Entendiendo los Ciber-Ataques

Parte I. “The Cyber-Kill Chain”, la secuencia de acciones en un ataque.

Adaptive Defense

pandasecurity.com/intelligence-platform/

Índice de Contenidos.

1. Introducción.

La siempre cambiante realidad de las amenazas de seguridad, y de la frecuencia, sofisticación y naturaleza de los adversarios, requieren que las prácticas operacionales de ciberseguridad combinen perfectamente **prevención, detección y respuesta** a ciber-ataques.

La mayoría de las organizaciones disponen de los medios para detectar ataques conocidos, aunque ya son muy pocos de este tipo los que ocurren todavía. Lo que es históricamente difícil de detener, son los ataques desconocidos. Ataques específicamente diseñados para superar cualquier tipo de protección preventiva cambiando firmas y patrones de comportamiento. Otras organizaciones han realizado grandes inversiones en la creación de su propio equipo de "cazadores" de amenazas y/o delegando en proveedores de servicios gestionados la inevitable y crítica tarea de evolucionar continuamente sus técnicas de defensa, en la búsqueda de mejores herramientas y mecanismos para mantener su propiedad intelectual y activos digitales seguros.

El grado de comprensión de cómo funcionan tus adversarios y cómo tu mapa de estrategias de defensa se alinea con el ciclo de vida de los ciber-atacantes, muestra la capacidad de tu organización para detectar, detener, interrumpir y recuperarse de un ataque y qué operaciones de seguridad necesitan ser reforzadas.

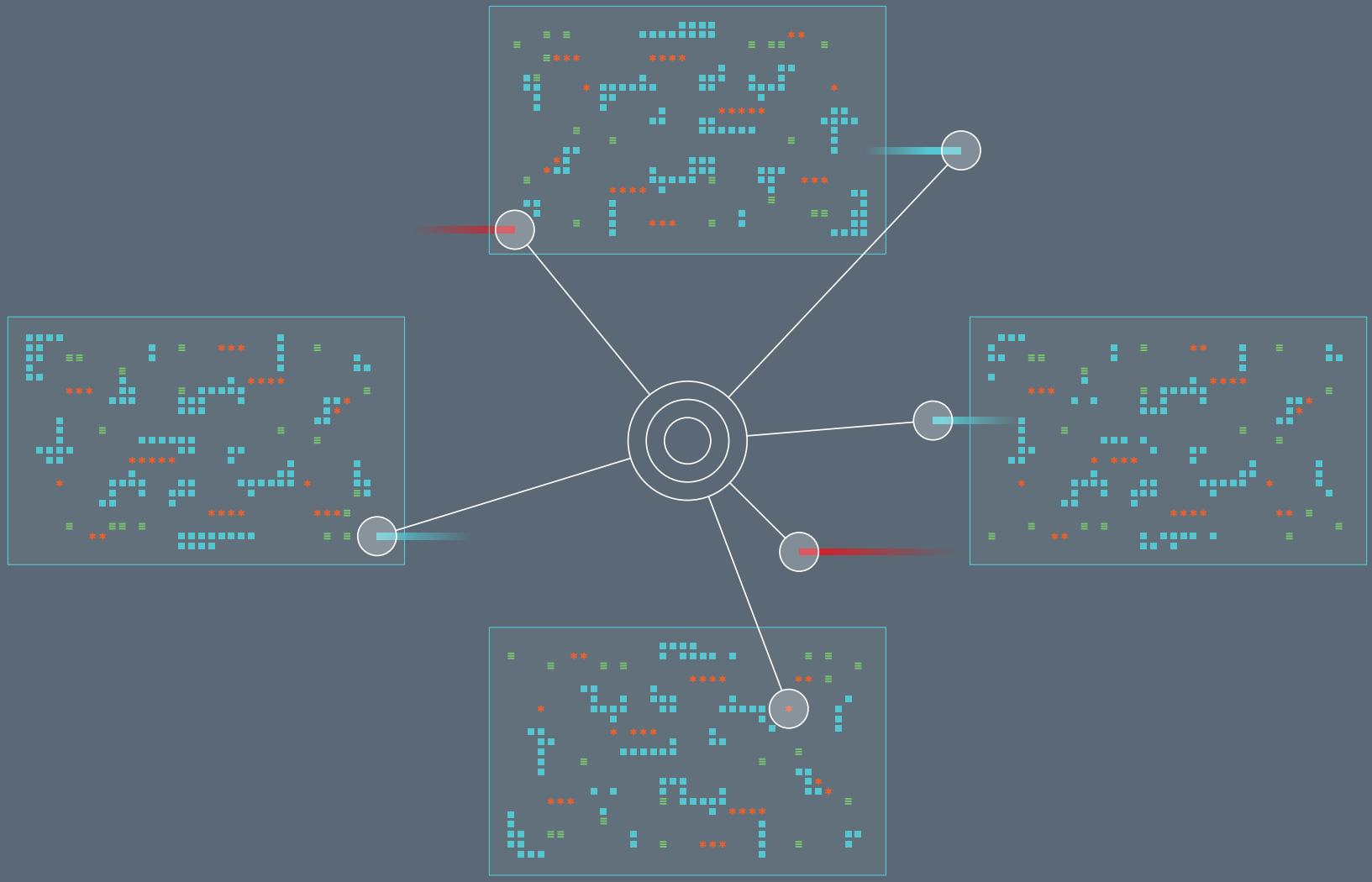
Este informe tiene como objetivo ayudar a los equipos de seguridad a entender el conocido modelo de ciclo de vida de los ciber-ataques denominado Cyber-Kill Chain y su extensión a toda la red, así como a explicar cómo Panda Adaptive Defense cubre todo el ciclo de vida en los puestos de trabajo y servidores.

