CSDE

Council to Secure the Digital Economy

GUÍA DE SEGURIDAD INTERNACIONAL DE BOTNET Y IOT 2020

US ECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association™

AVISO

La Guía Internacional de Seguridad de Botnets y IoT fue desarrollada para facilitar la mitigación de botnets y otras amenazas automatizadas y distribuidas a través de la participación voluntaria y la colaboración entre las distintas partes interesadas en todo el ecosistema global de Internet y las comunicaciones. La Guía proporciona información y aliento a las partes interesadas en las tecnologías de la información y las comunicaciones (TIC) sobre las medidas afirmativas que deben aplicarse para lograr este objetivo, según lo que consideren apropiado, sobre la base de sus circunstancias individuales y sus relaciones entre sí.

La Guía destaca las prácticas voluntarias de impacto para cada segmento del sector de las TIC, que van desde las "básicas" hasta las "avanzadas". Aunque los líderes del sector que han elaborado esta Guía reconocen que ninguna combinación de medidas puede garantizar la eliminación de todas las amenazas y riesgos, creen que estas
tanto de referencia como avanzadas, presentan un marco valioso para que las partes interesadas en las TIC se refieran a la identificación y elección de sus propias prácticas para mitigar las amenazas de los ataques automatizados y distribuidos. La Guía reconoce que las diferentes partes interesadas en las TIC se enfrentan a diferentes retos, consideraciones y prioridades a la hora de implementar medidas de seguridad. En consecuencia, las prácticas identificadas en esta Guía, y la Guía en su conjunto, son herramientas que las partes interesadas en las TIC deben aplicar según sus circunstancias; no son requisitos ni mandatos, ni son obligatorias en modo alguno.

Muchas de las prácticas y tecnologías analizadas en este documento ya son utilizadas por las grandes empresas para proteger sus redes y sistemas, desde la contratación de inspección profunda de paquetes (DPI) a los proveedores de servicios de red hasta la prohibición del uso de dispositivos que no tengan suficientes medidas de seguridad incorporadas. Sin embargo, la aplicación de estas capacidades en el espacio de los consumidores en general tiene implicaciones políticas más amplias. Por ejemplo:

Capacidades avanzadas como el DPI del tráfico IP, aunque útiles en ciertos contextos, podrían tener implicaciones significativas para la privacidad individual si se despliegan en las redes públicas.

- Si los gobiernos lo exigen para cumplir otros objetivos políticos, el filtrado del tráfico de la red pública basado en las direcciones IP y otros medios también puede tener implicaciones para la libre circulación de la información.

Las empresas cuentan con personal informático cualificado que negocia los requisitos detallados con sus proveedores e incorpora los análisis de costes y beneficios en la toma de decisiones. Esta dinámica no existe en el espacio de los consumidores, donde el análisis coste-beneficio puede diferir significativamente del de una empresa a gran escala. En el caso de los consumidores, las cuestiones relacionadas con los costes y la protección del consumidor tendrán que evaluarse en una escala de gestión de riesgos diferente.

- Los dispositivos que se consideren con capacidades de seguridad insuficientes no pueden ser simplemente prohibidos para su venta en un país determinado de forma ad hoc sin tener en cuenta las implicaciones para el comercio internacional y otras normativas locales.

Contenido

01 / Resumen ejecutivo

Desde la publicación el año pasado de la *Guía Internacional Anti-Botnet 2018* por parte del CSDE, la industria ha seguido intensificando sus esfuerzos para hacer frente a los ataques distribuidos. Sin embargo, los actores maliciosos también han intensificado sus esfuerzos. La versión de este año de la Guía ha sido refrescada y actualizada en su totalidad, pero hay dos adiciones significativas en la Guía 2020 que merecen un énfasis especial. En primer lugar, la sección 3 contiene un nuevo y significativo análisis del "año en curso" sobre la evolución de la amenaza de las redes de bots en el último año. Algunos de los puntos clave de nuestro análisis son:

Las redes de bots adoptan cada vez más estrategias que las hacen más eficaces a la hora de causar daños y evitar su detección.

Las redes de bots se dirigen con mayor frecuencia al IoT empresarial y a otros dispositivos del IoT con procesadores y arquitecturas más complejos.

Las redes de bots de criptomonedas están en auge, y los operadores de estas redes de bots suelen competir ferozmente entre sí.

Las redes de bots se utilizan cada vez más para el fraude comercial y minorista.

Los bots de las redes sociales falsifican las pruebas sociales y difunden contenidos con derechos de autor o de distribución ilegal.

Estamos empezando a ver ataques DDoS IPv6, con al menos un ejemplo probado.

En segundo lugar, las partes de la Sección 5 que abordan los dispositivos y los sistemas de dispositivos, así como la instalación de sistemas domésticos y de pequeñas empresas, se han beneficiado del desarrollo por parte del CSDE del principal consenso mundial de la industria sobre la seguridad del IoT. Aprovechando las aportaciones técnicas de cientos de expertos en seguridad de miles de empresas diferentes, el CSDE convocó a 20 importantes organizaciones tecnológicas y de ciberseguridad, asociaciones industriales, consorcios y organismos de normalización para identificar los requisitos de seguridad básicos para el mercado de la IO, que está creciendo rápidamente. Este esfuerzo, conocido como "Convene the Conveners" o "C2", pretendía abordar cuatro retos:

1. Promover la armonización mundial para evitar la fragmentación de las especificaciones y requisitos de seguridad.
2. Trabajar con las nuevas fuerzas del mercado mundial que favorecen naturalmente los dispositivos y sistemas seguros.
3. Desarrollar un lenguaje común coherente sobre estas cuestiones que resulte convincente para los distintos públicos políticos y técnicos.
4. Ayudar a la elaboración de políticas a nivel internacional y en Estados Unidos, incluso a nivel estatal.

El resultado de este esfuerzo histórico, el *C2 Consensus on IoT Device Baseline Capabilities*, o "C2 Consensus

Baseline", se publicó el 17 de septiembre de 2019. El C2 Consensus Baseline es un conjunto común de capacidades de seguridad de dispositivos que se puede aplicar a todos los nuevos dispositivos de IoT que se conectan a Internet, capacidades de mejores prácticas que son ampliamente aplicables, vertical y horizontalmente, en todos los mercados. Se aplica a la diversa gama de nuevos dispositivos IoT, dando cabida al amplio espectro de complejidad de los dispositivos, independientemente del entorno de despliegue.
La línea de base pretende ser flexible y no prescriptiva. Dependiendo de una serie de factores - incluyendo el dispositivo complejidad, capacidad de gestión del dispositivo, perfil de riesgo, caso de uso y contexto: las capacidades de seguridad descritas en la línea de base pueden lograrse de diversas maneras, siendo la clave que la capacidad de línea de base definitiva se logre de manera aplicable al dispositivo específico.

El amplio proceso de múltiples partes interesadas del NIST sobre la seguridad básica de los dispositivos IoT también ha servido de base para la Guía de este año. El borrador de NISTIR 82591 y el esfuerzo de C2 están de acuerdo en las capacidades básicas de los dispositivos, con recomendaciones adicionales para las capacidades de la organización, la información del cliente y las actividades del ciclo de vida en ambos lados.

Por último, debemos destacar que las empresas miembros del CSDE también desarrollaron un plan para la coordinación de la industria en caso de un ataque masivo de botnet, informado por el incidente de botnet basado en el IoT Mirai de 2016 que derribó partes significativas de Internet en los Estados Unidos y Europa. Este plan está incluido en nuestro informe *Cyber Crisis: Fundamentos de la coordinación de múltiples partes interesadas* o "Fundamentos de la cibercrisis". El informe considera estrategias para un total de 12 eventos significativos de ciberseguridad.

Activar la responsabilidad compartida para asegurar la economía digital global. La economía digital ha sido un motor de crecimiento comercial y de mejora de la calidad de vida en todo el mundo. Pero ninguna parte interesada, ni en el sector público ni en el privado, controla este sistema. Por el contrario, la gestión segura de las oportunidades que ofrece este crecimiento es un reto y una responsabilidad de todas las partes interesadas en la comunidad de las tecnologías de la información y la comunicación (TIC).

Sin embargo, en los últimos años, las redes de bots se han convertido en algo especialmente dañino y costoso para la economía digital. Las redes de bots son grandes redes de ordenadores y dispositivos conectados a Internet y comprometidos que los actores maliciosos pueden comandar para cometer ataques de denegación de servicio distribuidos (DDoS), propagación de ransomware, ataques de phishing y campañas de desinformación que amplifican los medios sociales no auténticos, así como otros actos maliciosos. [2] Desgraciadamente, a medida que aumenta el número de personas y empresas conectadas, y dispositivos crece, también lo hace el potencial de estos ataques maliciosos. En la actualidad, el potencial destructivo de las redes de bots ha aumentado exponencialmente a medida que atacan y aprovechan los miles de millones de dispositivos del Internet de las Cosas (IoT), que se calcula que alcanzarán los 20.000 millones de dispositivos conectados en 2020. Con esta sustancial y creciente superficie de ataque, no es casualidad que el coste global de los ciberataques sea tan elevado. Se espera que los delitos alcancen los billones de dólares. Las redes de bots son el motor a escala industrial de estas pérdidas, y son una amenaza persistente que tratará de evolucionar y adaptarse en los próximos años.

IBM Security Intelligence informa que la actividad de las variantes de Mirai casi se duplicó entre 2018 y 2019.

Esta Guía pretende invertir estas tendencias. Aunque los creadores de esta Guía apoyan firmemente el importante papel que desempeñan los gobiernos en la convocatoria de un ecosistema diverso, la imposición de

requisitos normativos prescriptivos y centrados en el cumplimiento de las normas inhibirá la innovación en materia de seguridad que es clave para adelantarse a las sofisticadas amenazas actuales. Además, los esfuerzos políticos anteriores se basaban en soluciones utópicas a estas amenazas, basadas en la idea de que los proveedores de servicios de Internet (ISP) pueden simplemente cerrar todas las redes de bots, o que los fabricantes pueden hacer que todos los dispositivos sean universalmente seguros. En cambio, las soluciones dinámicas y flexibles que se basan en normas de consenso voluntario, impulsadas por las demandas del mercado y aplicadas por las partes interesadas en toda la economía digital mundial, son la mejor respuesta a estos desafíos sistémicos en evolución.

Para hacer posible estas soluciones y fomentar el reparto de responsabilidades entre todas las partes interesadas, esta Guía establece un conjunto de *prácticas básicas* que las distintas partes interesadas deberían aplicar; además, destaca otras *capacidades avanzadas* que están disponibles en la actualidad pero que están infrautilizadas. La aplicación generalizada de las prácticas de seguridad que figuran en esta Guía reducirá drásticamente las redes de bots y ayudará a proteger la economía digital mundial. La Guía ofrece soluciones reales y disponibles en la actualidad para un reto global que no puede ser resuelto por un solo grupo de interesados o un solo país, ni por ningún mandato gubernamental. La Guía se basa en una colaboración continua con empresas de múltiples sectores y países para reducir drásticamente la amenaza de las redes de bots, y en un análisis de las amenazas y vulnerabilidades mundiales en rápida evolución, así como de los adversarios cada vez más capaces y decididos.

La Guía se basa en los siguientes principios básicos de seguridad y trata de promoverlos:

La seguridad exige soluciones dinámicas y flexibles impulsadas por las poderosas fuerzas del mercado mundial y tan ágiles y adaptables como las ciberamenazas que hay que mitigar, en lugar de mecanismos de cumplimiento normativo que difieren según la jurisdicción local o nacional.

La seguridad es una responsabilidad compartida entre todas las partes interesadas en el ecosistema de Internet y las comunicaciones.

- Los gobiernos y las partes interesadas de la industria deben promover soluciones que aumenten las responsabilidades entre todos los actores, en lugar de buscar soluciones fáciles entre ciertos componentes o partes interesadas seleccionadas.

La seguridad se basa en el trabajo en equipo y en la asociación mutuamente beneficiosa entre gobiernos, proveedores, investigadores, empresas y consumidores, mediante la acción colectiva contra los malos actores y la recompensa de las contribuciones de los actores responsables.

Estos principios son la base del nuevo enfoque de la mitigación de las redes de bots que exigen las circunstancias.

Guía internacional de seguridad de botnets e IoT: Resumen de prácticas y capacidades. La complejidad y la diversidad del "sistema de sistemas" que componen Internet y el ecosistema de comunicaciones asociado hacen imposible proporcionar un conjunto de orientaciones que se apliquen de manera uniforme a todas las partes interesadas. La Guía agrupa estos diversos componentes basándose en cinco tipos de partes interesadas proveedoras, suministradoras y usuarias: (1) Infraestructura, (2) Desarrollo de software, (3) Dispositivos IoT, (4) Instalación de sistemas domésticos y de pequeñas empresas, y (5) Empresas. Para cada uno de estos componentes, la Guía expone las prácticas de referencia que todas las partes interesadas deben aspirar a cumplir, así como las capacidades avanzadas que actualmente están disponibles -aunque infrautilizadas- en el mercado. Estas prácticas y capacidades, resumidas brevemente a continuación, constituyen el núcleo de esta Guía.

1. *Infraestructura.* A efectos de esta Guía, la "infraestructura" se refiere a todos los sistemas que permiten la conectividad y la operatividad, no sólo a las instalaciones físicas de los proveedores de servicios de Internet, la red troncal, la nube, el alojamiento web, la entrega de contenidos, el sistema de nombres de dominio y otros servicios, sino también a las redes definidas por software y otros sistemas que reflejan la evolución de

Internet desde las cosas tangibles a un concepto digital. Recomendamos prácticas de referencia y capacidades avanzadas para que la infraestructura incluya:

- Detectar el tráfico malicioso y las vulnerabilidades
- Mitigar las amenazas distribuidas
- Coordinarse con los clientes y los compañeros
- Abordar la incautación y retirada de dominios

2. *Desarrollo de software.* [3] El software es un elemento cada vez más omnipresente de todos los demás componentes del ecosistema. Hay una gran variedad de procesos de desarrollo complejos e interdependencias que impulsan la innovación y la mejora del software. Recomendamos que el software consista generalmente en prácticas de base y capacidades avanzadas que incluyan:
   - Prácticas de desarrollo seguro por diseño
   - Gestión de la vulnerabilidad de la seguridad
   - Transparencia de los procesos de desarrollo seguros

3. *Dispositivos IoT.* Un dispositivo individual conectado (o "dispositivo de punto final") puede estar formado por múltiples componentes, como módulos de hardware, chips, software, sensores u otros componentes operativos. Más allá del propio dispositivo individual hay múltiples capas adicionales de conectividad que constituyen un nuevo mercado muy dinámico, incluso para la innovación en seguridad. Para las "cosas" de los puntos finales en el IoT, recomendamos prácticas de referencia y capacidades avanzadas para incluir:
   - Desarrollo seguro
   - Capacidades seguras
   - Gestión del ciclo de vida del producto

4. *Instalación de sistemas para el hogar y la pequeña empresa.* [4] Los hogares y las pequeñas empresas se benefician de los dispositivos conectados en varias categorías. Estos sistemas pueden ser instalados por los propietarios de viviendas y negocios, o por profesionales: integradores, contratistas de alarmas y otros. Basándonos en gran medida en The Connected Home Security System[5] , recomendamos las prácticas básicas y las capacidades avanzadas que deben incluirse:
   - Autenticación y gestión de credenciales
   - Configuración de la red
   - Gestión del hardware de la red
   - Mantenimiento de la seguridad

5. *Empresas.* [6] Como principales propietarios y usuarios de dispositivos y sistemas en red, incluyendo un número exponencialmente creciente de sistemas de dispositivos IoT, las empresas de todo tipo - gobierno, sector privado, académico, sin fines de lucro - tienen un papel crítico que desempeñar en la seguridad del ecosistema digital. Para las empresas, recomendamos prácticas básicas y capacidades avanzadas que incluyan:
   - Actualizaciones seguras
   - Intercambio de información en tiempo real
   - Arquitecturas de red que gestionan con seguridad los flujos de tráfico
   - Mayor resistencia a los ataques DDoS
   - Gestión de identidades y accesos
   - Cómo mitigar los problemas con los productos obsoletos y pirateados

De cara al futuro. Al igual que la publicación de la Guía de 2018 fue solo un primer paso, esta Guía forma parte de la estrategia en curso del CSDE para involucrar a un amplio conjunto de partes interesadas, incluidos los gobiernos de países afines, con el fin de promover las prácticas de referencia y las capacidades avanzadas, y seguiremos mirando hacia adelante para lo que requiere la evolución de la amenaza. Como se indica en la Guía de 2018, actualizaremos, publicaremos y promoveremos una nueva versión de la Guía anualmente. A partir de este año, el título de nuestra Guía refleja el año que se avecina, de ahí que esta sea la edición de 2020.

Aunque el sello distintivo de los esfuerzos de este año para combatir las redes de bots es la seguridad de los dispositivos IoT, basada en la urgente necesidad de una línea de base ampliamente aceptada, no todas las redes de bots significativas tienen como objetivo los dispositivos conectados; de hecho, algunas de las redes de bots más destructivas del mundo no tienen como objetivo dispositivos conectados en absoluto. Así pues, aunque está claro que el futuro de las redes de bots está estrechamente entrelazado con el futuro de la seguridad del IoT, y el CSDE seguirá liderando este frente, también exploraremos otras formas que las botnets y otras amenazas distribuidas pueden reducirse drásticamente gracias al liderazgo de nuestros miembros. Al reconocer la naturaleza compleja y estratificada de la amenaza de las botnets, las empresas del CSDE se enfrentarán a estas amenazas en múltiples frentes.

> **The digital economy has been an engine for commercial growth and quality-of-life improvements across the world and may already represent 20% of global economic value.**

02 / Introducción

Los miembros del Consejo para la Seguridad de la Economía Digital (CSDE) abarcan la totalidad del complejo ecosistema mundial de Internet y las comunicaciones. Estas organizaciones cuentan entre sus miembros con empresas que proporcionan los sistemas humanos y técnicos que crean, gestionan e instalan las capacidades de conectividad, el software y los dispositivos que benefician a una parte importante de los consumidores, las pequeñas empresas, las grandes empresas privadas, los gobiernos y las organizaciones sin ánimo de lucro del mundo: en conjunto, la economía digital global.

Desde la elaboración de la *Guía Internacional Anti-Botnet 2018*, los miembros del CSDE -Akamai, AT&T, CenturyLink, Cisco, Ericsson, IBM,Intel, NTT,Oracle, Samsung, SAP,Telefónica y Verizon-, con el apoyo de USTelecom y la Asociación de Tecnología de Consumo (CTA), hanimpulsado la adopción de la mejora de la seguridad en el mercado global a través de la infraestructura, el software, los dispositivos y otros segmentos de la economía digital, con el fin de unir a la industria a nivel mundial en la batalla contra los botnets maliciosos.

El mundo ha tomado nota. En 2019, el Foro de Gobernanza de Internet de la ONU reconoció al CSDE por tomar medidas significativas para combatir las botnets y otras amenazas automatizadas y distribuidas a través de un enfoque colaborativo de todo el ecosistema, donde la seguridad es una prioridad compartida. También hemos sido reconocidos en la hoja de ruta sobre botnets del Gobierno de Estados Unidos como contribuyentes clave en la lucha. Nuestro proyecto global está teniendo un impacto en muchas partes del mundo, incluyendo Europa, Asia y América Latina, donde los miembros del CSDE hacen negocios.

Visión general del reto. La economía digital ha sido un motor de crecimiento comercial y de mejora de la calidad de vida en todo el mundo, creando puestos de trabajo y oportunidades en todos los continentes. Según algunas estimaciones, puede representar ya el 20% del valor económico mundial. [7] Aunque el PIB por sí solo no puede captar toda la contribución de la economía digital al valor económico mundial -no todo el valor proporcionado digitalmente implica una transacción comercial-, *The Wall Street Journal* informa de que la economía digital tenía un valor de 11,5 billones de dólares en 2016 y podría aumentar hasta los 23 billones de dólares, casi una cuarta parte del PIB mundial, en 2025.[8] El crecimiento de la economía digital se ve continuamente impulsado por la adopción de tecnologías nuevas y emergentes por parte de las empresas y los consumidores. [9] Gestionar con seguridad las oportunidades que se presentan
por este impresionante crecimiento es el reto y la responsabilidad de todas las partes interesadas en la comunidad de las tecnologías de la información y la comunicación (TIC).

Sin embargo, en los últimos años, las redes de bots se han convertido en algo especialmente dañino y costoso para la economía digital. Son capaces de propagar malware[10] , realizar ataques de denegación de servicio[11] y difundir desinformación corrosiva de forma artificial en las redes sociales. [12] Una sola red de bots puede incluir ahora más de 30 millones de puntos finales "zombis" y permitir a los actores maliciosos obtener ganancias de seis cifras al mes. [13] Hoy en día hay más sistemas vulnerables que nunca, debido al tremendo y, por otra parte, prometedor crecimiento de la propia economía digital, especialmente en lo que respecta al rápido despliegue de miles de millones de dispositivos de la Internet de las Cosas (IoT), que se calcula que alcanzarán los 20.000 millones de

dispositivos conectados en 2020.[14] Los beneficios de esta economía conectada están revolucionando para bien las actividades de las empresas y los consumidores, y las empresas que han desarrollado esta Guía están innovando nuevas medidas de seguridad a medida que despliegan los dispositivos. Sin embargo, siguen llegando al mercado dispositivos inseguros sin sistemas diseñados para protegerlos. [15] Además, ahora es posible que actores maliciosos relativamente inexpertos alquilen una potente red de bots para realizar actividades nefastas a gran escala. [16]

Estos acontecimientos infligen costes directos y tangibles a la economía digital. Por ejemplo, desde 2017, el malware se ha extendido por Europa, Asia y América, causando más de 10.000 millones de dólares en daños. [17] Se estima que en los próximos cinco años los ciberdelitos costarán globalmente a las empresas un total acumulado de 8 billones de dólares (en multas, pérdida de negocio, costes de reparación, etc.). [18]

Los costes intangibles son igualmente perjudiciales, ya que estas amenazas socavan la confianza fundamental en la economía digital.

Postura y objetivos estratégicos. Nuestro objetivo es invertir estas tendencias. Aunque reconocemos y apoyamos el importante papel de convocatoria que pueden desempeñar los gobiernos para ayudar a canalizar las actividades de los diversos actores del ecosistema, también creemos que los requisitos normativos basados en el cumplimiento inhiben en realidad la innovación en materia de seguridad que se requiere para adelantarse a las sofisticadas amenazas actuales. En otras palabras, los requisitos normativos prescriptivos no sólo no son eficaces, sino que suelen ser contraproducentes para el objetivo de la seguridad. [19] Las soluciones dinámicas y flexibles que se basan en normas de consenso voluntario, impulsadas por las demandas del mercado, y aplicadas por las partes interesadas en toda la economía digital global son la mejor respuesta a los desafíos sistémicos en evolución, como las redes de bots maliciosas que amenazan a todos los actores de este complejo ecosistema.

Por lo tanto, esta Guía pretende capacitar a los participantes responsables de la economía digital para asegurar su futuro y aprovechar todo su potencial. Creemos que la colaboración activa y la acción colectiva serán comercialmente beneficiosas para todas las partes interesadas, grandes y pequeñas, a largo plazo. Para ello, esta Guía puede utilizarse para aumentar la resistencia del ecosistema de Internet y las comunicaciones y mejorar la integridad de las transacciones de la infraestructura digital subyacente. La Guía insta a todas las partes interesadas en este mercado digital global a que apliquen un conjunto de herramientas, prácticas y procesos de referencia; además, destaca otras capacidades avanzadas que están disponibles en la actualidad, pero que tal vez todavía se infrautilizan. La aplicación generalizada de las prácticas de seguridad que figuran en esta Guía reducirá drásticamente las redes de bots y contribuirá a proteger la economía digital mundial.

