Abril de 2017

Informe sobre amenazas

McAfee Labs

Mirai, la red de bots para el IoT

La red de bots Mirai infectó y después aprovechó dispositivos IoT insuficientemente protegidos para llevar a cabo el mayor ataque de denegación de servicio distribuido hasta la fecha.

Desarrollo del ataque

1 Búsqueda de dispositivos IoT
Mirai analiza una gran cantidad de direcciones IP para buscar puertos Telnet o SSH abiertos y localiza los dispositivos IoT conectados a esos puertos.

2 Ataque de fuerza bruta
A continuación, Mirai lanza un ataque de fuerza bruta contra dichos dispositivos IoT, mediante el empleo de un diccionario de nombres de usuario y contraseñas predeterminados, con el fin de identificar los que no están lo suficientemente protegidos.

3 Envío de credenciales
Tras ejecutar el ataque de fuerza bruta, el malware envía la dirección IP y las credenciales del dispositivo IoT al servidor de control.

4 Descarga del bot de Mirai
Un servidor de carga descarga el binario del bot de Mirai en el dispositivo IoT.

5 Espera de instrucciones para el ataque
Una vez infectado el dispositivo IoT, el malware espera las instrucciones para llevar a cabo el ataque DDoS.

6 Inicio del ataque DDoS
Mirai puede lanzar ataques DDoS en las capas 3, 4 y 7 del modelo OSI.

2,5 millones
Aproximadamente 2,5 millones de dispositivos IoT han sido infectados por Mirai.

5 cada minuto
Cada minuto, se añaden aproximadamente cinco direcciones a las redes de bots Mirai.

1,2 Tbit/s de tráfico
En el punto álgido, una víctima de la red de bots Mirai recibió 1,2 Tbit/s de tráfico, el mayor volumen de tráfico DDoS registrado jamás.

De 50 a 7500 dólares al día
Los ataques DDoS basados en Mirai se ofrecen ahora como un servicio que cuesta de 50 a 7500 dólares al día.

Evolución de Mirai

1 *Entorno a agosto de 2016*
Fase inicial de Mirai
Empiezan a surgir los binarios ELF de Mirai.

2 *20 de septiembre de 2016*
DDoS en el sitio web "Krebs on Security"
Mirai infecta DVR y CCTV en el puerto Telnet.

3 *1 de octubre de 2016*
Publicación del código fuente de Mirai
Anna-Senpai publica el código fuente de Mirai.

4 *4 de octubre de 2016*
Red de bots Mirai como servicio
Un foro clandestino ofrece DDoS como servicio.

5 *28 de noviembre de 2016*
Apagón en Deutsche Telekom
Encontrada una nueva variante de Mirai. Objetivo: puerto 7547.

Agosto | Septiembre | Octubre | Noviembre

Intercambio de inteligencia sobre amenazas

Lo que desconoce puede hacerle daño.

¿Qué es la inteligencia sobre amenazas?

Inteligencia estratégica
Información procesada sobre actividades de planificación y directivas de seguridad a nivel organizativo. Incluye datos como, por ejemplo, los adversarios potenciales y sus objetivos, las probabilidades de riesgo y las evaluaciones de impacto, así como los requisitos legales y normativos.

Inteligencia táctica
Información que recopilan los sistemas de seguridad, analizadores y sensores. Suele incluir indicadores de peligro que resultan útiles para los análisis forenses y las iniciativas de reparación.

Inteligencia operativa
Los componentes esenciales para establecer el contexto. Incluye el ámbito y el alcance de un presunto ataque y datos sobre cómo coordinar mejor las medidas de respuesta al incidente. Se pueden aplicar a este problema análisis de big data, aprendizaje automático y otras ténicas automatizadas de toma de decisiones con el fin de aumentar la capacidad y el juicio humano.

