Counci to Secure the Digital

INTERNACIONAL GUÍA ANTI-BOTNET 2018

US ECOM THE BROADBAND ASSOCIATION

En colaboración con

Consumer Technology Association™

AVISO

La Guía Internacional Anti-Botnet fue desarrollada para facilitar la mitigación de las 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 estímulo a las partes interesadas en las tecnologías de la información y las comunicaciones (TIC) sobre las medidas positivas que deben aplicar para alcanzar este objetivo, según lo que consideren apropiado, en función de sus circunstancias individuales y de sus relaciones mutuas.

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 prácticas, tanto las básicas como las avanzadas, presentan un valioso marco de referencia para que las partes interesadas en las TIC identifiquen y elijan sus propias prácticas para mitigar las amenazas de los ataques automatizados y distribuidos. La Guía reconoce que las distintas partes interesadas en las TIC se enfrentan a diferentes retos, consideraciones y prioridades a la hora de aplicar medidas de seguridad.
Por lo tanto, 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 la 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 el análisis coste-beneficio 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 deberán 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

1 Resumen ejecutivo

Los miembros del Consejo para la Seguridad de la Economía Digital (CSDE) y de la Asociación de Tecnología del Consumidor (CTA)™ abarcan la totalidad del complejo ecosistema mundial de Internet y las comunicaciones, proporcionando infraestructura, software y 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 - colectivamente, la economía digital global.

Las empresas que han contribuido a esta Guía fueron de las primeras en adoptar prácticas voluntarias para proteger el ecosistema de las ciberamenazas. Mientras tanto, el sector tecnológico se ha beneficiado de las prácticas de seguridad por diseño, los servicios de seguridad gestionados y el soporte del ciclo de vida suministrado por los proveedores globales de hardware, software, dispositivos y sistemas, y servicios relacionados. Sin embargo, los desafíos abundan para los proveedores de infraestructura, los desarrolladores de software, los fabricantes de dispositivos y sistemas, los instaladores de sistemas y las empresas de todo tipo.
La Guía Internacional Anti-Botnet del CSDE, elaborada en estrecha colaboración con la CTA, se basa en las diversas perspectivas, prácticas y experiencias mundiales de estas partes interesadas para hacer frente a un desafío persistente y creciente para la economía digital mundial: las botnets y otras amenazas automatizadas y distribuidas.

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 botnets son grandes redes de ordenadores y dispositivos comprometidos y conectados a Internet que los actores maliciosos pueden comandar para cometer ataques de denegación de servicio distribuidos (DDoS), propagación de ransomware, ataques de phishing y desinformación campañas de amplificación de medios sociales no auténticos, y otros actos maliciosos. [1] Por desgracia, a medida que aumenta el número de personas, empresas y dispositivos conectados, también lo hace el potencial de estos ataques maliciosos. En la actualidad, el potencial destructivo de las redes de bots ha aumentado exponencialmente, ya que atacan y aprovechan los 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. Con esta importante y creciente superficie de ataque, no es casualidad que se prevea que el coste global de los ciberdelitos alcance los billones de dólares. Las redes de bots son el motor a escala industrial de estas pérdidas.

De hecho, la amenaza de las redes de bots es hoy más grave que en cualquier otro momento de la historia. Recientemente se han documentado enormes ataques de alto perfil contra grandes organizaciones, mientras que una corriente subterránea de ataques más pequeños y de menor perfil ha provocado un daño continuo y desconocido. Estos hechos infligen costes directos y tangibles -que ascienden a miles de millones de dólares- a la economía digital. La página web.

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

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
Los requisitos normativos prescriptivos y centrados en el cumplimiento de la normativa inhibirán la innovación en materia de seguridad que es clave para adelantarse a las sofisticadas amenazas actuales. Además, los anteriores esfuerzos normativos 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 posibilitar 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, pone de relieve otras *capacidades avanzadas* que están disponibles en la actualidad pero que están infrautilizadas. La aplicación generalizada de las prácticas de seguridad que aparecen 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. Las partes interesadas del gobierno y 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.

La Guía Internacional Anti-Botnet: 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 y sistemas de dispositivos, (4) Instalación de sistemas domésticos y de pequeñas empresas, y (5) Empresas. Para cada uno de estos componentes, la Guía expone las prácticas básicas a las que deben aspirar todas las partes interesadas, 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 los 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.* [2] 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 y sistemas de dispositivos.* [3] Un dispositivo individual conectado (o "dispositivo 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, y las aplicaciones y servicios que vienen con ellos, recomendamos prácticas de referencia y capacidades avanzadas para incluir:
   - Prácticas de desarrollo seguro por diseño
   - Raíces de la confianza
   - Gestión del ciclo de vida del producto, incluido el fin de la vida útil
   - Uso de la cadena de herramientas centrada en la seguridad

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 heredados y pirateados

Próximos pasos y aplicación. La publicación de esta Guía es sólo un primer paso. A continuación, comprometeremos estratégicamente a un amplio conjunto de partes interesadas, incluidos los gobiernos de países afines, para promover las prácticas básicas y las capacidades avanzadas de la Guía. Además, actualizaremos, publicaremos y promoveremos una nueva versión de la Guía cada año.

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. Puede representar ya el 20% del valor económico mundial.

2 Introducción

Los miembros del Consejo para la Seguridad de la Economía Digital (CSDE)[7] y de la Asociación de Tecnología de Consumo8 (CTA)™ 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. La Guía Internacional Anti-Botnet del CSDE, desarrollada en estrecha colaboración con la CTA, se basa en las diversas perspectivas internacionales de estas partes interesadas, así como en sus influyentes prácticas y acciones en el mundo real, para hacer frente a un desafío persistente y creciente para esa economía digital: las botnets y otras amenazas automatizadas y distribuidas. [9]

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. [10] Aunque el PIB por sí solo no puede reflejar 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.[11] El crecimiento de la economía digital se ve impulsado continuamente por la adopción de tecnologías nuevas y emergentes por parte de las empresas y los consumidores. [12] Gestionar con seguridad las oportunidades que ofrece 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[13] , realizar ataques de denegación de servicio[14] y difundir desinformación corrosiva de forma artificial en las redes sociales. [15] 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. [16] Hoy en día hay más sistemas vulnerables que nunca, debido simplemente a la tremenda y, por otra parte, el prometedor crecimiento de la propia economía digital, especialmente en lo que se refiere 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.[17] 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. [18] Además, ahora es posible que actores maliciosos relativamente inexpertos alquilen una potente red de bots para utilizarla en actividades nefastas a gran escala. [19]

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. [20] 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.). [21]

> **"La lucha contra las botnets requiere una colaboración transfronteriza y multidisciplinar, enfoques técnicos innovadores y el despliegue generalizado de medidas de mitigación que respeten los principios fundamentales de Internet."**
> **- LA SOCIEDAD DE INTERNET**

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. [22] 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 recogidas en esta Guía reducirá drásticamente las redes de bots y ayudará a proteger la economía digital mundial.

