Universitat Oberta de Catalunya

uoc.edu

Chatbots en el contexto de la limpieza de infecciones de malware IoT

Marc Alcalá Pizarro
Seguridad de las Tecnologías de la Información y de las Comunicaciones
Seguridad en la Internet de las cosas

Carlos Hernández Gañán
Victor Garcia Font

06/2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Chatbots en el contexto de la limpieza de infecciones de malware IoT*
Nombre del autor:	*Marc Alcalá Pizarro*
Nombre del consultor/a:	*Carlos Hernández Gañán*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	*06/2019*
Titulación:	*Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad en la Internet de las cosas*
Idioma del trabajo:	*Español*
Palabras clave	*IoT, chatbot, Automation*

Resumen del Trabajo:

En los últimos años hemos sido testigos de un aumento en la cantidad de *botnets* de *IoT*, las cuales afectan especialmente a dispositivos domésticos. Puesto que este tipo de infecciones suelen pasar desapercibidas y no se suele detectar más que una ralentización bien en el dispositivo infectado bien en la capacidad de conexión a Internet, los proveedores de servicios de Internet se han convertido en un punto de control para limpiar estas infecciones, pero estos carecen de los recursos humanos necesarios para tratar con una amenaza que sigue en aumento. Cientos de nuevas infecciones aparecen cada día dentro de estas redes de banda ancha y los departamentos de abusos de los proveedores de servicios de Internet deben proporcionar continuamente apoyo para limpiarlas, una situación que apunta a empeorar con la cada vez más cercana llegada del 5G.

En este contexto, este trabajo proporciona un procedimiento de uso genérico para la eliminación de infecciones de malware en dispositivos *IoT* y muestra el desarrollo de una solución *chatbot* que lo implementa. También incluye un análisis sobre el estado actual del *malware* en dispositivos *IoT*, así como del estado de la tecnología de los *chatbots*, los cuales sirven para exponer y razonar las decisiones acerca del diseño tanto del procedimiento como del *chatbot*.

Abstract:

In these last years we have witnessed an increase in the number of IoT botnets, which especially affect domestic devices. Internet service providers have become a checkpoint to clean these infections since these types of infections often go unnoticed and users con usually detect only a slowdown in the infected device or in its capacity to connect to the Internet, but they lack the necessary human resources to deal with a threat that keeps increasing. Hundreds of new infections appear every day within these broadband networks and the abuse department of the ISPs need to continuously provide support to clean those, a situation that points to worsen with the near arrival of 5G.

In this context, this work provides a generic use procedure for the elimination of malware infections in IoT devices and shows the development of a chatbot solution that implements it. It also includes an analysis of the current status of malware in IoT devices, as well as the status of the chatbots technology, which serve to expose and reason decisions about the design of both the procedure and the chatbot.

Índice

Lista de tablas

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Ya hace casi tres años desde la primera detección de un dispositivo infectado de la *botnet* Mirai (el 1 de agosto de 2016). Esta *botnet* marcó un antes y un después, ya que, si bien no era la primera de su tipo, logró cambiar el conocimiento de mucha gente acerca de las dimensiones y de lo que supone la amenaza de las infecciones en dispositivos de *IoT*.

La enorme popularización de estos dispositivos ha agravado los casos de infecciones de *malware* en ellos, haciendo que ya en 2018 se doblaran el número de detecciones y pasaran a representaran un 78% del total de infecciones detectadas.

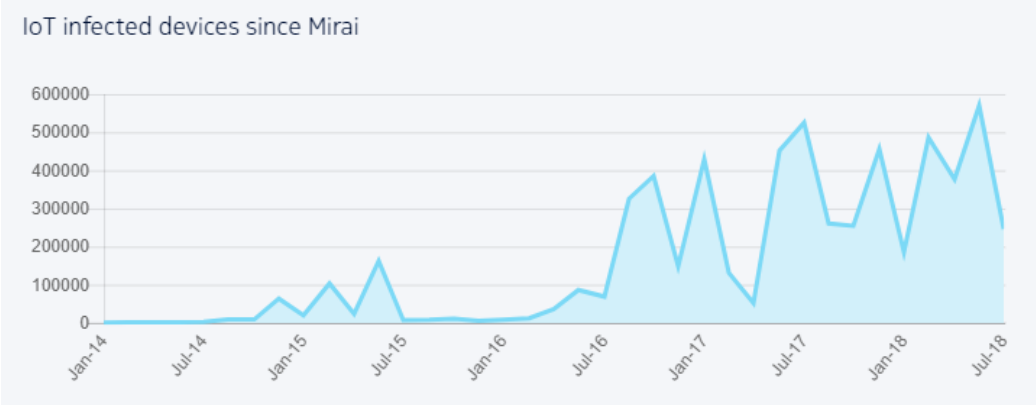


Ilustración 1: Aumento del numero de infecciones de dispositivos IoT detectades [1]

Puesto que estas infecciones suelen pasar desapercibidas y no se suele detectar más que una ralentización bien en el dispositivo infectado bien en la capacidad de conexión a Internet, los proveedores de servicios de Internet (*ISPs* por sus siglas en inglés) se han convertido en un punto de control, pero la falta de recursos humanos supone un problema, especialmente debido a la tendencia de crecimiento en la cantidad de detecciones, una tendencia que se prevé se dispare en los próximos años con la entrada del 5G. *[2]*

Ante este escenario, la cada vez también más popular tecnología de *chatbots* supone una considerable oportunidad gracias al enorme desarrollo que ha sufrido la inteligencia artificial en estos últimos diez años, que ha hecho que los *bots* ya sean capaces de llevar a cabo una considerable parte de las tareas más repetitivas de un equipo de servicio de soporte IT de primer nivel. Esta capacidad de reducir costes y optimizar el tiempo a la vez que se mejora la experiencia de los usuarios y se estimula la consumición de servicios no ha pasado desapercibida entre las empresas de todos los sectores, y ahora cada vez son más las empresas que apuestan por esta tecnología, algo que se puede ver con

especial claridad entre organizaciones del sector tecnológico como las *ISPs*. *[3] [4]*

Como analista de un centro de operaciones de seguridad, las infecciones de *botnets* no me son ajenas, y tanto la llegada del 5G como la previsión del aumento de las detecciones de *malware*, me han llevado a ver este proyecto como una forma de profundizar en múltiples tecnologías que en el panorama actual resultan muy interesantes a nivel profesional.

1.2 Objetivos del Trabajo

El trabajo tiene por objetivo estudiar el panorama actual tanto de las infecciones de *malware* en dispositivos de *IoT* como de la tecnología de *chatbots* para, de esta manera, poder desarrollar una solución de *chatbot* escalable y fácil de mantener que pueda interactuar con usuarios infectados brindando consejos de limpieza de *malware* en dispositivos de *IoT*.

Podemos por tanto esquematizar los objetivos del trabajo mediante los siguientes puntos:

- Investigar sobre las infecciones de *malware* en dispositivos de *IoT*.
- Investigar sobre el diseño de *chatbots* para brindar soporte de limpieza de *malware*.
- Diseñar e implementar una solución de *chatbot* escalable y fácil de mantener que pueda interactuar con usuarios infectados brindando consejos de limpieza de *malware* en dispositivos *IoT.*

1.3 Enfoque y método seguido

El enfoque y la metodología seguidos para cumplir con los objetivos del proyecto vienen definidos por las siguientes etapas:

- Definición del plan de trabajo
- Investigación sobre el estado del arte de los *chatbots*
- Investigación sobre el estado del arte del *malware* en *IoT*
- Desarrollo del procedimiento genérico de limpieza de *malware*
- Implementación del *chatbot*
- Conclusiones

Siendo más específico, durante la investigación sobre el estado del arte de los *chatbots* se ha hecho especial hincapié en los distintos tipos que existen, así como en sus capacidades específicas, usos actuales y soluciones existentes. A su vez, durante la investigación sobre el estado del arte del *malware* en *IoT*, se ha prestado especial atención a los vectores de infección y a los métodos de remediación y prevención.

A sido una vez finalizado el proceso de investigación que se ha podido desarrollar un procedimiento genérico de limpieza de *malware*, optando por una solución (reinicio de fabrica) que puede ser aplicada en todos los dispositivos de *IoT* (mientras que el reinicio de fabrica es una funcionalidad presente en la práctica totalidad de dispositivos *IoT*, otras soluciones como antivirus, actualizaciones y demás, son válidas únicamente para casos concretos, lo que las convierte en soluciones inviables para un procedimiento genérico) y a la que acompañan un seguido de medidas de prevención que tienen por objetivo evitar nuevas infecciones.

Llegado el turno de construir una solución de *chatbot* que implemente el procedimiento, existían dos opciones, programar nuestro propio *chatbot* o utilizar alguno de los servicios de creación de *chatbots* existentes. Al entender que el proyecto no debía estar centrado en la creación del *chatbot per se* sino en una solución que asistiera en la limpieza de *malware*, se ha optado por la segunda opción, ya que las soluciones encontradas no solo satisfacían las capacidades necesarias para implementar nuestro procedimiento, sino que requerían una menor inversión de recursos para obtener un mismo resultado.

Finalmente, se ha optado por incluir una última etapa para presentar las conclusiones derivadas de la ejecución del proyecto e identificar posibles líneas de desarrollo que no se han podido llevar a cabo pero que podrían resultar de interés para futuros proyectos.

1.4 Planificación del Trabajo

Para la realización de este proyecto he definido la siguiente planificación en base a las entregas requeridas:

Tabla 1: Planificación del proyecto

Entrega	Actividad	Inicio	Duración (dias)	Fin
PAC 1	Panificación del proyecto	20-02-19	13	05-03-19
PAC 2	Investigación de tipologías de malware en IoT	06-03-19	7	13-03-19
	Investigación de soluciones contra malware en IoT	14-03-19	7	21-03-19
	Diseño del procedimiento	22-03-19	11	02-04-19
	Diseño del chatbot	22-03-19	11	02-04-19
PAC 3	Implementación del chatbot y revisión	03-04-19	10	13-04-19
	Revisión	14-04-19	16	30-04-19
PAC 4	Redacción de la memoria	01-05-19	34	04-06-19

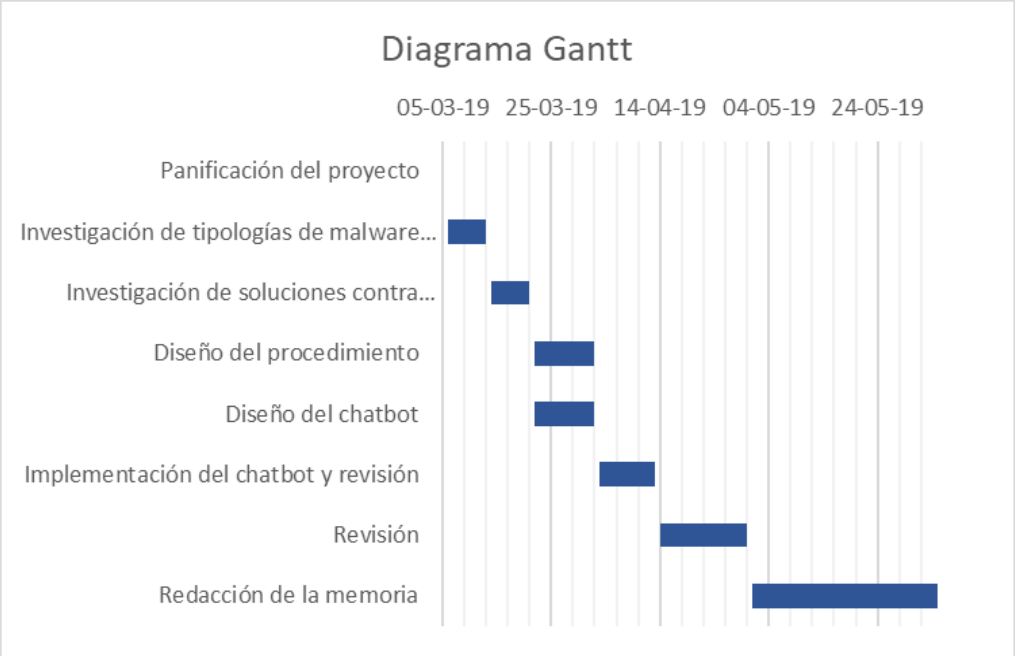


Ilustración 2: Diagrama de Gantt

- Investigación de tipologías de *malware* en *IoT*: investigar las características de las principales infecciones de *malware* que afectan a los dispositivos de *IoT* (vectores de infección. comportamiento, …).

- Investigación de soluciones contra *malware* en *IoT*: investigar métodos de detección y limpieza de *malware* en dispositivos de *IoT*.

- Diseño del procedimiento: desarrollar un procedimiento genérico de limpieza de *malware* para dispositivos de *IoT* en base a los resultados de las investigaciones previas.

- Diseño del *chatbot*: diseñar el flujo de trabajo de un *chatbot* de forma que implemente el procedimiento diseñando en la tarea anterior y que por tanto pueda proporcionar asistencia a los usuarios en la limpieza de infecciones de *malware* en dispositivos de *IoT*.

- Implementación del *chatbot* y revisión: implementar el diseño del *chatbot* obtenido anteriormente, así como añadir cualquier corrección o mejora resultante de las incidencias o de nuevas ideas obtenidas durante el proceso.

- Redacción de la memoria: documentar los resultados de las investigaciones y tanto del diseño como de la implementación del *chatbot*, así como las conclusiones derivadas de la ejecución del proyecto y demás informaciones que se consideren relevantes.

1.5 Breve sumario de productos obtenidos

A la finalización del proyecto se han obtenido dos productos:

- Un procedimiento genérico que sirve no solo para realizar exitosamente una eliminación de infecciones de *malware* en dispositivos de *IoT*, sino también para reducir todo lo posible las posibilidades de que el dispositivo vuelva a ser infectado.

- Una solución de *chatbot* sencilla de construir, actualizar y mantener que tiene como principal objetivo el poder servir de asistencia en la limpieza de dispositivos de *IoT* infectados mediante la implementación del procedimiento anterior.

1.6 Breve descripción de los otros capítulos de la memoria

Nuestro trabajo se divide esencialmente en dos partes.

En la primera parte se exponen los conocimientos obtenidos durante las tareas de investigación, necesarios para poder entender las decisiones y justificaciones tras los diseños e implementación tanto de nuestro procedimiento de limpieza como de nuestro *chatbot*.

La segunda parte, por otro lado, incluye precisamente los detalles del desarrollo tanto de nuestro procedimiento de limpieza como de nuestro *chatbot*, así como las justificaciones de nuestras decisiones y los resultados obtenidos.

2. Malware en IoT

Existe una enorme variedad de tipologías de *malware*, pero la cosa cambia si nos centramos en aquellos tipos que tienen como principal objetivo a los dispositivos de *IoT*. Esto se debe a la gran diversidad de *frameworks* existente en el ámbito de los dispositivos de *IoT* y a que por naturaleza suelen ser dispositivos de capacidades limitadas.

Con esto se pretende señalar que, por ejemplo, no tendría sentido intentar introducir un *keylogger* en un dispositivo de *IoT* regular, ya que más allá de la fase de configuración no es habitual que los usuarios introduzcan datos como contraseñas o números de tarjetas de crédito directamente en ellos. Tampoco es habitual encontrar troyanos que tengan como objetivo a dispositivos de *IoT*, ya que estos en muchas ocasiones no cuentan con la capacidad de ejecutar o tan siquiera de almacenar software extra.

Si bien existe una enorme variedad de tipologías de *malware*, por tanto, se pueden limitar aquellas que afectan a este proyecto en dos:

- *Botnet*: Este tipo de *malware* se basa en la infección de nodos que una vez comprometidos se mantienen a la espera de recibir una orden de un centro de comando y control (Command and control en inglés, usualmente abreviado C&C o C2) para, por ejemplo:
    - Realizar ataques de denegación de servicio distribuidos: en los que múltiples sistemas envían tantas solicitudes como sea posible a una sola computadora o servicio de Internet para causar una sobrecarga y evitar que se atiendan solicitudes legítimas.
    - Realizar tares de spyware: tales como enviar información a los atacantes sobre las actividades de un usuario (contraseñas, números de tarjetas de crédito y cualquier otro tipo de información con valor).
    - Enviar SPAM.

- Realizar fraude de clics: ocurre cuando un dispositivo visita sitios web sin que el usuario se dé cuenta para crear tráfico web falso que proporcione un beneficio personal o comercial.

- Realizar minería de criptomonedas: debido al aumento de la popularidad de las criptodivisas en los últimos años también ha aumentado el número de *botnets* que incluyen funciones de minería, con las que aprovechan la potencia de computación de los dispositivos infectados para minar diversas criptodivisas en beneficio del atacante.

- Auto-propagarse: mediante, por ejemplo, el escaneo de dispositivos en la red en busca de vulnerabilidades conocidas que pueda explotar, infectando y añadiendo así más nodos a la *botnet*.

- *Ransomware*: Este tipo de *malware* se basa en la infección de dispositivos que, una vez comprometidos, ven sus archivos valiosos encriptados a menos que se pague un rescate a los atacantes. Si bien aún no se conoce ningún *ransomware* que tenga como objetivo principal los dispositivos de *IoT*, estos sí pueden verse afectados, pese a ello a este tipo de amenazas no se le está prestando la misma atención que al tratar con dispositivos no-*IoT*.

  Esto se debe primeramente a que la mayoría de dispositivos IoT almacenan sus datos en la nube, de forma que incluso si los datos del dispositivo se encriptan no hay realmente necesidad que el propietario pague un rescate, lo que obligaría a los atacantes de *ransomware* a recurrir a la forma más antigua de *ransomware*, la que bloquea su dispositivo y lo rescata para recuperar el acceso a su funcionalidad. Algo tan trivial de superar en un dispositivo de *IoT* como restablecer de fabrica el dispositivo e instalar nuevos parches y actualizaciones.

  Además, un desarrollador de *ransomware* busca ganar más dinero con el menor esfuerzo. Por lo tanto, una vulnerabilidad de Windows o Adobe Flash o Internet Explorer permitiría a los piratas informáticos dirigirse a cientos de millones de usuarios, pero los dispositivos de *IoT* son tan diversos que cada uno de ellos debería ser dirigido de una manera diferente, lo que lo haría más difícil para los hackers.

También está el problema menor de necesitar una interfaz de usuario, como una pantalla, para informar al usuario de que ha sido pirateado por un *ransomware*. Un porcentaje considerable de dispositivos *IoT* carece de mecanismo de visualización y los piratas informáticos tendrían que realizar el paso adicional de descubrir el correo electrónico del usuario o piratear la aplicación que controla el dispositivo también.

