Universidad Galileo
Post-Grado Internet De Las Cosas.
Fundamentos de IOT Security I .
Dyllan Vela 19005889
24/06/2022

Investigación Final
IotRoop.

Contenido

Introducción.

En esta investigación buscaremos comprender de manera clara cómo funciona un ataque de seguridad de IOT el nombre del ataque que buscaremos comprender se llama IOTROOP o también conocido como Iotroop/Reaper que es una red de ataque muy similar a la red de mirai solo que con esteroides, veremos porque es más fuerte que mirai, también buscaremos resolver las interrogantes de cómo se produjo, que datos se vieron comprometidos, y la manera en que afecta el ataque a los negocios, veremos los métodos de mitigación del ataque también conoceremos como fue detectado y veremos algunas opiniones de algunos técnicos del área de informática, vamos a conocer detalles de su forma de operar y como fue que se propago mediante que vulnerabilidades y métodos aprovecho para ser posible el ataque, sin más que agregar, procedamos a la investigación.

¿Fecha de detección del Ataque?

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.

Al igual que Mirai, el malware se dirige a dispositivos conectados a la red mal protegidos, como enrutadores y cámaras IP inalámbricas fabricadas por D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys, Synology y GoAhead.

Hasta ahora, se estima que más de un millón de organizaciones ya se han visto afectadas en todo el mundo, incluidos EE. UU., Australia y todos los lugares intermedios, y el número no hace más que aumentar, según la investigación preliminar de Check Point publicada en ese momento.

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. La diferencia más interesante entre este malware y Mirai es que IOTroop es mucho más sofisticado, debido a que no solamente se explotan credenciales por defecto para comprometer dispositivos, además utilizan más de una docena de vulnerabilidades para obtener acceso a los mismos.

Los investigadores dijeron que se ha encontrado una gran cantidad de servidores C&C (Command and Control) manejados por los atacantes detrás de este malware, el cual actualiza el rango de direcciones IP a atacar de manera constante.

Cada dispositivo afectado genera un rango de direcciones IP, las cuales son utilizadas para escanear vulnerabilidades. Este malware tiene la característica de auto propagación con la intervención mínima del C&C. Se continúan realizando estudios e ingeniería inversa para conocer mejor el funcionamiento del mismo.

Los signos siniestros se detectaron por primera vez a través del Sistema de prevención de intrusiones (IPS) de Check Point en los últimos días de septiembre. Los piratas informáticos estaban haciendo un número cada vez mayor de intentos de explotar una combinación de vulnerabilidades encontradas en varios dispositivos IoT.

Botnets como Mirai, IoTroop y Echobot han avanzado en automatización, mejorando las capacidades de propagación. Mirai e IoTroop también son conocidos por propagarse a través de los ataques de IoT, luego se propagan a través del escaneo y la posterior infección de los hosts identificados.

¿Empresa/Grupo que lo detecto?

Check Point Research proporciona inteligencia líder sobre amenazas cibernéticas a los clientes de Check Point Software y a la comunidad de inteligencia en general. El equipo de investigación recopila y analiza datos de ataques cibernéticos globales almacenados en ThreatCloud para mantener a raya a los piratas informáticos, al tiempo que garantiza que todos los productos de Check Point estén actualizados con las protecciones más recientes. Desde el momento en que se inicia una brecha, ThreatCloud comienza a compartir datos en toda la red, proporcionando a los investigadores la inteligencia que necesitan para analizar en profundidad e informar sobre los ataques. Las publicaciones de Check Point Research y el intercambio de inteligencia impulsan el descubrimiento de nuevas amenazas cibernéticas y el desarrollo de la comunidad internacional de inteligencia de amenazas para mantenerlo seguro.

El equipo de investigación consta de más de 100 analistas e investigadores que cooperan con otros proveedores de seguridad, las fuerzas del orden público y varios CERT. Sus fuentes de datos incluyen fuentes abiertas, la red ThreatCloud y la inteligencia de la web oscura. Internamente, el equipo ha desarrollado sus propios módulos de aprendizaje automático, detección de anomalías, ingeniería inversa y técnicas de búsqueda de campañas que ayudan a mantenerse a la vanguardia de los piratas informáticos y las amenazas cibernéticas más recientes.

¿Como funciona el modelo IPS (INTRUSION PREVENTION SYSTEM)?

