ALERTA: AFECTACIÓN POR BOTNET MERIS (20/SEPTIEMBRE/2021)

Investigadores alertan de equipos comprometidos con la botnet MERIS.

Introducción

El Centro de Respuesta a Incidentes Informáticos de la ARCOTEL – EcuCERT, dentro de su gestión y como parte del apoyo recibió de su red de confianza internacional la notificación del uso del puerto TCP abierto 5678 para ataque de DDOS de la botnet Meris entre los equipos que usan este puerto están MikroTik y LinkSys.

Meris es una nueva botnet que funciona con dispositivos de Internet de las cosas (IoT). Los productos de IoT: PC, dispositivos domésticos, incluidas cámaras, VCR, televisores y enrutadores, que se secuestran se convierten en nodos esclavos en la red de una botnet y luego se pueden usar para realizar ataques distribuidos de denegación de servicio (DDoS), entre otros.

Qrator Labs un servicio de mitigación de ataques DDoS ruso, le ha calificado a Meris como un "nuevo tipo de botnet" que apareció por primera vez a fines de junio del 2021 y aún está creciendo. Según indican, Meris "puede abrumar a casi cualquier infraestructura, incluidas algunas redes altamente robustas. Todo esto se debe a la enorme potencia de RPS que trae consigo". A lo que hacen referencia con RPS es a las solicitudes por segundo que la botnet hace. Es una de las principales formas de medir el tamaño de un ataque, la otra importante es según la cantidad de datos que pide por segundo.

Generalmente los ataques se analizan por cantidad de datos que se pide por segundo, es relativamente raro ver ataques donde predomina la cantidad de peticiones por segundo. Además de esto, este ataque de Meris se muestra como una cantidad de RPS especialmente alta, de ahí que se le considere un "nuevo tipo de botnet".

Los ataques DDoS consisten principalmente en saturar los servidores a base de solicitudes para que el servidor se caiga. Es relativamente "inofensivo" ya que no se compromete la seguridad de los datos en sí (puede ocurrir después mediante otras técnicas). A partir de ahí lo que los atacantes suelen hacer es pedir dinero a las víctimas para dejar de atacarles y dejar inutilizados los servidores.

Cloudflare, que recientemente informó sobre otro gran ataque DDoS , corroboró los hallazgos de Qrator.

"Podemos confirmar que la fuente del ataque de 17.2M RPS que vimos anteriormente estaba compuesta casi en su totalidad por dispositivos MikroTik que ejecutaban proxies SOCKS abiertos y utilizaban canalización HTTP", dijo Patrick Donahue, director de producto de Cloudflare.

Donahue dijo que, a diferencia de la botnet Mirai, la nueva botnet consiste en una menor cantidad de dispositivos de infraestructura de red comprometidos y de altos recursos que se utilizan para el tráfico de ataque proxy que se origina en instancias de VPS en la nube.

"Seguimos viendo ataques diarios de esta botnet", dijo.

Según Qrator Labs y Yandex , Meris. En este caso, Meris se compone de una gran cantidad de enrutadores MikroTik.

MikroTik ha emitido una declaración sobre la botnet, señalando que el compromiso de sus dispositivos parece provenir de una vulnerabilidad parcheada en RouterOS en 2018, en lugar de una vulnerabilidad de día cero o nueva.

> "Desafortunadamente, cerrar la vulnerabilidad no protege inmediatamente estos enrutadores", dijo la compañía. "Si alguien obtuvo su contraseña en 2018, solo una actualización no ayudará. También debe cambiar [su] contraseña, volver a verificar su firewall [para que] no permita el acceso remoto a partes desconocidas y buscar scripts que usted hizo no crear. Hemos tratado de llegar a todos los usuarios de RouterOS sobre esto, pero muchos de ellos nunca han estado en contacto con MikroTik y no están monitoreando activamente sus dispositivos. También estamos trabajando en otras soluciones".

Vector de ataque

Utiliza túneles L2TP (Layer 2 Tunneling Protocol - es un protocolo de túneles que amplía el protocolo punto a punto (PPP) conocido también como PPP virtual) para comunicaciones entre redes. Para realizar el ataque, la botnet utiliza el proxy SOCKS4 en el dispositivo infectado y luego utiliza la técnica DDoS de canalización HTTP.

