BOLETÍN DE ALERTA

Boletín Nro.: 2016-13
Fecha de publicación: 31/10/2016
Tema: Botnet Mirai y otras amenazas a dispositivos conectados a Internet (IoT)

Sistemas afectados:

- Dispositivos que se conectan a Internet, tales como cámaras de CCTV, DVRs, routers, impresoras, SMART TV, etc., denominados normalmente como IoT (*Internet of Things* - "Internet de las cosas")

Descripción:

Días atrás, una serie de ataques de Denegación de Servicio Distribuido (DDoS) causó una interrupción generalizada de muchos servicios sobre Internet. Los ataques estaban dirigidos al Sistema de Nombres de Dominio (DNS), específicamente a los servidores de la empresa Dyn, uno de los proveedores más importantes de servicios de DNS para empresas. Esto causó que muchos servicios como Twitter, Whatsapp, Github, Paypal, Spotify y muchos otros portales web se vieran afectados y/o fueran interrumpidos por ciertos períodos de tiempo. Se registraron picos de tráfico de hasta 1.5 Tbps. Previo a este ataque, se observaron otros ataques muy similares.
Un análisis de estos ataques determinó que los mismos fueron causados por botnets de dispositivos IoT, principalmente cámaras de CCTV, DVRs y routers. y infectados con el código malicioso, un malware llamado Mirai. Se calcula que el tamaño de la botnet alcanzó los 380.000 equipos infectados, distribuidos en más de 164 países. Se detectaron 780 IPs de Paraguay entre ellas.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

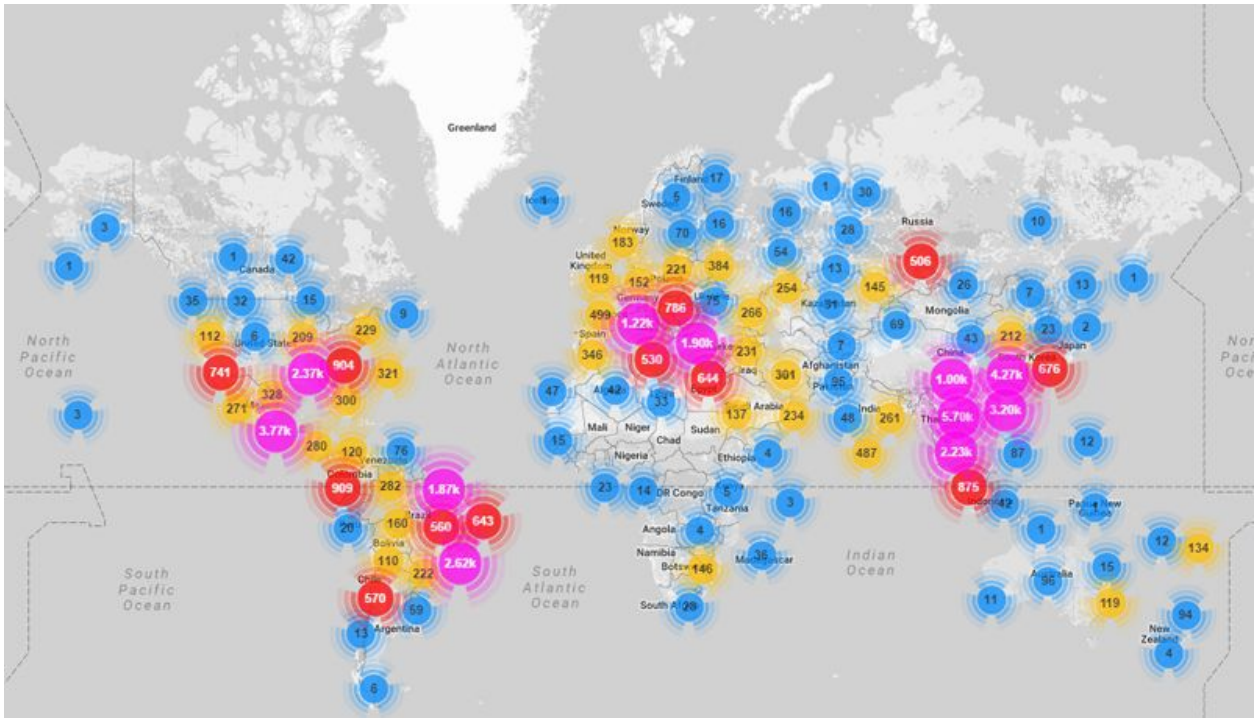

Figura 1: Mapa geográfico de equipos infectados por Mirai detectados por la empresa Imperva

El código fuente del malware Mirai ha sido publicado en Internet días atrás.