Los sistemas de prevención de intrusiones detectan o previenen los intentos de explotar las debilidades en sistemas o aplicaciones vulnerables, protegiéndolo en la carrera para explotar la última vulnerabilidad de última hora. El sistema de prevención de intrusiones (IPS) de Check Point proporciona una próxima generación completa, integrada, altas capacidades de prevención de intrusiones de Firewall a velocidades de varios gigabits con alta eficacia de seguridad y una baja tasa de falsos positivos. Protecciones IPS en nuestro Firewall de próxima generación se actualiza automáticamente. Ya sea que la vulnerabilidad se haya lanzado hace años u hoy, su organización está protegida.

Nuestro enfoque de defensa en profundidad combina firmas, validación de protocolos, detección de anomalías, análisis de comportamiento y otros métodos para proporcionar los niveles más altos de protección IPS de red. Check Point IPS proporciona cobertura completa contra amenazas para vulnerabilidades en clientes, servidores, sistemas operativos y aplicaciones ampliamente disponibles, como lectores de PDF y navegadores que son los objetivos preferidos de los actores de amenazas.

¿Características principales?

El malware IoTroop es la muestra principal utilizada en la campaña y se implementa como una carga útil de primera etapa. Comparte una extensa base de código con el código fuente filtrado de Mirai que se puede encontrar en varios recursos en línea.

Según la investigación completa de Check Point Research (se abre en una pestaña nueva), la botnet IoTroop se puede dividir en varias partes distintas, que incluyen:

- **Inicialización:** durante esta parte del ataque, IoTroop sigue un patrón similar al de Mirai, que 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 IoTroop a la vez, la ocultación del nombre del proceso, etc. .
- **Deshabilitar el malware de la competencia:** después de la inicialización, IoTroop comienza a ejecutar su propia funcionalidad única, 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.
- **Escaneo de vulnerabilidades :** la botnet IoTroop genera direcciones IP aleatorias utilizando un código idéntico al de Mirai durante este paso.
- **Comunicación C&C :** el servidor de informes recopila una lista de todos los dispositivos vulnerables después de haberlos escaneado en busca de debilidades.
- **Servidores de control :** estos dispositivos infectados extraen constantemente los comandos disponibles del servidor de C&C de control. Una vez que se recibe un comando, el dispositivo lo analiza para buscar "código" como la acción a realizar, lo que da como resultado una descarga simple o una descarga seguida de ejecución.
    - Descargando
    - Ejecución

La botnet IoTroop, que comparte una amplia base de código con el código fuente filtrado de Mirai, puede causar incluso más daño que su predecesor. Aún se desconoce el propósito de esta botnet, pero lo que sí sabemos es que los dispositivos de más de doce fabricantes son actualmente vulnerables, mientras que más del 60 por ciento de las empresas tienen al menos un dispositivo en su red que está en riesgo.

Si bien esto puede ser una amenaza emergente de millones de ataques realizados, los métodos de infección ya están siendo prevenidos por Check Point IPS. La vulnerabilidad enumerada ha sido cubierta y actualmente se están monitoreando los dispositivos en busca de nuevas variantes.

¿Modelo y numero de Dispositivos IoT comprometidos?

En su informe, Check Point advirtió que un millón de dispositivos IoT ya estaban infectados con el malware IOTroop y que el 60 % de las redes corporativas contenían un dispositivo vulnerable a una de varias vulnerabilidades explotables por los adversarios detrás del malware. NewSky Security dijo que los atacantes han ido más allá de reclutar bots y están desarrollando activamente scripts de ataque.

El malware IOTroop se dirige a dispositivos conectados mal protegidos, como enrutadores y cámaras IP inalámbricas fabricadas por D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys, Synology y GoAhead. Pero debido a que IOTroop no solo explota las credenciales predeterminadas para comprometer los dispositivos, como lo hizo Mirai, tiene el potencial de causar más daño al explotar casi una docena de vulnerabilidades.

El malware realiza un conjunto de pruebas de vulnerabilidad en cada una de las direcciones IP generadas. Estas pruebas localizan vulnerabilidades en cualquiera de los siguientes dispositivos y/o infraestructura:

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/

- Número de dispositivos vulnerables en una cola c2 que esperan ser infectados: más de 2 millones;
- Bots infectados controlados por un c2 en los últimos 7 días: más de 20k;
- Número de bots activos diarios controlados por un c2: alrededor de 10k para ayer (19 de octubre);
- Número de bots en línea simultáneos controlados por un c2: alrededor de 4k

¿Método de Ataque/Tipo de vulnerabilidad utilizada?

En su investigación, Anubhav dijo que revisó dos scripts de IOTroop puestos a disposición por piratas informáticos, incluido uno que explotó CVE-2017–8225 , una vulnerabilidad de autenticación de derivación conocida que afecta a las cámaras IP inalámbricas.

