Informe al Presidente sobre

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y distribuidas

---

Transmitido por
El Secretario de Comercio y
El Secretario de Seguridad Nacional

22 de mayo de 2018

Índice de contenidos

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Resumen ejecutivo

Este informe responde a la Orden Ejecutiva del 11 de mayo de 2017, "Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica". Esa orden pedía "resiliencia contra las redes de bots y otras amenazas automatizadas y distribuidas", ordenando al Secretario de Comercio, junto con el Secretario de Seguridad Nacional, que "lidere un proceso abierto y transparente para identificar y promover la acción de las partes interesadas apropiadas" con el objetivo de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos (por *ejemplo* , botnets)."

Los Departamentos de Comercio y Seguridad Nacional han trabajado conjuntamente en este esfuerzo a través de tres enfoques: la organización de dos talleres, la publicación de dos solicitudes de comentarios y el inicio de una investigación a través del Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC), con el objetivo de reunir una amplia gama de aportaciones de expertos y partes interesadas, incluyendo la industria privada, el mundo académico y la sociedad civil. Todas estas actividades contribuyeron al proceso de recopilación de información para los organismos que elaboran las recomendaciones de este informe.

Los Departamentos trabajaron en consulta con los Departamentos de Defensa, Justicia y Estado, la Oficina Federal de Investigación, los organismos específicos del sector, la Comisión Federal de Comunicaciones y la Comisión Federal de Comercio, y otros organismos interesados.

Los Departamentos determinaron que las oportunidades y los retos para trabajar en la reducción drástica de las amenazas de los ataques automatizados y distribuidos pueden resumirse en seis temas principales.

1. **Los ataques automatizados y distribuidos son un problema global.** La mayoría de los dispositivos comprometidos en las recientes redes de bots más destacadas han estado ubicados geográficamente fuera de Estados Unidos. Para aumentar la resistencia del ecosistema de Internet y de las comunicaciones frente a estas amenazas, muchas de las cuales se originan fuera de Estados Unidos, debemos seguir colaborando estrechamente con socios internacionales.
2. **Existen herramientas eficaces, pero su uso no está muy extendido.** Aunque todavía hay margen de mejora, las herramientas, procesos y prácticas necesarias para mejorar significativamente la resistencia del ecosistema de Internet y las comunicaciones están ampliamente disponibles y se aplican de forma rutinaria en determinados sectores del mercado. Sin embargo, no forman parte de las prácticas habituales para el desarrollo y despliegue de productos en muchos otros sectores por diversas razones, entre las que se incluyen (pero no se limitan a) la falta de concienciación, la evitación de costes, la insuficiencia de conocimientos técnicos y la falta de incentivos de mercado.
3. **Los productos deben estar protegidos durante todas las etapas del ciclo de vida. Los** dispositivos que son vulnerables en el momento de su despliegue, que carecen de medios para parchear las vulnerabilidades una vez descubiertas o que permanecen en servicio una vez finalizado el soporte del proveedor, facilitan en exceso el montaje de amenazas automatizadas y distribuidas.
4. **La concienciación y la educación son necesarias.** Los usuarios domésticos y algunos clientes empresariales a menudo no son conscientes del papel que sus dispositivos podrían desempeñar en un ataque de botnet y pueden no comprender plenamente las ventajas de los controles técnicos disponibles. Los desarrolladores de productos, los fabricantes y los operadores de infraestructuras a menudo carecen de los conocimientos y las habilidades necesarias para desplegar herramientas, procesos y prácticas que harían el ecosistema más resistente.
5. **Los incentivos del mercado deberían estar más alineados. Los incentivos del** mercado no parecen alinearse actualmente con el objetivo de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos". Los desarrolladores de productos, los fabricantes y los vendedores están motivados para minimizar el coste y el tiempo de comercialización, más que para incorporar seguridad u ofrecer actualizaciones de seguridad eficientes. Los incentivos del mercado deben reajustarse para promover un mejor equilibrio entre seguridad y comodidad a la hora de desarrollar productos.

6. **Los ataques automatizados y distribuidos son un reto para todo el ecosistema.** Ninguna comunidad de interesados puede abordar el problema de forma aislada.

Los Departamentos identificaron cinco objetivos complementarios que se apoyan mutuamente y que, de cumplirse, reducirían drásticamente la amenaza de ataques automatizados y distribuidos y mejorarían la resistencia y la redundancia del ecosistema. Una lista de acciones sugeridas para los principales interesados refuerza cada objetivo. Los objetivos son:

- Objetivo 1: Identificar un camino claro hacia un mercado tecnológico adaptable, sostenible y seguro.
- Objetivo 2: Promover la innovación en la infraestructura para la adaptación dinámica a las amenazas cambiantes.
- Objetivo 3: Promover la innovación en el borde de la red para prevenir, detectar y mitigar los ataques automatizados y distribuidos.
- Objetivo 4: Promover y apoyar las coaliciones entre las comunidades de seguridad, infraestructura y tecnología operativa a nivel nacional y mundial.
- Objetivo 5: Aumentar la concienciación y la educación en todo el ecosistema.

Las acciones y opciones recomendadas incluyen actividades en curso que deberían continuar o ampliarse, así como nuevas iniciativas. Ninguna inversión o actividad por sí sola puede mitigar todas las amenazas, pero los debates organizados y los comentarios de las partes interesadas nos permitirán seguir evaluando y priorizando estas actividades en función de su rendimiento esperado de la inversión y de su capacidad para influir de forma mensurable en la resiliencia de los ecosistemas. Este informe requiere una actualización de la situación que evalúe el nivel de progreso realizado por las partes interesadas para contrarrestar las amenazas automatizadas y distribuidas.

Este esfuerzo no terminará con la publicación de este informe. Queda mucho trabajo por hacer. Sin embargo, no esperamos que todas las acciones se lleven a cabo de forma simultánea, debido a consideraciones como la limitación de recursos en las comunidades de interesados pertinentes. Además, algunas acciones ya están en marcha, mientras que otras dependen de factores externos. Proponemos un modelo de apoyo a la coordinación y colaboración para la ejecución de las acciones descritas en la Sección III, con especial énfasis en los requisitos federales. Mientras que algunas acciones directamente relacionadas con el gobierno federal son claramente apropiadas para que el gobierno las lidere, este modelo proporciona una manera para que las partes interesadas colaboren con el gobierno mientras avanzan en aquellas acciones que se logran mejor a través del liderazgo del sector privado.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

I. Antecedentes

El 11 de mayo de 2017, el Presidente emitió la Orden Ejecutiva (OE) 13800, "Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica", pidiendo "resiliencia contra las redes de bots y otras amenazas automatizadas y distribuidas".[1] El Presidente ordenó al Secretario de Comercio y al Secretario de Seguridad Nacional "liderar un proceso abierto y transparente para identificar y promover la acción de las partes interesadas apropiadas" con el objetivo de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos (por *ejemplo* , botnets)."

Este tipo de ataques ha sido motivo de preocupación desde los primeros días de Internet,[2] y era un hecho habitual a principios de la década de 2000. [3] Los ataques automatizados y distribuidos constituyen una amenaza que va más allá de cualquier empresa o sector. Estas amenazas se utilizan para diversas actividades maliciosas, como los ataques de denegación de servicio distribuidos (DDoS) que saturan los recursos de la red, envían cantidades masivas de spam y difunden keyloggers y otros programas maliciosos; los ataques de ransomware distribuidos por redes de bots que toman como rehenes los sistemas y los datos; y las campañas de propaganda informática4 que manipulan e intimidan a las comunidades a través de los medios sociales. Las técnicas tradicionales de mitigación de DDoS, como los proveedores de redes que construyen un exceso de capacidad para absorber los efectos de las redes de bots, están diseñadas para proteger contra redes de bots de un tamaño previsto. Con las nuevas redes de bots que aprovechan el gran número de dispositivos del "Internet de las cosas" (IoT),[5] los ataques DDoS han crecido en tamaño hasta más de un terabit por segundo, superando con creces el tamaño previsto y el exceso de capacidad. Como resultado, el tiempo de recuperación de este tipo de ataques puede ser demasiado lento, especialmente cuando se trata de servicios de misión crítica. Además, estas técnicas de mitigación no fueron diseñadas para remediar otras clases de actividades maliciosas facilitadas por las redes de bots, como el ransomware o la propaganda informática.

A medida que surgen nuevos escenarios, existe una necesidad urgente de coordinación y colaboración entre un conjunto diverso de partes interesadas. El gobierno federal ha trabajado con las partes interesadas en el pasado para hacer frente a las nuevas amenazas a medida que surgen. Los esfuerzos anteriores incluyen el Grupo de Botnets de la Industria, que dio lugar a los Principios para los Esfuerzos Voluntarios para Reducir el Impacto de las Botnets en el Ciberespacio (2012); [6] los esfuerzos de intercambio de información y coordinación del sector de servicios financieros después de los ataques DDoS a los bancos en 2012 y

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22.391 (11 de mayo de 2017), *disponible en* https://www.federalregister.gov/d/2017-10004.
[2] Estados Unidos contra Morris, 928 F.2d 504 (2d Cir. 1991).
[3] *Véase, por ejemplo,* Stuart Staniford, Vern Paxson y Nicholas Weaver, How *to 0wn the Internet in Your Spare Time,* Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, 5-9 de agosto de 2002, *disponible en* https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf.
[4] La propaganda computacional es el "conjunto de plataformas de medios sociales, agentes autónomos y big data encargados de manipular la opinión pública". Samuel C. Woolley y Philip N. Howard, *Political Communication, Computational Propaganda, and Autonomous Agents-Introduction, 10* Int'l Journal of Commc'n 4882, 4886 (2016), *disponible en* http://ijoc.org/index.php/ijoc/article/viewFile/6298/1809.
[5] Algunos ejemplos de dispositivos de la IO incluyen (pero no se limitan a) bombillas conectadas, cerraduras de puertas, parquímetros, monitores personales de salud, automatización industrial y sensores, y automóviles.
[6] Industry Botnet Group, *Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace*, https://archive.is/20131015084520/www.industrybotnetgroup.org/principles/ (última visita el 4 de abril de 2018).

2013;[7] el Código de Conducta Anti-Bot del Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones (CSRIC)[8] (2013)[9] y los informes sobre Prácticas de Protección de la Red de los Proveedores de Servicios de Internet (ISP) (2010)[10] y Remediación de los Ataques DDoS Basados en el Servidor (2014); [11] y el trabajo activo y en curso del Departamento de Justicia y sus numerosos socios para abordar y "hundir" la infraestructura que soporta estas amenazas. [12] Aunque estas iniciativas han logrado algunos avances, los efectos han sido graduales y siguen existiendo importantes desafíos. Al abordar de forma proactiva estos retos, esta Administración y las principales partes interesadas tienen la oportunidad de mejorar la resistencia del futuro ecosistema de Internet y las comunicaciones.

Los ataques DDoS lanzados desde la red de bots Mirai en otoño de 2016, por ejemplo, alcanzaron un nivel de tráfico sostenido que sobrepasó muchas herramientas y servicios comunes de mitigación de DDoS, e incluso interrumpió un servicio de Sistema de Nombres de Dominio (DNS) que era un componente comúnmente utilizado en muchas estrategias de mitigación de DDoS. [13] Este ataque también puso de manifiesto la creciente inseguridad de los dispositivos IoT de consumo, y las amenazas que plantean. Al tratarse de una nueva tecnología, los dispositivos IoT suelen construirse y desplegarse sin que se hayan implementado importantes características y prácticas de seguridad. [14] Si bien la variante original de Mirai era relativamente sencilla, ya que explotaba las contraseñas débiles de los dispositivos, le han seguido redes de bots más sofisticadas; por ejemplo, la red de bots Reaper utiliza vulnerabilidades de código conocidas para explotar una larga lista de dispositivos,[15] y uno de los mayores ataques DDoS vistos hasta la fecha explotó recientemente una vulnerabilidad recién descubierta en el relativamente oscuro

[7] *Evaluación de la seguridad del sector financiero estadounidense: Hearing Before the Task Force to Investigate Terrorism Financing*, House Committee on Financial Services, 114th Cong. 40-59 (2015) (declaración de John W. Carlson, Jefe de Personal del Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC)), *disponible en* https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96997/pdf/CHRG-114hhrg96997.pdf.

[8] El CSRIC es un comité asesor de la Comisión Federal de Comunicaciones, cuya misión es hacer recomendaciones a la Comisión para promover la seguridad, la fiabilidad y la resiliencia de los sistemas de comunicaciones de la nación. Para más información, incluidos los esfuerzos de seguridad anteriores, véase CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability- council-0 (visitado por última vez el 4 de abril de 2018).

[9] Communications Security, Reliability and Interoperability Council III Working Group 7, *Final Report on U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs)*, (Mar. 2013), *disponible en* https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[10] Grupo de Trabajo 8 del Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones, *Informe final sobre las prácticas de protección de la red de los proveedores de servicios de Internet (ISP)*, (diciembre de 2010), *disponible en* http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101 213.pdf.

[11] Grupo de Trabajo 5 del Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones, *Informe final sobre la reparación de los ataques DDoS basados en el servidor*, (septiembre de 2014), *disponible en* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.

[12] *Véase, por ejemplo,* Departamento de Justicia de Estados Unidos, *Red Avalancha desmantelada en una operación cibernética internacional*, (5 de diciembre de 2016), https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.

[13] Equipo de Preparación para Emergencias Informáticas de los Estados Unidos, *Alerta (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*, https://www.us-cert.gov/ncas/alerts/TA16-288A (última revisión: 17 de octubre de 2017).

[14] El Comité Asesor de Telecomunicaciones de Seguridad Nacional, *NSTAC Report to the President on the Internet of Things*, (19 de noviembre de 2014), *disponible en* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20.pdf.

[15] Brian Krebs, *¿Miedo a la Parca, o locura de la Parca?* Krebs on Security (27 de octubre de 2017, 4:39 PM), https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/.

software MemCacheD. [16] Estos ejemplos demuestran claramente los riesgos que plantean las redes de bots de este tamaño y alcance, así como la innovación prevista y el aumento de la escala y la complejidad de los futuros ataques.

Acérquese a

Los Departamentos de Comercio y Seguridad Nacional trabajaron conjuntamente en este esfuerzo a través de tres enfoques destinados a recoger una amplia gama de aportaciones de expertos y partes interesadas, incluyendo la industria privada, el mundo académico y la sociedad civil. Los Departamentos trabajaron en consulta con los Departamentos de Defensa, Justicia y Estado, la Oficina Federal de Investigación, los organismos específicos del sector, la Comisión Federal de Comunicaciones y la Comisión Federal de Comercio, así como otros organismos interesados.

En junio de 2017, la Administración Nacional de Telecomunicaciones e Información (NTIA) del Departamento de Comercio publicó una solicitud de comentarios (RFC) sobre la "Promoción de la acción de las partes interesadas contra las redes de bots y otras amenazas automatizadas".[17] La RFC pedía comentarios sobre "los enfoques actuales, emergentes y potenciales para hacer frente a las redes de bots y otros ataques distribuidos y automatizados". La NTIA recibió 47 comentarios, con respuestas que iban desde grandes asociaciones comerciales (que representan a miles de empresas) hasta expertos técnicos individuales. Los comentaristas también representaban una gama diversa de industrias y sectores, incluidos los proveedores de servicios de Internet, las empresas de seguridad, los proveedores de infraestructura, los fabricantes de software, la sociedad civil y el mundo académico, tanto de organizaciones estadounidenses como no estadounidenses.

En julio de 2017, el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio organizó un taller sobre la "Mejora de la resiliencia del ecosistema de Internet y las comunicaciones".[18] El taller animó a las partes interesadas a explorar las soluciones actuales y emergentes que abordan las amenazas automatizadas y distribuidas de una manera abierta y transparente. Atrajo a 150 participantes de diversas comunidades interesadas, que identificaron una amplia gama de acciones coordinadas por todas las partes interesadas para hacer frente a estas amenazas.

Como se indica en la Orden Ejecutiva 13800, se publicó un proyecto de informe en enero de 2018, seguido de un segundo RFC y un taller, en el que las partes interesadas discutieron los comentarios públicos sustantivos y los próximos pasos. Estas actividades contribuyeron al proceso de recopilación de información para las agencias que desarrollan las recomendaciones en este informe final. Los comentarios y las discusiones del taller también informarán muchas de las acciones que se llevarán a cabo después de la publicación de este informe.

La participación del Departamento de Seguridad Nacional (DHS) en este esfuerzo se centró a través del subcomité del Comité Asesor de Seguridad Nacional de Telecomunicaciones (NSTAC) del Presidente, que finalizó y aprobó el *Informe del NSTAC al*

[16] Lili Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired (1 de marzo de 2018, 11:01 AM), https://www.wired.com/story/github-ddos-memcached/.

[17] Información adicional, incluyendo los comentarios públicos, está disponible en National Telecommunications and Information Administration, *Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats*, (8 de junio de 2017), https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting- stakeholder-action-against-botnets-and-other-automated-threats.

[18] Instituto Nacional de Normas y Tecnología, *Enhancing Resilience of the Internet and Communications Ecosystem*, https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications- ecosystem (última actualización: 10 de julio de 2017). Para un resumen de las actas, véase Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem: A NIST Workshop Proceedings*, (septiembre de 2017), NIST Interagency/Internal Report No. 8192, *disponible en* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Mientras elaboraba su informe, el NSTAC estudió las redes de bots, así como las formas de ataque que pueden ser facilitadas por las redes de bots, como los ataques DDoS y los vectores que podrían utilizarse para crear redes de bots (es *decir*, dispositivos de usuario final e IoT). A través de su estudio, el NSTAC llegó a la conclusión de que los ataques automatizados y distribuidos facilitados a través de botnets amenazan la seguridad y la resistencia del ecosistema de Internet y de las comunicaciones y, a su vez, la infraestructura crítica de la nación. Además, el NSTAC determinó que los dispositivos IoT comprometidos serán utilizados cada vez más por actores maliciosos para lanzar ataques automatizados globales.

Temas principales

Las oportunidades y los retos a los que nos enfrentamos para reducir drásticamente las amenazas de los ataques automatizados y distribuidos pueden resumirse en seis temas principales.

1. **Los ataques automatizados y distribuidos son un problema global.** La mayoría de los dispositivos comprometidos en las recientes redes de bots más destacadas han estado ubicados geográficamente fuera de Estados Unidos. Para aumentar la resistencia del ecosistema de Internet y de las comunicaciones frente a estas amenazas, muchas de las cuales se originan fuera de Estados Unidos, debemos seguir colaborando estrechamente con socios internacionales.
2. **Existen herramientas eficaces, pero su uso no está muy extendido.** Aunque todavía hay margen de mejora, las herramientas, procesos y prácticas necesarias para mejorar significativamente la resistencia del ecosistema de Internet y las comunicaciones están ampliamente disponibles y se aplican de forma rutinaria en determinados sectores del mercado. Sin embargo, no forman parte de las prácticas habituales para el desarrollo y despliegue de productos en muchos otros sectores por diversas razones, entre las que se incluyen (pero no se limitan a) la falta de concienciación, la evitación de costes, la insuficiencia de conocimientos técnicos y la falta de incentivos de mercado.
3. **Los productos deben estar protegidos durante todas las etapas del ciclo de vida. Los** dispositivos que son vulnerables en el momento de su despliegue, que carecen de medios para parchear las vulnerabilidades una vez descubiertas o que permanecen en servicio una vez finalizado el soporte del proveedor, facilitan en exceso el montaje de amenazas automatizadas y distribuidas.
4. **La concienciación y la educación son necesarias.** Los usuarios domésticos y algunos clientes empresariales a menudo no son conscientes del papel que sus dispositivos podrían desempeñar en un ataque de botnet y pueden no comprender plenamente las ventajas de los controles técnicos disponibles. Los desarrolladores de productos, los fabricantes y los operadores de infraestructuras a menudo carecen de los conocimientos y las habilidades necesarias para desplegar herramientas, procesos y prácticas que harían el ecosistema más resistente. Se necesitan mecanismos fáciles de usar para identificar las opciones más seguras, análogos a los programas como el Energy Star20 o las calificaciones de seguridad de 5 estrellas de la Administración Nacional de Tráfico por Carretera (NHTSA)21 , con el fin de aumentar la concienciación de los consumidores e informar sobre las decisiones de compra.
5. **Los incentivos del mercado deberían estar más alineados. Los incentivos del** mercado no parecen alinearse actualmente con el objetivo de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos". Los desarrolladores de productos, los fabricantes y los vendedores están motivados para minimizar el coste y el tiempo de comercialización, más que para incorporar la seguridad u ofrecer una seguridad eficiente

[19] Comité Asesor de Telecomunicaciones de Seguridad Nacional, *Informe del NSTAC al Presidente sobre la resiliencia de Internet y las comunicaciones*, (16 de noviembre de 2017), *disponible en* https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[20] Energy Star, *About Energy Star*, https://www.energystar.gov/about (visitado por última vez el 4 de abril de 2018). [21] National Highway Traffic Safety Administration, *Search NHTSA's 5-Star Safety Ratings*, https://www.safercar.gov/Vehicle-Shoppers (última visita el 4 de abril de 2018).

actualizaciones. Los incentivos del mercado deben reajustarse para promover un mejor equilibrio entre seguridad y comodidad a la hora de desarrollar productos.

6. **Los ataques automatizados y distribuidos son un reto para todo el ecosistema.** Ninguna comunidad de interesados puede abordar el problema de forma aislada.

Una nota sobre las amenazas

Este documento no distingue entre Estados-nación, ciberdelincuentes y otros actores de la amenaza. Aunque algunos ataques pueden ser difíciles de atribuir inicialmente, el ecosistema debe unirse para mitigar un ataque. Este proceso abierto y transparente se centró en las áreas que suscitarían la más amplia participación de las partes interesadas de todo el ecosistema de Internet y las comunicaciones en lo que respecta a las mejoras de seguridad, así como a la cooperación antes, durante y después de los ataques, entendiendo que la identidad de un determinado actor de la amenaza puede ser inicialmente desconocida. La Evaluación de Amenazas Mundiales de la Comunidad de Inteligencia de Estados Unidos de 2018, publicada por la Oficina del Director de Inteligencia Nacional, ofrece una visión del panorama de las ciberamenazas. [22] Aunque va más allá del alcance de este informe, será importante diferenciar entre el Estado-nación, los ciberdelincuentes y otros actores de la amenaza a la hora de determinar la mejor manera de aplicar una amplia gama de autoridades gubernamentales estadounidenses específicas de la amenaza. Algunos participantes en el taller también reconocieron sus limitaciones a la hora de abordar clases específicas de actores de amenazas. En el futuro habrá que prestar atención a estas cuestiones, implicando a las partes interesadas del ecosistema en general, según proceda.