Esta secuencia de acciones, denominada en la industria la Cyber-Kill Chain, y su extensión, es una excelente herramienta para entender cómo las organizaciones pueden aumentar significativamente sus capacidades de defensa detectando y bloqueando las amenazas en cada fase del ciclo de vida de los ataques. La Cyber-Kill Chain nos explica cómo mientras los adversarios deben progresar completamente a través de todas las fases de la cadena para su éxito, nosotros necesitamos "sólo" detener la cadena en cualquier paso del proceso para romper el ataque.

Los activos más valiosos de la compañía, en ocasiones sin control, se encuentran en los puestos de trabajo y servidores. De ahí que se hayan convertido en el objetivo de los atacantes. Y por eso, detener a los adversarios en los equipos y servidores, disminuye drásticamente la probabilidad de éxito del ciber-atacante. Además, se simplifican así los esfuerzos para romper la cadena y aumenta la eficiencia y eficacia de los equipos de seguridad.

Panda Adaptive Defense ayuda a todas estas organizaciones, y a sus equipos de operaciones de seguridad internos o externos, a mejorar su capacidad de **prevenir, detectar y responder a las amenazas en todo el ciclo de vida del ciber-ataque en los puestos de trabajo y servidores**.

Es un servicio gestionado que además, **proporciona información y visibilidad de los atacantes e inteligencia de seguridad**, incrementando así el conocimiento de tus adversarios para mejorar tus mecanismos de defensa.



2. Entendiendo la Cyber-Kill Chain.

El framework de la Cyber-Kill Chain, fue publicado originalmente por Lockheed Martin como parte del modelo de Intelligent Driven Defense[1] para la identificación y prevención de la actividad de intrusiones cibernéticas.

El modelo identifica los pasos que deben completar los adversarios para alcanzar su objetivo, centrándose en la red, en la exfiltración de datos y cómo mantener la resiliencia en la organización.

Gracias a ella aprenderemos que detener a los adversarios en cualquier etapa del ataque rompe su secuencia. Los adversarios deben progresar a través de todas las fases para el éxito, nosotros los "defensores", sólo tenemos que bloquearlos en cualquier etapa.

Veremos cómo el puesto de trabajo o servidor se ha convertido en el punto por el que pasan invelitablemente todos los ataques. De ahí que, detenerlos a este nivel eleve sustancialmente la posibilidad de romper cualquier ciber-ataque. La tasa de éxito será mayor si se detienen en etapas tempranas de la cadena.