Todos estos factores hacen parecer que no existe una motivación suficiente para que los piratas informáticos inviertan en *ransomware* para *IoT*, pero hay que tener en cuenta que la interconectividad de dispositivos está cambiando eso, imaginemos por ejemplo ir de vacaciones y recibir un correo amenazando con que han hackeado el termostato de casa y amenazando con aumentar o reducir la temperatura al máximo, o estar en la autopista y que el coche se quede bloqueado a menos que se pague un rescate. El modelo de *ransomware* de *IoT* es fundamentalmente diferente del paradigma de ordenadores de sobremesa y portátiles, pero no por ello menos peligroso. [5] [6]

Ilustración 3: Ransomware en un coche autónomo [7]

2.1 Mirai

Como parte del estudio del *malware* en dispositivos *IoT* es importante mencionar el que ha sido uno de los *malware* más relevantes y característicos dentro del ámbito, Mirai.

Mirai es un *malware* de tipo *botnet* que tiene como principal objetivo los dispositivos *IoT*. Su principal vector de infección consiste sencillamente en realizar ataques de fuerza bruta a través de Telnet o SSH contra dispositivos *IoT* mediante un diccionario de credenciales habituales tales como admin:admin, admin:1234, …. Este ataque tiene un considerable índice de aciertos debido a la escasa seguridad de los dispositivos *IoT*, tanto en lo relativo a los mecanismos implementados por el fabricante como en el trato por parte de los usuarios.

Una vez el dispositivo ha sido accedido con éxito, el nodo atacante notifica al *C&C* mediante el envío de la IP de la víctima y de las credenciales de acceso utilizadas, de forma que este introduzca y cargue de forma asíncrona el código malicioso en el dispositivo de la víctima.

Una vez infectado con éxito por el *malware* Mirai, el dispositivo pasa a formar parte de una *botnet*, las cuales son utilizadas principalmente para la realización de ataques de *DDoS*.

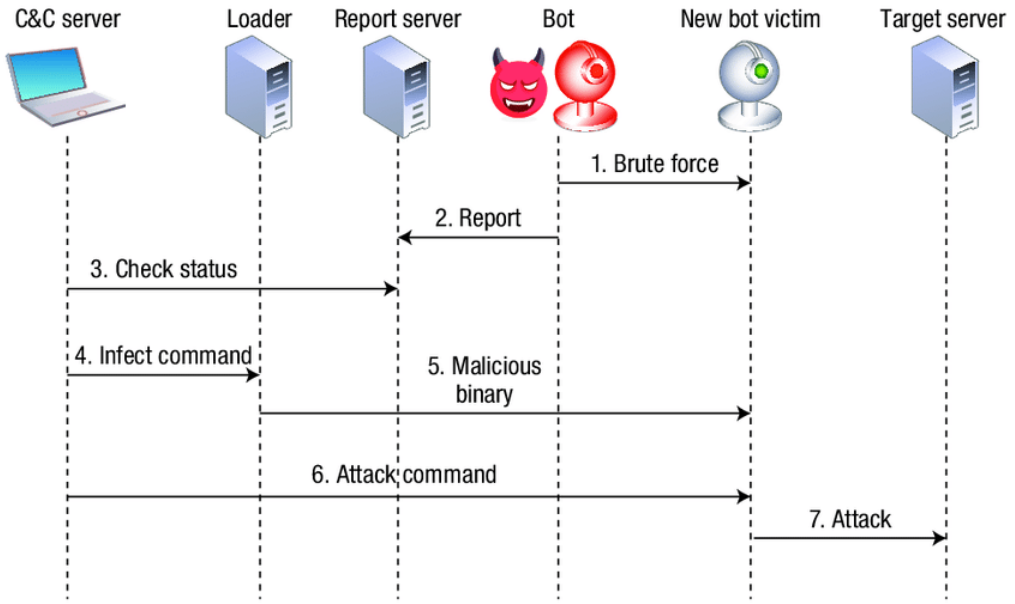


Ilustración 4: Esquema de actuación de Mirai [8]

Debido a la extensión que alcanzaría el documento resultante, resulta imposible tratar en profundidad este *malware* junto con todas sus variantes (o tan siquiera las más relevantes) en este documento, por lo que nos limitaremos a citar las que consideramos que son sus principales curiosidades:

- Ha protagonizado algunos de los mayores ataques de *DDoS* de los últimos años, dentro de los que se incluyen el realizado al sitio web de Brian Krebs (KrebsOnSecurity.com), a la empresa francesa de hosting OVH o al proveedor de DNS Dyn. También ha llegado a dejar fuera de servicio o con grandes problemas de disponibilidad a sitios como New York Times, Reddit, Twitter, Spotify o eBay.

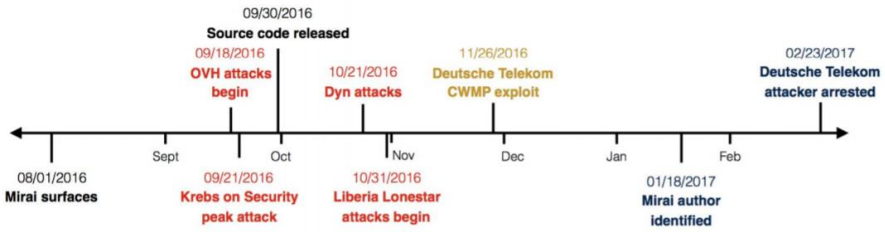


Ilustración 5: Linea temporal de la historia de Mirai [9]

- Mirai incluye una tabla de máscaras de red a las cuales no infecta, dentro de las que se encuentran redes privadas y direcciones pertenecientes al Servicio Postal de los Estados Unidos, el Departamento de Defensa, IANA, Hewlett-Packard y General Electric.

- El código fuente fue hecho público a finales de 2016, lo que provocó la aparición de múltiples variantes. Un ejemplo sería OMG, una variable protegida con una capa extra de cifrado y con capacidad de autopropagación que convierte los dispositivos *IoT* en servidores proxy alquilables para la realización de ataques de *DDoS*. *[10]*

- Una de las versiones más recientes y peligrosas se llama Wicked Mirai. Esta versión utiliza mejoras encontradas en variantes anteriores, como el análisis de vulnerabilidades y la descarga de un *payload* a petición de un servidor de C&C, pero también puede añadir código al firmware de muchos routers domésticos comunes, lo que provee al *malware* de persistencia, es decir, que permanece en el sistema incluso tras reiniciar el dispositivo. *[11]*

2.2 Soluciones contra malware en IoT

Tal y como se ha podido ver en el apartado anterior, la principal amenaza de los dispositivos de *IoT* son las infecciones de *botnets*, el 58% de las cuales suele durar menos de 24h de acuerdo con el informe de amenazas llamado “Threat Landscape Report” que publicó en 2018 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA por sus siglas en inglés).

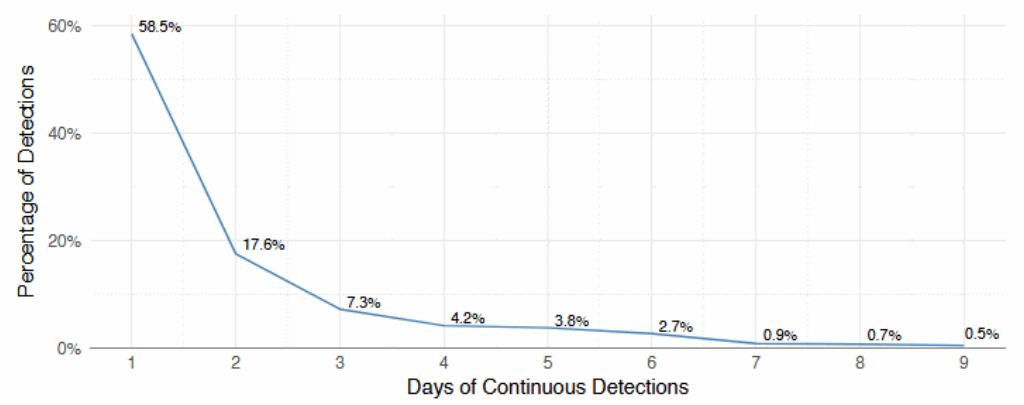


Ilustración 6: Persistencia de las botnets [12]

Esta baja persistencia se debe a que la mayoría de estas infecciones se almacenan en la memoria, por lo que solo pueden permanecer activas hasta que el dispositivo se reinicia, tras lo cual, pero, suele ser solo cuestión de tiempo hasta que vuelva a surgir la infección. [13]

Debido a la naturaleza tanto de los dispositivos de *IoT* como de su *malware*, parecería que las soluciones de remediación podrían resumirse en un reinicio de fábrica (factory reset en inglés), pero lo cierto es que en el ámbito del *malware* en *IoT* importa no solo el cómo limpiar los dispositivos de *malware* sino también el cómo prevenir que vuelvan a ser infectados.

Para entender esto basta un ejemplo simple, imaginemos un dispositivo *IoT* al que no se le ha cambiado las credenciales por defecto, que no cuenta con las últimas actualizaciones y que se descubre que está infectado con *malware*. La solución parecería ser simplemente reiniciar el dispositivo de fábrica, pero si ha sido infectado debido a una vulnerabilidad no parcheada o mediante un ataque de fuerza bruta debido a usar credenciales por defecto conocidas, nada impide que vuelva a infectarse. Lo mismo sucedería si, por ejemplo, el dispositivo contara con alguna vulnerabilidad conocida y no dispusiera de una debida actualización de seguridad.

Se puede ver, por tanto, que un reinicio de fábrica es efectivamente la manera más sencilla y segura de eliminar el *malware* de un dispositivo *IoT*, pero que un dispositivo que ha sido infectado puede volver a infectarse en poco tiempo si no se aplica ninguna medida adicional para protegerlo, por ello, para poder hacer un *chatbot* que realmente sea útil, es imprescindible que pueda ofrecer algo más que un mecanismo de limpieza como el reinicio de fábrica, debe ser capaz de proporcionar tanto unos mecanismos para limpiar de malware el dispositivo como una solución para que no vuelva a surgir la infección. *[14]*

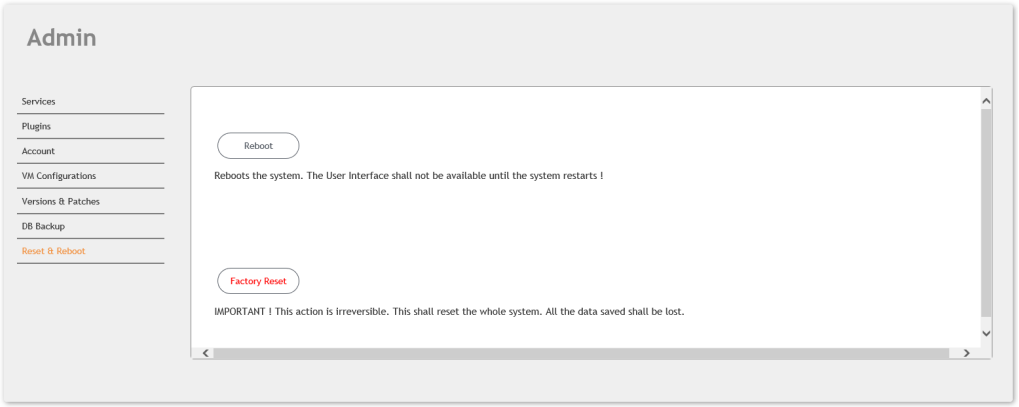


Ilustración 7: Reinicio de fàbrica [15]

3. Chatbots

Si bien para hablar del origen de los *chatbots* es posible retrotraernos hasta 1950 y al artículo “Computer Machinery and Intelligence.” que Alan Turing escribió en referencia a si las máquinas podían realmente pensar y donde exponía los principios del llamado test de Turing (cuyo objetivo sería medir si alguien está hablando con un ser humano o a un robot), lo cierto es que no sería hasta varios años más tarde que podríamos empezar a hablar de los primeros *chatbots*.

ELIZA sería uno de estos primeros *chatbots*. Creado por Joseph Weizenbaum en 1966, no fue capaz de superar el test de Turing pese a que fue capaz de engañar a algunos usuarios haciéndoles pensar que realmente hablaban con una persona. Pese a ello, el uso que hacía ELIZA de palabras clave, de frases específicas y de respuestas preprogramadas, se convertirían en los principios básicos para las primeras estructuras de *chatbots*.

En los años siguientes aparecerían múltiples *chatbots* que, pese a no ser capaces de pasar el test de Turing, sí que serían capaces de engañar con su realismo a un gran número de personas. Pero no sería hasta los años 2010-2015 que los *chatbots* alcanzarían su máxima popularidad entre las compañías tecnológicas, empezando por Siri (2010), Google Now (2012), Alexa (2015) y Cortana (2015), siendo todos ellos capaces de responder a comandos de voz, de reproducir música o de realizar búsquedas en Internet, entre otras tareas. *[16]*

Este crecimiento también se ve vinculado en parte a otra de las grandes tecnologías del momento, el “internet de las cosas” (Internet of things en inglés o IoT por sus siglas). Y es que la cantidad de dispositivos conectados a la red ha aumentado exponencialmente en los últimos años, llegando a afirmar el vicepresidente de la región EMEA del gigante tecnológico Intel que *"[…] De los 3.000 millones de personas conectadas a internet hoy, en 2020 habrá 6.000 millones. Entonces, por cada uno de ellos, habrá diez dispositivos conectados, que se volverán inteligentes al conectarse a la «nube» […]"* *[17]*

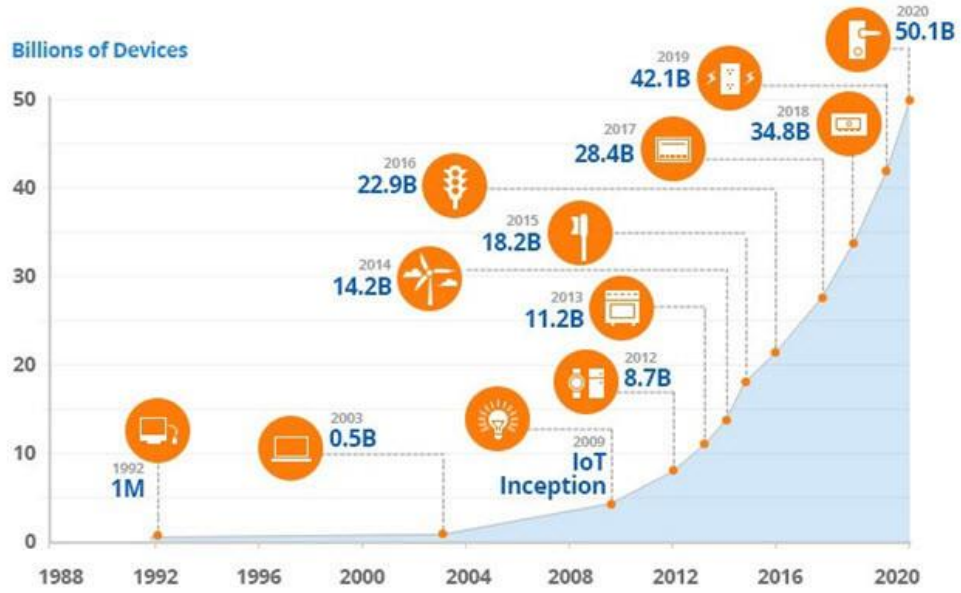


Ilustración 8: Gráfica del aumento en el número de dispositives conectados a Internet [18]

Junto con este crecimiento también se produce un aumento exponencial de las amenazas existentes, y es que a más tecnología de un tipo exista, más interés existirá por hackearla y más infecciones se detectarán.

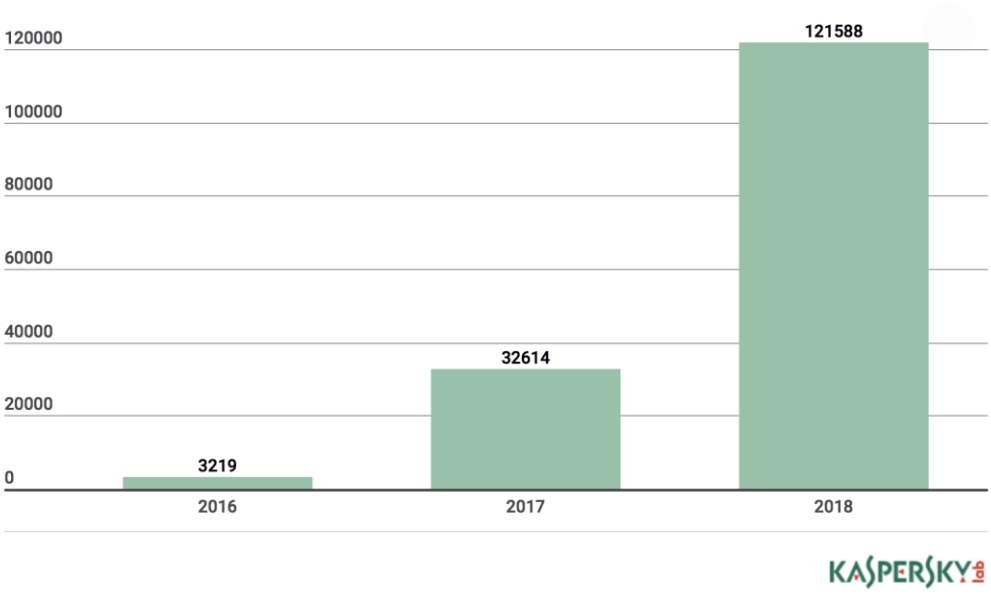


Ilustración 9: Gráfica del número de muestras de malware detectadas por Kaspersky Labs [19]

Ante esta situación, los *chatbots* suponen una oportunidad para rebajar la carga de trabajo de los profesionales, ya que permiten proporcionar una asistencia rápida y eficiente a errores concretos comunes sin necesidad de que el personal humano tenga que invertir un tiempo que podría dedicar a tares más complejas. Además, el entorno de los *chatbots* ha sufrido un gran desarrollo en los últimos años gracias a (entre otros factores) la popularización de las redes sociales, que han obligado a empresas y profesionales a publicar grandes cantidades de información en múltiples plataformas para poder mantener su visibilidad y nivel de comunicación frente al público, convirtiéndose en una de las soluciones más eficientes.

Esta popularización ha llevado a la creación de servicios orientados a la creación y mantenimiento de *chatbots*, haciendo que en la actualidad ya existan gran cantidad de soluciones de *chatbot* que permiten la creación de *bots* con gran capacidad y que funcionan 24/7 en algunos casos incluso sin necesidad de tener grandes recursos o conocimientos de programación.

