ATAQUES DDoS EN ENTORNOS IoT

Autor: Miguel Fraile Izquierdo
Director/es: Javier Vales Alonso

I. INTRODUCCIÓN Y CONTEXTO

A lo largo del desarrollo de los cuatro capítulos que conforman el presente trabajo, se trata de exponer y analizar, de forma detallada, diferentes aspectos que se refieren a los ataques de denegación de servicio distribuido (en adelante DDoS) desde el entorno del internet de las cosas (en adelante IoT).

Esta exposición se realiza desde una aproximación histórica a los términos a los que se refiere el título de este trabajo: los ataques de DDoS y el IoT. Entre otras cuestiones, se tratan las características principales del entorno en el que se desarrolla este concepto: la Red, que permite que los ataques de DDoS desde el IoT sean posibles, la forma en la que se establecen las infraestructuras sobre las que se soportan estos mecanismos de ataque, sus rasgos más característicos y sus peculiaridades.

También se presenta un modelo teórico de despliegue de una típica infraestructura de botnet del IoT y, sobre la base del análisis del código fuente de la botnet del IoT por excelencia, *Mirai*, se traslada el citado modelo teórico al plano de la más absoluta realidad, describiéndose el funcionamiento de la citada botnet y presentando algunas de las características más significativas de la botnet que ha resultado ser la base para el desarrollo de nuevas versiones con capacidades mucho más sofisticadas y peligrosas.

Mirai, a través de su evolución y en la forma de sus diferentes versiones, se ha llegado a constituir como uno de los mayores problemas de las compañías de ciberseguridad dedicadas a proporcionar servicios de mitigación ante este tipo de ataques, ya que los ataques de DDoS que han tenido un mayor impacto han sido atribuidos a esta botnet.

Precisamente, en otra de las secciones de este trabajo, se realiza un estudio de los ataques que han sido atribuidos a Mirai, sus características y el impacto que produjeron en las organizaciones que fueron víctima de los mismos.

La citada botnet, basada en dispositivos IoT, se reveló como la principalmente utilizada en los más importantes ataques de DDoS, como el que sufrió el sitio web de Brian Krebs, un importante periodista especializado en seguridad en sistemas de TI, el ataque que afectó a OVH, una empresa francesa de servicios en la nube, o el famoso ataque a Dyn, un importante proveedor de servicios de DNS.

En el trabajo, también se realiza una descripción detallada de las tácticas, técnicas y procedimientos (en adelante TTP) que han sido utilizadas en los ataques de DDoS más significativos, cuya información ha sido publicada por la literatura especializada, y que se han producido desde botnets conformadas por dispositivos del IoT constituidas para realizar ataques de este tipo.

En el documento también se expone la evolución de varios ataques de DDoS reales recibidos por una organización y las reacciones que, ante ellos, llevó a cabo la operadora que prestaba el servicio de mitigación. En esta sección se presenta la secuencia de los ataques, sus características, el tipo de tráfico, TTP empleadas, servicios afectados y el impacto causado a la organización, pero también a la operadora.

El trabajo finaliza con una análisis de las características de las últimas botnets del IoT detectadas, las TTP que están siendo utilizadas, y las que ya no, y en función de esto, la tendencia a la que apuntan este tipo de ciberataques.

II. DESARROLLO Y RESULTADOS

En el primer capítulo, se realiza una aproximación histórica que contextualiza perfectamente esta clase de ciberataques y como afectan de una manera fundamental a los procesos TIC de las organizaciones, ya que las características de los procesos de negocio de las organizaciones modernas, y el proceso de transformación digital en el que estas están inmersas, hace que dichos procesos estén soportados en tecnologías de información y telecomunicaciones que necesitan disponer de las capacidades necesarias para que la infraestructura tecnológica que conforma estos servicios sea lo suficientemente robusta como para soportar este tipo de ataques.

En este capítulo también se desarrollan básicamente los conceptos principales que intervienen en el resto del trabajo, y que sirven para realizar esta contextualización, como es el significado de denegación de servicio distribuido y el de internet de las cosas, y cómo se relacionan ambos en el contexto de los ataques de denegación de servicio.

En el segundo capítulo se desarrolla con detalle el estado del arte de este tipo de ataques, se expone la necesidad de que los dispositivos IoT se encuentren conectados a Internet para ser útiles, se presenta un modelo de interconexión, y se hace referencia a su accesibilidad desde cualquier parte de la Red y, por lo tanto, a los recursos computacionales que ponen a disposición de posibles atacantes.