Además cada intrusión, y las huellas que deja, son una oportunidad para aprender acerca de nuestros adversarios y poder utilizar su persistencia a nuestro favor. **Una mejor comprensión de los adversarios y sus acciones permite un diseño más efectivo de la defensa.**

La Cyber-Kill Chain indica que, para llevar a cabo sus fechorías, los adversarios deben seguir siempre siete fases básicas:

Reconocimiento Externo

Esta etapa puede definirse como la selección de objetivos: identificación de los detalles de la organización, requisitos legales de su industria, información sobre la tecnología utilizada, actividad en redes sociales o listas de correo.

El adversario busca esencialmente responder a estas preguntas: "¿Qué métodos de ataque funcionarán con la mayor probabilidad de éxito?" Y de aquellos, "¿Cuáles son los más fáciles de ejecutar en términos de nuestra inversión de recursos?".

Armamentismo y Paquetización

Este tiene varias formas: explotación de aplicaciones web, software disponible o malware personalizado (descargado para su reutilización o comprado), vulnerabilidades de documentos compuestos (en formato PDF, Office u otros formatos de documento) o ataques de "abrevadero"[2].

Los ataques y su forma de acceder a la víctima se preparan de forma oportunista o muy específica sobre un objetivo.

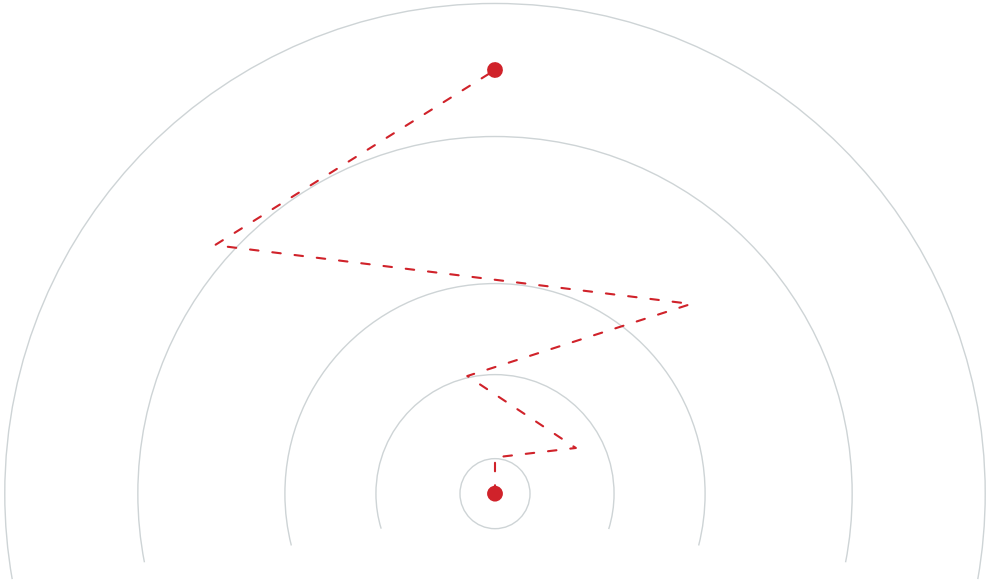
Entrega

El payload llega normalmente a la red normalmente de la mano de una acción iniciada por el usuario (por ejemplo, un usuario accede a una web maliciosa, esto llevará a la explotación de una vulnerabilidad que entrega el malware o un usuario que abre un archivo PDF malicioso) o por el propio atacante (inyección de SQL o compromiso de servicio de red).

Explotación

Después de ser entregado, el malware comprometerá el equipo o servidor, ganando así un punto de apoyo en la red. Esto suele producirse mediante la explotación de una vulnerabilidad conocida para la que normalmente ya existe parche previamente disponible.

Aunque algunos atacantes, y dependiendo del tipo de víctima, explotan vulnerabilidades de zero-day para incrementar así las probabilidades de éxito, en la mayoría de los casos no es necesario que los adversarios incurran en estos costes.



