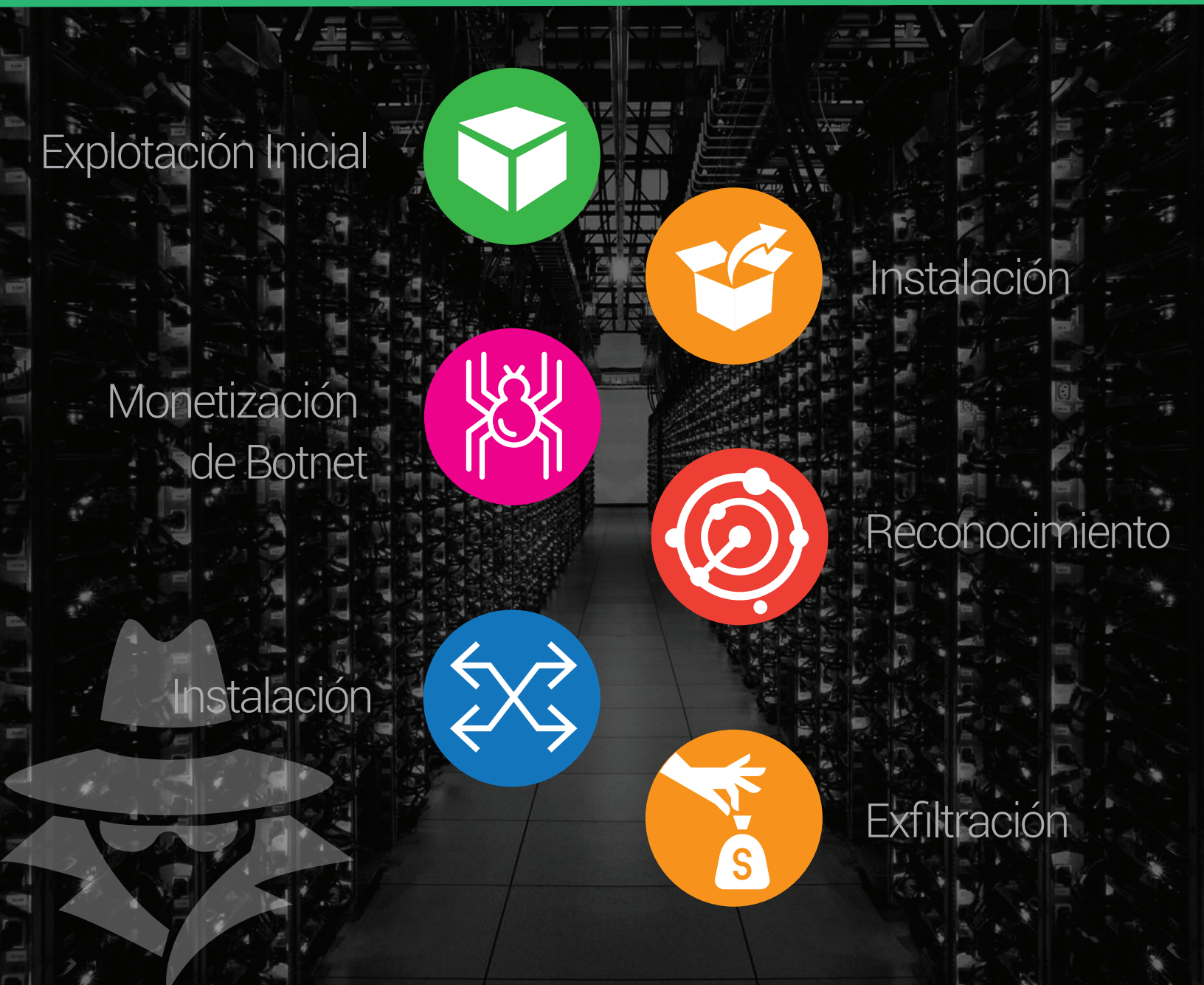
Hillstone NETWORKS

Firewall Inteligente de Próxima Generación de Hillstone Networks: Detección de Amenazas Post-Brechas Utilizando la Cyber Cadena de la Muerte



Nuevos Retos para la Defensa Cibernética

The cyber threat landscape has evolved from traditional "hit and smash" type of attacks to more sophisticated, targeted and well-coordinated techniques aiming to El ámbito de la amenaza cibernética ha evolucionado del tipo tradicional de "golpear y aplastar" a los ataques más sofisticados, específicos y técnicos, bien coordinados con el objetivo de robar valiosos datos corporativos y los secretos de estado o secretos personales. Estos ataques cibernéticos causan enormes daños financieros y políticos a las empresas, instituciones y agencias gubernamentales en todo el mundo.