La publicación de la Guía de 2018 fue solo un primer paso. En la actualidad, estamos involucrando a un amplio conjunto de partes interesadas, incluidos los gobiernos de países afines, para promover las prácticas de referencia y las capacidades avanzadas de la Guía. Además, seguiremos actualizando, publicando y promoviendo una nueva versión de la Guía cada año.

Nuevo material en la Guía 2020. La versión de este año de la Guía ha sido renovada y actualizada en su totalidad, pero hay dos adiciones significativas en la Guía 2020 que merecen un énfasis especial. En primer lugar, la sección 3 contiene un nuevo y significativo análisis del "año en curso" sobre la evolución de la amenaza de las redes de bots en el último año. Algunos de los puntos clave de nuestro análisis son:

- Las redes de bots adoptan cada vez más estrategias que las hacen más eficaces a la hora de causar daños y evitar su detección.
- Las redes de bots se dirigen con mayor frecuencia al IoT empresarial y a otros dispositivos del IoT con procesadores y arquitecturas más complejos.

- Las redes de bots de criptomonedas están en auge, y los operadores de estas redes de bots suelen competir ferozmente entre sí.

Las redes de bots se utilizan cada vez más para el fraude comercial y minorista.

Los bots de las redes sociales falsifican las pruebas sociales y difunden contenidos con derechos de autor o de distribución ilegal.

Estamos empezando a ver ataques DDoS IPv6, con al menos un ejemplo probado.

En segundo lugar, las partes de la sección 5 que abordan los dispositivos y los sistemas de dispositivos, así como la instalación de sistemas domésticos y de pequeñas empresas, se han beneficiado del desarrollo por parte del CSDE del principal consenso mundial de la industria sobre la seguridad del IoT. Aprovechando las aportaciones técnicas de cientos de expertos en seguridad de miles de empresas diferentes, el CSDE convocó a 20 importantes organizaciones tecnológicas y de ciberseguridad, asociaciones industriales, consorcios y organismos de normalización para identificar los requisitos de seguridad básicos para el mercado de la IO, que está creciendo rápidamente. Este esfuerzo, conocido como "Convene the Conveners" o "C2", pretendía abordar cuatro retos:

1. Promover la armonización mundial para evitar la fragmentación de las especificaciones y requisitos de seguridad.
2. Trabajar con las nuevas fuerzas del mercado mundial que favorecen naturalmente los dispositivos y sistemas seguros.
3. Desarrollar un lenguaje común coherente sobre estas cuestiones que resulte convincente para los distintos públicos políticos y técnicos.
4. Ayudar a la elaboración de políticas a nivel internacional y en Estados Unidos, incluso a nivel estatal.

El resultado de este esfuerzo histórico, el *C2 Consensus on IoT Device Baseline Capabilities* o "C2 Consensus Baseline", se publicó el 17 de septiembre de 2019. El C2 Consensus Baseline es un conjunto común de capacidades de seguridad de dispositivos que se puede aplicar a todos los nuevos dispositivos de IoT que se conectan a Internet, capacidades de mejores prácticas que son ampliamente aplicables, vertical y horizontalmente, en todos los mercados. Se aplica a la diversa gama de nuevos dispositivos IoT, dando cabida al amplio espectro de
complejidad de los dispositivos, independientemente del entorno de despliegue. La línea de base pretende ser flexible y no prescriptiva. Dependiendo de una serie de factores - desde la complejidad del dispositivo, la capacidad de gestión del dispositivo, el perfil de riesgo, el caso de uso
y el contexto - las capacidades de seguridad
La clave es que la capacidad final de la línea de base se logre de una manera aplicable al dispositivo específico.

Based on a study of 180 countries and territories, Verizon reported that 84% of botnets involved in data breaches targeted the finance and insurance industries.

El amplio proceso de múltiples partes interesadas del NIST sobre la seguridad básica de los dispositivos IoT también ha servido de base para la Guía de este año. El borrador del NISTIR 825920 y el esfuerzo del C2 están de acuerdo en las capacidades básicas de los dispositivos, con recomendaciones adicionales para las capacidades de la organización, la información del cliente y las actividades del ciclo de vida de ambas partes.

Por último, debemos destacar que las empresas miembros del CSDE también desarrollaron un plan para la coordinación de la industria en caso de un ataque masivo de botnet, informado por el incidente de botnet

basado en el IoT Mirai de 2016 que derribó partes significativas de Internet en los Estados Unidos y Europa. Este plan está incluido en nuestro informe *Cyber Crisis: Fundamentos de la coordinación de múltiples partes interesadas* o "Fundamentos de la cibercrisis". El informe considera estrategias para un total de 12 eventos significativos de ciberseguridad.

3 / La evolución de las redes de bots: Resumen del año

Tal y como ocurrió en el momento de la publicación de la *Guía Internacional Anti-Botnet 2018*, la categoría más destacada de amenazas automatizadas y distribuidas para el ecosistema global de Internet y las comunicaciones son las botnets, grandes redes de ordenadores y dispositivos conectados a Internet comprometidos que se comunican con servidores que tienen capacidad de mando y control.

Las redes de bots se propagan por todo el mundo a través de programas maliciosos que exploran Internet en busca de redes inseguras, ordenadores y otros dispositivos conectados. Cuando una red de bots ha comprometido un número suficiente de dispositivos, los delincuentes y otros malos actores pueden comandarlos para cometer una amplia variedad de actos nefastos, como ataques de denegación de servicio distribuidos (DDoS), propagación de ransomware, ataques de phishing y operaciones de desinformación que amplifican artificialmente las publicaciones no auténticas en las redes sociales. [21]

Redes de bots: Un problema global persistente. Mientras las empresas del CSDE trabajan continuamente con la comunidad mundial para ejercer una presión cada vez mayor sobre los operadores de botnets, estos actores maliciosos no están de brazos cruzados. No quieren ver sus operaciones desmanteladas, y ven que las acciones de nuestras empresas son una amenaza directa para los beneficios y otros objetivos críticos. A lo largo de 2019, hemos observado una serie de tendencias que nos llevan a concluir que, aunque se está avanzando en la lucha contra las redes de bots, los desafíos están aumentando.

Nuestros adversarios están atentos a cada movimiento que hacemos y evolucionan inteligentemente sus estrategias en respuesta. Los operadores de botnets inventan constantemente nuevas herramientas, adoptan nuevas técnicas y estudian cómo combatimos sus bots perturbadores, para contraatacar nuestros esfuerzos. Nos enfrentamos a enemigos muy motivados y cada vez más sofisticados, entre los que se encuentran estados nacionales y organizaciones criminales a gran escala, que están muy bien financiados. Estas organizaciones se han protegido eficazmente de la atribución, al tiempo que se mantienen en pie para obtener enormes ganancias financieras mal habidas a través de métodos criminales.

En esta sección, repasaremos cómo ha evolucionado la amenaza de las redes de bots en el último año. Algunos de los puntos clave de nuestro análisis son:

- Las redes de bots adoptan cada vez más estrategias que las hacen más eficaces a la hora de causar daños y evitar su detección.
- Las redes de bots se dirigen con mayor frecuencia al IoT empresarial y a otros dispositivos del IoT con procesadores y arquitecturas más complejos.
- Las redes de bots de criptomonedas están en auge, y los operadores de estas redes de bots suelen competir ferozmente entre sí.
- Las redes de bots se utilizan cada vez más para el fraude comercial y minorista.

Mirai no muere: más de 60 variantes, la actividad casi se duplica. Desde que el código fuente de la botnet Mirai se filtró en línea hace tres años, los actores maliciosos han experimentado continuamente y han creado sus propias versiones actualizadas. En julio de 2019, la red de bots Mirai tiene al menos 63 variantes confirmadas22 y es muy posible que queden otras sin descubrir.

IBM Security Intelligence informa de que la actividad de las variantes de Mirai *casi se duplicó* entre 2018 y 2019.[23] En una entrevista sobre nuevos exploits de IoT, publicada en marzo de 2019, un investigador de AT&T Cybersecurity declaró: "Siempre que observamos un nuevo malware de IoT - escasi inevitablementeuna nueva variantede Mirai. Todos los días vemos nuevas variantes de Mirai con diferentes cargas útiles... "[24] La actividad relacionada con Mirai había disminuido después de un ciberataque histórico en 2016 que dejó fuera de servicio partes importantes de Internet en Estados Unidos y Europa, pero este resurgimiento indica que el malware sigue siendo una amenaza grave.

Las diferentes variantes de Mirai están controladas por operadores que compiten entre sí por el dominio de los dispositivos IoT vulnerables. Como es de esperar, dada la carrera armamentística tecnológica que los operadores de botnets libran en múltiples frentes -contra las fuerzas de seguridad y entre sí-, las botnets más recientes suelen tener más recursos que Mirai. [25] Echobot, por ejemplo, es una variante de Mirai descubierta en 2019 que utiliza al menos veintiséis exploits para infectar dispositivos. [26]

En algunos casos, los creadores de botnets combinan el código de Mirai con el de otras fuentes para conseguir sus fines. Por ejemplo, Gafgyt, que según los datos de IBM X-Force representa el 27% de todo el malware dirigido a dispositivos IoT,[27] generalmente se considera y estudia como algo separado de Mirai, a pesar de compartir parte de su código fuente filtrado.

El Informe de Amenazas 2019 de CenturyLink28 contiene un cotejo de Gafgyt, Mirai y otro malware de redes de bots de IoT basado en los datos de Black Lotus Labs de CenturyLink. [29] Los datos revelan que el tiempo medio de actividad tanto de Gafgyt como de Mirai está disminuyendo. Las explicaciones incluyen que más investigadores y equipos de amenazas están siguiendo el movimiento del malware; los investigadores de amenazas están mejorando en la identificación de variantes de malware IoT que están diseñadas para evadir la detección; y los proveedores están mejorando en el seguimiento proactivo de las amenazas en sus redes. [30]

Las empresas y los dispositivos de alta complejidad corren un mayor riesgo. Aunque las empresas siempre han sido una parte importante del enfoque de todo el ecosistema para reducir las redes de bots, cada vez son más las que pueden sufrir daños y pérdidas. Estamos asistiendo a una rápida expansión del panorama de las amenazas de las redes de bots, y datos recientes de IBM X-Force revelan que los sistemas de las empresas están siendo infectados con mayor frecuencia por variantes de Mirai. [31] Los datos de Telefónica sugieren que las empresas tienen más probabilidades de ser infectadas por una red de bots durante los dos primeros meses tras el despliegue de un nuevo servicio. [32]

Las violaciones de datos son facilitadas por botnets con tanta frecuencia que el *Informe de Investigación de Violaciones de Datos 2019* de Verizon analizó los ataques de botnets por separado "para evitar eclipsar" otros tipos de incidentes. Cualquier industria puede ser objetivo. Sin embargo, algunas industrias están claramente en

mayor riesgo de ataques de botnets. Basándose en un estudio de 180 países y territorios, Verizon informó de que el 84% de las redes de bots implicadas en violaciones de datos tenían como objetivo los sectores de las finanzas y los seguros; el 10%, los sectores de la información; y el 5%, los sectores de los servicios profesionales, científicos y técnicos. El estudio no diferenciaba entre botnets de IoT y otros botnets.

En el pasado, las redes de bots basadas en el IoT infectaban sobre todo los dispositivos y sistemas conectados que se encontraban en el hogar, como cámaras, grabadoras de vídeo, dispositivos de iluminación y termostatos. Pero es lógico que, desde la perspectiva de los delincuentes, cualquier nueva categoría de dispositivo IoT -ya sea en el hogar, en la empresa o en cualquier otro lugar del ecosistema- sea un nuevo batallón en su ejército de botnets. Muchas partes interesadas con dispositivos conectados, no sólo las empresas, están en mayor riesgo.

Por ejemplo, a lo largo de 2019, Black Lotus Labs de CenturyLink ha elaborado un perfil de TheMoon, una botnet de IoT que se dirige a las vulnerabilidades de los routers en las redes de banda ancha. [34] Aunque esta amenaza en particular ha sido mitigada, muestra cómo la seguridad de IoT tiene implicaciones para la infraestructura y el ecosistema en su conjunto.

En febrero de 2019, los investigadores de seguridad descubrieron muestras de Mirai que afectaban a una colección de procesadores y arquitecturas que antes no podían ser objetivo. [35] Ahora podemos esperar infecciones de más tipos de routers, sensores en red, radios y microprocesadores para señales digitales. [36] Avances como estos abren la puerta a redes de bots más grandes.

Los expertos creen que los futuros vectores de ataque pueden incluir cada vez más los sistemas industriales de IoT y los wearables conectados[37] , por lo que será esencial que la industria y el gobierno se coordinen para identificar las capacidades de seguridad que reconocen las consideraciones únicas asociadas a los diferentes niveles de complejidad.

Botnets inteligentes y automatizados: Swarmbots y Hivenets. Imagínese miles de abejas pululando por un solo objetivo. Eso, en esencia, es un swarmbot. Los swarmbots a menudo pueden superar las defensas tradicionales sólo por su volumen. [38] Para empeorar las cosas, estos bots están dirigidos por una inteligencia artificial conocida como hivenet.

Las hivenets son "botnets que piensan por sí mismas" y tienen la capacidad de aprender durante un ataque. [39] La capacidad de aprender en tiempo real es gran parte de lo que las hace peligrosas. Mientras que las redes de bots tradicionales tenían que esperar las órdenes de sus operadores,[40] la hivenet coordina las estrategias automáticamente basándose en lo que aprenden los swarmbots.

Los Swarmbots comparten información sobre las vulnerabilidades descubiertas y otra información estratégica para aumentar la inteligencia colectiva de la colmena. Los bots también se coordinan y comparten recursos automáticamente. Los bots individuales pueden estar equipados con diferentes herramientas; cuando la hivenet descubre una vulnerabilidad, se moviliza el swarmbot con la herramienta adecuada para el trabajo. [41]

Al desplegar la tecnología basada en enjambres, los operadores de botnets pueden aumentar significativamente la eficiencia de un ataque al reducir el tiempo necesario para infiltrarse en un dispositivo o sistema de dispositivos. Una de las principales razones por las que los delincuentes necesitan una mayor eficiencia es para superar las herramientas de seguridad de la red que se están desplegando con una frecuencia cada vez mayor en todo el mercado mundial. [42] Estamos en una carrera armamentística tecnológica a largo plazo, y la tecnología

basada en enjambres es el esfuerzo de los delincuentes por escalar porque sus antiguas herramientas resultan cada vez más ineficaces.

Emotet vuelve con más de 200.000 correos electrónicos y contraseñas robadas. Talos, de Cisco, informa de que, tras un paréntesis de varios meses, la botnet Emotet regresó con fuerza en septiembre de 2019.[43] Emotet arroja spam a gran volumen a usuarios de todo el mundo, engañándolos para que liberen cargas útiles maliciosas, que ahora incluyen
el troyano TrickBot y el ransomware Ryuk, que son conocidos por adentrarse en las redes de las víctimas, aumentando el potencial de daño. [44]

NTT está utilizando actualmente capturas de datos de flujo de red, y aprovechando el conocimiento del 40% del tráfico global de Internet, para analizar la infraestructura y los actores de la amenaza detrás de TrickBot, que a finales del año pasado fue reconocido como la principal amenaza para las empresas. [45] Dado que TrickBot suele descargarse después de la infección con Emotet, mitigar TrickBot puede ayudar a limitar el potencial destructivo de Emotet.

A menudo, los correos electrónicos enviados por Emotet parecen proceder de contactos legítimos. Los correos electrónicos pueden incluir detalles de conversaciones reales en las que participaron los destinatarios. Emotet es conocido por citar hilos de correo electrónico anteriores e incluso enviar correos electrónicos de seguimiento como lo haría un ser humano. Tácticas como éstas hacen que la red de bots sea cada vez más difícil de detectar por los filtros de spam y los seres humanos. [46]

Emotet obtiene la información necesaria para engañar a los destinatarios de los correos electrónicos entrando en las cuentas de correo electrónico y robando las listas de contactos y los correos electrónicos de los ordenadores de las víctimas. En su estudio sobre Emotet, Talos de Cisco descubrió 202.675 combinaciones únicas de nombre de usuario y contraseña. [47] El Talos de Cisco también informa de que al analizar Emotet dentro de un sandbox de malware conocido como Threat Grid durante 10 meses, la botnet maliciosa intentó enviar spam casi 19.000 veces. [48]

Aunque las publicaciones de noticias tecnológicas se han referido a Emotet como "la red de bots más destructiva del mundo "[49] y "la red de bots más peligrosa de la actualidad "[50] , no es el único spambot de gran volumen que está activo actualmente. Por ejemplo, Gamut y Necurs, spambots que hace unos años representaban el 97% del tráfico de spam en Internet, siguen causando problemas. [51]

A partir de 2019, Cisco informa que la botnet Gamut ha estado enviando spam de citas y relaciones íntimas, así como anuncios de productos farmacéuticos y oportunidades de trabajo. [52] Necurs ha pasado de ser una red de bots que entrega troyanos bancarios y ransomwarea permitir también el tráfico de proxy, la criptominería y el lanzamiento de ataques DDoS. El análisis de CenturyLink revela que Necurs se ve principalmente en los países en desarrollo. [53] Sin embargo, dado que las redes de bots ignoran los límites jurisdiccionales, estas infecciones pueden tener efectos significativos en todas las partes del mundo.

Redes de bots en alquiler: ahora disponibles tanto en la Dark Web como en las redes sociales.

En la web oscura -áreas de Internet a las que se accede mediante un software específico- existen mercados criminales en los que los ciberdelincuentes pueden alquilar redes de bots por un módico precio. Este acuerdo, denominado malware como servicio (MaaS), pone las herramientas destructivas en manos de un conjunto más amplio de actores maliciosos. [54] Algunos de los delincuentes que alquilan una red de bots carecen de los conocimientos técnicos necesarios para crear una red de bots propia. Sin embargo, otros ven el alquiler de una botnet como una decisión comercial puramente pragmática. Al igual que los negocios legítimos, las empresas criminales están interesadas en el retorno de la inversión y están dispuestas a priorizar las inversiones que produzcan los mayores beneficios. [55] A veces, los delincuentes con conocimientos técnicos avanzados alquilan redes de bots para complementar sus ejércitos ya existentes; en estos casos, se puede pensar en las redes de bots alquiladas como mercenarios.

En el informe 2019 Cyber Crisis Foundations, el CSDE documenta el caso de una empresa de telecomunicaciones de Liberia que se convirtió en objeto de una demanda tras contratar a un hacker criminal para lanzar ataques DDoS contra un rival para obtener una ventaja competitiva injusta. [56] El hacker utilizó una red de bots personalizada basada en Mirai y alquiló cámaras de seguridad y routers infectados a otros hackers. [57] En su punto álgido, los ataques *inhabilitaron el acceso de la mayoría de los usuarios de Internet en el país*, lo que aumentó la preocupación mundial por la seguridad del IoT. [58]

Para que no pienses que toda la actividad maliciosa se desarrolla en el secreto de la web oscura, los creadores de botnets anuncian cada vez más sus creaciones en las plataformas convencionales. A veces, los creadores incluso alquilan redes de bots que son

todavía en desarrollo, ya que los delincuentes ansiosos hacen cola para asegurarse un lugar. Por ejemplo, los creadores de Cayosin -una red de bots descrita como "Frankenstein" porque está hecha de diferentes piezas de malware de código abierto (incluido Mirai)- han anunciado su proyecto en YouTube e Instagram, burlando abiertamente la ley y cobrando una baja cuota de alquiler para incentivar a los delincuentes a convertirse en sus clientes. [59]

Mediante el uso de las redes sociales, los creadores de botnets pueden realizar estudios de mercado con el objetivo de aumentar sus beneficios: a veces piden abiertamente la opinión de los clientes sobre los servicios prestados, para poder mejorar el servicio y establecer una relación con sus clientes criminales. [60] Se trata de un marcado cambio en la evolución cultural de los delincuentes de botnets.

Los **bots sigilosos utilizan trucos para evitar ser detectados.** Los desarrolladores de redes de bots evolucionan constantemente sus estrategias para mantener los bots ocultos y activos durante más tiempo. Un informe reciente de Akamai explica que "los bots pueden representar hasta el 60% del tráfico web total, pero menos de la mitad de ellos se declaran realmente como bots, lo que dificulta su seguimiento y bloqueo".[61] Otro factor que complica la situación es que no todos estos bots son maliciosos, lo que dificulta la erradicación de comportamientos delictivos cuando se detecta la automatización.

Por ejemplo, para evitar ser detectados al visitar un sitio web, los bots maliciosos se hacen pasar por navegadores y aplicaciones móviles populares, o en algunos casos se hacen pasar por bots buenos. [62] Algunos bots manipulan las propiedades del navegador para falsear las "características de la huella digital", que suelen estar en la lista blanca, o manipulan las cookies, ya sea eliminándolas o incluso cosechando cookies buenas para parecer legítimos. [63]

También hemos visto el continuo aumento de los "ataques bajos y lentos", en los que los bots intentan pasar desapercibidos, robando sin descanso una gran cantidad de información a lo largo del tiempo. [64] Al utilizar este método, los bots cambian sus direcciones IP o utilizan varias direcciones IP. Esto permite a los bots eludir las limitaciones de velocidad sin que se note; las múltiples direcciones IP envían un pequeño número de peticiones por hora. [65]

Los bots también utilizan otras técnicas para eludir los límites de velocidad cuando se mantienen "bajos y lentos". Con mayor frecuencia, los operadores de botnets anonimizan el tráfico malicioso enrutándolo a través de conexiones residenciales de banda ancha e inalámbricas. [66] Las redes de bots también han estado modificando sus direcciones IP a través de proxies, ocultándose en redes anónimas, como VPN y Tor67 , incluida una variante de Mirai descubierta recientemente. [68] Cuando el enemigo puede esconderse entre la multitud, sin exponerse, el trabajo de detección y defensa contra el enemigo es considerablemente más difícil.

Las redes de bots han estado haciendo uso de otro truco: esencialmente, hacerse el muerto. La red de bots Necurs, analizada por Black Lotus Labs de CenturyLink, entra en un periodo de inactividad sostenido en varios intervalos. En un caso observado, Necurs estuvo activo durante tres semanas, se calmó durante dos semanas y luego se activó de nuevo. [69] En 2019, Necurs estuvo prácticamente inactivo durante varios meses, y solo entraba en acción una vez a la semana durante breves periodos de tiempo. [70] Necurs demostró ser resistente a varios intentos de sinkholing - trampas para redes de bots desplegadas por las fuerzas del orden o los investigadores de

seguridad- debido a su algoritmo de generación de dominios (DGA). Sin embargo, el análisis del DGA de la red de bots
revela a los investigadores qué dominios se generarán en el futuro, para que puedan inspeccionar el tráfico DNS y de red pertinente y desplegar estrategias de mitigación. [71]

Los bots defraudan a los comerciantes y anunciantes en línea y se hacen pasar por humanos.

Un reciente informe de Akamai *sobre el estado de la seguridad en* Internet72 revela que los bots maliciosos representan ahora casi la mitad del ancho de banda de Internet dirigido a los comercios online. [73] A la luz de este dato aleccionador, el informe se refiere a los bots como "herramientas de destrucción masiva (del comercio)".