Instalación

Esto a menudo se lleva a cabo por algún elemento que comunica activamente con el exterior. El malware actúa de forma furtiva en el dispositivo, consiguiendo persistencia en los equipos donde ha conseguido entrar. El adversario puede entonces controlarlo sin alertar a la organización.

Command and Control

En esta fase, el adversario ya tiene el control absoluto de los puestos de trabajo, que actúan bajo control remoto mediante DNS, Internet Control Message Protocol, sitios web y redes sociales. El atacante utiliza esos canales para enviar órdenes al dispositivo sobre qué debe hacer y qué información ha de recopilar.

Los métodos utilizados para recopilar datos bajo un C&C incluyen capturas de pantalla, trazas, craqueo de contraseñas, inspección de la red en busca de credenciales, recopilación de contenido y documentos confidenciales. Suele identificarse un host en el que se copian todos los datos, se comprimen, se cifran y se preparan para la exfiltración.

Actuación en el Objetivo

En esta fase final, el adversario exfiltra los datos y/o daña los activos (ficheros, equipamiento) mientras permanece tiempo en la organización para identificar más objetivos, expandirse dentro de ella y -lo más crítico de todo- seguir exfiltrando datos.

La cadena se repite iterativamente. De hecho, un punto crítico de esta cadena es precisamente la característica de ser circular y no lineal. Una vez que el adversario entra en la red, vuelve al inicio de la Cadena, con más reconocimientos y movimientos laterales al interior de la red de la organización.

Si bien la metodología es la misma, los adversarios utilizan diferentes técnicas en la Cyber-Kill Chain Interna, cuando están dentro de la red; y en la Externa, para acceder a la red desde fuera.

Así, cuando el atacante se encuentra dentro de la red, se convierte en un insider: un usuario con privilegios y con persistencia. Esto impide a los equipos de seguridad de la organización sospechar del ataque y percatarse de que pueda estar en fases avanzadas del modelo extendido de la Cyber-Kill Chain.

External Cyber-Kill Chain

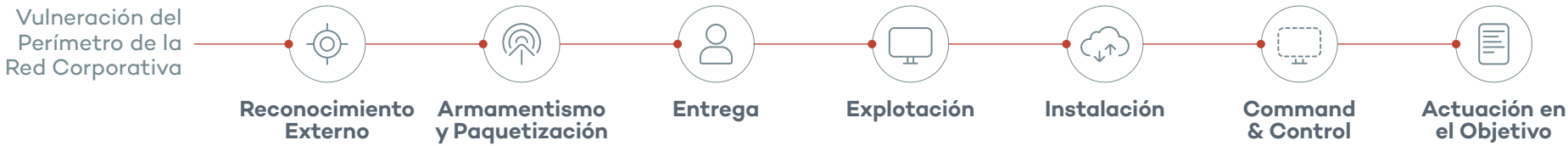


Figura 1. Diagrama de los estados en la secuencia del Cyber-Kill Chai desde el perímetro al puesto de trabajo o servidores. La secuencia externa de la Cyber-Kill Chain.

3. Versión extendida de la Cyber-Kill Chain.

La Cyber-Kill Chain es un proceso circular, no lineal, donde el adversario realiza continuos movimientos laterales dentro de la red. Las etapas que ejecuta en la red, son las mismas que utilizó cuando su objetivo era acceder a ella, aunque utiliza técnicas y tácticas distintas.

La combinación de la secuencia externa e interna de la Cyber-Kill Chain se denomina en la industria, la versión extendida de la Cyber-Kill Chain. Simplemente implica más pasos, aunque componen el mismo conjunto con las mismas etapas, pero de aplicación en el ámbito interno, por lo que se le añade la denominación “interna”: Reconocimiento Interno, Armamentismo y Paquetización Interna, Entrega Interna, etc.

Una vez dentro de la red, cada fase del ataque puede durar minutos o meses. Incluyendo el tiempo de espera durante el que el atacante se mantendrá latente esperando el momento óptimo para lanzar la última fase del ataque y conseguir el mayor impacto.

Las fases de reconocimiento y de armamentismo pueden llevar meses. Es difícil interrumpir estas fases ya que se llevan a cabo sin conexión con el atacante.