II. Estado actual del ecosistema y visión de futuro

Esta sección describe el estado actual de los dominios técnicos y políticos del ecosistema de Internet y las comunicaciones mundiales, y prevé un futuro mejorado. Los dominios técnicos del ecosistema incluyen:

- La ***infraestructura*** que conecta los demás ámbitos técnicos en un único sistema;
- ***Redes empresariales*** compuestas por dispositivos conectados localmente con direcciones de Internet versión 4 (IPv4) e IPv6 asignadas por el Registro Regional de Internet (RIR)[23] y redes de área sublocal (LAN) conectadas localmente que utilizan un espacio de direcciones IP privado o protocolos alternativos (por *ejemplo,* Bluetooth Low Energy);
- ***Dispositivos de borde***, como ordenadores personales, dispositivos móviles, servidores de borde, y dispositivos IoT y otros dispositivos conectados; y
- ***Redes domésticas y de pequeñas empresas*** compuestas por dispositivos que utilizan un espacio de direcciones IP privado direccionable externamente a través de la traducción de direcciones de red (NAT).

El dominio político está entrelazado con los dominios técnicos, e incluye:

- **Asociaciones público-privadas**, incluyendo acuerdos de intercambio de información;

[22] *Véase* Daniel R. Coats, Director de Inteligencia Nacional, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the Record at the Senate Select Committee on Intelligence, (13 de febrero de 2018), *disponible en* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23] "Los Registros Regionales de Internet (RIR) son corporaciones sin ánimo de lucro que administran y registran el espacio de direcciones del Protocolo de Internet (IP) y los números del Sistema Autónomo (AS) dentro de una región definida." Registro Americano de Números de Internet, *Registros Regionales de Internet*, https://www.arin.net/knowledge/rirs.html (visitado por última vez el 4 de abril de 2018).

- **Procesos de certificación voluntarios**, en los que proveedores y clientes optan por compartir objetivos y expectativas de seguridad;
- **Normas y directrices** elaboradas en foros de múltiples partes interesadas;
- **Políticas de contratación**, especialmente en el gobierno federal, para crear incentivos de mercado;
- **Acciones reguladoras y legislativas** a nivel federal y/o estatal; y
- **Compromiso internacional** para aprovechar los objetivos compartidos y las mejores prácticas.

La mejora de la resiliencia frente a los ataques automatizados y distribuidos requerirá la colaboración en conjuntos de soluciones técnicas, políticas y de otro tipo entre naciones, sectores y capas técnicas. Las políticas eficaces proporcionarán expectativas claras para el uso de normas y directrices que sigan siendo flexibles y adaptables a medida que evolucione el riesgo de seguridad. Ninguna solución o marco único abordará todos los riesgos, pero una mejor colaboración en todos los ámbitos mejorará la capacidad de los miembros del ecosistema para mitigar la amenaza de las redes de bots.

Dominios técnicos

Infraestructura: Estado actual

Frente a los ataques automatizados y distribuidos, la actual infraestructura subyacente al ecosistema digital ha demostrado una notable resistencia, pero el tamaño y el alcance crecientes de los ataques parecen estar poniendo a prueba los límites de esa resistencia. Estas dos perspectivas surgieron tras los ataques de la red de bots Mirai de 2016, que interrumpieron temporalmente los servicios de un proveedor de infraestructuras de Internet, interrumpiendo muchos de los principales servicios en línea y sitios web en Norteamérica y Europa. Sin embargo, las interrupciones fueron temporales y los principales actores respondieron rápidamente. Esta respuesta pone de manifiesto tanto la interdependencia de la infraestructura como la capacidad de las personas y las organizaciones para aprender y adaptarse rápidamente.

En este informe, la "infraestructura" incluye la tecnología y las organizaciones que permiten la conectividad, la interoperabilidad y la estabilidad, yendo más allá de los cables físicos, los transmisores y receptores inalámbricos y los enlaces por satélite para incluir el hardware, el software, las herramientas, las normas y las prácticas de las que depende el ecosistema, por ejemplo, los routers, los conmutadores, los proveedores de servicios de Internet, los proveedores de DNS, las redes de distribución de contenidos, el alojamiento y los proveedores de servicios en la nube. [24] Debido a la complejidad de la infraestructura moderna, con herramientas y actores clave intercalados en el ecosistema, ninguna herramienta por sí sola puede asegurar la infraestructura. Tradicionalmente, a medida que surgen nuevas amenazas, determinados subconjuntos de actores de la infraestructura trabajan juntos para comprender el riesgo y la vía de mitigación.

El filtrado del tráfico cuando entra y sale de una red -la técnica conocida como filtrado de entrada y salida- es una de esas herramientas. La suplantación de IP es una técnica común empleada en los ataques DDoS, en la que el atacante fabrica la dirección IP de origen para evitar que la víctima filtre el tráfico malo por el origen del tráfico.
Los proveedores de red pueden limitar el spoofing restringiendo el tráfico entrante a lo que realmente se origina en su red declarada, filtrando el tráfico que dice venir de fuera de su espacio de red previsto. [25] El filtrado de entrada está reconocido como una buena práctica desde hace tiempo por la Internet Engineering

[24] Aunque la Directiva Política Presidencial (PPD) 21 reconoce los sistemas y activos de los sectores de las comunicaciones y la tecnología de la información como infraestructuras críticas, este documento utiliza el término "infraestructura de Internet" para abarcar además las organizaciones y prácticas de las que depende el ecosistema de Internet.
[25] El DHS está desarrollando y apoyando herramientas de software de código abierto para evaluar e informar sobre el despliegue de las mejores prácticas anti-spoofing de validación de direcciones de origen (SAV). Para más información, véase Center for Applied Internet Data Analysis, *Spoofer*, https://www.caida.org/projects/spoofer/.

(IETF) y otras organizaciones centradas en la infraestructura. [26] Puede complementarse con el filtrado de salida, en el que una organización u operador de red despliega filtros en el borde de su red para evitar que el tráfico que no parece originarse dentro de la red salga a la Internet global.

Los principales operadores nacionales aplican las normas de filtrado de entrada en al menos una parte de sus redes. Sin embargo, estas normas no son universalmente apoyadas en todo el mundo, ni por los pequeños proveedores de infraestructuras nacionales. Muchos expertos técnicos y empresariales se han opuesto a las propuestas de aplicar el filtrado de entrada en un nivel superior de Internet, a nivel de las redes troncales internacionales, porque sería más probable que bloqueara el tráfico legítimo. [27] El filtrado de entrada se defiende como una práctica de seguridad común para las empresas,[28] pero sigue siendo poco común para las pequeñas y medianas empresas. Aunque no se implementa de forma universal, el filtrado de entrada/salida de la red, cuando se implementa, es eficaz para mitigar la clase de ataques DDoS que aprovechan la suplantación de direcciones IP de origen.

Los proveedores de infraestructuras y otras empresas ofrecen servicios comerciales anti-DDoS, que pueden desempeñar un papel fundamental a la hora de limitar el impacto de los ataques contra determinados objetivos. Sin embargo, no todos los clientes empresariales adquieren la gama completa de servicios anti-DDoS, debido al gasto y a la complejidad de integrar esos servicios en los demás componentes de la red de la empresa. Mientras tanto, los atacantes aprenden rápidamente a explotar los agujeros de los servicios existentes. Cuando se enfrentan a ataques que se basan en el gran volumen de tráfico, las soluciones de mitigación de DDoS fuera de las instalaciones proporcionan más capacidad de red o utilizan la forma de la propia red para limitar el volumen de tráfico que llega al objetivo. Otros ataques se dirigen al servidor web o a la propia aplicación. Los dispositivos y herramientas locales de una empresa detectan y filtran estos ataques en la red objetivo.

Las mejores prácticas actuales implican el empleo de un enfoque híbrido que utiliza tanto el filtrado local como las herramientas de defensa DDoS que aumentan la capacidad fuera de las instalaciones. Sin embargo, la aplicación de las mejores prácticas puede ser costosa, difícil de gestionar y requiere personal cualificado. Estas mejores prácticas también suelen construirse en torno a crisis pasadas, lo que hace difícil, por ejemplo, argumentar un gran exceso de capacidad hasta que se produzca un ataque. Un programa de detección activa de amenazas que detecte las vulnerabilidades y las tendencias de los ataques puede complementar estos esfuerzos, ayudando a la organización víctima a responder según sea necesario. Las redes de distribución de contenidos (CDN) son otra herramienta que puede aprovechar las grandes infraestructuras privadas dedicadas para proteger a los clientes. A medida que surgen diferentes ataques, o los adversarios seleccionan nuevos objetivos, las organizaciones suelen invertir en defensas específicas para las amenazas.

Responder a tiempo requiere preparación y conocimientos. Dado el amplio conjunto de controles de seguridad necesarios en la Internet moderna, no todo el personal de los proveedores de infraestructuras más pequeños o de las empresas más importantes conoce las ventajas del filtrado y otras herramientas. Muchos proveedores de infraestructura ofrecen advertencias sobre compromisos y ataques en curso, pero si las empresas ignoran esas advertencias, es menos probable que el proveedor de infraestructura haga un seguimiento diligente con más advertencias. Las víctimas a menudo luchan

[26] *Véase, por ejemplo,* P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, (mayo de 2000), Internet Engineering Task Force - Network Working Group, *disponible en* https://tools.ietf.org/html/bcp38 ("BCP 38"); y F. Baker & P. Savola, Ingress *Filtering for Multihomed Networks, (*marzo de 2004), Internet Engineering Task Force - Network Working Group, *disponible en* https://tools.ietf.org/html/bcp84 ("BCP 84").

[27] Los paquetes pueden ser enrutados entre los puntos finales de Internet a través de rutas significativamente diferentes en diferentes instancias en el tiempo por razones legítimas.

[28] *Véase, por ejemplo,* Chris Brenton, *Egress Filtering FAQ*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059 (última revisión: 19 de abril de 2006).

cuando se encuentran con su primer ataque sustancial sin un plan de respuesta en marcha, porque dependen de la propia red atacada para entenderlo y contactar con los proveedores de servicios para obtener ayuda.

Visión del futuro de las infraestructuras

Los proveedores de infraestructura de todo tipo deben desarrollar una amplia comprensión de los beneficios de los enfoques de defensa compartida, y las comunidades deben trabajar juntas para impulsar la adopción de las mejores prácticas. Este trabajo incluye la adopción ubicua del filtrado en la interfaz con las redes de los clientes, incluidas las infraestructuras de varios inquilinos, como los proveedores de la nube. Lo ideal sería que los proveedores de infraestructuras conocieran los niveles actuales de ataques, mantuvieran una capacidad suficiente para absorber los niveles de tráfico malicioso previstos de forma realista y comunicaran estas capacidades a sus clientes. Los servicios de los proveedores de infraestructuras para la mitigación de DDoS deberían integrarse con las soluciones de red existentes de los clientes, independientemente del nivel de servicio que haya elegido el cliente.

A medida que los nuevos productos y herramientas están disponibles, los actores del ecosistema deben entender cómo su comportamiento puede ayudar -o dificultar- su eficacia. Una red cada vez más inteligente puede segmentar diferentes tipos de tráfico de forma automática, para aislar o mitigar aplicaciones o dispositivos que son fuentes y objetivos de ataques. Las empresas son cada vez más capaces de hacer frente a los ataques a nivel de aplicación con las herramientas adecuadas, y los proveedores de estas herramientas deben trabajar tanto con los clientes como con los proveedores de aplicaciones pertinentes para que las decisiones de seguridad sean más fáciles y eficaces.

Una mayor implantación de varias tecnologías existentes ayudará a mitigar estos ataques. Parte de la infraestructura existente se basa en protocolos antiguos, como la red IPv4 y los protocolos de enrutamiento heredados. Una mayor adopción de las normas y las mejores prácticas actuales aportará ventajas en materia de seguridad. Por ejemplo, la red IPv6 puede permitir mejor el reconocimiento de dispositivos específicos en la red para detectar comportamientos aberrantes a nivel de dispositivo.[29] Las organizaciones pequeñas y medianas deberían incorporar las mejores prácticas de la industria y, a medida que se necesiten y prueben nuevas normas y prácticas de infraestructura, los proveedores de infraestructura deberían adoptarlas de manera eficiente.

En el núcleo de la infraestructura, los principales actores ya comparten información sobre la naturaleza cambiante de las amenazas. Aunque muchas de estas organizaciones emplean a expertos que se coordinan con sus pares en todo el mundo, en el futuro, el intercambio de información debe ampliarse para incluir a los actores más pequeños, menos financiados o de nicho a través de nuevas herramientas y prácticas automatizadas. Los incentivos podrían promover la inversión en una detección mejor y más eficiente del tráfico malicioso, así como más compromisos públicos para evitar el transporte de tráfico malicioso. Estos compromisos se basarían en las relaciones existentes en la comunidad para ayudar a construir una red global más estable.

Redes empresariales: Estado actual

Las redes que dan soporte a las empresas (por *ejemplo,* medianas y grandes empresas, agencias gubernamentales e instituciones académicas) son otro dominio técnico clave en el ecosistema de Internet y las comunicaciones. Estas redes suelen ser complejas, con enrutadores de Protocolo de Pasarela Fronteriza (BGP) propiedad de la empresa y operados por ella, resolvedores de DNS y aplicaciones que dependen de una combinación de servicios locales y basados en la nube. Los dispositivos de borde suelen incluir servidores potentes, dispositivos informáticos personales, teléfonos móviles y dispositivos IoT gestionados y no gestionados por la empresa. Los dispositivos de las redes empresariales pueden utilizar una mezcla de servicios estáticos o

[29] La actual solución de IPv4, la traducción de direcciones de red (NAT), ofrece ventajas de cortafuegos, especialmente en el ámbito de la red doméstica. Sin embargo, hay que tener en cuenta que, una vez que se implemente IPv6, los atacantes podrían identificar direcciones específicas de dispositivos objetivo que antes habrían sido más difíciles de reconocer detrás de NAT. Los expertos también han expresado cierta preocupación por la seguridad de algunas implementaciones de IPv6.

direcciones asignadas dinámicamente de uno o más rangos de direcciones IP públicas (por *ejemplo,* direcciones adquiridas de un RIR), así como direcciones asignadas de rangos de direcciones IP privadas administradas localmente. La gran presencia de redes empresariales conectadas a Internet hace que no sólo sean víctimas potenciales, sino también fuentes de riesgo.

Muchos de los ataques DDoS más conocidos, como los que sufrieron los bancos estadounidenses en 2012 y 2013, se dirigieron a servicios de cara al cliente asociados a grandes empresas. [30] Al igual que los ataques Mirai de 2016 permitieron a algunas empresas demostrar su resistencia frente a la vulnerabilidad, los ataques de 2012-2013 estimularon al sector financiero y a sus socios a descubrir debilidades y a demostrar vías para una mayor resistencia.
Estos ataques fueron perturbadores, pero el sector mitigó sus efectos gracias a una mayor inversión en tecnología y recursos, así como a la colaboración activa de toda la comunidad, incluidos sus proveedores de servicios de red y socios técnicos, así como con el gobierno. Las organizaciones compartieron las lecciones aprendidas a medida que los ataques continuaban, e instituciones como el Centro de Análisis e Intercambio de Información de Servicios Financieros (ISAC) y la Mesa Redonda de Servicios Financieros facilitaron el intercambio de información y la coordinación con los principales proveedores de servicios de Internet. La magnitud de los ataques inspiró el liderazgo de los más altos niveles de dirección e impulsó una relación más duradera con los expertos gubernamentales, así como el compromiso de invertir en herramientas y servicios.

Los recursos asociados a las redes empresariales también son un factor importante en la ejecución de amenazas automatizadas y distribuidas. Los dispositivos a nivel empresarial, desde los dispositivos IoT hasta los servidores de los centros de datos, pueden verse comprometidos e incorporados a las redes de bots. Los recursos empresariales mal administrados, como los resolutores de DNS abiertos, a menudo se aprovechan para amplificar los ataques. Para algunas empresas, puede ser un reto mantener todos los sistemas y dispositivos parcheados y actualizados en sus redes globales. Los routers operados por las empresas que no aplican el filtrado de entrada y salida han facilitado los ataques que incluyen la suplantación de direcciones, lo que permite a los participantes en las redes de bots ocultar su verdadera ubicación. En el caso de los proveedores de la nube, se han alquilado recursos empresariales (normalmente con tarjetas de crédito robadas) para montar rápidamente importantes redes de bots. En muchos países, los problemas que rodean a los sistemas heredados se ven agravados por el uso generalizado de software pirata, que normalmente no está parcheado y, por tanto, es vulnerable a los exploits conocidos.
Las empresas con un uso intensivo de software pirata son extremadamente difíciles de proteger, lo que proporciona a los actores maliciosos una reserva de sistemas que se ensamblan fácilmente en amenazas distribuidas.

Las empresas que se han enfrentado a ataques DDoS, o que pertenecen a sectores ampliamente afectados por estos ataques, a menudo incorporan posibles ataques en su modelo de riesgo y emplean una combinación de mitigaciones DDoS ofrecidas por proveedores de infraestructura y mitigaciones gestionadas por la empresa en sus propias instalaciones. Las empresas que comprenden los riesgos y aplican estos mecanismos son la excepción. Muchas empresas de riesgo no son conscientes del impacto potencial de los ataques DDoS en sus operaciones. Es posible que estas empresas no comprendan del todo su capacidad para proteger sus redes y responder y recuperarse de un ataque. Por ejemplo, es posible que no conozcan las limitaciones de sus contratos con los proveedores de infraestructuras, o la disponibilidad de productos y servicios para mitigar los ataques DDoS. También es posible que no comprendan plenamente el coste de recuperación de un ataque de este tipo.

En ausencia de un ataque en curso, las empresas se centran tradicionalmente en la disponibilidad, la funcionalidad y el coste. Como resultado de este enfoque, es probable que las empresas confíen en dispositivos heredados que ya no pueden ser protegidos adecuadamente, o desplegarán dispositivos IoT y otros que nunca fueron diseñados para ser seguros. Donde

[30] *Véase* David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN (28 de septiembre de 2012, 9:27 AM ET), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

las actualizaciones de seguridad están disponibles, las empresas pueden tener procesos extremadamente onerosos para evaluar los parches o largos períodos entre el mantenimiento programado, ampliando la ventana de vulnerabilidad. [31]

Aunque las empresas suelen contar con personal profesional de operaciones de tecnologías de la información (TI), a menudo faltan conocimientos específicos de ciberseguridad. Este reto se ve agravado a menudo por una falta de conocimiento similar entre los responsables de la toma de decisiones de las organizaciones, que son los encargados de dotar de recursos a las operaciones de TI dentro de sus organizaciones o de supervisar las operaciones de TI. Los equipos de operaciones de TI a menudo desconocen los riesgos de los resolvedores abiertos y otras fuentes de amplificación de ataques, o la importancia del filtrado de entrada y salida. Cuando los ISP, por ejemplo, informan a los clientes de un posible compromiso, a menudo se encuentran con que la empresa no puede identificar o localizar los dispositivos comprometidos, e incluso si la empresa puede identificar y localizar los dispositivos, es posible que no tenga las herramientas o la experiencia para recuperar un estado seguro. Las empresas pueden tener dificultades para trabajar en colaboración con los proveedores de servicios cuando son atacadas. El hecho de no aplicar procedimientos básicos de copia de seguridad hace que las empresas corran un mayor riesgo de tener que recuperarse del ransomware distribuido por las redes de bots.

Las empresas pueden contribuir a un ecosistema más resistente mediante una combinación de tecnologías actuales y emergentes, políticas operativas y de adquisición, y la concienciación y educación del personal de TI y los responsables de la toma de decisiones.

Visión del futuro de las redes empresariales

Un paso fundamental hacia esta visión sería una mayor aplicación empresarial de los principios contenidos en el Marco de Ciberseguridad del NIST (CSF). [32] La mayoría de las acciones necesarias pueden atribuirse a las cinco funciones concurrentes y continuas del marco:

- **Identificar.** Las empresas localizan los dispositivos heredados y otros dispositivos que no pueden protegerse. Las empresas retiran del servicio estos dispositivos de alto riesgo siempre que sea posible y los sustituyen por dispositivos intrínsecamente seguros o que puedan protegerse.
- **Proteger.** La arquitectura del sistema proporciona capas adicionales de protección a cualquier dispositivo de alto riesgo restante (por *ejemplo, el* acceso a los dispositivos heredados estaría restringido por la arquitectura de la red). Las empresas despliegan o adquieren servicios de mitigación de DDoS dentro y fuera de las instalaciones. Las arquitecturas de red de las empresas limitan la exposición de los dispositivos a los actores maliciosos y limitan los daños causados por dispositivos comprometidos. Se implementa un filtrado de entrada y salida para evitar la suplantación de direcciones de red, y se reconfiguran los amplificadores de ataque (por *ejemplo, los* resolvedores abiertos). Los procesos de actualización eficientes minimizan la ventana de vulnerabilidad para todos los dispositivos de la red. Las infraestructuras de varios inquilinos también aplican el filtrado de entrada y salida para reducir el impacto de las redes de bots basadas en la nube.
- **Detección.** Una combinación de servicios de detección basados en el ISP y la supervisión de la red y los servicios de la empresa detectan el tráfico malicioso saliente, los ataques entrantes e identifican los dispositivos comprometidos casi en tiempo real.
- **Responder.** Las empresas tienen políticas y procedimientos para abordar los dispositivos comprometidos (por *ejemplo,* reemplazar, mitigar o parchear un dispositivo que participa en una red de bots) cuando son detectados por la empresa o

[31] *Véase* Dan Goodin, *Failure to Patch Two-month-old Bug Led to Massive Equifax Breach*, Ars Technica (13 de septiembre de 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch- two-month-old-bug/. *Véase también* Comisión Federal de Comercio, *Mobile Security Updates: Understanding the Issues* (febrero de 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

[32] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cybersecurity- framework (última visita el 4 de abril de 2018).

ISP. Las empresas también cuentan con procesos para ponerse en contacto con sus ISP u otros proveedores de servicios anti-DDoS cuando se detectan ataques a nivel local. Los recursos operativos clave siguen funcionando con recursos limitados.

- **Recuperación.** Las empresas tienen la posibilidad de reconstituir los sistemas comprometidos (por *ejemplo,* a partir de una copia de seguridad) en lugar de tener que pagar por el ransomware para reanudar las operaciones.

Las tecnologías y las políticas operativas destacadas anteriormente sólo son realistas si se apoyan en una combinación adecuada de políticas de adquisición e iniciativas de concienciación y educación. El personal y la dirección de la empresa deben ser conscientes de los riesgos de seguridad para los recursos de la empresa derivados de las amenazas distribuidas, así como de las opciones de protección, respuesta y recuperación. El personal de TI debe poseer las habilidades para implementar las opciones seleccionadas para la mitigación y la prevención. Las políticas de adquisición de la organización deben garantizar que las cuestiones relativas al ciclo de vida de la seguridad ocupen un lugar destacado en las decisiones de adquisición, para evitar que se añadan productos inseguros al sistema o que permanezcan conectados a él. Estos cambios deben producirse en las empresas a nivel global, y no sólo a nivel nacional, para tener un impacto significativo en el ecosistema.

