"EL INTERNET DE LAS COSAS (IOT) COMO VECTOR DE ATAQUES CIBERNÉTICOS E INCIDENTES DE PRIVACIDAD"

The Internet of Things (IoT) As a Vector for Cyberattacks and Privacy Incidents

Recibido: 12 / 09 / 2019 Aprobado: 31 / 10 / 2019

Ingeniero
Felix Uribe
Estados Unidos

El autor es un profesional de la ciberseguridad y la privacidad en la tecnología de la información (TI) con una larga experiencia en los sectores públicos y privados. En el ámbito Académico, es Profesor Asociado Adjunto en el Programa de Política y Gestión de Ciberseguridad de la University of Maryland, Global Campus (UMGC) donde imparte cursos de ciberseguridad, privacidad y cibercriminalidad. En el ámbito gubernamental, actualmente es un Oficial Federal de Privacidad y Analista de Seguridad de TI en el Departamento del Interior de los Estados Unidos. En el Departamento de Justicia de los Estados Unidos, trabajó como auditor de seguridad de TI en la Oficina de Auditoria del Inspector General. En el Departamento de la Administración de la Seguridad Social de los Estados Unidos (SSA) y bajo el auspicio del Consejo de Administración de la Oficina del presidente de los Estados Unidos llevó a cabo la elaboración de los documentos de base para la creación de una Ciber-Academia en ese Departamento.
felix.uribe@faculty.umuc.edu

RESUMEN

El crecimiento exponencial de dispositivos electrónicos que forman lo que hoy se conoce como el Internet de las Cosas (IoT por sus siglas en inglés) y la implementación y uso de estos tanto en instituciones públicas y privadas, así como la ciudadanía en sus hogares, exige abordar las preocupaciones y retos actuales de ciberseguridad y privacidad que afectan la confiabilidad del actual ecosistema del Internet de las Cosas en el mundo.

Palabras clave:
Internet de las Cosas, IoT, dispositivos inteligentes, ciberataques, privacidad.

ABSTRACT

The exponential growth of electronic devices that form what is now known as the Internet of Things (IoT) and the implementation and use of these in both public and private institutions as well as citizens in general in their homes, requires addressing cybersecurity and privacy concerns and challenges that affect the reliability of the current Internet of Things ecosystem in the world.

Keywords:
Internet of Things, IoT, smart devices, cyberattacks, privacy.

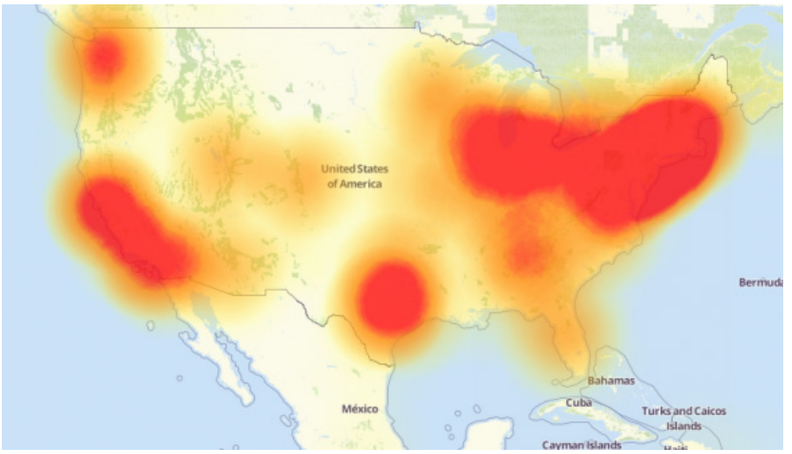
INTRODUCCIÓN

El Internet de las Cosas se usa generalmente para describir aquellos dispositivos electrónicos o electrodomésticos conectados a internet o una red informática. Aunque no existe una definición formal del término, lo describiré personalmente como "la red de dispositivos (cosas) capaces de interactuar con otros dispositivos y/o seres vivos a través de sensores y a través de internet o de una red privada local o global no conectada a internet".

