlo.

Cyber Kill Chain resalta la importancia de educar y concienciar a los usuarios sobre las tácticas utilizadas por los atacantes. Al comprender cómo los ciberdelincuentes aprovechan las vulnerabilidades y cómo se propagan dentro de una red, los usuarios pueden tomar precauciones adecuadas, como no hacer clic en enlaces sospechosos o descargar archivos adjuntos no confiables.

También se muestra que los ataques cibernéticos no son eventos aislados, sino procesos complejos que involucran múltiples etapas. Para hacer frente a estos ataques de manera efectiva, es crucial implementar una estrategia de seguridad integral que aborde cada una de las etapas. Esto puede incluir la implementación de medidas de seguridad en capas, como firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, autenticación multifactor, cifrado y políticas de seguridad robustas.

REFERENCES

[1] "Exploring the Cyber Kill Chain Model" por SANS Institute: https://www.sans.org/reading-room/whitepapers/analyst/exploring-cyber-kill-chain-model-36612

[2] "Introducing the Cyber Kill Chain" por Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[3] "Understanding the Cyber Kill Chain for Effective Threat Hunting" por MITRE: https://attack.mitre.org/docs/Cyber_Kill_Chain.pdf

[4] "The 7 Phases of the Cyber Kill Chain" por FireEye: https://www.fireeye.com/current-threats/what-is-the-cyber-kill-chain.html

[5] "Anatomy of an Attack: Understanding the Seven Phases of Advanced Persistent Threats" por Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/anatomy-of-an-attack-understanding-the-seven-phases-of-apt

[6] "Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics" por Yuri Diogenes y Erdal Ozkaya

[7] "The Practice of Network Security Monitoring: Understanding Incident Detection and Response" por Richard Bejtlich

[8] "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" por Dafydd Stuttard y Marcus Pinto