Dispositivos de borde: Estado actual

Los dispositivos son un dominio técnico diverso y creciente del ecosistema. [33] Internet soporta simultáneamente sistemas informáticos multiusuario, dispositivos informáticos personales y móviles, tecnología operativa (por *ejemplo,* sistemas de control de supervisión y adquisición de datos [SCADA] en entornos industriales o de fabricación) y dispositivos IoT en todo el ecosistema. Por regla general, los dispositivos de borde desempeñan dos papeles diametralmente opuestos con respecto a las amenazas distribuidas: los actores maliciosos comprometen los dispositivos de borde para crear amenazas distribuidas, y los dispositivos de borde también pueden ser el objetivo de la amenaza (por *ejemplo,* ataques de ransomware distribuidos por redes de bots). Los puntos finales mal protegidos pueden ser tanto las fuentes como las víctimas de los ataques.

Los actores maliciosos están motivados para construir botnets de la forma más barata y eficiente posible. A lo largo de los años, los objetivos han evolucionado, desde las máquinas de las empresas hasta los dispositivos domésticos poco seguros, pasando por los sistemas vulnerables gestionados por los proveedores de alojamiento y de servicios en la nube y, más recientemente, por los dispositivos del IoT. Estos cambios en los objetivos reflejan la promesa y los retos que ofrece este dominio técnico con respecto a la creación de un ecosistema más resistente. Los ordenadores personales y los dispositivos móviles son más seguros que en años anteriores. Mientras tanto, los dispositivos conectados han alcanzado un nivel de sofisticación y densidad que facilita su focalización mediante códigos automatizados, al tiempo que esos dispositivos carecen de las ventajas de las herramientas de seguridad modernas.

Los dispositivos de borde pueden ser vulnerables a un compromiso por una variedad de razones:

- A menudo, los dispositivos no se han diseñado pensando en la seguridad. Los desarrolladores desconocen las buenas prácticas de diseño de seguridad, suponen que el dispositivo será inaccesible (por *ejemplo,* en una red local inaccesible desde Internet) o quieren evitar soluciones de seguridad que impongan un coste adicional, aumenten el tiempo de comercialización o dificulten el uso del dispositivo por parte de los consumidores. Las opciones de diseño resultantes, como las contraseñas administrativas codificadas, crean dispositivos intrínsecamente inseguros. En otros casos, existen controles de seguridad adecuados, pero la usabilidad y las interfaces de usuario dan lugar a configuraciones menos seguras.

[33] Gartner, *Gartner dice que en 2017 se utilizarán 8.400 millones de "cosas" conectadas, un 31% más que en 2016*, (7 de febrero de 2017), *disponible en:* https://www.gartner.com/newsroom/id/3598917.

- Las técnicas habituales de desarrollo de software dan lugar, siendo optimistas, a un fallo cada 2.000 líneas de código34 , o más según muchas otras métricas. [35] Muchos de estos fallos crean vulnerabilidades de seguridad explotables, como desbordamientos de búfer.
- Cuando los fallos se descubren después de que los productos se hayan desplegado, puede ser difícil o imposible parchearlos. Estas vulnerabilidades suelen ser mucho más fáciles de explotar que de corregir.
- Los sistemas que se envían con ajustes de configuración por defecto inadecuados, como contraseñas codificadas, son más vulnerables en su funcionamiento.
- Los sistemas también pueden ser vulnerables porque el soporte no está disponible. Este suele ser el caso de los dispositivos antiguos.
- La escala y la diversidad de los dispositivos desplegados dificultan las correcciones fáciles y proporcionan superficies de ataque adicionales para la actividad maliciosa.

Varios de los principales desarrolladores de software se han tomado en serio estas lecciones y han establecido las mejores prácticas actuales que pueden reducir significativamente las vulnerabilidades de los dispositivos de borde. Por ejemplo, el ciclo de vida de desarrollo de software de Microsoft, o SDLC, garantiza que la seguridad se tenga en cuenta desde el principio.
Las herramientas de desarrollo de software seguro, como el input fuzzing36 o el análisis estático[37] , reducen el número de vulnerabilidades en el software. Los servicios de actualización seguros pueden corregir las vulnerabilidades tras su descubrimiento. [38] Los sistemas se entregan con configuraciones más seguras, por lo que no es necesario cambiar la configuración por defecto. Como resultado, los servidores, ordenadores de sobremesa, portátiles y teléfonos inteligentes modernos ofrecen muchas menos oportunidades para el compromiso.
Esto se traslada también al entorno de la nube, con dispositivos de borde más seguros que se convierten en una posibilidad práctica. Las raíces de confianza del hardware, que demuestran que los sistemas no han sido manipulados, son otra innovación que aparece en los sistemas modernos.

Desgraciadamente, los dispositivos IoT suelen carecer de características centradas en la seguridad. Estos sistemas ofrecen ahora el objetivo más atractivo para los actores maliciosos, y constituyen un porcentaje cada vez mayor de los dispositivos del ecosistema. De hecho, el Informe de Movilidad de Ericsson de noviembre de 2016 predijo que los dispositivos IoT superarán a los teléfonos móviles como la mayor categoría de dispositivos conectados en 2018.[39] Dado el nivel de seguridad de los dispositivos IoT, es una predicción desalentadora.

---

[34] *Véase Coverity Scan: Open Source Report 2014*, Synopsys, página 4, (2015), http://go.coverity.com/rs/157-LQW- 289/images/2014-Coverity-Scan-Report.pdf.
[35] *Véase, por ejemplo,* Steve McConnell, *Code Complete: A Practical Handbook of Software Construction*, páginas 521, 652, (Microsoft Press, 2ª ed. 2004), ISBN: 0735619670.
[36] "Las pruebas fuzz (fuzzing) son una técnica de garantía de calidad utilizada para descubrir errores de codificación y lagunas de seguridad en el software, los sistemas operativos o las redes. Consiste en introducir cantidades masivas de datos aleatorios, llamados fuzz, en el sujeto de la prueba para intentar que se bloquee." TechTarget - SearchSecurity.com, definición de fuzz testing (fuzzing), https://searchsecurity.techtarget.com/definition/fuzz-testing (última actualización: marzo de 2010).
[37] "El análisis estático, también llamado análisis de código estático, es un método de depuración de programas informáticos que se realiza examinando el código sin ejecutar el programa". TechTarget - SearchWinDevelopment.com, definición de análisis estático (análisis de código estático), https://searchwindevelopment.techtarget.com/definition/static-analysis (última actualización en noviembre de 2006).
[38] El Software Assurance Forum for Excellence in Code (SAFECode), un consorcio de la industria, ha publicado un informe para codificar estas lecciones y ofrecer más orientaciones sobre el modelo SDLC. Mark Belk y otros, *Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today*, SAFECode, (2ª ed.) (8 de febrero de 2011), *disponible en* https://www.safecode.org/wp- content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf.
[39] Ericsson, *Informe de movilidad de Ericsson: On the Pulse of the Networked Society*, (Nov. 2016), https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november- 2016.pdf.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Además, este ámbito del ecosistema no está compuesto únicamente por dispositivos modernos. Hay muchos servidores, ordenadores de sobremesa, portátiles y teléfonos móviles heredados que se utilizan hoy en día, y así será en un futuro previsible. Los dispositivos heredados ya no cuentan con el apoyo de sus fabricantes, por lo que sus vulnerabilidades no pueden abordarse fácilmente. [40] Para empeorar las cosas, las herramientas de ataque para estos dispositivos o sus componentes de código vulnerables siguen estando ampliamente disponibles.

Por último, un alto porcentaje de sistemas informáticos personales en Internet utilizan software pirata; las estadísticas de una asociación del sector para 2015 oscilaban entre el 17% en Estados Unidos, el 70% en China y el 84% en Indonesia. [41] Los fabricantes suelen restringir la distribución de parches de seguridad solo a los sistemas que ejecutan software adquirido legalmente, por lo que estos sistemas no pueden estar protegidos contra las vulnerabilidades conocidas. Aunque no se puede esperar razonablemente que los vendedores proporcionen soporte para el software sin licencia, estos sistemas desprotegidos proporcionan otra clase de objetivos fáciles para los actores maliciosos, y subraya la naturaleza internacional de este desafío.

Los dispositivos inseguros no suelen ser el resultado de las limitaciones de la tecnología subyacente. Aunque imperfectas, cuando se aplican correctamente, las mejores prácticas actuales son bastante eficaces, dan lugar a dispositivos razonablemente seguros en el momento de su entrega e incluyen herramientas para mantener ese nivel de seguridad durante todo el ciclo de vida del dispositivo. Los sectores comerciales que han adoptado estas prácticas, como los desarrolladores de sistemas operativos, han demostrado mejoras significativas en la seguridad y la resistencia. [42] Desgraciadamente, estas prácticas de seguridad se aplican de forma incoherente. Muchos productos se envían con errores conocidos, no incluyen un mecanismo de actualización y/o no siguen las mejores prácticas actuales para el acceso administrativo.

Parte de este reto puede abordarse con una mayor concienciación y educación. Algunos desarrolladores de productos no saben cómo aprovechar las herramientas disponibles actualmente para el desarrollo de productos seguros. Los desarrolladores de productos de tecnología operativa comprenden su línea de productos (por *ejemplo*, frigoríficos), pero pueden no entender los requisitos básicos de seguridad para la conectividad de red de sus productos. Los clientes empresariales toman decisiones de compra sin tener en cuenta los costes del ciclo de vida completo, así como las externalidades de tener una red insegura. Los consumidores finales pueden carecer de las herramientas necesarias para entender cómo ciertas características del producto les protegen de los riesgos de seguridad o cómo sus dispositivos pueden tener un impacto negativo en el ecosistema.

Los incentivos del mercado parecen exacerbar el problema. Los desarrolladores de productos priorizan el tiempo de comercialización y la funcionalidad innovadora sobre la seguridad y la resistencia. Las características de seguridad no se entienden ni se comunican fácilmente al consumidor, lo que dificulta la generación de demanda.

---

[40] Por ejemplo, Microsoft dejó de dar soporte a Windows XP, de doce años de antigüedad, en abril de 2014. Dos años después, entre el 7,4 y el 10,9% de todos los ordenadores de sobremesa seguían ejecutando XP y fueron descritos como "blancos fáciles para que los ciberdelincuentes los ataquen." John Zorabedian, *Millions of People Are Still Running Windows XP*, Naked Security (11 de abril de 2016), https://nakedsecurity.sophos.com/2016/04/11/millions-of-people-are-still-running-windows-xp/.

[41] *Véase BSA* | The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey*, (mayo de 2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[42] *Véase* Steven J. Vaughan-Nichols, *Security 2014: The Holes Are in the Apps, not the Operating Systems*, ZDNet (28 de febrero de 2014, 19:46 GMT), http://www.zdnet.com/article/security-2014-the-holes-are-in-the-apps-not-the- operating-systems/.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Visión del futuro de los dispositivos de borde

Los amplios avances en el ámbito técnico de los dispositivos de borde son posibles y esenciales si queremos construir un ecosistema de Internet y comunicaciones más resistente. Para que sean efectivos, estos avances deben ser globales, ya que la mayoría de los dispositivos de Internet se encuentran fuera de Estados Unidos. Esta acción global requerirá que las normas y prácticas de seguridad aceptadas a nivel mundial sean sólidas, ampliamente comprendidas y aplicadas de forma ubicua. Dichas normas deben ser flexibles, estar debidamente programadas, ser abiertas, ser voluntarias y estar impulsadas por la industria.

Los dispositivos deben ser capaces de resistir los ataques a lo largo de su ciclo de vida: en el momento del envío, durante el uso y hasta el final de su vida útil. Para ello, la seguridad debe convertirse en un requisito principal de diseño. Los proveedores no deben enviar dispositivos con fallos de seguridad graves conocidos, deben incluir un mecanismo de actualización seguro y deben seguir las mejores prácticas actuales (por *ejemplo*, no codificar contraseñas, desactivar funciones de software que no sean críticas para el funcionamiento) para la configuración y administración del sistema.
Los vendedores deben revelar a los clientes la duración mínima del soporte, y los fabricantes de dispositivos deben mantener los servicios de actualización seguros durante la duración prometida. [43]

Las raíces de confianza del hardware y las tecnologías de ejecución de confianza son ahora un componente de muchas plataformas informáticas disponibles en el mercado. Los productos del futuro tendrán que aprovechar estas tecnologías para demostrar su autenticidad e integridad en el momento de la implantación inicial y durante todo el periodo de uso. Las técnicas modernas de desarrollo se basan en una combinación de componentes de código abierto y comerciales. Para satisfacer las futuras demandas de seguridad, estos componentes deben ser rastreables a lo largo de la cadena de suministro y ofrecer mayores garantías.

Tales avances requerirán pasos significativos en la concienciación y educación de los desarrolladores de productos. Todos los desarrolladores de productos deben estar equipados con los conocimientos y habilidades necesarios para aplicar las herramientas disponibles para el desarrollo de productos seguros. Los kits de herramientas y los componentes utilizados por estos proveedores deben reflejar las preocupaciones de seguridad para lograr la escala y mantener el ritmo de una fuerza de trabajo de desarrolladores cambiante, y las asociaciones y consorcios que impulsan la tecnología estandarizada deben capacitar a los desarrolladores para tomar y comunicar las decisiones de seguridad. Mientras tanto, los desarrolladores de productos de tecnología operativa deben añadir los requisitos básicos de seguridad a sus conocimientos y habilidades específicos del producto. Al mismo tiempo, los clientes deben estar equipados con conocimientos e información suficientes para seleccionar productos diseñados para ser seguros en sus entornos, y deben ser conscientes de los riesgos que presentan todos los dispositivos, incluidos los heredados.

Por último, los incentivos del mercado tendrán que ajustarse a estos avances en materia de seguridad, de modo que se recompense a los desarrolladores de productos que den la misma prioridad a la seguridad y la resistencia que al tiempo de comercialización y la funcionalidad innovadora. Unas señales claras sobre la seguridad y la resistencia de los productos que sean accesibles a los clientes ayudarán a mejorar estos incentivos. Sin embargo, la propuesta de valor para mejorar la seguridad comenzará probablemente en el entorno empresarial debido a sus economías de escala; una vez que exista una postura de seguridad generalmente aceptada en una clase de producto determinada, es probable que pocos fabricantes la ignoren.

[43] *Véase, por ejemplo,* NTIA's Multistakeholder Process on Internet of Things Security Upgradability and Patching - Communicating Upgradability and Improving Transparency Working Group, *Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, (14 de julio de 2017), https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-_ntia_multistakeholder_process.pdf (ayudar a los fabricantes a compartir detalles sobre las actualizaciones de seguridad con los consumidores, y dar a los consumidores las herramientas para saber qué buscar).

Redes domésticas y de pequeñas empresas: Estado actual

Las redes domésticas y de pequeñas empresas son cada vez más complejas. Los dispositivos informáticos tradicionales interactúan con la nube y otros proveedores de servicios para dar soporte a un conjunto cada vez mayor de aplicaciones empresariales y personales. Los dispositivos IoT ya están proliferando en gran número en los hogares de los consumidores, desde dispositivos de automatización del hogar como luces, abridores de puertas de garaje y termostatos, hasta electrodomésticos conectados y monitores personales de salud y fitness. Esta proliferación se da también en las pequeñas empresas, donde los empresarios y directivos pueden querer beneficiarse de la tecnología disponible, pero carecen de un administrador o de estrategias o políticas informáticas concertadas. Según todas las estimaciones, se espera que el número de dispositivos de consumo conectados crezca.

Desgraciadamente, esta área de crecimiento es también un área en la que la seguridad presenta graves carencias. La gran mayoría de los usuarios domésticos y de pequeñas empresas no son conscientes de los riesgos de ciberseguridad, y muchos no toman las medidas de seguridad más básicas cuando conectan dispositivos a sus redes. Las decisiones relevantes para la seguridad pueden tomarse sin la participación o el conocimiento del cliente si el dispositivo es instalado y configurado por otra persona en su nombre o si el dispositivo utiliza una red distinta de la propia del consumidor (por ejemplo, una red celular). Mientras tanto, el intercambio de información sobre amenazas es un reto para las pequeñas empresas, que normalmente carecen de los recursos de las grandes organizaciones para recibir y procesar la información sobre amenazas.

Al igual que en las áreas detalladas anteriormente, en general existen muchas herramientas para mitigar el riesgo de ciberseguridad, pero no es realista esperar que la población en general sea capaz de navegar por el complejo entorno de seguridad. Las pequeñas empresas y los consumidores pueden ser víctimas de ataques DDoS -a menudo a cambio de un rescate para que cesen los ataques-, así como anfitriones involuntarios de dispositivos utilizados en una red de bots. Los productos para redes domésticas no suelen estar diseñados de forma que permitan a los usuarios domésticos segmentar fácilmente las redes o configurar las políticas de seguridad. Muchos usuarios domésticos dependen de dispositivos heredados o de sistemas sin licencia. Además, cuando el dispositivo de un usuario doméstico pasa a formar parte de una red de bots, a menudo es difícil para el proveedor de la red saber qué dispositivo está transmitiendo, porque la función NAT, que permite a los usuarios domésticos compartir una única dirección IPv4 entre numerosos dispositivos detrás de un router doméstico, oculta qué dispositivo está siendo explotado. [44]

En el mercado doméstico y de la pequeña empresa, la mayoría de los dispositivos domésticos no están gestionados y, por tanto, es poco probable que se actualicen manualmente, si no se dispone de funciones de actualización automática. Los dispositivos de los consumidores suelen venir con software obsoleto que contiene vulnerabilidades conocidas o contraseñas administrativas codificadas. Los usuarios típicos pueden no ser capaces de determinar si el software del dispositivo está actualizado o si incluso tiene un mecanismo para las actualizaciones de software; muchos dispositivos de consumo no lo tienen. Es posible que el usuario típico ni siquiera sea consciente de la importancia de este aspecto y que no tenga acceso a información sustancial sobre el software de un determinado dispositivo.

Incluso si la red del hogar o de la pequeña empresa está bien diseñada y cuenta con fuertes controles de seguridad, es probable que algunos de los dispositivos soportados sean móviles y se conecten a múltiples redes durante un día normal. Estas redes pueden no estar tan bien gestionadas, y los dispositivos pueden verse comprometidos durante su estancia en la red exterior. Estos dispositivos suponen un riesgo adicional para la ciberseguridad, ya que permiten la introducción de código malicioso al tiempo que eluden los controles locales.

Por lo general, los usuarios domésticos y de pequeñas empresas no tienen fácil acceso a la información que necesitan para seleccionar productos seguros, y no suelen tener herramientas para gestionar los productos que tienen. Aunque

[44] También observamos que la tecnología NAT ofrece algunas ventajas de seguridad al limitar el acceso del tráfico entrante a puntos finales específicos. Esto impide (pero no elimina por completo) la amenaza de las herramientas automatizadas de exploración e infección.

Las puertas de enlace de las empresas tienen más probabilidades de ofrecer ofertas de seguridad integradas, pero es poco probable que los usuarios domésticos tengan acceso al mismo nivel de servicio y, en el caso de los que sí lo tienen, muchos no son conscientes de las ofertas de seguridad ni de la razón por la que deben implementarse esos servicios. Las medidas de seguridad fundamentales, como cambiar la contraseña de un dispositivo de la contraseña por defecto o activar el cifrado seguro, a menudo están fuera del conocimiento o las capacidades de los consumidores. En algunos casos, la aplicación deficiente de estos requisitos puede frustrar los esfuerzos de los usuarios por aplicar estas prácticas básicas.

Existe la preocupación de que los consumidores no paguen más por dispositivos con mayor seguridad. [45] La realidad es que, por lo general, las experiencias de los consumidores no se ven directamente afectadas por los compromisos de sus dispositivos; de hecho, el consumidor puede no saber nunca que el dispositivo forma parte de una red de bots. Desde la perspectiva del consumidor, la cámara web sigue transmitiendo, o el refrigerador sigue enfriando. Por esta razón, puede ser difícil responsabilizar a los propietarios si sus dispositivos se utilizan en una red de bots. Esta falta de consecuencias claras de la infección supone un reto a la hora de motivar a los consumidores para que tomen medidas para mejorar la seguridad; por ejemplo, para que actualicen los dispositivos que se pueden actualizar.

Visión del futuro de las redes domésticas y de las pequeñas empresas

No es realista esperar que los usuarios domésticos y los propietarios de pequeñas empresas se conviertan en expertos en seguridad. Sin embargo, hay medidas que las partes interesadas de la industria y otros pueden tomar para mejorar la situación. Además de los esfuerzos de concienciación y educación para cambiar el comportamiento de los consumidores, otro enfoque es diseñar los dispositivos teniendo en cuenta el comportamiento de los usuarios. Lo ideal es que los dispositivos comercializados para los consumidores se diseñen con la seguridad incorporada. Los productos de consumo deberían diseñarse de la forma más segura posible, incluir mecanismos de actualización automática seguros y tener pocos o ningún requisito para la gestión de los productos.

Lo ideal es que los consumidores tengan acceso a ofertas comerciales que apliquen las mejores prácticas de seguridad actuales y puedan reconocerlas fácilmente. Los propietarios de pequeñas empresas también podrán adaptar sus compras a sus preocupaciones y obligaciones de seguridad específicas. Serán conscientes de los diversos riesgos relacionados con los dispositivos IoT inseguros, y elegirán dispositivos más seguros.
Las organizaciones sin ánimo de lucro y las entidades comerciales han comenzado a evaluar los productos en cuanto a la privacidad y la seguridad de los datos; [46] esfuerzos como estos aumentarán la concienciación, y a medida que ésta aumente, también debería aumentar el interés de los fabricantes de dispositivos por el desarrollo seguro. Con el tiempo, debería ser más fácil y barato para los fabricantes e integradores adoptar un ciclo de vida de desarrollo seguro.

Aunque los usuarios domésticos no estén especialmente motivados por el temor a que sus dispositivos puedan ser utilizados en una red de bots, pueden sentirse más obligados por la preocupación de que su privacidad, sus datos o el acceso a los servicios puedan verse comprometidos. Muchos dispositivos conectados utilizan servicios en la nube para la gestión y el almacenamiento de la información, lo que tiene implicaciones adicionales para la seguridad y la privacidad. Afortunadamente, muchas de las mismas medidas que tomarían para mejorar su privacidad o la seguridad de sus datos y garantizar un acceso ininterrumpido a los servicios también mitigarían la posibilidad de que sus dispositivos formen parte de una red de bots.

Si se aplican correctamente los incentivos, las fuerzas del mercado pueden desempeñar un papel fundamental en la mejora de la seguridad de los dispositivos. Para que los consumidores adopten de forma generalizada dispositivos más seguros, éstos no pueden costar mucho más que

[45] Bruce Schneier, *Security Economics of the Internet of Things*, Schneier on Security (10 de octubre de 2016, 10:26 AM) https://www.schneier.com/blog/archives/2016/10/security_econom_1.html (última actualización: 17 de octubre de 2016).
[46] Consumer Reports, *Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security*, (6 de marzo de 2017), *disponible en* https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating- products-services-for-privacy-and-data-security/.

dispositivos inseguros. Los productos y servicios de consumo deben diseñarse con protecciones básicas de privacidad y seguridad incorporadas. Unas guías de compra fáciles de comprender y que ofrezcan recomendaciones prácticas, orientadas a las necesidades específicas del hogar y la pequeña empresa, pueden generar las señales de mercado necesarias para recompensar a los desarrolladores y proveedores por invertir en seguridad.

