IotRoop/Reaper

Presented by Dyllan Vela

CONTENIDO DE LA PRESENTACION.

Introducción.
¿Fecha de detección del Ataque?
¿Empresa/Grupo que lo detecto?
¿Como funciona el modelo IPS (INTRUSION PREVENTION SYSTEM)?
¿Características principales?
•Inicialización:
•Deshabilitar el malware de la competencia
•Escaneo de vulnerabilidades :
•Comunicación C&C :
•Servidores de control :
¿Modelo y numero de Dispositivos IoT comprometidos?
¿Método de Ataque/Tipo de vulnerabilidad utilizada?
¿Impacto en continuidad de negocios / Motivación ataque?
¿Medidas para evitarlo/contrarrestarlo?
¿Importancia?
¿Reflexiones individuales?
Conclusión.
Bibliografía.

Semenjanzas con otros ataques.

Mirai

Fue un ataque de DDoS que explotaba vulnerabilidades de contraseñas empleadas por default, y tambien contraseñas debiles en seguridad

IotRoop

Es la version mejorada de Mirai, debido a que no solo explora las contraseñas empleadas por default, tambien aprovecha las vulnerabilidades de software.

INTRODUCIÓN

Aunque aun no se sabe cual es el verdadero objetivo de esta red, con esta investigacion buscaremos aclarar ese punto y verificar a que medio se orienta mas, si al mal o simplemente una advertencia para mejorar la seguridad de nuestros iot

Deteccion de la botnet Iotroop

El malware y botnet, denominado IOTroop, fue descubierto en septiembre del año 2017, por investigadores de Check Point, quienes advirtieron que el 60 por ciento de las redes corporativas tienen al menos un dispositivo vulnerable.

Como es el codigo de Iotroop

Si bien este malware parece compartir parte del código de Mirai, es un malware y una campaña nuevos, y más potentes.

Este malware tiene un rango de vulnerabilidades mayor, por lo que puede afectar a más productos.

No solamente se explotan credenciales por defecto para comprometer dispositivos, además utilizan más de una docena de vulnerabilidades para obtener acceso a los mismos.

Checked Point Research

Proporciona inteligencia líder sobre amenazas cibernéticas a sus clientes

El equipo de investigación recopila y analiza datos de ataques cibernéticos globales

El equipo de más de 100 analistas e investigadores que cooperan con otros proveedores de seguridad

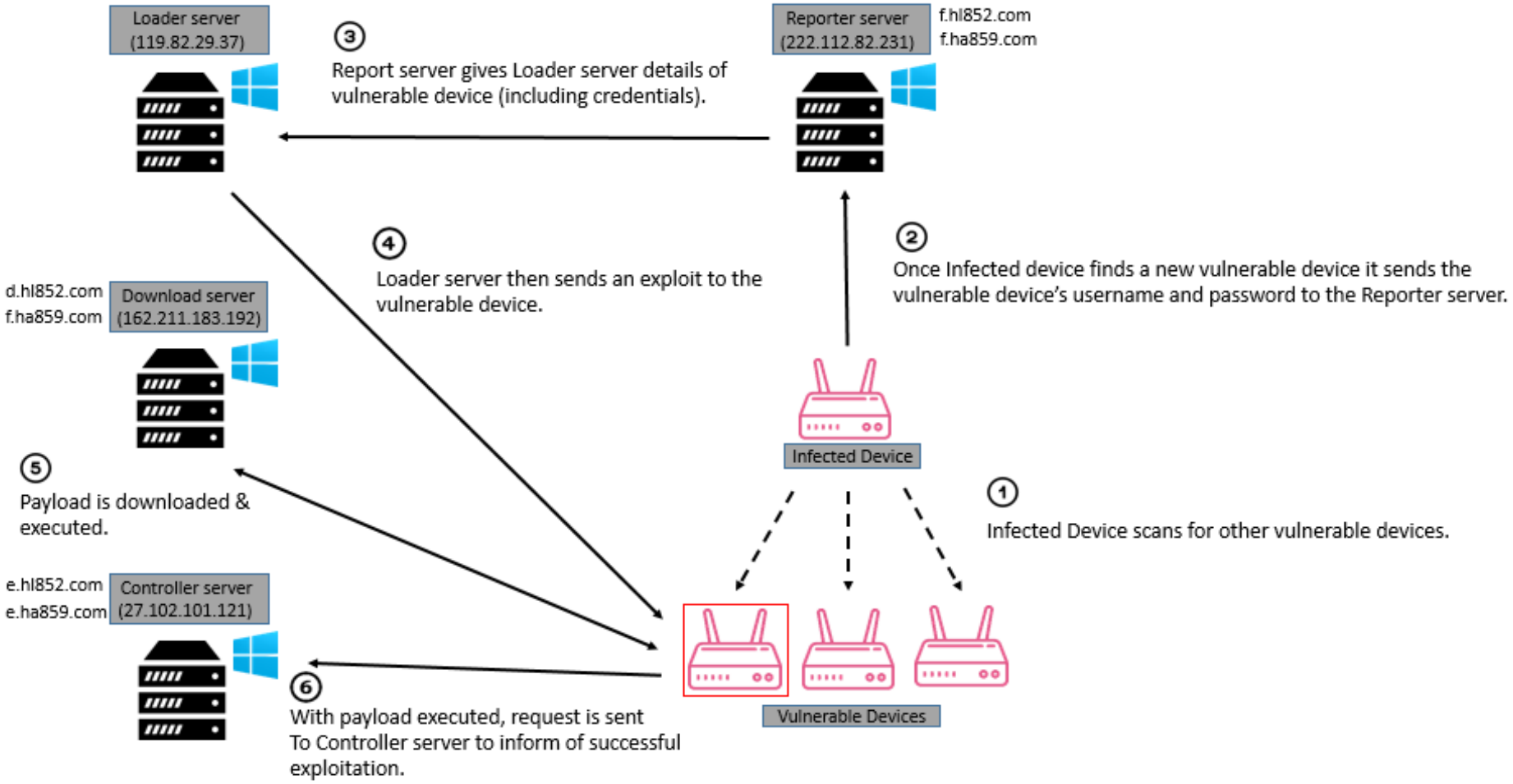
impulsan el descubrimiento de nuevas amenazas cibernéticas