Los atacantes utilizan varios métodos que incluyen la explotación de las vulnerabilidades de día cero, utilizando software malicioso modificado, la personalización de herramientas de amenazas, el empleo de técnicas anti-sandboxing para escapar de las detecciones de los firewalls tradicionales e incluso contra los firewalls de próxima generación basados en firmas (NGFW) en el perímetro de la red. Estas técnicas de defensa de legado han demostrado ser ineficaces para proteger a las organizaciones contra este tipo de ataques.

Los ataques y amenazas cibernéticos modernos tienen varias características distintivas:

- Largo periodo de invisibilidad después de la infiltración inicial: Los datos de las investigaciones muestran que el promedio de tiempo de detección del ataque es de 225 días durante el cual el código malicioso permanece invisible y puede llevar a cabo actividades lentas y de bajo perfíl dentro de la red víctima. Esto requiere que los administradores supervisen y analicen continuamente los eventos de amenaza o sus registros durante un largo periodo para cualquier alerta sospechosa.

- Múltiples fases antes de obtener su objetivo final: Los ataques suelen pasar por varias fases durante el período de pos-violación antes de enviar los datos robados por último a servidores externos. Los atacantes pueden realizar diferentes actividades en diferentes etapas. Por ejemplo, puede haber actividades de descarga de archivos y actividades de DNS en el host víctima para descargar código malicioso y para conectarse a mando y control (C & C por su sigla en inglés) a un servidor externo, etc.

Como resultado, los métodos de detección de amenazas y de defensa modernos necesitan controlar continuamente tanto en el perímetro usando un firewall de próxima generación, como en el interior la red víctima utilizando tecnologías de comportamiento y análisis de datos, para detectar comportamientos anormales y actividades sospechosas dentro de la red.

Esto se puede lograr de manera efectiva por medio de técnicas para ganar visibilidad para rastrear el comportamiento anormal y malicioso para los ataques que han entrado en la red violada y donde se están preparando para robar datos de los activos críticos.

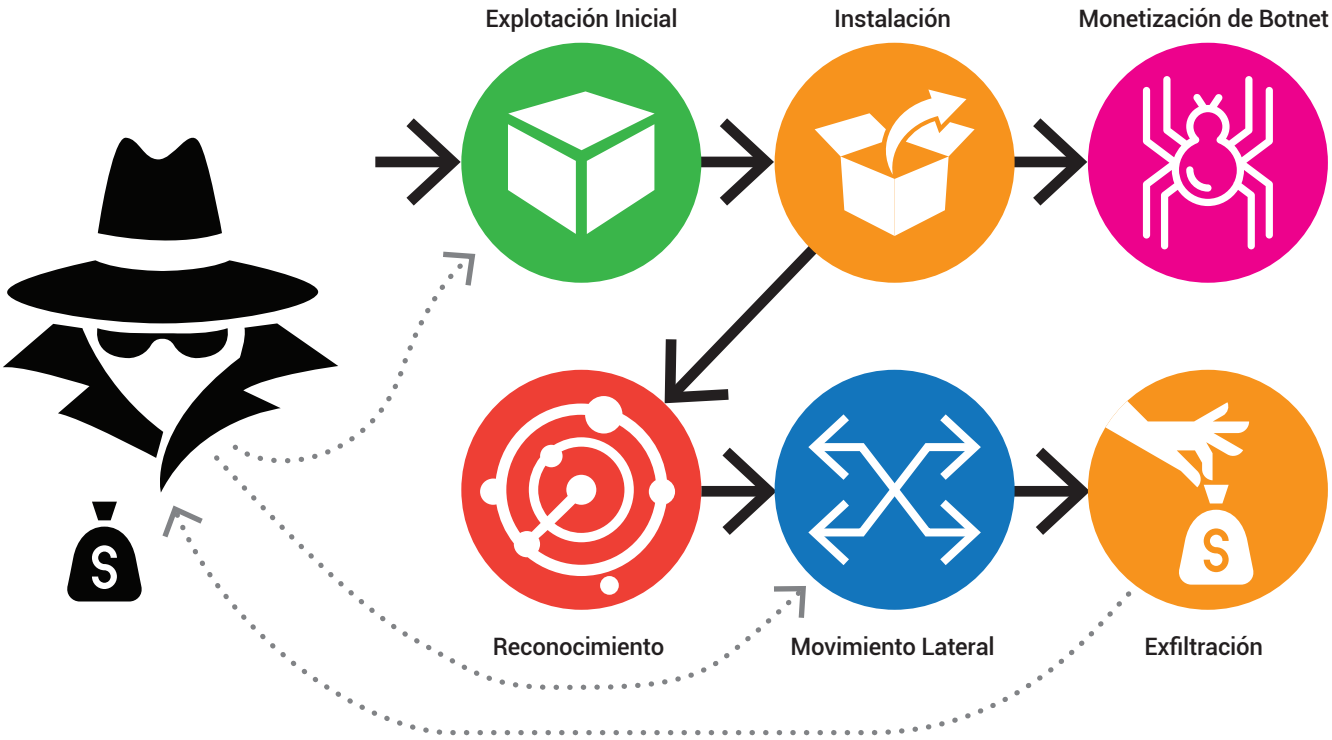
Una vez que entendemos las tácticas que utiliza el atacante, las acciones de mitigación efectivas pueden ser tomadas en cada etapa para romper la cadena de ataque y en última instancia, evitar la exfiltración de datos.