Durante años, los delincuentes han utilizado redes de bots para perpetrar fraudes publicitarios enviando bots en lugar de ojos humanos reales a los destinos en línea. Esto cuesta a los anunciantes millones de dólares y proporciona a los usuarios peores experiencias de navegación en la web. [74] Los bots también se han utilizado en otras actividades con fines lucrativos, como la compra de productos populares o de entradas para eventos populares y su reventa. [75]

A principios de este año, los expertos en seguridad de Oracle descubrieron una importante operación de fraude relacionada con DrainerBot, que se propagaba a través de un kit de desarrollo de software (SDK) encontrado en cientos de aplicaciones y juegos para teléfonos móviles. Las aplicaciones infectadas, una vez instaladas en los teléfonos de los usuarios desprevenidos, utilizaban más de 10 GB de datos al mes (incluso si el teléfono estaba en modo de suspensión) y engañaban a los anunciantes haciéndoles creer que recibían tráfico humano. [76]

En 2019, es mucho más difícil saber si la actividad en línea es humana. En el pasado, si se levantaban sospechas, era relativamente fácil identificar comportamientos no humanos, como abrir y cerrar millones de ventanas. [77] Sin embargo, la actividad de los bots maliciosos se asemeja cada vez más a la navegación web real de los humanos, de tal manera que incluso los expertos tienen problemas para distinguir la diferencia.

Las redes **sociales de bots difunden desinformación y enlaces ilegales.** La capacidad del tráfico de las redes de bots para parecerse al tráfico humano ordinario tiene implicaciones que van más allá de la estafa a minoristas y anunciantes. Las redes de bots están abusando de las redes sociales de diferentes maneras, desde suplantar la identidad de millones de personas hasta facilitar el acceso a contenidos protegidos por derechos de autor o de distribución ilegal.

En la guía del año pasado, observamos que las redes de bots pueden desempeñar un papel en la difusión de desinformación corrosiva que puede privar al público de la oportunidad de tomar decisiones informadas. Los bots que imitan el comportamiento humano podrían utilizarse para influir en las opiniones humanas sobre casi cualquier tema, desde las tendencias musicales hasta la política, falsificando la prueba social. [78]

Para un ejemplo común de botnets que difunden contenido con derechos de autor, podemos mirar a los deportes. En diciembre de 2018, Telefónica publicó un informe de tendencias sobre la "detección de botnets en Twitter en eventos deportivos". [79] Los bots difunden masivamente enlaces a contenidos en streaming de forma ilegal, interfiriendo en los beneficios de los titulares de los derechos.

Reducir las redes de bots que explotan las redes sociales no será una tarea fácil. En septiembre de 2019, el informe de transparencia de Twitter reveló que la plataforma había eliminado miles de cuentas con aparentes conexiones con campañas de medios sociales respaldadas por el Estado. [80] En total, la plataforma ha purgado millones de cuentas falsas. [81] Sin embargo, las redes de bots aprenden, se adaptan y se actualizan constantemente para evadir las prohibiciones y continuar sus operaciones sin ser detectadas.

Los bots surgen para minar criptodivisas anónimas. El auge de la criptodivisa se ha convertido en combustible para la actividad de las redes de bots. En 2018, la Cyber Threat Alliance detectó un aumento del 459% en el malware de minería de criptomonedas,[82] y es posible que a finales de 2019 nos encontremos con

cifras igualmente impactantes.

Las operaciones de minería de botnets están impulsadas por los beneficios. Así, cuando la criptodivisa Monero triplicó su valor en el verano de 2019, se produjo un notable aumento de la actividad de las redes de bots. [83] En general, los delincuentes prefieren criptodivisas como Monero y ZCash que son relativamente anónimas, en lugar de bitcoin que es más fácil de rastrear para las fuerzas del orden. [84]

Aunque los sistemas infectados de las víctimas suelen seguir funcionando, el delito no carece de víctimas; la tensión añadida en la infraestructura informática puede tener graves consecuencias, incluidos los daños físicos. [85] Las víctimas pueden notar un rendimiento más lento y un mayor tiempo de retraso porque los recursos se están desviando a la tarea de beneficiar a los delincuentes.
Las operaciones comerciales pueden verse afectadas negativamente y las víctimas pueden notar un aumento en las facturas de energía. [86]

Las guerras de botnets se trasladan a la nube. La competencia entre los delincuentes por apoderarse del mayor número posible de dispositivos y sistemas da lugar con frecuencia a "guerras territoriales" de botnets. Las redes de bots infectan dispositivos ya infectados por otras redes de bots -y eliminan a sus rivales- para aumentar su propio poder y beneficios.

En 2019, vimos una escalada de la rivalidad entre Rocke y Pascha, grupos de hacking de criptominería que compiten por el dominio del entorno de computación en la nube de Linux. [87] Ambos grupos utilizan recursos mal habidos en la nube para avanzar en las operaciones de criptominería. Mientras tanto, Smominru, otra red de bots de criptominería, ha estado borrando rivales de los ordenadores con Windows 7. [88] Mientras que otros dos bots de criptominería, Fbot y Trinity, continuaron una lucha que comenzó el año pasado para controlar decenas de miles de dispositivos Android no seguros. [89]

A medida que los bots que eliminan a otros bots se hacen más comunes, y los beneficios están en juego, existe una importante presión sobre los operadores de botnets para que luchen contra sus rivales utilizando las últimas herramientas, o al menos tomen medidas para defenderse. Para
Por ejemplo, algunas redes de bots parchean activamente las vulnerabilidades de seguridad después de entrar en un dispositivo, con el fin de evitar que un rival entre en él.

La demanda de potentes redes de bots que puedan cerrar a sus rivales se ha reflejado en los mercados delictivos de la web oscura, lo que ha dado lugar a la proliferación de potentes programas maliciosos como Mylobot, que dispone de un número sin precedentes de herramientas. [90]

Mientras los hackers criminales se preocupan de que sus rivales les dejen obsoletos, también tienen que considerar la amenaza que suponen para sus operaciones los "cibervigilantes". Redes de bots como BrickerBot91 y Hajime92 fueron diseñadas para borrar las redes de bots maliciosas y mejorar ostensiblemente la seguridad de un
sistema infectado. Aunque las intenciones detrás de estos botnets no son en apariencia maliciosas, los vigilantes
Sin embargo, las redes de bots infringen las leyes de muchos países.

> **Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.**

El **futuro de la seguridad del IPv6 y el Internet de los objetos. El** IPv6 es un protocolo de Internet definido por el Grupo de Trabajo de Ingeniería de Internet (IETF)[93] y fue creado para sustituir al antiguo protocolo IPv4 con el tiempo. [94] A medida que crece el número de usuarios de Internet y de dispositivos conectados en todo el mundo, las redes ofrecen cada vez más conectividad IPv6,[95] y en muchos casos IPv6 e

IPv4 se despliegan conjuntamente.

Sin embargo, el informe *State of the Internet Security* de Akamai señala que "como el IPv6 todavía se considera una minoría del tráfico, no es un punto de venta importante para varias herramientas de seguridad. No todas las organizaciones consideran que merezca la pena vigilar el espacio IPv6, incluso cuando la capacidad está presente".[96]

Las redes de bots como Mirai obtienen nuevos bots mediante escaneos automáticos del espacio de direcciones IPv4, y los dispositivos vulnerables suelen infectarse a los pocos minutos de conectarse a Internet. [97] En cambio, el escaneo del espacio de direcciones IPv6 se ha considerado extremadamente difícil debido a su gran tamaño. [98] No obstante, los expertos llevan años advirtiendo de que las vulnerabilidades no descubiertas en el protocolo IPv6, combinadas con el crecimiento del IoT, podrían permitir ataques masivos de redes de bots. [99]

Ahora hay al menos un caso documentado de un ataque DDoS con IPv6, que utilizó una técnica conocida como amplificación de DNS en lugar de una red de bots. [100] Aunque no supuso un incidente importante, hay que preguntarse: ¿podría IPv6 dar lugar a más ataques DDoS y de mayor envergadura con el tiempo? El aumento de los ataques de redes de bots IPv6 presentaría retos únicos que no tienen una solución fácil. Por ejemplo, el increíble número de direcciones IPv6 (más de 8.000 veces más que las IPv4) podría permitir a los atacantes desbordar la memoria de los sistemas de seguridad diseñados para manejar las amenazas basadas en IPv4. [101]

Conclusión. Mientras la industria realiza avances tangibles en la lucha contra las botnets, la amenaza ha seguido evolucionando y creciendo. En un futuro próximo, la preocupación por la seguridad global de las botnets podría verse agravada por la nube
y el crecimiento del Internet de las Cosas - ambos desarrollos aumentan radicalmente la superficie de ataque que los actores maliciosos pueden atacar. Lo que necesitamos para luchar contra esta amenaza en rápida evolución es un movimiento global, basado en el mercado, hacia una mayor seguridad en todos los segmentos de la economía digital. Al mismo tiempo, necesitamos políticas que fomenten la innovación y permitan a la industria evolucionar de forma tan flexible y dinámica como los adversarios.

4 / Cómo hacer frente a las amenazas automatizadas y distribuidas en un ecosistema de Internet diverso

El reto fundamental de hacer frente a las redes de bots en el ecosistema global de Internet, altamente diverso, complejo e interdependiente, sigue siendo: la naturaleza esencial de Internet es no jerárquica e hiperconectada. Ninguna parte interesada -gobierno o sector privado- controla este sistema y, sin embargo, dependemos de él para conectarnos a todos. La lucha contra las redes de bots malintencionadas es el clásico reto de la "tragedia de los comunes": si todo el mundo participa en los bienes comunes de Internet, pero nadie los controla, ¿quién es responsable de limpiar las redes de bots malintencionadas que amenazan las funciones básicas de las que todos dependen?

La respuesta es que todas las partes interesadas deben asumir su responsabilidad, y no sólo con el propósito altruista de limpiar el patrimonio común. Cada entidad del ecosistema tiene un interés propio en reducir las redes de bots maliciosas. Las redes de bots se utilizan para atacar Internet, de la que dependen todas las ofertas de TIC, y estar involucrado en un ataque de redes de bots perjudica a las empresas implicadas, ya sea por el impacto directo en la ejecución o por el daño a la reputación.

La mitigación de las redes de bots requiere un enfoque reflexivo y holístico. Las distintas partes de este complejo ecosistema deben -por su bien individual y colectivo- profundizar y agudizar su comprensión de sus propias responsabilidades y de cómo se complementan con las de otros. Y en los casos en los que las líneas actualmente no están claras o se desconocen, las partes interesadas deben trabajar juntas para aclararlas. En ausencia de este trabajo, las estrategias para combatir las redes de bots volverán a la falacia de las soluciones utópicas centradas en sólo una o dos piezas del rompecabezas - por ejemplo, que los proveedores de servicios de Internet deberían simplemente cerrar todas las redes de bots, o que miles de millones de dispositivos deberían ser universalmente seguros, o que los consumidores deberían convertirse en usuarios omniscientes de la tecnología.

A recent Akamai State of the Security report reveals that malicious bots now account for nearly half of the internet bandwidth directed at online retailers.

Estas soluciones simplistas han fracasado hasta ahora y es poco probable que tengan más éxito en el futuro. En su lugar, este intrincado sistema compuesto por miles de millones de componentes humanos y automatizados en los mercados de consumidores y empresas del sector privado, el mundo académico, la sociedad civil y los gobiernos de todo el mundo debe aplicar métodos de mitigación en todos los niveles para aumentar su seguridad. Eso es lo que pretende esta Guía Internacional de Seguridad de Botnets e IoT.

¿Qué es diferente ahora?

Esta Guía ofrece soluciones reales y disponibles en la actualidad para un reto del mercado actual que no puede ser resuelto por ningún requisito gubernamental ni por un solo país. Estamos trabajando con empresas globales de múltiples sectores para reducir la amenaza de las redes de bots de forma drástica. Desarrollamos esta Guía, basándonos en el análisis
de las amenazas globales en rápida evolución, las vulnerabilidades de todo el ecosistema y los adversarios cada vez más capaces y decididos, teniendo en cuenta los siguientes principios rectores consensuados:

La seguridad exige soluciones dinámicas y flexibles impulsadas por las poderosas fuerzas del mercado mundial y tan ágiles y adaptables como las ciberamenazas que hay que mitigar, en lugar de mecanismos de cumplimiento normativo que difieren según la jurisdicción local o nacional.

La seguridad es una responsabilidad compartida entre todas las partes interesadas en el ecosistema de Internet y las comunicaciones. Los gobiernos y las partes interesadas de la industria deben promover soluciones que aumenten las responsabilidades entre todos los actores, en lugar de buscar soluciones fáciles entre ciertos componentes o partes interesadas seleccionadas.

La seguridad se basa en el trabajo en equipo y en la asociación mutuamente beneficiosa entre gobiernos, proveedores, investigadores, empresas y consumidores, sobre la base de un marco que adopta medidas colectivas contra los malos actores y recompensa las contribuciones de los actores responsables.

Visión general del ecosistema global de Internet y las comunicaciones. Como se ha señalado anteriormente, la economía digital se basa en un complejo ecosistema global de Internet y de las comunicaciones, que se compone de numerosos sistemas, cada uno de los cuales es muy complejo por sí mismo y muy interdependiente de todos los demás. Y todos estos diferentes componentes constituyen parte de la vulnerabilidad del ecosistema -y de su resistencia- a las amenazas planteadas por las redes de bots y otros ataques automatizados y distribuidos.

La complejidad y la diversidad del "sistema de sistemas" que componen Internet y el ecosistema de comunicaciones asociado hacen imposible ofrecer una serie de orientaciones que se apliquen de manera uniforme a todas las partes interesadas. Varios informes destacados del gobierno y del sector privado han definido y descrito el ecosistema de internet y las comunicaciones utilizando taxonomías similares pero diferentes, adaptadas a los propósitos y objetivos de cada foro. [102] En lugar de servir como visiones opuestas de cómo debe entenderse el ecosistema, estas definiciones se complementan y refuerzan mutuamente.

Esta Guía no es una excepción. Agrupamos los componentes del ecosistema de forma que se facilite la identificación y aplicación de prácticas anti-botnet entre los grupos de interés que lo componen. En concreto, la Guía se organiza en torno a los siguientes cinco tipos de proveedores, suministradores y usuarios:

1. Infraestructura
2. Desarrollo de software
3. Dispositivos IoT
4. Instalación de sistemas para el hogar y la pequeña empresa
5. Empresas

No cabe duda de que cualquier esfuerzo por definir este complejo ecosistema conlleva el riesgo de ser poco inclusivo de alguna manera, ya sea real o percibida. Por ejemplo, la experiencia puede revelar que ninguna de las cinco categorías enumeradas anteriormente puede acomodar razonablemente algunas plataformas ubicuas (por ejemplo, las grandes plataformas de medios sociales) que implican alguna combinación de categorías. Por ello, esta taxonomía debe considerarse de forma flexible, con la expectativa de que los límites entre los sistemas sigan evolucionando.

5 / Prácticas y capacidades de los componentes del ecosistema

A. INFRAESTRUCTURA

A efectos de esta Guía, "infraestructura" se refiere a todos los sistemas que permiten la conectividad y la operatividad, no sólo a las instalaciones físicas de los proveedores de servicios de Internet, la red troncal, la nube, el alojamiento web, la entrega de contenidos, el sistema de nombres de dominio y otros servicios, sino también a las redes definidas por software y otros sistemas que reflejan la evolución de Internet desde las cosas tangibles a un concepto digital. Recomendamos prácticas de referencia y capacidades avanzadas para diversas infraestructuras en el ecosistema moderno de Internet y las comunicaciones.

Tipos de infraestructuras

Proveedores de servicios de Internet

Un proveedor de servicios de Internet (ISP) es una organización que proporciona a los clientes un medio para acceder a Internet utilizando tecnologías como el cable, la DSL (línea de abonado digital), la conexión telefónica y la conexión inalámbrica. Los ISP están conectados entre sí a través de puntos de acceso a la red, instalaciones de red pública que se encuentran en la red troncal de Internet. Los ISP utilizan estos vastos sistemas de componentes troncales interconectados para transferir información a través de largas distancias en cuestión de segundos. Los ISP pueden ofrecer servicios que van más allá del acceso a Internet, como alojamiento de sitios web, registro de nombres de dominio, alojamiento virtual, paquetes de software y cuentas de correo electrónico. Muchos ISP ofrecen servicios diseñados para reducir las redes de bots, incluyendo soluciones de seguridad gestionadas por las que el proveedor asume un papel activo en la mitigación de las amenazas a los clientes. La mayoría de los ISP de banda ancha proporcionan antivirus como parte de su oferta, y muchos notifican a los clientes infectados sin ningún cargo adicional.

Proveedores de redes troncales de Internet

La red troncal de Internet es un conjunto de vastas redes informáticas conectadas que suelen estar alojadas en puntos de acceso a la red comerciales, gubernamentales, académicos y otros. Estas organizaciones suelen controlar grandes redes de alta velocidad y líneas troncales de fibra óptica, que son esencialmente un conjunto de cables de fibra óptica agrupados para aumentar su capacidad. Permiten velocidades de datos más rápidas y un mayor ancho de banda en largas distancias, y son inmunes a las interferencias electromagnéticas. Los proveedores de backbone suministran a los ISP el acceso a Internet y los conectan entre sí, lo que permite a los ISP ofrecer a los clientes un acceso a Internet de alta velocidad.

Los mayores proveedores de redes troncales se denominan proveedores de "nivel 1". Estos proveedores no se limitan a un país o región y tienen vastas redes que conectan países de todo el mundo. Algunos proveedores de red troncal de nivel 1 son también ISP y, debido a su tamaño, estas organizaciones venden sus servicios a ISP más pequeños.

Proveedores de DNS

El Sistema de Nombres de Dominio (DNS) es esencialmente una libreta de direcciones de nombres de dominio asociados a direcciones IP copiadas y almacenadas en millones de servidores de todo el mundo. Cuando un usuario desea visitar un sitio web y escribe el nombre del dominio en la barra de búsqueda, el ordenador envía esa información a un servidor DNS. Este servidor (también conocido como resolvedor) suele ser gestionado por el proveedor de servicios de Internet del usuario. El resolvedor hace coincidir el nombre de dominio con una dirección IP

y envía la dirección IP correspondiente al navegador del usuario, que a su vez abre una conexión con el servidor web.

Los proveedores de DNS son organizaciones que ofrecen estos servicios de resolución de DNS. Proporcionan las funciones de DNS más comunes, como la traducción de dominios, la búsqueda de dominios y el reenvío de DNS. Los proveedores de DNS también actualizan rutinariamente sus servidores de nombres para proporcionar la información más actualizada.

Redes de distribución de contenidos

Una red de entrega (o distribución) de contenidos (CDN) es una red geográficamente dispersa de centros de datos y servidores proxy. El término CDN se utiliza para describir muchos tipos diferentes de servicios de entrega de contenidos, como: descargas de software, aceleración de contenidos web y móviles, y transmisión de vídeo. Los vendedores de CDN también pueden cruzar a
otros sectores, como el de la ciberseguridad, con protección DDoS y cortafuegos de aplicaciones web (WAF). Las CDN se diseñaron para resolver un problema conocido como latencia, el retraso que se produce entre el momento en que un usuario solicita una página web
hasta el momento en que su contenido aparece en pantalla. La duración del retraso suele depender de la distancia entre el usuario final y el servidor de alojamiento. Para acortar esta duración, las CDN reducen esa distancia física y mejoran la velocidad y el rendimiento del sitio almacenando una versión en caché de sus contenidos en varios lugares, conocidos como puntos de presencia o PoP; cada PoP conecta a los usuarios finales que se encuentran en su proximidad con los servidores de caché responsables de la entrega de contenidos. Al almacenar el contenido de un sitio web en muchos lugares a la vez, una empresa puede ofrecer una cobertura superior a los usuarios finales que se encuentran lejos.

Proveedores de nube y alojamiento

Los servicios de alojamiento en Internet permiten a los clientes hacer accesibles los contenidos en Internet a personas y organizaciones de todo el mundo. En los últimos años, la creciente adopción de los servicios de alojamiento en la nube, que utilizan servidores remotos alojados en línea en lugar de un servidor local o un dispositivo personal, ha dado a los clientes acceso a soluciones de alojamiento escalables y más seguras. El software, la infraestructura y las plataformas alojadas en la nube son accesibles mediante suscripción y permiten a los clientes realizar una gran variedad de funciones informáticas.
Dado que las redes en la nube están descentralizadas, normalmente pueden soportar la interrupción de numerosos componentes de la red. Esta característica arquitectónica hace que la nube sea más resistente a las redes de bots altamente distribuidas y proporciona capacidades adicionales de mitigación. En esencia, los servicios en la nube proporcionan una capa adicional de seguridad fuera de la infraestructura proporcionada por un ISP. Esta capa de protección es cada vez más útil a medida que aumenta la escala de los ataques de las redes de bots. Dado que la nube se encuentra en una posición anterior a la de los ISP respecto al objetivo de un ataque, puede mitigar el problema más cerca del origen del mismo. Los servicios de seguridad en la nube complementan y no disminuyen el papel de los ISP en la mitigación de las redes de bots.

Prácticas básicas y capacidades avanzadas para la infraestructura

Los miembros del CSDE toman medidas críticas para aumentar la resistencia de sus propias redes, las de sus clientes y el ecosistema global contra las redes de bots. Los expertos del gobierno y de la industria han observado que, debido a la complejidad del ecosistema, ninguna herramienta única será siempre eficaz para mitigar las amenazas[103], lo que significa que la industria debe conservar la suficiente flexibilidad para adaptarse a las amenazas emergentes y a las nuevas tecnologías y herramientas. Sin embargo, ya se ha demostrado que ciertas prácticas básicas reducen el impacto de los ataques impulsados por redes de bots, como los DDoS ataques y deberían aplicarse en todo el ecosistema.[104] A continuación, identificamos las prácticas básicas y las capacidades más avanzadas que los líderes del sector utilizan para proteger el ecosistema contra las amenazas distribuidas.

1. DETECTAR EL TRÁFICO MALICIOSO Y LAS VULNERABILIDADES

El primer paso para mitigar las amenazas distribuidas, como las redes de bots, es identificar los activos que necesitan ser defendidos de los ataques y las posibles vulnerabilidades (es decir, las superficies de ataque) que potencialmente exponen estos activos. Además, las empresas deben mantenerse informadas sobre los últimos exploits (es decir, vectores de ataque) para cada vulnerabilidad identificada.

Los proveedores pueden aprovechar las fuentes de datos de terceros de confianza y los mecanismos de intercambio de información, tanto dentro de su industria como entre sectores. Además, los mecanismos gubernamentales de intercambio de información en muchos países permiten que la información se comparta entre el sector público y el sector privado rápidamente a velocidad de máquina. [105]

Resumen de las prácticas de detección de referencia: Los proveedores comprueban los tipos de malware conocidos en bases de datos que se actualizan regularmente. Una empresa responsable puede contribuir a los esfuerzos de detección compartiendo oportunamente la información sobre nuevos programas maliciosos con los proveedores e investigadores de seguridad.