Por ello que es de vital importancia que las medidas de seguridad en los equipos de trabajo y servidores analicen y monitoricen todos los sistemas y las aplicaciones que se ejecutan en los dispositivos. De esta forma se dificulta significativamente el trabajo a los atacantes, e implicará que el ataque no sea rentable para ellos.

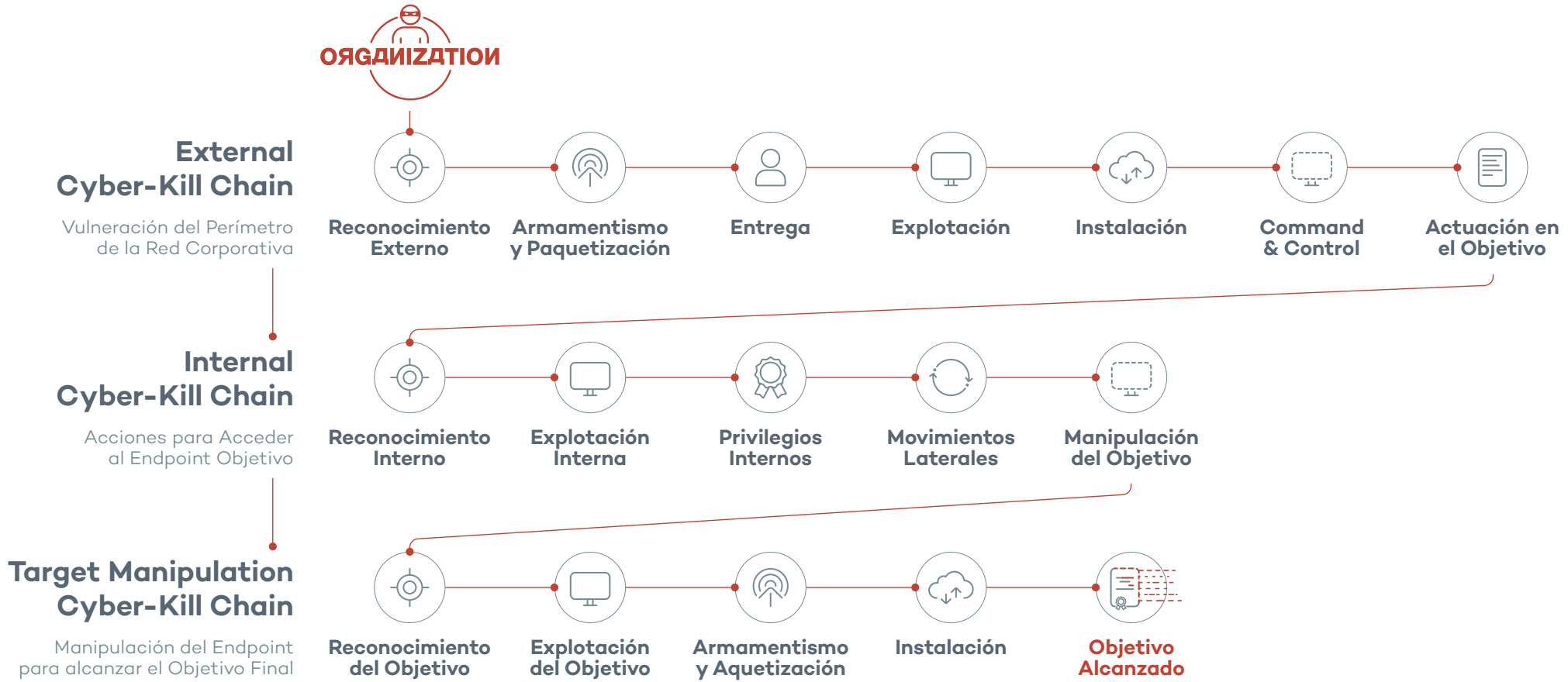
Reconocimiento Interno

En esta etapa, el atacante tiene acceso a la estación de trabajo de un solo usuario y analizará sus archivos locales, el tráfico de red, el historial del navegador y el acceso a wikis y SharePoint. El objetivo es averiguar cómo esa máquina podría ayudar a mapear la red y permitir la exfitración de activos más valiosos.