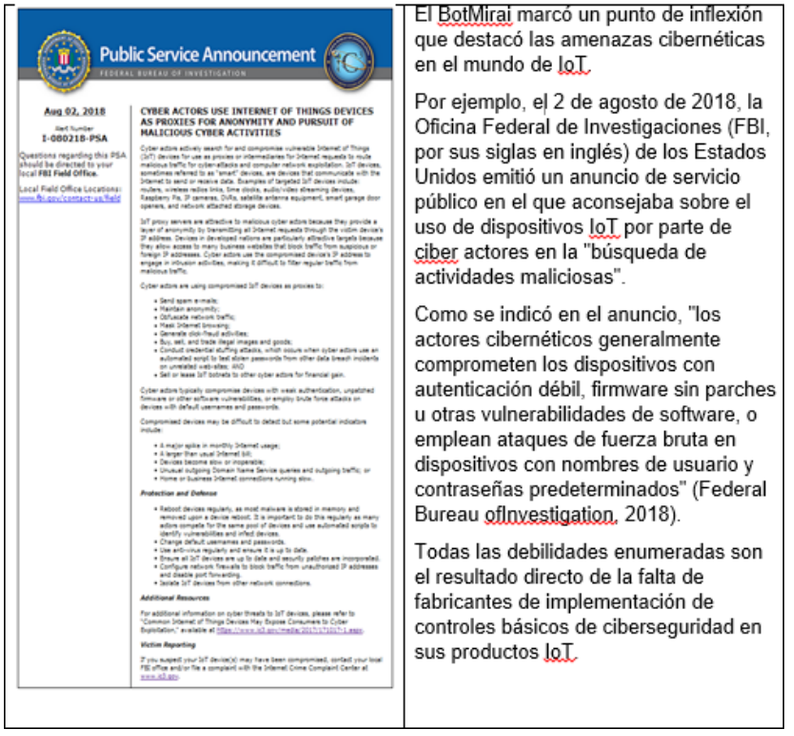
Hay muchas predicciones sobre el crecimiento exponencial de los dispositivos IoT en los próximos años. El rango va de 20 a 30 mil millones de dispositivos conectados a internet para el próximo año (2020) y se espera que siga creciendo en los próximos años. Es obvio que, en un futuro no muy lejano, gran parte del mundo va a estar completamente conectado y lo que llamamos hoy en día "dispositivos IoT" se convertirá en parte de la estructura de este nuevo mundo ciber físico totalmente conectado. Lo que también es obvio es que cuanto más nos conectamos, más nos tenemos que preocupar por los riesgos de ciberseguridad y privacidad.

VECTORES DE CIBERATAQUES

La introducción de miles de millones de nuevos dispositivos inseguros de IoT en la infraestructura actual de internet, abre al mismo tiempo, miles de millones de vectores de ataque a hogares, industrias, organizaciones y cualquier otra infraestructura tocada por esos dispositivos. En 2016, el ahora famoso "MiraiBot", infectó cientos de miles de dispositivos IoT inherentemente inseguros (routers, DVR y cámaras) que se utilizaron para lanzar varios ataques masivos con un récord de denegación de servicio distribuido (DDoS) contra altos objetivos como el sitio web de "Krebs on Security" y el proveedor del sistema de nombres de dominio "Dyn" (adquirido por Oracle en 2016) entre otros. En todos estos ataques, los servicios de internet de la víctima se desactivaron temporalmente (Ragan, 2016). McAfee Labs estimó que 2.5 millones de dispositivos IoT estaban infectados por Mirai a fines de 2016 (Business Wire, 2016).