Ayudan a mantenerse a la vanguardia de los piratas informáticos y las amenazas cibernéticas más recientes.

Gracias a la red de sensores web de Check Point, descubrieron una nueva y masiva botnet de IoT, 'IoTroop'

Infraestructura principal

Diagrama de la infraestructura de propagación de malware



Caracteristicas principales.

01. Inicialización.

Incluye la inicialización de cadenas ofuscadas, la prevención de un reinicio por parte del sistema de seguridad del sistema, la garantía de que solo se ejecuta un loTroop a la vez

02. Matar a la competencia.

Incluida la eliminación de cualquier proceso de telnet abierto mediante el puerto TCP/23 y el escaneo de la memoria del dispositivo en busca de cadenas existentes que utilizan otros malware de IoT, eliminándolos en el proceso.

03. Escaneo de vulnerabilidades

La botnet IoTroop genera direcciones IP aleatorias utilizando un código idéntico al de Mirai durante este paso.

04. Comunicación C&C.

El servidor de informes recopila una lista de todos los dispositivos vulnerables después de haberlos escaneado en busca de debilidades.

05. Servidores de control.

Estos dispositivos infectados extraen constantemente los comandos disponibles del servidor de C&C de control.

Mapa de vizualizacion de botnet al inicio del despliegue.

Funcionamiento IPS.

Eficiencia.

Baja tasa de falsos positivos, facil de instalar.

01

Seguridad.

Miles de firmas de seguridad asociadas, y protección preventiva de comportamientos maliciosos

02

Unidad.

Diversidad de motods para habilitar checkpoint.

03

Proteccion.

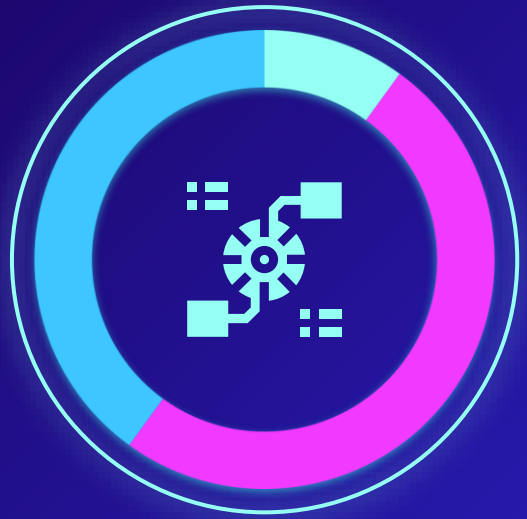
Respaldo de mas de 100 analistas y empresas asociadas.

04

Dispositivos afectados.

Device or I/S	Vulnerability
WIFICAM	https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
DLINK DIR-600	http://www.s3cur1ty.de/m1adv2013-003
DLINK DIR-8	https://blogs.securiteam.com/index.php/archives/3364 https://embedi.com/blog/enlarge-your-botnet-top-d-link-routers-dir8xx-d-link-routers-cruisin-bruisin;https://github.com/embedi/DIR8xx_PoC
NetGear	https://blogs.securiteam.com/index.php/archives/3409
VACRON	https://blogs.securiteam.com/index.php/archives/3445
NetGear DGN1000	http://seclists.org/bugtraq/2013/Jun/8
Linksys	http://www.s3cur1ty.de/m1adv2013-004
Avtech	https://github.com/Trietptm-on-Security/AVTECH
JAWS Web Server	https://www.pentestpartners.com/blog/pwning-cctv-cameras/

Impacto en el negocio.