La publicación del código fuente de *Mirai* marca un punto de inflexión importante en lo referente a la proliferación de nuevas versiones y variantes de esta botnet. En este capítulo se realiza una introducción a *Mirai*, la botnet IoT por excelencia.

A lo largo del desarrollo de este capítulo, se describe el funcionamiento y capacidades de la botnet, deteniéndose en la explicación de algunos de sus aspectos más significativos y características más marcadas, basándose en el estudio de algunas fracciones de su código fuente. Además, se hace referencia a su atribución respecto a los ataques de DDoS más significativos, se realiza un extenso desarrollo sobre los mismos, se realiza una clasificación y se exponen las TTPs utilizadas y que se identifican en los ataques realizados desde botnets IoT. Para finalizar, se exponen las características de los ataques de DDoS más significativos atribuidos a botnets del IoT.

En el tercer capítulo se desarrolla el concepto de ataques de DDoS desde un punto de vista diferente. Se presenta la evolución que han manifestado distintos ataques reales de DDoS contra los servicios de una organización y el impacto que tuvieron sobre la operadora que prestaba el servicio de mitigación contra ataques de DDoS. Además, se

detallan las medidas que se vio obligada a tomar la operadora durante el desarrollo de cada uno de estos ataques, y la repercusión que tuvieron sobre el coste operacional de la mencionada organización.

Este capítulo se basa en datos proporcionados por personal perteneciente al centro de operaciones de seguridad de ciberdefensa de la operadora que prestaba el servicio de mitigación durante entrevistas que fueron realizadas a dicho personal.

El capítulo cuatro se desarrolla con la exposición de un estudio sobre la evolución de las botnets IoT y las TTP utilizadas, desde el año 2016 hasta la actualidad, donde se pueden observar las tendencias en lo referente al desarrollo de sus infraestructuras y nuevas capacidades y TTP utilizadas, finalizando con una serie de conclusiones que se derivan del análisis de los diferentes aspectos desarrollados en este trabajo.

III. CONCLUSIONES

Durante el desarrollo del trabajo, se pone de manifiesto que el problema de los ataques de DDoS es cada vez mayor. El incremento, en la cantidad de cosas conectadas, que se prevé a un corto y medio plazo se manifiesta según órdenes de magnitud exponenciales ya que, en todos los sectores de la industria, este aspecto se considera como una oportunidad.

Mirai ha evolucionado y se ha convertido, bajo otros nombres, o actualizándose en sus versiones, para convertirse en una botnet cada vez más peligrosa y dañina. Todo esto, en un dominio, el del IoT, donde los aspectos que tienen que ver con la seguridad de este tipo de dispositivos, aún no empieza a tenerse seriamente en consideración.

También se ha podido comprobar que no es necesario contar con una grandísima infraestructura para realizar ataques de DDoS que pongan en serios problemas a organizaciones (e incluso a operadoras de telecomunicaciones), obligando a estas a contratar a terceros especializados en este tipo de servicios.

Se está investigando bastante sobre este tema, y las empresas proveedoras de servicios anti-DDoS ponen en práctica distintas soluciones que, fundamentalmente, pasan en primer lugar por disponer por una poderosísima infraestructura de red donde distribuir el tráfico para ser procesado mientras se produce un ataque. Esto supone ya una importante barrera de entrada y, por tanto, un nicho de mercado muy importante para estas operadoras.

Estudiar las características de los ataques y las peculiaridades del tráfico ilegítimo generado, y analizar las muestras de piezas de malware correspondientes a nuevas botnets detectadas es fundamental para el desarrollo de nuevas técnicas y algoritmos de mitigación, y pueden constituir perfectamente nuevas líneas de investigación para ser desarrolladas en otros TFM, e incluso en trabajos de mayor nivel.

En cualquier caso, la solución más efectiva pasa por adecuar el mercado de estos dispositivos a las propuestas que se establecen en el último capítulo del trabajo y, por supuesto y principalmente, por desarrollar una política de seguridad común en internet que, entre otras cosas, establezca una serie de estándares que permitan implementar medidas en los sistemas intermedios, de modo y manera que se puedan detectar y mitigar estos ataques lo más cerca posible del origen.