Resumen de las capacidades avanzadas de detección: Las empresas con acceso a mayores recursos pueden contar con un equipo de investigadores de seguridad dedicados que pueden analizar la heurística y los comportamientos anómalos para detectar el malware. Los hallazgos de los investigadores pueden compartirse con otras partes interesadas.

a. Análisis de firmas

Cuando los expertos en seguridad encuentran un malware, buscan un patrón único o "firma" (por ejemplo, una parte del código del malware y el código del exploit). El análisis basado en firmas puede ser utilizado por cualquiera que tenga acceso a una base de datos actualizada de firmas de malware, de modo que la amenaza pueda ser identificada independientemente de dónde se encuentre. Este tipo de análisis es común en el software antivirus y en los sistemas de detección de intrusos, y puede utilizarse para detectar la mayoría de las amenazas maliciosas en una red. Aunque el análisis de firmas se utiliza habitualmente, los actores maliciosos más sofisticados pueden limitar la utilidad de esta técnica al cambiar las características específicas del malware cada vez que se propaga. Al igual que un virus real, el malware puede adaptarse y evolucionar a medida que se desplaza de un host a otro. [106] Una limitación más obvia del análisis de firmas es que requiere el conocimiento previo del malware, lo que significa que el
La eficacia del análisis de firmas depende de las actualizaciones oportunas y del intercambio de información en todo el ecosistema. Idealmente, el análisis de firmas debería combinarse con otros tipos de análisis, como el heurístico o el de comportamiento que se comenta más adelante, para superar las limitaciones inherentes a esta técnica. [107]

Prácticas básicas: Los proveedores deben asegurarse de que sus bases de datos de firmas están actualizadas y deben contribuir a la puesta en común de información sobre el malware.

Capacidades avanzadas: Los proveedores pueden combinar el análisis de firmas con el análisis de la heurística del código (que se describe a continuación) y los comportamientos del tráfico de red (que también se describe a continuación) para conseguir mejores resultados.

b. Análisis heurístico

El análisis heurístico detecta el malware examinando el código en busca de signos conocidos de problemas. El código no tiene que coincidir exactamente con el malware conocido para ser marcado como potencialmente malicioso. El análisis heurístico busca muchas pistas diferentes para determinar si el código es sospechoso. En el análisis heurístico estático, el código potencialmente malicioso se compara con el código del malware en una base de datos y, si hay suficientes similitudes, el código se marca.

Aunque existe la posibilidad de que se produzcan falsos positivos, el análisis heurístico es mucho más eficaz que el análisis de firmas para combatir amenazas desconocidas y en evolución. A veces, para deconstruir el código de forma segura, los científicos almacenan
código sospechoso que creen que es malware dentro de una máquina virtual llamada "caja de arena", impidiendo así que se propague a otros hosts. Esto se conoce como análisis heurístico dinámico. [108]

Capacidades avanzadas: Los proveedores pueden detectar amenazas previamente desconocidas utilizando una combinación de análisis heurístico tanto estático como dinámico. Los proveedores que cuentan con equipos de investigadores pueden analizar el código sospechoso dentro de un sandbox para determinar estrategias de mitigación eficaces, que pueden compartirse con otras partes interesadas del ecosistema.

c. Análisis del comportamiento

Mientras que el análisis de firmas y el análisis heurístico se centran en el código del malware, el análisis de comportamiento se centra en los "síntomas" de la infección del malware. Cuando el tráfico de la red indica un comportamiento inesperado, puede que no esté claro al principio cuál es la causa del cambio de comportamiento. Sin embargo, existen indicadores conocidos de que un software puede ser malicioso, por ejemplo, cuando intenta obtener privilegios elevados o interactúa de forma anómala con otro software o archivos de un sistema. A menudo, el análisis del comportamiento se compara con la profesión médica: un
A menudo, el médico puede saber cuándo alguien está enfermo incluso antes de saber exactamente cuál es el problema. El análisis de comportamiento complementa otros tipos de análisis al descubrir amenazas desconocidas que aún no han sido identificadas y, por tanto, no tienen firmas conocidas. [109]

Capacidades avanzadas: Los proveedores pueden utilizar algoritmos para detectar patrones de tráfico anómalos y aprovechar los conocimientos institucionales o, si es necesario, contratar a expertos en seguridad externos para diagnosticar las causas subyacentes del tráfico anómalo.

d. Muestreo de paquetes

Para dar sentido a las enormes cantidades de datos que fluyen por una red, muchos proveedores líderes utilizan una técnica llamada muestreo de paquetes. Esta técnica consiste en desarrollar vistas enriquecidas del flujo de tráfico a partir de muestras del tráfico de la red captadas por los routers. Al reducir la cantidad de datos que hay que inspeccionar, el muestreo de paquetes permite a los operadores de grandes redes analizar el tráfico, incluso cuando el tamaño y la velocidad de las redes modernas aumentan.

Prácticas básicas: Los proveedores deberían al menos muestrear los paquetes de forma pseudoaleatoria†, dando a los paquetes una oportunidad de ser seleccionados para su inspección. Este muestreo puede realizarse de forma neutral en cuanto al contenido.

Capacidades avanzadas: Los proveedores pueden hacer uso de técnicas de muestreo más complejas que ponderan la probabilidad y se adaptan de forma reactiva a los cambios de tráfico. Los proveedores pueden

inspeccionar contenidos específicos asociados a amenazas de malware.

L o s números o procesos "pseudoaleatorios" tienen características imprevisibles similares a las de los números o procesos verdaderamente aleatorios, pero en realidad no son matemáticamente aleatorios o imprevisibles. En los sistemas que no tienen medios para generar una verdadera aleatoriedad, se utiliza la pseudoaleatoriedad.

e. Honeypots y señuelos a nivel de datos

Además de las soluciones a nivel de red descritas anteriormente, los proveedores pueden hacer uso de señuelos a nivel de datos, como los honeypots, para "cebar" a los atacantes. Un honeypot suele ser un dato o un sistema dentro de una red que parece ser de valor para los actores maliciosos, que luego son bloqueados o vigilados cuando intentan acceder a él. Cabe señalar que los honeypots y otros señuelos pueden ser desplegados por terceros, y los proveedores pueden trabajar con dichas entidades para descubrir posibles actividades delictivas u otros ciberataques. Debido a su utilidad para descubrir actividades delictivas, los honeypots se utilizan en operaciones de picadura de las fuerzas del orden.

Prácticas básicas: Los proveedores pueden desplegar un honeypot de baja interacción, que tiene características limitadas y capacidades de recopilación de información, pero es de bajo riesgo porque no se produce una intrusión real. El honeypot simula una intrusión exitosa para engañar a los atacantes y recopilar información sobre ellos.

Capacidades avanzadas: Los proveedores pueden aprender más sobre los atacantes desplegando un honeypot de alta interacción. En este escenario, un atacante interactúa con el sistema real del proveedor en lugar de con una imitación, lo que a menudo expone vectores de ataque previamente desconocidos. Debido a la mayor exposición a los ataques, los honeypots de alta interacción son intrínsecamente más arriesgados, pero también más reveladores de los métodos de los atacantes.

2. MITIGAR LAS AMENAZAS DISTRIBUIDAS

Teniendo en cuenta la detección del tráfico malicioso y las posibles amenazas, los proveedores de infraestructuras también pueden aplicar diversos métodos de mitigación, que se describen a continuación, para hacer frente a estos retos.

Resumen de las prácticas básicas de mitigación: Los proveedores deben utilizar el filtrado de entrada, es decir, aplicar un filtro que pueda limitar la tasa de tráfico entrante. Los proveedores también deben hacer un esfuerzo razonable para dar forma al tráfico en sus redes y utilizar blackholing y sinkholing como herramientas de gestión de la red.

Resumen de las capacidades avanzadas de mitigación: Las empresas con acceso a mayores recursos pueden utilizar el filtrado de salida además del filtrado de entrada, limitando así la tasa de tráfico tanto de salida como de entrada. Pueden utilizar listas de control de acceso (ACL) para reducir los vectores de ataque. Las empresas pueden tomar medidas para minimizar las interrupciones del servicio al conformar el tráfico, por ejemplo, desplegando agujeros negros selectivos. Pueden utilizar tecnologías como BGP flowspec para aumentar las opciones de gestión del tráfico. Pueden trabajar en colaboración con el gobierno y la industria para acabar con las redes de bots maliciosas. También pueden ofrecer servicios comerciales como la depuración del tráfico y la protección DDoS.

a. Filtrado

Una de las complicaciones a la hora de mitigar las redes de bots es que los actores malintencionados utilizan la suplantación de IP para hacer que el tráfico malintencionado parezca proceder de un lugar distinto al de su origen real. [110] Al filtrar el tráfico malicioso cuando entra en la red del proveedor (es decir, filtrado de entrada, BCP38 y BCP84),[111] los proveedores pueden reducir la eficacia de la suplantación y, por tanto, dificultar los

ataques DDoS. Debido a los beneficios fácilmente observables de esta práctica, el Grupo de Trabajo de Ingeniería de Internet (IETF) ha reconocido el filtrado de entrada como una mejor práctica. [112] Cabe señalar que el filtrado de entrada funciona mejor en los puntos de entrada de la red, como las instalaciones del cliente, mientras que es mucho más difícil en los puntos de intercambio de la red.

Además, aunque los proveedores suelen estar bien situados para filtrar el tráfico malicioso, técnicas como BCP38 deberían ser empleadas por cualquier entidad que opere su propio espacio de direcciones IP, incluidas las empresas. Los proveedores, como los ISP, asignan muchas direcciones IP a sus clientes que, a su vez, pueden operar sus propias capacidades de filtrado y también necesitan seguir BCP38.

Además, al desplegar filtros en el borde de sus redes, los proveedores pueden supervisar el tráfico que sale de sus rincones del ecosistema y reducir el daño a otras partes. El filtrado de salida no sustituye al de entrada, sino que es una solución complementaria. Una combinación de filtrado de entrada y salida es la mejor manera de que los proveedores aumenten su capacidad de recuperación. [113]

Por último, en un entorno de red, las ACL se utilizan para identificar los flujos de tráfico en función de parámetros como su origen y destino, protocolo IP, puertos, EtherType y otras características. Un ejemplo común es que el tráfico de una interfaz de menor seguridad no puede acceder a una interfaz de mayor seguridad. [114] En algunos contextos, las ACLs pueden configurarse para tener en cuenta los privilegios de acceso de los usuarios individuales para limitar aún más los vectores de ataque por los que el malware puede infiltrarse en una red.

Prácticas básicas: Los proveedores deben filtrar el tráfico entrante (filtro de entrada) en los puntos de entrada de la red para reducir la cantidad de tráfico malicioso que entra en sus redes. El filtro debería ser capaz de limitar la tasa de tráfico entrante en caso de un ataque que pudiera saturar los recursos de la red.

Capacidades avanzadas: Lo ideal es que los proveedores filtren el tráfico saliente (filtrado de salida) además del tráfico entrante, y que puedan limitar la tasa de tráfico independientemente de si es saliente o entrante. Esta solución híbrida proporciona una mayor protección y convierte a los proveedores en vecinos responsables ante los demás en el ecosistema. Además, los proveedores pueden utilizar las ACL para reducir los vectores de ataque.

b. Conformación del tráfico

Cuando se identifica el tráfico potencialmente malicioso, los proveedores pueden gestionar el tráfico de forma segura, ya sea utilizando técnicas que normalmente provocan la caída del tráfico o retrasando el tráfico cuando la tasa de datos es anormalmente alta. Ambas técnicas pueden ser útiles en circunstancias específicas y pueden formar parte de una estrategia global de gestión del tráfico. [115]

Prácticas básicas: Los proveedores deben hacer un esfuerzo razonable para dar forma al tráfico en sus redes. Como mínimo, los proveedores deberían ser capaces de desplegar un "agujero negro" que impida que el tráfico llegue a un objetivo. Deberían esforzarse por reducir las interrupciones de los servicios legítimos redirigiendo el tráfico o eliminándolo sólo dentro de regiones geográficas definidas.

Capacidades avanzadas: Los proveedores con más recursos pueden moldear el tráfico sin causar tantas interrupciones al tráfico legítimo. Por ejemplo, los centros comerciales de depuración pueden limpiar el tráfico filtrando los elementos maliciosos y enviando el tráfico legítimo a su destino. Los pequeños proveedores pueden asociarse con los grandes para ofrecer estos servicios a sus clientes.

c. Blackholing

El blackholing es una técnica que hace caer todo el tráfico que se dirige a un destino específico en línea. Una versión común de esta técnica es el blackholing basado en el destino desencadenado de forma remota (RTDBH), en el que las redes ascendentes, que suelen ser las más cercanas al origen del ataque, eliminan el tráfico malicioso antes de que llegue a una víctima potencial.

Aunque el blackholing es eficaz para evitar que el tráfico malicioso llegue a su destino, un inconveniente obvio es que el tráfico legítimo tampoco puede llegar al destino, lo que puede ser el objetivo explícito de los actores maliciosos. Para minimizar este problema, los proveedores pueden emplear una técnica conocida como blackholing selectivo, que elimina el tráfico de determinadas regiones geográficas (como un país o un continente) mientras permite que el tráfico de otras regiones llegue a su destino.

Prácticas básicas: Los proveedores deberían hacer uso del blackholing para proteger sus redes. Aunque lo ideal es que los proveedores minimicen las interrupciones del tráfico legítimo, deberían al menos desplegar el RTDBH básico en circunstancias en las que no se disponga de herramientas más granulares o no funcionen tan bien.

Capacidades avanzadas: Los proveedores pueden mejorar la eficacia del blackholing aprovechando las asociaciones con otros proveedores tanto para los sensores como para los puntos de presencia de filtrado. Además, los proveedores pueden desplegar agujeros negros selectivos que minimicen las interrupciones del tráfico legítimo al dirigirse a una región geográfica específica.

d. Sinkholing

El sinkholing es una técnica en la que el tráfico dentro de un rango de IP concreto se envía a un servidor designado (el "sinkhole") mientras que el tráfico fuera de ese rango de IP continúa con normalidad. El propósito del sinkholing es capturar botnets tanto para fines de investigación como de mitigación. [116] El sinkholing se realiza a menudo a través de políticas de enrutamiento u otros métodos de enrutamiento, que atrapan el malware que compone una botnet en el sinkhole, donde puede ser estudiado por las fuerzas del orden y los investigadores. Cuando el malware atrapado en un sumidero intenta comunicarse con los servidores de mando y control, los expertos en seguridad pueden rastrear las direcciones IP de las máquinas a las que el malware suministra información, obteniendo así información sobre las actividades delictivas. Los proveedores también pueden cortar completamente las comunicaciones entre el malware y los servidores de mando y control. Los agujeros negros son esenciales para el desmantelamiento a gran escala de las redes de bots, que utilizan cientos de miles de sistemas con acceso a Internet en varios países del mundo.

Prácticas básicas: Los proveedores deben utilizar el sinkholing como una herramienta de gestión de la red para redirigir el tráfico malicioso entrante y recoger información sobre las amenazas a la red del proveedor para su análisis o para compartir información.

Capacidades avanzadas: Los líderes del sector pueden utilizar los sumideros para interrumpir y recopilar información sobre las amenazas de todo el ecosistema en colaboración con otros proveedores y las fuerzas del orden. Los proveedores también pueden ayudar a las operaciones internacionales de aplicación de la ley mediante la coordinación eficaz con las autoridades y las partes interesadas en numerosas jurisdicciones.

e. Fregado

Las soluciones de scrubbing suelen ser implementadas por centros de scrubbing dedicados, que analizan el tráfico de red y lo limpian de tráfico malicioso, incluido el DDoS. Dado que el scrubbing consume muchos recursos en comparación con otras soluciones, varios grandes proveedores ofrecen el scrubbing como servicio comercial. Al redirigir el tráfico a los centros en lugar de descartarlo, el scrubbing permite que el tráfico legítimo llegue a su destino con un alto grado de éxito. Esto hace que el scrubbing sea una alternativa preferible al blackholing y al sinkholing para muchas empresas.

Capacidades avanzadas: Los centros de depuración pueden añadir una importante capa de protección a las defensas de un proveedor o de un cliente, filtrando muchos tipos de ataques, que no se limitan únicamente a los ataques de inundación volumétrica. Por ejemplo, los centros pueden integrar tecnología que proteja contra los ataques basados en SSL (enlaces cifrados).

f. BGP flowspec

La especificación de flujos (flowspec) del Protocolo de Pasarela Fronteriza (BGP) es una tecnología dinámica que permite a los proveedores desplegar rápidamente una variedad de opciones de mitigación diferentes, permitiendo así a los expertos tomar decisiones en función de la situación. A diferencia de los enrutadores que sólo admiten el blackholing, los enrutadores de flowspec permiten opciones adicionales como el sinkholing del tráfico para que pueda ser estudiado por los expertos o, alternativamente, dar forma al tráfico y permitir que avance a una velocidad definida. [117]

Capacidades avanzadas: Los proveedores pueden utilizar BGP flowspec para desarrollar instrucciones personalizadas para los routers de frontera en lugar de las soluciones tradicionales de talla única. Con BGP flowspec, los enrutadores pueden recibir instrucciones para eliminar el tráfico, redirigirlo o limitar la velocidad del tráfico bajo la validación adecuada del originador del flowspec.

3. COORDINAR CON LOS CLIENTES Y LOS COMPAÑEROS

Para remediar las redes de bots u otras amenazas distribuidas puede ser necesario que los proveedores notifiquen a sus clientes o a sus compañeros sobre un desarrollo para asegurar su cooperación. Obviamente, la eficacia de las notificaciones depende en gran medida del usuario. Un estudio encargado por el M3AAWG descubrió que las llamadas telefónicas y el correo postal son las formas más eficaces de ponerse en contacto con los usuarios. [118] Otros métodos disponibles, que pueden y deben utilizarse, son el correo electrónico y los avisos en la página web. Otro método para ponerse en contacto con los usuarios es el "jardín amurallado": este enfoque limita el acceso de los usuarios a los servicios en línea hasta que tomen medidas específicas determinadas por su proveedor. En algunos países, los enfoques de este último tipo plantean problemas legales o de política pública. [119] Los compañeros pueden ser notificados con muchos de los mismos métodos que los clientes. Las notificaciones serán más eficaces si existe una relación establecida. Es útil que los proveedores se familiaricen con los actores clave de sus sectores para no tener que hacer presentaciones por primera vez durante una emergencia.

Prácticas básicas: Los proveedores deben notificar a los clientes o pares que violan la política de uso aceptable o se involucran en actividades nefastas. Si se bloquea el tráfico de un cliente o par, proporcionar tanto (1) un mensaje de texto o telefónico *como* (2) un aviso por correo electrónico/página web de la cuenta de usuario. El cliente o compañero debe recibir instrucciones claras sobre cómo ponerse en contacto con el proveedor a través de los canales de comunicación que no están siendo bloqueados.

Capacidades avanzadas: Los proveedores que cuentan con personal capacitado y recursos dedicados pueden reducir en gran medida la tasa de falsos positivos, de modo que los clientes rara vez experimentan interrupciones cuando utilizan los servicios de manera legítima.

4. ABORDAR LA INCAUTACIÓN Y RETIRADA DE DOMINIOS

Las fuerzas del orden disponen de herramientas específicas que se han utilizado en los últimos años para mitigar con cierto éxito las redes de bots maliciosas y los actores criminales. Cuando existen pruebas fehacientes de que una red delictiva está utilizando determinados dominios para llevar a cabo sus nefastos propósitos (por ejemplo, ataques de botnets), un proveedor puede trabajar en cooperación con las fuerzas del orden -y normalmente bajo su dirección obligatoria- para eliminar los dominios, de acuerdo con las leyes pertinentes. La acción de las fuerzas del orden que conlleva consecuencias en el mundo real para los malintencionados

Los actores son la única solución que aborda la causa de las redes de bots y los ataques DDoS, en lugar de los síntomas. Las acciones policiales de este tipo consumen muchos recursos y a menudo requieren un amplio análisis forense. Las incautaciones de dominios a gran escala también pueden requerir esfuerzos internacionales coordinados. [120] Por ejemplo, en 2016, los proveedores trabajaron con funcionarios gubernamentales de más de 30 países para derribar la red de bots Avalanche y tomar el control de más de 800.000 dominios repartidos por todo el ecosistema global de Internet y las comunicaciones. [121]

Prácticas de referencia: Los proveedores deben mantener una lista fácil de encontrar de puntos de contacto para las fuerzas de seguridad y los investigadores de seguridad. Los proveedores también deben tener una política bien definida que describa cómo pueden y no pueden apoyar los esfuerzos de las fuerzas del orden.

Capacidades avanzadas: Por lo general, los líderes del sector dispondrán de más procedimientos y tecnologías con los que

apoyar a las fuerzas del orden. También tendrán políticas definidas y posiciones legales sobre tácticas específicas de aplicación de la ley. Pueden llevar a cabo una evaluación global del riesgo para tener en cuenta los requisitos legales globales. Además de cooperar con las fuerzas del orden, los proveedores pueden tener procesos para colaborar con los competidores durante eventos excepcionales.

B. DESARROLLO DE SOFTWARE

El software es un elemento cada vez más omnipresente en todos los demás componentes del ecosistema abordado en esta Guía. Como se discute a lo largo de esta Guía, hay una amplia variedad de procesos de desarrollo complejos e interdependencias que impulsan la innovación y la mejora del software en los principales usuarios sistémicos del software destacados en la Guía: Infraestructura, dispositivos IoT, instaladores de sistemas y empresas. Por lo tanto, esta sección no pretende capturar las diversas prácticas de seguridad de base y las capacidades avanzadas que son pertinentes
al desarrollo de software especializado en cada parte del ecosistema. Por el contrario, pretende subrayar la importancia vital del software seguro en todas las partes de ese ecosistema. Cuando no se aborda específicamente en otra parte de esta Guía, el desarrollo de software debe consistir generalmente en estas prácticas.

Prácticas básicas y capacidades avanzadas para el software

1. PRÁCTICAS DE DESARROLLO SEGURAS POR DISEÑO

El software y las aplicaciones se integran cada vez más en nuestros procesos y productos comerciales y de infraestructura para mejorar la eficiencia. Pero esto los convierte en un objetivo principal para los hackers. La economía global, las infraestructuras críticas y las operaciones gubernamentales han aumentado su dependencia del software.

Las organizaciones que siguen las mejores prácticas hacen de la seguridad un elemento de calidad, llevando a cabo una serie de prácticas de desarrollo seguras, como la formación de los desarrolladores, el escaneo estático de la seguridad de las aplicaciones, el modelado de amenazas, las pruebas dinámicas de seguridad de las aplicaciones y las pruebas de penetración manuales a lo largo del ciclo de vida del desarrollo sobre la base de la gestión de riesgos. Los recursos para ayudar a los desarrolladores a adoptar estas mejores prácticas están disponibles públicamente. Por ejemplo, SAFECode (Software Assurance Forum for Excellence in Code), una organización líder dedicada a
que promueve el aseguramiento del software, publica recursos de formación sobre el desarrollo de software seguro disponibles de forma gratuita para el público, incluyendo las *Prácticas Fundamentales para el Desarrollo de Software Seguro*. [122]

Prácticas básicas: El desarrollo seguro por diseño debe incluir como mínimo lo siguiente:

Fuerte encriptación de los datos en reposo y en tránsito: El cifrado impide la visibilidad de los datos en caso de que sean robados o se acceda a ellos de forma indebida. Tanto si los datos están en reposo (es decir, almacenados) como en tránsito, el cifrado es una herramienta esencial para proteger la información. Aunque existen diferentes opciones de cifrado que se adaptan a las necesidades de organizaciones y productos específicos, el cifrado debe utilizar generalmente un
Un algoritmo fuerte que no pueda romperse fácilmente en el contexto de su caso de uso particular. La fuerza de un algoritmo puede variar contextualmente, dependiendo de factores como el tipo de ataque en cuestión y la necesidad de ciertos tipos de servicios para funcionar correctamente. Por ejemplo, un cifrado fuerte puede impedir el

funcionamiento de la mayoría de los cortafuegos y otros servicios de inspección de paquetes de seguridad.