El propósito de Mirai es ejecutar ataques de denegación de servicio distribuidos, comandados por un servidor comando y control (C&C) remoto, así como también localizar y comprometer otros dispositivos IoT para aumentar el tamaño de la botnet. El malware cuenta con una lista de 62 usuarios y contraseñas comunes, con las cuales intenta acceder a los dispositivos. Muchos dispositivos IoT se encuentran completamente o pobremente protegidos, expuestos a Internet, con contraseñas por defecto o débiles, permitiendo una infección fácil. Las combinaciones que el malware prueba son:

```
root      xc3511
root      vizxv
root      admin
admin     admin
root      888888
root      xmhdipc
root      default
root      juantech
root      123456
root      54321
support   support
root      (none)
admin     password
root      root
root      12345
user      user
admin     (none)
root      pass
admin     admin1234
root      1111
admin     smcadmin
admin     1111
root      666666
root      password
root      1234
root      klv123
Administrator admin
service   service
supervisor supervisor
guest     guest
guest     12345
guest     12345
admin1    password
administrator 1234
666666    666666
888888    888888
ubnt      ubnt
root      klv1234
root      Zte521
root      hi3518
root      jvbzd
root      anko
```


CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

```
root     zlxx.                root     realtek              admin    7ujMko0admin
root     7ujMko0vizxv         root     00000000             admin    1234
root     7ujMko0admin         admin    1111111              admin    pass
root     system               admin    1234                 admin    meinsm
root     ikwb                 admin    12345                tech     tech
root     dreambox             admin    54321                mother   fucker
root     user                 admin    123456
```

Una vez que el malware Mirai logra acceder al equipo, lo infecta y establece comunicación con el servidor C&C, el cual le podrá brindar instrucciones para el ataque. Es capaz de ejecutar varios tipos de ataques de denegación de servicio, de diversas capas: inundación HTTP, GRE IP y GRE ETH, SYN, ACK, STOMP (Simple Text Oriented Message Protocol), DNS y UDP.
Además, el dispositivo infectado escanea un amplio rango de IPs al puerto 48101/TCP, de modo a detectar dispositivos accesibles desde Internet, mediante Telnet.
Se ha observado la aparición de varios códigos maliciosos similares, como por ejemplo *Bashlite*, cuyo código fuente todavía no se conoce, sin embargo se calcula que ha infectado alrededor de 1 millón de dispositivos de manera similar a Mirai.

Impacto:
El malware Mirai y similares pueden comprometer diversos tipos de dispositivos IoT tales como cámaras de CCTV, DVRs, routers, entre otros, pudiendo ser utilizados para ataques de denegación de servicio distribuidos (DDoS), escaneos masivos para identificar otros dispositivos vulnerables, así como otros tipos de ataques.
Los ataques de denegación de servicio pueden interrumpir la comunicación de servicios de Internet.
Además, los dispositivos infectados podrían sufrir una sobrecarga de procesos y/o de tráfico, afectando su normal funcionamiento.

Mitigación y Prevención:

En caso de observar indicadores de compromiso de Mirai en algún dispositivo conectado a Internet y/o tener un dispositivo conectado a Internet con puertos expuestos a Internet y con credenciales por defecto o contraseñas fáciles, se recomienda seguir los siguientes pasos:

- Desconectar el dispositivo de su red y de Internet
- Realizar un reboot o reseteo del dispositivo. Debido a que el malware Mirai se aloja en la memoria dinámica del dispositivo, el reseteo lo eliminará

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- Cambiar la contraseña del equipo, evitando utilizar la contraseña por defecto o contraseñas débiles. Se recomienda contraseñas de no menos de 10 ~ 12 caracteres, combinación de minúsculas, mayúsculas, números y caracteres especiales, evitando palabras o nombres comunes o predecibles.
- Reconectar el dispositivo a la red. Es importante no reconectar el dispositivo antes de haberlo reseteado y cambiado la contraseña.

Puede utilizar la siguiente herramienta para verificar si se ha observado actividad de Mirai desde su IP: https://www.cert.gov.py/index.php/consultar-ip

Obs.: Esta herramienta utiliza datos de terceros y sólo registra la actividad observada en operaciones de *sinkholing*, por lo que es posible que la IP de un equipo infectado puede no estar registrada como maliciosa. Además, en el caso de utilizar IPs dinámicas, es posible que un registro de actividad maliciosa no corresponda a su equipo.

De modo a prevenir infecciones y ataques similares en un futuro, se recomienda seguir las siguientes buenas prácticas:

- Cambiar siempre las contraseñas por defecto y utilizar siempre contraseñas seguras para cualquier dispositivo
- Mantener actualizado el firmware de los dispositivos y aplicar los parches de seguridad disponibles.
- Desactivar Universal Plug and Play (UPnP) en los router u otros dispositivos, a menos que sea absolutamente necesario.
- Monitorear los intentos de acceso a su dispositivo, así como los puertos de administración/gestión, incluidos, pero no limitado a: 22, 23, 80, 81, 443, 8080, 9090, 2323, 48101, etc. En caso de no necesitar administrar remotamente el dispositivo, desactivar la misma o restringirla a ciertas IPs.

Cualquier equipo que transmite datos y/o que puede ser operado remotamente, es un potencial blanco a este tipo de ataques: cámaras, Smart TVs, dispositivos médicos, etc. Es importante conocer cómo funcionan estos equipos, cómo se conectan y qué características de seguridad ofrecen. Evitar

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

equipos que no ofrezcan características mínimas de seguridad, tales como cambio de contraseña, control de puertos y servicios, actualización de firmware, etc.

Información adicional:

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html
https://www.us-cert.gov/ncas/alerts/TA16-288A

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py