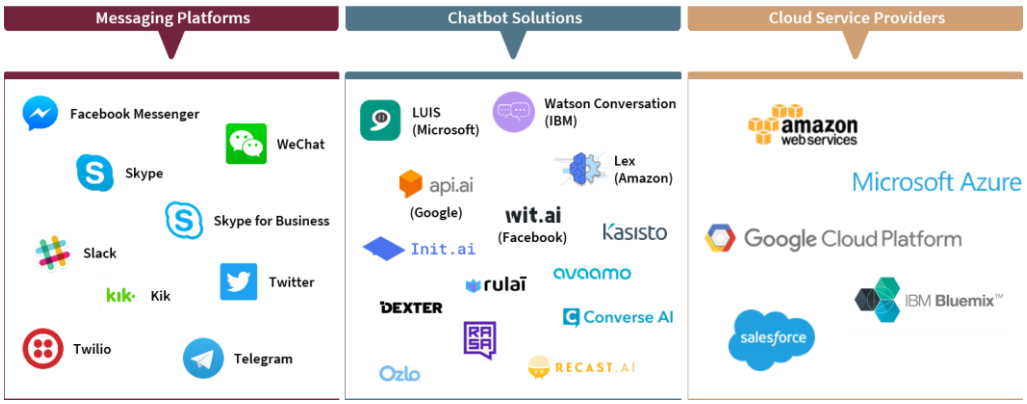


Ilustración 10: Ejemplos de ecosistemas de chatbots [20]

3. Tipos de chatbots

Existe una enorme cantidad de *chatbots* distintos con elementos muy diferenciados (interacción con los usuarios, integración con redes sociales, aplicaciones prácticas, uso de IA, …), lo que dificulta enormemente realizar una clasificación única, para el propósito de este proyecto, pero, se utilizará la división que resulta más simple a la vez que relevante, la basada en la tecnología utilizada:

- Parámetros predefinidos
- Inteligencia Artificial (IA)

Los *chatbots* con parámetros predefinidos giran en torno a palabras clave que reconoce y frente a las que proporciona respuestas secuenciales predefinidas por el programador. Es el tipo de *chatbot* que se suele escoger cuando no se quiere que los usuarios se salgan de unos ciertos límites, ya que pueden responder a un conjunto limitado de preguntas.

Por el contrario, los *chatbots* con IA son capaces de responder preguntas ambiguas mediante respuestas propias creadas por ellos mediante el procesamiento de lenguaje natural, entrenando para ello con posibles preguntas de forma que puedan aprender y así proporcionar mejores respuestas. Este tipo de *chatbots* se vuelven mejores a medida que pasa el tiempo, pero necesitan una gran cantidad de datos de aprendizaje. *[21] [22]*

3.2 Las elecciones de las ISPs

Debido a la gran cantidad de *chatbots* existentes, no resulta extraño ver que las distintas *ISPs* se han decantado por opciones distintas. En los últimos años, por ejemplo, dos de la mayores *ISPs* de nuestro país han optado por soluciones casi opuestas:

- Moviestar: Movistar España desarrolló con Twitter un *chatbot* conectado a su *call center*, el cual no solo da información, sino que puede realizar acciones directamente sobre la línea del usuario. Esta solución es un *chatbot* de parámetros predefinidos que interactúa con los usuarios mediante un menú de botones. *[23] [24] [25]*

Ilustración 11: Chatbot de Moviestar en Twitter

- Vodafone: Vodafone UK desarrolló a TOBI, un *chatbot* accesible a través de la aplicación móvil de la compañía y que utiliza lo último en tecnología de inteligencia artificial. Esta solución *chatbot* interactúa con los usuarios mediante el procesamiento del texto que recibe de estos, lo que le permite proporcionar un abanico de respuestas mucho mayor de forma natural, pero que a su vez le obliga a solicitar una aclaración a los usuarios cuando no es capaz de entender correctamente el texto. *[26] [27]*

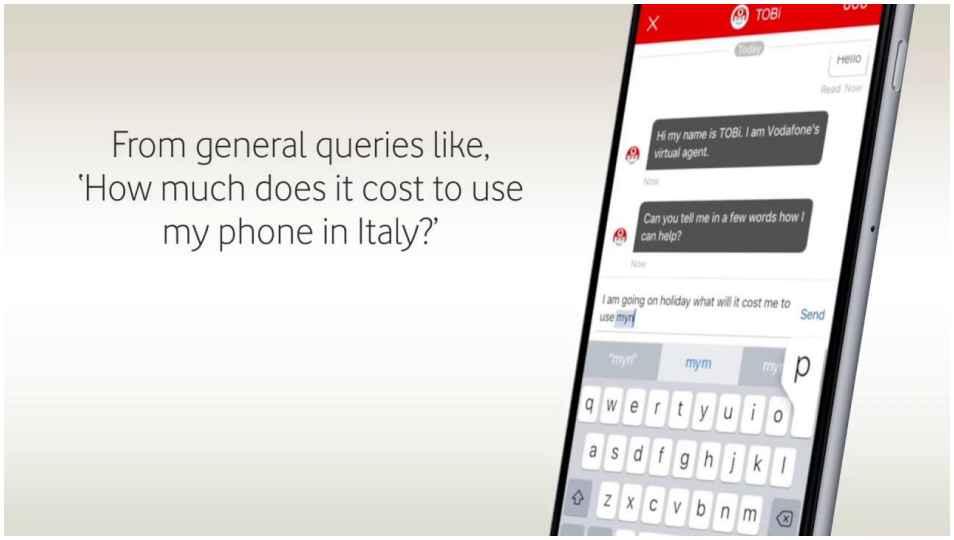


Ilustración 12: Chatbot de Vodafone [28]

4. Desarrollo del procedimiento de limpieza

Acabada la investigación sobre *malware* se puede ya empezar a desarrollar un procedimiento genérico para la limpieza de infecciones en dispositivos *IoT*. Para ello se han tenido en cuenta tres puntos esenciales:

- La base del procedimiento será el reinicio de fabrica del dispositivo, puesto que la naturaleza heterogenia y simple de los dispositivos *IoT* la convierte en la decisión más eficiente al ser fácil y rápida de llevar a cabo a la vez que tiene como única consecuencia el tener que volver a configurar el dispositivo, con todo, algo que puede ser llevado a cabo en pocos minutos en la mayoría de casos.

- Un dispositivo que ha sido infectado puede volver a infectarse, por ello, el reinicio de fabrica deberá acompañarse de un seguido de pasos que aseguren la protección del dispositivo y prevengan una nueva infección. Por ejemplo, se ha encontrado que alrededor de tres de cada cuatro infecciones en dispositivos *IoT* se producen debido al uso de contraseñas de Telnet débiles y/o configuradas por defecto, una cantidad muy por encima de cualquier otro vector de infección como podrían ser los ataques de fuerza bruta contra contraseñas SSH, que apenas superan el 10%. [29]

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	–
winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	–
RDP	3389	0.12%	Bruteforce	–
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–

Ilustración 13: Tabla de ataques y vectores de infección [30]

- La enorme heterogeneidad de los dispositivos *IoT* hace que no se pueda contar ni con que los dispositivos permitan la modificación de las credenciales configuradas por defecto ni con que reciban actualizaciones de seguridad.

Con todos estos puntos en mente, hemos diseñado el siguiente procedimiento:

1. Comprobar si el dispositivo tiene alguna puerta trasera

    - Algunos proveedores y fabricantes colocan puertas traseras para, por ejemplo, facilitar el soporte remoto. Esto, pero, supone una grave vulnerabilidad a nivel de seguridad.

      Para comprobar si un dispositivo es accesible desde fuera de la red doméstica y si tiene alguna puerta trasera, se puede optar por utilizar un escáner de vulnerabilidades para *IoT* como:

        - Bitdefender Home Scanning

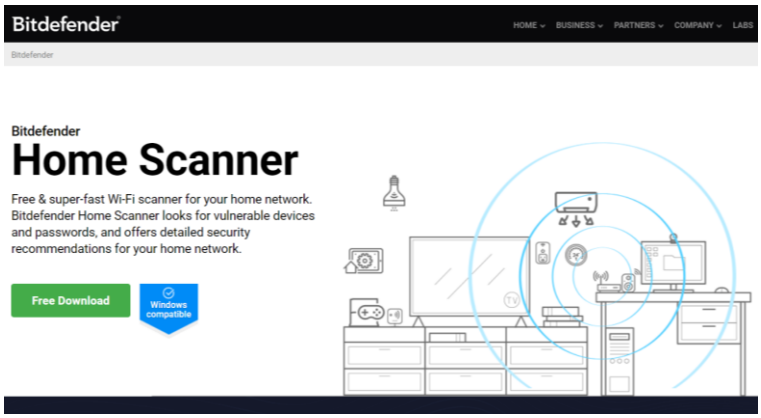


Ilustración 14: Bitdefender Home Scanner [31]

        - BullGuard Online IoT Scanner

Ilustración 15: BullGuard Online IoT Scanner [32]

2. Desconectar el dispositivo de la red

    - Para poder evitar cualquier tipo de interferencia durante la limpieza del dispositivo, como comunicaciones con C&Cs o nuevas infecciones, es importante desconectar el dispositivo infectado de la red para que quede aislado.

3. Realizar un reinicio de fábrica

    - Tal y como ya se ha explicado, el método más eficaz y eficiente para eliminar el *malware* de un dispositivo de *IoT* es restablecerlo a su estado de fábrica.

      El como llevar a cabo este paso es distinto en cada dispositivo, por lo que para cada caso concreto habrá que buscar en Internet los pasos a seguir.

4. Cambiar las credenciales del dispositivo

    - Anteriormente ya se ha mostrado que el principal vector de infección en dispositivos de *IoT* son ataques de fuerza bruta. Por ello, una vez limpiado el dispositivo de cualquier infección presente, se deberán cambiar las credenciales de acceso por defecto, siguiendo para ello siempre las reglas de seguridad esenciales para el establecimiento de una contraseña:

        - No usar información personal ni palabras o patrones comunes
        - Utilizar una longitud mínima de entre 8 y 12 caracteres
        - Combinar mayúsculas, minúsculas, números y símbolos

5. Conectar el dispositivo de forma segura e instalar las últimas actualizaciones

    - Llegados a este punto tocará asegurarse que el dispositivo se vuelve a conectar a la red de forma segura. Este paso es especialmente importante para aquellos casos donde no se permitan el establecimiento o modificación de credenciales.

      Para ello se puede:

        - Revisar el resto de dispositivos de la red en busca de más dispositivos infectados que pudieran haber sido o bien el origen de la infección o bien haber sido comprometidos a causa de ella

- Conectar el dispositivo de forma que no pueda ser accedido desde fuera de la red, por ejemplo, tras un firewall adecuadamente configurado

- Instalar las ultimas actualizaciones de seguridad del dispositivo

6. Instalar una solución de protección para dispositivos *IoT*

   - Como paso final, es recomendable instalar alguna solución para la protección de dispositivos de *IoT*.

     Esto se debe a que a pesar de que los antivirus no suponen una protección debido a la falta de capacidad de procesamiento o memoria de los dispositivos de *IoT*, si que existen soluciones de seguridad para entornos *IoT*, como dispositivos que sustituyen o complementan al router doméstico y que monitorizan y controlan el tráfico de la red para así detectar y bloquear comportamientos que indiquen una infección de *malware*.

     Algunos ejemplos interesantes de estos dispositivos serían:

     - Norton Core: un router para inexpertos en seguridad que se controla desde el móvil y que identifica y aísla con la conectividad justa a todos aquellos dispositivos que no requieren acceso a toda la red local.

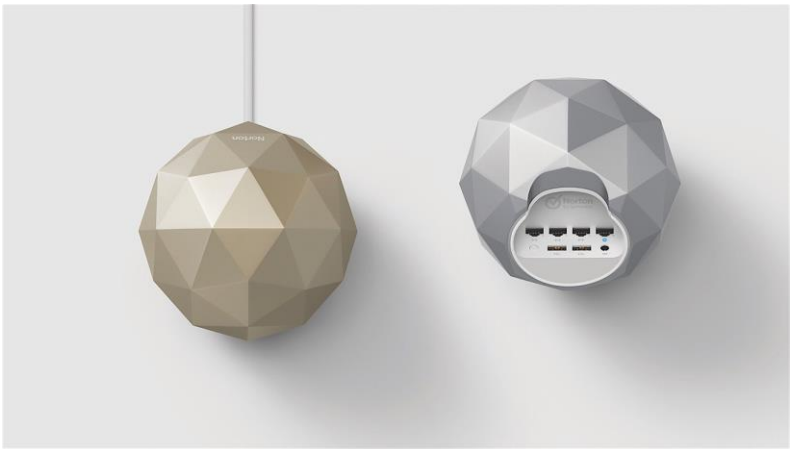


Ilustración 16: Norton Core [33]

- Bitdefender Box: de forma similar al Norton Core, es un producto de protección doméstica que se controla desde el móvil y que se puede utilizar o como router principal o como puerta de acceso junto al router.

Ilustración 17: Bitdefender Box 2 [34]

5. Desarrollo de nuestra solución chatbot

5.1 Diseño del chatbot

El primer punto será escoger nuestra plataforma de mensajería, es decir, a través de que medio interactuaremos con el *chatbot*. En este caso, principalmente por preferencias personales, se ha escogido Telegram, pero otras plataformas de chat como Facebook o WhatsApp también serían opciones válidas.

Seguidamente se ha procedido a realizar el diseño de un diagrama de flujo que implemente el procedimiento desarrollado anteriormente para la limpieza de dispositivos de *IoT* infectados:

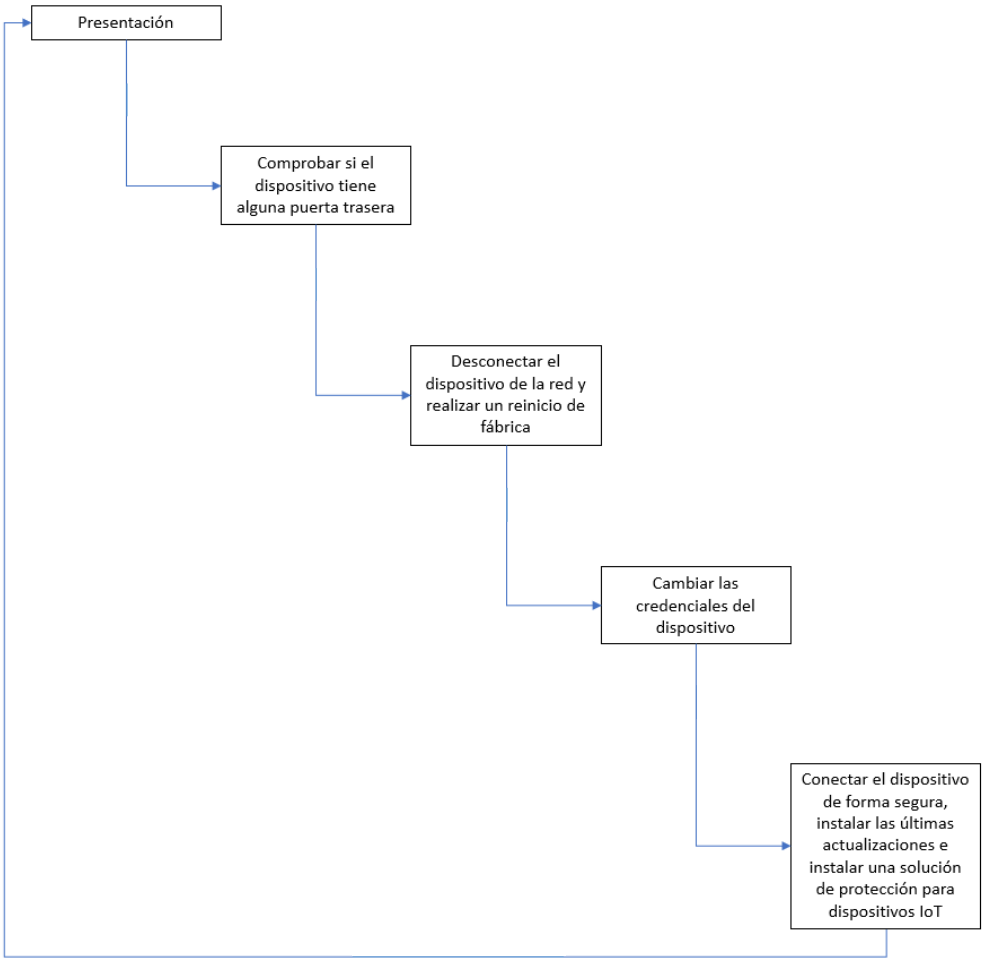


Ilustración 18: Esquema de procedimiento de limpieza de malware en dispositivos IoT 1

Sabiendo sobre que plataforma se va a trabajar y qué se quiere a hacer, se puede proceder a decidir con qué tecnología implementar el *chatbot*. Tal y como se ver en el diagrama de flujo, el diseño no requiere mucho, se trata de un *bot* simple para guiar a los usuarios paso a paso en el proceso de limpiar de *malware* su dispositivo *IoT,* por ello, se ha considerado que la mejor solución es un *chatbot* de parámetros predefinidos que interactúe con el usuario mediante un menú de botones. Con esto en mente se han realizado las siguientes correcciones en el diagrama:

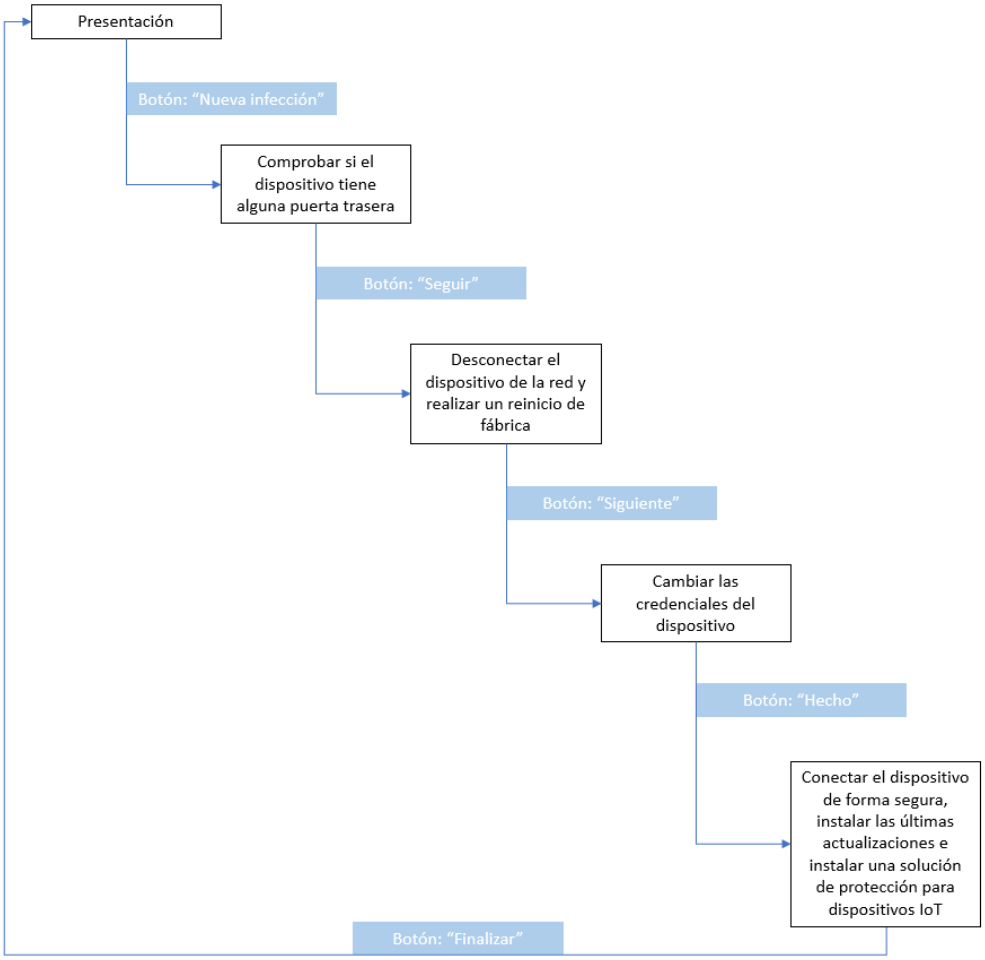


Ilustración 19: Esquema de procedimiento de limpieza de malware en dispositivos IoT 2

En este segundo diagrama de flujo se pueden ver tres tipos de elementos: las flechas, las cuales señalan el paso de un estado a otro; los cuadros azules, los cuales representan los comandos o botones que se deberán activar para pasar de un estado a otro; y los cuadros blancos de estado, que representan la clase de mensaje que recibirá el usuario, es decir, que al estar en estado "Presentación" y pulsar el botón "Nueva infección", el usuario pasará a estado "Comprobar si el dispositivo tiene alguna puerta trasera", donde el usuario deberá recibir un mensaje relacionado donde se le solicite hacer la comprobación y se le proporcionen los pasos o consejos adecuados para ello.