Metodología y próximos pasos. Las empresas que han contribuido a esta Guía han llevado a cabo una revisión exhaustiva de las prácticas y los materiales que muestran la tecnología y las herramientas que se sabe que son eficaces para combatir los ataques automatizados y distribuidos, como las redes de bots; también han investigado los informes de los gobiernos y los organismos internacionales y han consultado a expertos externos y fuentes de la industria, el mundo académico y la sociedad civil. [23] Pero para ser claros, la publicación de esta Guía es sólo un primer paso. A continuación, vamos a involucrar estratégicamente a un amplio conjunto de partes interesadas, incluidos los gobiernos
de países afines, para promover las prácticas básicas y las capacidades avanzadas de la Guía. Además, actualizaremos, publicaremos y promoveremos una nueva versión de la Guía cada año.

03 Redes de bots: Cómo hacer frente a las amenazas automatizadas y distribuidas en un ecosistema de Internet diverso

La categoría más destacada de las amenazas automatizadas y distribuidas para el ecosistema global de Internet y las comunicaciones son las redes de bots: grandes redes de ordenadores y dispositivos conectados a Internet que se comunican con servidores con 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. [24]

La amenaza de las redes de bots es hoy más grave que en cualquier otro momento de la historia. A principios de la década de 2000, los delincuentes utilizaban principalmente las redes de bots para realizar ataques rudimentarios de denegación de servicio (DoS) que inundaban y abrumaban los sitios web objetivo y las actividades de la red con tráfico de Internet artificial. Sin embargo, con el paso del tiempo, sus capacidades aumentaron. Al infectar un gran número de dispositivos con malware, los hackers descubrieron que podían realizar actividades maliciosas a una escala mucho mayor. En 2007, se descubrió que una red de bots llamada "Storm Worm" había reunido a casi 50 millones de ordenadores en sus filas, utilizándolos para cometer delitos como fraudes en las cotizaciones bursátiles y robos de identidad. En 2009, se descubrió que una red de bots enviaba la increíble cifra de 74.000 millones de correos electrónicos basura al día. [25] Y en 2011-2013, un atacante utilizó redes de bots para llevar a cabo una campaña de ataques DDoS contra bancos norteamericanos, enviando oleadas de tráfico de Internet a sus sitios web desde nodos de redes de bots de todo el mundo. [26]

En la actualidad, los delincuentes utilizan grandes redes de bots para todo tipo de ciberdelitos, desde la minería de criptomonedas hasta los ataques DDoS, como el histórico ataque de la red de bots Mirai de 2016 al proveedor de DNS Dyn. El malware de la red de bots Mirai de 2016 se propagó utilizando una lista de credenciales de inicio de sesión por defecto para acceder a casi 400.000
dispositivos de punto final, como cámaras de videovigilancia y grabadores de vídeo digital, sin que los propietarios se dieran cuenta o internalizaran ninguna de las consecuencias económicas de que sus dispositivos estuvieran infectados. [27] El ataque -que por volumen de tráfico impulsado por la red de bots fue *cuatro* veces mayor que el de los anteriores ataques contra los principales bancos- inhabilitó temporalmente el acceso de los usuarios a plataformas y servicios en línea clave, causando graves problemas a los numerosos usuarios que dependían de los servicios en línea de empresas como Airbnb, Amazon.com, BBC, CNN y Netflix, por nombrar algunas. [28]

Aunque la mayoría de las redes de bots no alcanzan la escala de Mirai[29], muchos ataques de redes de bots de menor tamaño son capaces de cerrar sitios web y servicios, difundir ransomware e impulsar la desinformación en las redes sociales. Por desgracia, las capacidades de ataque más pequeñas se han vuelto mucho más accesibles para los delincuentes que carecen de los conocimientos técnicos para construir sus propias redes de bots. Los mercados en línea que se encuentran en la web oscura permiten a los hackers principiantes comprar los kits de herramientas para diseñar redes de bots únicas que satisfagan sus necesidades individuales, lo que se denomina "Malware as a Service" (MaaS). Si el cliente criminal no quiere desarrollar o comprar una red de bots, puede alquilar una por tan sólo 0,66 céntimos de dólar al día.[30] Y el delincuente puede simplemente comprar la función -digamos, un ataque DDoS- por tan sólo 20 dólares.[31] Es un sector floreciente y

mercado innovador. Poco después de los ataques de Mirai, por ejemplo, el creador de la red de bots publicó el código fuente de Mirai en línea, y desde entonces muchos otros aspirantes a hackers han creado variantes del código original de Mirai.

Los actores maliciosos encuentran constantemente nuevos usos para las redes de bots. Por ejemplo, los hackers utilizaron redes de bots en un intento de revivir el infame ransomware WannaCry, que incapacitó a más de 200.000 sistemas informáticos en más de 150 países, obligando a bancos, hospitales, universidades y otras instituciones a cerrar o a pagar un rescate a los delincuentes. [32] El brote de WannaCry remitió cuando un investigador de seguridad se dio cuenta de que el malware estaba consultando un dominio no registrado. El registro del dominio tuvo el efecto de un "interruptor de apagado" que cerró la red de bots. [33] Los hackers han utilizado "imitadores de la red de bots Mirai" para atacar este dominio sin descanso
con el objetivo de devolver a la vida el ransomware temporalmente derrotado. [34] Mientras tanto, un ransomware aún más sofisticado que WannaCry -Petya- ha surgido para causar estragos en todo el mundo, y el malware basado en Petya (llamado NotPetya) ya ha costado más de 10.000 millones de dólares en daños. [35]

Las capacidades de las redes de bots maliciosas amenazan con socavar la confianza fundamental en la economía digital.

Por desgracia, a medida que aumenta el número de personas, empresas y dispositivos conectados, también lo hace el potencial, el poder y los beneficios de los grandes malintencionados
ataques. Como se ha descrito anteriormente, el número total de dispositivos conectados que se utilizan en todo el mundo asciende a miles de millones y, no por casualidad, se espera que el coste global de los ciberdelitos sea de billones. Las redes de bots son el motor a escala industrial de este problema. Además de las obvias pérdidas económicas, las capacidades de los botnets maliciosos amenazan con socavar la confianza fundamental en la economía digital. Este resultado desafía la cuantificación, pero su impacto negativo puede tener un efecto debilitante, al igual que la preocupación por la contaminación amenaza nuestra confianza en el aire que respiramos y el agua que bebemos.