Desafíos fundamentales del uso compartido de la inteligencia sobre amenazas

Volumen
Los sensores de seguridad, análisis de big data y herramientas de aprendizaje automático han generado un importante problema de relación señal-ruido que afecta a la capacidad de clasificar, procesar y utilizar la inteligencia.

Validación
Debemos investigar las fuentes de inteligencia sobre amenazas para garantizar que los datos proceden de un origen legítimo, y no de adversarios que presentan informes falsos a fin de provocar confusión o inundar de datos las herramientas de inteligencia sobre amenazas.

Correlación
Para que las medidas sean eficaces es fundamental validar los datos casi en tiempo real, correlacionarlos en distintos sistemas operativos, dispositivos y redes, así como clasificar los eventos y delimitar la respuesta.

Calidad
Las fuentes legítimas pueden enviar distinta información, desde indicadores de peligro hasta el ciclo del evento completo, lo que en ocasiones resulta irrelevante para el receptor. Para que la inteligencia sobre amenazas sea práctica se deben automatizar filtros, etiquetas y desduplicación.

Rapidez
La comunicación abierta, estandarizada y en tiempo real es esencial para limitar el tiempo que transcurre entre la detección de un ataque y la recepción de la inteligencia sobre amenazas.

Estadísticas sobre amenazas

Hay 176 amenazas nuevas cada minuto, o casi 3 cada segundo.

Incidentes — 974
Hemos contabilizado 197 incidentes públicos conocidos en el 4.º trimestre y 974, en 2016.

Malware — 24 %
El número de nuevas muestras de malware en el 4.º trimestre —23 millones— descendió un 17 % respecto al 3.er trimestre. **Sin embargo, el número total aumentó un 24 % en 2016, hasta alcanzar los 638 millones de muestras.**

Malware para Mac OS — 744 %
Aunque aún es pequeño comparado con la cantidad de amenazas que recibe Windows, el número de muestras de malware para Mac OS ha aumentado un 245 % en el 4.º trimestre, debido al adware. **El total de malware para Mac OS aumentó un 744 % en 2016.**

Malware para móviles — 99 %
El número de nuevas muestras de malware para móviles se redujo un 17 % en el 4.º trimestre. **Pero el total de malware para móviles aumentó un 99 % en 2016.**

Redes de bots de spam — 24 %
Los mensajes de spam de las 10 principales redes de bots disminuyeron un 24 % en el 4.º trimestre, hasta los 181 millones de mensajes. Estas 10 redes de bots principales generaron 934 millones de mensajes de correo electrónico de spam en 2016.

Ransomware — 88 %
El número de nuevas muestras de ransomware descendió un 71 % en el 4.º trimestre, debido a una caída de las detecciones de ransomware genérico, así como a una disminución de Locky y CryptoWall. **El total de muestras de ransomware aumentó un 88 % en 2016.**

McAfee Global Threat Intelligence

McAfee GTI recibió de media 49 600 millones de consultas al día.

McAfee GTI

66 millones
Las protecciones de McAfee GTI contra URL maliciosas **aumentaron hasta los 66 millones al día en el 4.º trimestre**, desde los 57 millones del 3.er trimestre.

37 millones
Las protecciones de McAfee GTI contra programas potencialmente no deseados mostraron un **aumento hasta los 37 millones al día en el 4.º trimestre**, desde los 32 millones del 3.er trimestre.

71 millones
Las protecciones de McAfee GTI contra archivos maliciosos **descendieron hasta los 71 millones al día en el 4.º trimestre**, desde los 150 millones del 3.er trimestre, debido a un incremento del bloqueo de descargas.

35 millones
Las protecciones de McAfee GTI contra direcciones IP peligrosas **aumentaron hasta los 35 millones al día en el 4.º trimestre**, desde los 27 millones diarios del 3.er trimestre.

Informe de McAfee Labs sobre amenazas: abril de 2017

Visite www.mcafee.com/April2017ThreatsReport para ver el informe completo.

intel Security