El siguiente paso a realizar, por tanto, ha sido la redacción de los mensajes a mostrar al usuario, los cuales pueden ser vistos detalladamente en el apartado de implementación.

Para terminar esta fase se ha tenido en cuenta que, si bien el diseño del *chatbot* actual implementa correctamente el procedimiento de limpieza de *malware*, este tiene por objetivo ser de utilidad para usuarios que pueden tener en algunos casos un bajo nivel tecnológico. Por ello, se han añadido nuevos comandos y textos de respuesta que puedan servir de asistencia en caso de duda o dificultad, tal y como veremos en el apartado de implementación.

5.2 Implementación del chatbot

Acabada la fase de diseño, falta decidir como implementar-lo. Para lo cual existían dos posibilidades, programar nuestro *chatbot* desde cero o utilizar alguna de los múltiples servicios de creación *chatbots* ya existentes.

La primera opción, programar nuestro *chatbot* desde cero, es una opción más versátil y permitiría agregar prácticamente cualquier funcionalidad que se pudiera necesitar, pero no solo se ha podido ver que la solución propuesta no requiere más que responder a comandos predefinidos, sino que programar el código desde cero requería una considerable cantidad de horas para desarrollar-lo, además de requerir el uso de un servidor o de una solución en la nube para que pueda estar siempre disponible, todo ello sin ofrecer nada a favor en términos de seguridad.

Puesto que se ha concluido que el proyecto no debía centrarse en el desarrollo del *chatbot* en sí, sino en el desarrollo de una solución para la limpieza de infecciones de malware en dispositivos *IoT* mediante un *chatbot*, se ha considerado que la mejor opción era utilizar un servicio de creación de *chatbots*, ya que muchos de estos servicios son gratuitos, no requieren mantenimiento por parte de los usuarios y son fáciles de utilizar (la mayoría de estos servicios están pensados para poder ser utilizados incluso por personas sin conocimientos de programación).

Tras investigar los detalles de múltiples servicios, se han podido encontrar varias opciones interesantes como por ejemplo Snatchbot, un servicio de creación de *chatbots* con inteligencia artificial totalmente gratuito y multiplataforma. También existen otros servicios como Chatfuel o Botsat, ambos dedicados a la creación de *chatbots* con parámetros predefinidos que están principalmente enfocados a Facebook (aunque pueden integrarse en más plataformas) y que ofrecen su sistema de creación de *bots* mediante un sistema de tarifas, incluyendo también una tarifa básica gratuita. *[35] [36] [37]*

La mayoría de estos servicios son utilizados por multitud de grandes empresas, y cualquiera nos serviría para hacer una demostración de cómo crear un *chatbot* para asistir en la limpieza de *malware* en dispositivos de *IoT*, pero en nuestro caso, puesto que es un servicio totalmente gratuito, integra Telegram y es una opción bastante recomendada en múltiples tutoriales y blogs, utilizaremos el servicio Manybot. *[38] [39] [40]*

Acabaremos por tanto la fase de implementación de nuestro proyecto con una guía paso a paso de cómo utilizar el servicio de creación de *chatbots* Manybot para desarrollar un *chatbot* de Telegram que tenga por objetivo asistir en la limpieza de infecciones de *malware* en dispositivos de *IoT*.

El primer paso será la obtención de un token para Telegram. Para ello, empezaremos por acceder al servicio gratuito de creación de *bots* de Telegram, llamado BotFather. Accederemos para ello a BotFather desde el buscador de un cliente Telegram y, tal y como se indica en el texto, introduciremos el comando /newbot, tras lo cual le proporcionaremos al *bot* un nombre y un nombre de usuario (en nuestro caso IoT_AntiMalware_bot).

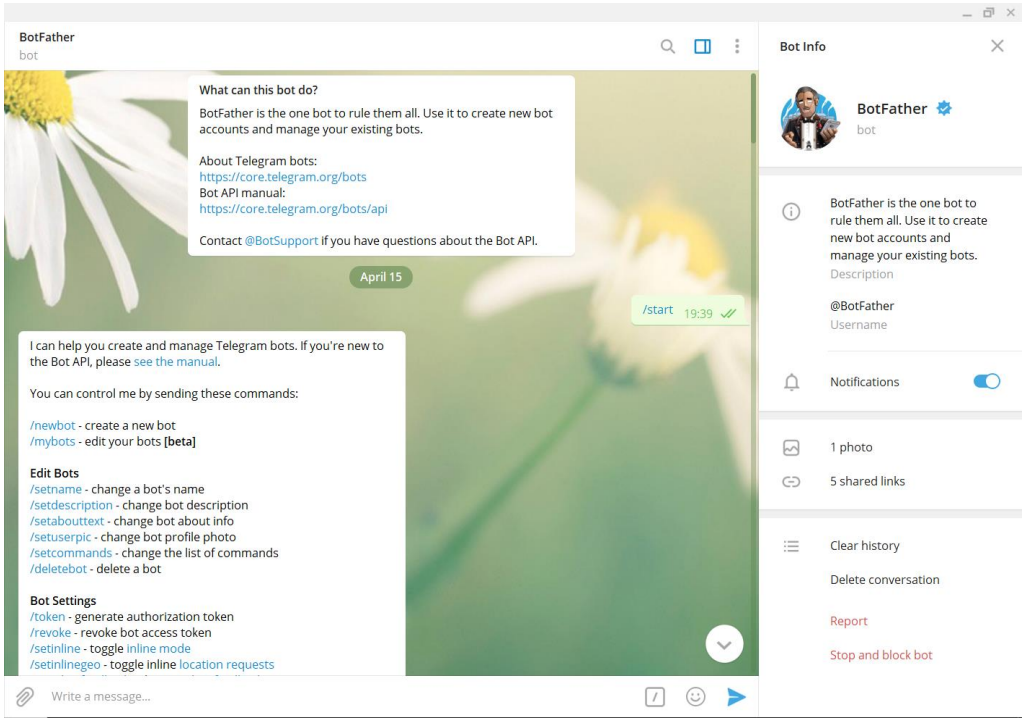


Ilustración 20: Creación de bot de Telegram 1

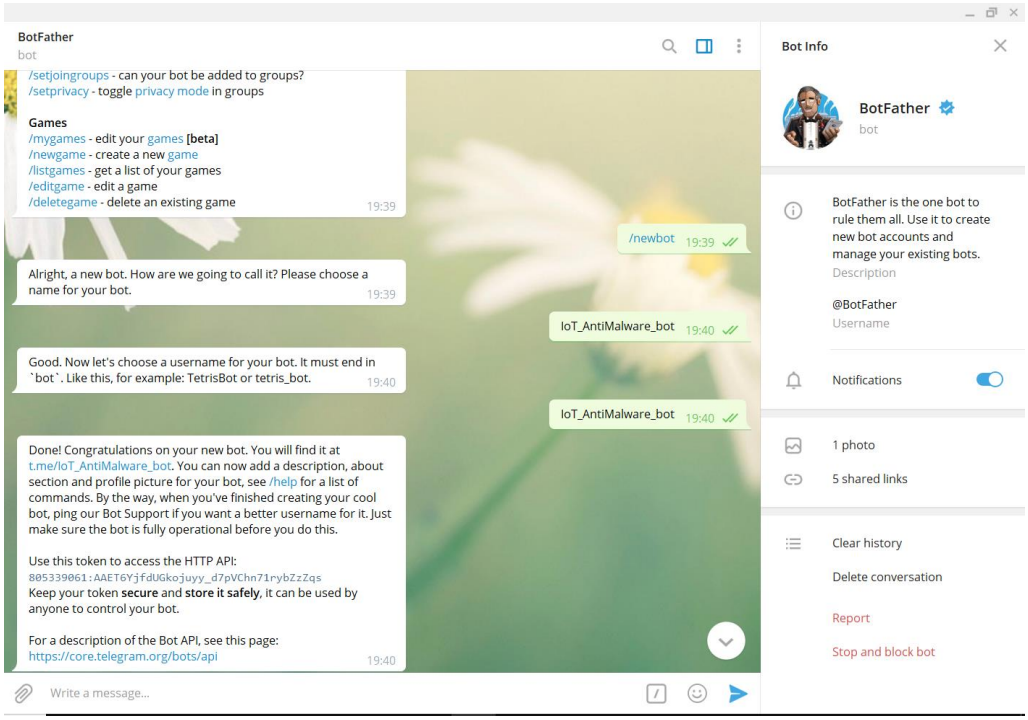


Ilustración 21: Creación de bot de Telegram 2

Una vez proporcionados un nombre y un nombre de usuario correctos, se nos proporcionará el token del *bot*, con el cual podremos acceder a la API de Telegram y empezar a programar nuestro *bot*.

Antes de empezar a implementar nuestro *bot* pero, podemos seguir haciendo uso de BotFather para personalizarlo. En nuestro caso, hemos optado por añadir un texto inicial, una descripción y una foto de perfil mediante los comandos:

- /setabouttext
- /setdescription
- /setuserpic

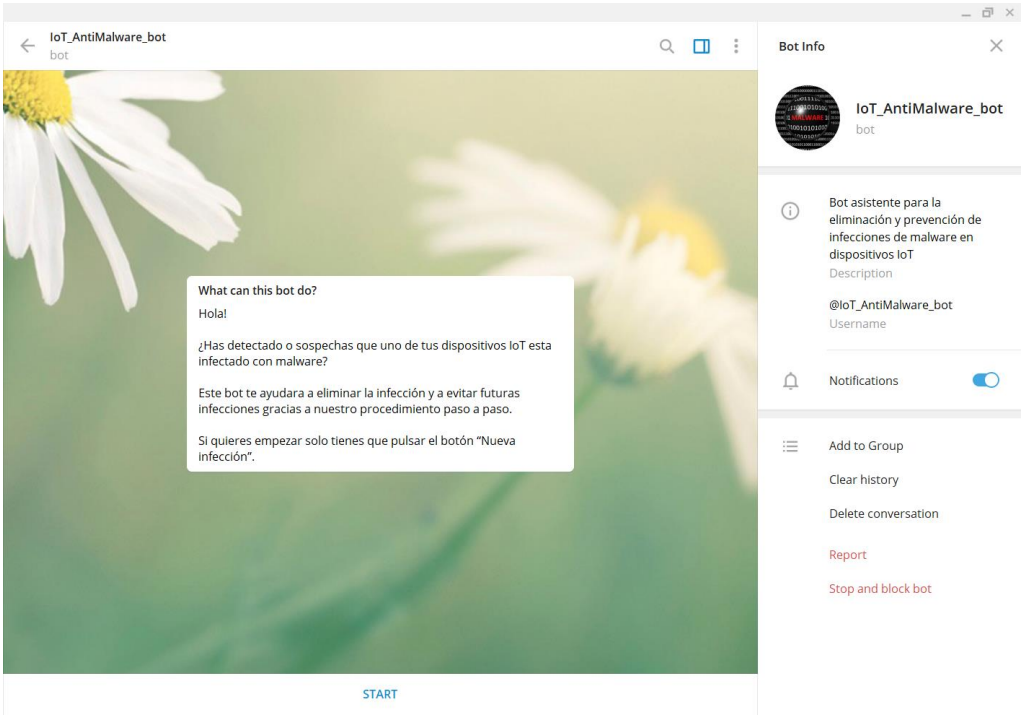


Ilustración 22: Creación de bot de Telegram 3

Accederemos ahora sí al *bot* de ManyBot desde nuestro cliente de Telegram tal y como hicimos con BotFather, y una vez encontrado el *bot* pulsaremos el botón del menú o enviaremos el comando /addbot para poder proporcionar el token obtenido de BotFather y empezar así a programar nuestro *bot* mediante el servicio de ManyBot. Una vez enviado el token de nuestro *bot*, ManyBot pasará a tener control sobre él, esto hará que se produzcan algunos cambios al volver a la ventana de nuestro *bot*.

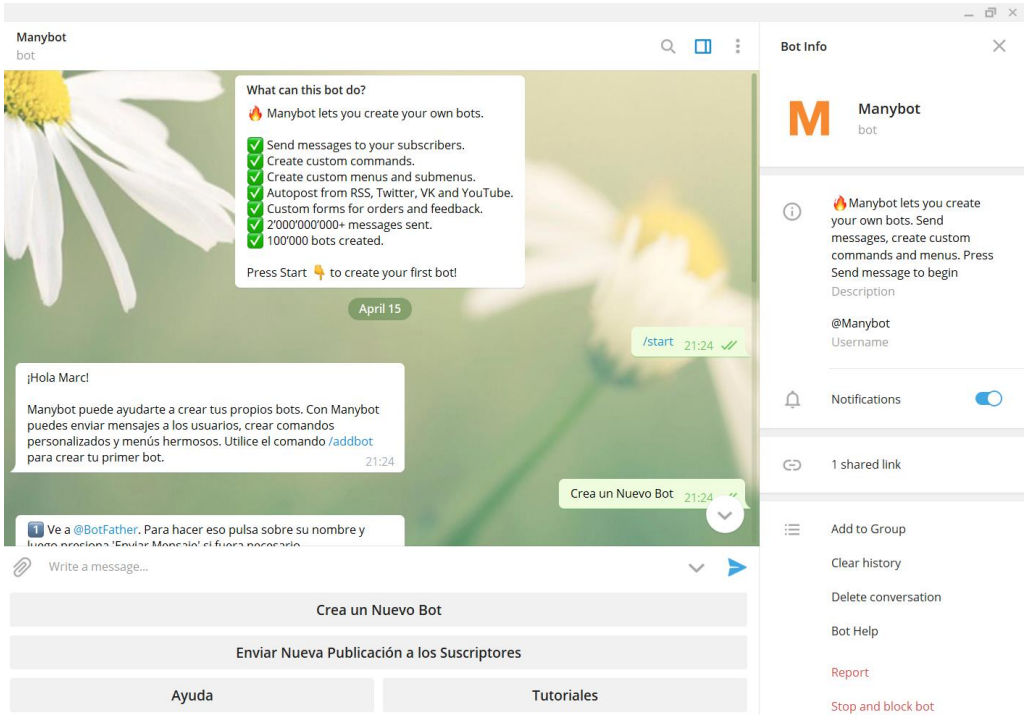


Ilustración 23: Creación de bot de Telegram 4

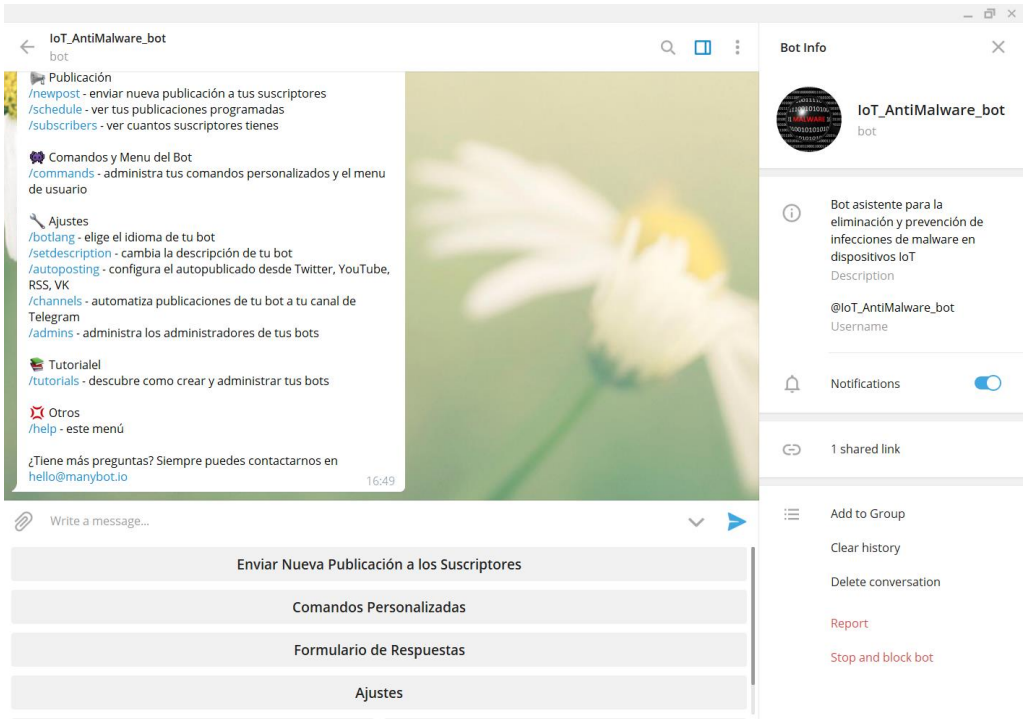


Ilustración 24: Creación de bot de Telegram 5

Mediante los botones del nuevo menú podemos configurar fácilmente nuestro *bot* a través de dos fases:

- Creación de comandos
- Configuración del menú

La creación de comandos consiste básicamente en las ordenes que recibirá nuestro *bot* por parte de los usuarios y a partir de las cuales realizará acciones.