Seguridad por defecto: Los ajustes de configuración por defecto del software deberían poner un gran énfasis en la seguridad. Los ajustes deberían tener que ser cambiados deliberadamente para que el software baje sus defensas y permita más opciones. Este principio reduce significativamente los vectores de ataque que los actores maliciosos pueden explotar.

- *Capacidad de aplicación de parches y diseño para la actualización:* Los programas informáticos deben diseñarse con la previsión de que serán necesarios parches y actualizaciones para protegerse de los ataques en constante evolución y cada vez más sofisticados de los agentes maliciosos. Los parches y las actualizaciones deben poder suministrarse con una intervención manual mínima y de forma razonablemente rápida y segura a los sistemas con el software instalado.
- *Principio del mínimo privilegio:* Limitando el acceso de los usuarios y de las aplicaciones únicamente a los privilegios esenciales para realizar las tareas necesarias, los desarrolladores de software pueden reducir la superficie de ataque de un producto. La aplicación del principio de mínimos privilegios en la fase de diseño reduce la posibilidad de que un actor malicioso o un servicio comprometido obtenga acceso administrativo y control sobre un sistema.

Análisis de la composición del software: El propósito de este análisis es crear un inventario de componentes de código abierto y de terceros en el producto. De este modo, los desarrolladores de software pueden tener conocimiento de los componentes que no han desarrollado ellos mismos en caso de que surjan problemas, aunque no puedan garantizar la seguridad de los componentes de terceros y de código abierto. Tener un inventario de los componentes que se utilizan en los productos y aplicaciones también puede ayudar a las organizaciones de desarrollo a rastrear e identificar las vulnerabilidades conocidas asociadas.

Concienciación y educación en materia de seguridad del software: La concienciación debe extenderse a todo el personal que forma parte del proceso de desarrollo de software, incluidos los desarrolladores, los gestores de productos y otros. Deberían ofrecerse oportunidades educativas o ejercicios de formación rentables.

Capacidades avanzadas: Las principales prácticas de seguridad por diseño incluyen lo siguiente:

- *Pruebas dinámicas de seguridad de aplicaciones (DAST):* Esta tecnología avanzada utiliza las pruebas de penetración (un ataque simulado) para descubrir las vulnerabilidades mientras se ejecuta una aplicación. Este tipo de pruebas puede ser especialmente útil en el contexto del IoT. Sin embargo, requiere opciones de configuración manejables y la capacidad de contratar especialistas altamente cualificados.

Pruebas estáticas de seguridad de aplicaciones (SAST): Con esta tecnología avanzada, los desarrolladores pueden escanear el código fuente o los binarios e identificar las vulnerabilidades. Está limitada a los lenguajes y plataformas compatibles. Para muchos productos del espacio IoT, esto podría no ser una opción. Sin embargo, puede utilizarse una cuidadosa revisión del código de los componentes especialmente sensibles para aumentar la seguridad.

- *Modelado de amenazas y análisis de riesgos para la arquitectura:* Las empresas que trabajan con gobiernos o cuyas operaciones son altamente sensibles pueden contratar equipos de expertos para determinar cómo los actores maliciosos crearían o explotarían hipotéticamente las vulnerabilidades de un sistema para lograr fines nefastos. Un modelo de amenazas puede considerar muchos tipos de riesgos, incluidos los que implican ataques automatizados y distribuidos.

Cadenas de herramientas centradas en la seguridad: Los desarrolladores pueden hacer uso de cadenas de herramientas centradas en la seguridad para crear nuevo software. Una cadena de herramientas es un conjunto de herramientas de software o hardware que facilitan el desarrollo de software. Cuando las cadenas de herramientas dan prioridad a la seguridad, los errores de codificación son menos frecuentes y los proveedores pueden aplicar controles de calidad. Las empresas pueden integrar las nuevas vulnerabilidades y las lecciones aprendidas en las herramientas de desarrollo.

Asegure los componentes de terceros y de código abierto: Las empresas líderes se asegurarán de que los componentes de terceros y las bibliotecas de código abierto que se utilicen estén libres de vulnerabilidades conocidas.

- Además, las empresas pueden dar fe a los clientes sobre los elementos del proceso de desarrollo de software seguro y buscar la certificación de la alineación con las normas internacionales.

2. GESTIÓN DE LA VULNERABILIDAD DE LA SEGURIDAD

Las distintas empresas del mundo tienen políticas diferentes en cuanto a cuándo y durante cuánto tiempo están disponibles los parches de seguridad para los clientes después de la comercialización de un producto con el fin de remediar las vulnerabilidades recién descubiertas. Mientras que los grandes fabricantes de productos tienden a publicar parches para sus productos con mayor regularidad, los fabricantes más pequeños suelen dedicar menos recursos a desarrollar y poner a disposición parches de seguridad. [123]

Prácticas básicas: Los proveedores deben priorizar las vulnerabilidades críticas en las aplicaciones de misión crítica.

Capacidades avanzadas: Los proveedores más avanzados pueden corregir casi todas las vulnerabilidades conocidas, especialmente las priorizadas durante la evaluación de riesgos. Tienen la capacidad de ofrecer garantías de seguridad a quienes compran software de su empresa o interactúan con ella a través de aplicaciones.

3. TRANSPARENCIA DE LOS PROCESOS DE DESARROLLO SEGUROS

Cada una de estas prácticas desempeña un papel importante en el desarrollo de software y hardware seguros. Las organizaciones de desarrollo de software y el sector privado han iniciado el desarrollo de evaluaciones basadas en el mercado de los procesos de desarrollo seguro. [124] Sin embargo, un marco desarrollado en asociación entre las partes interesadas del gobierno y la industria podría ayudar a estandarizar la terminología y los procesos, creando una mayor confianza en el mercado. El NIST está colaborando actualmente con SAFECode y otras partes interesadas para elaborar una publicación especial sobre procesos y prácticas de desarrollo de software seguro. La NTIA está convocando un proceso de múltiples partes interesadas para explorar cómo las organizaciones pueden comunicar información sobre componentes de software de terceros y ofrecer una mayor transparencia. [125]

Prácticas de referencia: Proporcionar un certificado de seguridad a las empresas que compran software.

Capacidades avanzadas: Proporcionar garantías de seguridad a quienes compran software de la empresa e interactúan con ella a través de aplicaciones

C. DISPOSITIVOS IOT

Esta edición de 2020 de la Guía se beneficia del trabajo realizado en el *C2 Consensus on IoT Device Baseline* Capabilities[126] , un proyecto relacionado auspiciado por el CSDE. El CSDE convocó a veinte importantes organismos de normalización, alianzas técnicas y grupos de la sociedad civil para aprovechar la amplia experiencia en ciberseguridad de las organizaciones. El libro blanco del C2 Consensus de capacidades recomendadas se publicó en septiembre de 2019.

En esta actualización de la Guía para 2020, el CSDE reafirma las prácticas de la Guía de 2018, pero reorganiza el material y cambia la redacción de las orientaciones para alinearlas con el Consenso C2 y otros esfuerzos de la industria. Se añaden dos prácticas adicionales a la guía de 2018 basadas en los resultados del Consenso C2 (*registro de eventos y documentación de la intención del dispositivo*).

Prácticas básicas y capacidades avanzadas para los dispositivos IoT

1. DESARROLLO SEGURO

La seguridad debe integrarse en el proceso de desarrollo, empezando por la planificación de los requisitos y continuando hasta la cualificación y la liberación. [127] Esta sección enumera las prácticas de desarrollo que son importantes para la seguridad de los dispositivos IoT pero que no suelen ser observables fuera de la organización.

a. Proceso del ciclo de vida del desarrollo seguro

En el proceso de SDL, cada fase de desarrollo tiene actividades de seguridad que pueden realizarse de forma manual o automática. [128]

Prácticas básicas: Debe existir un proceso de ciclo de vida de desarrollo seguro (SDL).

Aunque los elementos específicos de una SDL pueden variar, las SDL deben incluir los siguientes elementos orientados a la seguridad: identificación y disposición de amenazas; normas de codificación; requisitos de software de terceros; controles de seguridad de software y prueba y validación de capacidades; e identificación y tratamiento de nuevas vulnerabilidades.

Capacidades avanzadas: Después de establecer un proceso de ciclo de vida de desarrollo seguro, la empresa avanzada está midiendo y aumentando las capacidades del proceso. La medición de las capacidades de SDL forma parte del proyecto BSIMM (Building Security In - Maturity Model129); los materiales del BSIMM son de código abierto y pueden ser un recurso para este esfuerzo.

b. Uso de la cadena de herramientas centrada en la seguridad

Las cadenas de herramientas centradas en la seguridad son conjuntos de software o hardware que no sólo permiten el desarrollo, la producción y la gestión de productos, sino que también han sido diseñadas para mejorar la seguridad del producto final.

Prácticas básicas: Para el desarrollo, la compilación, la construcción y el mantenimiento del software deben utilizarse herramientas capaces de comprobar si la implementación sigue las directrices de codificación segura y de buscar un subconjunto de vulnerabilidades y exposiciones comunes (CVE) conocidas. También deben utilizarse lenguajes seguros para la memoria.

Capacidades avanzadas: Las técnicas de prueba como el fuzzing, la ejecución simbólica, el sandboxing, el análisis estático y el análisis dinámico deben utilizarse para complementar la cadena de herramientas centradas en la seguridad, para encontrar vulnerabilidades durante el proceso de desarrollo.

2. CAPACIDADES DE SEGURIDAD

Esta sección enumera las capacidades del dispositivo que suelen ser propiedades observables de un dispositivo después de su envío e instalación. En algunas arquitecturas de sistemas, estas importantes propiedades del dispositivo pueden encontrarse no en el propio dispositivo, sino en una pasarela o concentrador que forma parte de la estructura general. Cuando un dispositivo utiliza una determinada tecnología alámbrica o inalámbrica, necesitará un concentrador o una pasarela para conectarse a la Internet general. En ocasiones, las propiedades

que se indican a continuación pueden estar situadas en el concentrador o la pasarela en lugar de en el dispositivo, y seguir siendo plenamente efectivas porque no hay acceso al dispositivo salvo a través del concentrador o la pasarela.

a. Identificadores de dispositivos

La identidad de un dispositivo desempeña un papel durante todo su ciclo de vida. Los identificadores se utilizan para incorporar los dispositivos a una o varias redes, registrarlos, autenticarlos, autorizarlos, asignarles listas de acceso y políticas, controlarlos y gestionarlos en el desempeño de servicios y aplicaciones. Los identificadores también pueden ayudar a entender lo que ha ocurrido después de que un dispositivo o una red se hayan visto comprometidos.

Prácticas básicas: El dispositivo debe tener asociado un valor único que sea distinto y distinga al dispositivo de todos los demás.

Capacidades avanzadas: La seguridad del identificador del dispositivo debe reforzarse con protecciones criptográficas adicionales para la confidencialidad, la integridad y la disponibilidad.

b. Acceso seguro

Los productos IoT suelen requerir servicios administrativos locales o remotos. Durante el desarrollo y la fabricación del producto puede haber requisitos para otros tipos de acceso de bajo nivel a la memoria, el procesador, los periféricos o el flujo de control que no son necesarios o no están disponibles para el usuario final del dispositivo. Estas capacidades adicionales deben protegerse cuidadosamente.

Prácticas básicas: El dispositivo debe estar cuidadosamente protegido requiriendo la autentificación del usuario para leer o modificar el software, el firmware y la configuración, incluyendo medios para asegurar credenciales únicas para el acceso administrativo, y protegiendo el acceso a las interfaces.

Los pasos típicos a este nivel incluyen: Credenciales únicas de "administrador" por dispositivo o un requisito de primer arranque para cambiar las contraseñas; técnicas de limitación de velocidad para evitar la adivinación de contraseñas por fuerza bruta; asegurar o deshabilitar los puertos y servicios a nivel de desarrollador antes del envío del producto; eliminar los servicios administrativos locales y remotos no utilizados o inseguros, como telnet.

Capacidades avanzadas: Se debe considerar el control de acceso de los usuarios con autenticación multifactorial.

c. Los datos están protegidos

Esta categoría se refiere principalmente a la protección de los datos almacenados en el dispositivo y al cifrado de las comunicaciones de datos. La implementación de dichas protecciones puede implicar decisiones relativas, por ejemplo, a elementos de hardware seguros, proceso de arranque seguro, etc.; véase también la discusión sobre Criptografía en relación con la discusión sobre Seguridad arraigada en el hardware.

Prácticas básicas: Se debe proteger la confidencialidad e integridad de los datos en reposo y en tránsito. Para ello, las comunicaciones de datos deben estar encriptadas, salvo en los casos en que el análisis de riesgos indique lo contrario. Los datos sensibles deben almacenarse encriptados.

En general, deben emplearse los mecanismos de seguridad disponibles en cualquier sistema que se utilice para proteger los datos en reposo y en tránsito.

Capacidades avanzadas: Deben seleccionarse cuidadosamente las versiones actualizadas de los protocolos y mecanismos de seguridad; téngase en cuenta que la versión más reciente de una especificación puede no dejar obsoleta una versión anterior. La organización responsable del mantenimiento de la especificación pertinente (para el protocolo o el mecanismo de seguridad) debe utilizarse para determinar la aplicabilidad de la versión.

La memoria segura puede utilizarse en lugar del cifrado para la información almacenada. Deben utilizarse métodos de clave de cifrado que se ajusten a NIST FIPS 140-2 o ISO/IEC 24759. [130]

d. Protocolos aceptados por la industria

La buena criptografía es difícil. La criptografía que ha sido revisada y probada por expertos tiene muchas más posibilidades de éxito. Los protocolos aceptados por la industria han pasado por este proceso y han incorporado la experiencia de los expertos.

Prácticas básicas: Uso de protocolos seguros y ampliamente utilizados, excluyendo las versiones y protocolos obsoletos y sustituidos, para las comunicaciones hacia y desde el dispositivo.

Capacidades avanzadas: La memoria segura puede utilizarse en lugar de la encriptación para la información almacenada. Deben utilizarse métodos de clave de cifrado que cumplan o sean equivalentes a NIST FIPS 140-2 o ISO/IEC 24759. [131]

e. Validación de datos

Los datos que pueden ser proporcionados por un factor externo pueden ser elaborados para incluir caracteres especiales más allá de los caracteres alfanuméricos básicos. Caracteres como ".", "\N", "%" y ":" pueden tener consecuencias no previstas por el desarrollador. Las cadenas de datos maliciosas forman parte de muchos exploits.

Prácticas básicas: Cualquier entrada recibida desde el exterior del sistema debe ser gestionada de manera que un adversario externo no pueda disponer de ella para utilizarla directamente como código, comandos u otras entradas de flujo de ejecución. La entrada debe ser validada en cuanto a longitud, tipo de caracteres y valores o rangos aceptables. La salida de un subsistema a otro o a otro sitio también debe ser filtrada.

Capacidades avanzadas: Cualquier dato que se origine fuera del dispositivo y que vaya a ser procesado internamente es validado a la entrada y canonizado a la salida de cada etapa de procesamiento interno del dispositivo.

f. Registro de eventos

El registro es importante para el análisis forense y la comprensión en tiempo real de los fallos del sistema. Cuando algo va mal, es importante entender qué cadena de eventos condujo al fallo y qué dispositivos se vieron afectados. El registro en un sistema externo es deseable, pero no siempre es posible.

Prácticas de referencia: Los eventos de ciberseguridad relevantes deben ser registrados (sujetos a espacio de memoria disponible), asegurados y disponibles para los usuarios autorizados. Los eventos relevantes son específicos de la aplicación, pero algunos ejemplos son los intentos fallidos de inicio de sesión o los resultados negativos de las comprobaciones de ciberseguridad, como la medición del tiempo de arranque o la verificación del hash.

g. Criptografía

Prácticas básicas: Cuando se utilicen métodos criptográficos para garantizar la integridad y la confidencialidad de los datos, la autenticación de los derechos y el no repudio de las solicitudes, deben elegirse en función del riesgo evaluado. La implementación debe utilizar métodos criptográficos abiertos, publicados, probados y revisados por pares, con selecciones adecuadas de parámetros, algoritmos y opciones.

Siempre que sea posible, los métodos criptográficos deben ser actualizables. Deben evitarse los métodos obsoletos.

La seguridad basada en el hardware debe considerarse en cuanto a cómo encaja en los ciclos de desarrollo seguros de los productos actuales y futuros.

Los fabricantes de dispositivos no deben confiar únicamente en el uso de la ofuscación para asegurar los secretos (por ejemplo, las claves del dispositivo, los datos sensibles), pero la ofuscación puede utilizarse para aumentar la dificultad de un atacante para localizar el secreto. Aun así, el secreto debería estar protegido por otros medios, como el control de acceso y el cifrado.

Capacidades avanzadas: Criptografía sólida, probada y actualizable que utiliza métodos y algoritmos abiertos y

revisados por pares. Garantizar que la criptografía tiene la capacidad de soportar longitudes de clave resistentes a los efectos cuánticos para el cifrado simétrico. La seguridad basada en hardware se utiliza cuando es técnicamente posible.

En cuanto a las raíces de confianza, varios tipos de ataques se basan en la imitación de otra entidad. Por ejemplo, una fuente de confianza para el nuevo software de un dispositivo suele ser el fabricante original del hardware. La instalación de software corrompido con malware es obviamente algo que hay que evitar. Esto plantea la cuestión de cómo distinguir la diferencia.

La solución es tener un sistema de confianza. Una cadena de confianza es un enlace de elementos de hardware y software en el que cada elemento se valida a medida que se añade a la cadena. Al principio de la cadena hay una raíz de confianza, proporcionada por una entidad autorizada. La validación se realiza de forma criptográfica, utilizando firmas digitales. Como el primer elemento está vinculado a una autoridad de confianza, cada elemento validado criptográficamente por la cadena también puede ser de confianza.

Cuando el sistema recibe una actualización de software firmada, puede comprobar la firma digital. Dado que el propio sistema se basa en la confianza de la entidad autorizada original, una vez validada la actualización del software, se puede confiar en él.

h. Patchability

Esta capacidad puede ser bastante difícil desde el punto de vista técnico y de viabilidad. Sin embargo, ningún producto puede considerarse perfectamente seguro desde su fabricación hasta el final de su vida útil. Hasta que el dispositivo sea retirado de la red o puesto fuera de servicio, pueden ser necesarias actualizaciones para hacer frente a los exploits recién descubiertos. La industria está ofreciendo soluciones: Algunas empresas ofrecen "plataformas" de IoT que incluyen la actualización remota del software.

Prácticas básicas: Un plan de actualizaciones seguras con protección antiretroceso y un control de acceso adecuado a lo largo de un período definido de apoyo a la seguridad, cuando sea técnicamente posible. [132]

i. Reaprovisionamiento

La capacidad de revertir un dispositivo a un estado "en blanco" conocido como bueno permite eliminar los datos sensibles de un dispositivo cuando cambia de manos, como en la venta de una casa para los dispositivos domésticos inteligentes, o para el reciclaje de todo tipo de dispositivos.

Prácticas básicas: El fabricante proporciona a los usuarios autorizados la capacidad de reconfigurar y reimplantar de forma segura un dispositivo después de su comercialización, especialmente para devolver el producto a los valores predeterminados de fábrica o a un punto de restauración autorizado, y eliminar de forma segura los datos recogidos por el dispositivo (que no son esenciales para su
funcionamiento), dentro de un período definido establecido por la organización.

j. Señalización de la intención del dispositivo

Por razones similares a las de la documentación sobre la intención de los dispositivos (véase más adelante), la propagación de las redes de bots puede reducirse significativamente mediante protocolos como el Descriptor de Uso del Fabricante (MUD). [133] Otras herramientas son OMA-DM134 y TR- 69135 (estas dos últimas aplicables en los casos en que los dispositivos pueden gestionarse directamente), requisitos de seguridad como los perfiles de seguridad del Foro de Conectividad Abierto (Negro, Azul y Púrpura), y propuestas como IoTSense. [136]

Capacidades avanzadas: El dispositivo soporta el proceso de autenticación del dispositivo, autorizándolo con credenciales, y configurarlo para que se comunique dentro del dominio de seguridad apropiado.

k. Incorporación a la red de dispositivos

Si un dispositivo tiene acceso a la red, debe estar autorizado a ese acceso. Los dispositivos no autorizados en entornos domésticos y empresariales crean puntos débiles en la seguridad de la red. Un proceso de incorporación seguro y definido reduce los inconvenientes de la incorporación de un dispositivo a la red y le permite participar bajo autorización.

Capacidades avanzadas: El dispositivo soporta un protocolo para que el dispositivo proporcione información a los routers o firewalls aguas arriba en relación con el uso previsto de la red. De forma equivalente, el dispositivo proporciona heurística relacionada con su propio comportamiento en el funcionamiento normal en apoyo del análisis de la red.

3. GESTIÓN DEL CICLO DE VIDA DEL PRODUCTO

La gestión del ciclo de vida del producto (PLM) se refiere a la gestión activa de un producto desde su concepción hasta el diseño, la fabricación, el soporte y el fin de su vida útil.

a. Tratamiento de la vulnerabilidad

Las vulnerabilidades ocurren. Una organización debe tener procesos activos para encontrarlas, como esfuerzos internos, intercambio de amenazas y apertura a la divulgación externa (ética).

Prácticas básicas: Los proveedores -fabricantes y minoristas- deben crear una política y un proceso de vulnerabilidad de seguridad para identificar, priorizar, mitigar y, en su caso, revelar las vulnerabilidades de seguridad conocidas en sus productos.

b. Actualización y divulgación de la EdC

Esta capacidad debe ser considerada cuidadosamente dentro de la organización. Está vinculada a la gestión de la vulnerabilidad, al ciclo de vida del producto, a las condiciones de servicio, etc.

Prácticas básicas: Los proveedores de dispositivos deben tener una política de soporte de seguridad definida que incluya el manejo de cualquier vulnerabilidad de seguridad de fin de vida (EoL) o de fin de servicio (EoS), si las actualizaciones estarán disponibles y cómo, y qué hacer con el dispositivo en ese momento.

c. Documentación sobre la intención del dispositivo

El uso de la red diseñado y previsto de un dispositivo -puertos, protocolos, sitios que se van a visitar, niveles de tráfico de datos esperados, comunicaciones con otros dispositivos- es una información importante a la hora de determinar si la unidad ha sido comprometida, incluso en una red de bots.

Prácticas de referencia: El fabricante del dispositivo proporciona documentación sobre el uso de la red tal y como se ha diseñado públicamente, ya sea en la documentación del producto o en otros medios para los usuarios del dispositivo.

D. INSTALACIÓN DE SISTEMAS PARA EL HOGAR Y LA PEQUEÑA EMPRESA

Los hogares y las pequeñas empresas se benefician de los dispositivos conectados en varias categorías. Los sistemas de calefacción, ventilación y aire acondicionado (HVAC) se conectan para ofrecer funciones inteligentes y acceso remoto por parte del ocupante. Los sistemas de seguridad incluyen cámaras, cerraduras y sistemas de alarma que pueden gestionarse a través de Internet. Entretenimiento se benefician de los controles centrales para poder gestionar con facilidad las complejas configuraciones de audio y vídeo. Hay una gran diversidad de fabricantes y sistemas en estas categorías. Estos sistemas pueden ser instalados por los propietarios de viviendas y negocios, o por profesionales: integradores, contratistas de alarmas y otros.

