Investigadores de seguridad cibernética descubrieron una nueva amenaza emergente de botnet de IoT que aprovecha los dispositivos inteligentes comprometidos para organizar ataques de *«denegación de servicio distribuido»,* potencialmente desencadenados a pedido por medio de plataformas que ofrecen servicios DDoS de alquiler.

La botnet, denominada como *«dark_nexus»* por los investigadores de Bitdefender, funciona empleando ataques de relleno de credenciales contra una variedad de dispositivos, como enrutadores (de Dasan Zhone, Dlink y ASUS), grabadoras de video y cámaras térmicas, para cooptarlos en la botnet.

Hasta ahora, dark_nexus compromete al menos 1372 bots, que actúan como un proxy inverso, que abarca varias ubicaciones en China, Corea del Sur, Tailandia, Brasuil y Rusia.

> *«Si bien podría compartir algunas características con botnets IoT previamente conocidas, la forma en que se han desarrollado algunos de sus módulos lo hace significativamente más potente y robusto. Por ejemplo, las cargas útiles se compilan para 12 arquitecturas de CPU diferentes y se entregan dinámicamente en función de la configuración de la víctima»*, dijeron los investigadores.

La evidencia reunida por Bitdefender apunta a greek.Helios como la persona detrás del desarrollo de dark_nexus, quien es un conocido autor de botnets por vender servicios DDoS en plataformas de redes sociales y utilizar un canal de YouTube para anunciar sus capacidades.

Similitudes con otras botnets

Al observar las similitudes de dark_nexus con el malware bancario Qbot y Mirai, los investigadores de Bitdefender afirmaron que sus módulos principales son *«en su mayoría originales»* y que se actualizan con frecuencia, con más de 30 versiones lanzadas durante el período de diciembre de 2019 a marzo de 2020 (versiones 4.0 a 8.6).

> *«El código de inicio del bot se paree al Qbot: se bifurca varias veces, bloquea varias señales y se separa del terminal»*, dijeron los investigadores.
>
> *«Luego, en la línea de Mirai, se une a un puerto fijo (7630), asegurando que una sola instancia de este bot pueda ejecutarse en el dispositivo. El bot intenta disfrazarse cambiando su nombre a '/bin/busybox'. Otra característica prestada de Mirai es la desactivación del watchdog mediante llamadas periódicos ioctl en el dispositivo virtual»,* agregaron.

La infraestructura consta de varios servidores de comando y control C2 (switchnets [.] Net: 30047 amd thiccnigga [.] Me: 30047), que emiten comandos remotos a los bots infectados y servidores de informes en los que los bots comparten detalles acerca de servicios vulnerables.

Una vez que el ataque de fuerza bruta tiene éxito, el bot se registra en el servidor C2 identificando la arquitectura de la CPU del dispositivo para transmitir una carga útil de infección personalizada por medio de Telnet, descargar binarios de bot y otros componentes de malware desde un servidor de alojamiento (switchnets[.]Net:80) y ejecutarlos.

Además, algunas versiones de las botnets (4.0 a 5.3) vienen como una función de proxy inverso que le permite a la víctima actuar como un proxy para el servidor de alojamiento, lo que le indica al dispositivo infectado que descargue y almacene los ejecutables necesarios en lugar de tener que conectarse al servidor central de alojamiento.

Además de eso, dark_nexus viene con comandos de persistencia que evitan que el dispositivo se reinicie al detener el servicio cron y eliminar los privilegios a los servicios que podrían usarse para reiniciar dicho dispositivo en cuestión.

> *«También utiliza una técnica destinada a garantizar la supremacía en el dispositivo comprometido»*, dijo Bitdefender.
>
> *«Excepcionalmente, dark_nexus utiliza un sistema de puntuación basado en pesos y umbrales para evaluar qué procesos pueden presentar un riesgo. Esto implica mantener una lista de procesos incluidos en la lista blanca y sus PID, y eliminar cualquier otro proceso que cruce un umbral (mayor o igual a 100) de sospecha».*

La botnet Mirai, desde su descubrimiento en 2016, se ha relacionado con una serie de ataques DDoS a gran escala. Desde entonces, han surgido numerosas variantes de Mirai, en parte debido a la disponibilidad de su código fuente en Internet.

Asimismo, los autores de botnets han organizado ataques de fuerza bruta en sitios de WordPress para insertar el troyano bancario Qbot y descargar malware adicional.

El hecho de que dark_nexus esté construido sobre los cimientos de Mirai y Qbot es una prueba de la evolución de las tácticas de los operadores de botnets y piratas informáticos sin experiencia, lo que les permite agregar nuevas funcionalidades explotando una variedad de vulnerabilidades en dispositivos de IoT mal asegurados y acumulando ejércitos de botnets modernos.

> *«Utilizando videos de YouTube que muestran algunos de sus trabajos anteriores y publicando ofertas en distintos foros cibercriminales, greek.Helios parece tener experiencia con habilidades de malware IoT, perfeccionándolas hasta el punto de desarrollar la nueva botnet dark_nexus»,* dijeron los investigadores.