“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) idiota conocida de Shodan”, escribió NewSKy en su informe. “Ahora, una vez que se recopilan todas las direcciones IP vulnerables, el segundo script usa CVE-2017–8225 para volcar las credenciales de estos dispositivos”.

“Esta combinación ayudará a los scripts kiddies a tomar el control de una variedad de dispositivos IoT sin preocuparse por dos cuestiones importantes: dónde (encontrar dispositivos, cuáles pueden ser pirateados) y cómo (hackear estos dispositivos)”, dice el informe.

También se observó que, aunque el hilo en los foros de piratería comenzó primero con secuencias de comandos que revelarían credenciales de IOT comprometidas, pronto se desplazó hacia el desarrollo de una botnet completamente funcional que se puede propagar. Los atacantes discutieron su incapacidad para realizar el comando WGET y lo reemplazaron con un netcat funcional para realizar un shell inverso. Esto también fue observado en dispositivos infectados por IOTroop por investigadores de Check Point y NewSky. La única pieza que falta es la escala. Según Anubhav, 117 055 dispositivos son vulnerables a CVE-2017-8225. Para llegar efectivamente a esos dispositivos, los piratas informáticos necesitaban acceso a Shodan Premium para escalar el reclutamiento y armar dispositivos IoT vulnerables. Anubhav dijo que, si bien la vulnerabilidad CVE-2017-8225 ya se conocía, el uso del motor de búsqueda de Shodan para encontrar dispositivos vulnerables reduce el nivel de un ataque.

Una gran cantidad de dispositivos vulnerables a través de CVE-2017-8225 eran simplemente visibles en Shodan, esperando ser atacados. Sin ningún tipo de seguridad o parche, ahora son vulnerables para convertirse en parte de la botnet IoTroop, dijo Anubhav. Los atacantes pueden actualizar fácilmente el script e instruir fácilmente a la botnet para que realice cualquier tarea. Esta poderosa configuración brinda a los atacantes un control flexible y dinámico de los dispositivos infectados, lo que les permite apuntar fácilmente a cualquier cosa con un código de ataque personalizado y actualizable, y alterar el comportamiento del malware sin actualizar el binario en sí.

¿Impacto en continuidad de negocios / Motivación ataque?

Mark Thomas, que dirige el Centro de Inteligencia de Amenazas Globales de NTT Ltd., comenta: “El sector de la tecnología experimentó un aumento del 70% en el volumen total de ataques. El aumento de los ataques de IoT también contribuyó a este aumento y, si bien ninguna actividad dominada por un único botnet, vimos volúmenes significativos de actividad tanto de Mirai como de IoTroop.

Algunos de los puntos mas importantes y que pueden ser de mucho riesgo para la continuidad de servicio de las empresas son las siguientes:

- Interrupción de servicios: Deterioro intencionado y temporal de la disponibilidad de la información, los sistemas de información o los servicios de información.
- Sabotaje: Deterioro intencionado y a largo plazo de la disponibilidad de la información, los sistemas de información o los servicios de información, incluyendo su eventual destrucción.
- Manipulación de la información: Alteración intencionada de la información, con pérdida de su integridad.
- Robo de información: Copiado o eliminación de la información, afectando a su confidencialidad.
- Espionaje: Menoscabo de la confidencialidad de la información, generalmente protagonizado por actores estatales o patrocinados por Estados, que copian o eliminan información.
- Manipulación de sistemas: Acciones de deterioro de sistemas o servicios de información, orientadas a atacar la confidencialidad o integridad de la información o los sistemas, pudiéndose utilizar para perpetrar otros ataques.
- Amenazas híbridas: Acciones coordinadas y sincronizadas -con origen, habitualmente, en Estados y elementos patrocinados por Estados-, que atacan deliberadamente vulnerabilidades sistémicas de otros Estados y/o sus instituciones, a través de una amplia gama de medios y en distintos sectores-objetivo: políticos, económicos, militares, sociales, informativos, infraestructuras y legales, utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos.

¿Medidas para evitarlo/contrarrestarlo?