Los routers inteligentes y los cortafuegos deberían utilizarse ampliamente para mitigar los ataques y detectar cuando un dispositivo ha sido comprometido. A medida que los dispositivos IoT de los usuarios domésticos pasen a tener direcciones IPv6 de acceso público, a los proveedores de servicios de Internet les resultará más fácil identificar los dispositivos finales que transmiten tráfico malicioso. Las redes de los usuarios domésticos refuerzan la segmentación de la red virtual. Limitar las capacidades de los dispositivos en función de sus usos previstos -por ejemplo, limitar las actividades de una tostadora conectada a la red únicamente a las actividades necesarias para realizar sus funciones de tostado- limitaría significativamente la capacidad de las redes de bots para capturar dispositivos domésticos. Un descenso global en el uso doméstico de productos heredados y de software pirata también limitaría enormemente las oportunidades de los autores de botnets.

Los usuarios domésticos deben ser capaces de identificar los dispositivos de sus redes que aumentan su riesgo de ciberseguridad. Se está investigando y desarrollando para ayudar a los consumidores preocupados por la seguridad a gestionar mejor sus redes. En 2017, el Reto del Inspector Doméstico del IoT de la Comisión Federal de Comercio (FTC) concedió su primer premio a una propuesta de herramienta basada en una aplicación móvil que ayudaría a los usuarios a gestionar los dispositivos del IoT en sus hogares. La aplicación señalaría los dispositivos con software desactualizado y otras vulnerabilidades comunes y proporcionaría instrucciones sobre cómo actualizar el software de cada dispositivo y corregir otras vulnerabilidades. [47]

La educación de los consumidores tendrá que ser más eficaz, incluso si los dispositivos están mejor diseñados para el nivel de habilidad esperado de los consumidores. Mientras tanto, existe una oportunidad para que una nueva mano de obra apoye las necesidades de los consumidores y las pequeñas empresas en materia de redes; esta función podría convertirse en una nueva vocación, más parecida a la de los electricistas que a la de los ingenieros eléctricos, con la formación adecuada. Las industrias de redes y dispositivos también pueden facilitar y abaratar la asistencia mediante la estandarización y la coordinación.

Gobernanza, política y coordinación

Dado que los ataques automatizados y distribuidos en la Internet global son un problema que afecta a todo el ecosistema, la cuestión requerirá la coordinación de soluciones políticas y de gobernanza en todos los sectores. Ningún actor o sector es responsable de abordar estos riesgos por sí solo, y ninguna entidad puede argumentar que estos riesgos son un problema de otros. Por ejemplo, si bien muchas soluciones implican una coordinación activa con los proveedores de servicios de Internet, atribuir la responsabilidad exclusiva al nivel de la red haría que todo el tráfico dependiera de esta capa de conexión para determinar cómo es el tráfico "bueno", obligando a los proveedores de servicios de Internet a decidir qué es lo que está permitido y lo que no en Internet. Además, esta toma de decisiones de los ISP bloquearía invariablemente el tráfico que de hecho es "bueno" y pasaría por alto el tráfico que debería bloquearse; el tráfico codificado agravaría el problema.

Dada la naturaleza en red de los riesgos, es necesaria una verdadera coordinación para comprender plenamente el problema e identificar las vías de solución. Aunque los sectores de las tecnologías de la información y de las comunicaciones trabajan activamente para comprender los riesgos de seguridad, a algunos sectores les resulta difícil compartir información y coordinarse fuera de sus propios sectores. Algunas entidades se coordinan a nivel nacional o regional, pero es necesario compartir más información sobre las amenazas, las soluciones y su adopción y eficacia a nivel mundial. En

[47] Comisión Federal de Comercio, *IoT Home Inspector Challenge*, https://www.ftc.gov/iot-home-inspector-challenge (última visita el 4 de abril de 2018).

En muchos casos, la falta de claridad en torno a las funciones y responsabilidades ha impedido la acción colectiva, lo que ha provocado fallos en la seguridad.

Algunos gobiernos se basan en regulaciones demasiado específicas que rápidamente quedan obsoletas, obstaculizan la innovación y limitan el beneficio de los consumidores en sectores dinámicos. Los requisitos de cumplimiento, o la imposición de normativas específicas, pueden abordar algunos riesgos, pero pueden conllevar una carga mayor y seguir dejando el ecosistema más amplio inseguro o enviando la señal de que el cumplimiento de la normativa es suficiente y no el mínimo necesario. El panorama normativo se complica aún más por la regulación estatal o local de los dispositivos de borde, la tecnología operativa y la infraestructura. Las soluciones específicas para determinados países o jurisdicciones ponen en riesgo la naturaleza global de un ecosistema en el que tanto los bits como los productos fluyen con relativa facilidad, y pueden poner en desventaja a los innovadores locales.

Este problema se agrava aún más por la naturaleza transversal de la tecnología en red. Los límites se han difuminado entre la tecnología de consumo, las herramientas y dispositivos de grado empresarial de los que dependen las organizaciones y la tecnología de seguridad crítica de la que pueden depender vidas. El mismo hardware y software puede utilizarse en todo el ecosistema. Los servicios de infraestructura clave pueden ser utilizados tanto por una red de videojuegos como por la red corporativa de una empresa.

En el ámbito de la aplicación de la ley, la cooperación de la industria en el desmantelamiento de las redes de bots está mejorando, pero todavía no es habitual. Los recientes desmantelamientos de botnets que han tenido éxito han implicado una amplia colaboración con la industria en los casos de, por ejemplo, Kelihos, Gameover Zeus y Coreflood. La colaboración activa entre las fuerzas de seguridad y el sector privado ha permitido la interrupción a través de la incautación de activos clave de mando y control. En Estados Unidos, en 2016, se modificó la Regla Federal de Procedimiento Penal 41(b)(6) para abordar los desafíos únicos en la investigación de la actividad de las redes de bots, aclarando que los tribunales pueden emitir órdenes que autoricen el registro de múltiples ordenadores cuando los ordenadores identificados se encuentran en múltiples distritos judiciales. Además, la capacidad de las fuerzas de seguridad federales para obtener mandatos civiles -que ha sido indispensable en anteriores desmantelamientos de botnets- se limita a los casos que incluyen elementos de intervención telefónica o ciertos tipos de fraude. El desmantelamiento de botnets de forma segura es un proceso largo y laborioso. Además, la aplicación de la ley se enfrenta a los retos de identificar y perseguir a los actores maliciosos responsables de las redes de bots, especialmente a los que operan fuera de Estados Unidos.

Visión para el futuro de la gobernanza, la política y la coordinación

En el futuro, los compradores -ya sean consumidores finales o empresas sofisticadas- deberán ser más capaces de entender los riesgos y las propiedades de seguridad de los dispositivos conectados. Se necesitan enfoques para la IO y los dispositivos informáticos que ayuden no solo a promover la concienciación de los consumidores, sino también a impulsar el mercado, aumentando la adopción general y el uso de mejores prácticas de ciberseguridad por parte de los fabricantes de dispositivos. Dicho esto, el riesgo de seguridad evoluciona rápidamente; lo que hoy se considera seguro puede no serlo mañana, y es poco probable que lo sea dentro de una década. Las soluciones de transparencia del mercado pueden ayudar a los compradores a tomar buenas decisiones, pero también deben tener en cuenta el contexto y la escala temporal del ciclo de vida del producto. Las instituciones que han confiado en enfoques que tradicionalmente reflejaban un riesgo estático, como los requisitos de compra o los seguros, se adaptarán para reflejar la naturaleza evolutiva del riesgo de ciberseguridad. La mejora de la transparencia sobre los componentes de software y hardware de los sistemas ayudará, al igual que los incentivos adecuados para comprender los riesgos relevantes para un contexto determinado y para el ecosistema en su conjunto.

Los actores de la infraestructura compartirán y analizarán mejor los datos para fomentar un conocimiento compartido de las reputaciones en todo el ecosistema, y evaluarán la forma en que los socios de la red están abordando los riesgos de una manera evolutiva, eficiente y descentralizada. Los mecanismos de intercambio de información deben basarse en los

mecanismos y comunidades de múltiples partes interesadas, creando nuevas oportunidades para comprometerse a nivel local y global.

A medida que evolucionan las amenazas distribuidas, pueden ser necesarias nuevas normas, directrices y métricas para responder a preguntas nuevas y emergentes como: ¿Cómo pueden las terceras partes evaluar mejor los productos para los beneficios de los consumidores de una manera lo suficientemente ágil como para mantenerse al día con las prácticas de seguridad que evolucionan rápidamente? ¿Qué métricas y visibilidad de las prácticas de gestión de la red pueden informarnos sobre la inversión en infraestructura? Unas expectativas de seguridad más formalizadas pero adaptables nos permitirán introducir cierta responsabilidad en las prácticas de seguridad. Mecanismos como los marcos voluntarios pueden contribuir tanto a crear incentivos que motiven un diseño más seguro como a responsabilizar a quienes no tengan en cuenta la seguridad ni inviertan en dispositivos seguros. Cualquier mecanismo de responsabilidad debería recompensar a quienes toman buenas decisiones basadas en el riesgo, reconociendo al mismo tiempo que no existe la seguridad perfecta.

Para hacer frente a toda esta gama de amenazas, todas las partes interesadas, tanto nacionales como internacionales, deben abordar en mayor medida los ataques automatizados y distribuidos. En esencia, esto implica reducir el número de dispositivos no seguros con acceso a Internet para mantener las redes de bots en un tamaño manejable, y desarrollar mecanismos para compartir información sobre los sistemas comprometidos y las tendencias de ataque emergentes hacia arriba y abajo de la pila de la red a la parte (o partes) en la mejor posición para responder a la amenaza.

Dado que el despliegue de la tecnología es verdaderamente transnacional y la información fluye a través de las fronteras internacionales, nada de esto puede lograrse sin la colaboración internacional. En el ámbito internacional, el gobierno de EE.UU. defiende firmemente los enfoques dirigidos por la industria y las normas voluntarias basadas en el consenso. Tal y como se indica en el informe del NSTAC, las soluciones dependen tanto de las normas como de la innovación en la capa de infraestructura de la red e Internet. Aunque existe una variedad de normas, marcos y mejores prácticas pertinentes, no se aprovechan plenamente en todo el mundo.

Los gobiernos pueden influir de forma constructiva en el desarrollo de productos más seguros mediante medidas como el apoyo a normas abiertas, voluntarias e impulsadas por la industria, y tomando sus propias decisiones de adquisición de tecnología y dispositivos de forma que se creen incentivos de mercado para los productos más seguros.
La seguridad también puede fomentarse mediante un mayor compromiso de las partes interesadas entre las comunidades de lucha contra el abuso y de infraestructura de red global, así como entre los elementos de ciberseguridad y de tecnología operativa de las industrias que no se han centrado tradicionalmente en las TI (por *ejemplo,* servicios públicos o dispositivos médicos). Por ejemplo, el compromiso operativo y de múltiples partes interesadas relacionado con los recursos de Internet utilizados por los gestores de botnets para el mando y el control es fundamental para la señalización de amenazas para la gestión de redes y la detección de botnets. Estados Unidos debería aumentar su compromiso internacional en este ámbito, en particular con los países que ya son activos en esta cuestión.

Además, la industria y las fuerzas de seguridad deben trabajar para encontrar formas de coordinarse más a menudo y antes para detectar y prevenir la actividad de las amenazas, y en la gestión de los incidentes que se produzcan. Las nuevas herramientas y procesos pueden mejorar el intercambio de información entre los organismos policiales internacionales. Las fuerzas del orden y los grupos de la industria deberían comunicarse más eficazmente sobre lo que se necesita para desbaratar con éxito las redes maliciosas y perseguir a los actores que están detrás de ellas, sin dejar de tener en cuenta las cuestiones de privacidad. Las políticas de protección de datos, tanto en Estados Unidos como a nivel internacional, no deberían perturbar las herramientas existentes, como la base de datos WHOIS de propiedad de dominios, ampliamente utilizada.

Panorama jurídico

Algunas partes interesadas destacaron la importancia de minimizar la incertidumbre y el riesgo legal para fomentar la colaboración del sector privado con las fuerzas del orden, un mayor intercambio de información, la divulgación de vulnerabilidades y la capacidad de llevar a cabo contramedidas eficaces. Muchos también hicieron hincapié en la necesidad de armonizar los enfoques legales en todos los sectores para evitar un mosaico de leyes que podría obstaculizar el mercado de la IO.

Ya se están realizando esfuerzos para mejorar las relaciones entre el sector público y el privado. El Centro Nacional de Integración de la Ciberseguridad y las Comunicaciones (NCCIC) del DHS sirve como lugar central donde un conjunto diverso de socios del sector privado y del gobierno involucrados en la ciberseguridad coordinan sus esfuerzos,[48] incluyendo el intercambio de información, la colaboración y la asistencia técnica. [49] La legislación federal ya incluye una estructura para abordar parte de la incertidumbre y el riesgo legal. La Ley de Intercambio de Información sobre Ciberseguridad de 2015 (CISA, por sus siglas en inglés), por ejemplo, concede protección de la responsabilidad y otras protecciones legales -como protecciones antimonopolio, excepciones a las leyes de divulgación y a ciertos usos reglamentarios, y protecciones de las renuncias a los privilegios- a las entidades privadas que comparten indicadores de ciberamenazas y medidas defensivas en cumplimiento de la Ley. [50] La CISA designa al NCCIC como eje central para compartir indicadores de ciberamenazas y medidas defensivas con el gobierno federal. [51] Estas capacidades de ciberseguridad del NCCIC y las protecciones legales de la CISA se aplican a la ciberseguridad de la IO de la misma manera que se aplican a la ciberseguridad en general. Por otra parte, nada en la CISA impide que las entidades privadas compartan de forma sólida con las fuerzas del orden como parte del curso normal de una investigación criminal; de hecho, la CISA autoriza a compartir indicadores de ciberamenazas y medidas defensivas con las fuerzas del orden -o con cualquier otra entidad federal- y, además, su protección de responsabilidad se aplica cuando dicha información se comparte con las fuerzas del orden en determinadas circunstancias.

Muchas partes interesadas también destacaron la importancia de los incentivos del mercado para asegurar los dispositivos de la IO. Algunos se refirieron a la posibilidad de que un régimen de responsabilidad basado en las mejores prácticas y normas comunes pueda mejorar la responsabilidad en la seguridad de los dispositivos de la IO. Aunque este informe no realiza un análisis exhaustivo de la responsabilidad relacionada con la seguridad de los dispositivos de la IO, esperamos que esta cuestión siga suscitando interés a medida que aumente el uso de los dispositivos conectados -dispositivos que pueden tener un impacto en el mundo físico- y surjan preguntas sobre los daños, las cuestiones de privacidad, la protección del consumidor, las cadenas causales, la gestión de riesgos y las posibles acciones estatales y judiciales. La responsabilidad es un ámbito jurídico complejo, al igual que el mercado emergente del IoT, y hay que tener cuidado para evitar requisitos de cumplimiento estáticos e ineficaces, especialmente en medio de un panorama dinámico de ciberseguridad. Hay que invertir para abordar el riesgo mediante prácticas innovadoras, y con las partes interesadas comprometidas en la coordinación intersectorial. La presión para abordar directamente esta cuestión aumentará si la inseguridad jurídica es endémica y persistente.

Algunas partes interesadas señalaron que cualquier nuevo régimen legal o reglamentario puede tener efectosnegativos no deseados en la industria de las tecnologías de la información si no se incluyen orientaciones claras sobre lo que un proveedor puede hacer para limitar su exposición. Sin embargo, los defensores advierten del peligro de una protección general de la responsabilidad sin que haya beneficios sociales claros derivados de la mejora de los procesos de seguridad. Algunas partes interesadas, incluidas las organizaciones de la sociedad civil, pidieron más claridad sobre cómo se aplican las leyes existentes en varias jurisdicciones en este ámbito, cómo pueden o deben afectar estas leyes a las diferentes partes interesadas a lo largo de las cadenas de suministro y distribución, y cómo abordar adecuadamente los daños. A medida que esta área continúa evolucionando, es vital que el gobierno federal comprenda mejor la interacción entre la responsabilidad y los incentivos del mercado, así como la forma en que cualquier cambio propuesto podría alterar esa dinámica. Hay que tener cuidado para garantizar que nuestras leyes de responsabilidad beneficien a los consumidores, protejan a las partes interesadas cuando corresponda y eviten frenar la innovación en el entorno digital actual. Mientras continúa la colaboración entre los sectores público y privado en este ámbito, el gobierno federal

debe seguir vigilando si la protección de la responsabilidad relacionada con el intercambio de información es suficiente en el entorno actual para hacer frente eficazmente a las amenazas actuales y a las nuevas.

III. Objetivos y acciones

Estos objetivos y acciones pretenden presentar una cartera de acciones que se apoyan mutuamente y que, de aplicarse, mejorarían drásticamente la resiliencia del ecosistema. Las acciones recomendadas incluyen actividades en curso que deberían continuar o ampliarse, así como nuevas iniciativas. Ninguna inversión o actividad por sí sola puede mitigar todas las amenazas, pero los debates organizados y los comentarios de las partes interesadas nos permitirán seguir evaluando y priorizando estas actividades en función de la rentabilidad esperada de la inversión y de la capacidad de influir de forma mensurable en la resiliencia del ecosistema. Esperamos que las partes interesadas de todo el ecosistema colaboren con el gobierno para poner en práctica las actividades propuestas, aprovechen las oportunidades de apoyo y liderazgo y eliminen los impedimentos para su aplicación.

Objetivo 1: Identificar un camino claro hacia un mercado tecnológico adaptable, sostenible y seguro.

Para mejorar la resistencia del ecosistema de Internet y las comunicaciones, es fundamental que nuestro mercado tecnológico apoye y recompense el desarrollo, la adopción y la evolución continuos de tecnologías y procesos de seguridad innovadores. Cuando los incentivos del mercado animan a los fabricantes a presentar innovaciones en materia de seguridad como complemento equilibrado de la funcionalidad y el rendimiento, aumenta la adopción de herramientas y procesos que dan lugar a productos más seguros. A medida que estas características de seguridad se hacen más populares, el aumento de la demanda impulsará nuevas investigaciones. A medida que estas herramientas se perfeccionan, resulta más barato para los fabricantes, integradores y propietarios/operadores de sistemas adoptar los componentes de un ciclo de vida de desarrollo seguro, lo que anima a más fabricantes a diferenciar sus productos en función de la calidad de sus características de seguridad y permite así una mayor competencia. En esta sección se identifican las medidas que pueden adoptar las principales partes interesadas para establecer un mercado tecnológico adaptable, sostenible y seguro.

Acción 1.1 Utilizando procesos inclusivos dirigidos por la industria, establecer líneas de base de capacidades de la IO aplicables internacionalmente que apoyen la seguridad del ciclo de vida de las aplicaciones domésticas e industriales, basadas en normas internacionales voluntarias e impulsadas por la industria.

[48] *Véase* 6 U.S.C. § 148.
[49] *Id.* § 148(c).
[50] *Véase la* Ley de Asignaciones Consolidadas, 2016, División N - Ley de Ciberseguridad de 2015 (Pub. L. No. 114-113, 129 Stat. 2242) (codificada en 6 U.S.C. §§ 1501-1510).
[51] La CISA proporciona una serie de protecciones legales para los indicadores de amenazas cibernéticas y las medidas defensivas que se comparten con una entidad federal de acuerdo con el estatuto. Por ejemplo, ofrece protección contra la responsabilidad antimonopolio (6 U.S.C. § 1503(e)); leyes federales y estatales de divulgación (6 U.S.C. §§ 1504(d)(3) y 1503(d)(4)(B)); renuncia a los privilegios (6 U.S.C. § 1504(d)(1)); y el uso reglamentario federal y estatal (6 U.S.C. §§ 1503(d)(4)(C) y 1504(d)(5)(D)). Cuando los indicadores de amenazas cibernéticas y las medidas defensivas se comparten con el NCCIC a través de la capacidad del gobierno federal y el proceso operado por el DHS, dicho intercambio también recibe protecciones adicionales de responsabilidad. 6 U.S.C. § 1504(c)(1)(B). Estas protecciones de responsabilidad adicionales también están disponibles para compartir con otras entidades federales en circunstancias limitadas. *Véase 6 U.S.C. § 1504(c*)(1)(B)(i) y (ii).

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Los estándares de seguridad, las líneas de base y las mejores prácticas han evolucionado con el tiempo para los dispositivos informáticos tradicionales, lo que ha aumentado el coste de montar redes de bots con estos dispositivos. El rápido aumento del despliegue de dispositivos IoT inseguros ha tenido el pernicioso efecto secundario de permitir el desarrollo rentable de redes de bots extremadamente grandes y ampliamente distribuidas. Por ejemplo, las redes de bots Mirai han comprometido cientos de miles de dispositivos como resultado de las contraseñas administrativas codificadas. Más recientemente, la red de bots Reaper ha puesto en peligro dispositivos al atacar vulnerabilidades de software bien conocidas. Aunque existen medidas de mitigación, muchos de los dispositivos afectados no se pueden parchear. Dado que las contraseñas no se pueden cambiar y las vulnerabilidades no se pueden parchear, estos dispositivos seguirán siendo vulnerables durante todo su ciclo de vida. Estas vulnerabilidades podrían mitigarse en los futuros sistemas de IoT si se aplicaran a los dispositivos de IoT las mejores prácticas de seguridad actuales para los dispositivos informáticos tradicionales, como configuraciones seguras por defecto y mecanismos eficaces de actualización de software.

El impacto de las anteriores redes de bots se ha mitigado con medidas adoptadas por los proveedores de infraestructuras, como los proveedores de servicios de Internet -principalmente acciones de cese y desistimiento y la absorción del exceso de tráfico-, pero las mitigaciones anteriores eran principalmente de naturaleza reactiva, y el aumento exponencial de los dispositivos y sistemas de Internet de las Cosas indica que estas estrategias tradicionales de mitigación tienen un rendimiento decreciente. El ecosistema debe ser más resistente a las amenazas distribuidas, empezando por un enfoque proactivo y centrado en la reducción de las vulnerabilidades conocidas de los dispositivos conectados a Internet a lo largo de su ciclo de vida.

