Una hoja de ruta

Hacia la resiliencia contra las redes de bots

---

29 de noviembre de 2018

Índice de contenidos

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", en la que pedía "resiliencia contra las botnets y otras amenazas automatizadas y distribuidas".[1] El Presidente ordenó a los Secretarios de Comercio y Seguridad Nacional que "lideraran 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)".[2]

Los Departamentos de Comercio y Seguridad Nacional trabajaron conjuntamente en el esfuerzo, publicando el informe sobre la mejora de la resiliencia del ecosistema de Internet y las comunicaciones contra las redes de bots y otras amenazas automatizadas y distribuidas, conocido como el informe sobre redes de bots, en mayo de 2018.[3] Basado en las aportaciones de las partes interesadas de la industria y el gobierno, el informe pidió al gobierno federal que delineara claramente las prioridades de acción.

Esta hoja de ruta inicial establece acciones que podrían reducir drásticamente la amenaza de las botnets y ataques similares, en consonancia con las prioridades de la Administración establecidas en la Estrategia Cibernética Nacional. [4] La hoja de ruta identifica cinco líneas de esfuerzo, cada una con un conjunto de tareas y plazos para su realización. En esta versión inicial, se enumeran 85 tareas, pero ese número cambiará con el tiempo a medida que se completen algunas tareas y surjan otras nuevas.

Como se explica en el informe de la red de bots, muchas de las acciones del informe se apoyan mutuamente por su diseño, incluso entre objetivos. Algunas acciones ya están en marcha, otras dependen de factores externos, y un conjunto final espera el liderazgo y/o la financiación. No esperamos que todas las acciones se lleven a cabo de forma simultánea, debido a consideraciones como la limitación de recursos o los diferentes niveles de sofisticación de las comunidades interesadas. También cabe destacar que, aunque estas acciones se identificaron en el Informe sobre redes de bots, su aplicación hará que el ecosistema general de Internet sea más seguro y tendrá un impacto que va mucho más allá de los límites del propio informe.

La hoja de ruta que sigue establece las tareas relacionadas con cada acción en el contexto de cinco líneas de esfuerzo:

1. Internet de las cosas;
2. Empresa;
3. Infraestructura de Internet;
4. Desarrollo y Transición Tecnológica; y
5. Sensibilización y educación.

Algunas tareas serán responsabilidad directa del gobierno federal, mientras que otras son específicas del sector privado. Algunas tareas 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 acciones dirigidas por la industria con dependencia federal darán resultados productivos.

---

[1] Exec. Order No. 13,800, 82 Fed. Reg. 22.391, en 22.394 (11 de mayo de 2017), *disponible en* https://www.federalregister.gov/d/2017-10004.

[2] *Id.*

[3] Departamento de Comercio y Departamento de Seguridad Nacional de Estados Unidos, A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (mayo de 2018), *disponible en* https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets.

[4] Nat'l Sec. Council, National Cyber Strategy of the United States of America (septiembre de 2018), *disponible en* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Los Departamentos de Comercio y Seguridad Nacional siguen acogiendo con agrado el interés de los miembros del sector privado que deseen contribuir a una acción del Informe sobre redes de bots. Muchas de las acciones de la hoja de ruta deberían ser dirigidas por la industria, el mundo académico o la sociedad civil. Cuando procede, esta hoja de ruta identifica a los líderes del sector privado o las estructuras de gobierno existentes para las tareas pertinentes. Cuando los organismos existentes ya están llevando a cabo acciones relacionadas, o ya representan a comunidades clave, se les anima a liderarlas. El gobierno tiene el poder de convocatoria y lo hará, pero la consecución de los resultados establecidos en el Informe sobre redes de bots requerirá la participación de la industria y la sociedad civil de todo el ecosistema. Las tareas identificadas y la información asociada deben considerarse como no vinculantes y flexibles para adaptarse a los cambios en el ecosistema digital a lo largo del tiempo.