Al seleccionar el botón “Comandos personalizadas” aparecerá un nuevo menú con la opción “Crear Comando”. Al seleccionarlo se nos pedirá un nombre para el comando y se nos darán tres opciones:

- Introducir y enviar un texto respuesta que el *bot* utilizará cuando un usuario ejecute ese comando.

- Realizar una pregunta, la cual esperara una respuesta del usuario que se almacenara en un formulario.

- Activar el modo de mensajes aleatorios, para que el *bot* utilice una respuesta al azar de entre un determinado número de posibles respuestas.

En nusestro caso, queremos que al iniciar el *bot* el usuario tenga que pulsar un botón para reportar una nueva infección y que una vez pulsado le aparezca un determinado texto, para ello, crearemos un comando al que llamaremos “/new_infection” y que al ejecutarse simplemente responderá un texto:

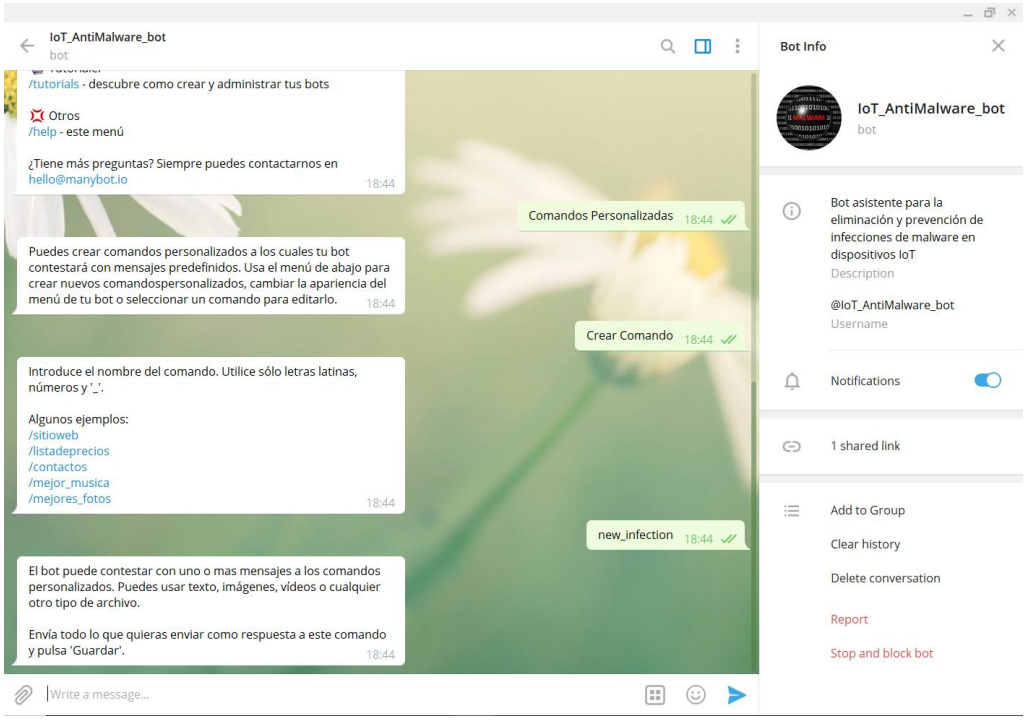


Ilustración 25: Creación de bot de Telegram 6

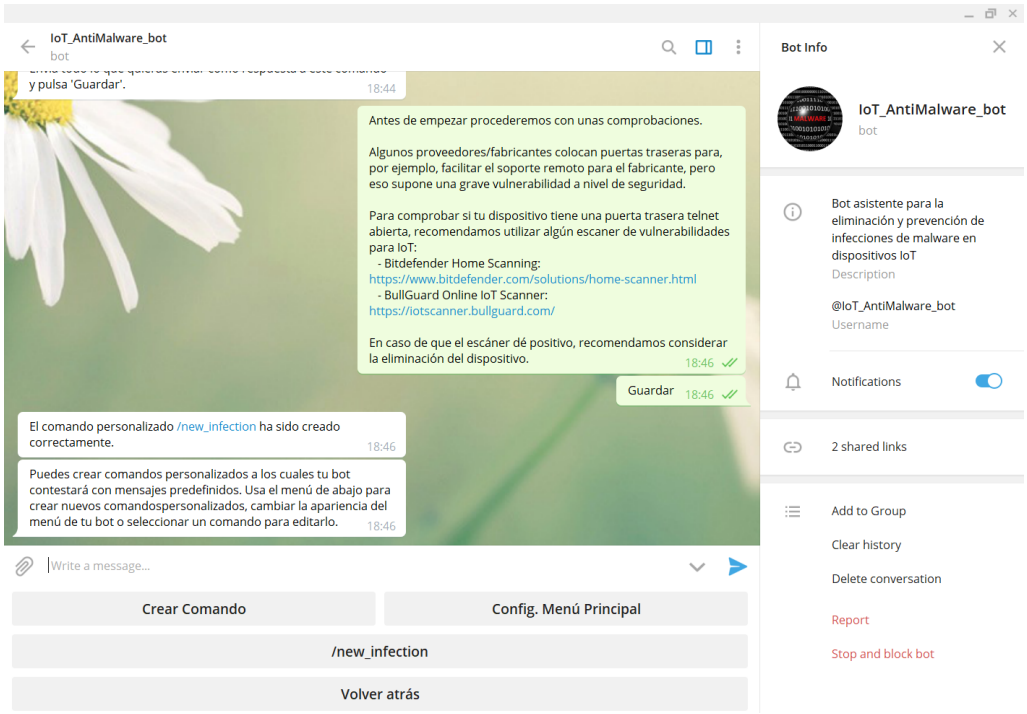


Ilustración 26: Creación de bot de Telegram 7

Una vez el mensaje haya sido enviado y guardado, y tengamos confirmación de que el comando se ha creado correctamente, procederemos a crear el resto de comandos necesarios para nuestro *bot*, concretamente, crearemos los comandos “/ini”, “/what_is”, “/how_to”, “/next”, “/cant_connect”, “/cant_modify”, “/done” y “/close” siguiendo los mismos pasos que con el comando “/new_infection”.

También crearemos un comando llamado “/rate_and_comment” que en lugar de simplemente mostrar texto realizará preguntas al usuario:

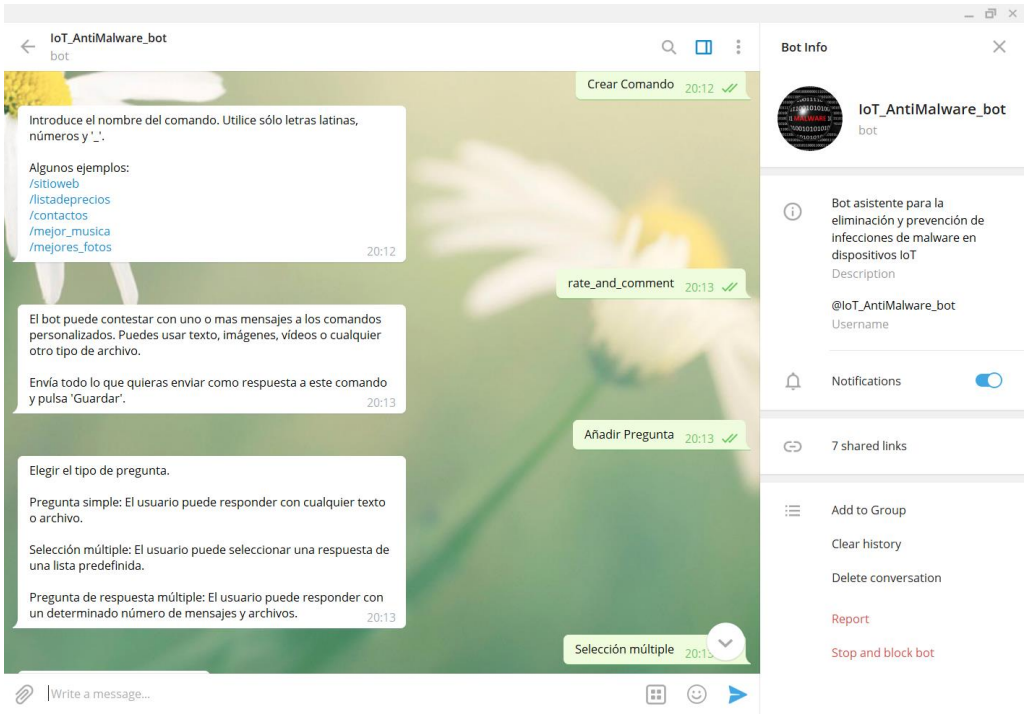


Ilustración 27: Creación de bot de Telegram 8

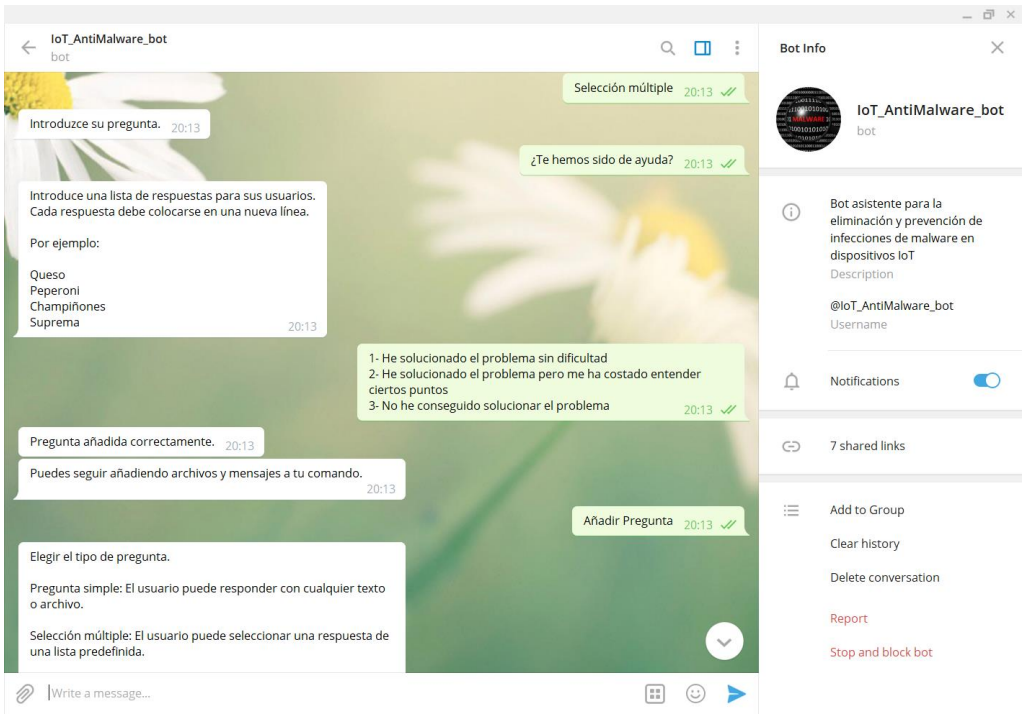


Ilustración 28: Creación de bot de Telegram 9

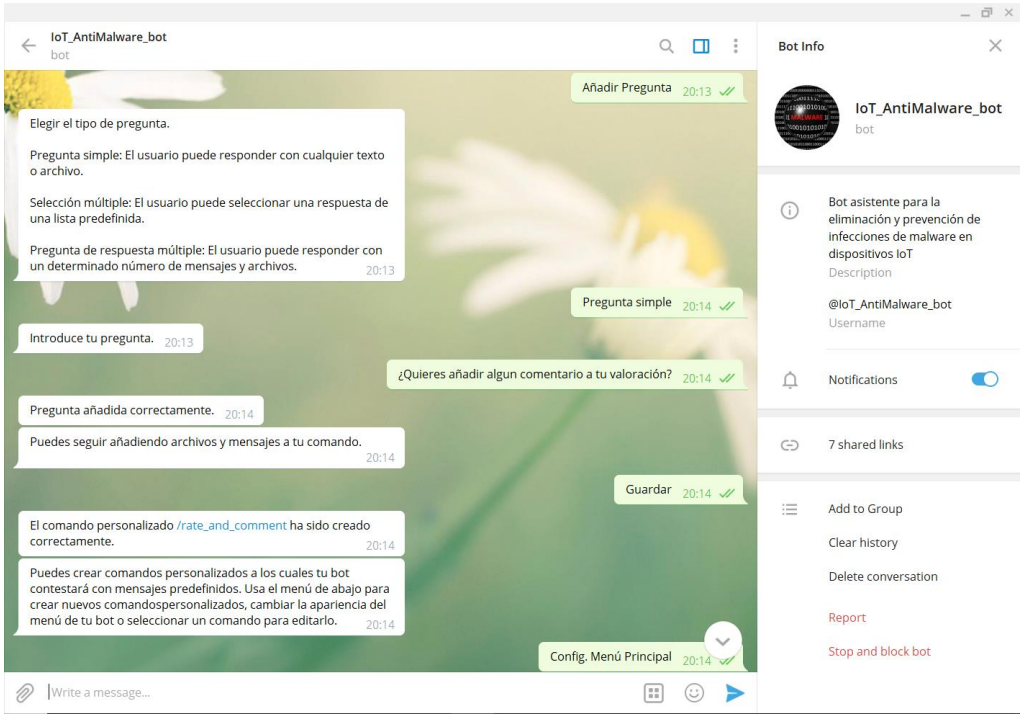


Ilustración 29: Creación de bot de Telegram 10

Una vez creados todos los comandos pasaremos a configurar el menú, los botones que utilizarán los usuarios para moverse a través del chatbot. Esto lo haremos a través de “Comandos personalizadas” > “Config. Menú principal” > “+ Añadir Opción al Menú +”.

Al seleccionar la opción se nos pedirá escoger el comando que se ejecutará al pulsar el botón, para ello tenemos que escoger el comando deseado de entre la lista de comandos disponibles que aparecerá en lugar del menú. Tras esto solo quedará darle un nombre al botón y se creará el primer botón del menú principal.

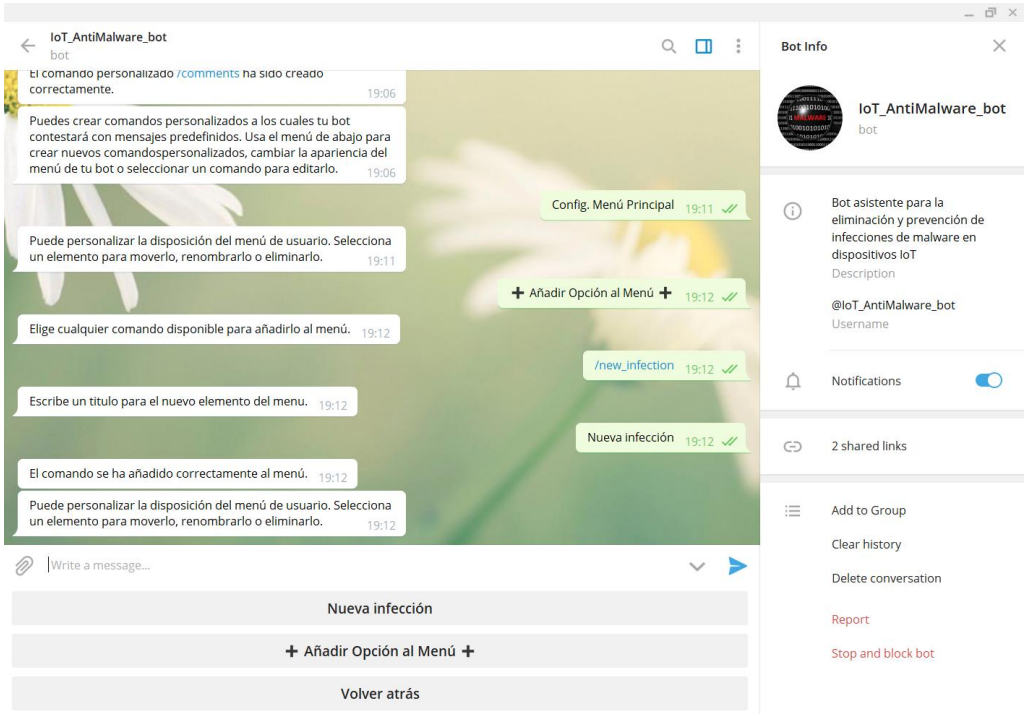


Ilustración 30: Creación de bot de Telegram 11

Seguidamente podríamos crear más botones para el menú principal, pero de acuerdo con el diseño que hicimos no es necesario, sino que tocaría proceder a crear un seguido de botones que aparecieran tras haber pulsado otro botón, es decir, que tras pulsar, por ejemplo, “Nueva infección”, este menú desapareciera y apareciera otro con botones distintos. Esto podemos lograrlo mediante submenús, para ello seleccionamos el botón dentro del cual queremos crear un submenú y veremos que aparecen varias opciones relativas al botón junto con otra vez el nombre del botón escogido:

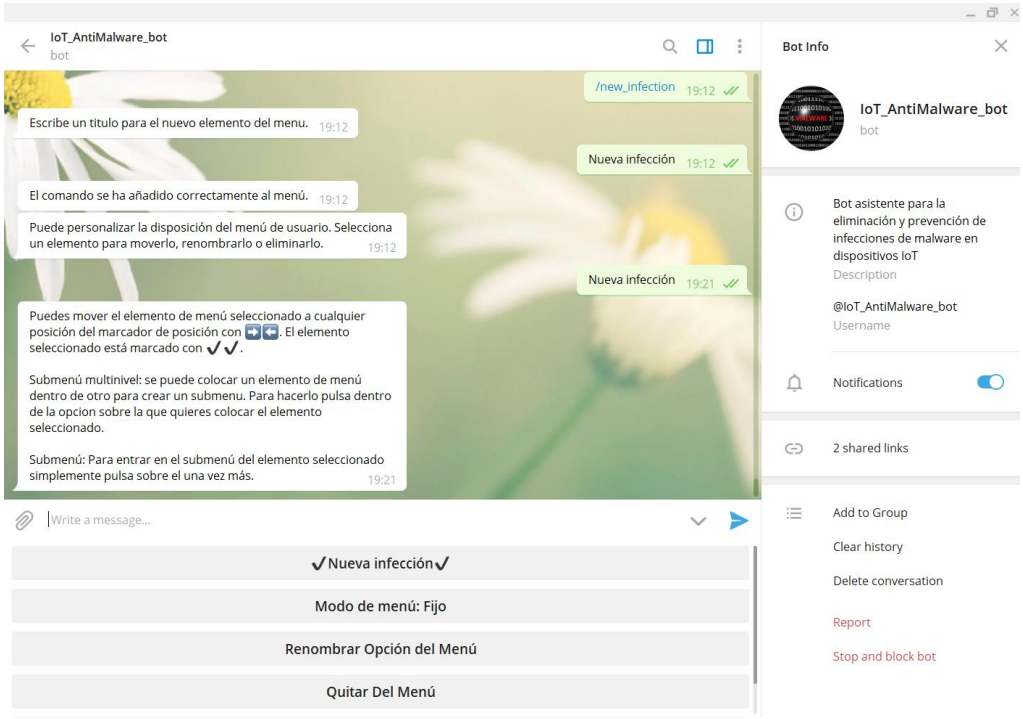


Ilustración 31: Creación de bot de Telegram 12

Tal y como aparece en los mensajes de ayuda, si pulsamos el botón marcado con "✓ ✓" tendremos la posibilidad de añadir un botón en el submenú del botón escogido.