El modelo de la Cadena Cyber Kill (CKC por su sigla en inglés), inicialmente creado por Lockheed Martin para el modelado de inteligencia de defensa militar, es ampliamente utilizado en la industria de seguridad para describir la trayectoria de amenaza ataque cibernético después de la violación inicial en la red víctima.

Mientras que diferentes investigadores de seguridad o vendedores interpretan el modelo CKC de forma ligeramente diferente, hay un entendimiento común de cómo progresa el ataque dentro de la red violada.

En la página siguiente vemos una breve descripción de las principales etapas del modelo CKC que utilizan los firewalls de próxima generación inteligente de Hillstone (iNGFW).

El atacante debe completar todas estas fases con el fin de lograr su objetivo final. El modelo CKC traza los caminos que va a ejecutar. Diferentes técnicas de detección y mitigación pueden ser desarrollados para diferentes etapas, de manera que los administradores de seguridad pueden tomar las medidas adecuadas en cada etapa de detener la exfiltración de datos sensibles y prevenir que el atacante alcance su objetivo final.



Explotación Inicial

El atacante realiza la penetración inicial de los computadores anfitriones o redes específicas. Esto lo puede hacer por medio de un correo electrónico de phishing, visitando sitios web que parecen ser legítimos u otras formas de medios de comunicación social.

Entrega

Después de que el atacante gana con éxito el acceso a la red víctima, puede tratar de descargar e instalar algunos archivos o scripts desarrollados por los atacantes e instalar algo como Portable Ejecutable (PE) y realizar tareas destinadas tales como la comunicación con el servidor externo.

Comando y Control

El código malicioso previamente entregado intenta establecer la conexión entre el host comprometido y el servidor C & C a distancia, generalmente controlado por el atacante fuera de la red víctima. Esto se hace a través de actividades de DNS y la conexión a los servidores de nombres de dominio cuyos son generados utilizando el Algoritmo para Generar Dominios (DGA por su sigla en inglés). El propósito de esto es poder obtener más instrucciones desde el servidor C&C.

Reconocimiento Interno

El atacante puede explorar la red víctima, mapear la topología de la red, buscar e identificar los activos críticos, y sentar las bases para futuras acciones de infiltración.

Movimiento Lateral

En esta etapa, el atacante puede realizar otras actividades como la escalada de privilegios y niveles de acceso, para obtener el control de los activos críticos dentro de la red víctima. Estas actividades se llevan a cabo en preparación para la exfiltración final monetaria o de datos.

Exfiltración de datos

Esta es la etapa final en el CKC. En esta etapa, los atacantes han tomado el control de los activos críticos dentro de la red víctima y han establecido el acceso y han identificado los datos de destino. Los datos se envían fuera de la red al servidor del atacante, a menudo por transferencia de archivos cifrados.

Detección de amenazas luego de una violación mediante el uso de Cyber Kill Chain en iNGFW

El modelo Cyber Kill Chain del iNGFW de Hillstone Networks brinda visibilidad a fondo de cualquier amenaza del pos-ataque dentro de la red víctima.

Se proporciona información de inteligencia de amenazas a partir de múltiples motores de detección y se asigna en contra de las etapas del CKC con los datos de las pruebas forenses y otras opciones viables.

