Publicado en Ciudad de México el 05/12/2018

# [Investigación de Avast: 7 nuevas variantes de Mirai y el candidato a hacker que está detrás](http://www.notasdeprensa.es)

## Dos años después de Mirai, las botnets se han convertido en juguetes de los ¨script kids¨

 En septiembre de 2016, el ataque DDoS más grande de la historia dejó sin conexión a Twitter, CNN, Spotify, entre otros. La fuerza detrás del ataque fue una botnet conocida como Mirai. En ese momento, nadie esperaba que una multitud de dispositivos de Internet de las cosas (IoT) improvisados formaran una botnet que estuviera detrás de un ataque de tal magnitud. El Equipo de inteligencia de amenazas de Avast analizó un grupo de 7 nuevas variantes de Mirai e investigó quién podría estar detrás de ellas. Los resultados muestran que el ciberdelincuente que está detrás, renta estas botnets como servicio a otros. Modificar el código Mirai para lanzar y distribuir una nueva versión de botnet es relativamente simple, y si bien las investigaciones de Avast muestran que es posible que un chico script un tanto inexperto esté detrás de estas siete versiones, aun pueden causar destrucción. El código fuente de Mirai lanzado desencadena la creación de nuevas variantes de botnetDespués de acabar con gran parte de Internet, el creador de malware de Mirai, autodenominado and #39;Anna-Senpai and #39;, lanzó el código fuente. El código Mirai se convirtió rápidamente en un marco de referencia, como una plantilla, y cualquier persona que encuentre una nueva forma de explotar un nuevo dispositivo puede simplemente agregarlo, lo que crearía una and #39;nueva and #39; variante de la botnet. En 2018, el usuario de Twitter @ 400kQBOT lanzó un enlace con el código fuente de siete variantes de Mirai, y el Equipo de Inteligencia de amenazas de Avast comenzó a investigar sus orígenes. Las investigaciones llevaron a la suposición de que un ciberdelincuente apodado Scarface # 1162 podría estar detrás de las siete variantes botnets, y está alquilando el acceso como servicio, promocionándolas en Youtube y Twitter. La suposición del El equipo de Avast de que 400kQbot y Scarface eran la misma persona se confirmó cuando a mediados de septiembre, se identificó en un tweet desde el punto de control de 400kQBot. Una mirada más profunda a las versiones alteradas de MiraiAl observar de cerca las siete nuevas variantes de Mirai, el Equipo de inteligencia de amenazas de Avast descubrió que difieren de la variante original en la lista de contraseñas que usan para forzar los dispositivos IoT vulnerables, los puertos en los que intervienen y la arquitectura: Combinaciones de credenciales: cuando se trata de combinaciones de credenciales, el código original de Mirai utilizó una lista de sesenta y dos contraseñas codificadas para realizar un ataque de fuerza bruta (ataque de diccionario) contra dispositivos vulnerables de IoT. Al analizar las variantes, el equipo de Avast descubrió que la lista de contraseñas cambia por bot. El equipo recuperó y decodificó todas las contraseñas utilizadas por cada variante para averiguar si la lista de contraseñas se reutilizó desde el código de Mirai y si hay alguna superposición. La lista de contraseñas más grande se implementó en la variante de Saikin con ochenta contraseñas, donde solo cuatro se superponen con el código original de Mirai. Al elegir implementar la lista de contraseñas diferentes, el atacante probablemente está apuntando a una variedad más amplia de dispositivos IoT. Puertos nuevos: al igual que Mirai, todas sus variantes tienen un módulo killer.c que tiene varios propósitos. Primero, se deshace de otro malware que posiblemente se ejecute en el dispositivo actual. Segundo, evita que otros obtengan acceso remoto al dispositivo a través de Telnet, SSH o HTTP. El análisis reveló que además de tener los puertos de eliminación estándar de Mirai, cinco de las siete variantes (excepto Saikin y Josho\_V3) agregaron un nuevo puerto específico de protocolo / dispositivo a sus listas de eliminación. La adición de estos puertos permitiría al autor de la botnet conectarse a más dispositivos y al mismo tiempo evitar que otros se conecten a estos dispositivos de forma remota. Nuevas arquitecturas: todas las variantes de Mirai que el Equipo de inteligencia de amenazas de Avast observó apuntan a las mismas arquitecturas que Mirai, y solo tres de ellas: Sora, Saikin y Akiru agregaron dos nuevas arquitecturas: ARC (Argonaut RISC Core) y RCE (Motorola RCE). El equipo de Inteligencia de amenazas explica: "Nuestro análisis revela que si bien las nuevas variantes no tienen notables alteraciones del código fuente original de Mirai, son capaces de causar mucho daño. Su objetivo es apuntar a diferentes dispositivos de IoT y más que la variante original de Mirai, cambiando las listas de contraseñas utilizadas para ataques de fuerza bruta y agregando nuevos puertos a su objetivo. Cuantas más variantes de botnet haya, más daño se puede hacer, y para el usuario, esto significa que la amenaza es real. Si un dispositivo en el hogar es atacado, como un monitor de bebés o un router, un ciberdelincuente también puede acceder a todos los dispositivos en el hogar. Los usuarios deben cambiar las contraseñas predeterminadas de sus dispositivos por contraseñas complejas y asegurarse de actualizar su firmware cuando haya nuevas actualizaciones disponibles". Avast recomienda los siguientes pasos para proteger los dispositivos IoT y la casa inteligente: Cambiar la contraseña de administrador predeterminada del enrutador y cualquier dispositivo de IoT mientras configura el dispositivo. Mantenga los dispositivos con las últimas actualizaciones de firmware. Deshabilite la administración remota en la página de configuración del router. Si no está seguro si el dispositivo ha sido infectado, considere restablecer el dispositivo con la configuración del fabricante y repita desde el paso uno. Más información en el blog de Avast: https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/investigacion-de-avast-7-nuevas-variantes-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Programación Ciberseguridad Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)