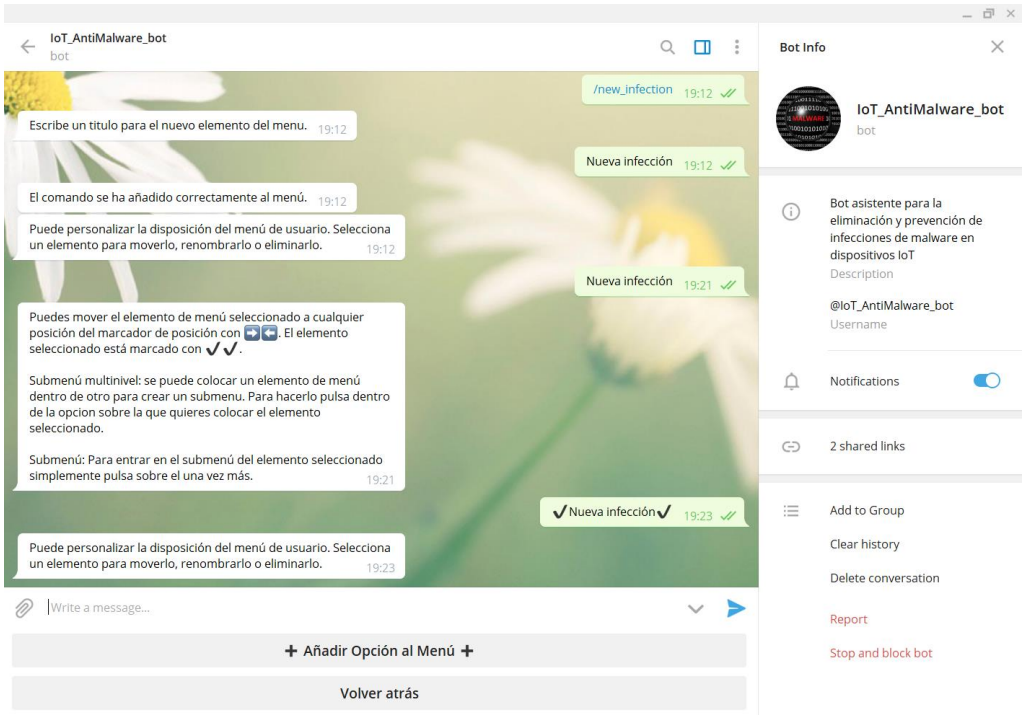


Ilustración 32: Creación de bot de Telegram 13

Procederemos ahora a crear los distintos botones en los distintos menús y submenús, y a asignarles sus respectivos comandos de acuerdo con la estructura siguiente:

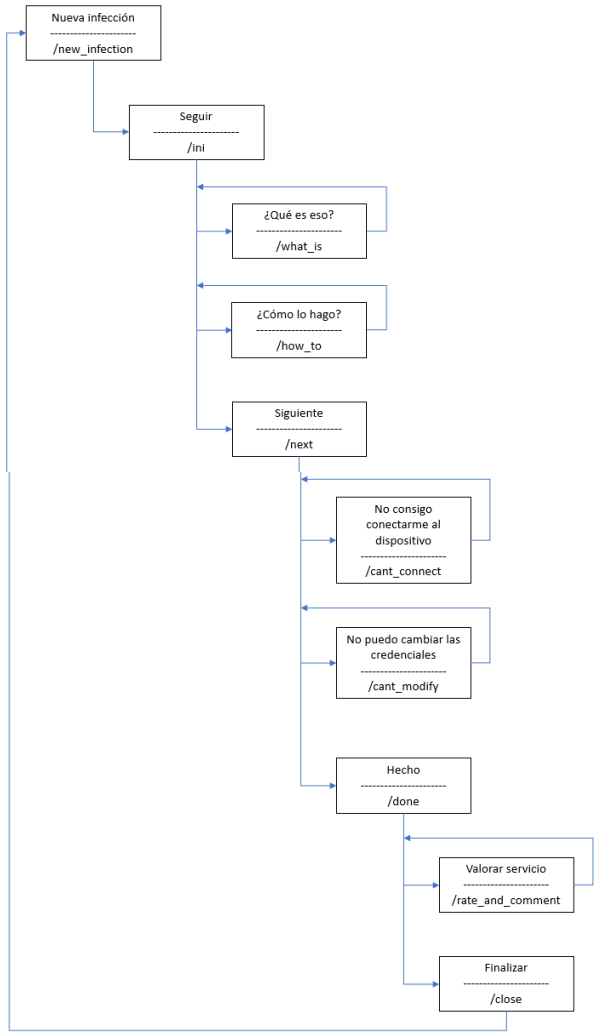


Ilustración 33: Diagrama de flujo del chatbot

Para finalizar, realizaremos un cambio en el último botón. Puesto que queremos que el usuario sea devuelto al menú principal una vez haya acabado de realizar el procedimiento, cambiaremos su modo de Fijo a Ocultar. Para ello accederemos al botón y seleccionaremos “Modo de menú: Fijo”:

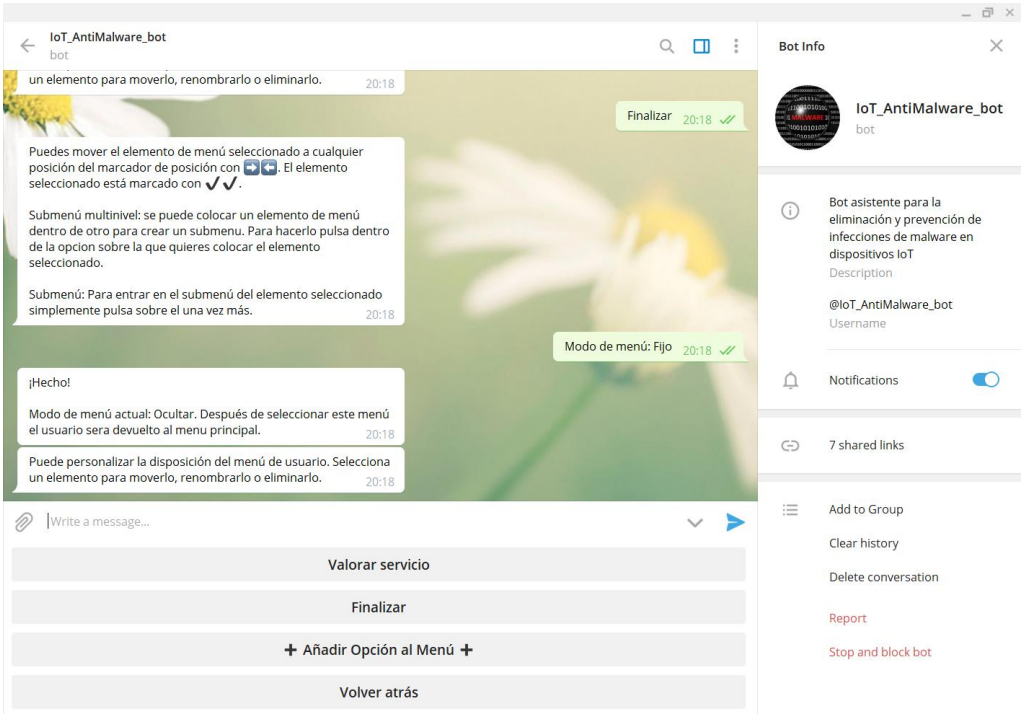
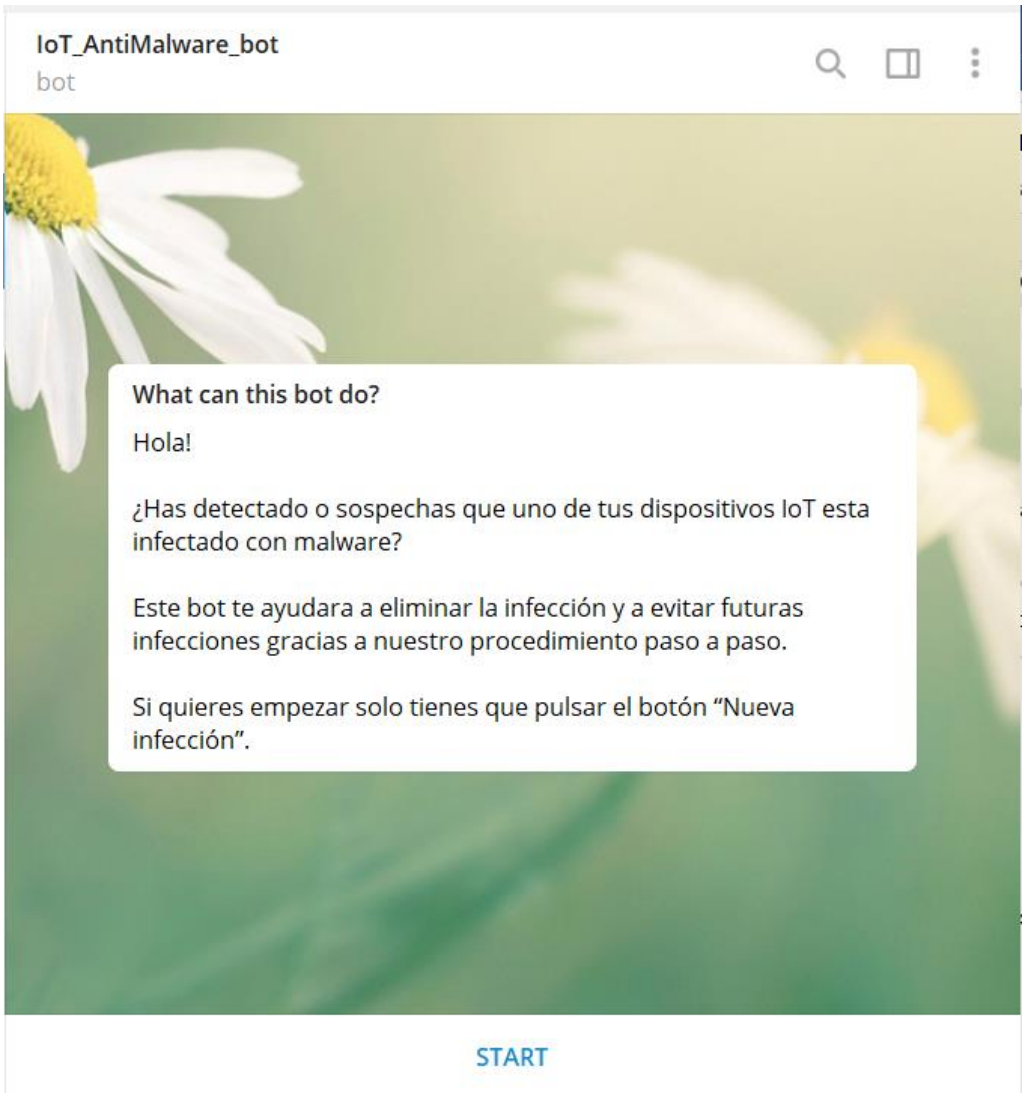
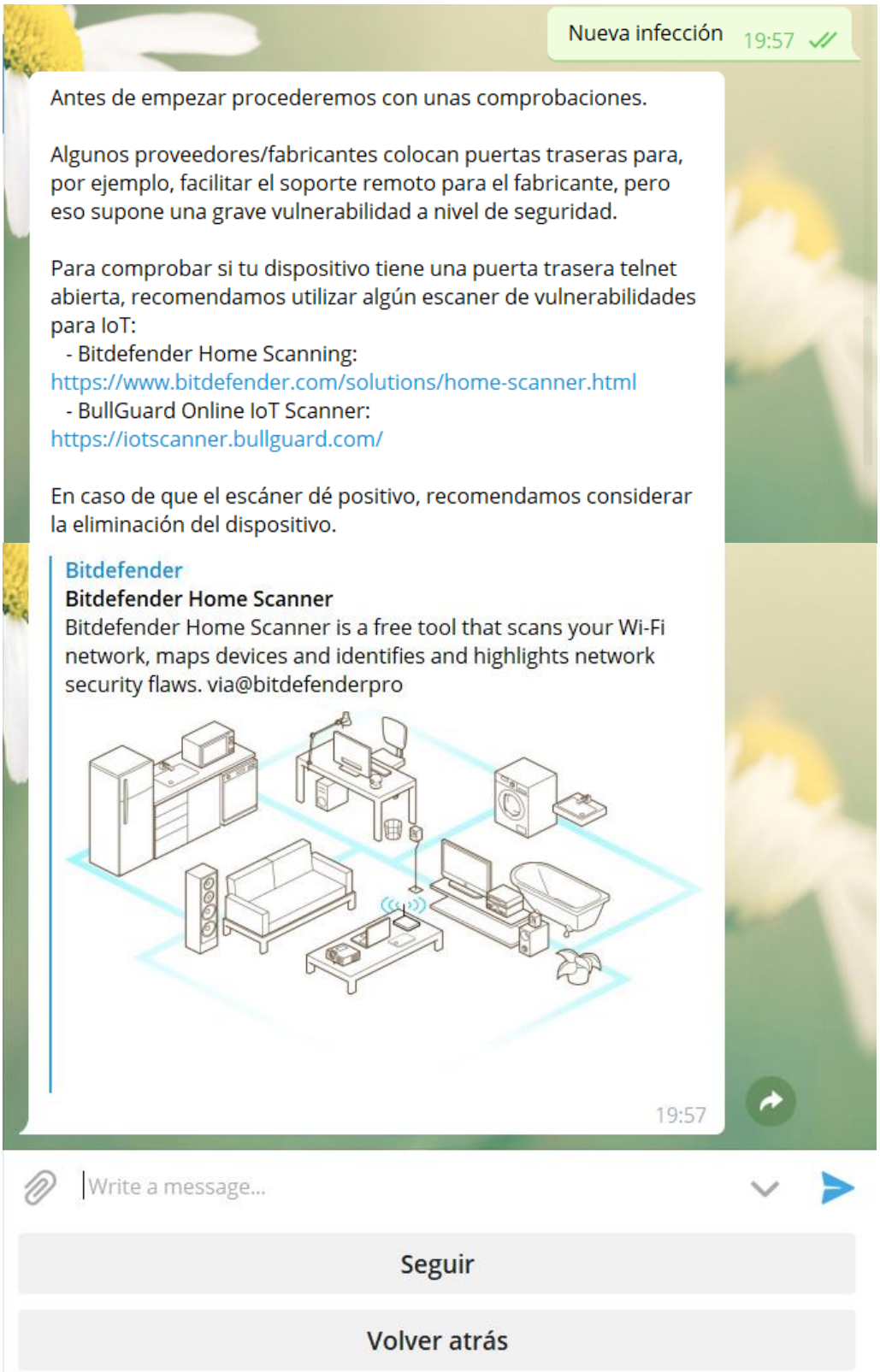


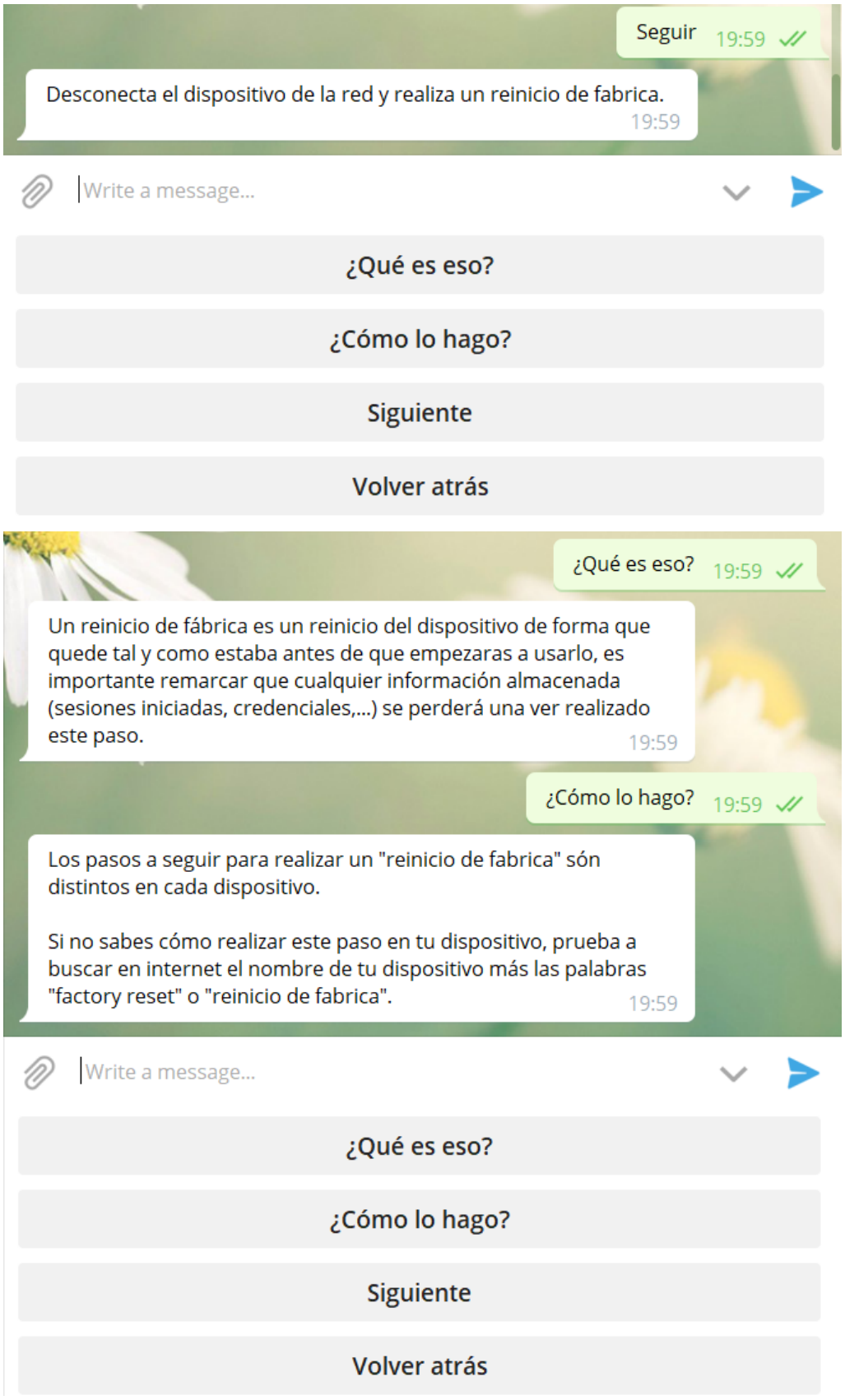
Ilustración 34: Creación de bot de Telegram 14

