Nro. Alerta:	09F-202112091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
Versión:	1.0	**ALERTAS DE SEGURIDAD**	
Fecha:	09-dic-2021	**BOTNET DARK MIRAI PONE EN LA MIRA A POPULAR ENRUTADOR DE LA MARCA TPLINK PARA EJECUCIÓN DE RCE**	

I. DATOS GENERALES:

Clase de alerta: Instrucción,

Tipo de incidente: Código de Ejecución remoto (RCE)

Nivel de riesgo: Bajo

TLP: Blanco

II. ALERTA

La función PING en el enrutador TP-Link TL-WR840N EU v5 con firmware TL-WR840N (EU) _V5_171211 es vulnerable a la ejecución remota de código a través de una carga útil diseñada en un campo de entrada de dirección IP; vulnerabilidad que es explotada por el botnet Dark Mirai.

Figura 1.- Marca, modelo y versión de Firmware que presenta vulnerabilidad
Fuente: Kamilló Matek (<ᖴᙅ ı ᑎᖘ)

Nro. Alerta:	09F-202112091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
Versión:	1.0	**ALERTAS DE SEGURIDAD**	
Fecha:	09-dic-2021	**BOTNET DARK MIRAI PONE EN LA MIRA A POPULAR ENRUTADOR DE LA MARCA TPLINK PARA EJECUCIÓN DE RCE**	

III. INTRODUCCIÓN

Según un informe de investigadores de Fortinet , quienes han estado siguiendo la actividad del ciberataque Dark Mirai, ésta botnet agregó un RCE particular en su arsenal, solo dos semanas después de que TP-Link lanzó una actualización de firmware.

La variante actualizada de la campaña MANGA (también conocida como Dark), distribuye muestras basadas en el código fuente publicado por Mirai. ésta campaña de botnet distribuida de denegación de servicio (DDOS) basada en Mirai, es una que FortiGuard Labs ha estado monitoreando activamente . La campaña originalmente despertó interés debido a la actualización continua de su lista de vulnerabilidades objetivo, más que otras campañas que se han visto hasta ahora.

Es posible que Mirai se haya ido, pero su código ha generado numerosas redes de bots nuevas que causan problemas a gran escala en dispositivos no seguros.

IV. VECTOR DE ATAQUE:

FIRMWARE / RCE

Criminales informáticos explotan la vulnerabilidad CVE-2021-41653, descubierta el 12 de noviembre de 2021, para obligar a los dispositivos a descargar un script malicioso, "tshit.sh", el cual descarga a su vez payloads de tipo binario para complementar su ataque.

Los actores aún necesitan autenticarse para que este exploit funcione, pero si el usuario ha dejado el dispositivo con las credenciales predeterminadas, se vuelve trivial explotar la vulnerabilidad.

Al igual que el Mirai estándar, MANGA detecta la arquitectura de la máquina infectada y obtiene la carga útil correspondiente.

Luego, bloquea las conexiones a los puertos de destino común para evitar que otras botnets se apoderen del dispositivo capturado.

Finalmente, el malware espera un comando del servidor C&C (comando y control) para realizar algún tipo de ataque DoS (denegación de servicio).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	09F-202112091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
Versión:	1.0	**ALERTAS DE SEGURIDAD**	
Fecha:	09-dic-2021	**BOTNET DARK MIRAI PONE EN LA MIRA A POPULAR ENRUTADOR DE LA MARCA TPLINK PARA EJECUCIÓN DE RCE**	

V. IMPACTO:

Al explotar las vulnerabilidades publicadas recientemente, esta campaña de malware aprovecha la brecha entre el momento de la divulgación de una vulnerabilidad y la aplicación de un parche para comprometer los dispositivos de IoT. Esto le da un mayor potencial de propagación, lo que lo hace más prolífico que redes de bots similares. La última incorporación a su lista en constante crecimiento de vulnerabilidades específicas son los enrutadores inalámbricos domésticos TP-Link, en particular el modelo TL-WR840N EU (V5), equipos que son comunes en muchos hogares, oficinas e incluso empresas alrededor del mundo, sumado a su bajo costo de adquisición.