El sector de la tecnología experimentó un aumento del 70% en el volumen total de ataques.

Interupcion de servicios

Deterioro intencionado y temporal de la disponibilidad de la información

Sabotaje

Deterioro intencionado de los sistemas de información o los servicios de información, incluyendo su eventual destrucción.

Robo de informacion.

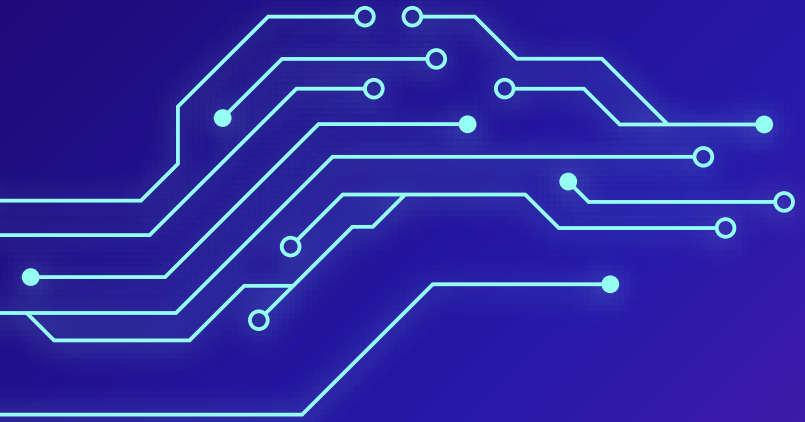
Copiado o eliminación de la información, afectando a su confidencialidad

2 MILLONES

2 MILLONES DE DISPOSITIVOS INFECTADOS CON ESTA BOTNET.

20,000

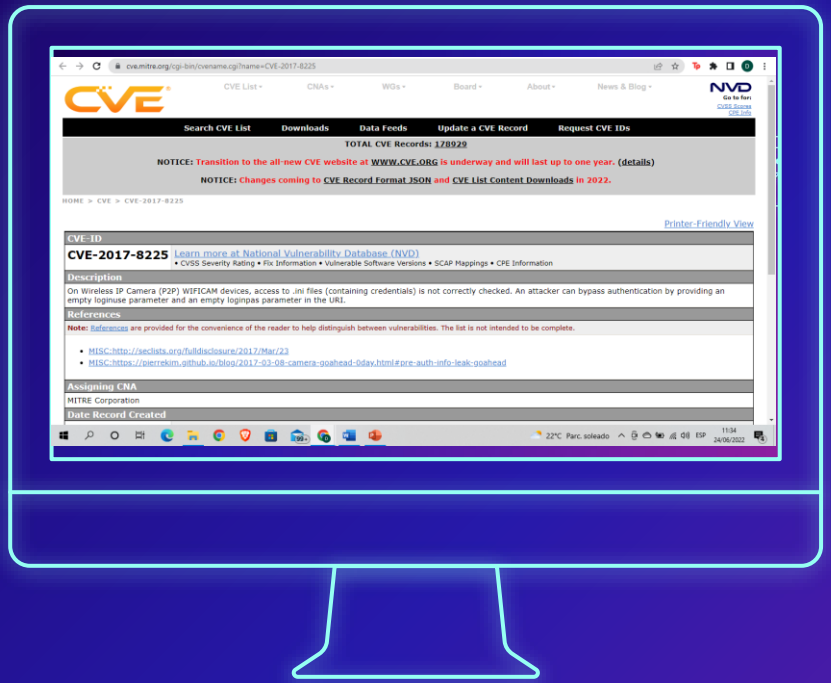
Dispositivos infectados y controlados por C2



10,000

Bots controlados diarios por medio de C2

Debilidad mas explotada.



El primer script utiliza una consulta de Shodan para volcar todas las direcciones IP que son dispositivos vulnerables a CVE-2017–8225 mediante el uso de una (consulta) conocida de Shodan

Como protegernos.

- Investiguen minuciosamente a los proveedores que instalarían hardware o software en su sistema, que estos proveedores externos sean confiables, cumplan y, sobre todo, sean cuidadosos.
- Mantenga los sistemas actualizados, busque siempre actualizar el firmware de fuentes confiables.
- Mejore la seguridad de sus contraseñas y modifique los parámetros default de equipo.

Importancia.

En este momento, Reaper es una lección objetiva para los fabricantes de IoT y los investigadores de seguridad. Es como una luz roja gigante que parpadea en nuestras caras todos los días advirtiéndonos que será mejor que descubramos cómo solucionar la seguridad de IoT pronto.

Refelxiones individuales.

THANKS

Preguntas, puede realizarlas al correo:
19005889@galileo.edu
+502-4768-9551
Dyllan_vela77