Hackers siguen explotando el malware Mirai

La firma de rendimiento de red **Netscout Arbour ha analizado cuatro de las variantes actuales del código fuente de Mirai: Satori, JenX, OMG y Wicked**. Su equipo de respuesta e ingeniería de seguridad de Arbor (ASERT) explican cómo cada una de estas botnets parte de los bloques de construcción básicos de Mirai y se agrega a la funcionalidad original de este malware y algunas veces se elimina de ella, agregando, dice, ASERT, "su propio estilo".

El ataque de la botnet Mirai, es visto como revolucionario para el malware que se dirige al Internet de las cosas (IoT), ya que ha causado destrucción en todo el mundo y ha popularizado el malware basado en IoT.

Mirai se extendió buscando otros dispositivos IoT (cámaras IP y enrutadores del hogar) y accesando mediante la 'fuerza bruta' a través de una lista de contraseñas de proveedores predeterminadas. Dado que tan pocos consumidores cambian la contraseña que viene con el dispositivo, el proceso es notablemente exitoso.

Todos estos dispositivos forman parte de los casi 27 mil millones de dispositivos de Internet de las Cosas en 2017, que llegarán a 125 mil millones para 2030, según un nuevo análisis de IHS Markit2.

NETSCOUT Arbor informó que este crecimiento constituye un objetivo extremadamente atractivo para los autores de malware.

René Hernández, especialista en ciberseguridad de esta firma, indicó que entre las principales vulnerabilidades a dispositivos IoT se incluyen credenciales predeterminadas dentro del código fuente, desbordamientos de búfer e inyección de comandos. "La mayoría de los dispositivos IoT para consumidores contienen este tipo de vulnerabilidades; cuando se lanzan parches para abordar estos problemas, rara vez se aplican.

Satori (o al menos la tercera variante de Este malware) utiliza la misma tabla de configuración y la misma técnica de ofuscación de cuerdas que Mirai. Sin embargo, dice ASERT, "vemos que el autor amplía el código fuente de Mirai para incluir diferentes exploits, como el exploit Huawei Home Gateway".

El exploit fue CVE-2017-17215. En diciembre de 2017, Check Point informó que se habían realizado cientos de miles de intentos para explotar esta vulnerabilidad en los enrutadores de origen Huawei HG532 que intentaban descargar y ejecutar la botnet Satori .

“Actualmente parece que JenX solo se enfoca en ataques DDoS contra jugadores del videojuego Grand Theft Auto San Andreas, que ha sido notado por otros investigadores.

“Los autores de este malware continuarán aprovechando el código malicioso basado en IoT de forma automatizada, aumentando rápidamente el tamaño de botnets a través de la distribución similar a gusanos, funcionalidad de proxy de red y explotación automatizada de vulnerabilidades en dispositivos con conexión a Internet. Es importante que las organizaciones apliquen parches adecuados, actualizaciones , y estrategias de mitigación DDoS para defender sus organizaciones “, advierte ASERT.