Explotación Interna

Aprovechando la ausencia de parches, vulnerabilidades de aplicaciones de navegación web, protocolos de broadcast, spoofing o incluso algo tan simple como las credenciales por defecto, los atacantes pasan de estaciones de trabajo a estación de trabajo y a los servidores mediante privilegios escalados, movimientos laterales y manipulación de equipos.

Figura 2. La Cyber-Kill Chain Extendida. Acciones para obtener acceso a los dispositivos y servidores objetivo del ataque y su manipulación por el atacante.



4. Panda Adaptive Defense en la Cyber-Kill Chain.

Los atacantes tienen metas y están dispuestos a invertir una cierta cantidad de recursos para lograrlas. Si los mecanismos de seguridad de los puestos de trabajo y servidores de toda la organización pueden aumentar el coste -ya sea monetario, de personal o de tiempo- por encima del valor que los atacantes esperan obtener, la probabilidad de éxito será menor o incluso pueden decidir no atacar a esa organización.

Todas las organizaciones tienen que estar preparadas para responder a esta pregunta: ¿Qué haría si el adversario tiene acceso a la red corporativa, a nombres de usuario y contraseñas, a toda la documentación y a especificaciones de los dispositivos, a sistemas, a copias de seguridad y a aplicaciones red y hacerlo de forma inmediata y automática?

La meta final de toda estrategia de seguridad de los puestos de trabajo y servidores de una organización debe ser construir una empresa más resistente. No es realista pensar que se prevendrán todos los ataques, pero sí que se detendrán una mayor cantidad y antes.

Uno de los objetivos es disponer de eficientes mecanismos de defensa en cada etapa de la versión extendida de la Cyber-Kill Chain para retrasar y dificultar a los atacantes. Hacer que sea más difícil y más costoso continuar y complicar lo máximo que puedan moverse de una etapa a otra. Si los atacantes no pueden lograr su objetivo de forma rentable, buscarán otros objetivos.

La estrategia de seguridad de las organizaciones debe diseñarse con un enfoque que tenga en cuenta cómo se ejecuta un ataque, desde el exterior y especialmente desde el interior. Ya que, una vez dentro de la red, los atacantes actúan como personas con acceso los dispositivos, servidores y a sus activos.

El enfoque de seguridad tradicional debe ser extendido con métodos basados en la comprensión de la Cyber-Kill Chain y proporcionar tecnologías que sean capaces de evitar que los atacantes accedan a puestos de trabajo y servidores, pero también para detenerlos en cualquier etapa de la Cyber-Kill Chain interna.

El mapeo de la estrategia de defensa al modelo de la Cyber-Kill Chain extendido demuestra cómo la organización puede prevenir, detectar, interrumpir y recuperar cualquier ataque a largo de sus fases, alineando la seguridad de la organización con los mismos criterios de éxito que los adversarios.

Esto es difícil de lograr debido a varios factores como el hecho de que las aplicaciones han aumentado exponencialmente tanto en cantidad, como en complejidad y en interconexión. Las aplicaciones son vulnerable porque la mayoría no se desarrolla bajo los principios de seguridad. Además, las personas son un vector principal de riesgo y una puerta abierta a ataques basados en ingeniería social.

Panda Adaptive Defense y Panda Adaptive Defense 360 cubren los pilares centrales que, entregados al cliente en forma de **servicio gestionado, previene y detecta las técnicas y tácticas de ataque más avanzados en cada etapa de la Cyber-Kill Chain extendida**. Ayudando así a los equipos de seguridad de las organizaciones a diseñar una estrategia de seguridad alineada a la Cyber-Kill Chain extendida.

5. Pilares de Adaptive Defense y Adaptive Defense 360.

Prevención de Malware Conocido

La búsqueda de amenazas conocidas no protege contra ataques desconocidos, pero complementado con capas de seguridad adicionales, puede detener preventivamente las amenazas conocidas cuando son entregadas en los dispositivos y servidores.