Las líneas de base de las capacidades de seguridad basadas en el rendimiento -que identifican conjuntos de normas, especificaciones y mecanismos de seguridad voluntarios que representan la combinación de las mejores prácticas para la seguridad del ciclo de vida para un entorno de amenaza concreto- son necesarias para acelerar el desarrollo y el despliegue de los dispositivos y sistemas del IoT que son menos vulnerables a las amenazas a lo largo de su ciclo de vida. [52] Por ejemplo, una línea de base para entornos domésticos podría incluir mecanismos de actualización seguros, como la aplicación automática de parches de seguridad y configuraciones seguras por defecto, que minimicen la necesidad de la acción del usuario. Una línea de base de seguridad para una industria podría suponer un personal de seguridad dedicado y con conocimientos que utilice procesos como las actualizaciones gestionadas de forma centralizada. Estas líneas de base deben ser lo suficientemente flexibles como para aplicarse cuando los dispositivos IoT son tanto un producto como un servicio (es *decir,* cuando los servicios en la nube son parte integral del funcionamiento del producto) y cuando las capacidades de seguridad están distribuidas en un sistema de dispositivos IoT.

Al desarrollar estas líneas de base, debemos equilibrar la inversión en los requisitos de las líneas de base con los costes de no utilizarlas (es *decir,* los costes para los posibles perjudicados, el coste para el fabricante del producto y los costes para otras partes interesadas). Las líneas básicas de capacidad deben ser pragmáticas para garantizar que los fabricantes puedan cumplir los requisitos de forma rentable, al tiempo que ofrecen un claro beneficio al cliente y al ecosistema. Para lograr este equilibrio, estas líneas de base deben desarrollarse con el liderazgo de la industria en colaboración con el cliente previsto (por *ejemplo,* un consorcio que represente a un sector industrial, o grupos de defensa de los consumidores y de la sociedad civil que representen a los usuarios domésticos) y con la contribución y participación activa de los gobiernos, según proceda. El desarrollo colaborativo de líneas de base proporciona a los fabricantes un tiempo de espera y una visión temprana de las expectativas de los clientes, y aumenta la probabilidad de que los productos conformes estén disponibles a tiempo. La participación de los clientes en el desarrollo de la línea de base también puede proporcionar una señal al mercado de que los compradores prefieren los dispositivos de la IO que están diseñados para ser seguros en sus entornos de destino y también permiten la alineación de las actividades de educación que se describen a continuación. A medida que las capacidades especificadas en la línea de base se conviertan en la norma de facto, esto apoyará un mercado sostenible para dispositivos más seguros.

[52] Las normas basadas en el rendimiento describen *lo que* debe lograrse, en lugar de *cómo* lograrlo, reduciendo o eliminando los impactos negativos sobre la innovación.

Para garantizar que los costes de oportunidad de innovación perdidos no sobrepasen el valor de la línea de base, las líneas de base de seguridad de la IO que identifican un pequeño número de capacidades de seguridad flexibles deben imponer restricciones mínimas (si es que hay alguna) en el diseño y la implementación. [53] La especificación de las capacidades en términos de rendimiento en lugar de diseño (es *decir,* un enfoque basado en los resultados en lugar de prescriptivo) ayudará a gestionar los costes asociados a los programas de evaluación correspondientes. Como ventaja añadida de la limitación del conjunto de características, también resulta más práctico para las plataformas de desarrollo comunes incorporar esos conjuntos de características en los componentes de la IO, simplificando el desarrollo de productos conformes.

Una base para las futuras líneas de base

Recientemente se han publicado varias especificaciones que ofrecen, como mínimo, una base sólida para las futuras líneas de base de las capacidades de seguridad del IoT. Estos esfuerzos van desde especificaciones de alto nivel hasta documentos extremadamente detallados y se dirigen a una serie de entornos de aplicación. Ejemplos notables de especificaciones de alto nivel centradas en dispositivos de grado de consumidor, todos publicados desde junio de 2017, incluyen el Marco de Seguridad de IoT de la Alianza de Confianza en Línea,[54] el Estándar Digital (desarrollado por una coalición que incluye a Consumer Reports, Ranking Digital Rights y el Laboratorio de Pruebas Independientes Cibernéticas),[55] y *Secure by Design: Improving the cyber security of consumer Internet of Things56 , del* Departamento de Digital, Cultura, Medios de Comunicación y Deporte del Reino Unido. Un ejemplo de especificación de referencia detallada es el documento *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures,*[57] publicado en noviembre de 2017 por la European Union Agency For Network And Information Security, que identifica 83 medidas técnicas y buenas prácticas de seguridad aplicables a la seguridad de la IO. Otro ejemplo es "Security Tenets for Life Critical Embedded Systems", que fue desarrollado por un grupo de trabajo intersectorial compuesto por miembros de la base industrial de defensa y del sector de las tecnologías de la información. [58]

Acción 1.2 El gobierno federal debe aprovechar las líneas de base de capacidades desarrolladas por la industria, cuando sea apropiado, para establecer líneas de base de capacidades para los dispositivos de la IO en los entornos del gobierno de los Estados Unidos para cumplir con los requisitos federales de seguridad, promover la adopción de líneas de base dirigidas por la industria y acelerar la estandarización internacional.

La acción 1.1 se centra en el desarrollo por parte de la industria de líneas de base de capacidades para los dispositivos de la IO en diferentes entornos de amenaza. Este enfoque plantea múltiples retos, que van desde el desarrollo de múltiples perfiles que compiten entre sí hasta la ausencia de una línea de base para un entorno crítico. Además, cuando los esfuerzos liderados por la industria se centran en el ámbito nacional, puede haber problemas para conseguir la aceptación internacional. El gobierno federal puede acelerar la convergencia en los casos en que existen múltiples líneas de base, impulsar nuevos esfuerzos

[53] Por ejemplo, una línea de base podría especificar un requisito para la gestión de parches desatendidos sin especificar un modelo pull o push, si los parches deben ser encriptados, o el tipo exacto de protección de la integridad aplicada al parche.[54] *Véase* Online Trust Alliance, *Internet of Things*, https://otalliance.org/initiatives/internet-things (última visita el 4 de abril de 2018).

[55] The Digital Standard, *The Standard*, https://www.thedigitalstandard.org/the-standard (visitado por última vez el 4 de abril de 2018). [56] Departamento de Digital, Cultura, Medios de Comunicación y Deporte, *Secure by Design: Improving the cyber security of consumer Internet of Things*, (7 de marzo de 2018), *disponible en* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_. pdf.

[57] Agencia de Seguridad de las Redes y de la Información de la Unión Europea, *Baseline Security Recommendations for Internet of Things in the context of Critical Information Infrastructures*, (20 de noviembre de 2017), *disponible en* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[58] Departamento de Seguridad Nacional de Estados Unidos, *Security Tenets for Life Critical Embedded Systems*, https://www.dhs.gov/publication/security-tenets-lces (publicado por última vez el 12 de enero de 2017).

estableciendo un borrador para el debate en los casos en los que no existe una línea de base, y fomentar la normalización internacional estableciendo líneas de base federales para la IO.

Al establecer líneas de base de las capacidades de seguridad de la IO a nivel federal en coordinación con la industria, la sociedad civil y los socios internacionales, el gobierno federal puede demostrar la practicidad y eficacia de las capacidades especificadas, contribuir a los incentivos del mercado y establecer una base para los programas de evaluación práctica (véanse las acciones 5.1 y 5.2). Este enfoque también garantizará que las líneas de base del gobierno federal reflejen el estado de la técnica y evolucionen a medida que la industria y el mercado evolucionen. El Instituto Nacional de Normas y Tecnología (NIST) es responsable de desarrollar normas y directrices de seguridad de la información, incluidos los requisitos mínimos para los sistemas federales. El NIST debería identificar los requisitos de seguridad para los dispositivos y sistemas de la IO en entornos federales. Cuando existan líneas de base consensuadas por la industria, el NIST debería evaluar su aplicabilidad a los requisitos de seguridad federales y, si procede, desarrollar una norma federal por referencia. Estas líneas de base de la capacidad federal serían similares (y seguirían la progresión de) las líneas de base dirigidas por la industria desarrolladas en la Acción 1.1. Si no se dispone de una línea de base adecuada, el NIST debería buscar socios de la industria para el desarrollo de una línea de base práctica y un borrador para el debate de futuros esfuerzos dirigidos por la industria.

A medida que se demuestre la eficacia de estas líneas de base, el gobierno y la industria de EE.UU. también deberían colaborar con los desarrolladores de normas y especificaciones internacionales voluntarias dirigidas por la industria para establecer normas relevantes a nivel mundial. A medida que vayan surgiendo estas normas y especificaciones, deberán crearse, actualizarse o sustituirse las líneas básicas federales, según proceda.

El lugar de estandarización de estas líneas de base debe seleccionarse cuidadosamente. Las líneas básicas de seguridad y cualquier norma y especificación de apoyo deben desarrollarse en organismos del sector privado que estén abiertos a la participación de todas las partes interesadas, y deben desarrollarse de manera transparente, utilizando procesos equilibrados basados en el consenso, y adoptando un enfoque basado en los resultados -en lugar de en los requisitos- siempre que sea posible. Estas normas basadas en el rendimiento son las más adecuadas para abordar los retos que plantea un espacio tecnológico en rápida evolución, como la IO. Estos procesos no excluyen la participación de los gobiernos, sino que garantizan que los intereses de los gobiernos, la industria, la sociedad civil y los usuarios estén bien representados, y que las soluciones resultantes reflejen el estado del arte en ese espacio tecnológico.
La flexibilidad de estos procesos también permite actualizar las normas a medida que evolucionan la tecnología, las amenazas y las soluciones. La fuerte alineación entre el uso por parte de las empresas de las normas que han ayudado a desarrollar y el apoyo de los gobiernos al desarrollo de estas herramientas facilita la adopción de estas normas a gran escala.

Es importante reconocer que, dada la amplitud del espacio tecnológico, ninguna organización de desarrollo de normas o especificaciones puede desarrollar todas las soluciones. Los gobiernos de todo el mundo deben apoyar la cooperación y la coordinación entre los organismos de normalización y especificación que cuentan con los conocimientos y la experiencia necesarios, y desarrollar productos de acuerdo con los principios expuestos anteriormente, para garantizar soluciones sólidas, oportunas y adecuadas a su finalidad. En Estados Unidos, el NIST debería seguir liderando y coordinando el compromiso de las agencias federales en las actividades de normalización relacionadas, incluyendo el compromiso con el sector privado, explorando una estrategia del gobierno federal en apoyo de las normas internacionales para hacer frente a los desafíos de las botnets y otras amenazas automatizadas y distribuidas.

Las acciones complementarias del gobierno de Estados Unidos y del sector privado podrían mejorar significativamente los impactos de estas líneas básicas federales de capacidades de IoT. El gobierno federal puede utilizar las normas de adquisición y las directrices de contratación para amplificar la señal del mercado exigiendo las capacidades de la(s) línea(s) base (véase

Acción 2.3) y, en su caso, preferir productos que también se ajusten a un determinado sistema de etiquetado del sector privado (véanse las acciones 5.1 y 5.2).

Acción 1.3 Las herramientas y procesos de desarrollo de software para reducir significativamente la incidencia de las vulnerabilidades de seguridad en el software comercial deben ser adoptadas más ampliamente por la industria. El gobierno federal debería colaborar con la industria para fomentar la mejora y la aplicación de estas prácticas y para mejorar la adopción y la responsabilidad del mercado.

Las técnicas habituales de desarrollo de software dan como resultado un software con al menos un fallo por cada 2.000 líneas de código[59], y los sistemas modernos incluyen decenas de millones de líneas de código. Esto implica decenas de miles de errores en un sistema, muchos de los cuales crean vulnerabilidades de seguridad. Los mecanismos de actualización segura (señalados como una importante característica de base en la acción 1.1) permiten a los vendedores corregir estos errores tras un periodo de vulnerabilidad relativamente breve. Sin embargo, evitar por completo estas vulnerabilidades tendría un impacto aún más significativo en términos de reducción del riesgo de seguridad. Aunque es posible desarrollar código con un número muy reducido de errores, cuando la importancia de la misión justifica una reducción significativa de la productividad, el reto consiste en desarrollar mecanismos que produzcan un código significativamente mejor sin reducir indebidamente la productividad.

Un grupo de trabajo interinstitucional (documentado en el Informe Interinstitucional/Interno del NIST [NISTIR] 815160) identificó numerosos enfoques para desarrollar software con menos vulnerabilidades, aplicando tres estrategias básicas:

- Detener las vulnerabilidades antes de que se produzcan, incluyendo métodos mejorados para especificar y construir software;
- Encontrar vulnerabilidades, incluyendo mejores técnicas de prueba y un uso más eficiente de múltiples métodos de prueba; y
- Reducir el impacto de las vulnerabilidades mediante la construcción de arquitecturas más resistentes, de modo que las vulnerabilidades no puedan ser explotadas de manera significativa.

Ya existen herramientas para apoyar estos enfoques[61], y han sido adoptadas por algunas empresas con visión de futuro. [62] Los desarrolladores de software deberían comenzar la transición a estas herramientas inmediatamente, centrándose inicialmente en los productos que presentan el mayor riesgo. El DHS y la FTC también ofrecen recursos para los desarrolladores de software más pequeños. [63]

---

[59] *Véase Coverity Scan,* nota 34 *supra*, en la página 4.

[60] Paul E. Black, Lee Badger, Barbara Guttman y Elizabeth Fong, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*, (Nov. 2016), NIST Interagency/Internal Report No. 8151, *disponible en* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

[61] *Véase, por ejemplo*, *CWE/SANS Top 25 Most Dangerous Software Errors*, SANS Institute, https://www.sans.org/top25- software-errors/ (última actualización: 27 de junio de 2011).

[62] Por ejemplo, el Software Assurance Marketplace (SWAMP) pretende facilitar la comprobación sistemática de la calidad y la seguridad de estas aplicaciones y aportar un cambio transformador al panorama del aseguramiento del software, reduciendo el número de puntos débiles desplegados en el software. Para más información, véase Software Assurance Marketplace, https://continuousassurance.org/ (última visita el 4 de abril de 2018).

[63] El DHS apoyó el desarrollo del SWAMP, que ofrece herramientas de aseguramiento de software basadas en la nube y de código abierto. Para más información, véase Software Assurance Marketplace, *About Swamp*, https://continuousassurance.org/about-us/ (visitado por última vez el 4 de abril de 2018); Comisión Federal de Comercio, *Careful Connections: Building Security in the Internet of Things,* (enero de 2015),

El gobierno federal debería apoyar la adopción de estas herramientas por parte de la industria mediante esfuerzos que mejoren el rendimiento de la inversión o creen incentivos de mercado para los sectores o grupos industriales rezagados, como también recomendó el NSTAC en su informe. El gobierno federal debería promover el desarrollo de herramientas para prácticas de codificación seguras patrocinando o realizando investigaciones específicas (véase la acción 1.4), y patrocinando concursos para cadenas de herramientas seguras (procesos de herramientas múltiples para el desarrollo de software) para demostrar su eficacia y productividad. El gobierno federal también debería trabajar con la industria y la sociedad civil para desarrollar estrategias que faciliten y abaraten la adopción de estos enfoques -incluyendo la educación y la formación que se analizan en detalle más adelante-, teniendo en cuenta los requisitos de las pequeñas empresas, y trabajar con toda la gama de partes interesadas para que dicho proceso sea observable y verificable para terceros.

Por ejemplo, los productos modernos utilizan muchos componentes, bibliotecas y módulos de software, algunos de los cuales pueden estar obsoletos o ser vulnerables y no siempre son seguidos de cerca por los fabricantes en el rápido ciclo de desarrollo. Aunque la noción de transparencia en torno a los componentes de software no es nueva, no se ha logrado un amplio apoyo y adopción. La NTIA debería involucrar a diversas partes interesadas en el examen de las estrategias y políticas necesarias para fomentar un mercado para una mayor transparencia de los componentes de software, incluyendo la identificación y exploración de las barreras de mercado y de otro tipo que puedan inhibir el progreso en este espacio.
Saber qué software se ha incorporado a un producto es un paso fundamental para poder mantenerlo actualizado y mitigar las amenazas cuando surjan.

Acción 1.4 La industria debería acelerar el desarrollo y despliegue de tecnologías innovadoras para la prevención y mitigación de las amenazas distribuidas. En consecuencia, cuando sea pertinente, el gobierno debería priorizar la aplicación de fondos de investigación y desarrollo y los esfuerzos de transición tecnológica para apoyar los avances en la prevención y mitigación de DDoS, así como las tecnologías fundacionales para prevenir la creación de botnets. En su caso, la sociedad civil debería ampliar estos esfuerzos.

El rápido crecimiento de la capacidad de DDoS que ofrecen las redes de bots basadas en el IoT pone en peligro la eficacia de las actuales técnicas de mitigación de DDoS. La investigación y el desarrollo de técnicas que ofrezcan una mitigación más cercana a la fuente, o que aprovechen los nuevos análisis de datos, el aprendizaje automático o la inteligencia artificial (IA), se necesitan urgentemente para adelantarse a los actores maliciosos. Se necesitarán innovaciones para hacer frente a otras actividades maliciosas apoyadas por redes de bots, como el ransomware y la propaganda informática. Para hacer frente a estos y futuros ataques, se necesitarán tecnologías básicas para prevenir, detectar y recuperarse de un compromiso y de la incorporación a una red de bots.

Para mejorar la resistencia del ecosistema, los éxitos en investigación y desarrollo deben ser capitalizados mediante un despliegue agresivo. Las tecnologías innovadoras de los dispositivos, como las raíces de confianza del hardware o los mecanismos mejorados de autenticación de los dispositivos, ofrecen la posibilidad de reforzar considerablemente la seguridad a lo largo del ciclo de vida del producto. Los avances en las herramientas de red, como la Descripción de Uso del Fabricante (MUD), una norma actualmente en desarrollo en el IETF,[64] podrían mejorar la resistencia de la red gestionando las comunicaciones para la seguridad y haciendo una gestión granular de la red

https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections- buildingecurityinternetofthings.pdf.
[64] *Véase* E. Lear, R. Droms y D. Romascanu, *Manufacturer Usage Description Specification (*Draft), Internet Engineering Task Force - Network Working Group, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (última actualización: 19 de abril de 2018).

más barato y más fácil. La adopción acelerada de estas tecnologías innovadoras mejoraría la resistencia del ecosistema, pero la comercialización y adopción de resultados de investigación prometedores para crear productos viables o servicios comercializables es notoriamente difícil. La sociedad civil y los grupos sin ánimo de lucro también pueden amplificar las nuevas plataformas o soluciones, como han hecho la Internet Society y la Global Cyber Alliance en sus respectivas iniciativas de promoción de la seguridad de las rutas,[65,66] y la American Civil Liberties Union en su iniciativa sobre privacidad y tecnología. [67]

Como fuente clave de financiación para la investigación básica en ciberseguridad, el gobierno federal debería apoyar esta acción a través de financiación específica y actividades de transición tecnológica en colaboración. Los departamentos y agencias también patrocinan la investigación aplicada en apoyo de los requisitos de la misión y una variedad de actividades de transición tecnológica. [68] Las agencias deberían dar prioridad al desarrollo y despliegue de innovaciones que aumenten la resistencia del ecosistema y coordinar estas inversiones a través del programa de Investigación y Desarrollo de Redes y Tecnologías de la Información (NITRD). [69] Al igual que con el uso de cualquier técnica de mitigación, deben tomarse medidas para garantizar que estas tecnologías innovadoras no expongan a los consumidores a un riesgo innecesario para su privacidad. Esto puede hacerse mediante las herramientas de evaluación del riesgo para la privacidad descritas en el NISTIR 8062,[70] o mediante una evaluación del impacto sobre la privacidad. [71]

Acción 1.5 El gobierno, la industria y la sociedad civil deben colaborar para garantizar que las mejores prácticas, los marcos y las directrices existentes relevantes para la IO, así como los procedimientos para garantizar la transparencia, se adopten más ampliamente en todo el ecosistema digital. Los riesgos emergentes en el espacio de la IO deben abordarse de forma abierta e inclusiva.

Varios esfuerzos anteriores han producido orientaciones y mejores prácticas relacionadas con las redes de bots y una mejor seguridad del IoT, pero las redes de bots siguen siendo un problema. Por ejemplo, las partes interesadas en el proceso multisectorial de la NTIA sobre la capacidad de actualización y parcheado de la seguridad de la IO desarrollaron un conjunto de documentos que ofrecían soluciones tanto para el lado de la oferta como de la demanda del mercado de consumo de la IO, pero las partes interesadas también hicieron hincapié en el papel compartido en la promoción de estas ideas en toda la comunidad de la IO. [72] Publicar documentos no es suficiente: debemos trabajar para garantizar que se adopten ampliamente en todo el ecosistema. La comunidad de la IO debe trabajar en colaboración para identificar y adoptar las mejores prácticas, los marcos y las directrices existentes que son

[65] *Véase* Internet Society, *MANRS: Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (última visita el 4 de abril de 2018).
[66] *Véase* Global Cyber Alliance, *Quad9: Four Simple Steps to Security, Privacy and Performance*, https://www.globalcyberalliance.org/initiatives/quad9.html (última visita el 4 de abril de 2018).
[67] *Véase* ACLU, *Privacy & Technology,* https://www.aclu.org/issues/privacy-technology (visitado por última vez el 4 de abril de 2018).
[68] El proyecto Distributed Denial of Service Defense del DHS es un ejemplo de este tipo de investigación. *Véase* Departamento de Seguridad Nacional de Estados Unidos, *Distributed Denial of Service Defense*, https://www.dhs.gov/science-and-technology/csd-ddosd (última visita el 4 de abril de 2018). Véase *también* National Science Foundation, *Secure and Trustworthy Cyberspace (SaTC)*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709 (última visita el 4 de abril de 2018).
[69] The Networking and Information Technology Research and Development Program (Programa de investigación y desarrollo en materia de redes y tecnologías de la información), https://www.nitrd.gov/ (visitado por última vez el 4 de abril de 2018).
[70] Sean Brooks, Michael García, Naomi Lefkovitz, Suzanne Lightman y Ellen Nadeau, An *Introduction to Privacy Engineering and Risk Management in Federal Systems, (*enero de 2017), NIST Interagency/Internal Report No. 8062, *disponible en* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[71] Para más información sobre un tipo de evaluación del impacto sobre la privacidad, véase U.S. Department of Homeland Security, *Privacy Impact Assessment Guidance*, https://www.dhs.gov/publication/privacy-impact-assessment-guidance (publicado por última vez el 13 de abril de 2018).
[72] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (actualizado por última vez el 7 de noviembre de 2017).

relevantes para la IO. La comunidad de la IO también debería trabajar para dar a conocer estas mejores prácticas, marcos y directrices. El informe del NSTAC también señalaba esta necesidad, en relación con su recomendación de que la industria debería trabajar con el DHS y el Comercio para acelerar la adopción de directrices de seguridad.

El gobierno federal debería apoyar la adopción generalizada de las mejores prácticas haciendo partícipe a la comunidad para determinar por qué las recomendaciones anteriores no se aplicaron de forma generalizada o no tuvieron éxito, identificar las vías adecuadas para impulsar la aplicación con éxito y centrarse en herramientas y palancas prácticas y probadas. Por ejemplo, las prácticas de desarrollo actuales hacen hincapié en la reutilización de software comercial y de código abierto, que puede estar anticuado o ser vulnerable, pero estos atributos de (in)seguridad quedan ocultos tanto para los desarrolladores como para los clientes. El proceso de múltiples partes interesadas de la NTIA sobre la transparencia de los componentes de software (véase la acción 1.3) puede explorar cómo aumentar las garantías de que no se envían vulnerabilidades conocidas con los productos.