El reto fundamental de hacer frente a las redes de bots en el ecosistema global de Internet, altamente diverso, complejo e interdependiente, es que la naturaleza esencial de Internet no es jerárquica y está 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 maliciosas es el clásico reto de la "tragedia de los comunes": si todo el mundo tiene un interés en los comunes de internet y está ineludiblemente conectado a ellos, pero nadie los controla, entonces ¿quién es responsable de limpiar las redes de bots maliciosas que amenazan las funciones básicas de las que todo el mundo depende?

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

UNA SOLA RED DE BOTS PUEDE INCLUIR AHORA MÁS DE

30

MILLÓN

PUNTOS FINALES "ZOMBIS" Y PERMITIR QUE LOS ACTORES MALICIOSOS SE BENEFICIEN SEIS CIFRAS AL MES

Esfuerzos anteriores para abordar este reto en todo el ecosistema

Las empresas responsables de esta Guía han sido de las primeras en adoptar prácticas voluntarias para proteger el ecosistema de las redes de bots. Por ejemplo, en 2012, los líderes del sector de las comunicaciones de Estados Unidos desarrollaron el Código de Conducta Anti-Botnet para los ISP, adoptando medidas significativas para erradicar las botnets a través de la educación, la detección, la notificación, la remediación y la colaboración. Mientras tanto, el sector tecnológico se ha beneficiado de prácticas de seguridad en el diseño, servicios de seguridad gestionados y soporte del ciclo de vida suministrados por proveedores mundiales de hardware, software, dispositivos y sistemas, y servicios relacionados. Aun así, los retos abundan en todo el ecosistema:

- Muchos ISP y otros proveedores de infraestructuras con capacidades avanzadas están impulsando continuamente el mercado hacia un estado de mayor seguridad para mitigar la amenaza de las botnets. A medida que aumentan el tamaño y la complejidad de las botnets, las empresas que operan redes de infraestructura han añadido capacidad de red para proteger a los clientes de ataques cada vez más grandes. Sin embargo, todas las partes interesadas pueden hacer algo más para operar eficazmente en el ecosistema, y los proveedores más pequeños a menudo necesitan orientación y recursos para ponerse a la altura.

  El software forma parte de todos los procesos comerciales y gubernamentales mundiales. Las diversas partes interesadas en la economía digital dependen cada vez más de un software seguro. Esta dependencia ha incentivado a los malos actores a desarrollar cada vez más sofisticados exploits. En respuesta, las empresas responsables han desarrollado prácticas seguras para el desarrollo de software y han establecido objetivos básicos de seguridad para cada etapa del ciclo de vida del producto. Son prácticas que los desarrolladores más pequeños pueden emular.

- Las asombrosas innovaciones en el desarrollo, despliegue y uso de los sistemas de dispositivos conectados son un arma de doble filo, ya que introducen en el mundo miles de millones de nuevos dispositivos con acceso a Internet y otros tantos nuevos puntos de entrada para que los ciberdelincuentes los exploten. Como se ha indicado anteriormente, muchos de estos dispositivos simplemente no fueron diseñados o desplegados con la seguridad en mente - y no se despliegan dentro de los sistemas que son capaces de mitigar sus vulnerabilidades individuales.

Los ordenadores y los dispositivos conectados en un hogar o una empresa deben estar protegidos durante todo el ciclo de vida del dispositivo, y lo que es más importante, desde su instalación y configuración inicial. Sin embargo, la instalación y la configuración correctas siguen siendo demasiado raras, por lo que los productos no suelen alcanzar su mejor rendimiento de seguridad disponible.

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 este contexto, el error común de los esfuerzos políticos anteriores ha sido su estrecho enfoque en uno o dos componentes del ecosistema, el equivalente en la elaboración de políticas a tratar de eliminar un bosque de árboles enfermos simplemente cortando las ramas más cercanas. Lo más probable es que el resultado sea un bosque todavía lleno de árboles enfermos. Del mismo modo, la mitigación de las redes de bots requiere un enfoque más 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 complementan las de los demás. Y en los casos en los que las líneas 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 políticas utópicas centradas en 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.

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 Anti-Botnet.

¿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. Hemos desarrollado esta Guía, basándonos en el análisis de la rápida evolución de las amenazas globales, 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.

04 Panorama del ecosistema mundial 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 conforman 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 definió y describió el ecosistema de Internet y las comunicaciones utilizando taxonomías similares pero diferentes, adaptadas a los propósitos y objetivos de cada foro. [36] En lugar de servir como visiones opuestas de cómo debe entenderse el ecosistema, estas definiciones se complementan y refuerzan mutuamente.

La economía digital tuvo un valor de 11,5 billones de dólares en 2016 y puede aumentar hasta los 23 billones, casi una cuarta parte del PIB mundial, en 2025

Esta Guía no es una excepción. Agrupamos los componentes del ecosistema de manera que se facilite la identificación y la aplicación de medidas anti prácticas de botnet entre los grupos de interés que la 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 y sistemas de dispositivos
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.

05 Prácticas y capacidades de lo 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 el alojamiento de sitios web, el registro de nombres de dominio, el 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 les permite ofrecer a los clientes una Internet de alta velocidad. acceso. Los mayores proveedores de redes troncales se denominan proveedores de "nivel 1". Estos proveedores no se limitan a un país o una 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 compara el nombre de dominio con una dirección IP y envía la dirección IP correspondiente al navegador del usuario, que 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 proveedores de CDN también pueden cruzar a otras industrias como 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 y el momento en que su contenido aparece en pantalla. La duración del retraso depende normalmente 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 varias ubicaciones, conocidas como puntos de presencia o PoP; cada PoP conecta a los usuarios finales dentro de su proximidad a 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 proporcionar una cobertura superior a los usuarios finales lejanos.

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 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.