Panda Adaptive Defense 360 utiliza una amplia colección de servicios de reputación para bloquear proactivamente a los atacantes durante la fase de entrega utilizando datos de la nube.

Detección de Malware Avanzado

Panda Adaptive Defense y Panda Adaptive Defense 360 detectan y bloquean malware desconocido y ataques dirigidos, gracias a un modelo de seguridad basado en tres principios: monitorización continua en profundidad de todas las aplicaciones que se ejecutan en la red, clasificación automática de los procesos mediante técnicas de big data y machine learning en una plataforma en la nube, y análisis de comportamiento en profundidad por técnicos expertos para los ataques más complejos.

Detección Dinámica de Exploits[3]

Durante la fase de explotación de la Cyber-Kill Chain extendida, los atacantes usan exploits para aprovechar vulnerabilidades a nivel de código y poder así comprometer aplicaciones y sistemas, para instalar y ejecutar su malware.

Adaptive Defense y Adaptive Defense 360 ofrecen capacidades anti-exploits dinámicas para proteger contra ataques tanto de aplicación como de memoria. Ambas soluciones detectan y bloquean las técnicas utilizadas por los atacantes durante la fase de explotación -por ejemplo: heap spraying (pulverizar pila), stack pivots, ataques ROP y modificaciones de permisos de memoria-. Además detecta dinámicamente ataques desconocidos mediante la monitorización de todos los procesos en ejecución, y correlaciona datos a través de algoritmos de machine learning en la nube pudiendo detener cualquier intento de explotación conocido y desconocido.

Las tecnologías Anti-exploit de Adaptive Defense detendrán al adversario en las primeras etapas del ataque interno identificando cuándo una aplicación o proceso confiable está siendo comprometido.

Mitigación

Una protección de tipo Next-Generation tiene que prevenir y detectar atacantes durante las diferentes etapas de la Cyber-Kill Chain, y la detección tiene que ir seguida por una rápida mitigación de las etapas incipientes en la cadena.

Panda Adaptive Defense 360 mitiga automática y oportunamente el ataque, y pone en cuarentena al malware, para finalizar un proceso comprometido o incluso reiniciando completamente el sistema para minimizar el daño.

Remediación o Resolución

Durante la ejecución el malware a menudo crea, modifica o elimina la configuración de archivos y registros del sistema.

Estos cambios, o restos que va dejando, pueden causar inestabilidad y mal funcionamiento del sistema e incluso una puerta abierta a nuevos ataques. Panda Adaptive Defense 360 restaura los puestos de trabajo y servidores a su estado confiable previo al malware.

Forense

Dentro de la realidad cambiante de las amenazas y la frecuencia, sofisticación y naturaleza específica de los adversarios, no debería haber ninguna tecnología de seguridad que afirme ser 100% efectiva y por lo tanto es una necesidad la de disponer de herramientas o sistemas que proporcionen puntos de referencia forense en tiempo real y visibilidad.

Los equipos corporativos de ciberseguridad necesitan tener un plan establecido para manejar las notificaciones de violaciones de seguridad, ponerse en contacto con las fuerzas del orden público o gestionar adecuadamente publicidad adversa y similar.

Panda Adaptive Defense y Panda Adaptive Defense 360 además de bloquear los ataques, proporcionan una visibilidad clara de la actividad maliciosa en toda la organización. Esta visibilidad permite a los equipos de seguridad evaluar rápidamente el alcance de un ataque y tomar acciones apropiadas en respuestas.