Un problema especialmente molesto que requerirá la aportación de las partes interesadas es la cuestión del código heredado y huérfano, o "software muerto". Las partes interesadas en el proceso de aplicación de parches de la NTIA identificaron la importancia de comunicar el periodo durante el cual se ofrecerían actualizaciones de seguridad, pero no ofrecieron una orientación explícita sobre lo que sucedería cuando ya no se ofrecieran actualizaciones de seguridad. [73] A medida que los bienes duraderos con una larga vida útil estén cada vez más conectados con un código frágil, este problema aumentará. Un experto en seguridad llegó a abogar por que el software abandonado sea de código abierto. [74] Sin embargo, el acceso al código es sólo un obstáculo. Todavía hay que escribir y probar las actualizaciones. Los vendedores en quiebra presentan más problemas si los certificados de firma o los archivos MUD (véase la acción 1.4) están vinculados a los dominios. Un modelo para hacer frente a las externalidades del software insuficientemente soportado procede de la Iniciativa de Infraestructura Central[75] , pero la perspectiva de hacer frente sistemáticamente a los sistemas no mantenidos distribuidos globalmente requerirá la aportación de una amplia gama de partes interesadas.

Las prácticas transparentes y verificables de gestión de activos de software (SAM) pueden ayudar a las empresas a identificar el software que no puede ser parcheado porque las actualizaciones ya no están disponibles o las licencias han caducado. Una vez identificadas, las empresas pueden abordar estas vulnerabilidades sustituyendo los productos o rediseñando las redes para gestionar el riesgo. Las empresas y las administraciones públicas deben adoptar prácticas de SAM basadas en las normas internacionales de adquisición y gestión de activos, así como procedimientos para mitigar los riesgos identificados mediante estas prácticas.

Los esfuerzos complementarios para aumentar la concienciación y educar a los desarrolladores y fabricantes de productos podrían mejorar significativamente el impacto de estas mejores prácticas, marcos y directrices, como se describe en las acciones 5.3, 5.4 y 5.5.

[73] El informe de la FTC sobre las actualizaciones de seguridad de los móviles recomienda que las empresas consideren la posibilidad de divulgar el período mínimo de soporte y las notificaciones antes de que finalice el período de soporte de seguridad. Comisión Federal de Comercio, Actualizaciones de seguridad para móviles*: Understanding the Issues*, (febrero de 2018), https://www.ftc.gov/system/files/documents/reports/mobile- security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf . [74] Dan Geer, Discurso de apertura en Black Hat USA 2014: *Cybersecurity as Realpolitik*, (6 de agosto de 2014), disponible *en* http://geer.tinho.net/geer.blackhat.6viii14.txt (borrador de entrega nominal). Vídeo disponible en: https://www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.

[75] Core Infrastructure Initiative, https://www.coreinfrastructure.org/ (visitado por última vez el 4 de abril de 2018).

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Objetivo 2: Promover la innovación en la infraestructura para la adaptación dinámica a las amenazas cambiantes.

Para establecer un ecosistema de Internet y comunicaciones más resistente, las normas y prácticas que disuaden, previenen y/o mitigan las redes de bots y las amenazas distribuidas deben implementarse y actualizarse continuamente en todos los dominios del ecosistema en respuesta y anticipación a la evolución de la amenaza. Esta sección identifica las acciones disponibles para las partes interesadas para apoyar el desarrollo de una infraestructura eficaz y dinámica.

Acción 2.1 Los proveedores de servicios de Internet y sus socios de interconexión[76] deberían ampliar el actual intercambio de información para lograr un intercambio más oportuno y eficaz de información sobre amenazas procesables tanto a nivel nacional como mundial.

Una vez establecidas, las redes de bots se revenden o alquilan a múltiples clientes y se redirigen para atacar nuevos objetivos. Esto significa que muchos ISP y sus socios de peering experimentarán ataques similares a lo largo del tiempo. Cuando un ISP se enfrenta por primera vez a una amenaza concreta, hay que analizar el comportamiento anómalo y desarrollar métodos de mitigación. Las redes de bots suelen estar distribuidas entre muchos ISP, cada uno de los cuales puede contribuir a las actividades de mitigación si tiene los conocimientos suficientes. Compartir las técnicas de gestión de la red y las tácticas defensivas que son efectivas contra determinadas amenazas es otra forma en que los grandes proveedores de redes aumentan el valor preventivo de la información compartida.

Los acuerdos actuales de intercambio de información entre los ISP y sus socios de peering son muy eficaces dentro de su ámbito. Al compartir información sobre las amenazas conocidas, en curso y emergentes, los ISP pueden responder con mayor eficacia. Sin embargo, los acuerdos actuales de intercambio de información se basan a menudo en relaciones personales y no son exhaustivos, especialmente cuando se trata de amenazas más matizadas o sensibles. La evolución del panorama de las redes -y los cambios en el alcance, la escala, el enfoque y la diversidad de los actores de la red- también afecta a la eficacia de las relaciones de intercambio. La colaboración entre los ISP y sus socios de interconexión debe formalizarse e incluir el intercambio de detección, notificación y métodos de mitigación planificados o utilizados dentro de la red. Cuando la compartición se vea obstaculizada por cuestiones comerciales, los ISP deberían buscar formas de abordar los acuerdos de compartición y la coordinación de la respuesta en sus acuerdos de interconexión y tránsito.

La industria debe liderar los esfuerzos para ampliar el alcance y la utilidad del intercambio de información entre los proveedores de servicios de Internet y sus socios de interconexión, así como para abordar las lagunas en la operatividad de la información compartida. En particular, la industria debe trabajar en colaboración con la sociedad civil y el gobierno para mejorar las respuestas coordinadas a la información procesable y liderar el desarrollo, el perfeccionamiento y la estandarización de los protocolos de intercambio de información para aumentar la velocidad y permitir una respuesta automatizada. Debe prestarse especial atención al compromiso y a la inclusión de los pequeños proveedores de servicios de Internet y al desarrollo de protocolos que mejoren su participación.

Aunque la industria tiene el papel principal, el gobierno federal puede facilitar esta actividad a nivel nacional a través del Centro de Análisis e Intercambio de Información de las Comunicaciones (ISAC) (es *decir,* el Centro Nacional de Coordinación de las Comunicaciones [NCC]), forjando asociaciones con los grupos de operadores de redes (NOG), a nivel internacional a través de la participación continua en el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST), y ampliando los acuerdos de intercambio de información con pares internacionales como Telecom ISAC Japón. El gobierno puede desempeñar un papel importante en estos debates, convocando

[76] Esto incluye a las empresas que operan sus propios routers BGP y servidores DNS.

reuniones de múltiples partes interesadas cuando sea necesario, proporcionando una visión global y garantizando que el proceso sea equitativo para todas las partes interesadas. Los Equipos Nacionales de Respuesta a Incidentes de Seguridad Informática (CSIRT) también pueden coordinar directamente, y pueden catalizar una respuesta por parte de los gestores de recursos locales y los actores de la infraestructura.

Acción 2.2 Las partes interesadas y los expertos en la materia, en consulta con el NIST, deberían liderar el desarrollo de un perfil de CSF para la prevención y mitigación de DDoS en la empresa.

Las empresas que desean mitigar el impacto de futuros ataques DDoS y reducir la probabilidad de que los recursos internos se incorporen a las redes de bots para atacar a otras empresas se encuentran con que no hay directrices completas disponibles. Las grandes empresas se ven obligadas a dedicar importantes recursos de personal para identificar y adquirir o desplegar los mecanismos adecuados. Las empresas más pequeñas a menudo carecen de la experiencia o no pueden permitirse desviar esos recursos para desarrollar una estrategia anti-DDoS. Las soluciones integrales son complejas y a menudo requieren una combinación de servicios comerciales externos y gestionados localmente, por lo que es fundamental comunicar las necesidades a los proveedores.

La versión 1.0 del Marco para la Mejora de la Ciberseguridad de las Infraestructuras Críticas (conocido como CSF, por sus siglas en inglés) fue desarrollada por el NIST con amplias aportaciones del sector privado, al igual que la versión 1.1, publicada en abril de 2018. El CSF proporciona un enfoque flexible para gestionar el riesgo de ciberseguridad que incorpora las normas y las mejores prácticas de la industria, es lo suficientemente general para permitir una amplia aplicabilidad en una variedad de entornos -incluyendo IoT- y ha sido ampliamente aceptado por la industria. El CSF puede complementarse con perfiles del marco, que aplican los componentes del marco a una situación específica. En particular, los sectores industriales pueden utilizar los perfiles para documentar las mejores prácticas de protección contra amenazas específicas. El CSF está diseñado para evolucionar con el tiempo a medida que cambia el entorno de la ciberseguridad.

Las empresas que desean mejorar la resistencia de sus propias redes contra los ataques DDoS y protegerse contra las redes de bots que incorporan sus recursos se beneficiarían significativamente de la disponibilidad de un Perfil CSF77 para la Prevención y Mitigación de DDoS en la Empresa. Un esfuerzo liderado por la industria, en consulta con el NIST, el mundo académico y otros expertos en la materia, debería desarrollar un Perfil CSF para la Prevención y Mitigación de DDoS en Empresas, centrándose en el estado deseado de la ciberseguridad de las organizaciones para mitigar los ataques DDoS. [78] El Perfil CSF proporcionaría orientación a las empresas y establecería un lenguaje común para las discusiones relativas a los mecanismos de protección DDoS con los vendedores de productos, los ISP y otros proveedores de infraestructura. El perfil ayudaría a las empresas a identificar oportunidades para mejorar la mitigación de las amenazas DDoS y ayudaría a priorizar la ciberseguridad comparando su estado actual con el estado deseado. El perfil incluiría probablemente varios niveles para apoyar a los sectores de la industria con diferentes requisitos de resiliencia.

El alcance del Perfil CSF debe incluir, como mínimo, los mecanismos de mitigación DDoS dentro y fuera de las instalaciones, las características de seguridad de enrutamiento (por *ejemplo,* el filtrado de entrada de la Mejor Práctica Actual [BCP] 38/84), y la orientación sobre el cierre de los vectores de reflexión. Para una aplicabilidad más amplia, el Perfil debe ser escrito para cubrir tanto las grandes empresas, que pueden operar los componentes clave de sus estrategias de mitigación de DDoS, como las pequeñas empresas, que a menudo dependen totalmente de los proveedores de servicios.

[77] Los perfiles de los MCA son recopilaciones de orientaciones y mejores prácticas en torno a determinadas amenazas que siguen el modelo bien establecido de los MCA.

[78] La Coalición para la Política y la Ley de Ciberseguridad (Coalición de Ciberseguridad) ha iniciado un esfuerzo prometedor, actualmente en forma de borrador. *Véase* Cybersecurity Coalition, *Threat Profile for DDoS Attacks Using NIST Framework*, https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework (28 de julio de 2017).

Las partes interesadas del gobierno deberían participar en el desarrollo para asegurar que el perfil es lo suficientemente amplio como para servir como un Perfil CSF para la Prevención y Mitigación de DDoS Federal. Para crear incentivos de mercado, esta acción debe ser apoyada por la adopción agresiva en todo el gobierno federal como se especifica en la Acción 2.3, ya sea a través de la aplicación directa del perfil o mediante la aplicación de los controles correspondientes utilizando el proceso existente de la Ley Federal de Modernización de la Seguridad de la Información.

Acción 2.3 El gobierno federal debería dar ejemplo y demostrar la viabilidad de las tecnologías, creando incentivos de mercado para los primeros en adoptarlas.

Tras la publicación de las líneas básicas de seguridad de los dispositivos de la IO (acción 1.1), el gobierno federal debería establecer directrices de adquisición para ofrecer incentivos de mercado a los primeros en adoptarlas. Muchos vendedores de productos de IoT han articulado planes para mejorar la seguridad de sus productos, pero los observadores han expresado su preocupación por el hecho de que los incentivos del mercado están fuertemente orientados hacia el coste y el tiempo de comercialización. Sin pruebas de que los clientes absorberán el coste adicional de desarrollar productos más seguros, la industria puede verse incentivada hacia una carrera hacia el fondo. Aunque la contratación pública federal ya no domina el mercado, su poder de compra y su influencia siguen siendo fuertes, y el gobierno de Estados Unidos puede dar ejemplo. Mediante el desarrollo de directrices para las acciones de contratación federal basadas en las líneas de base de seguridad para los dispositivos de la IO, el gobierno de los EE.UU. puede establecer incentivos de mercado para los primeros adoptantes. La Oficina de Gestión y Presupuesto, la Administración de Servicios Generales (GSA) y el Departamento de Defensa pueden facilitar estos requisitos de adquisición a través de políticas y modificaciones del calendario de la GSA y de la normativa federal de adquisiciones. [79]

Tras la publicación de un perfil de LCR adecuado (acción 2.2), el gobierno federal debería aplicar medidas básicas de prevención y mitigación de DDoS para todas las redes federales con el fin de mejorar la resistencia del ecosistema y demostrar la viabilidad y eficacia del perfil. En el pasado, los piratas informáticos han aprovechado las redes federales en los ataques DDoS utilizando resolvedores abiertos y otros recursos de la agencia para amplificar sus ataques. El gobierno federal debería predicar con el ejemplo, asegurando que los recursos federales no sean participantes involuntarios y que las redes federales estén preparadas para detectar, mitigar y responder según sea necesario. La Administración debería ordenar la implementación del Perfil Federal CSF para la Prevención y Mitigación de DDoS por parte de todas las agencias gubernamentales dentro de un periodo fijo tras la finalización y publicación del perfil.

El gobierno federal debería evaluar e implementar formas efectivas de incentivar el uso de herramientas y procesos de desarrollo de software que reduzcan significativamente la incidencia de las vulnerabilidades de seguridad en todas las adquisiciones de software federal, como por ejemplo a través de requisitos de atestación o certificación. Para establecer incentivos de mercado para el desarrollo de software seguro, el gobierno federal debería establecer regulaciones de adquisición que favorezcan o requieran software comercial que se desarrolle usando tales procesos, cuando estén disponibles. El gobierno federal también debería garantizar que los proyectos de desarrollo de software financiados por el gobierno utilicen las mejores herramientas disponibles para obtener información sobre el impacto de estas regulaciones.

[79] El Grupo de Trabajo de Seguridad de la IO del Consejo de Coordinación de Tecnologías de la Información, dirigido por el DHS, está redactando actualmente unas orientaciones para los responsables de adquisiciones sobre las preguntas que deben formular a sus clientes, a sus equipos de TI y de seguridad, y a los proveedores, para garantizar que un dispositivo conectado adquirido se ajuste a la postura de gestión de riesgos de la agencia. Esta orientación complementará, pero no es lo mismo que las directrices de cumplimiento elaboradas en relación con las líneas básicas de seguridad.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Acción 2.4 La industria, los gobiernos y la sociedad civil deberían colaborar con todas las partes interesadas para seguir mejorando y normalizando los protocolos de intercambio de información.

Para hacer frente a las amenazas automatizadas y distribuidas, las partes interesadas deben compartir información sólida en tiempo casi real. Como lección clave aprendida, el informe del NSTAC indicó que la colaboración entre los sectores público y privado es vital para mitigar las redes de bots. Los protocolos de intercambio de información que se utilizan actualmente fueron promovidos por el gobierno federal, con la participación activa de una amplia gama de partes interesadas, pero pueden no satisfacer las necesidades de todas las partes interesadas.

Por ejemplo, las pequeñas empresas están infrarrepresentadas; no contribuyen ni se benefician de la mayoría de los acuerdos actuales de intercambio de información. Para satisfacer las necesidades de las pequeñas empresas, que por lo general carecen de un sólido equipo interno de ciberseguridad, puede ser necesario que los protocolos permitan una acción automatizada. Por ejemplo, los proveedores de servicios de Internet a menudo pueden identificar la red del cliente asociada a un dispositivo comprometido, pero carecen de la visibilidad necesaria para identificar dispositivos específicos. Las pequeñas empresas pueden no ser capaces de identificar estos dispositivos si son contactadas por sus ISP. Los protocolos de intercambio de información que permitieran a los ISP compartir información sobre los dispositivos comprometidos detectados con los routers que dan soporte a las pequeñas empresas podrían permitir la identificación automática y un control más sólido de los clientes sobre sus dispositivos en red. Los clientes también podrían optar por compartir los resultados de cualquier medida de mitigación con sus ISP, de forma similar a lo que ocurre cuando se comparte información sobre fallos de software con los proveedores.

Para satisfacer las necesidades de coordinación y colaboración de una infraestructura altamente resistente, estos protocolos de intercambio de información deben tener un alcance completo, ser accesibles a una amplia gama de empresas y ser lo suficientemente precisos como para permitir el procesamiento y la respuesta automáticos. Para garantizar el cumplimiento de estos objetivos, la industria debe liderar los esfuerzos, en colaboración con el gobierno federal y otras partes interesadas, para mejorar los protocolos de intercambio de información para satisfacer las necesidades de las partes interesadas y establecer normas internacionales para facilitar la coordinación global.

Acción 2.5 El gobierno federal debería colaborar con los proveedores de infraestructuras estadounidenses y mundiales para ampliar las mejores prácticas de gestión del tráfico de red en todo el ecosistema.

Aunque no se puede esperar que los proveedores de red actúen como policías del tráfico e identifiquen todos los paquetes malos, tanto las herramientas y prácticas comunes como las más recientes pueden ayudar a filtrar algunos tipos de tráfico malo. Muchos agentes del mercado utilizan la señalización informal de la reputación o los acuerdos más formales de interconexión y tránsito para abordar la gestión del tráfico. Una amplia coalición de expertos nacionales e internacionales -la industria, el mundo académico, la sociedad civil y el gobierno- debería examinar hasta qué punto los acuerdos de tránsito y de interconexión entre sistemas autónomos y redes pueden mejorar la responsabilidad de la gestión del tráfico, por ejemplo, en lo que respecta a la suplantación y el filtrado. La comunidad académica y de ingeniería debería investigar cómo podrían incorporarse y aplicarse las nuevas herramientas y prácticas en desarrollo. La industria, el mundo académico, la sociedad civil y el gobierno federal deberían basarse en estos hallazgos para ampliar las políticas constructivas y las mejores prácticas de gestión del tráfico de red en todo el ecosistema, teniendo en cuenta los requisitos de las pequeñas empresas. Deberían revisarse las herramientas y marcos existentes, como el Código de Conducta Anti-Bot de Estados Unidos para los ISP y las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS), de carácter voluntario, y deberían explorarse nuevas soluciones en un proceso con múltiples partes interesadas que incluya una representación diversa de los actores de la red que se ajusten al entorno actual del ecosistema.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Objetivo 3: Promover la innovación en el borde de la red para prevenir, detectar y mitigar los ataques automatizados y distribuidos.

Para establecer un ecosistema de Internet y comunicaciones resistente, los servicios de infraestructura diseñados para proteger contra los ataques deben complementarse con una mayor detección y mitigación de los dispositivos comprometidos en las redes domésticas o empresariales, y en los lugares en los que esas redes se conectan a Internet. Un mayor contexto a partir del conocimiento local puede mejorar la detección, y puede ser más fácil simplemente segmentar o hacer un cortafuegos de determinados dispositivos o servicios que se comportan de forma anómala. Esta sección identifica las acciones que las partes interesadas pueden llevar a cabo para gestionar el impacto de los dispositivos comprometidos utilizados en ataques automatizados y distribuidos.

Acción 3.1 El sector de las redes debería ampliar los actuales esfuerzos de desarrollo de productos y de normalización para una gestión eficaz y segura del tráfico en los entornos domésticos y empresariales.

El sector de las redes está aplicando una serie de mecanismos propios y basados en estándares para gestionar mejor el tráfico dentro de las redes empresariales. Estos mecanismos tienen como objetivo evitar las comunicaciones con sistemas sospechosos o restringir las comunicaciones a los hosts específicamente necesarios para el correcto funcionamiento. Estos sistemas pueden aprovechar la IA o el aprendizaje automático, los métodos de detección y mitigación de amenazas proporcionados por servicios comerciales externos o la información específica de los dispositivos. La industria debe ampliar estos esfuerzos para acelerar la entrega de una seguridad de red eficiente y rentable para los entornos domésticos y empresariales.

Los concentradores y las pasarelas de la red local80 pueden actuar como gestores del tráfico, identificando e impidiendo que el tráfico malicioso acceda a los dispositivos IoT y limitando el tráfico perjudicial que emana de los dispositivos de la red local. Los proveedores de la nube también están desarrollando soluciones que podrían complementar estas soluciones centradas en las puertas de enlace, proporcionando potencialmente múltiples controles y equilibrios en la pila de la red para proteger mejor el ecosistema de la IO. A medida que surgen estas innovaciones en materia de seguridad, las administraciones públicas y las partes interesadas deben asociarse para dar a conocer las soluciones de seguridad a los consumidores, las pequeñas y medianas empresas y los socios internacionales. Cuando existan barreras específicas para la adopción o el avance, las administraciones públicas y las partes interesadas deberían reunirse para identificar los obstáculos, promover el despliegue de las normas emergentes y examinar políticas prácticas de cortafuegos para el espacio de productos más amplio.

Acción 3.2 Los productos de TI e IO del hogar deben ser fáciles de entender y sencillos de utilizar de forma segura.

Los productos de TI e IoT domésticos deben reducir o eliminar los conocimientos necesarios para utilizarlos de forma segura y privada. Las redes empresariales se benefician de la atención del personal profesional encargado de mantener la seguridad de la red y los sistemas. Este personal suele conocer y estar suficientemente capacitado para configurar estos dispositivos de forma segura. Las interfaces administrativas de la mayoría de los dispositivos de TI e IoT están diseñadas para personal con esta formación y nivel de conocimientos.

Los propietarios de redes domésticas y de pequeñas empresas tienen menos probabilidades de contar con ese apoyo, con el resultado inevitable de redes y productos desplegados de forma insegura. En lugar de esperar que los consumidores se conviertan en expertos en seguridad, las industrias de TI e IoT deberían dar prioridad a los procesos de despliegue y configuración simples y sencillos para los dispositivos comercializados para el hogar y las pequeñas empresas. Para

[80] Las pasarelas son componentes de la arquitectura de red que se sitúan entre los subcomponentes de la red. *Véase el* apartado II para conocer las pasarelas inteligentes, etc.

Por ejemplo, si el proceso de instalación no obliga a actualizar las contraseñas administrativas, estos productos seguirán siendo objetivos fáciles de incorporar a las redes de bots. Las configuraciones por defecto deben ser las más seguras para el ámbito de uso previsto, y las interfaces basadas en la nube o en aplicaciones deben ser intuitivas y basarse en las mejores prácticas de diseño actuales. La instalación de parches de seguridad debería ser automática o muy fácil de gestionar (por *ejemplo*, no debería requerir descargas en unidades flash).