Los motores de detección incluyen los IPS/AV basados en firmas, también incluyen motores que se basan en modelos de aprendizaje automático que utilizan grandes cantidades de muestras de malware, así como la modelización basada en el comportamiento L3-L4 de los equipos host o servidor.

En la figura 1, se detectan eventos de amenazas que apuntan a presuntas actividades de C&C con información detallada. Estos eventos de amenaza pueden ser reportados a partir de uno de los motores IPS/AV de Hillstone, por el motor de detección de malware avanzado y por el motor de detección de la DGA.

En la Figura 2, se ven eventos detectados de amenazas que apuntan a presuntas actividades laterales con información detallada. Estos comportamientos anormales son detectados por el motor de detección de comportamiento anormal de Hillstone.

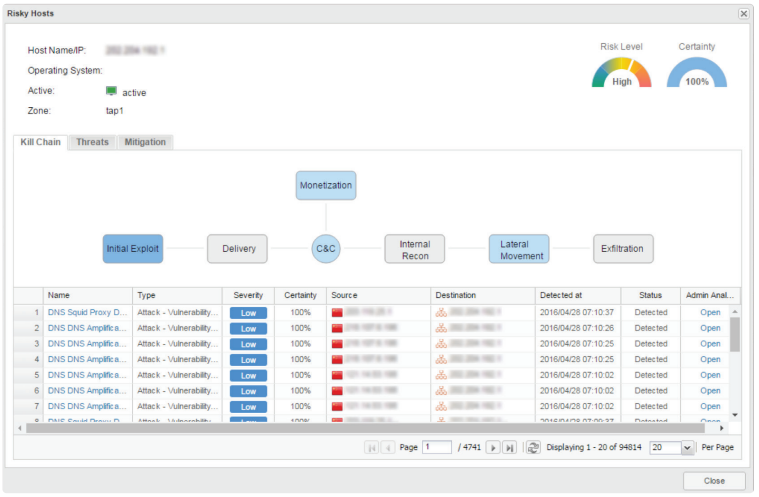


Figura 1. Actividades C&C Detectadas

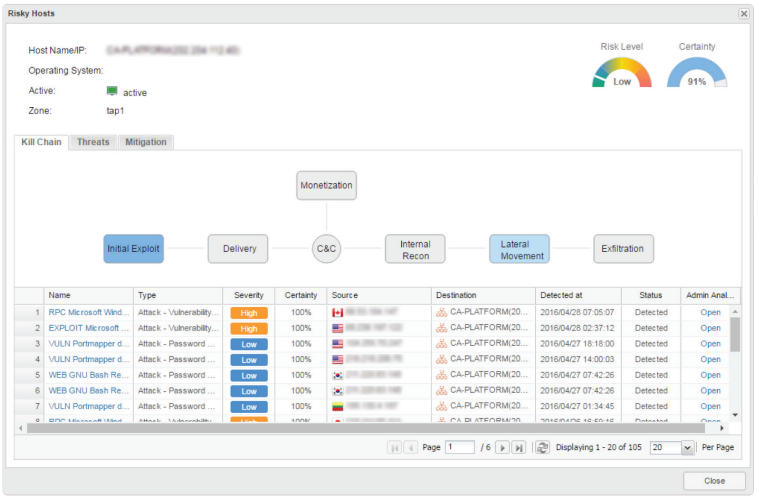


Figura 2. Actividad de Movimiento Lateral Detectado

Conclusión

Para los ataques de amenaza cibernética de hoy en día, sólo es necesario poder ganar entrada a una máquina host víctima y su red ya no es el único objetivo. En su lugar, los atacantes cuidadosamente diseñan y utilizan actividades de pos-violación en diferentes etapas para lograr diferentes propósitos. En tal caso, se requiere que los proveedores de seguridad constantemente desarrollen tecnologías de defensa, tanto en el perímetro de la red, así como dentro de la red víctima para la detección de amenazas pos-violacion y la protección necesaria.

La Cadena Hillstone de Cyber Kill iNGFW, construida sobre varios motores de detección, proporciona una visibilidad completa y pruebas forenses para monitorear continuamente un ataque en curso después de que haya violado la red de destino. Juntos, con otros mecanismos de detección de amenazas de post violación, son un arma poderosa y efectiva para defenderse contra los ataques cibernéticos más sofisticados de hoy en día.

Hillstone NETWORKS

America: **+1-408-508-6750** | APAC: **+65-6678-7660**
MEA: **+971-4557-125-1493** | Europa: **+420-721-125-070**