Lo ideal es que todos los dispositivos y sistemas que entren en un entorno doméstico, de oficina, comercial, médico o industrial estén protegidos por las mejores prácticas en todo el ciclo de vida del dispositivo. Este ciclo de vida incluye la instalación y configuración de el dispositivo. Una buena instalación logrará la "mejor seguridad disponible" del producto fabricado. En esta sección se encuentran las prácticas básicas y las capacidades avanzadas para lograr esa mejor seguridad disponible de los tipos de dispositivos más comunes.

El material que figura a continuación se ha extraído en gran medida de *The Connected Home Security System*. [137]

Prácticas básicas y capacidades avanzadas para la instalación de sistemas domésticos y de pequeñas empresas

1. AUTENTICACIÓN Y GESTIÓN DE CREDENCIALES

Las instalaciones pueden beneficiarse de los sistemas de gestión de contraseñas, que son un almacenamiento cifrado de las mismas. Estos sistemas quitan a los usuarios la carga de recordar y gestionar las contraseñas y las ponen en un lugar seguro.

Prácticas básicas: Si una contraseña no es única para el dispositivo, el instalador debe cambiarla por una contraseña fuerte. (Véase [1], "Contraseñas"). Deben utilizarse contraseñas diferentes para todos los dispositivos y sistemas. La instalación debe utilizar un sistema de gestión de contraseñas de confianza.

Capacidades avanzadas: Se utiliza el control de acceso de usuarios con autenticación multifactor.

2. CONFIGURACIÓN DE LA RED

La configuración de la red se refiere a la disposición física y lógica y a las conexiones y ajustes de los componentes de la red.

a. General

Prácticas de referencia: Los sistemas (ordenadores de sobremesa, portátiles, etc.) deben tener actualizados los antivirus y

Los herramientas de malware instaladas y en funcionamiento. No deben ejecutarse sistemas con privilegios administrativos a menos que se requiera específicamente.

b. Configuración del cortafuegos, el punto de acceso y el router

Prácticas básicas: UPnP debe estar deshabilitado en el lado WAN (lado que da a Internet) a menos que sea necesario para un propósito legítimo (por ejemplo, juegos entre pares). Se debe asignar un espacio DHCP adecuado para el uso previsto, pero sin excederlo. Debe activarse un cortafuegos con los puertos necesarios desbloqueados. El reenvío de puertos debe estar desactivado, excepto para aplicaciones específicas en las que sea necesario.

Capacidades avanzadas: Las redes deben ser monitoreadas, utilizar valores de puerto no estándar en las aplicaciones y tener el reenvío de puertos sólo selectivamente habilitado para aplicaciones específicas en conjunto con las protecciones del firewall. Aunque un atacante sofisticado puede superarlo, debe utilizarse el filtrado de direcciones MAC.

c. Estructura física y lógica

Prácticas básicas: El acceso a la red debe limitarse desde fuera de la estructura física del sitio del cliente en términos de potencia inalámbrica y colocación del cableado físico. Los segmentos deben estar separados según su finalidad y utilizar redes físicas o lógicas separadas, utilizando opciones como canales de radio separados, cableado, puntos de acceso separados o pasarelas.

Capacidades avanzadas: Los segmentos deben separarse adicionalmente para diferentes propósitos usando VLANs o VPNs. Se puede utilizar una herramienta de escaneo de puertos para supervisar la red privada.

3. GESTIÓN DEL HARDWARE DE LA RED

La gestión del hardware de la red se refiere al proceso continuo de mantener los dispositivos de la red correctamente identificados y configurados.

a. Módems y routers, dispositivos de gestión de red

Prácticas básicas: Los dispositivos de red deben tener un proceso o medio para actualizar regularmente el firmware.

Capacidades avanzadas: Para los sistemas de módem/enrutador/AP proporcionados por el ISP, se puede añadir un enrutador/AP independiente del mercado secundario para manejar el tráfico de la LAN para el control local de las actualizaciones de software.

b. Protocolos

Los protocolos de red son los lenguajes de varios niveles que se utilizan para comunicarse en las redes, como TCP, UDP, IP, RTP, etc.

Prácticas básicas: No se deben utilizar protocolos obsoletos. En particular, no utilice o permita que se negocie SSL (cualquier versión), o TLS 1.0 o 1.1.

Capacidades avanzadas: Configure para los protocolos más recientes cuando corresponda.

c. Enlaces inalámbricos

Los enlaces inalámbricos son conexiones de red basadas en la radio entre dispositivos. Estos enlaces pueden ser unidireccionales, bidireccionales o utilizar una topología de red entre múltiples dispositivos.

1)Bluetooth

Prácticas básicas: Las funciones de seguridad disponibles deben estar activadas. Las opciones "no descubribles" deben cuando esté disponible. No debe exponerse ninguna información sensible en las señales de balizas de Bluetooth de baja energía (BLE)

2) NFC

Prácticas básicas: Los lectores NFC no deben estar situados o montados para permitir un fácil "olfateo" o para fácil de manipular.

3) Wi-Fi

Prácticas **básicas:** Además de las prácticas de configuración de la red de referencia mencionadas en otras secciones, deben utilizarse opciones de cifrado Wi-Fi actualizadas, como WPA2 o WPA3 (la versión más reciente). El WPS debe estar desactivado. No se deben utilizar SSIDs por defecto ni de difusión.

Muchos puntos de acceso disponen de una opción de "red de invitados"; debería estar habilitada y disponible para los usuarios de mayor riesgo, como los visitantes o los residentes/trabajadores temporales. Si está disponible, debería habilitarse la protección del marco de gestión 802.11aw. Asegúrese de que el acceso a la configuración del Punto de Acceso está protegido con una contraseña fuerte según las mejores prácticas descritas en este documento. Habilite el filtrado de puertos cuando corresponda. Elija un Punto de Acceso/Router con firmware actualizable.

4) Z-WAVE

Prácticas básicas: La seguridad básica implica identificaciones únicas de la casa, funciones administrativas protegidas por contraseña y el uso de dispositivos habilitados con AES-128 cuando estén disponibles.

Capacidades avanzadas: Para aumentar la seguridad, la potencia de RF puede cumplir los requisitos de distancia y se pueden utilizar exclusivamente dispositivos habilitados para AES-128.

5) Zigbee

Prácticas básicas: El único dispositivo conectado a Internet debe ser la pasarela ZigBee y debe haber un cortafuegos que la proteja.

Capacidades avanzadas: El tráfico de Internet puede filtrarse al entrar y salir de la red ZigBee por dirección (origen y destino) y número de puerto. Las funciones de seguridad 802.15.4 opcionales pueden habilitarse en el nivel 802.15.4 y en el nivel de red más aplicación, cuando estén disponibles.

6) Control de acceso a dispositivos remotos

Esta categoría incluye todo tipo de control de acceso remoto de las funciones normales de los dispositivos, como el vídeo de la cámara de seguridad, el control de la temperatura de la calefacción y la ventilación, los subsistemas del vehículo, como el arranque a distancia o el desbloqueo de la puerta, etc.

Prácticas básicas: Las alertas de fallo o manipulación del dispositivo deben estar activadas cuando estén disponibles. Todos los accesos remotos deben estar detrás de un cortafuegos con restricción de IP, permitiendo sólo direcciones IP y subredes de la lista blanca para acceder al dispositivo, independientemente del puerto. Si el acceso remoto desde fuera del cortafuegos es una característica necesaria, deben utilizarse VPN y puertos de Internet no estándar para el acceso remoto.

4. MANTENIMIENTO DE LA SEGURIDAD

Prácticas de referencia: Siempre que sea posible, los intentos de violación en la red u otros intentos en la instalación deben ser rastreados y revisados para tomar medidas. Los intentos de violación deben correlacionarse para identificar a los individuos u objetivos comúnmente atacados dentro de la red. La configuración de la red debe documentarse, los dispositivos conectados deben enumerarse y debe definirse claramente un plan de mantenimiento de la seguridad.

E. EMPRESAS

Como principales propietarios y usuarios de dispositivos y sistemas en red, incluyendo un número exponencialmente creciente de sistemas de dispositivos IoT, las empresas de todo tipo - gobierno, sector privado, académico, sin ánimo de lucro - tienen un papel crítico que desempeñar en la seguridad del ecosistema digital. [138] Si bien las empresas suelen ser víctimas de ataques automatizados y distribuidos, así como de intentos de exfiltración de datos, sus vastos sistemas también pueden ser secuestrados para aumentar el impacto de los ataques DDoS y otros ataques distribuidos en otros. En consecuencia, las empresas se encuentran colectivamente entre las partes interesadas importantes que comparten la responsabilidad de asegurar adecuadamente sus redes y sistemas con el fin de ayudar a asegurar el ecosistema digital más amplio.

Los millones de empresas del sector privado y de la administración pública de todo el mundo difieren considerablemente en cuanto a sus conocimientos y habilidades técnicas, acceso a recursos e incentivos para adoptar prácticas de seguridad básicas. Las empresas más grandes, por ejemplo, suelen tener un director de información y un director de seguridad de la información, cada uno de los cuales se encarga en parte de proteger los sistemas y dispositivos en red de la organización, incluidos los sistemas de IoT. Las empresas más pequeñas pueden carecer de recursos para dedicar personal de TI y de seguridad de la información y, en su lugar, dependen de soluciones estándar.

Las organizaciones están desarrollando y ofreciendo cada vez más herramientas para ayudar a las empresas, tanto pequeñas como grandes, a proteger sus redes y sistemas. Tal vez lo más relevante para esta Guía es el esfuerzo de la Coalición de Ciberseguridad para desarrollar y avanzar en los Perfiles para la Prevención y Mitigación de DDoS y Botnet bajo el Marco de Ciberseguridad,[139] destinado a ayudar a las empresas y otras organizaciones a abordar y mitigar los ataques DDoS y otros ataques automatizados y distribuidos.

Las empresas deben suscribirse a múltiples fuentes o servicios de inteligencia sobre amenazas para utilizarlos junto con los esfuerzos de correlación/automatización de la información de seguridad y la gestión de eventos (SIEM). Las empresas deben contar con procesos para compartir la información sobre amenazas obtenida interna o externamente con los accionistas internos de manera oportuna y procesable. Las empresas deben mantener el contacto con las comunidades de intercambio y ser conscientes de los procesos y salvaguardias para informar/compartir adecuadamente los incidentes de ciberseguridad dentro de su región y sector. Las empresas deben compartir la información interna sobre amenazas de forma continua. Los indicadores de compromiso (IOC) y las amenazas notables deben compartirse con regularidad.

Capacidades avanzadas: Las empresas avanzadas deben comprometerse a mejorar la comunidad de intercambio de información sobre ciberamenazas mediante el intercambio responsable y oportuno de información sobre ciberamenazas desensibilizada con las distintas comunidades de intercambio adecuadas (gobierno, industria, etc.). Las empresas avanzadas deben asegurarse de que cuentan con las capacidades suficientes para detectar, analizar y capturar la información sobre ciberamenazas en formatos que favorezcan las actividades de intercambio. Las empresas avanzadas deben participar activamente en la gobernanza y la mejora de las comunidades de intercambio de información sobre ciberamenazas adecuadas a su región e industria. Las empresas avanzadas deben tratar de mejorar continuamente sus capacidades de detección, análisis, respuesta e intercambio.

3. ARQUITECTURAS DE RED QUE GESTIONAN DE FORMA SEGURA LOS FLUJOS DE TRÁFICO

Las empresas pueden ejercer el control sobre el diseño de sus arquitecturas de red para limitar el flujo de tráfico malicioso durante un ataque DDoS realizado mediante botnets u otros medios. [142] Una arquitectura de red diseñada con la seguridad como objetivo explícito puede complementar otras medidas de precaución, como los servicios anti-DDoS ofrecidos por los proveedores de infraestructura y otros participantes del ecosistema. Las interfaces de programación de aplicaciones (API) gestionan las conexiones entre las aplicaciones, los dispositivos y los sistemas de datos back-end. En términos generales, las API permiten a las empresas abrir sus datos y funcionalidades de back-end para su reutilización en nuevos servicios de aplicación. El despliegue de la seguridad en el perímetro, a través de un API Gateway, puede ayudar a las empresas a detener las amenazas antes de que penetren en la empresa, permitiéndoles proporcionar acceso a los datos de la empresa a los desarrolladores de aplicaciones al tiempo que mantienen una fuerte seguridad.

Prácticas básicas: Las empresas deben obtener una defensa de la intranet contra los DDoS mediante el consumo de las capacidades y servicios proporcionados por los proveedores de servicios de red. Las empresas deben estandarizar la arquitectura de interconexión de Internet a la intranet, la política y los procesos operativos, y los ajustes de configuración de control de acceso y flujo de paquetes. Las empresas deben aplicar un régimen que garantice la correcta implantación y funcionamiento de esta arquitectura. Además, las empresas deben inspeccionar todos los flujos de datos entrantes y salientes y el correo electrónico y bloquear los paquetes o correos electrónicos con malware; bloquear el tráfico de red no autorizado en la intranet; y utilizar la arquitectura y las prácticas operativas de la DMZ estándar del sector.

Capacidades avanzadas: Las empresas avanzadas pueden identificar comportamientos observables que indican flujos de

botnets, como flujos de C&C de botnets, DNS de flujo rápido y acceso a URLs sospechosas. Las empresas avanzadas pueden bloquear automáticamente los flujos de las redes de bots y remediar las fuentes de los flujos; eliminar los enlaces de URLs accesibles desde Internet de los correos electrónicos entrantes; compartir y recibir información que se utiliza para identificar a los actores de las redes de bots; y evitar acciones de DNS inadecuadas tanto por parte del solicitante de DNS como del servidor de DNS.

Para aumentar la resistencia frente a los ataques distribuidos, las empresas avanzadas pueden hacer uso de pasarelas de interfaz de programación de aplicaciones. Las interfaces de programación de aplicaciones (API) gestionan las conexiones entre las aplicaciones, los dispositivos y los sistemas de datos back-end. El despliegue de la seguridad en una arquitectura centralizada a través de un API Gateway puede ayudar a las organizaciones a proporcionar acceso a los datos de la empresa para la aplicación
desarrolladores manteniendo una fuerte seguridad.

4. MAYOR RESISTENCIA AL DDOS

Incluso con esfuerzos muy exitosos de concienciación y educación de los clientes, muchos de ellos carecerán de los conocimientos técnicos necesarios para asegurar sus propias redes. En lugar de ignorar la amenaza que pueden suponer las redes de bots y otros ataques distribuidos, las empresas deberían adquirir una protección comercial contra DDoS adecuada a su perfil de riesgo. [143] Los servicios comerciales pueden incluir protección fuera de las instalaciones o una combinación de protección fuera y dentro de las instalaciones que proteja más sólidamente a la empresa contra los ataques distribuidos. Cuando los clientes adquieren productos y servicios comerciales, disminuyen sustancialmente la amenaza de las redes de bots y otros ataques distribuidos.

Los miembros del CSDE proporcionan algunas de las soluciones comerciales de DDoS de más alta gama del mercado. Algunos ejemplos son las pasarelas domésticas con seguridad integrada, los servicios Anycast y una variedad de servicios de seguridad gestionados. Los servicios Anycast aumentan la resistencia a los ataques DDoS proporcionando múltiples rutas para la entrega de contenidos y equilibrando las cargas de trabajo a través de múltiples elementos de red, que pueden estar repartidos por todo el mundo. Si un ataque DDoS compromete ciertas partes de una red, el tráfico se redirige automáticamente a otra parte. Los servicios de seguridad gestionados incluyen servicios comerciales de depuración. [144] Otros servicios comerciales incluyen cortafuegos basados en la red, sistemas de gestión de dispositivos móviles, análisis de amenazas y detección de eventos, conectividad VPN segura a la nube, seguridad web y de aplicaciones, y seguridad del correo electrónico.

Los proveedores pueden ofrecer soluciones de filtrado adaptadas a las necesidades únicas y a los perfiles de riesgo de sus clientes. Lo ideal es que estas soluciones integren las defensas locales y externas. Los servicios comerciales pueden permitir bloquear el tráfico malicioso más cerca del origen del ataque, creando una capa adicional de seguridad para los clientes.

Prácticas básicas: Las empresas deben disponer de un soporte retenido/de contingencia capaz de responder eficazmente a los incidentes de ciberseguridad y mantener un nivel razonable de seguridad. Las empresas deben seleccionar proveedores comerciales cuyos productos y servicios incluyan capacidades de seguridad adecuadas (es decir, proveedores de servicios de Internet y de alojamiento en la nube que tengan capacidades de protección contra DDoS, software con capacidades de actualización automática, etc.). Las empresas deben tener planes documentados y probados para la respuesta a incidentes, incluida la respuesta a DDoS y botnets. Las empresas deben seleccionar proveedores comerciales que puedan proporcionar una respuesta automatizada o por defecto. Las empresas deben reevaluar periódicamente la eficacia de los proveedores comerciales.

Capacidades avanzadas: Las empresas avanzadas deben adoptar un enfoque de varios niveles para la protección contra DDoS y botnets que incluya capacidades bien respaldadas dentro y fuera de las instalaciones. Las empresas avanzadas deben aumentar de forma proactiva los conocimientos técnicos de su personal, determinar las lagunas en estos conocimientos y abordar estas lagunas con la formación adecuada, apoyo contratado/de contingencia y personal adicional. Las empresas avanzadas deben considerar los servicios comerciales y los programas informáticos que ofrecen capacidades avanzadas, como el aprendizaje automático y el análisis de patrones, para permitir resultados de mayor calidad. Las empresas avanzadas

deben tratar de mejorar continuamente sus capacidades reevaluando periódicamente las capacidades disponibles en el mercado.

5. GESTIÓN DE IDENTIDADES Y ACCESOS

Las identidades constituyen el punto de control unificador entre aplicaciones, dispositivos, datos y usuarios. Las herramientas de gestión de identidades y accesos autentifican a los individuos y servicios y gobiernan las acciones que se les permite realizar. Una de las áreas más importantes del riesgo de TI se refiere a los usuarios privilegiados, como los administradores de TI, los CISO y otros
personas con mayor acceso a los sistemas. Ya sea de forma involuntaria o maliciosa, las acciones indebidas de los usuarios con privilegios pueden tener efectos desastrosos en las operaciones de TI y en la seguridad y privacidad general de los activos y la información de la organización. Los sistemas deben estar configurados para que los administradores sólo realicen las acciones esenciales para su función, lo que permite un "acceso menos privilegiado" para reducir el riesgo. Los análisis de amenazas pueden proporcionar información sobre la actividad y trabajar para prevenir o señalar cualquier cosa inusual que indique un riesgo para la seguridad. [145]

Un avance reciente que merece la pena destacar es el uso de claves de seguridad físicas en lugar de contraseñas o códigos de un solo uso. Desde principios de 2017, cuando Google comenzó a exigir a todos sus empleados - más de 85.000 en total- el uso de claves de seguridad físicas, no se ha producido el phishing de ninguna cuenta relacionada con el trabajo de ningún empleado. [146]

Prácticas de referencia: Las prácticas de gestión de identidades y accesos de las organizaciones deberían incluir al menos lo siguiente:

- *Autenticación* (incluida la autenticación multifactorial y la basada en el riesgo): una operación de acceso que garantiza que el sujeto es realmente el sujeto real y no un suplantador;
- *Autorización* - una operación de acceso que determina, dado el estado actual, si se debe conceder el acceso;
- *Gobernanza del acceso*: un proceso para ayudar a los líderes empresariales a definir y perfeccionar las políticas para determinar el acceso adecuado;
- *Contabilidad*: proceso de registro de datos sobre la actividad de los usuarios individuales que acceden a los recursos del sistema para analizar tendencias e identificar comportamientos sospechosos;
- *Aprovisionamiento/Orquestación*: conjunto de operaciones que se producen en los momentos de cambio y que facilitan el proceso de unión/traslado/abandono y la coordinación de los eventos de cambio entre recursos dispares conectados; y

Repositorio de Identidad - un almacén persistente para mantener el estado actual y los valores de los atributos de los perfiles de los sujetos.

Las empresas también deberían adoptar la práctica del offboarding, que es la eliminación oportuna de la identidad del directorio de la empresa y la revocación de la identidad y los accesos asociados, en un plazo de 24 horas para los accesos privilegiados y los accesos a los recursos en la nube.

Para mejorar la autenticación, las empresas deberían utilizar frases de contraseña más fuertes y fáciles de recordar en lugar de contraseñas basadas en reglas de sintaxis; cotejarlas con un diccionario de contraseñas; y utilizar un medidor de fortaleza de contraseñas. Además, las empresas deberían hacer uso de una segunda autenticación o autenticación multifactorial (2FA/ MFA) para los

accesos privilegiados, por ejemplo, los administradores de sistemas. Las organizaciones deberían utilizar un servicio de autenticación centralizado para las aplicaciones web y SaaS con Single Sign-on que requiera 2FA - autenticación escalonada - para los dispositivos que no sean previamente investigados y de confianza. Además, las empresas deberían utilizar tokens FIDO U2F para frustrar los ataques de phishing o tomar otras precauciones razonables para reducir el riesgo que suponen los ataques de phishing.

Las empresas deben adherirse al principio de acceso menos privilegiado - solicitud de acceso basada en roles a través del Control de Acceso Basado en Roles (RBAC) y/o aprobaciones, detección y remediación de accesos fuera de proceso, atípicos, inactivos y de violación de la Separación de Funciones (SoD), y gobierno de los accesos a través de la revalidación periódica de los mismos (Continuación de las Necesidades de Negocio o CBN).

Las empresas deben llevar a cabo una supervisión y auditoría de usuarios privilegiados y una gestión segura de eventos de información (SIEM). También deberían tener una bóveda de credenciales/secretos para los ID de servicios o aplicaciones; los ID no deberían almacenarse en archivos de configuración en texto plano.

Capacidades avanzadas: Las empresas avanzadas pueden tener métodos más sofisticados para gestionar la identidad y el acceso:

- Los métodos de *autenticación continua* aprovechan la monitorización del comportamiento y la biometría a lo largo de una sesión de usuario para determinar si la sesión se ha visto comprometida.
- *La autenticación basada en el riesgo* proporciona a las empresas una mejor comprensión del contexto en torno a la identidad, por ejemplo, mediante datos de geolocalización o comportamiento de compra. Un sistema puede reconocer la identidad, determinar que la autenticación tradicional es innecesaria y permitir el acceso. Por el contrario, si el sistema detecta anomalías, como el inicio de sesión desde un país extranjero en medio de la noche después de tener unas cuantas contraseñas fallidas, entonces se trata de una operación de muy alto riesgo y se denegará el acceso en ausencia de pasos adicionales de autenticación.
- Las soluciones *de gestión de accesos privilegiados* proporcionan la visibilidad, la supervisión y el control necesarios para aquellos usuarios y cuentas que tienen las "llaves del reino". Es esencial que se permita a los administradores realizar sólo las acciones esenciales para su función, lo que permite el "acceso menos privilegiado" para reducir el riesgo. Esta visibilidad proporciona una visión de la actividad y trabaja para prevenir o señalar cualquier cosa inusual que indique un riesgo para la seguridad.
- La *autenticación adaptativa* utiliza la 2FA/MFA, con un cálculo de riesgos más completo y sofisticado, por encima de la huella digital del dispositivo, incorporando factores como la intranet o internet, el acceso simultáneo desde múltiples ubicaciones o geografías, el inicio de sesión a horas muy extrañas, etc.