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[37], 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, algunos Las prácticas básicas ya han demostrado que reducen el impacto de los ataques impulsados por redes de bots, como los ataques DDoS, y deberían aplicarse en todo el ecosistema.[38] A continuación, identificamos las prácticas básicas, así como 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.[39]

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.[40] Una limitación más obvia del análisis de firmas es que requiere el conocimiento previo del malware, lo que significa
que 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.[41]

Prácticas básicas: Los proveedores deben asegurarse de que sus bases de datos de firmas están actualizadas y deben contribuir a compartir la 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. Heurística
El análisis heurístico busca muchos indicios diferentes para determinar si el código es sospechoso. En el análisis heurístico estático, el código potencialmente malicioso se compara con el código de los programas maliciosos de 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 las amenazas desconocidas y en evolución. A veces, para deconstruir el código de forma segura, los científicos almacenan el 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. [42]

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, hay indicadores conocidos de que un software puede ser malicioso, por ejemplo cuando intenta
Obtiene privilegios elevados o interactúa de forma anómala con otros programas o archivos de un sistema. A menudo, el análisis de comportamiento se compara con la profesión médica: un médico a menudo puede decir cuando 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. [43]

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.

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 las 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.

Los 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.

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. [44] Al filtrar tráfico malo cuando entra en la red del proveedor (es decir, filtrado de entrada, BCP38 y BCP84)[45], los proveedores pueden reducir la eficacia de la suplantación de identidad y, por tanto, dificultar la realización de 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 de las mejores prácticas. [46] 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.

Al filtrar el tráfico malicioso cuando entra en la red del proveedor, éste puede reducir la eficacia de la suplantación de identidad y, por tanto, dificultar los ataques DDoS.

Además, aunque los proveedores suelen estar bien situados para filtrar el tráfico malicioso, técnicas como la BCP38 deberían ser empleadas por cualquier entidad que opere su propio espacio de direcciones IP, incluidas las empresas. Proveedores como ya que los ISP asignan muchas direcciones IP a sus clientes que, a su vez, pueden operar sus propias capacidades de filtrado y también necesitan seguir el 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. [47]

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. [48] 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 cantidad
de 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. [49]

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 redes de bots tanto para fines de investigación como de mitigación. [50] 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. Como el scrubbing requiere 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 routers que sólo admiten el blackholing, los routers 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. [51]

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 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. [52] 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. [53] 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 que no haya 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. Una acción policial que tenga consecuencias reales para los actores maliciosos es la única solución que aborda la causa de las redes de bots y los ataques DDoS, en lugar de los síntomas. Una acción policial de este tipo requiere muchos recursos y a menudo un análisis forense exhaustivo. Dominio a gran escala incautaciones también pueden requerir esfuerzos internacionales coordinados. [54] 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 mundial de Internet y las comunicaciones. [55]

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 y sistemas de dispositivos, instaladores de sistemas y empresas. Por lo tanto, esta sección no pretende captar las diversas prácticas básicas de seguridad y las capacidades avanzadas que son pertinentes para el desarrollo de software especializado en cada parte del ecosistema. En cambio, pretende subrayar la importancia vital de un 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 la promoción de la seguridad del software, publica recursos de formación sobre desarrollo de software seguro disponibles de forma gratuita para el público, incluyendo las *Prácticas fundamentales para el desarrollo de software seguro.* [56]

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 hay diferentes opciones de cifrado que se adaptan a las necesidades de organizaciones y productos específicos, el cifrado debe utilizar generalmente 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 que funcionen 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:* Al limitar el acceso de los usuarios y de las aplicaciones sólo a los privilegios esenciales necesarios 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
Las aplicaciones también pueden 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.

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.

Componentes seguros 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 para desarrollar y poner a disposición parches de seguridad. [57]

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. [58] Sin embargo, un

El marco desarrollado en colaboración entre el gobierno y las partes interesadas de 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. [59]

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 las aplicaciones.

C. DISPOSITIVOS Y SISTEMAS DE DISPOSITIVOS

Un dispositivo individual conectado (o "dispositivo final") puede estar formado por múltiples componentes, como módulos de hardware, chips, software, sensores u otros componentes operativos. Cientos de miles de empresas y millones de desarrolladores contribuyen potencialmente a los miles de millones de dispositivos individuales desplegados en todo el mundo. 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. En pocas palabras, los dispositivos conectados ya no son simplemente dispositivos individuales. En su lugar, teniendo en cuenta esta complejidad, esta Guía aborda los sistemas de dispositivos: la unión de un dispositivo de punto final conectado -es decir, una "cosa" en el Internet de las cosas- y sus elementos de apoyo asociados en otros lugares de Internet, incluidas las aplicaciones y los servicios en la nube. [60]

Prácticas básicas y capacidades avanzadas para dispositivos y sistemas de dispositivos

1. PRÁCTICAS DE DESARROLLO SEGURAS POR DISEÑO

La seguridad es mejor y más eficaz si forma parte del proceso de desarrollo inicial y se incluye como un factor clave a lo largo de dicho proceso. Ciertas categorías de buenas prácticas se han aceptado comúnmente como herramientas necesarias para garantizar que el producto final tenga una confidencialidad esencial,
integridad y disponibilidad. [61] Las redes de bots se aprovechan de los puntos débiles en la implementación de dispositivos y sistemas, por lo que es conveniente incluir la planificación de la seguridad desde el principio y en todas las etapas del desarrollo del producto para evitar dichos puntos débiles.

a) Proceso del ciclo de vida del desarrollo seguro

Prácticas básicas: Debe existir un proceso de ciclo de vida de desarrollo seguro (SDL). En el proceso SDL, cada fase de desarrollo tiene actividades de seguridad que se pueden realizar de forma manual o automática. [62]

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 Model63); los materiales del BSIMM son de código abierto y pueden ser un recurso para este esfuerzo.

b) Elementos de diseño seguro

Esta sección enumera las prácticas que se dan a nivel de desarrollador en el diseño de productos.

(1) Medios para proteger los datos en reposo y en tránsito

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 estas protecciones puede implicar decisiones relativas, por ejemplo, a elementos de hardware seguros, proceso de arranque seguro, etc.; véase también Capacidades avanzadas: Raíces de la confianza.

Prácticas básicas: Las comunicaciones de datos deben estar encriptadas. Los datos sensibles deben almacenarse cifrados. Independientemente de los protocolos que se utilicen, si la autenticación está disponible, debe utilizarse. En general, deben emplearse los mecanismos de seguridad disponibles en cualquier sistema que se utilice. Las técnicas criptográficas utilizadas deben evitar los métodos obsoletos.

Capacidades avanzadas: Deben utilizarse las últimas versiones de protocolos y mecanismos de seguridad. Se puede utilizar una memoria segura en lugar del cifrado para la información almacenada. Deben utilizarse métodos de clave de encriptación conformes con NIST FIPS 140-2 o ISO/IEC 24759. [64]

(2) Medios para restringir el acceso no autorizado

Prácticas de base: 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.

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: El control de acceso de los usuarios con autenticación multifactorial debe ser compatible.