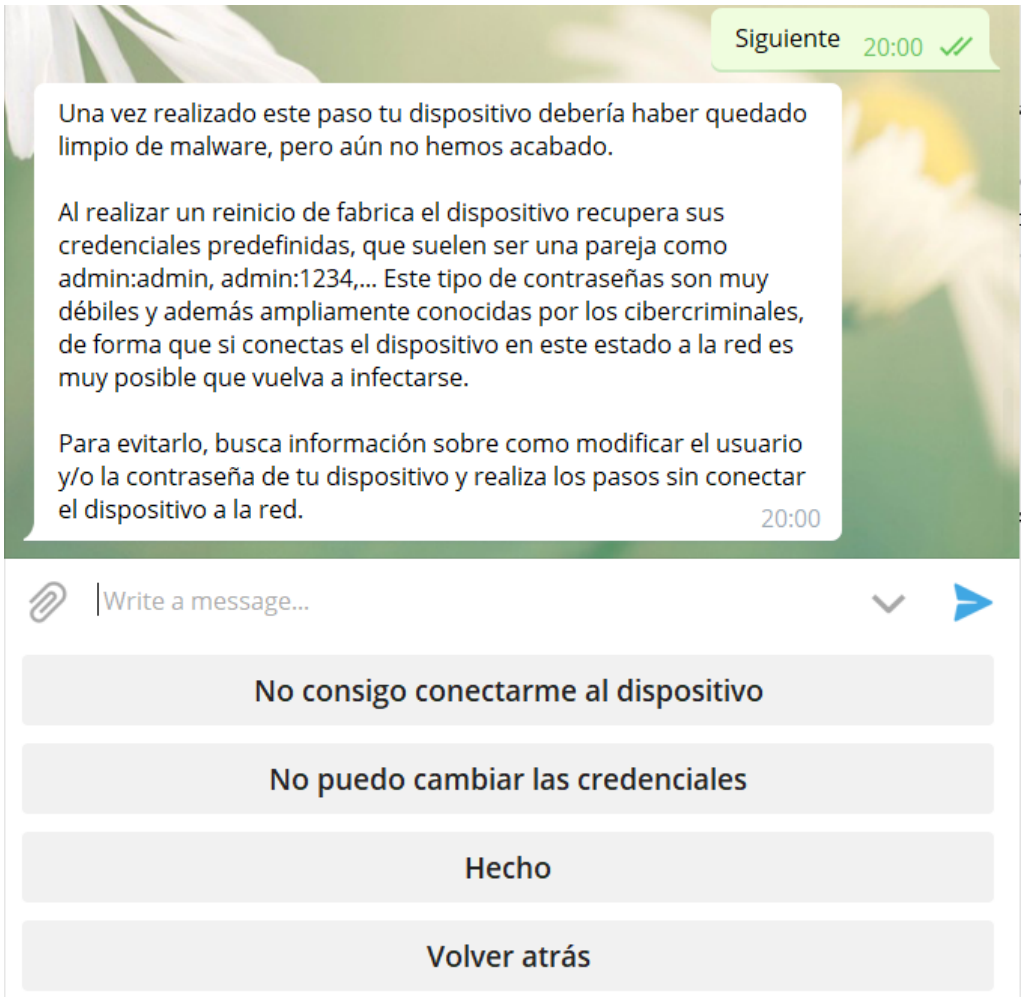
Una vez acabados todos los pasos anteriores se obtendrá el siguiente resultado final:

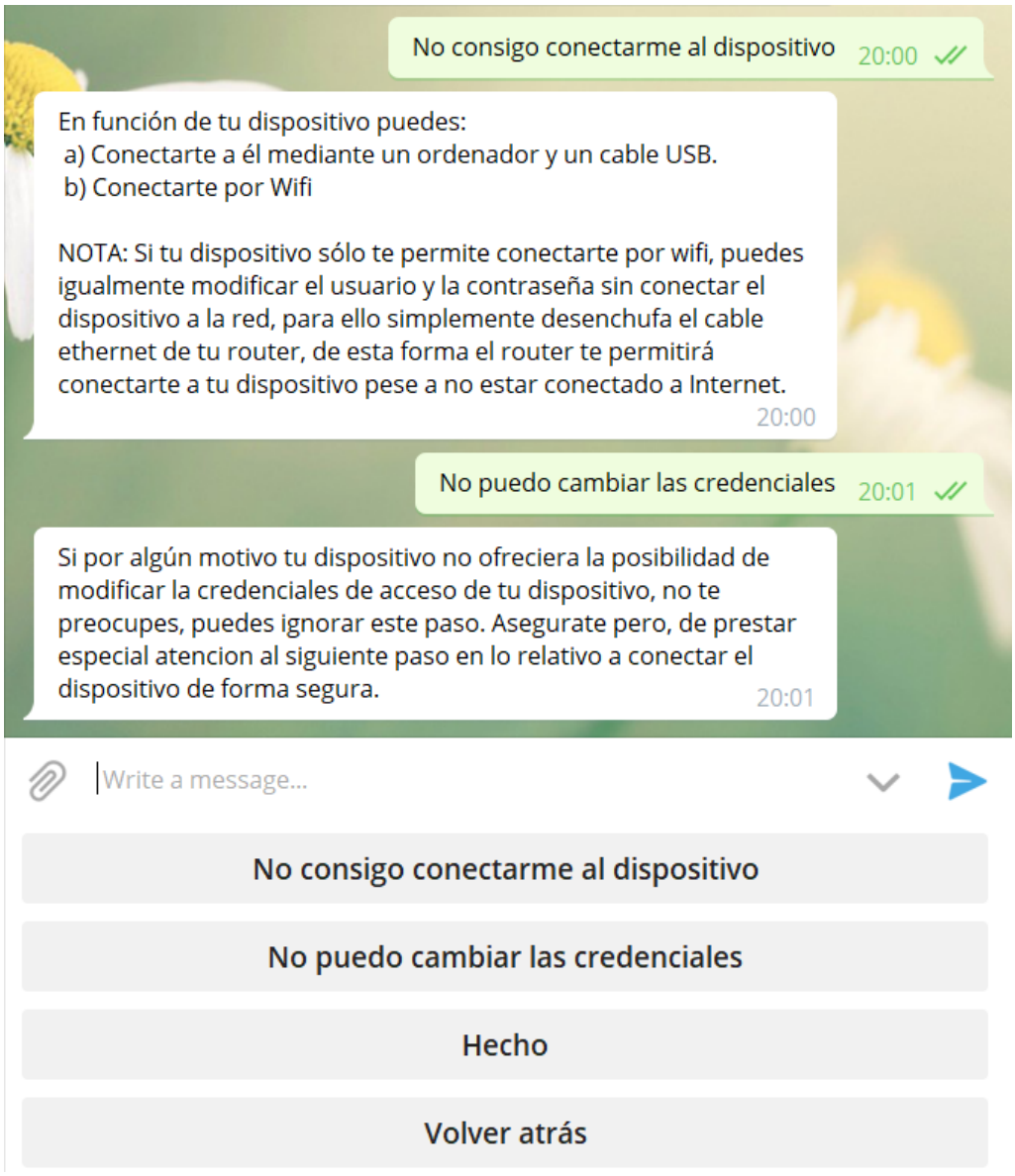

IoT_AntiMalware_bot
bot
What can this bot do?
Hola!
¿Has detectado o sospechas que uno de tus dispositivos IoT esta infectado con malware?
Este bot te ayudara a eliminar la infección y a evitar futuras infecciones gracias a nuestro procedimiento paso a paso.
Si quieres empezar solo tienes que pulsar el botón “Nueva infección”.
START

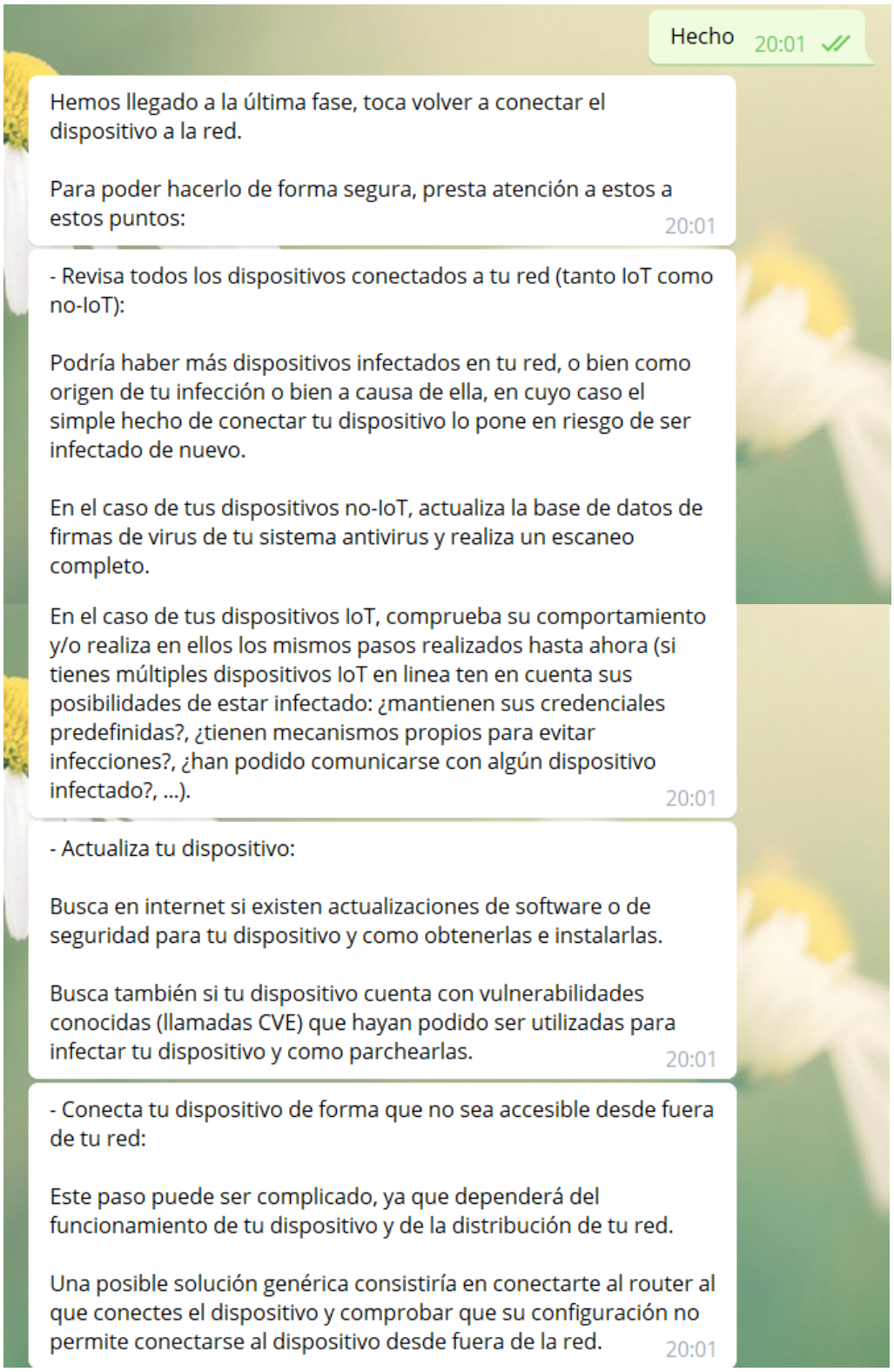

/start 19:56
¡Felicidades! Te has suscrito a IoT_AntiMalware_bot.
Usa /off para parar tu suscripción. 19:56
Write a message...
Nueva infección

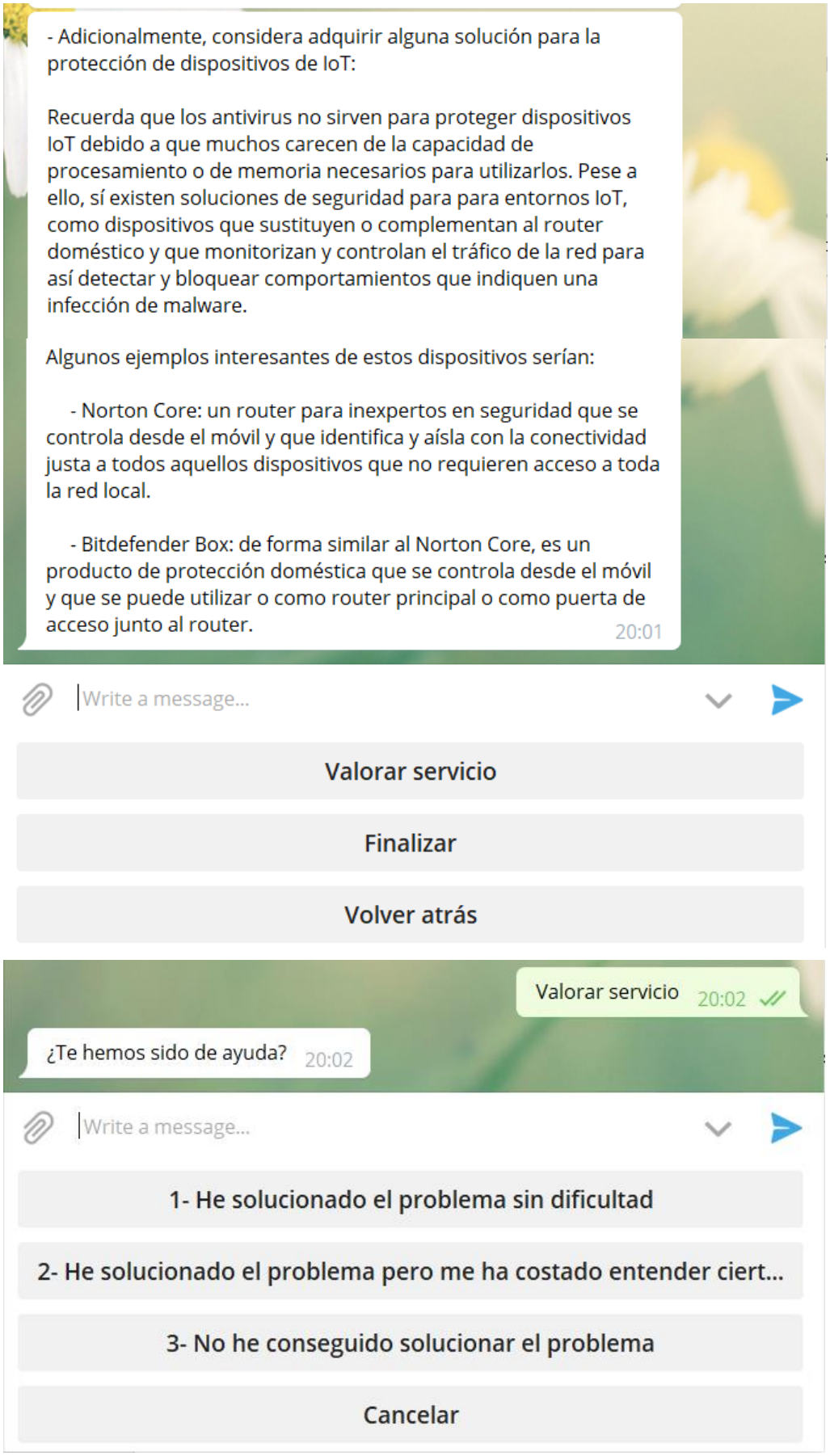

Nueva infección 19:57
Antes de empezar procederemos con unas comprobaciones.
Algunos proveedores/fabricantes colocan puertas traseras para, por ejemplo, facilitar el soporte remoto para el fabricante, pero eso supone una grave vulnerabilidad a nivel de seguridad.
Para comprobar si tu dispositivo tiene una puerta trasera telnet abierta, recomendamos utilizar algún escaner de vulnerabilidades para IoT:
- Bitdefender Home Scanning:
https://www.bitdefender.com/solutions/home-scanner.html
- BullGuard Online IoT Scanner:
https://iotscanner.bullguard.com/
En caso de que el escáner dé positivo, recomendamos considerar la eliminación del dispositivo.
Bitdefender
Bitdefender Home Scanner
Bitdefender Home Scanner is a free tool that scans your Wi-Fi network, maps devices and identifies and highlights network security flaws. via@bitdefenderpro
19:57
Write a message...
Seguir
Volver atrás


Seguir 19:59
Desconecta el dispositivo de la red y realiza un reinicio de fabrica. 19:59
Write a message...
¿Qué es eso?
¿Cómo lo hago?
Siguiente
Volver atrás
¿Qué es eso? 19:59
Un reinicio de fábrica es un reinicio del dispositivo de forma que quede tal y como estaba antes de que empezaras a usarlo, es importante remarcar que cualquier información almacenada (sesiones iniciadas, credenciales,...) se perderá una ver realizado este paso. 19:59
¿Cómo lo hago? 19:59
Los pasos a seguir para realizar un "reinicio de fabrica" són distintos en cada dispositivo.
Si no sabes cómo realizar este paso en tu dispositivo, prueba a buscar en internet el nombre de tu dispositivo más las palabras "factory reset" o "reinicio de fabrica". 19:59
Write a message...
¿Qué es eso?
¿Cómo lo hago?
Siguiente
Volver atrás