Acción 3.3 Las empresas deben migrar a arquitecturas de red que faciliten la detección, interrupción y mitigación de las amenazas automatizadas y distribuidas. También deberían considerar cómo sus propias redes ponen en riesgo a otras.

En la actualidad existen diversos productos y servicios anti-DDoS eficaces, y recientemente han aparecido nuevos productos innovadores (como los descritos en la acción 3.1). Sin embargo, la mayoría de las empresas han diseñado sus redes en función de la simplicidad y el rendimiento más que de la seguridad. En combinación con el perfil del MCA para la prevención y mitigación de DDoS, las empresas tienen la oportunidad de rediseñar sus redes para aislar los dispositivos inseguros, gestionar los flujos de comunicación y, en general, mejorar la resistencia de sus áreas del ecosistema. Por ejemplo, las empresas que dependen de los sistemas heredados deben diseñar sus redes de manera que estos dispositivos inseguros no estén expuestos a los ataques de la Internet general.

Los riesgos procedentes de las redes empresariales van más allá del peligro de los dispositivos IoT secuestrados. Algunos servicios basados en la red permiten a los actores maliciosos amplificar un ataque a través de "reflectores", o servicios que pueden enviar grandes cantidades de tráfico a un objetivo falsificado. Si están mal configurados para permitir consultas desde cualquier parte de Internet, los servicios vulnerables, como los servidores DNS, permiten a los atacantes enviar enormes volúmenes de tráfico contra las víctimas. En 2018, uno de los mayores ataques DDoS vistos hasta la fecha explotó una vulnerabilidad recién descubierta en el software relativamente oscuro MemCacheD. [81] Estas fallas suelen ser más problemáticas porque los sistemas vulnerables están en máquinas y redes de escala empresarial con alta disponibilidad y gran ancho de banda. Las organizaciones deben seguir las mejores prácticas para las herramientas orientadas a Internet y asegurarse de que están actualizadas.

Parte de esta evolución hacia mejores prácticas de red puede producirse de forma orgánica a medida que las empresas integren más dispositivos IoT en sus entornos de red y sean más conscientes de los riesgos de las aplicaciones orientadas al exterior. Sin embargo, el gobierno, la industria y la sociedad civil deberían trabajar para mejorar el conocimiento de los usuarios y las empresas sobre las amenazas y las mejores prácticas de seguridad a través de colaboraciones como campañas de asociación y actividades de compromiso estratégico. A medida que estos conocimientos se formalicen, podrían considerarse para su inclusión en futuras versiones del Marco de Ciberseguridad del NIST.

Acción 3.4 El gobierno federal debería investigar cómo un mayor despliegue de IPv6 puede alterar la economía de los ataques y la defensa.

América del Norte se quedó sin direcciones IPv4 no utilizadas de fácil distribución en 2015, pero muy pocos consumidores y pequeñas empresas aprovechan actualmente el espacio y las capacidades de las direcciones IPv6. El gobierno y la industria han estado planificando y trabajando para una mayor adopción de IPv6, pero también deben considerar cómo esto cambiará el espacio de ataque potencial y la magnitud de los ataques automatizados y distribuidos.

[81] Lili Hay Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired (1 de marzo de 2018, 11:01 AM), https://www.wired.com/story/github-ddos-memcached/.

Uno de los retos que plantea la notificación a los consumidores de que un dispositivo de su red ha sido vinculado a una actividad maliciosa es el gran número de dispositivos que suelen estar conectados a una red doméstica o de pequeña empresa. Los routers con NAT, que pueden hacer que muchos dispositivos parezcan tener la misma dirección IP, pueden impedir la notificación. Con la transición a IPv6, los ISP de los consumidores pueden estar mejor posicionados para observar el mal comportamiento de los dispositivos cuando las direcciones IPv6 no están sujetas a NAT. Esta información puede, a su vez, asignarse a otras soluciones centradas en el borde.

La implementación de routers con NAT a nivel de consumidores y pequeñas empresas ha servido en ocasiones como protección clave de los puntos finales vulnerables. Las herramientas NAT actúan como un cortafuegos incidental, impidiendo que los dispositivos del hogar sean alcanzados directamente por el tipo de herramientas de escaneo masivo que propagan el malware y conducen a una infección generalizada; las cámaras de seguridad fueron un objetivo común en la red de bots Mirai porque normalmente no se encuentran detrás de un router con NAT. En las arquitecturas actuales, una red basada en IPv6 probablemente permitiría direccionar cada dispositivo. En teoría, el espacio de direcciones IPv6 es tan grande que no sería escaneable con las herramientas actuales, pero los expertos han observado que los patrones permitirían que las nuevas técnicas de escaneo siguieran descubriendo dispositivos vulnerables.

La NTIA debería trabajar con las partes interesadas para identificar las lecciones aprendidas de la industria y de otros países, examinando además los impedimentos y las opciones para alinear los incentivos con el fin de animar a los ISP a realizar la transición completa al IPv6 más rápidamente. La habilitación de la defensa y la mitigación del riesgo requerirán una mayor innovación en el borde de la red. Comprenderlo antes permitirá encontrar mejores soluciones cuando se generalice el uso de IPv6.

Objetivo 4: Promover y apoyar las coaliciones entre las comunidades de seguridad, infraestructura y tecnología operativa a nivel nacional y mundial.

Para mejorar la resistencia de Internet y de la infraestructura de comunicaciones, es preciso facilitar la aplicación de acciones coordinadas que traspasen las fronteras geopolíticas, público-privadas, del sector industrial y técnicas. Esta sección identifica las acciones clave para aumentar el compromiso entre las comunidades de partes interesadas críticas.

Acción 4.1 Los proveedores de servicios de Internet y las grandes empresas deberían aumentar el intercambio de información con los organismos gubernamentales y entre sí para proporcionar información más oportuna y procesable sobre las amenazas automatizadas y distribuidas.

Mientras que muchas de las acciones de este informe aumentarán el coste o reducirán la eficacia de los ataques automatizados y distribuidos, las acciones de las fuerzas de seguridad tienen un impacto único en la comunidad de botnets. Al derribar los sistemas de mando y control, las fuerzas del orden pueden "lobotomizar" rápidamente una amenaza distribuida. La persecución de los principales actores de la economía de las redes de bots no sólo frena el desarrollo de las amenazas distribuidas por parte de los participantes actuales, sino que también disuade a los posibles desarrolladores de unirse a ellas.

Las fuerzas del orden confían en los grandes y pequeños ISP, los equipos de respuesta a incidentes, las empresas de ciberseguridad y respuesta a incidentes, los proveedores de antivirus, las entidades comerciales y las empresas de inteligencia sobre ciberamenazas para apoyar las investigaciones en curso y otros esfuerzos para contrarrestar las amenazas automatizadas, proporcionando información procesable sobre las amenazas y las tendencias que afectan a sus redes y clientes. Al proporcionar información aún más oportuna y procesable, los ISP y otros proveedores de infraestructuras clave pueden facilitar, apoyar y acelerar las acciones de las fuerzas de seguridad, incluidas las que afectan a las redes de bots distribuidas por la

mundo. Por ejemplo, las partes interesadas han sugerido que la ampliación de la notificación de incidentes para incluir los ataques fallidos podría proporcionar alertas tempranas y apoyar una intervención más temprana de las fuerzas del orden. Este tipo de datos también ayudaría a la comunidad de seguridad a comprender mejor el panorama de riesgos.

Las fuerzas de seguridad pueden identificar de forma proactiva qué tipo de datos les ayudarán a investigar y perseguir a los malos actores, y trabajar con los proveedores de infraestructuras para abaratar y facilitar el intercambio de esta información con el gobierno, protegiendo al mismo tiempo la privacidad de los usuarios de Internet. [82] La mejora del intercambio de información sobre ciberseguridad sigue siendo uno de los elementos clave para prevenir y mitigar los problemas actuales y emergentes de la ciberdelincuencia. Para promover la confianza y las relaciones más amplias que han demostrado ser útiles, las fuerzas de seguridad deberían continuar con los esfuerzos de divulgación con las comunidades de seguridad y de redes para ayudarles a identificar y comprender a los socios adecuados en el gobierno.

Los organismos gubernamentales, incluidas las fuerzas de seguridad, deben seguir mejorando la puntualidad y la pertinencia de la información sobre ciberseguridad que comparten para prevenir y mitigar los ciberincidentes. Las fuerzas del orden tratan a las empresas que han sufrido una intrusión o un ataque distribuido como víctimas de un delito, y llevan a cabo sus investigaciones sobre estos delitos denunciados con discreción para evitar la divulgación injustificada de información relativa al incidente, siempre que sea posible. Además, las organizaciones privadas deben compartir la información sobre ciberseguridad dentro de sus sectores a través de las Organizaciones de Intercambio y Análisis de Información y con las agencias gubernamentales cuando sea apropiado, al tiempo que identifican claramente qué información debe compartirse con otras entidades para evitar daños adicionales.

Los RIR y los registradores pueden facilitar la atribución de los malos actores manteniendo bases de datos WHOIS precisas. Además, el gobierno federal debe trabajar para comprometerse con sus homólogos europeos a fin de garantizar que la información de WHOIS se conserve a tiempo, ya que las protecciones europeas de privacidad de datos se aplican para preservar una herramienta crítica para los esfuerzos nacionales y mundiales de investigación de botnets. Los gobiernos pueden trabajar con las entidades del sector privado responsables del cumplimiento de la normativa de protección de la privacidad de los datos, así como con las entidades que participan en la labor de investigación de las redes de bots, para garantizar que se preservan ambas partes (el cumplimiento y las investigaciones de las redes de bots).

Acción 4.2 El gobierno federal debe promover la adopción internacional de las mejores prácticas y las herramientas pertinentes a través de un compromiso internacional bilateral y multilateral.

Las mejoras significativas de la resistencia del ecosistema no pueden lograrse únicamente con medidas nacionales. Estados Unidos debería colaborar regularmente con socios internacionales en materia de ciberseguridad a nivel bilateral, regional e internacional, aprovechando la experiencia de las agencias federales. Para las cuestiones relacionadas con el DNS, la NTIA debería coordinarse con las agencias federales y representar las posiciones de Estados Unidos en los foros de múltiples partes interesadas, como la Corporación para la Asignación de Nombres y Números de Internet (ICANN) y el Foro de Gobernanza de Internet.

La normalización internacional podría ser especialmente beneficiosa. Las normas internacionales para los productos y servicios de la IO, así como las normas que podrían perturbar los ataques automatizados y distribuidos, podrían ampliar el mercado de productos que contribuyen a la resiliencia del ecosistema. Como recomendaba el informe del NSTAC, la industria y las agencias federales que participan en el desarrollo de normas deberían

[82] *Véase, por ejemplo,* Organización de Normas de Intercambio y Análisis de Información (ISAO), *ISAO SP 4000: Protecting Consumer Privacy in Cybersecurity Information Sharing v1.0*, (26 de julio de 2017), https://www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1- 0/.

coordinar una estrategia para participar en los organismos internacionales de normalización adecuados impulsados por la industria para garantizar la representación y el liderazgo de Estados Unidos y, a través de esa participación, defender un conjunto flexible e interoperable de normas internacionales para la seguridad de la IO.

Medida 4.3 Los organismos reguladores de sectores específicos, cuando sea pertinente, deberían colaborar con la industria para garantizar una comercialización no engañosa y fomentar las consideraciones de seguridad específicas del sector.

Debido a la complejidad y diversidad del panorama de la IO, es difícil imaginar un conjunto de normas únicas que puedan garantizar la seguridad al mismo tiempo que se mantiene el ritmo de cambio y la naturaleza dinámica del entorno de las amenazas. Sin embargo, las agencias reguladoras de sectores específicos pueden promover la resistencia del ecosistema trabajando con la industria para garantizar que la seguridad de los productos desplegados es adecuada para el uso de los mismos. Por ejemplo, la Administración de Alimentos y Medicamentos ha establecido directrices para los dispositivos médicos que desvinculan las actualizaciones básicas de seguridad de los regímenes de certificación de productos existentes. [83] Estas directrices son beneficiosas para los consumidores, ya que los dispositivos médicos de los que dependen son más resistentes a las amenazas de ciberseguridad, y para los fabricantes, que ganan en claridad respecto a los requisitos de certificación. Las partes interesadas destacaron que el gobierno federal podría beneficiarse de un mecanismo de coordinación interinstitucional de la IO para promover y compartir este tipo de prácticas innovadoras y lecciones aprendidas, y para evitar conflictos normativos.

Las acciones de aplicación cuidadosas pueden beneficiar a los consumidores y a los participantes honestos en el mercado. La FTC ha tomado medidas en numerosos casos relacionados con la privacidad y la seguridad, y los dispositivos de IO figuran en algunas de estas acciones de aplicación. [84] Al detener y disuadir la comercialización engañosa, la FTC puede aumentar la confianza de los consumidores en las afirmaciones de seguridad de los proveedores de tecnologías de la información y de la IO y apoyar los incentivos positivos del mercado. La FTC también ha utilizado su autoridad de deslealtad en virtud del artículo 5 de la Ley de la FTC para desafiar las prácticas de seguridad no razonables, incluso en el espacio de la IO. Además, las agencias de sectores específicos, como el Departamento de Salud y Servicios Humanos de los Estados Unidos, hacen cumplir las normas de seguridad de la información en las industrias pertinentes. Estas políticas pueden contribuir al debate sobre la seguridad del ecosistema más amplio y beneficiarse de él.

Acción 4.4 La comunidad debería identificar los puntos de influencia y tomar medidas concretas para alterar las herramientas e incentivos de los atacantes, incluyendo el intercambio y uso activo de datos de reputación.

Muchas amenazas se derivan de asimetrías que favorecen a los atacantes al distribuir la explotación entre actores difusos del ecosistema. Los defensores pueden utilizar medidas de intercambio de datos e información para rastrear las herramientas de los atacantes y pueden utilizar la incidencia de los daños para identificar las herramientas y los actores. En algunos casos, los esfuerzos de coordinación relativamente ligeros deberían ser capaces de desbaratar clases de ataques más amplias. La sección 3.3 destaca la importancia de que las organizaciones identifiquen los reflectores que amplifican los ataques DDoS. La comunidad puede rastrear la presencia de estas amenazas para ayudar a la concienciación y a la reducción de la amenaza. Este tipo de intercambio ha ayudado a hacer frente a amenazas como el spam, y puede aprovecharse contra otros vectores de ataque.

[83] Administración de Alimentos y Medicamentos, *Postmarket Management of Cybersecurity in Medical Devices*, (28 de diciembre de 2016), *disponible en* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. [84] *Véase, por ejemplo,* Comisión Federal de Comercio, *In the Matter of TRENDnet, Inc.* , FTC Matter/File Number 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter (última actualización: 7 de febrero de 2014).

El "fast flux hosting" es la modificación rápida y automatizada de las direcciones IP asignadas a los hosts en el DNS para ocultar la ubicación de los sitios web que apoyan actividades maliciosas, ilegales o delictivas. En 2008, el Comité Asesor de Seguridad y Estabilidad (SSAC)85 consideró las medidas que algunos registradores y registros implementan hoy en día: la supervisión de los cambios en los registros del DNS que son indicativos de alojamiento fast flux, la restricción de las frecuencias de cambio del DNS y los rangos de valores, y la supervisión del acceso a la cuenta del registrador para evitar la automatización. Además, consideró cómo los registradores podrían aplicar estas medidas para agilizar los procesos de suspensión de sitios web y nombres de dominio ilegales. Estas medidas podrían suponer una diferencia sustancial en los esfuerzos por frenar la actividad de las redes de bots, pero no se han aplicado de forma generalizada. Los nuevos avances de los atacantes, como las "redes de doble flujo", requieren más innovación y colaboración a nivel de red. La comunidad en general, incluido el gobierno federal, debería abogar en los foros pertinentes de múltiples partes interesadas (por *ejemplo*, ICANN y los RIR) por una aplicación más amplia de estas medidas, o por mecanismos alternativos para lograr este objetivo.

Algunas amenazas del ecosistema están impulsadas por mercados ilícitos concretos. El mercado activo de DDoS por encargo está floreciendo en las comunidades de jugadores. La colaboración entre las empresas de juegos y los procesadores de pagos puede rastrear y castigar a quienes utilizan estos servicios, secando el mercado. Del mismo modo, el mercado de credenciales robadas puede verse alterado si se dificulta la validación de los datos. [86] El uso de herramientas básicas contra la automatización en la web puede aumentar el coste para los atacantes de verificar el valor de las credenciales robadas, reduciendo así el beneficio de su robo y uso. En términos más generales, las investigaciones sugieren que dirigirse a los socios anteriores con la notificación de las vulnerabilidades expuestas puede desempeñar un papel clave para impulsar la reparación. [87]

La inversión gubernamental puede ser otra palanca. Las agencias han sido receptivas a las métricas y la transparencia en torno a cuestiones de seguridad como la adopción de HTTPS. [88] Con un poco de orientación y curación, la reputación de la higiene de la red podría incluirse como un factor en el proceso de adquisición del gobierno. El gobierno del Reino Unido ha comenzado a experimentar con este enfoque. [89]

Acción 4.5 La comunidad de la ciberseguridad debería seguir colaborando con la comunidad de la tecnología operativa para promover la concienciación y acelerar la incorporación de las tecnologías de ciberseguridad.

La incorporación de la funcionalidad de red en la tecnología operativa (OT) (por *ejemplo, los* sistemas SCADA en entornos industriales) ha introducido nuevos retos de ciberseguridad que sólo pueden abordarse mediante la experiencia combinada de las comunidades de ciberseguridad y OT. Los requisitos principales asociados a los casos de OT suelen estar fuera del alcance de los expertos en materia de ciberseguridad, y los expertos en materia de OT no suelen estar familiarizados con las prácticas básicas de ciberseguridad.

---

[85] Comité Asesor de Seguridad y Estabilidad de ICANN, *SAC 025: SSAC Advisory on Fast Flux Hosting and DNS*, (Mar. 2008), https://www.icann.org/en/system/files/files/sac-025-en.pdf.

[86] *Véase* Timothy Peacock y Allan Friedman, *Automation and Disruption in Stolen Payment Card Markets, (*2014), *disponible en* http://www.econinfosec.org/archive/weis2014/papers/PeacockFriedman-WEIS2014.pdf.

[87] *Véase, por ejemplo,* Orcun Cetin, Carlos Gañán, Maciej Korczyński y Michel van Eeten, Make *Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning*, (2017), *disponible en* http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_17.pdf.

[88] *Véase, por ejemplo,* Eric Mill, *Tracking the U.S. Government's Progress on Moving to HTTPS*, General Services Administration - 18F, (4 de enero de 2017), https://18f.gsa.gov/2017/01/04/tracking-the-us-governments-progress-on- moving-https/.

[89] *Véase* Ian Levy, *Active Cyber Defence-One Year On*, UK National Cyber Security Centre, (5 de febrero de 2018), *disponible en* https://www.ncsc.gov.uk/information/active-cyber-defence-one-year.

El gobierno federal puede facilitar este proceso ampliando los compromisos actuales que reúnen a las comunidades de ciberseguridad y OT para compartir conocimientos y experiencia y que promueven la concienciación y aceleran la adopción de tecnologías de la comunidad de ciberseguridad. Las agencias sectoriales trabajan estrechamente con sus sectores para comprender el riesgo de ciberseguridad, para vincular a los sectores con los recursos federales y para promover la planificación de la resiliencia. El Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial (ICS-CERT) trabaja para reducir los riesgos dentro y entre todos los sectores de infraestructuras críticas y colabora con equipos de respuesta a incidentes informáticos (CIRT) internacionales y del sector privado para compartir incidentes de seguridad relacionados con los sistemas de control y medidas de mitigación. La comunidad de ciberseguridad del gobierno federal está llevando a cabo actualmente compromisos específicos de dispositivos con comunidades específicas de OT, en temas como las actualizaciones seguras de las bombas de infusión. La comunidad de OT debería participar en las acciones de la industria citadas en este informe para impulsar soluciones específicas del sector para sus riesgos cibernéticos individualizados.

Objetivo 5: Aumentar la concienciación y la educación en todo el ecosistema.

Para mejorar la resistencia del ecosistema de Internet y las comunicaciones frente a las amenazas distribuidas, todas las partes interesadas deben comprender y estar preparadas para ejecutar sus funciones y responsabilidades. Esta sección identifica acciones específicas para las amenazas distribuidas que cerrarían las brechas entre las habilidades y responsabilidades actuales.

Estas acciones propuestas no sustituyen los esfuerzos generales para aumentar la concienciación y la educación en materia de ciberseguridad. Las partes interesadas han indicado que estas amplias iniciativas de concienciación y educación en materia de ciberseguridad son fundamentales para aumentar la resistencia del ecosistema de forma sostenible. Por ejemplo, la importancia de comenzar la educación sobre ciberseguridad en una etapa temprana del proceso K-12 se destacó repetidamente en los comentarios públicos y las contribuciones en reuniones y talleres.

La Iniciativa Nacional para la Educación en Ciberseguridad90 (NICE), dirigida por el NIST en el Departamento de Comercio de Estados Unidos, es una asociación entre el gobierno, el mundo académico y el sector privado centrada en la educación, la formación y el desarrollo de la mano de obra en materia de ciberseguridad. Su misión es dinamizar y promover una sólida red y un ecosistema de educación, formación y desarrollo de la mano de obra en materia de ciberseguridad, centrándose en los trabajadores de la ciberseguridad. Los programas abarcan desde la educación en ciberseguridad desde el jardín de infancia hasta el 12º grado y las vías académicas universitarias, como los Centros Nacionales de Excelencia Académica en Ciberseguridad91 , hasta el desarrollo y la gestión de programas de evaluación y formación basados en el rendimiento. El Departamento de Seguridad Nacional complementa las contribuciones del NICE, desempeñando un papel vital en los esfuerzos de concienciación a través del programa STOP. PENSAR. CONNECT. [92].

Las siguientes acciones se basan en estos esfuerzos más generales de concienciación y educación en materia de ciberseguridad, identificando oportunidades de concienciación y educación específicamente relacionadas con la mitigación o prevención de las amenazas distribuidas.

[90] Iniciativa Nacional para la Educación en Ciberseguridad, Instituto Nacional de Normas y Tecnología, https://www.nist.gov/itl/applied-cybersecurity/nice (última visita el 4 de abril de 2018).
[91] Centros de Excelencia Académica en Ciberseguridad, Agencia de Seguridad Nacional, https://www.nsa.gov/resources/educators/centers-academic-excellence/ (última visita el 10 de abril de 2018). [92] Stop. Think. Connect., https://www.stopthinkconnect.org/ (visitado por última vez el 4 de abril de 2018).

Mejora de la resistencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y

Acción 5.1 El sector privado debería establecer y administrar herramientas informativas voluntarias para los dispositivos domésticos de la IO, con el apoyo de un proceso de evaluación escalable y rentable, en el que los consumidores puedan confiar y comprender intuitivamente.