Además, los desarrolladores de dispositivos de punto final y routers deberían considerar los estándares nuevos y emergentes que ayudan específicamente a prevenir el acceso no autorizado y el uso por parte de botnets. Por ejemplo, el descriptor de uso del fabricante del IETF (recomendación propuesta) o "MUD "[65] puede ser apropiado para muchos casos de uso. El MUD es "un estándar de software integrado definido por el IETF que permite a los fabricantes de dispositivos IoT anunciar las especificaciones del dispositivo, incluidos los patrones de comunicación previstos para su dispositivo cuando se conecta a la red".[66] Cuando tanto el dispositivo como el enrutador se adhieren a los requisitos del MUD, el enrutador tiene un mecanismo para limitar un dispositivo a los fines previstos por el fabricante. Las actividades ajenas a esos fines -como la participación en un ataque DDoS masivo- pueden ser identificadas y bloqueadas por el router local. Otros estándares como el IEEE 802.1AR67 y la arquitectura Device Identifier Composition Engine (DICE)[68] pueden mejorar la seguridad del dispositivo IoT y sus componentes MUD.

(3) Uso de la ofuscación

Prácticas básicas: 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: Implementación de la línea de base también.

(4) Validación de la entrada del usuario y codificación de la salida del sistema

Prácticas de base: Cualquier entrada recibida desde el exterior del sistema debe ser gestionada para que un adversario externo no pueda aprovecharse de las consecuencias no deseadas. La entrada debe ser validada en cuanto a longitud, tipo de caracteres y valores o rangos aceptables; véase también la lista blanca
filtrado. La salida de un subsistema a otro o a otro sitio también debe filtrarse; véase "canonización de caracteres".

Capacidades avanzadas: Implementación de la línea de base también.

(5) Criptografía acorde con las necesidades del producto

Prácticas básicas: Se requieren métodos criptográficos para garantizar la integridad y confidencialidad de los datos, la autenticación de los derechos y el no repudio de las solicitudes. Esta criptografía debe elegirse en función del riesgo evaluado, pero debe utilizar métodos y algoritmos abiertos y revisados por pares. Cuando sea posible, los métodos criptográficos son actualizables.

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 admitir longitudes de clave resistentes a la posverdad para el cifrado simétrico.

2. 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 corrupto 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.

a) Seguridad basada en el hardware

Prácticas de referencia: Considere cómo la seguridad basada en el hardware encaja en los ciclos de vida de desarrollo seguro de los productos actuales y futuros.

Capacidades avanzadas: La seguridad basada en el hardware se utiliza cuando es técnicamente posible.

3. GESTIÓN DEL CICLO DE VIDA DE LOS PRODUCTOS, INCLUIDO EL FIN DE LA VIDA ÚTIL

La gestión del ciclo de vida del producto 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. La gestión del fin de la vida útil se refiere a tener una política definida en cuanto a lo que debe hacerse cuando el producto ha llegado a un punto final definido en su ciclo de vida, incluyendo el final de un plazo de soporte definido, o el final de la funcionalidad, o el final de un período de calendario, etc.

Prácticas de base: Los fabricantes de dispositivos pueden avisar al consumidor sobre la política de soporte de seguridad y sobre cómo el dispositivo es soportado con actualizaciones durante y qué esperar después del periodo de soporte. Siempre que sea posible, el dispositivo debe apoyar la gestión de los activos de la red permitiendo la capacidad de identificar y auditar el dispositivo lógica y físicamente y con un control de acceso adecuado.

Tras el periodo de asistencia, los consumidores deben tener la posibilidad de "retirar" el dispositivo y ser informados de cómo hacerlo. El desmantelamiento debe permitir al consumidor devolver el producto a los valores de fábrica y eliminar cualquier información personal identificable (PII). Esta capacidad cubre una variedad de escenarios como la venta, el abandono o el reciclaje del producto, incluyendo la venta de una propiedad con dispositivos IoT instalados.

Los proveedores deben crear una política y un proceso de vulnerabilidad de seguridad para identificar, mitigar y, en su caso, revelar las vulnerabilidades de seguridad conocidas en sus productos.

Capacidades avanzadas: Un plan de actualizaciones seguras con protección antirretroceso y un control de acceso adecuado a lo largo de un periodo de soporte de seguridad definido, cuando sea técnicamente viable. [69]

4. 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 de referencia: Deben utilizarse herramientas capaces de comprobar si la aplicación sigue las directrices de codificación segura y de buscar un subconjunto de vulnerabilidades y exposiciones comunes (CVE) conocidas en el software de código abierto.

Capacidades avanzadas: Se utilizan herramientas como el fuzzing, la ejecución simbólica, el sandboxing, el análisis estático y dinámico y los lenguajes a prueba de memoria para encontrar y mitigar las vulnerabilidades.

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. Los sistemas de entretenimiento se benefician de los controles centrales para que las complejas configuraciones de audio y vídeo puedan gestionarse con facilidad. 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 la configuración del dispositivo. Una buena instalación logrará la "mejor seguridad disponible" del producto fabricado. En esta sección se presentan 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*. [70]

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 básicas: Los sistemas (ordenadores de sobremesa, portátiles, etc.) deben tener instaladas y en funcionamiento herramientas antivirus y antimalware actualizadas. 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 de red

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. Deben utilizarse opciones "no descubribles" cuando estén disponibles. No se debe exponer 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 de forma que permitan un fácil "olfateo" o una fácil manipulación.

(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-Personal con AES (preferido) o WPA2-Personal con TKIP. 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 bajo las mejores prácticas descritas en otra parte de 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 ser correlacionados 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. [71] 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 los 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 las redes de la organización.
sistemas y dispositivos, incluidos los sistemas IoT. Las empresas más pequeñas pueden carecer de los recursos necesarios para contar con personal especializado en TI y 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 asegurar sus redes y sistemas. Tal vez lo más relevante para la Guía Anti-Botnet sea el esfuerzo de la Coalición de Ciberseguridad por desarrollar y avanzar en los Perfiles para DDoS y Botnet
Perfil de Prevención y Mitigación del Marco de Ciberseguridad,[72] destinado a ayudar a las empresas y otras organizaciones a abordar y mitigar los ataques DDoS y otros ataques automatizados y distribuidos.

Las empresas de todos los tamaños también pueden tomar sus propias medidas proactivas para mitigar el riesgo del ecosistema mediante, por ejemplo, la aplicación de técnicas adecuadas de gestión de la identidad y el acceso y la interrupción del uso de productos y software heredados y pirateados que no reciben actualizaciones, entre otras cosas. Medidas como éstas pueden ayudar a las empresas a proteger los datos sensibles y la propiedad intelectual en sus redes, además de ayudar a proteger el ecosistema en general reduciendo la superficie de ataque para DDoS y otros ataques distribuidos.