Hasta la actualidad, muchos siguen sin ser parchados, actualizados, sus contraseñas de fábrica no han sido modificadas; convirtiéndolos en una gran brecha de seguridad perimetral.

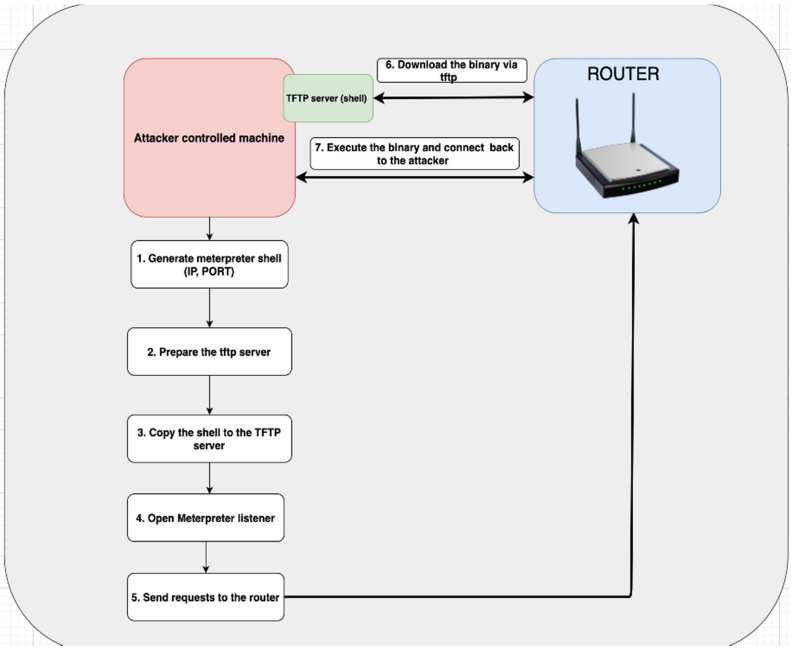

Figura 2.- Prueba de concepto POC de vulnerabilidad en equipo TPLINK
Fuente: Kamilló Matek (<ᖴᙅ I ᑎᖘ)

Nro. Alerta:	09F-202112091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
Versión:	1.0	**ALERTAS DE SEGURIDAD**	
Fecha:	09-dic-2021	**BOTNET DARK MIRAI PONE EN LA MIRA A POPULAR ENRUTADOR DE LA MARCA TPLINK PARA EJECUCIÓN DE RCE**	

VI. INDICADORES DE COMPROMISO:

URLs de Descarga

http[:]//194.85.248.176/bins/eh.x86
http[:]//194.85.248.176/bins/eh.mips
http[:]//194.85.248.176/bins/eh.mpsl
http[:]//194.85.248.176/bins/eh.arm4
http[:]//194.85.248.176/bins/eh.arm5
http[:]//194.85.248.176/bins/eh.arm6
http[:]//194.85.248.176/bins/eh.arm7
http[:]//194.85.248.176/bins/eh.ppc
http[:]//194.85.248.176/bins/eh.m68k
http[:]//194.85.248.176/bins/eh.sh4
http[:]//194.85.248.176/bins/eh.86_64
http[:]//194.85.248.176/local.sh
http[:]//194.85.248.176/tshit.sh
http[:]//2.56.59.215/apache2.sh
http[:]//212.192.241.72/lolol.sh

Muestras (SHA256)