Este mapa muestra las interrupciones (en rojo) causadas por el BotMiraia la infraestructura Dyn durante el ataque del 2016. Fuente: Downdetector.com


Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Aug 02, 2018

Alert Number
I-080218-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

Local Field Office Locations: www.fbi.gov/contact-us/field

CYBER ACTORS USE INTERNET OF THINGS DEVICES AS PROXIES FOR ANONYMITY AND PURSUIT OF MALICIOUS CYBER ACTIVITIES

El BotMirai marcó un punto de inflexión que destacó las amenazas cibernéticas en el mundo de IoT.

Por ejemplo, el 2 de agosto de 2018, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) de los Estados Unidos emitió un anuncio de servicio público en el que aconsejaba sobre el uso de dispositivos IoT por parte de ciber actores en la "búsqueda de actividades maliciosas".

Como se indicó en el anuncio, "los actores cibernéticos generalmente comprometen los dispositivos con autenticación débil, firmware sin parches u otras vulnerabilidades de software, o emplean ataques de fuerza bruta en dispositivos con nombres de usuario y contraseñas predeterminados" (Federal Bureau ofInvestigation, 2018).

Todas las debilidades enumeradas son el resultado directo de la falta de fabricantes de implementación de controles básicos de ciberseguridad en sus productos IoT.

Anuncio del Servicio Público del FBI. Fuente: https://www.ic3.gov/media/2018/180802.aspx

Con el fin de ayudar y brindar orientación y conciencia a los fabricantes de IoT, algunos gobiernos han tomado la iniciativa de desarrollar guías de IoT que tengan como objetivo proporcionar una base de seguridad mínima de características de ciberseguridad que los fabricantes puedan seguir voluntariamente al desarrollar y fabricar dispositivos de IoT. Como ejemplo, en el Reino Unido, el "Código de Prácticas para la Seguridad de IoT del Consumidor" tiene como objetivo "apoyar a todas las partes involucradas en el desarrollo, fabricación y venta minorista de IoT del consumidor con un conjunto de pautas para garantizar que los productos sean seguros por diseño y para facilitar que las personas se mantengan seguras en un mundo digital " (UnitedKingdomDepartmentfor Digital, Culture, Media and Sport, 2018).

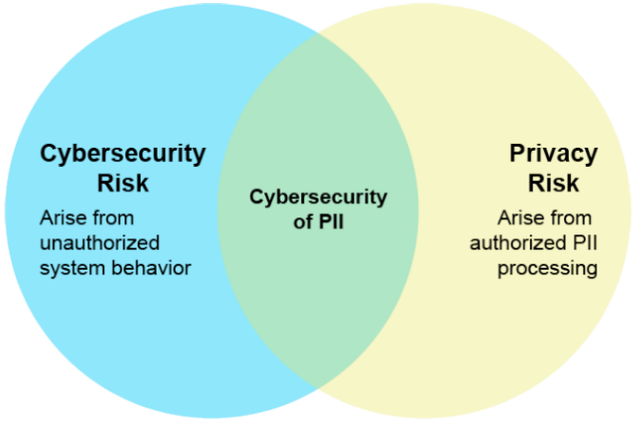
En los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) publicaron recientemente un borrador titulado "Línea de base de la característica de ciberseguridad básica para dispositivos IoT asegurables: un punto de partida para los fabricantes de dispositivos IoT", aunque todavía está en borrador, este documento está "destinado para ayudar a los fabricantes de dispositivos de internet de las cosas (IoT) a comprender los riesgos de ciberseguridad que enfrentan sus clientes para que los dispositivos de IoT puedan proporcionar características de ciberseguridad que los hagan al menos mínimamente asegurables para las personas y organizaciones que los adquieren y usan" (NIST, julio 2019).

Es obvio que hasta que los fabricantes de IoT se pongan al día con la implementación correcta de los controles de ciberseguridad en la fabricación de dispositivos de IoT, corresponde a las organizaciones y a los consumidores estar informados e implementar buenas prácticas de ciberseguridad al comprar e implementar estos dispositivos. Algunas recomendaciones básicas, como evaluar la configuración de seguridad y las características de los dispositivos IoT, el uso de contraseñas seguras y mantener el software actualizado, entre otras cosas, pueden ayudar a prevenir el uso de estos para perpetrar ataques cibernéticos y delitos cibernéticos.