Por supuesto, los proveedores y suministradores que han desarrollado esta Guía son nosotros mismos grandes empresas mundiales. Además, ofrecemos soluciones de alta gama para asegurar 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 creciendo; un mayor desarrollo del lado de la "demanda" de este mercado en términos de empresas de todos los tamaños que solicitan y negocian estos servicios traerá más innovación, sofisticación y eficiencia de costes en estos servicios.

Prácticas básicas y capacidades avanzadas para las empresas

1. ACTUALIZACIONES SEGURAS

Aunque los fabricantes de productos se encargan de crear actualizaciones seguras, éstas no suelen instalarse por sí mismas sin el permiso u otra acción del usuario. El nivel de control que las organizaciones pueden necesitar sobre las actualizaciones varía considerablemente según el tipo de cliente. Una gran empresa o agencia gubernamental con personal cualificado, por ejemplo, puede determinar razonablemente qué tipo de actualizaciones de seguridad son apropiadas y cuándo aplicarlas. Por otro lado, los usuarios domésticos habituales pueden beneficiarse más de las actualizaciones automáticas. [73]

Prácticas básicas: Las empresas deben instalar las actualizaciones tan pronto como estén disponibles. En general, son preferibles las actualizaciones automáticas.

Capacidades avanzadas: Las empresas con personal técnico cualificado pueden tomar decisiones informadas sobre la aplicación de las actualizaciones de seguridad.

Las empresas se encuentran colectivamente entre las partes interesadas importantes que comparten la responsabilidad de asegurar adecuadamente sus redes y sistemas para ayudar a asegurar el ecosistema digital más amplio.

2. INTERCAMBIO DE INFORMACIÓN EN TIEMPO REAL

Las empresas con grandes redes o redes muy sensibles (por ejemplo, grandes empresas y organismos gubernamentales) pueden compartir información sobre amenazas críticas con otras partes interesadas y participantes del ecosistema. Estos esfuerzos han mejorado significativamente en los últimos años y constituyen un gran paso adelante en la lucha contra la amenaza de los botnets y otras amenazas automatizadas y distribuidas. [74]

Prácticas básicas: Las empresas deben. estar preparadas para recibir y actuar de forma responsable ante la información sobre ciberamenazas proporcionada por las actividades de intercambio de información, incluso cuando no se hayan comprometido a compartir activamente la información. Algunos ejemplos son la información procedente de actividades de intercambio de información del gobierno y de las fuerzas de seguridad, varios CERT, grupos de la industria, proveedores de redes, direcciones RFC2142 y actualizaciones y alertas de proveedores y otras fuentes.

Las empresas deben suscribirse a varios servicios o fuentes de información sobre amenazas para utilizarlos junto con la correlación de la información de seguridad y la gestión de eventos (SIEM).
esfuerzos de automatización. 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. [75] 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 paquetes o correos electrónicos con malware; bloquear el tráfico de red no autorizado en la intranet; y utilizar la arquitectura DMZ estándar del sector y las prácticas operativas.

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 a los desarrolladores de aplicaciones, manteniendo al mismo tiempo 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 los botnets y otros ataques distribuidos, las empresas deberían adquirir una protección comercial contra los DDoS adecuada a su perfil de riesgo. [76] 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 ofrecen 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. [77] 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 apoyo 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 apropiadas (es decir, ISP y proveedores de nube/hosting que tengan capacidades de protección contra DDoS, software con capacidades de auto-actualización, 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 servicios automatizados o por defecto.
sobre la respuesta. Las empresas deben reevaluar periódicamente la eficacia de los proveedores comerciales.

Capacidades avanzadas: Las empresas avanzadas deben adoptar un enfoque multicapa para la protección contra DDoS y botnets que incluya capacidades bien soportadas dentro y fuera de las instalaciones.
Las empresas avanzadas deben aumentar de forma proactiva los conocimientos técnicos de su personal, determinar las carencias de estos conocimientos y abordarlas con la formación adecuada, apoyo contratado/contingente 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 la identidad y el acceso autentifican a las personas y los servicios y rigen las acciones que se les permite realizar. Una de las áreas más importantes de riesgo de TI se refiere a los usuarios privilegiados, como los administradores de TI, los CISO y otras personas con mayor acceso a los sistemas. Ya sea de forma involuntaria o maliciosa, las acciones indebidas de los usuarios privilegiados 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 el "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.
[78]

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. [79]

Cuando los clientes adquieren productos y servicios comerciales, disminuyen sustancialmente la amenaza de las redes de bots y otros ataques distribuidos.

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;
- *Gobierno 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 de una autenticación multifactorial (2FA/MFA) para los accesos privilegiados, por ejemplo, Sistema
Administradores. 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 de 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 las aplicaciones internas con las herramientas de gestión del acceso, por ejemplo, revocando 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. [80] Un problema estrechamente relacionado desde el punto de vista del soporte técnico es el software pirata. En EE.UU., casi uno de cada cinco ordenadores personales utiliza software pirata, mientras que en China el porcentaje de ordenadores personales con software pirata supera a menudo el 70%. [81] Por supuesto, los fabricantes no suelen poner parches al software pirata, lo que significa que sigue siendo vulnerable a los exploits conocidos. [82] 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. [83]

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 1.0 de esta guía constituye el primer paso de una campaña estratégica sin precedentes liderada por la industria contra las botnets y otras amenazas automatizadas y distribuidas. El CSDE, USTelecom, ITI y CTA instan a las partes interesadas a poner en práctica las prácticas recomendadas para hacer frente a los desafíos comunes y cambiar el rumbo de los malos actores.

Como se señala en la introducción de la Guía, 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 actualizar, publicar y promover 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.

De forma más inmediata, nuestro siguiente paso en los próximos meses es promover esta Guía 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, NTT, Oracle, Samsung, SAP, Telefónica y Verizon. La CSDE está coordinada por USTelecom y el Consejo de la Industria de las Tecnologías de la Información (ITI).

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 ITI

El Consejo de la Industria de las Tecnologías de la Información (ITI) es la voz global del sector tecnológico. Es la principal organización de defensa y política de las principales empresas innovadoras del mundo,
El ITI navega por las relaciones entre los responsables políticos, las empresas y las organizaciones no gubernamentales, aportando soluciones creativas que hacen avanzar el desarrollo y el uso de la tecnología en todo el mundo.