Todas las empresas deben prepararse para un ataque como este en sus dispositivos a través de los siguientes pasos críticos:

- Sepa con quién está trabajando: Atrás quedaron los días de los dispositivos empresariales conectados creados internamente por los departamentos de TI: con cada dispositivo emergente cada vez más inteligente, las empresas subcontratan el desarrollo y el mantenimiento de estos dispositivos cada vez más complejos a terceros. Debido a esto, es imperativo que estas empresas investiguen minuciosamente a los proveedores que instalarían hardware o software en su sistema. Dejar estas funciones en manos del proveedor inherentemente abre a una empresa a las vulnerabilidades, por lo que debe asegurarse de que estos proveedores externos sean confiables, cumplan y, sobre todo, sean cuidadosos.
- Mantenga los sistemas actualizados : las empresas deben auditar todos los dispositivos existentes en su red para crear una imagen clara y completa de todo su sistema de defensa. Esto puede parecer básico, pero a menudo son los pasos más rudimentarios que las personas pasan por alto, lo que deja a sus empresas susceptibles a una gran cantidad de amenazas. Cada dispositivo debe actualizarse individualmente y verificar que esté ejecutando los sistemas de defensa más actualizados. Esto es especialmente importante para los dispositivos conectados a IoT, ya que los fabricantes de estos productos no siempre son claros al comunicar actualizaciones o amenazas. Hasta que los productores de estos dispositivos desarrollen una forma más consistente de comunicarse con los usuarios, el departamento de TI tiene la responsabilidad de mantener estos sistemas actualizados.
- No olvide los conceptos básicos: Mirai pudo usar tácticas relativamente simples para atacar a millones de dispositivos porque muchas de sus credenciales predeterminadas nunca se cambiaron durante la implementación. Nuevamente, este es un paso básico, pero uno que fácilmente puede pasarse por alto. Independientemente de si un dispositivo está conectado a una red, es necesario cambiar y actualizar periódicamente sus contraseñas e inicios de sesión. No hacer esto con la suficiente constancia hace que los dispositivos sean susceptibles tanto a los bots grandes como a otros actores maliciosos que buscan atacar a una empresa y su propiedad intelectual.

¿Importancia?

La razón por la que Reaper se ha vuelto tan grande y, sinceramente, la razón por la que estamos tan impresionados con su construcción es que, a diferencia de sus predecesores, Mirai y Persirai, Reaper usa múltiples vectores de ataque. Mirai usó contraseñas predeterminadas.

Reaper casi se jacta al ni siquiera intentar descifrar la contraseña y, en cambio, simplemente explota diferentes vulnerabilidades (RCE, shells web, etc.) en nueve dispositivos de proveedores de IoT diferentes.

A diferencia de muchos de los dispositivos que infecta, Reaper tiene un mecanismo de actualización. Si no fuera malicioso, podría calificar para cumplir con los estándares de los nuevos requisitos federales de la " Ley de mejora de la seguridad cibernética de Internet de las cosas (IoT) de 2017 ". Diablos, los autores podrían incluso hacer una distribución y podría convertirse en la plataforma de administración remota predeterminada para IoT.

Hasta ahora, no se ha visto a Reaper atacando a nadie con ataques DDoS volumétricos masivos. Sí, eso es algo bueno. Al menos uno de nosotros piensa que nunca podría ser visto atacando a nadie. Si Reaper comenzara a usarse como el arma definitiva de la Estrella de la Muerte, eso abarataría su valor. También daría lugar a campañas activas de eliminación.

Si Reaper comienza a atacar a las personas con DDoS, pasará de ser una maravilla de la ingeniería de infraestructura de los bots a otra herramienta de ataque volumétrico. Los pastores de bots serían perseguidos por las fuerzas del orden (al estilo del caso Mirai 3) y el bot se desmontaría.

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.

Si Reaper no ataca a nadie ni revela sus intenciones, puede entrar en el mismo espacio mítico que ocupó el gusano Conficker de finales de la década de 2000. En su apogeo, Conficker infectó a más de 10 millones Computadoras con Windows y causó gran preocupación porque podría haber causado una gran cantidad de daño. Pero nunca se activó y sigue siendo un estudio en la construcción de bots.

La lección obvia es que el estado de la seguridad de IoT todavía es increíblemente pobre, y necesitamos hacer un mejor trabajo de modelado de amenazas Internet de cosas.

¿Reflexiones individuales?