Incidentes de privacidad

El NIST en su publicación titulada "Consideraciones para gestionar los riesgos de privacidad y ciberseguridad de Internet de las Cosas (IoT)" afirma que "el riesgo de ciberseguridad y el riesgo de privacidad están relacionados, pero son conceptos distintos" (NIST, junio 2019). Por un lado, los riesgos de ciberseguridad se refieren a la protección de la confidencialidad, integridad o disponibilidad de la información y el dispositivo IoT, mientras que los riesgos de privacidad se refieren a la protección de datos personales. (NIST).

Desafortunadamente, en el entorno actual, debido a la rápida fabricación y despliegue de dispositivos IoT sin los controles de ciberseguridad adecuados, por una parte, y por otra, el uso erróneo de estos por parte de organizaciones e individuos, a veces conduce a la divulgación no intencional de datos personales.



Relación entre ciberseguridad y riesgos de privacidad.
Fuente: https://csrc.nist.gov/publications/detail/nistir/8228/final

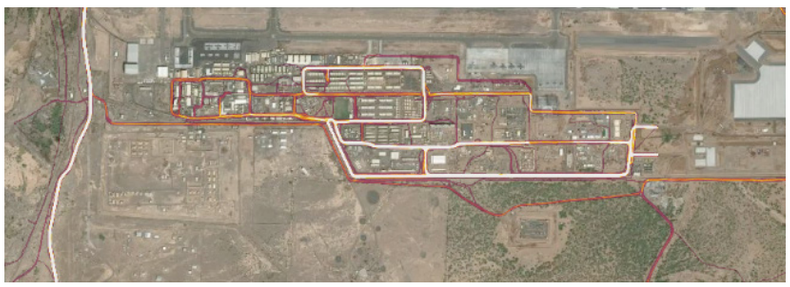
Datos personales como de geolocalización, datos de comportamiento y biométricos, etc., son recopilados por millones de dispositivos IoT en todo el mundo. Un caso interesante que demostró la recopilación masiva y la divulgación involuntaria de datos personales cuando se utilizan dispositivos IoT, es el caso Strava. Strava es una compañía que desarrolló una aplicación móvil que es utilizada por millones de personas para monitorizar sus actividades físicas (trotar, caminar, andar en bicicleta, etc.).

Además, los usuarios del servicio también pueden enviar al sistema sus actividades registradas en otros dispositivos que también monitorizan la actividad física de estos.

La compañía creó lo que se conoce como Strava Global Heatmap. Este "mapa de calor" se crea utilizando billones de puntos de datos

recopilados de los usuarios del servicio y que se visualizan en un mapa que muestra los millones de actividades físicas registradas por la empresa.

Desafortunadamente, en enero del 2018, se descubrió que el mapa mostraba bases militares secretas en todo el mundo (Hsu, 2018). En el mapa, se mostraba claramente cómo las actividades físicas del personal militar revelaron la ubicación de las bases e identificaron rutas de patrulla que se pueden utilizar para resaltar los perímetros de la base.



Campamento base expedicionario naval de los Estados Unidos Lemonnier en Djibouti. Fuente: mapa de calor de Strava.

En respuesta a las revelaciones de Strava, el Pentágono anunció ese mismo año una nueva política que prohíbe el uso de funciones de geolocalización en áreas operativas donde el Ejército está llevando a cabo ciertas misiones.

El caso Strava mostró cómo la recopilación masiva y el uso de los datos recopilados a través de dispositivos IoT Puede causar resultados negativos si se realizan de manera incorrecta. En este caso, la geolocalización anónima de individuos podría haber puesto vidas en peligro al revelar rutas de patrulla.