Acerca de la Asociación de Consumidores de Tecnología

La Consumer Technology Association (CTA)™ es la asociación comercial que representa a los 377.000 millones de dólares La industria de la tecnología de consumo de Estados Unidos, que mantiene más de 15 millones de puestos de trabajo en el país. Más de 2.200 empresas -el 80% son pequeñas y nuevas empresas; otras se encuentran entre las marcas más conocidas del mundo- disfrutan de los beneficios de la afiliación a la CTA, que 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.

8 Notas finales

1 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

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

3 Un dispositivo individual conectado (o "dispositivo final") puede estar formado por múltiples componentes, como módulos de hardware, chips, software, sensores u otros componentes operativos. Cientos de miles de empresas y millones de desarrolladores contribuyen al desarrollo de los miles de millones de dispositivos desplegados en todo el mundo. 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. En pocas palabras, los dispositivos conectados ya no son simplemente dispositivos individuales. Teniendo en cuenta esta complejidad, esta Guía aborda los sistemas de dispositivos: la unión de un dispositivo de punto final conectado -una "cosa" en el IoT- y sus elementos de apoyo asociados en otros lugares de Internet, incluidas las aplicaciones y los servicios en la nube.

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 los controles centrales para poder gestionar con facilidad las 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,
todo sistema de dispositivos que entre en un entorno doméstico, de oficina, de venta al por menor, médico o industrial estará 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 Tech. Ass'n, *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).

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 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. Estas 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 reduciendo la superficie de ataque de las redes de bots. Los proveedores y suministradores que desarrollaron esta Guía son grandes empresas mundiales, y también ofrecemos soluciones de alta gama para asegurar 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 cuanto a las empresas de todos los tamaños que solicitan y negocian estos servicios, aportará más innovación, sofisticación y eficiencia de costes en estos servicios

7 Descripciones de CSDE, ITI y USTelecom *infra* p. 41.

8 Descripción de la CTA *infra* p. 41.

9 En aras de la brevedad, en lo sucesivo nos referiremos a las "redes de bots y otras amenazas automatizadas y distribuidas" como "botnets".

10 Andrew Sheehy, *GDP Cannot Explain The Digital Economy*, Forbes (6 de junio de 2016), https://www.forbes. com/sites/andrewsheehy/2016/06/06/gdp-cannot-explain-the-digital-economy/#47c4db1218db.

11 Irving Wladawsky-Berger, *GDP Doesn't Work in a Digital Economy*, The WallStreetJournal(3denoviembrede2017) https://blogs.wsj.com/cio/2017/11/03/ gdp-doesnt-work-in-a-digital-economy.

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

13 *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."

14 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.

15 Michael Newberg, *As Many as 48 Million Twitter Accounts Aren't People, Says Study*, CNBC (10 de marzo de 2017), https://www. cnbc.com/2017/03/10/ nearly-48-million-twitter-accounts-could-be-bots-says-study.html.

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

17 Daniel Newman, *The Top 8 IoT Trends for 2018,* Forbes (19 de diciembre de 2017), https://www.forbes. com/sites/danielnewman/2017/12/19/the-top-8-iot- trends-for-2018/#2523096867f7 (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* (7defebrero 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.

18 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.

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

20 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 de 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-wired-investigation (donde se habla de cómo el malware NotPetya causó más de 10.000 millones de dólares en daños)

21 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.

22 Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* 4 (Mar. 2015), disponible en https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_ IV_WG4_Final_Report_031815.pdf (donde se reconocen "las ventajas de un enfoque no normativo frente a un régimen de cumplimiento prescriptivo y estático").

23 *Véanse las* notas 1-22 *supra* y las notas 24-83 *infra*.

24 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").

25 Tobias Knecht, *A Brief History of Bots and How They've Shaped the Internet Today,* Abusix (23 de agosto de 2017), https://www.abusix.com/blog/a-brief- history-of-bots-and-how-theyve-shaped-the-internet-today.

26 Dustin Volz y Jim Finkle, *U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam,* Reuters (Mar. 2016), https://www.reuters. com/article/ us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new- york-dam-idUSKCN0WQ1JF.

27 Lee Matthews, *World's Biggest Mirai Botnet Is Being Rented Out for DDoS* Attacks*,* Forbes (29 de noviembre de 2016), https://www.forbes. com/sites/ leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out- for-ddos-attacks/#6bdec4cb58ad.

28 *Compárese con* Elie Bursztein, *Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis,* Cloudflare (14 de diciembre de 2017), https://blog.cloudflare. com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis ("el ataque de Mirai fue, con mucho, el mayor, alcanzando un máximo de 623 Gbps") con Sean Gallagher, *Federal Grand Jury Indicts 7 Iranians for "Campaign of Cyber Attacks"*, Ars Technica (Mar. 24, 2016) ("En su punto álgido, los ataques DDoS alcanzaron los 140 gigabits por segundo").

29 Hay que tener en cuenta que en marzo de 2018, el récord de volumen de tráfico de la red de bots Mirai fue pulverizado por los atacantes dirigidos a GitHub con un ataque DDoS que alcanzó 1,35 Terrabytes por segundo (bps). *Véase* Lily Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded,* Wired (1 de marzo de 2018) https://www.wired. com/story/github-ddos-memcached. En particular, el ataque no utilizó un

botnet. En su lugar, los atacantes falsificaron las peticiones a servidores vulnerables de "memcached" utilizados para acelerar los sitios web, haciendo que las víctimas se vieran inundadas con una cantidad de tráfico de Internet 50 veces superior a la normal. ("Memcached" se refiere a los sistemas de almacenamiento en caché de memoria distribuida, que suelen utilizarse para aumentar la velocidad de los sitios web mediante el "almacenamiento en caché" de datos en la memoria de acceso aleatorio en lugar de depender de fuentes de datos externas). Dado que los servidores de memcached responden a cualquiera -incluidos los actores maliciosos- no deberían estar expuestos a la Internet pública. Sin embargo, unos 100.000 de estos servidores están expuestos y son vulnerables; muchos pertenecen a pequeñas empresas y organizaciones con recursos de seguridad limitados. *Véase* Liam Tung, *New World Record DDoS Attack Hits 1.7Tbps Days after* Landmark *GitHub Outage,* ZDNet (6 de marzo de 2018), https:// www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days- after-landmark-github-outage. Los ataques de inundación de este tipo que explotan las vulnerabilidades del servidor se han vuelto cada vez más populares entre los malos actores. Solo unos días después de que GitHub sobreviviera al "mayor ataque DDoS jamás registrado" se volvió a batir el récord: Un cliente de Arbor Networks fue objeto de un ataque similar que alcanzó 1,7 Tbps.