La gobernanza de *la identidad en bucle cerrado* integra la supervisión y el análisis de la actividad de los usuarios en los servidores y en las aplicaciones internas con herramientas de gestión del acceso, por ejemplo, para revocar el acceso de un usuario privilegiado si se detecta que accede a datos protegidos en el servidor o en las aplicaciones internas de forma no autorizada.

Puede lograrse *una* gobernanza de *acceso más inteligente* con análisis e IA, por ejemplo, detectando y revocando los accesos inactivos, es decir, los accesos que no han sido utilizados por sus propietarios durante un período prolongado, lo que indica posibles lagunas en la gobernanza de acceso o en la incorporación.

- *La detección y la protección contra la piratería informática* pueden mejorarse con la integración de la gestión del acceso a los privilegios y el análisis del comportamiento de usuarios y entidades (UEBA): el malware introducido en las estaciones de trabajo a través de la suplantación de identidad mediante información de redes sociales y correos electrónicos se comportará de manera diferente y puede indicar que una estación de trabajo y las credenciales privilegiadas han sido comprometidas.

6. MITIGAR LOS PROBLEMAS DE LOS PRODUCTOS ANTICUADOS Y PIRATEADOS

Las empresas deben dejar de utilizar los productos heredados para los que ha finalizado el soporte del fabricante. [147] Un problema estrechamente relacionado desde el punto de vista del soporte técnico es el software pirata. En Estados Unidos, casi uno de cada cinco ordenadores personales utiliza software pirata, mientras que en China el porcentaje de ordenadores personales con software pirata a menudo supera el 70%. [148] Por supuesto, los fabricantes no suelen poner parches al software pirata, lo que significa que sigue siendo vulnerable a los exploits conocidos. [149] Las empresas deberían evitar el software pirata y disminuir el número total de vulnerabilidades en el ecosistema global de Internet y las comunicaciones.

Prácticas básicas: Las empresas deben reemplazar los productos legítimos con soporte antes de que el soporte del fabricante expire. Las empresas deben evitar siempre los productos piratas. Dichos productos son ilegales en la mayoría de los países y, además, contribuyen en gran medida a las vulnerabilidades de seguridad en todo el ecosistema. [150]

Capacidades avanzadas: Las empresas avanzadas pueden disponer de los últimos productos compatibles con las funciones y capacidades de seguridad más actualizadas.

6 / Próximos pasos y conclusión

La publicación de la versión 2020 de esta Guía constituye la continuación de una campaña estratégica sin precedentes liderada por la industria contra las botnets y otras amenazas automatizadas y distribuidas. El CSDE, USTelecom y la CTA instan a las partes interesadas a aplicar las prácticas recomendadas para hacer frente a los retos comunes y cambiar el rumbo de los malos actores.

Como se señaló en la introducción, la economía digital ha sido un motor de crecimiento comercial y de mejora de la calidad de vida en todo el mundo. Ninguna parte interesada -del sector público o privado- controla este sistema, por lo que la gestión segura de las oportunidades que ofrece este crecimiento es responsabilidad imperativa de todas las partes interesadas de la comunidad de las TIC.

Para ello, presentamos estas prácticas básicas y capacidades avanzadas para que las consideren todas las partes interesadas. Se trata de soluciones dinámicas y flexibles, basadas en normas de consenso voluntario e impulsadas por las poderosas fuerzas del mercado, que pueden ser aplicadas por las partes interesadas en toda la economía digital mundial. Esta es la mejor respuesta a los retos de ciberseguridad sistémica a los que nos enfrentamos.

Con este imperativo en mente, planeamos continuar actualizando, publicando y promoviendo una nueva versión de esta Guía anualmente, reflejando los últimos desarrollos y avances tecnológicos que ayudarán a nuestras empresas y a otras empresas de todo el mundo a impulsar mejoras de seguridad observables y medibles, no sólo dentro de sus propias redes y sistemas, sino también en todo el ecosistema más amplio.

Por ejemplo, aunque el distintivo de los esfuerzos de este año para combatir las redes de bots es la seguridad de los dispositivos de IoT, basada en la urgente necesidad de una línea de base ampliamente aceptada, no todas las redes de bots significativas tienen como objetivo los dispositivos conectados; de hecho, algunas de las redes de bots más destructivas del mundo no tienen como objetivo los dispositivos conectados en absoluto. Por lo tanto, aunque está claro que el futuro de las redes de bots está estrechamente relacionado con el futuro de la seguridad del IoT, y el CSDE seguirá liderando este frente, también exploraremos otras formas en que las redes de bots y otras amenazas distribuidas pueden reducirse drásticamente a través del liderazgo de nuestros miembros. Al reconocer la naturaleza compleja y estratificada de la amenaza de las redes de bots, las empresas de la CSDE se enfrentarán a estas amenazas en múltiples frentes.

De forma más inmediata, nuestros próximos pasos en los próximos meses son comprometernos con un amplio espectro de partes interesadas nacionales e internacionales del ecosistema de Internet y las comunicaciones que están bien posicionadas tanto para promover las prácticas recomendadas como para fomentar un compromiso constructivo. La responsabilidad compartida que asumen estas diversas partes interesadas es la clave para asegurar el futuro de nuestra economía digital.

7 / Organizaciones colaboradoras

Sobre el CSDE

El Consejo para la Seguridad de la Economía Digital (CSDE) reúne a empresas de todo el sector de las tecnologías de la información y la comunicación (TIC) para combatir las ciberamenazas cada vez más sofisticadas y emergentes mediante acciones de colaboración. Entre los socios fundadores figuran Akamai, AT&T, CA Technologies, CenturyLink, Cisco, Ericsson, IBM, Intel, NTTOracle, Samsung, SAP,Telefónicay Verizon. La CSDE está coordinada por USTelecom y la Consumer Technology Association (CTA).

Acerca de USTelecom

USTelecom es la principal asociación comercial que representa a los proveedores de servicios y al sector de las telecomunicaciones. Su variada base de miembros abarca desde grandes corporaciones de comunicaciones que cotizan en bolsa hasta pequeñas empresas y cooperativas, todas ellas proveedoras de servicios avanzados de comunicaciones tanto en mercados urbanos como rurales.

Acerca de la Asociación de Consumidores de Tecnología

La Consumer Technology Association (CTA)™ es la asociación comercial que representa al sector de la tecnología de consumo de Estados Unidos, con un valor de 377.000 millones de dólares, que mantiene más de 15 millones de puestos de trabajo en el país. Más de 2.200 empresas -el 80% son pequeñas empresas y startups; otras se encuentran entre las marcas más conocidas del mundo- disfrutan de la
Los beneficios de la afiliación a la CTA incluyen la defensa de políticas, la investigación de mercados, la educación técnica, la promoción de la industria, el desarrollo de normas y el fomento de las relaciones comerciales y estratégicas. La CTA también es propietaria y productora de CES®, el lugar de encuentro mundial para todos los que prosperan en el negocio de las tecnologías de consumo. Los beneficios de CES se reinvierten en los servicios industriales de CTA.

08 / Notas finales

1 Instituto Nacional de Normas y Tecnología, NISTIR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (julio de 2019), https://csrc.nist.gov/publications/ detail/nistir/8259/draft.

2 Los actores maliciosos también se denominan comúnmente hackers, aunque no todos los hackers son maliciosos. En general, este documento utiliza los términos indistintamente, asumiendo que el contexto indicará si el individuo al que se hace referencia es un actor malicioso o no. También hay que tener en cuenta que este documento se centra en los actores maliciosos, por lo que, en general, "hacker" en este documento es un actor malicioso.

3 No es práctico establecer los requisitos de todos los tipos de software del ecosistema IoT simultáneamente. Los dispositivos IoT, las empresas y la infraestructura tienen requisitos específicos. Esta sección se aplica a las áreas no cubiertas en otras partes de la Guía

4 Los sistemas de calefacción, ventilación y aire acondicionado (HVAC) están conectados para ofrecer funciones inteligentes y acceso remoto por parte del ocupante. Los sistemas de seguridad incluyen cámaras, cerraduras y sistemas de alarma gestionados a través de Internet. Los sistemas de entretenimiento se benefician de controles centrales para poder gestionar con facilidad complejas configuraciones de audio y vídeo. Hay una enorme diversidad de fabricantes y sistemas en estas categorías. Estos sistemas pueden ser instalados por los propietarios de viviendas y negocios, o por profesionales: integradores, contratistas de alarmas y

otros. Lo ideal es que todo sistema de dispositivos que entre en un entorno doméstico, de oficina, de venta al por menor, médico o industrial esté protegido por las mejores prácticas en todo el ciclo de vida del dispositivo, incluidas la instalación y la configuración del dispositivo que logre la "mejor seguridad disponible" del producto fabricado.

5 Consumer Technology Association, *The Connected Home Security System*, https://www.cta.tech/Membership/Member-Groups/Smart-Home- Division/Device-Security-Checklist.aspx (última visita el 10 de octubre de 2018).

6 Como principales propietarias y usuarias de dispositivos y sistemas en red, incluido un número cada vez mayor de sistemas de dispositivos IoT, las empresas de todo tipo (gubernamentales, del sector privado, académicas y sin ánimo de lucro) tienen un papel fundamental que desempeñar en la seguridad del ecosistema digital.
Aunque las empresas suelen ser objeto de ataques automatizados y distribuidos, así como de intentos de exfiltración de datos, sus vastos sistemas también pueden ser
secuestrados para aumentar el impacto de los ataques DDoS y otros ataques distribuidos en otros. Por lo tanto, las empresas se encuentran entre las partes interesadas que comparten la responsabilidad de asegurar adecuadamente sus redes y sistemas con el fin de ayudar a asegurar el ecosistema digital más amplio. Los millones de empresas del sector privado y de la administración pública de todo el mundo difieren considerablemente en cuanto a sus conocimientos y habilidades técnicas, acceso a los recursos e incentivos para adoptar prácticas de seguridad básicas. Las empresas de todos los tamaños pueden tomar sus propias medidas proactivas para mitigar el riesgo del ecosistema. Dichas medidas pueden ayudar a las empresas a proteger los datos sensibles y la propiedad intelectual en sus redes, al tiempo que ayudan a proteger el ecosistema en general al reducir la superficie de ataque de las redes de bots. Los proveedores y suministradores que han elaborado esta Guía son grandes empresas mundiales, y también ofrecemos soluciones de alta gama para proteger las redes empresariales y mitigar los ataques DDoS y otras amenazas automatizadas y distribuidas. El lado de la "oferta" de este mercado es robusto y está en crecimiento, y un mayor desarrollo del lado de la "demanda" de este mercado en términos de empresas de todos los tamaños que solicitan y negocian por estos
aportará más innovación, sofisticación y eficiencia de costes en estos servicios.

8 Irving Wladawsky-Berger, *GDP Doesn't Work in a Digital Economy*, The Wall Street Journal (3 de noviembre de 2017) https://blogs.wsj.com/cio/2017/11/03/ gdp-doesnt-work-in-a-digital-economy.

9 Paul Tentena, *Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025*, East African Business Week (30 de mayo de 2018), https://www. busiweek.com/artificial-intelligence-to-double-digital-economy-to-23- trillion-by-2025/.

10 *Véase, por ejemplo*, Catalin Cimpanu, *Sly Malware Author Hides Cryptomining Botnet Behind* Ever-shifting *Proxy Service*, ZDNet (13 de septiembre de 2018), https:// www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet- behind-ever-shifting-proxy-service ("[B]otnets centradas en operaciones de minería de criptomonedas han sido una de las formas más activas de infecciones de malware en 2018.")

11 Sam Thielman y Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, The Guardian, (21 de octubre de 2016), https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn- internet-denial-service.

12 Michael Newberg, *Hasta 48 millones de cuentas de Twitter no son personas, dice un estudio,* CNBC (10 de marzo de 2017), https://www. cnbc. com/2017/03/10/casi-48-millones-de-cuentas-de-twitter-podrían-ser-robots-dice-un-estudio.html.

13 JP Buntinx, *Top 4 Largest Botnets to Date*, Null TX (7 de enero de 2017), https://themerkle.com/top-4-largest-botnets-to-date/

14 Daniel Newman, *Las 8 principales tendencias del IoT para 2018*, Forbes (19 de diciembre de 2017), https://www.forbes.com/sites/danielnewman/2017/12 /19/ the-top-8-iot-trends-for-2018/#48d7f78e67f72523096867f7 (cita HIS Markit IoT Trend Watch 2018, *disponible en* https://ihsmarkit.com/industry/ telecommunications.html); *véase también* Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (7 de febrero de 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02- 07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31- percent-from-2016.

15 Jan-Peter Kleinhans, *Internet of Insecure Things: ¿Puede la evaluación de la seguridad curar los fallos del mercado?* Stiftung Neue Verantwortung (diciembre de 2017), https://www.stiftung-nv.de/sites/default/files/internet_of_ insecure_things.pdf.

16 Bill Connor, *Ransomware-As-A-Service: ¿La próxima gran amenaza cibernética?* , Forbes (17 de marzo de 2017), https://www.forbes.com/sites/ forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great- cyber-threat/#14a38e5b4123.

17 Andy Greenberg, *La Casa Blanca culpa a Rusia de NoPetya, el 'ciberataque más costoso de la historia'*, Wired (15 de febrero de 2018) https://www. wired.com/story/white-house-russia-notpetya-attribution/; Damien Sharkov, *Russia Accused of 1.2 mil millones del ciberataque NoPetya*, Newsweek (15 de febrero de 2018) https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867; CBS News, *¿Qué podemos aprender del ciberataque más devastador de la historia?* (22 de agosto de 2018), https://www.cbsnews. com/news/ lessons-to-learn-from-devastating-notpetya-cyberattack-

18 Alex Zaharov-Reutt, *Cyber Crime, Data Breaches to Cost Businesses US $8 Trillion Thru 2022*, ITWire (25 de abril de 2017), https://www.itwire. com/ security/77782-$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html.

19 Sec. de Com., Consejo de Fiabilidad e Interoperabilidad IV Grupo de Trabajo 4, *Informe final sobre gestión de riesgos de ciberseguridad y mejores prácticas* 4 (mar. 2015), *disponible en* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (reconoce "las ventajas de un enfoque no normativo frente a un régimen de cumplimiento prescriptivo y estático").

20 Instituto Nacional de Normas y Tecnología, NISTIR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (julio de 2019), https://csrc.nist.gov/publications/ detail/nistir/8259/draft.

21 Daniel Palmer, *Researchers Discover Huge Crypto Scam Botnet on Twitter*, Coindesk (7 de agosto de 2018), https://www.coindesk.com/researchers- discover-huge-crypto-scam-botnet-on-twitter ("Los investigadores han descubierto una enorme red de bots que imitan cuentas legítimas en Twitter para difundir una estafa de "regalo" de criptomonedas").

22 Charles DeBeck, Joshua Chung y Dave McMillen, I *Can't Believe Mirais: Tracking the Infamous IoT Malware,* SecurityIntelligence (18 de julio de2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

23 Charles DeBeck, Joshua Chung y Dave McMillen, I *Can't Believe Mirais: Tracking the Infamous IoT Malware,* SecurityIntelligence (18 de julio de2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

24 Mark Mayne, *New Mirai variant targets enterprises with 11 new exploits*, SC Media (19 de marzo de 2019), https://www.scmagazineuk.com/new-mirai-variant- targets-enterprises-11-new-exploits/article/1579535.

25 *Véase* SentinelOne, *Mirai Botnet* Descendants *Will Lead to Even* Bigger *Internet Outages*, CSO (22 de diciembre de 2016), https://www.csoonline.com/ article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet- outages.html.

26 Larry Cashdollar, *Último Echobot: 26 vectores de infección*, Akamai (13 de junio de 2019, 11:17 AM), https://blogs.akamai.com/sitr/2019/06/latest-echobot-26- infection-vectors.html.

27 Charles DeBeck, Joshua Chung y Dave McMillen, I *Can't Believe Mirais: Tracking the Infamous IoT Malware,* SecurityIntelligence (18 de julio de2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

28 *2019 Threat Report*, CenturyLink 5-7, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (última visita el 8 de octubre de 2019).

29 *2019 Threat Report*, CenturyLink 5-7, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (última visita el 8 de octubre de 2019).

30 *2019 Threat Report*, CenturyLink 16, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (última visita el 8 de octubre de 2019).

31 Charles DeBeck, Joshua Chung y Dave McMillen, I *Can't Believe Mirais: Tracking the Infamous IoT Malware,* SecurityIntelligence (18 de julio de2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/.

32 Warick Ashford, *Phishing top security threat to business*, Computerweekly.com (12 de agosto de 2019, 16:00), https://www.computerweekly.com/news/252468231/Phishing-top-security-threat-to-business.

33 *Incident Classification Patterns and Subsets*, Verizon, https://enterprise. verizon.com/resources/reports/dbir/2019/incident-classification-patterns- subsets/ (última visita el 8 de octubre de 2019).

34 *A New Phase of TheMoon*, CenturyLink (31 de enero de 2019), https://blog. centurylink.com/a-new-phase-of-themoon/.

35 Sergiu Gatlan, *Mirai Botnet Variants Targeting New Processors and Architectures*, BleepingComputer, (9 de abril de 2019, 8:40 AM), https://www. bleepingcomputer.com/news/security/mirai-botnet-variants-targeting-new- processors-and-architectures/.

36 Sean Gallagher, New variants of Mirai botnet detected, targeting more IoT devices, Ars Technica (9 de abril de 2019, 1:49 PM), https://arstechnica.com/ information-technology/2019/04/new-variants-of-mirai-botnet-detected-targeting-more-iot-devices/.

37 Charles DeBeck, Joshua Chung y Dave McMillen, I *Can't Believe Mirais: Tracking the Infamous IoT Malware,* SecurityIntelligence (18 de julio de2019), https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the- infamous-iot-malware-2/.

38 Derek Manky, *The Evolving Threat Landscape - Swarmbots,* Hivenets*, Automation in* Malware, CSO (29 de agosto de 2018, 9:00 AM), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots- hivenets-automation-in-malware.html.

39 Derek Manky, *Rise of the 'Hivenet': Botnets That Think for Themselves*, DarkReading (16 de febrero de 2018, 10:30 AM), https://www. darkreading.com/ vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/ a/d-id/1331062.

40 Derek Manky, *Rise of the 'Hivenet': Botnets That Think for Themselves*, DarkReading (16 de febrero de 2018, 10:30 AM), https://www. darkreading.com/ vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/ a/d-id/1331062.

41 Derek Manky, *The Evolving Threat Landscape - Swarmbots,* Hivenets*, Automation in* Malware, CSO (29 de agosto de 2018, 9:00 AM), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots- hivenets-automation-in-malware.html.

42 Derek Manky, *The Evolving Threat Landscape - Swarmbots,* Hivenets*, Automation in* Malware, CSO (29 de agosto de 2018, 9:00 AM), https://www. csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots- hivenets-automation-in-malware.html.

43 Colin Grady, William Largent & Jaeson Schultz, Emotet *está de vueltadespués de un descansode verano,* Cisco Talos Intelligence Group (17 de septiembrede2019), https://blogs. cisco.com/security/talos/emotet-is-back-after-a-summer-break.

44 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (19 de septiembre de 2019, 2:45 PM), https:// arstechnica.com/information-technology/2019/09/worlds-most-destructive- botnet-returns-with-stolen-passwords-and-email-in-tow/.

45 *Analyzing the botnet infrastructure and threat actors behind TrickBot*, NTT (28 de marzo de 2019), https://technical.nttsecurity.com/post/102fhgo/ analyzing-the-botnet-infrastructure-and-threat-actors-behind-trickbot.

46 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (19 de septiembre de 2019, 2:45 PM), https:// arstechnica.com/information-technology/2019/09/worlds-most-destructive- botnet-returns-with-stolen-passwords-and-email-in-tow/.

47 Colin Grady, William Largent & Jaeson Schultz, *Emotet vuelve tras un parón veraniego,* Cisco Talos Intelligence Group (17 de septiembre de 2019), https://blog. talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html.

48 Colin Grady, William Largent & Jaeson Schultz, *Emotet vuelvetras un parón veraniego,* Cisco Talos Intelligence Group (17 de septiembre de 2019), https://blog. talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html.

49 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (19 de septiembre de 2019, 2:45 PM), https://arstechnica.com/information-technology/2019/09/worlds-most- destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/.

50 Catalin Cimpanu, *Emotet, today's most dangerous botnet, comes back* to life, ZDNet (16 de septiembre de 2019), https://www.zdnet.com/article/emotet- todays-most-dangerous-botnet-comes-back-to-life/.

51 Catalin Cimpanu, *Necurs and Gamut Botnets Account for 97% of the Internet's Spam Emails*, BleepingComputer (Mar. 12, 2018, 5:20 AM), https://www.bleepingcomputer.com/news/security/necurs-and-gamut- botnets-account-for-97-percent-of-the-internets-spam-emails/.

52 *Correo electrónico: Haga clic con precaución*, Cisco 31, https://www.cisco.com/c/dam/ es/us/products/collateral/security/email-security/email-threat-report.pdf (última visita el 8 de octubre de 2019)

53 *2019 Threat Report*, CenturyLink 19, https://www.centurylink.com/ asset/business/enterprise/report/2019-threat-research-report.pdf (última visita el 8 de octubre de 2019).

54 Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CyberScoop (27 de octubre de 2016), https://www.cyberscoop.com/mirai- botnet-for-sale-ddos-dark-web.

55 Derek Manky, *The Evolving Threat Landscape - Swarmbots, Hivenets, Automation in Malware*, CSO (29 de agosto de 2018, 9:00 AM), https:// www.csoonline.com/article/3301148/the-evolving-threat-landscape- swarmbots-hivenets-automation-in-malware.html.

56 Catalin Cimpanu, *Liberian ISP suits rival for hiring hacker to attack its network*, ZDNet (14 de enero de 2019), https://www.zdnet.com/article/liberian- isp-sues-rival-for-hiring-hacker-to-attack-its-network.

57 Catalin Cimpanu, *Liberian ISP suits rival for hiring hacker to attack its network*, ZDNet (14 de enero de 2019), https://www.zdnet.com/article/liberian- isp-sues-rival-for-hiring-hacker-to-attack-its-network.

58 Catalin Cimpanu, *Liberian ISP suits rival for hiring hacker to attack its network*, ZDNet (14 de enero de 2019), https://www.zdnet.com/article/liberian- isp-sues-rival-for-hiring-hacker-to-attack-its-network.

59 Curtis Franklin Jr., *New Botnet Shows Evolution of Tech and Criminal Culture*, DarkReading (4 de febrero de 2019, 18:30), https://www.darkreading. com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal- culture/d-id/1333792.

60 Curtis Franklin Jr., *New Botnet Shows Evolution of Tech and Criminal Culture*, DarkReading (4 de febrero de 2019, 18:30), https://www.darkreading. com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal- culture/d-id/1333792.

61 Akamai, *Retail Attacks and API Traffic,* State of the Internet Security 5, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (última visita el 8 de octubre de 2019)

62 Akamai, *Ataques a comercios y tráfico API*, Estado de la seguridad en Internet 5, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (última visita el 8 de octubre de 2019).

63 Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 18, https://www.akamai.com/us/en/multimedia/documents/state-of- the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic- report-2019.pdf (última visita el 8 de octubre de 2019).