Otro riesgo de los dispositivos IoT que crea nuevos desafíos de privacidad tanto para los fabricantes como para el consumidor, es la producción de los llamados "juguetes conectados". Como su nombre lo indica, los juguetes tienen la capacidad de comunicarse con el mundo exterior a través de cámaras, micrófonos y otros sensores diseñados para hacer que la experiencia de juego del niño sea más humana. Desafortunadamente, se ha descubierto que algunos juguetes tienen características de recolección de datos muy invasivas que ponen en riesgo la privacidad y la seguridad de los niños.

En un ejemplo clásico sobre la protección de la privacidad de los niños, en 2017, la Agencia de la Red Federal del gobierno alemán (Bundesnetzagentur) emitió una advertencia oficial para aconsejar al público que destruyera una muñeca llamada Cayla, porque la muñeca podría haber sido utilizada por un actor malicioso para hablar y escuchar a cualquier niño jugando con ella (BBC, 2017).

CONCLUSIÓN

Los casos relacionados con los desafíos de ciberseguridad y privacidad presentados en este documento, son solo un ejemplo mínimo de los muchos otros casos que han ocurrido en el pasado y los que vendrán en el futuro cercano. El crecimiento exponencial de los dispositivos IoT y sus aplicaciones cotidianas requiere la implementación de controles de ciberseguridad y privacidad para abordar las preocupaciones de seguridad y privacidad actuales que afectan la confiabilidad del dominio IoT que existe en la actualidad.

Los fabricantes de dispositivos IoT deben tener en cuenta las guías gubernamentales actuales al diseñar y fabricar dispositivos IoT y sus componentes para garantizar que la seguridad y la privacidad se implementen por diseño y no surjan como una ocurrencia tardía durante el ciclo de vida de desarrollo de dispositivos IoT.

A medida que se construyen e introducen millones y millones de dispositivos IoT en el ecosistema del mundo, quiero finalizar con dos recomendaciones: La primera es la creación de "Unidades de Ciberseguridad y Privacidad IoT" en organizaciones públicas y privadas cuya especialización sea exclusivamente el análisis, estudio y la creación de normas para el uso e implementación de esos dispositivos durante el ciclo de vida del producto para garantizar el cumplimiento de los requisitos mínimos de ciberseguridad y privacidad. La segunda, es la creación de unidades especializadas en instituciones gubernamentales y policiacas encargadas de la investigación y la prosecución del ciberdelito donde los dispositivos IoT fueron utilizados para cometer el ciber delito.

REFERENCIAS

Federal Bureau of Investigation. (2018). *Cyber actors use internet of things devices as proxies for anonymity and pursuit of malicious cyber activities.* Recuperado de https://www.ic3.gov/media/2018/180802.aspx

German parents told to destroy Cayla dolls over hacking fears. (2017). *BBC.* Recuperado de https://www.bbc.com/news/world-europe-39002142

Hsu, J. (2018). The strava heat map and the end of secrets. *Wired.* Recuperado de https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

McAfee labs report highlights critical challenges to threat intelligent sharing (2016). *Business Wire.* Recuperado de https://www.businesswire.com/news/home/20170405006423/en/McAfee-Labs-Report-Highlights-Critical-Challenges-Threat

National Institute of Standards and Technology. (2019). *Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers.* Recuperado de https://csrc.nist.gov/publications/detail/nistir/8259/draft

National Institute of Standards and Technology. (2019). *Considerations for managing internet of things (IoT) cybersecurity and privacy risks.* Recuperado de https://csrc.nist.gov/publications/detail/nistir/8228/final

Ragan, S. (2016). *DDoS knocks down DNS, data centers across the U.S. affected.* Recuperado de https://www.csoonline.com/article/3133992/ddos-knocks-down-dns-datacenters-across-the-u-s-affected.html

United Kingdom Department for Digital, Culture, Media and Sport. (2018). *Code of practice for consumer internet of things (IoT) security.* Recuperado de https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security