Siguiente 20:00
Una vez realizado este paso tu dispositivo debería haber quedado limpio de malware, pero aún no hemos acabado.
Al realizar un reinicio de fabrica el dispositivo recupera sus credenciales predefinidas, que suelen ser una pareja como admin:admin, admin:1234,... Este tipo de contraseñas son muy débiles y además ampliamente conocidas por los cibercriminales, de forma que si conectas el dispositivo en este estado a la red es muy posible que vuelva a infectarse.
Para evitarlo, busca información sobre como modificar el usuario y/o la contraseña de tu dispositivo y realiza los pasos sin conectar el dispositivo a la red.
20:00
Write a message...
No consigo conectarme al dispositivo
No puedo cambiar las credenciales
Hecho
Volver atrás


No consigo conectarme al dispositivo 20:00
En función de tu dispositivo puedes:
a) Conectarte a él mediante un ordenador y un cable USB.
b) Conectarte por Wifi
NOTA: Si tu dispositivo sólo te permite conectarte por wifi, puedes igualmente modificar el usuario y la contraseña sin conectar el dispositivo a la red, para ello simplemente desenchufa el cable ethernet de tu router, de esta forma el router te permitirá conectarte a tu dispositivo pese a no estar conectado a Internet.
20:00
No puedo cambiar las credenciales 20:01
Si por algún motivo tu dispositivo no ofreciera la posibilidad de modificar la credenciales de acceso de tu dispositivo, no te preocupes, puedes ignorar este paso. Asegurate pero, de prestar especial atencion al siguiente paso en lo relativo a conectar el dispositivo de forma segura.
20:01
Write a message...
No consigo conectarme al dispositivo
No puedo cambiar las credenciales
Hecho
Volver atrás


Hecho 20:01
Hemos llegado a la última fase, toca volver a conectar el dispositivo a la red.
Para poder hacerlo de forma segura, presta atención a estos a estos puntos:
20:01
- Revisa todos los dispositivos conectados a tu red (tanto IoT como no-IoT):
Podría haber más dispositivos infectados en tu red, o bien como origen de tu infección o bien a causa de ella, en cuyo caso el simple hecho de conectar tu dispositivo lo pone en riesgo de ser infectado de nuevo.
En el caso de tus dispositivos no-IoT, actualiza la base de datos de firmas de virus de tu sistema antivirus y realiza un escaneo completo.
En el caso de tus dispositivos IoT, comprueba su comportamiento y/o realiza en ellos los mismos pasos realizados hasta ahora (si tienes múltiples dispositivos IoT en linea ten en cuenta sus posibilidades de estar infectado: ¿mantienen sus credenciales predefinidas?, ¿tienen mecanismos propios para evitar infecciones?, ¿han podido comunicarse con algún dispositivo infectado?, ...).
20:01
- Actualiza tu dispositivo:
Busca en internet si existen actualizaciones de software o de seguridad para tu dispositivo y como obtenerlas e instalarlas.
Busca también si tu dispositivo cuenta con vulnerabilidades conocidas (llamadas CVE) que hayan podido ser utilizadas para infectar tu dispositivo y como parchearlas.
20:01
- Conecta tu dispositivo de forma que no sea accesible desde fuera de tu red:
Este paso puede ser complicado, ya que dependerá del funcionamiento de tu dispositivo y de la distribución de tu red.
Una posible solución genérica consistiría en conectarte al router al que conectes el dispositivo y comprobar que su configuración no permite conectarse al dispositivo desde fuera de la red.
20:01


- Adicionalmente, considera adquirir alguna solución para la protección de dispositivos de IoT:
Recuerda que los antivirus no sirven para proteger dispositivos IoT debido a que muchos carecen de la capacidad de procesamiento o de memoria necesarios para utilizarlos. Pese a ello, sí existen soluciones de seguridad para para entornos IoT, como dispositivos que sustituyen o complementan al router doméstico y que monitorizan y controlan el tráfico de la red para así detectar y bloquear comportamientos que indiquen una infección de malware.
Algunos ejemplos interesantes de estos dispositivos serían:
- Norton Core: un router para inexpertos en seguridad que se controla desde el móvil y que identifica y aísla con la conectividad justa a todos aquellos dispositivos que no requieren acceso a toda la red local.
- Bitdefender Box: de forma similar al Norton Core, es un producto de protección doméstica que se controla desde el móvil y que se puede utilizar o como router principal o como puerta de acceso junto al router.
20:01
Write a message...
Valorar servicio
Finalizar
Volver atrás
Valorar servicio 20:02
¿Te hemos sido de ayuda? 20:02
Write a message...
1- He solucionado el problema sin dificultad
2- He solucionado el problema pero me ha costado entender ciert...
3- No he conseguido solucionar el problema
Cancelar

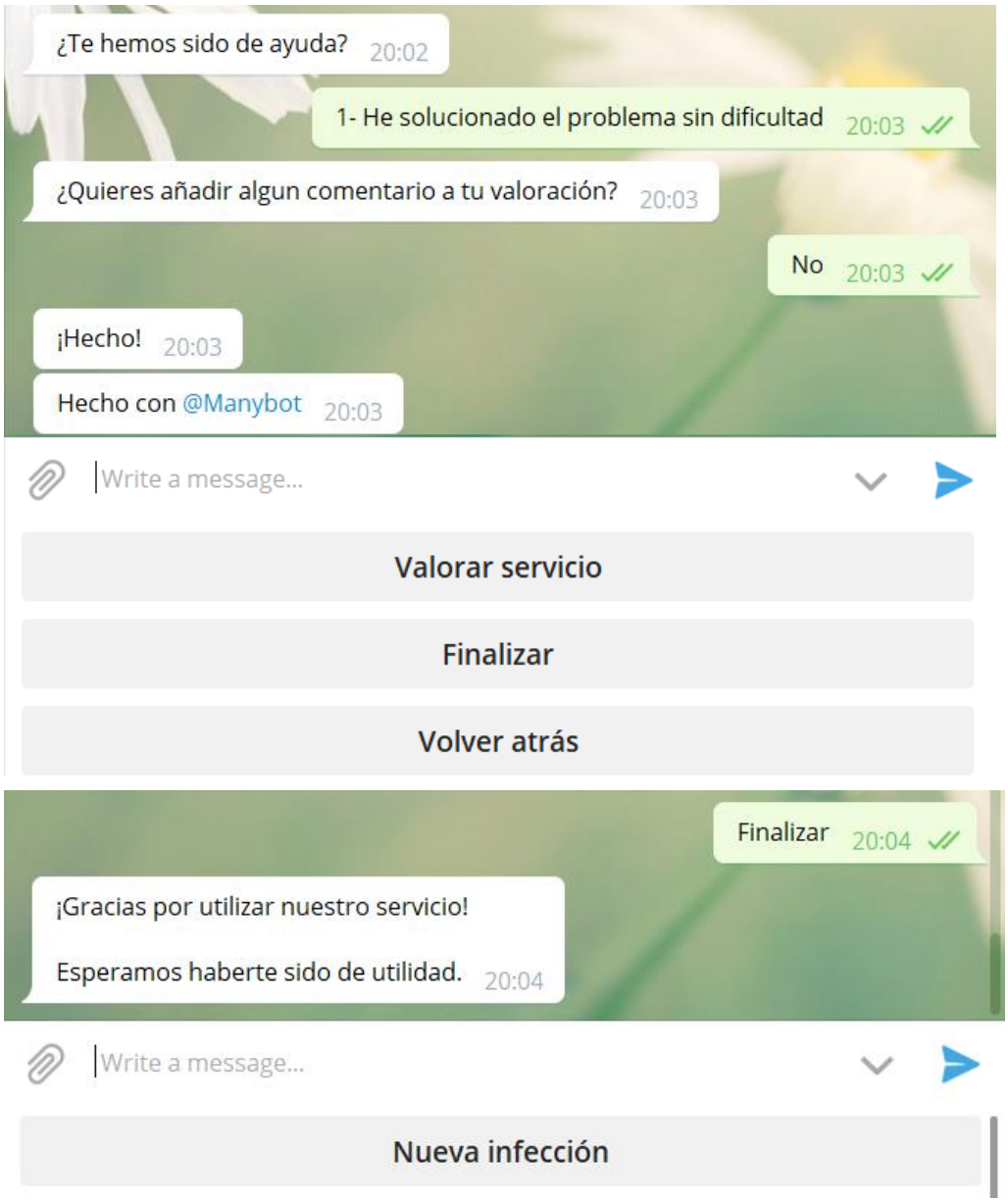


Ilustración 35: Resultado final de la implementación del chatbot

6. Conclusiones

El resultado final del proyecto ha sido el esperado y se han podido alcanzar satisfactoriamente sus dos objetivos principales, desarrollar un procedimiento genérico para limpiar de *malware* dispositivos *IoT* infectados y una solución que lo implemente para poder asistir a los usuarios en el proceso, todo ello sin necesidad de aplicar ningún cambio especialmente relevante ni en las metodologías ni en la planificación prevista.

Pese a esto, el proyecto aún seria susceptible de ser expandido de múltiples formas, ya que debido al tiempo y recursos disponibles hemos desarrollado una solución que no aprovecha al máximo el potencial de la tecnología de los *chatbots.*

Una de las posibles líneas de desarrollo pasaría por integrar el *chatbot* con una plataforma de *ticketing* como Zendesk, lo que permitiría a las *ISPs* tener un registro de las incidencias reportadas y de su resultado.

Otra posible vía seria la integración de una IA para resolver las dudas de los usuarios acerca del procedimiento (bien en sustitución o en adición de los mensajes de ayuda incluidos durante la implementación del *chatbot*), y es que, si bien esta opción se rechazó inicialmente, considero que sí podría resultar una característica interesante de cara a un complemento de soporte.

7. Glosario

- Botnet: grupo de dispositivos electrónicos infectados y controlados por un atacante de forma remota.

- Command and Control (C&C o C2): parte de una *botnet* encargada de enviar comandos y de controlar a los dispositivos que la integran.

- Chatbot: programa informático que simula mantener conversaciones con usuarios mediante el uso de respuestas automáticas a entradas hechas estos.

- Data stealer: tipo de *malware* dedicado a recabar información de un dispositivo (por ejemplo: contraseñas, números de tarjetas de crédito, …) y a transmitirla a un atacante.

- DDoS: ataque de denegación de servicio, también llamado ataque DoS (por sus siglas en inglés, Denial of Service). Es un tipo de ataque informático que causa que un servicio o recurso no sea accesible para los usuarios.

- Frameworks: entorno pensado para proporcionar una base con la que facilitar la programación de aplicaciones o herramientas.

- Internet of Things (IoT): hace referencia a cualquier objeto cotidiano interconectado con otro/s objeto/s mediante Internet.

- ISP: proveedor de servicios de Internet, (ISP, por las siglas en inglés de Internet service provider). Es toda aquella empresa que proporciona conexión a Internet a sus clientes.

- Keylogger: tipo *malware* dedicado a capturar y enviar a un atacante las pulsaciones del teclado de un dispositivo infectado.

- Malware: programa informático de origen malicioso que trata de afectar a un dispositivo electrónico.

- Payload: parte del *malware* que realiza la acción maliciosa.

- Ransomware: tipo de *malware* que impide que los usuarios accedan a determinadas partes de su sistema operativo o a sus archivos personales y que pide un rescate a cambio de devolverles el acceso.

- SSH (Secure Shell): protocolo y programa que lo implementa que permite el acceso remoto a dispositivo por medio de un canal seguro en el que toda la información está cifrada.

- Telnet: protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

- Troyano: tipo de *malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que lleva a cabo acciones maliciosas al ejecutarlo.

8. Bibliografía

[1] Recuperada de: https://www.verdict.co.uk/wp-content/uploads/2018/12/botnet-600x334.png

[2] Veredict, Priya Kantaria, 05/12/2018, <<Rise of the IoT botnet: The problem in securing hundreds of billions of connected devices>>, https://www.verdict.co.uk/rise-of-the-iot-botnet/

[3] Chatbots Magazine, Parlo, 19/12/2017, <<The 3 Essentials of AI Bots for IT Help Desk>>, https://chatbotsmagazine.com/the-3-essentials-of-ai-bots-for-it-help-desk-9bce2ffa4446

[4] Guelcom, Alejandra L Villar, 28/12/2018, <<9 empresas usan chatbots: casos de éxito>>, https://guelcom.net/9-empresas-usan-chatbots-casos-exito/

[5] Tech Talks, Ben Dickson, 22/08/2016, << The IoT ransomware threat is more serious than you think >>, https://bdtechtalks.com/2016/08/22/the-iot-ransomware-threat-is-more-serious-than-you-think/

[6] CSO, Simon Howe, 27/08/2018, << Why IoT could be the next ransomware target >>, https://www.cso.com.au/article/645755/why-iot-could-next-ransomware-target/

[7] Recuperada de: http://domainingafrica.com/transportation-industry-vulnerable-ransomware-iot-attacks/

[8] Recuperada de: https://www.researchgate.net/figure/Mirai-botnet-operation-and-communication-Mirai-causes-a-distributed-denial-of-service_fig1_318288727

[9] Berkeley (Universidad de California), Ehimare Okoyomon, 07/11/2018, <<The Mirai Botnet>>, https://inst.eecs.berkeley.edu/~cs261/fa18/presentations/11_05_01.pdf

[10] Silicon Week, Karen Ortega, 13/03/2018, <<Alerta: nueva variante de malware Mirai>>, https://www.siliconweek.com/e-enterprise/alerta-nueva-variante-malware-mirai-94608

[11] IoT Security News, 05/2018, <<7 Variants of Mirai (So Far)>>, http://iotsecuritynews.com/7-variants-of-mirai-so-far/

[12] Recuperada de: https://www.bleepingcomputer.com/news/security/58-percent-of-botnet-malware-infections-last-under-a-day/

[13] Corero, <<Mirai Botnet DDoS Attack Type>>, https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

[14] IBM, J Steven Perry, 31/10/2017, <<Anatomy of an IoT malware attack>>, https://developer.ibm.com/articles/iot-anatomy-iot-malware-attack/

[15] Recuperada de: http://docs.ruckuswireless.com/iot/iot-1.0-controllerguide/GUID-8414DE2E-DA50-48C0-9074-8F94E614B015.html

[16] Brigham Young University, Dylan Valverde, 26/03/2018, <<A Brief History of Chatbots>>, https://pcc.cs.byu.edu/2018/03/26/a-brief-history-of-chatbots/

[17] ABC, Jon Oleaga, 25/09/2017, <<En 2020 habrá diez dispositivos conectados a cada persona>>, https://www.abc.es/tecnologia/informatica/software/abci-christian-morales-intel-2020-habra-diez-dispositivos-conectados-cada-persona-201603040454_noticia.html

[18] Recuperada de: https://blogginzenith.zenithmedia.es/wp-content/uploads/2018/04/iot-datos.jpg

[19] Recuperada de: https://media.threatpost.com/wp-content/uploads/sites/103/2018/09/18141701/TL-1.png

[20] Recuperada de: https://www.synpulse.com/en/publications/article-en/get-ready-for-chatbots-part-1

[21] Planeta Chatbot, Planeta Chatbot, 29/05/2017, <<¿Qué tipos de chatbots existen?>>, https://planetachatbot.com/tipos-de-chatbots-40682128324

[22] EngageBS, Enedino Villaverde Page, 01/01/2018, <<¿Que son los Chatbots y que tipos hay?>>, https://www.engagebs.com/2018/01/01/los-chatbots-tipos/

[23] Marketing 4 Ecommerce, Alberto González, 19/06/2018, <<Movistar, la primera teleco del mundo en contar con un chatbot conectado al call center>>, https://marketing4ecommerce.net/movistar-la-primera-teleco-del-mundo-contar-chatbot-conectado-al-call-center/

[24] Movistar, Movistar, 19/06/2018, <<Movistar y Twitter desarrollan una solución pionera de atención al cliente a través de un bot>>, https://comunidad.movistar.es/t5/Blog-Movisfera/Movistar-y-Twitter-desarrollan-una-soluci%C3%B3n-pionera-de-atenci%C3%B3n/ba-p/3497860

[25] Perspectiva, Diario Perspectiva, 19/06/2018, <<Movistar conecta un "chatbot" a su "call center" de Twitter>>, https://diarioperspectiva.com/movistar-conecta-un-chatbot-a-su-call-center-de-twitter/

[26] Econsultancy, Ben Davis, 11/10/2018, <<Vodafone's chatbot is delivering double the conversion rate of its website>>, https://econsultancy.com/vodafones-chatbot-is-delivering-twice-the-conversion-rate-of-its-website/

[27] Vodafone, Vodafone, 13/11/2017, <<Meet TOBi – the first live chatbot in UK telecoms>>, http://labs.vodafone.co.uk/case-studies/tobi

[28] Recuperada de: https://www.youtube.com/watch?v=d402EY-AZ-w

[29] Threat Post, Lindsey O'Donnell, 18/09/2018, <<ThreatList: Malware Samples Targeting IoT More Than Double in 2018>>, https://threatpost.com/threatlist-malware-samples-targeting-iot-more-than-double-in-2018/137528/

[30] Recuperada de: https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

[31] Recuperada de: https://www.bitdefender.com/solutions/home-scanner.html

[32] Recuperada de: https://iotscanner.bullguard.com/

[33] Recuperada de: https://www.xataka.com/perifericos/norton-core-es-el-router-preparado-para-la-iot-que-no-solo-te-conecta-sino-que-ademas-te-protege

[34] Recuperada de: https://www.pcmag.com/review/357433/bitdefender-box-2

[35] Snatchbot, https://es.snatchbot.me/

[36] Botstar, https://botstar.com/

[37] Chatfuel, https://chatfuel.com/

[38] El Zompopo Electronico, Mcalle, 22/02/2017, <<¿Cómo crear un bot de Telegram sin programar? I>>, http://www.elzompopoelectronico.com.es/2017/02/como-crear-un-bot-de-telegram-sin.html

[39] El Android libre, Manuel J. Gutiérrez, 21/02/2018, <<Cómo crear tu propio bot de Telegram paso a paso>>, https://elandroidelibre.elespanol.com/2018/02/como-crear-tu-propio-bot-de-telegram.html

[40] GeekFlare, Chandan Kumar, 22/04/2018, <<10 Tools to Create Your Personal or Business Chatbot>>, https://geekflare.com/create-chatbot/