Como reflexión individual, puedo argumentar que este tipo de ataque son ataques bastantes elaborados, que requieren de demasiada habilidad técnica para llevarse a cabo, me parece que es de suma importancia hacer énfasis en que las violaciones de nuestra privacidad inician principalmente por nosotros mismos, vemos que el punto más fácil para poder vulnerabilizar nuestros dispositivos era por medio de contraseñas predeterminadas, y usuarios igualmente predeterminados, es importante conocer los métodos que utilizar en estos ataques, primero por que al conocer nosotros esos detalles ya podemos armar nuestro propio plan de contingencia, segundo por que al momento de nosotros saber que vulnerabilidades explotaron esos ataques nosotros podemos verificar si en algún punto de nuestra carrera utilizamos dichas configuraciones o quizá dichos puertos de comunicación que fueron vulnerados, me gustaría aplicar bastantes conceptos de los cuales se mencionaron durante la investigación, tales como poder utilizar el servicio de la empresa de checkpoint para resguardar datos, aplicando los conceptos del curso y utilizando la herramienta de CVSS luego de hacer un análisis este es el tipo de amenaza que generan un 10 de alerta según la herramienta, evaluando los criterios que de amenaza que se genera tenemos un riesgo totalmente alto, si evaluamos en cualquier herramienta nos daremos cuenta que tenemos un alto riesgo de seguridad reflejado por este tipo de amenaza, vemos también que según el curso el eslabón más débil de toda red de IOT es el dispositivo final, vemos que la mayoría de dispositivos atacados eran dispositivos finales, por ejemplo cámaras, que es un elemento muy vulnerable, lo cual hace que se pierda toda la privacidad por que sin necesidad de nuestra autorización el atacante puede ver en tiempo real lo que nosotros hacemos día a día y nosotros podemos estar siendo vigilados sin saber, también las ejecuciones de comando a distancia es otro tema el cual es de suma importancia mitigar, por que por medio de comandos pueden bloquear nuestros servicios, me llama la atención que también menciona que hay algunos dispositivos que eran atacados mediante de faltas de procesos de autenticación, donde las aplicaciones permitían el uso de sus recursos sin necesidad de autenticar la información, ahora por supuesto hay muchos conceptos que mitigan esa vulnerabilidad sin embargo puedo decir que hasta el día de hoy yo era una persona que no aplicaba uno de los métodos de autenticación que sería el 2FA, gracias a estas investigaciones pude conocer muchas aplicaciones de como mejorar mis resultados de seguridad en mis dispositivos, ahora ya me creo conciencia de estar verificando los puerto que tengo disponibles y los servicios que no me son útiles para desactivarlos y evitar riesgos de violación de privacidad.

Conclusión.

Esta red de bots se apodero fácilmente de más de 2 millones de dispositivos, es increíble como el tráfico de información por los piratas surge en los blog públicos, siempre bajo un nombre que no tiene sentido pero tiene sus conversaciones como que fuera un proyecto universitario el que están desarrollando, es increíble lo mucho que pueden llegar a dañar los servicios de las empresas y de la misma red de internet, me sorprendió la facilidad con la que se detectó la amenaza y me llamo la atención el nivel de importancia que le dieron, logre comprender que es una amenaza de alto nivel, creo que al leer la investigación se nota que en verdad la categorizan como un monstro de ataque por todas las vulnerabilidades que puede explotar este ataque, me gustó mucho realizar la investigación, ayudo a comprender la importancia de mantener los firmware actualizados y aplicar diferentes métodos de contingencia para frenar ese tipo de ataques.

Bibliografía.

https://research.checkpoint.com/2017/iotroop-botnet-full-investigation/

https://research.checkpoint.com/2017/new-iot-botnet-storm-coming/

https://www.seguridad.unam.mx/botnet-iotroopreaper-podria-superar-la-devastacion-generada-por-mirai

https://threatpost.com/iotroop-botnet-could-dwarf-mirai-in-size-and-devastation-says-researcher/128560/

https://www.computerworlduniversity.es/ciberseguridad/la-cantidad-de-ataques-aumentan-a-medida-que-los-ciberdelincuentes-innovan-mas-rapido-y-automatizan-los-ataques

https://www.checkpoint.com/downloads/products/intrusion-prevention-system-ips-datasheet.pdf

https://www.checkpoint.com/es/

https://research.checkpoint.com/about-us/

https://www.itproportal.com/features/iotroop-botnet-how-to-protect-yourself-from-the-cyber-storm-of-the-century/

https://cyware.com/news/the-mirai-mania-a-brief-look-into-the-notorious-mirai-botnet-and-its-variants-37c443f8

https://threatpost.com/hackers-prepping-iotroop-botnet-with-exploits/128608/

https://www.wirelesswatchdogs.com/blog/why-iotroop-/-reaper-remains-a-persistent-threat

https://www.wirelesswatchdogs.com/blog/why-iotroop-/-reaper-remains-a-persistent-threat

https://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

https://www.first.org/cvss/specification-document

https://www.f5.com/labs/articles/threat-intelligence/reaper-the-professional-bot-herders-thingbot