El sector privado, en consulta con la sociedad civil y los expertos gubernamentales, debe diseñar un enfoque de evaluación y etiquetado eficiente y eficaz para los dispositivos de la IO, de modo que los consumidores conscientes de la seguridad puedan elegir con conocimiento de causa y crear incentivos de mercado para el desarrollo de productos seguros desde el punto de vista del diseño. Muchos de los productos de la IO disponibles en el mercado no se han diseñado teniendo en cuenta la seguridad. Estos dispositivos crean un riesgo sistémico para todos los miembros del ecosistema y ponen en peligro la privacidad y la seguridad de los consumidores. En un mundo ideal, los consumidores preferirían productos IoT que también protegieran su seguridad y privacidad, pero los consumidores preocupados por la seguridad no pueden identificar fácilmente qué productos IoT fueron diseñados para ser seguros.
Sin esta información, sus criterios de selección se limitan al precio y al conjunto de características.

El sector privado es el más adecuado para crear y mantener mecanismos ligeros y ágiles, pero a menudo puede beneficiarse del poder de convocatoria del gobierno. El gobierno federal debería convocar a la industria, la sociedad civil y las partes interesadas del gobierno en un proceso de múltiples partes interesadas para explorar los requisitos de un enfoque de etiquetado viable. Este esfuerzo puede basarse en los éxitos iniciales de programas como el proceso de múltiples partes interesadas de la NTIA sobre la capacidad de actualización y parcheado de la seguridad del IoT, que produjo un documento que detalla los elementos clave que los fabricantes deberían considerar comunicar a los consumidores tanto antes como después de la compra. [93] Las partes interesadas deben considerar si un mecanismo que se basa en la afirmación del proveedor es viable y satisface las necesidades de los consumidores domésticos. La viabilidad de dicho mecanismo podría basarse en parte en las prohibiciones existentes contra el engaño comercial. Por ejemplo, la Comisión Federal de Comercio podría proteger la integridad del mecanismo de evaluación tomando medidas contra el marketing engañoso (por *ejemplo, las* falsas afirmaciones de cumplimiento), entendiendo que las garantías de seguridad en este espacio no pueden ofrecer garantías similares en comparación con las afirmaciones de seguridad que permanecen estáticas en el tiempo. El DHS también podría apoyar el programa de evaluación a través de sus actuales actividades de concienciación, como STOP. PENSAR. CONECTAR. (Véase la acción 5.3). [94]

Aunque la seguridad y la privacidad de la IO no son perfectamente análogas, mecanismos como los programas de calificación de seguridad de 5 estrellas de la NHTSA y Energy Star han logrado concienciar a los clientes y crear mercados para vehículos seguros y electrodomésticos de bajo consumo, lo que apoya la hipótesis de que un enfoque de etiquetado bien concebido ayudaría a reducir los ataques automatizados y distribuidos. Sin embargo, el gran número de dispositivos IoT diferentes y el periodo de venta relativamente breve de muchos de estos dispositivos (en comparación con los coches y los calentadores de agua) indican que se necesitará un mecanismo más ligero y ágil. Dada la naturaleza global de los negocios hoy en día, el esquema de evaluación debería basarse en normas reconocidas internacionalmente siempre que sea posible. Además, cualquier uso de un enfoque de evaluación y etiquetado de seguridad tendría que reflejar las diferencias entre las afirmaciones de seguridad, que permanecen estáticas a lo largo del tiempo, y las afirmaciones de seguridad, que no pueden ofrecer garantías similares. El DHS podría complementar estos mecanismos de amplia aplicación explorando las oportunidades relativas a un régimen de certificación que pueda ser eficaz para apoyar las necesidades de las infraestructuras críticas.

También hay un papel para la evaluación subjetiva de los dispositivos IoT y su usabilidad. Las organizaciones de pruebas orientadas al consumidor suelen complementar los análisis basados en las características y los historiales de reparación con evaluaciones más subjetivas de la comodidad o la usabilidad. La usabilidad de las interfaces de gestión de la seguridad es un aspecto especialmente

[93] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (actualizado por última vez el 7 de noviembre de 2017). [94] Stop. Think. Connect., https://www.stopthinkconnect.org/ (visitado por última vez el 4 de abril de 2018).

problema difícil. Al incluir evaluaciones reflexivas sobre la usabilidad, las organizaciones de pruebas orientadas al consumidor pueden ayudar a los consumidores a identificar los productos que son apropiados para sus niveles de habilidad.

Acción 5.2 El sector privado debería establecer sistemas de etiquetado voluntarios para las aplicaciones industriales de la IO, con el apoyo de un proceso de evaluación escalable y rentable, para ofrecer una garantía suficiente para las aplicaciones de la IO en infraestructuras críticas.

Las infraestructuras críticas y las aplicaciones industriales del IoT presentan riesgos significativamente mayores para la nación que las aplicaciones domésticas en el contexto de los ataques automatizados y distribuidos. Estos dispositivos también se despliegan en entornos muy diferentes, con el apoyo de administradores profesionales. El mecanismo voluntario de evaluación ligera previsto en la acción 5.1 no ofrecería un nivel de garantía suficiente para estos clientes, y es probable que se necesiten características adicionales. Funciones de evaluación como la autenticación de dispositivos, las raíces de confianza del hardware o las funciones de actualización gestionadas requerirían una interacción directa con los productos, si no la revisión del código fuente.

Existen ejemplos de éxito de este proceso tanto en el sector público como en el privado. Por ejemplo, el Programa de Validación de Módulos Criptográficos del NIST ha recurrido a laboratorios de ensayo independientes para evaluar la seguridad de los módulos criptográficos con respecto a la norma FIPS 140 durante más de dos décadas. En el sector privado, la empresa de seguridad y certificación UL tiene una variedad de esquemas de certificación y cumplimiento para los mercados comerciales y de consumo, con más de 20 mil millones de marcas UL que aparecen en los productos en 2016. Sin embargo, un etiquetado fragmentado o demasiado complejo puede ser contraproducente. La FTC, con su considerable experiencia en materia de etiquetado, apoya la información clara, pero advierte de que "una información deficiente, incluida una información demasiado extensa, puede impedir la capacidad de los consumidores para tomar decisiones informadas".[95]

El sector privado debe establecer un proceso de evaluación eficiente pero sólido para garantizar que los dispositivos de la IO para estos sectores ofrezcan una mayor resistencia con un nivel de garantía adecuado. El establecimiento de una lista de productos evaluados permitirá a las empresas preocupadas por la seguridad elegir con conocimiento de causa y creará incentivos de mercado para los procesos de ciclo de vida de desarrollo seguro.

Acción 5.3 El gobierno debería animar a los sectores académico y de formación a integrar plenamente las prácticas de codificación segura en los programas de informática y afines.

Como se indica en la acción 1.3, muchas de las vulnerabilidades de seguridad más comunes (por *ejemplo,* los desbordamientos del búfer) pueden evitarse o remediarse durante el desarrollo del producto aplicando las herramientas de desarrollo de seguridad adecuadas, como los fuzzers, los analizadores estáticos y los lenguajes de programación seguros. Aunque las instituciones académicas, los campamentos de iniciación a la codificación y los programas de reciclaje laboral están creando una mayor mano de obra de codificación, sus graduados rara vez son hábiles en estos lenguajes o expertos en el uso de estas herramientas de desarrollo. En su lugar, los estudiantes adquieren una experiencia significativa con herramientas de desarrollo de software que no tienen en cuenta la seguridad, y con metodologías de desarrollo de software que no dan prioridad a la seguridad, lo que crea una mentalidad de "atornillar" en la mano de obra de desarrollo de software.

Las empresas que desean mejorar las prácticas de codificación pueden verse disuadidas por una mano de obra poco preparada y a veces resistente: los codificadores cualificados pueden cambiar fácilmente de trabajo si no están interesados en aprender las nuevas

[95] Comisión Federal de Comercio, *Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers",* en la página 6, (2017), *disponible en* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications- information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

prácticas, y pueden ser difíciles de sustituir. Si enseñamos metodologías de software seguras y fomentamos el uso de cadenas de herramientas de desarrollo de software que tengan en cuenta la seguridad en todos los planes de estudios de informática y de ciberseguridad, podemos preparar a nuestros trabajadores para crear software de mayor calidad y aumentar la aceptación de las cadenas de herramientas de desarrollo de software centradas en la seguridad.

El gobierno federal puede facilitar estos cambios a través de las relaciones existentes con el mundo académico y la industria de la formación. En particular, el NICE debería comprometerse con el mundo académico y el sector privado para incorporar los principios de seguridad por diseño y las herramientas de apoyo en cada paso del curso de estudio. La categoría de "Provisión segura" del Marco de Ciberseguridad del NICE (NICE Framework) incluye los conocimientos, habilidades y destrezas que se necesitan para el desarrollo de software y productos seguros. El NICE debería asociarse con los proveedores de educación y formación para animarles a utilizar el Marco NICE como herramienta de referencia para el desarrollo del contenido de los cursos. Como otro ejemplo, la FTC organiza una conferencia anual, la PrivacyCon, que proporciona un escaparate para el trabajo sobre privacidad y seguridad de académicos e investigadores de seguridad. [96]

Acción 5.4 El sector académico, en colaboración con la Iniciativa Nacional para la Enseñanza de la Ciberseguridad, debería establecer la ciberseguridad como requisito fundamental en todas las disciplinas de la ingeniería.

A medida que la TI se integra en toda la gama de productos y servicios, surgen amenazas de ciberseguridad en nuevas clases de productos. Los diseñadores de productos no suelen ser conscientes de los riesgos que pueden introducirse al integrar las TI en las líneas de productos tradicionales. La necesidad de que estos trabajadores comprendan la gestión de los riesgos de ciberseguridad es cada vez mayor, ya que incorporamos sensores en numerosos entornos, como el suelo, las carreteras y los edificios. Por ejemplo, las cámaras de circuito cerrado de televisión (CCTV) han estado disponibles comercialmente desde 1949, pero solo recientemente han evolucionado hacia dispositivos conectados a Internet. En 2016, la red de bots Mirai comprometió más de 100.000 cámaras de CCTV para apoyar los ataques DDoS. En otros casos, las cámaras conectadas a Internet utilizadas como monitores de bebés han sido hackeadas explotando las contraseñas administrativas por defecto, violando la privacidad de los propietarios. [97]

Para garantizar que los diseñadores de productos sean conscientes de los riesgos introducidos en la tecnología operativa, las instituciones académicas que enseñan ingeniería y disciplinas afines deberían integrar la ciberseguridad básica en el plan de estudios requerido. Al igual que en el caso anterior, el NICE debería colaborar con el mundo académico y el sector privado para incorporar los principios en el curso de estudios de ingeniería y disciplinas afines.

Acción 5.5 El gobierno federal debería establecer una campaña de concienciación pública para apoyar el reconocimiento y la adopción de la línea de base y la marca de seguridad de los dispositivos del IoT en el hogar.

Para lograr un impacto, la línea de base de la seguridad de los dispositivos IoT en el hogar debe ser reconocida y preferida por los consumidores conscientes de la seguridad, mejorando la resistencia de las redes domésticas donde se instalan los dispositivos y estableciendo incentivos de mercado para los vendedores conscientes de la seguridad. El gobierno federal tiene un largo historial de campañas de concienciación pública, llevadas a cabo con el apoyo de las partes interesadas, para abordar una amplia variedad de temas: cómo prevenir los incendios forestales, el valor de los cinturones de seguridad y la importancia de las pruebas del VIH. La campaña Stop. Think.
Connect. es una campaña nacional de concienciación patrocinada por el DHS que tiene como objetivo aumentar la

[96] *Véase* Comisión Federal de Comercio, *PrivacyCon 2018*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018 (última visita el 4 de abril de 2018).
[97] *Véase* Darlene Storm, *Hacker Hijacks Wireless Foscam Baby Monitor,* Talks *and Freaks Out Nanny*, Computerworld (2 de febrero de 2015, 12:09 PM PT), https://www.computerworld.com/article/2878741/hacker-hijacks- wireless-foscam-baby-monitor-talks-and-freaks-out-nanny.html.

de las ciberamenazas y capacitar al público estadounidense para que esté más seguro en línea. El gobierno federal debería considerar la posibilidad de aprovechar Stop. Think. Connect. o establecer una campaña de concienciación pública complementaria para alertar a los usuarios domésticos y a las pequeñas organizaciones sobre la importancia de la línea de base de los dispositivos IoT en el hogar y educarlos sobre cómo identificar productos más seguros. En términos más generales, una mayor concienciación de los usuarios sobre el riesgo de la ciberseguridad es fundamental para un ecosistema resistente, y el gobierno debería aumentar su compromiso estratégico y su poder de convocatoria con comunidades de usuarios específicas y con la sociedad civil para mejorar la adopción y la concienciación sobre la seguridad, dando la bienvenida a cualquier parte interesada no gubernamental que desee desempeñar un papel más importante.

* * *

Próximos pasos iniciales para la acción de las partes interesadas

La sección anterior detalla 24 acciones diseñadas para alcanzar cinco objetivos. Los cinco objetivos se apoyan mutuamente; los cinco objetivos deben alcanzarse para aumentar de forma sostenible la resistencia del ecosistema de Internet y las comunicaciones. Muchas de las acciones también se apoyan mutuamente por diseño, incluso entre objetivos, por lo que excluir u omitir una acción podría retrasar la consecución de varios objetivos. Sin embargo, no esperamos que todas las acciones se lleven a cabo simultáneamente, debido a consideraciones tales como la limitación de recursos en las comunidades de partes interesadas pertinentes. Además, algunas acciones ya están en marcha, mientras que otras dependen de factores externos. El gobierno federal no liderará la implementación de acciones específicas para la industria. Sin embargo, entendiendo que en algunos casos puede llevar tiempo que el sector privado se organice, el gobierno de EE.UU. empezará a coordinar inmediatamente los pasos iniciales que se describen a continuación.

Desarrollar una hoja de ruta prioritaria para las acciones coordinadas con el fin de aumentar la resistencia del ecosistema de Internet y las comunicaciones contra las amenazas distribuidas.

Para garantizar que las acciones más importantes cuenten con los recursos adecuados y sean ejecutadas de forma eficiente por las partes interesadas, éstas han instado encarecidamente al gobierno federal a delinear claramente las prioridades de acción. [98] En particular, algunas acciones no implican directamente al gobierno federal, pero apoyan, o son apoyadas por, acciones que dependen de la participación o el liderazgo federal. Al indicar sus propias prioridades, el gobierno federal puede aumentar la confianza de las partes interesadas en que los recursos invertidos en las acciones dirigidas por la industria que dependen del gobierno federal darán resultados productivos.

Además de las dependencias federales, algunas acciones tienen un orden temporal natural: por ejemplo, los programas de evaluación de las acciones 5.1 y 5.2 dependen del establecimiento de líneas de base de capacidad de seguridad adecuadas en la acción 1.1. Otras acciones están listas para ser priorizadas porque el trabajo preparatorio está en marcha, como el perfil de la CSF descrito en la Acción 2.2. Por último, algunas acciones tienen una urgencia especial debido a su largo plazo (por *ejemplo,* las acciones 1.3, 5.3 y 5.4) o a que los acontecimientos están reduciendo el margen de maniobra de Estados Unidos para influir en la dirección (acción 1.2).

Los Departamentos de Comercio y Seguridad Nacional, en coordinación con la industria, la sociedad civil y en consulta con los socios internacionales, deberían encargarse de desarrollar una hoja de ruta inicial con acciones prioritarias en un plazo de 120 días tras la aprobación de este informe. Esta hoja de ruta debería alinearse con

[98] Esta solicitud se destacó tanto en las respuestas de las partes interesadas a la solicitud de comentarios del 5 de enero de 2018 como en el taller del 28 de febrero al 1 de marzo de 2018.

Las prioridades de la Administración, tal y como se han establecido tras la finalización de las tareas asignadas en virtud del Decreto 13800. La Administración y el sector privado colaborarán para garantizar que la hoja de ruta se actualice y se mantenga a medida que las partes interesadas realicen las acciones identificadas.

El gobierno federal predicará con el ejemplo.

Las partes interesadas indicaron que el liderazgo federal mediante el ejemplo es fundamental para la aplicación del informe por otras partes interesadas. Las partes interesadas indicaron que la adopción por parte del gobierno federal de prácticas de "buena vecindad" que benefician principalmente al ecosistema y a las actividades de adquisición proporcionaría una base para otras actividades destinadas a reducir las amenazas automatizadas y distribuidas. En particular, las medidas adoptadas por los organismos federales para aplicar el filtrado de salida con el fin de evitar la falsificación de direcciones de red, cerrar los reflectores utilizados para amplificar los volúmenes de tráfico y medir el cumplimiento de los organismos (y potencialmente nombrar y avergonzar a los malos actores) demostrarían la determinación federal y fomentarían la acción beneficiosa de otras partes. El NIST, la OMB y el DHS deberían explorar los pasos para garantizar que estas mejores prácticas se reflejen adecuadamente en las políticas, normas, directrices y supervisión de las agencias federales.

Del mismo modo, las actividades de contratación pública federal que exigen la adquisición de productos y servicios más seguros o resistentes que los disponibles actualmente se consideraron un paso importante para establecer incentivos de mercado. Las partes interesadas sugirieron centrarse inmediatamente en las acciones 1.1, 1.2 y 2.3 para apoyar la orientación de la contratación pública federal. Este trabajo de diseño puede conducir a una evaluación de las orientaciones y normas de contratación existentes, así como a recomendaciones específicas para actualizar dichas orientaciones de modo que reflejen los requisitos de seguridad.

Fomentar el liderazgo del sector privado y apoyar la coordinación intersectorial para seguir la aplicación de la hoja de ruta.

Muchas de las acciones de la hoja de ruta deberían ser dirigidas por un sector industrial, académico o de la sociedad civil. La identificación o el establecimiento de estructuras de gobierno del sector privado para estas actividades será un factor crítico para la sostenibilidad y la aceptación internacional de los productos del trabajo (por *ejemplo,* especificaciones técnicas o esquemas de evaluación). En los casos en los que los organismos existentes ya están llevando a cabo acciones relacionadas, o ya representan a comunidades clave, se les debe animar a liderarlas. Las acciones pueden requerir la inclusión más allá de las estructuras actuales, por ejemplo, añadiendo participantes o perspectivas de la sociedad civil o internacionales.

A medida que se formen comunidades para implementar estas acciones, será cada vez más importante establecer un lugar para la coordinación regular entre estas comunidades. El valor de una línea de base de seguridad de la IO es limitado si no se puede establecer un esquema de evaluación de manera oportuna. Es necesario alinear y coordinar las inversiones para maximizar el impacto en la resiliencia de la infraestructura. Hasta que se identifique una o varias partes del sector privado de mutuo acuerdo, el gobierno federal proporcionará un mecanismo de coordinación y comunicación para la aplicación continua, y convocará reuniones periódicas de las partes pertinentes.

Presentar al Presidente un informe de situación de 365 días sobre la aplicación de la hoja de ruta.

Para hacer un seguimiento de los avances, los Departamentos de Comercio y Seguridad Nacional elaborarán una actualización de la situación de 365 días para el Presidente, que deberá presentarse un año después de la publicación inicial de la hoja de ruta. Esta actualización revisará:
1) los progresos que la comunidad en su conjunto está realizando con respecto a la hoja de ruta; 2) las repercusiones de esas actividades de la hoja de ruta; 3) una reevaluación de la amenaza de los ataques automatizados y distribuidos, incluyendo si la

amenaza está aumentando o disminuyendo, y cualquier razón conocida para tal cambio; y 4) si se requiere algún ajuste en la hoja de ruta.

Promover la participación global a través de un mayor compromiso de las partes interesadas y del gobierno de Estados Unidos en el desarrollo de políticas y normas internacionales.

La naturaleza global de las amenazas distribuidas se destacó con frecuencia durante el proceso ejecutado por Comercio y Seguridad Nacional. Las partes interesadas destacaron la importancia de las normas, políticas y mejores prácticas internacionales para promover la participación y la colaboración internacional. Al seguir defendiendo los enfoques dirigidos por la industria y participar activamente en el desarrollo de normas internacionales voluntarias y consensuadas, el gobierno federal puede contribuir a la elaboración de normas pragmáticas y eficaces basadas en resultados que satisfagan las necesidades de todas las partes interesadas. El gobierno federal también está en una posición única para liderar el compromiso internacional necesario para establecer políticas y mejores prácticas ampliamente aceptadas y mejorará la coordinación con las partes interesadas en estos esfuerzos.

Apéndice: Lista de acrónimos

AI	Inteligencia artificial
BCP	Mejores prácticas actuales
BGP	Protocolo de pasarela fronteriza
CCTV	Circuito cerrado de televisión
CDN	Red de distribución de contenidos
CIRT	Equipo de respuesta a incidentes informáticos
CISA	Ley de intercambio de información sobre ciberseguridad de 2015
LCR	Marco de ciberseguridad del NIST
CSIRT	Equipo de respuesta a incidentes de seguridad informática
CSRIC	Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones
DDoS	Negación de servicio distribuido
DHS	Departamento de Seguridad Nacional
DNS	Sistema de nombres de dominio
FIPS	Normas federales de tratamiento de la información
PRIMERO	Foro de Equipos de Seguridad y Respuesta a Incidentes
FTC	Comisión Federal de Comercio
GSA	Administración de Servicios Generales
HTTPS	Protocolo de transferencia de hipertexto seguro
ICANN	Corporación de Asignación de Nombres y Números de Internet
ICS-CERT	Equipo de respuesta a emergencias cibernéticas en sistemas de control industrial
IETF	Grupo de Trabajo de Ingeniería de Internet
IoT	Internet de los objetos
IP	Protocolo de Internet
IPv4	Protocolo de Internet versión 4
IPv6	Protocolo de Internet versión 6
ISAC	Centro de análisis e intercambio de información
ISP	Proveedor de servicios de Internet
IT	Tecnología de la información
LAN	Red de área local
MANRS	Normas mutuamente acordadas para la seguridad de las rutas
MUD	Descripción del uso del fabricante
NAT	Traducción de direcciones de red
NCC	Centro Nacional de Coordinación de Comunicaciones
NCCIC	Centro Nacional de Integración de la Ciberseguridad y las Comunicaciones
NHTSA	Administración Nacional de Seguridad Vial
NICE	Iniciativa Nacional para la Educación en Ciberseguridad
NIST	Instituto Nacional de Normas y Tecnología
NISTIR	Informe interinstitucional/interno del NIST
NITRD	Investigación y desarrollo de redes y tecnologías de la información
NOG	Grupo de operadores de red

NSTAC	Comité Asesor de Seguridad Nacional de Telecomunicaciones del Presidente
NTIA	Administración Nacional de Telecomunicaciones e Información
OT	Tecnología operativa
PPD	Directiva Política Presidencial
RFC	Solicitud de comentarios
RIR	Registro regional de Internet
SAM	Gestión de activos de software
SCADA	Control de supervisión y adquisición de datos
SSAC	Comité Consultivo de Seguridad y Estabilidad