64

Jay Cole, *Bots try to break the internet, and other trends for 2019*, TechRadar (21 de febrero de 2019), https://www. techradar.com/news/bots-try-to-break-the-internet-and-other-trends-for-2019.

65 Akamai, *DDoS and Application Attacks*, State of the Internet Security 17, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf (última visita el 8 de octubre de 2019).

66 *The Rise of "Bulletproof" Residential Networks*, KrebsonSecurity (19 de agosto de 2019), https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof- residential-networks.

67 Akamai, *DDoS and Application Attacks*, State of the Internet Security 18, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf (última visita el 8 de octubre de 2019).

68 Charlie Osborne, *New Mirai botnet lurks in the Tor network to stay under the radar*, ZDNet (1 de agosto de 2019), https://www.zdnet. com/article/new-mirai- botnet-lurks-in-the-tor-network-to-stay-under-the-radar.

69 Tara Seals, *Necurs Botnet Evolves to Hide in the Shadows, with New Payloads*, Threatpost (1 de marzo de 2019, 10:41 AM), https://threatpost.com/necurs- botnet-hide-payloads/142334.

70 Casting Light On The Necurs Shadow, CenturyLink (28 de febrero de 2019), https://blog.centurylink.com/casting-light-on-the-necurs-shadow.

71 *Casting Light On The Necurs Shadow*, CenturyLink (28 de febrero de 2019), https://blog.centurylink.com/casting-light-on-the-necurs-shadow.

72 *Véase* Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 5, https://www.akamai.com/us/en/multimedia/documents/state- of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic- report-2019.pdf (última visita el 8 de octubre de 2019).

73 *The Rise of "Bulletproof" Residential Networks*, Krebs on Security (19 de agosto de 2019), https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks.

74 Robin Kurzer, *Oracle descubre otra gran operación de fraude que afecta a los usuarios de Android y a los* anunciantes *móviles*, Marketing Land (20 de febrero de 2019, 7:00 AM), https://marketingland.com/oracle-discovers-another-major-fraud- operation-affecting-android-users-and-mobile-advertisers-257322.

75 Conor Reynolds, *Ataques de botnet: From DDoS to Hivenets and Sextoration*, CBR (29 de agosto de 2019), https://www. cbronline.com/feature/botnet-attacks-changing-theatre.

76 Robin Kurzer, *Oracle descubre otra gran operación de fraude que afecta a los usuarios de Android y a los* anunciantes *móviles*, Marketing Land (20 de febrero de 2019, 7:00 AM), https://marketingland.com/oracle-discovers-another-major-fraud- operation-affecting-android-users-and-mobile-advertisers-257322.

77 Jeff Stone, *De los ataques DDoS al fraude publicitario: Los bots más inteligentes están copiando el comportamiento humano*, CyberScoop (10 de diciembre de 2018), https://www. cyberscoop.com/ smart-botnet-human-behavior-ddos-ad-fraud-methbot.

78 Jeff Stone, *De los ataques DDoS al fraude publicitario: Los bots más inteligentes están copiando el comportamiento humano*, CyberScoop (10 de diciembre de 2018), https://www. cyberscoop.com/ smart-botnet-human-behavior-ddos-ad-fraud-methbot.

79 *Véase* Telefónica, Etisalat y Singtel, *detección de botnets de Twitter en eventos deportivos,* Trend Report, https://www. elevenpaths.com/wp-content/ uploads/2018/12/twitter-botnets-detection-in-sports-events.pdf (última visita el 8 de octubre de 2019).

80 Christine Fisher, *Twitter prohíbe miles de cuentas respaldadas por el Estado que difunden información errónea*, Engadget (20 de septiembre de 2019), https://www.engadget. com/2019/09/20/twitter-bans-state-backed-misinformation.

81 Ben Collins & Shoshana Wodinsky, *Twitter retira la red de bots que impulsó puntos de conversación* pro-saudíes *sobre el periodista desaparecido, NBCNews* (18 de octubre de 2018, 6:39 PM), https://www.nbcnews. com/tech/tech-news/exclusive- twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871.

82 Jessica Lyons Hardcastle, *Cyber Threat Alliance Reports 459% Spike in Cryptomining Malware*, SDxCentral (21 de septiembre de 2018, 1:18 PM), https://www. sdxcentral.com/articles/news/cyber-threat-alliance-459-spike-cryptomining- malware/2018/09.

83 Catalin Cimpanu, Crypto-mining mal*ware* saw new-life-over-the-summer as *Monero value tripled*, ZDNet (18 de septiembre de 2019), https://www.zdnet. com/ article/crypto-mining-malware-saw-new-life-over-the-summer-as-monero- value-tripled.

84 Michael Nadeau, *¿Qué es el criptojacking? How to prevent, detect, and recover from it*, CSO (2 de agosto de 2019, 3:00 AM), https://www. csoonline.com/ article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-it.html.

85 *The Illicit Cryptocurrency Mining Threat*, Cyber Threat Alliance 4, https:// www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit- CryptoMining-Whitepaper.pdf (última visita el 8 de octubre de 2019).

86 *The Illicit Cryptocurrency Mining Threat*, Cyber Threat Alliance 15, https://www. cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit- CryptoMining-Whitepaper.pdf (última visita el 8 de octubre de 2019).

87 Catalin Cimpanu, *Two crypto-mining groups are fighting a turd war on over* unsecured *Linux servers*, ZDNet (10 de mayo de 2019), https://www.zdnet. com/ article/two-crypto-mining-groups-are-fighting-a-turf-war-over-unsecured-linux- servers/.

88 Lucian Constantin, *Secrets of latest Smominru botnet* warrant *revealed in new attack*, CSO (18 de septiembre de 2019, 6:00 AM), https://www. csoonline.com/ article/3439400/secrets-of-latest-smominru-botnet-variant-revealed-in-new- attack.html.

89 Catalin Cimpanu, *Two botnets are fighting over control of thousands of* unsecured *Android device*, ZDNet (2 de noviembre de 2018), https://www.zdnet. com/ article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured- android-devices.

90 Tara Seals, *Mylobot Botnet Emerges with Rare Level of Complexity*, Threatpost (20 de junio de 2018, 1:12 PM), https://threatpost.com/mylobot-botnet- emerges-with-rare-level-of-complexity/132967.

91 Catalin Cimpanu, *A* mysterious grey-hat *is patching people's outdated MikroTik routers*, ZDNet (12 de octubre de 2018), https://www.zdnet. com/article/a- mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers.

92 Mark Samuels, *Vigilante* White-Hate H*acker Boosts IoT Device Security*, SecurityIntelligence (20 de abril de 2017, 1:31 PM), https://securityintelligence.com/ news/vigilante-white-hat-hacker-boosts-iot-device-security.

93 RFC 2460 Network Working Group, *Internet Protocol, Version 6 (IPv6) Specification*, IEFT (dic. 1998), https://tools.ietf.org/html/rfc2460.

94 Marek Šimon & Ladislav Huraj, A *Study of DDoS ReflectionAttackon Internet of Things in IPv4/IPv6 Networks,* SpringerLink, https://link.springer. com/chapter/10.1007/978-3-030-19807-7_12 (última visita el 10 de octubre de 2019).

95 Erik Nygren, *Seis años desde el lanzamiento del IPv6 mundial: Entrando en las* fases *mayoritarias*, Akamai (6 de junio de 2018, 12:00 PM), https://blogs.akamai. com/2018/06/six-years-since-world-ipv6-launch-entering-the-majority- phases.html.

96 Akamai, *Ataques a comercios y tráfico API*, Estado de la seguridad en Internet 4, https://www.akamai. com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf (última visita el 10 de octubre de 2019).

97 *[illegible]evices under attack within minute of turn-up*, RCR Wireless (6 de agosto de 2019), https://www.rcrwireless.com/20190806/ internet-of-things/netscout-iot-devices-under-attack-within-minutes-of- turn-up.

98 Martin Zeiser & Aleksandar Nikolich, IPv6 *unmaking via UPnP,* Cisco (18 de marzo de 2019), https://blog.talosintelligence.com/2019/03/ipv6-unmasking- via-upnp.html.

99 Rene Paap, *IPv6 And the Growing DDoS Danger*, DarkReading (2 de noviembre de 2015, 10:30 AM), https://www. darkreading.com/attacks-breaches/ipv6-and- the-growing-ddos-danger/a/d-id/1322942.

100 Kieren McCarthy, *It's begun: 'First' IPv6 denial-of-service attacks puts IT bods on notice,* The Register (Mar. 3, 2018, 9:30 AM), https://www.theregister. co.uk/2018/03/03/ipv6_ddos/.

101 Mark Mayne, *'First true' nativeIPv6 DDoS attack spotted in wild*, SCMedia (28 de febrero de 2018), https://www.scmagazineuk.com/first-true-native- ipv6-ddos-attack-spotted-wild/article/1473177.

102 Departamento de Comercio y Departamentode Seguridad Nacional de los Estados Unidos, A *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats,* NIST (22 de mayo de 2018), *disponible en* https://csrc.nist.gov/publications/detail/ white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to- the-president/draft; Commc'n Sec, Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), disponible *en* https://transition.fcc.gov/pshs/ advisory/csric4/CSRIC_IV_WG4_Final_ Report_031815.pdf; ENISA, Botnet Measurement, Detection, Disinfection and Defence (Mar. 7, 2011), https:// www.enisa.europa.eu/publications/botnets-measurement-detection- disinfection-and-defence; Int'l Telecomm.Union, ITU Botnet Mitigation Toolkit (Jan. 2008), https://www.itu.int/ITU-D/cyb/cybersecurity/projects/ botnet.html.

103 Departamento de Comercio y Departamentode Seguridad Nacional de Estados Unidos, A *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (*22 de *mayo* de 2018), *disponible en* https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the- president/draft

104 Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 7-9 (septiembre de 2017) (donde se analizan herramientas y técnicas para la protección contra DDoS, incluido el filtrado de entrada/salida; protección contra DDoS dentro y fuera de las instalaciones), *disponible en* https://doi. org/10.6028/NIST.IR.8192; *véase también*, Ctr. for Democracy and Tech, Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats 2 (12 de febrero de 2018) (de acuerdo con el proyecto de informe de la NTIA de que "las técnicas comunes para la mitigación de botnets incluyen el filtrado de entrada y salida, el redireccionamiento y la conformación del tráfico de Internet, y el aislamiento de dispositivos u otras entidades"), *disponible en* https://cdt.org/files/2018/02/CDT-NTIA-Botnet- Comments-Feb-2018.pdf; Commc'n Sec, Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), disponible en https://transition.fcc.gov/pshs/ advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

105 *Véase, por ejemplo*, Estados Unidos, DHS Automated Indicator Sharing (AIS) System, https://www.us-cert.gov/ais (consultado por última vez el 17 de octubre de 2018); Reino Unido, Cyber Security Information Sharing Partnership (CiSP), https://www.ncsc.gov. uk/section/keep-up-to-date/cisp (consultado por última vez el 17 de octubre. 17 de octubre de 2018); Japón, Cyber Clean Center, https://www. telecom-isac.jp/ccc/en_index.html (último acceso el 17 de octubre de 2018); Nueva Zelanda, CORTEX, https://www.gcsb.govt.nz/our-work/ information-assurance/cortex-faqs (último acceso el 17 de octubre de 2018).

106 *Véase* David Strom, *¿Qué es el malware polimórfico y por qué debería importarme?* (16 de octubre de 2015), https://securityintelligence.com/what-is- polymorphic-malware-and-why-should-i-care.

107 Verizon, 2012 *Data Breach Investigations Report* 71 (2012), https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

108 *Véase* Stephen Sladaritz, *About Heuristics*, SANS Institute 4 (23 de marzo de 2002), *disponible en* https://www.sans.org/reading-room/whitepapers/ malicious/about-heuristics-141 (en el que se comparan los dos tipos diferentes de análisis heurístico); *véase también* John Aycock, Computer Viruses and Malware 74 (2006) (en el que se explica que la única diferencia entre la heurística estática y la dinámica es "la forma en que se recogen los datos" y que, por lo demás, los datos son idénticos).

109 *Véase, por ejemplo*, Cisco, *Cisco Cognitive Threat Analytics v1* (febrero de 2016), https:// dcloud-cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1

110 Nat'l Inst. of Standards and Tech., *Advanced DDoS Mitigation Techniques* (18 de octubre de 2017) ("Durante más de una década la industria ha desarrollado especificaciones de técnicas y guías de despliegue para técnicas de filtrado a nivel de IP para bloquear el tráfico de red con direcciones de origen falsas"), *disponible en* https://www.nist.gov/programs-projects/advanced-ddos- mitigation-techniques.

111 Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employed IP Source Address Spoofing*, Internet Engineering Task Force (IETF) Network Working Group (mayo de 2000), *disponible en* https://tools.ietf.org/html/bcp38; F. Baker & P. Savola, Ingress Filtering for Multihomed Networks, Internet Engineering Task Force (IETF) Network Working Group (marzode 2004), *disponible en* https://tools.ietf.org/html/bcp84.

112 Id.

113 *Véase, por* ejemplo, Chris Benton, *Egress Filtering FAQ*, SANS Institute (19 de abril de 2006), *disponible en* https://www.sans.org/reading-room/ whitepapers/firewalls/egress-filtering-faq-1059

114 *Véase* Cisco, *Access Control Lists* (última actualización del 17 de julio de 2018), https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls.html.

115 *Véase* Cisco, *Policing and Shaping Overview* (última actualización: 23 de noviembre de 2017), https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-oview.html.

116 *Véase*, *por* ejemplo, Guy Bruneau, *DNS Sinkhole*, SANS Institute (7 de agosto de 2010), https://isc.sans.edu/forums/diary/DNS+Sinkhole+ISO+Version+20/21153/.

117 *Véase* Cisco, *Implementing BGP Flowspec* (última actualización: 31 de enero de 2018), https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/ asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html.

118 *Véase* Georgia Tech Researchers, *DNS Changer Remediation Study, Presentation to M3AAWG 27th General Meeting, San Francisco, CA* (19 de febrero de 2013), *disponible en* https://www.m3aawg.org/news/independent- georgia-tech-study-reveals-best-ways-to-tell-customers-"you're-botted" (consultado por última vez el 17 de octubre de 2018); *véase también* Commc'n Sector Coordinating Consejo, Botnet Whitepaper 24-25 (17 de julio de 2017) (donde se enumeran las múltiples formas en que los proveedores de infraestructuras pueden notificar a los usuarios, como el correo electrónico, la llamada telefónica, el correo postal, el mensaje de texto, la notificación a través del navegador web, el jardín amurallado y otros métodos como las redes sociales), *disponible en* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

119 *Ver* Ctr. for Democracy and Tech, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares

(14 de noviembre de 2011) (en el que se expresa la preocupación de la industria de "cortar o interferir de otro modo en la conexión a Internet de un cliente" para obligar a la reparación de la botnet), *disponible en* https://www.nist.gov/sites/default/files/ documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf; Elec. Frontier Found., Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares 5 (14 de noviembre de 2011) (explicando cómo las partes no infectadas podrían ver afectado su acceso a Internet por la cuarentena), *disponible en* https://www.nist.gov/sites/default/files/documents/itl/AT-Ts-Comments-to- BotNet-FRN-11-14-11.pdf.

120 *Véase* Commc'n Sector Coordinating Council, Botnet Whitepaper 21 (17 de julio de 2017), ("Ninguna técnica es más eficaz que las acciones policiales que conducen a la detención de los autores. Esta es la única solución que aborda la causa raíz del problema, y no solo un síntoma... [E]xperimentar una El desmantelamiento de las redes de bots requiere un importante análisis forense previo y una cuidadosa coordinación entre muchas partes interesadas, a menudo a través de las fronteras internacionales.... La mayoría de las redes de bots son de carácter internacional, lo que exige una cooperación entre países que requiere muchos recursos y tiempo"), *disponible en* https://docs. wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

121 *Véase* Robert Wainright y Frank J. Cilluffo, Responding to Cyber Crime at Scale: A Case Study, Europol & the George Washington Univ. Ctr.for Cyber and Homeland Sec.(Mar. 2017), *disponible en* https://cchs.gwu. edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20 at%20Scale%20 FINAL.pdf.

122 *Véase* SAFECode, *Fundamental Practices for Secure Software Development* (Mar. 2018), https://safecode.org/wp-content/ uploads/2018/03/SAFECode_Fundamental_Practices_ for_Secure_ Software_Development_March_2018.pdf.

123 Arora et al., *An Empirical Analysis of Software Vendors' Patching Behavior: Impact of Vulnerability Disclosure*, Carnegie Mellon University (enero de 2006) (analiza los incentivos de los vendedores más grandes en relación con otros vendedores), *disponible en* https://www. heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

124 *Véase* SAFECode, Principles for Software Assurance Assessment (2015), *disponible en* https://safecode.org/wp-content/uploads/2015/11/SAFECode_ Principles_for_Software_Assurance_Assessment.pdf.

125 Instituto Nacional de Normas y Tecnología, *NTIA Software Component Transparency* (21 de octubre de 2019), https://www.ntia.doc.gov/SoftwareTransparency

126 Council to Secure the Digital Economy, *The C2 Consensus on IoT Device Baseline Capabilities* (2019), https://securingdigitaleconomy.org/ wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

127 La planificación temprana de los requisitos y, en última instancia, la certificación son esenciales para este proceso. Por ejemplo, la CTIA gestiona un programa de certificación para dispositivos IoT, que establece los requisitos del sector para la seguridad de los dispositivos en las redes inalámbricas y ofrece un programa de certificación. Los detalles del programa, incluidos los requisitos y la forma de certificar un dispositivo, pueden encontrarse aquí: https://www. ctia.org/about-ctia/programs/certification-resources.

128 Microsoft, *desarrollo de la seguridad?* , https:// www.microsoft.com/en-us/sdl/default.aspx (consultado por última vez el 19 de octubre de 2018).

129 *Véase* BSIMM, https://bsimm.com (consultado por última vez el 6 de noviembre de 2018).

130 Para más normas internacionales, *véase el* Instituto Nacional de Normas y Tecnología, *Cryptographic Module Validation Program*, https://csrc.nist.gov/ projects/cryptographic-module-validation-program/standards. Además, el NIST tiene un proyecto de resumen de normas internacionales: Nat'l Inst. of Standards and Tech., *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, https://csrc.nist.gov/ publications/detail/nistir/8200/draft (consultado por última vez el 10 de octubre de 2018).

131 *Id.*

132 Para un debate sobre las actualizaciones, véase Nat'l Inst. Of Standards and Tech, *Stakeholder-Drafted Documents on IoT Security*, https://www.ntia.doc.gov/ IoTSecurity (consultado por última vez el 10 de octubre de 2018).

133 *Especificación de descripción de uso del fabricante*, IETF (19 de marzo de 2019), https://datatracker.ietf.org/doc/rfc8520/.

134 *Véase OMA Device Management Overview* (20 de abril de 2018), http://www. openmobilealliance.org/wp/overviews/dm_overview.html.

135 *Véase CPE WAN Management Protocol*, Broadband Forum (Mar. 2018), https://www. broadband-forum.org/download/TR-069.pdf.

136 Bruhadeshwar Bezawada et al., *IoTSense: Behavioral Fingerprinting of IoT Devices*, Colorado State University (abril de 2018), https://arxiv.org/ pdf/1804.03852.pdf.

137 Consumer Technology Association, *The Connected Home Security System*, https://cta.tech/Membership/Member-Groups/TechHome-Division/ Device-Security-Checklist.aspx (última visita el 10 de octubre de 2018).

138 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., A *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 12-15* (22 de mayo de 2018), *disponible en* https://www. commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

139 Cybersecurity Coalition, DDoS Threat Mitigation Profile, https://www. cybersecuritycoalition.org/ddos-framework (consultado por última vez el 14 de noviembre de 2018), *y* Cybersecurity Coalition, Botnet Threat Mitigation Profile, https://www. cybersecuritycoalition.org/botnet-framework (consultado por última vez el 14 de noviembre de 2018).

140 *Véase* Sec. de Com., Consejo de Fiabilidad e Interoperabilidad II Grupo de Trabajo 8, *Informe final sobre la protección de la red ISP 16* (en el que se recomienda, *entre otras cosas,* que los usuarios "[c]onfiguren [el] ordenador para descargar automáticamente las actualizaciones críticas tanto del sistema operativo como de las aplicaciones instaladas"). (Nov. 2011), *disponible en* https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

141 Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 13 (septiembre de 2017) (cita las opiniones de los participantes en el taller NIST Enhancing Resilience of the Internet and Communications Ecosystem del 11 y 12 de julio de 2017), *disponible en* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

142 Scott Bowen, Akamai, *Defensa por diseño: How To Dampen DDoS Attacks With A Resilient Network*, Forbes (14 de septiembre de 2017) https://www.forbes. com/sites/akamai/2017/09/14/defense-by-design-how-to-dampen-dos- attacks-with-a-resilient-network/#79144da56f8a.

143 *Véase, por ejemplo,* AT&T, Distributed Denial of Service (DDoS) Defense (2014), disponible en https://www. business.att.com/content/productbrochures/ ddos_prodbrief.pdf; Verizon, DDoS Shield Solutions Brief (2016), *disponible en* http://www.verizonenterprise.com/resources/ddos_shield_solutions_brief_en_xg.pdf; CenturyLink, DDoS Mitigation (2014), disponible *en* http://www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation.pdf; Telefónica, Anti-DDoS, https://www. elevenpaths.com/technology/anti-ddos/index.html (última visita el 3 de noviembre de 2019); NTT, DDoS Protection Service, https://www.ntt.com/es/servicios/red/gin/tránsito/ddos.html (visitado por última vez el 14 de mayo de 2018).

144 *Véase* el debate *en la* Parte 5.A.2(e) (donde se explica la función de los centros de depuración para mitigar las redes de bots).

145 Instituto Nacional de Normas y Tecnología, *Digital Identity Guidelines* (junio de 2017), *disponible en* https://doi.org/10.6028/NIST.SP.800-63-3.

146 Brian Krebs, *Google: Security Keys Neutralized Employee Phishing*, Krebs on Security (23 de julio de 2018) https://krebsonsecurity.com/2018/07/ google-security-keys-neutralized-employee-phishing.

147 Véase *Soporte de Windows XP ha finalizado*, https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support (visitado por última vez el 15 de mayo de 2018).

148 Véase BSA The Software Alliance, Seizing Opportunity Through License Compliance: BSA Global Software Survey 6-7 (2016), https://globalstudy.bsa. org/2016/.

149 *Id*. en 4 (donde se habla de la "fuerte correlación" entre el malware y el software sin licencia).

150 Universidad Nacional de Singapur, *Cybersecurity Risks from Non- Genuine Software, The Link Between Pirated Software Sources and Cybercrime Attacks in Asia Pacific* 6 (1 de noviembre de 2017), https://news.microsoft. com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine- Software.pdf ("[E]n muchas partes del mundo, el uso de software pirata/falsificado/no genuino contribuye seriamente al crecimiento de los riesgos cibernéticos y es responsable de grandes daños económicos y pérdidas de productividad. También está provocando un aumento de los ataques de ciberdelincuencia y de las pérdidas correspondientes").

Para más información sobre el Consejo para la Seguridad de la Economía Digital (securingdigitaleconomy.org)

o información sobre este informe, póngase en contacto con

Robert Mayer

Vicepresidente Senior - Ciberseguridad USTelecom

rmayer@ustelecom.org

Mike Bergman

Vicepresidente - Tecnología y Normas Asociación de Tecnología del Consumidor mbergman@cta.tech


CSDE
Council to Secure the
Digital Economy