30 Cyren, Cyren Cyber Threat Report 8 (enero de 2017), http://www.vcwsecurity. com/wp-content/uploads/2017/01/Cyren_2017Q1_Botnet_Threat_Report.pdf.

31 Denis Makrushin, *The Cost of Launching a DDoS Attack,* Kaspersky (23 de marzo de 2017), https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.

32 Alfred Ng, *WannaCry Ransomware Loses Its Kill Switch, So Watch Out,* CNET (15 de mayo de 2017), https://www. cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch.

33 Ellen Nakashima, *Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes,* Washington Post (12 de enero de 2018), https://www. washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.bc4ce7d72018.

34 Andy Greenberg, *Hackers Are Trying to Reignite WannaCry with Nonstop Botnet Attacks,* Wired (19 de mayo de 2017), https://www. wired.com/2017/05/ wannacry-ransomware-ddos-attack.

35 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-wired-investigation.

36 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 (May*22, 2018), disponible en https://www. commerce.gov/sites/commerce.gov/ files/media/files/2018/eo_13800_botnet_report_-_finalv2.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; 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 (enero de 2008), https://www.itu.int/ITU-D/cyb/ cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

37 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 10 (*22 de mayo de 2018), *disponible en* https://www. commerce.gov/sites/commerce. gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

38 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 y 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/ 50
advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

39 *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/cisp (consultado por última vez el 17 de octubre de 2018); Japón, Cyber Clean Center, https:// www.telecom-isac.jp/ccc/en_index.html (consultado por última vez el 17 de octubre de 2018); Nueva Zelanda, CORTEX, https://www.gcsb.govt.nz/our-work/information- assurance/cortex-faqs (último acceso: 17 de octubre de 2018).

40 *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.

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

42 *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).

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

44 Nat'l Inst. of Standards and Tech., *Advanced DDoS Mitigation Techniques (*18 de octubre de 2017) ("Durante más de una década la industria había desarrollado especificaciones de técnicas y orientación 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

45 P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employed IP Source Address Spoofing,* Internet Engineering TaskForce (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 (marzo de 2004), *disponible en* https://tools.ietf.org/html/bcp84.

46 Id.

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

48 *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.

49 *Véase* Cisco, *Policing and Shaping Overview* (última actualización, 23 de noviembre de 2017), https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.html.

Véase, por ejemplo, Guy Bruneau, *DNS Sinkhole,* SANS Institute (7 de agosto de 2010), https://www.sans.org/reading-room/whitepapers/dns/dns- sinkhole-33523.

51 *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.

52 *Véase* Georgia Tech Researchers, *DNS Changer Remediation Study, Presentation to M3AAWG 27th General Meeting, San Francisco, CA* (Feb. 19, 2013), *disponible en* https://www.m3aawg.org/sites/default/files/document/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (consultado por última vez el 17 de octubre de 2018); *véase también* Commc'n Sector Coordinating Council, Botnet Whitepaper 24-25 (17 de julio de 2017) (en el que se enumeran múltiples formas en las que los proveedores de infraestructuras pueden notificar a los usuarios, como el correo electrónico, la llamada telefónica, el correo postal, mensaje de texto, notificación a través del navegador web, walled garden y otros métodos como las redes sociales), *disponible en* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

53 *Véase* 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 por la práctica de "cortar o interferir de otro modo en la conexión a Internet de un cliente" para obligar a
botnet remediation), *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 (4 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/EFF- Comments-to-BotNet-RFI_11-4-11.pdf.

54 *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.

55 *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. (marzo de 2017), *disponible en* https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20 FINAL.pdf.

56 *Véase* SAFECode, Fundamental Practices for Secure Software Development (2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

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

58 *Véase* SAFECode, Principles for Software Assurance Assessment (2015), *disponible en* https://safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf; CA Tech., Veracode, https://www.veracode.com/verified (consultado por última vez el 18 de junio de 2018).

59 Nat'l Inst. of Standards and Tech., NTIA Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency (consultado por última vez el 6 de noviembre de 2018).

60 Esta sección sobre dispositivos y sistemas se basa en Consumer Tech. Ass'n, *Securing Connected Devices for Consumers in the Home - A Manufacturer's Guide* (CTA-CEB33), https://members.cta.tech/ctaPublicationDetails/?id=c12 ebabe-84cd-e811-b96f-0003ff52809d (último acceso: 15 de octubre de 2018).

61 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.

62 *Véase* Microsoft, ¿Qué es el ciclo de vida del desarrollo de la seguridad?, https://www. microsoft.com/en-us/sdl/default.aspx (consultado por última vez el 19 de octubre de 2018).

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

64 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).

65 Para la Recomendación propuesta actual, *véase* IETF, Manufacturer Usage Description Specification, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud (consultado por última vez el 19 de octubre de 2018).

66 Cisco, ¿Qué es la descripción de uso del fabricante? (MUD), https://developer.cisco.com/docs/mud/#!what-is-mud (último acceso: 19 de octubre de 2018).

67 IEEE, 802.1AR: Secure Device Identity, https://1.ieee802.org/ security/802-1ar/ (último acceso: 19 de octubre de 2018).

68 Trusted Computing Group, Device Identifier Composition Engine (DICE) Architectures, https://trustedcomputinggroup.org/work-groups/dice- architectures (consultado por última vez el 19 de octubre de 2018).

69 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).

70 Consumer Tech. Ass'n, *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).

71 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.

72 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).

73 *Véase el* Grupo de Trabajo 8 del Consejo de Fiabilidad e Interoperabilidad de la Secretaría de Estado de Comunicaciones, *Informe final sobre la protección de las redes de los proveedores de servicios de Internet* 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://www.atis.org/01_legal/docs/CSRICII/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

74 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://doi.org/10.6028/NIST.IR.8192.

75 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-ddos-attacks-with-a-resilient-network/#79144da56f8a.

76 *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. cloud.telefonica.com/en/open-cloud/products/security/anti-ddos (última visita el 14 de mayo de 2018); NTT, DDoS Protection Service, https://www.ntt. com/en/services/network/gin/transit/ ddos.html (última visita el 14 de mayo de 2018).

77 *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).

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

79 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.

80 *Véase* Microsoft, *El 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).

81 Véase BSA The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey* 6-7 (2016), http://www.bsa.org/~/ media/Files/StudiesDownload/BSA_GSS_US.pdf.

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

83 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").

Council to Secure the Digital Economy

securingdigitaleconomy.org

CSDE