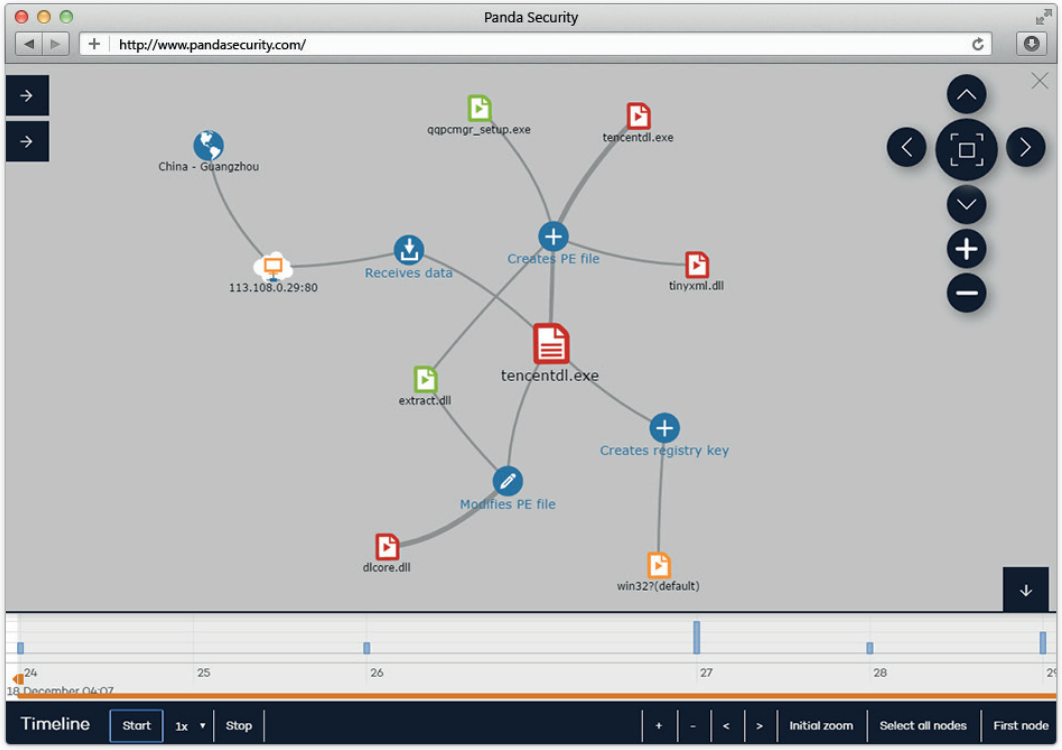


Figura 3. Gráfico del ciclo de vida de un ataque para su análisis forense.

Figura 4. Pilares de Adaptive Defense 360 en la versión extendida de la Cyber-Kill Chain.

Referencias.

- Lockheed Martin's Cyber-Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, at Black Hat 2016: Extended Cyber kill chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 07 April 2016

---

[1] Eric M. Hutchins,Michael J. Cloppert,and Rohan M.Amin,Ph.D.,Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kili Chains.

[2] **Ataques de "Abrebadero" (watering hole attacks)**. Un tipo específico de ataque dirigido donde la víctima pertenece a un grupo particular (organización, industria o región). En este ataque, el atacante imagina u observa qué sitios web el grupo a menudo usa e infecta uno o más de ellos con malware. Con gran probabilidad, algún miembro del grupo objetivo se infecta.

El malware utilizado en estos ataques generalmente recopila información sobre el usuario. Los atacantes que buscan información específica sólo atacan a usuarios procedentes de una dirección IP específica. Esto también hace que los ataques sean más difíciles de detectar e investigar. El nombre se deriva de los depredadores en el mundo natural, que esperan una oportunidad para atacar a sus presas cerca de los abrevaderos.

Basarse en sitios web que el grupo confía hace que esta estrategia sea eficiente, incluso con grupos que son resistentes al phishing y a otras formas de phishing.

[3] **Detección dinámica de Exploits** es la tecnología innovadora de Panda Security basada en la supervisión de todos los procesos en ejecución en el puesto de trabajo y servidores y su análisis en la nube mediante tecnologías de Machine Learning (ML) orientadas a detectar intentos de explotación de aplicaciones de confianza.

El objetivo de esta nueva tecnología es detener los ataques en las primeras etapas de la Cyber-Kill Chain en el puesto de trabajo y servidores. Contener al atacante antes, dificultándole su acceso al dispositivo tanto que el potencial beneficio del ataque no sea rentable y desista en su intento y por consiguiente aumentar la tasa de éxito en la detección de ciber-atacantes.


Adaptive Defense
Más información en:
pandasecurity.com/intelligence-platform/
Hablemos:
900 90 70 80