ebfc95372427f8b845daff9ff4aebe2451fa78e35a24edd084685f06ba3daee4
57f50f34e6df8ee9006e46b5fe5c4ee11febe9e33b087c809f1384563e9f1d4e
8ebef715ddb0b4e973b2f8c7529f4480b5caa9c4a25f8fd05a7eaacf036cca20
113be1f9db8af2469b82ce1b5d1b0c61c50586567b3898f2b8a614cd6e8f47a8
b4c3c79d148db638f891143a1910c3d17f973c512a719b1f7525a823b14d29a8
d3928d0b6dedce6a083123028e50ba76e1b29666e70a96eec1a7061b7303bf1a
6b463e9f5d9e8edbc235bceb854367b26ed6effb0dee9881a4f4e88a967318d5
d88052c0a76cac7e571870a4e87c5354594c26b4955cd934870dc12d48f129d5
265396023cbbad6b3480b851873ece9fa2f32c63739a7a0ac32d196843080cc8
83566400bdb09c5e2438c0d9ff723c88328ca93f29e648f97088342e239bfa09
af9ac01e9e8cf7064d590044df43adca566521d223662cf5e0e2500badff6998
de01f26209a085eeff8c217782d283640a6226ccf1bd27eefd696658b55d10ba
a4b16a5bf9b6e662050a3c5ff157d7b2f0be301a1f8f5d1359170132b8b22e58
7a47e5b83e3c42df2ab72adf4a041b2e382f61a0ff378f593156353a78c2c702
1bd895ed050ce42d0f39b6baa0b6a454e05eb5bff72290857cb8fb77a9e4b4b9

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

71ca57bbba49aa877f7ded340328342c6e82e3a99720734c8b0de150d44d906c
23b03aa7d1dadd2e71016702f3e1b278b3a2c4f0c7d0cdc272774a428b88d09c
fb7b03e7619d3ac5c4cbadc6b38841b11e3b19214b776073a590b571f91fe51e
3c978e02d21c7c12631d56c41aceb305fc11348a53eed47e29f7ce62ea0da4df
4832cff5666433a784d6ba48a0e400367d25314ef15d08a216b6286226eff342
95e4ac3ae03646cda56d80df80d775ed4bf23f98be42274fb440e7bc0d03ce88
8d390ad5af8d70692bda123b96e9745816ec7893d84682adb6d243619538b9d3
66adea50e0de8e1d664bb18c9f80596d1443b90e9ba57a59425720886a0c97e0
a87b502575d0db1b6257f1cf75edf4894bc84598f79148525b5cc449d143a495

VII. RECOMENDACIONES:

El Centro de Respuesta a Incidentes Informáticos EcuCERT, recomienda:

- Cambie la(s) contraseña(s) de administrador predeterminadas en sus dispositivo proveedor de servicios de internet (enrutador doméstico), la contraseña debe ser robusta, de 20 o más caracteres
- No comparta sus contraseñas de cualquier tipo con ningún individuo.
- Instale actualizaciones de seguridad y firmware disponibles lo antes posible en sus dispositivos proveedores de internet, únicamente desde sitios oficiales.
- Verifique su configuración de DNS con regularidad
- Activar firewalls que a menudo están deshabilitados de forma predeterminada en los enrutadores domésticos
- Desactive todas las funciones de administración remota de su dispositivo proveedor de internet.
- Desactive las funciones de UPnP y WPS en su enrutador doméstico, si no los está utilizando
- Si su enrutador está desactualizado, y llegó al final de su vida útil junto con finalización de soporte técnico oficial, reemplácelo por uno nuevo
- De ser el caso, verifique que todas las recomendaciones descritas con anterioridad, sean ejecutadas en los enrutadores domésticos entregados por su proveedor de servicio de internet (ISP) contratado.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	09F-202112091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
Versión:	1.0	**ALERTAS DE SEGURIDAD**	
Fecha:	09-dic-2021	**BOTNET DARK MIRAI PONE EN LA MIRA A POPULAR ENRUTADOR DE LA MARCA TPLINK PARA EJECUCIÓN DE RCE**	

VIII. REFERENCIAS:

- Bill Toulas (9 de Dic de 2021). Obtenido de https://www.bleepingcomputer.com/news/security/dark-mirai-botnet-targeting-rce-on-popular-tp-link-router/
- Kamilló Matek (12 de Nov de 2021). Obtenido de https://k4m1ll0.com/cve-2021-41653.html
- Joie Salvio (8 de diciembre de 2021). Obtenido de https://www.fortinet.com/blog/threat-research/manga-aka-dark-mirai-based-campaign-targets-new-tp-link-router-rce-vulnerability