El tráfico de ataque mediante proxy facilita a los atacantes generar altos volúmenes de tráfico de ataque L7 (capa de aplicación) utilizando potentes servidores en la nube, y hace que sea más difícil averiguar de dónde se genera el tráfico de ataque.

La botnet está explotando la 'canalización HTTP', una función que permite a los clientes enviar solicitudes a servidores web en lotes sin esperar respuestas individuales.

La canalización HTTP es lo que permite que esta botnet logre números tan asombrosamente altos en RPS y, al mismo tiempo, hace que la detección y mitigación de ataques sea mucho más fácil. Sin embargo, incluso cuando se detecta y bloquea un ataque de canalización, un lote completo de solicitudes HTTP permanecerá en la canalización del servidor de destino. El ascenso de Meris es un recordatorio de la complejidad y la evolución continua de los ataques DDoS.

El código fuente de Mirai se filtró, provocando que aparecieran muchas variantes que todavía están en funcionamiento.

Indicadores de compromiso

Bloquee estos dominios de punto final de túnel:

* .eeongous.com
* .leappoach.info
* .mythtime.xyz

Bloquee estos dominios de descarga de secuencias de comandos:

1abcnews.xyz
1awesome.net
7standby.com
audiomain.website
bestony.club
ciskotik.com
cloudsond.me
dartspeak.xyz
fanmusic.xyz
gamedate.xyz
globalmoby.xyz
hitsmoby.com
massgames.space
mobstore.xyz
motinkon.com
my1story.xyz
myfrance. xyz

phonemus.net
portgame.website
senourth.com
sitestory.xyz
spacewb.tech
specialword.xyz
spgames.site
strtbiz.site
takebad1.com
tryphptoday.com
wchampmuse.pw
weirdgames.info
widechanges.best
zancetom.com

Dominios utilizados por la botnet:

bestmade.xyz
gamesone.xyz
mobigifs.xyz
myphotos.xyz
onlinegt.xyz
picsgifs.xyz

Recomendaciones de mitigación provistas por el fabricante Mikrotik para BOTNET MĒRIS

- Mantenga su dispositivo MikroTik actualizado con actualizaciones periódicas.
- No abra el acceso a su dispositivo desde el lado de Internet para todos, si necesita acceso remoto, solo abra un servicio VPN seguro, como IPsec.
- Use una contraseña segura e incluso si la usa, ¡cámbiela ahora!
- No asuma que se puede confiar en su red local. El malware puede intentar conectarse a su enrutador si tiene una contraseña débil o no tiene contraseña.
- Inspeccione la configuración de su RouterOS en busca de configuraciones desconocidas (ver más abajo).
- MikroTik en colaboración con investigadores independientes han descubierto que existe malware que intenta reconfigurar su dispositivo MikroTik desde una computadora con Windows dentro de su red. Esta es la razón por la que es importante establecer una mejor contraseña ahora (para evitar el inicio de sesión sin contraseña o un ataque de diccionario por parte de este malware) y mantener actualizado su enrutador MikroTik

(ya que este malware también intenta explotar la vulnerabilidad CVE-2018-14847 mencionada que ha ha sido arreglado).

- Configuración a tener en cuenta y eliminar:
- Sistema -> Reglas del programador que ejecutan un script de recuperación. Elimínelos.
- IP -> Calcetines proxy. Si no usa esta función o no sabe lo que hace, debe deshabilitarla.
- Cliente L2TP llamado "lvpn" o cualquier cliente L2TP que no reconozca.
- Ingrese la regla de firewall que permite el acceso al puerto 5678.

Referencias

- Charlie Osborne. La botnet Meris ataca a KrebsOnSecurity. (15 de septiembre de 2021). Recuperado el 20 de septiembre de 2021. Disponible en https://www.zdnet.com/article/meris-botnet-assaults-krebsonsecurity/
- Cristian Rus. Así es Meris, una nueva botnet que ha conseguido batir dos veces el récord del ataque DDoS más grande de la historia.10 de septiembre de 2021). Recuperado el 20 de septiembre de 2021. Disponible en: https://www.xataka.com/seguridad/asi-meris-nueva-botnet-que-ha-conseguido-batir-dos-veces-record-ataque-ddos-grande-historia
- Mikrotik 2021. BOTNET MĒRIS (15 de septiembre del 2021) Recuperado el 20 de septiembre de 2021. Disponible en: https://blog.mikrotik.com/security/meris-botnet.html