En los casos en los que aún no se haya identificado una o varias partes del sector privado de mutuo acuerdo para liderar, el gobierno federal proporcionará un mecanismo de coordinación y comunicación. El gobierno federal también se reunirá periódicamente con las partes pertinentes para facilitar la colaboración y compartir los resultados. Las organizaciones identificadas como "contribuyentes" en los desgloses de tareas que se indican a continuación constituyen una lista no exhaustiva de los esfuerzos actuales que están contribuyendo a las soluciones. Se anima a las organizaciones a buscar oportunidades para colaborar y asociarse en la medida de lo posible. El gobierno de Estados Unidos valora la innovación y espera que el mercado determine las soluciones más rápidas para los problemas identificados.

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, y por tanto no pueden comenzar inmediatamente. Otras acciones están listas para ser priorizadas porque el trabajo ya está en marcha, como el perfil del Marco de Ciberseguridad (CSF) del Instituto Nacional de Normas y Tecnología (NIST) descrito en la Acción 2.2. Por último, algunas acciones tienen una urgencia especial debido a su largo plazo de ejecución (por ejemplo, las acciones 1.3, 5.3 y 5.4) o porque los acontecimientos están reduciendo el margen para que Estados Unidos influya en la dirección (acción 1.2).

Por último, para hacer un seguimiento de los avances, el Departamento de Comercio (Commerce) y el Departamento de Seguridad Nacional (DHS) elaborarán una actualización de la situación de 365 días para el Presidente, prevista 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) los impactos 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) qué actividades deben ser priorizadas en el próximo año.

II. Mapa de carreteras

Las siguientes subsecciones presentan tareas extraídas de las 24 acciones establecidas en el Informe sobre la red de bots en el contexto de cinco *líneas de esfuerzo*:

1. Internet de las cosas;
2. Empresa;
3. Infraestructura de Internet;
4. Desarrollo y Transición Tecnológica; y
5. Sensibilización y educación.

Las cinco líneas de esfuerzo se subdividen a su vez en *flujos de trabajo compuestos* por *tareas* breve resumen y una referencia a un número de acción del Informe sobre redes de bots, identifica los líderes de las tareas (si se determinan) y los actores de apoyo, identifica las tareas que deben completarse antes de comenzar o completar, y propone fechas de inicio y finalización por trimestre del año natural**.** El Departamento de Comercio y el DHS agradecen los comentarios de las partes interesadas sobre todos los elementos de las tareas de la hoja de ruta, en particular la identificación de los líderes y los socios que contribuyen a las acciones identificadas, así como los plazos.

Línea de esfuerzo de IoT: Subiendo el listón de la seguridad del IoT

El Informe sobre redes de bots reconoció el impacto de los dispositivos conectados en la capacidad de ampliar el alcance y la escala de los ataques automatizados y distribuidos contra objetivos del ecosistema. La línea de esfuerzo del Internet de las Cosas (IoT) se centra en reducir el riesgo de seguridad en todo el ecosistema del IoT mediante el establecimiento de normas de seguridad básicas aplicadas en todo el ciclo de vida de los dispositivos conectados.

Corriente de trabajo de IoT 1: Desarrollo de mercados sólidos para dispositivos de IoT fiables

Esta línea de trabajo se centra en el desarrollo de un mercado sólido de dispositivos que ofrezcan capacidades de seguridad adecuadas para tres sectores: consumidores/usuarios domésticos, usuarios industriales y el gobierno federal. La tarea inicial fundacional describe un conjunto básico de capacidades de seguridad que son ampliamente aplicables (idealmente, aplicables a los tres sectores) y que pueden ser apoyadas por una amplia gama de esquemas de evaluación. Una vez definido el núcleo, se lanzan series de tareas concurrentes para cada uno de los tres sectores. Cada serie de tareas define un superconjunto del núcleo de referencia adecuado para ese sector, seguido de un conjunto de actividades de apoyo diseñadas para desarrollar un mercado sólido para los productos conformes.

Definición de una línea de base de la capacidad de seguridad básica

Esta tarea establece un conjunto básico de capacidades de seguridad necesarias para el despliegue seguro de los dispositivos IoT, independientemente del entorno previsto. Las capacidades básicas de seguridad deben ser proporcionadas o facilitadas por plataformas de desarrollo comunes para limitar el impacto en el tiempo de comercialización y permitir la innovación. Estas capacidades básicas también deben ser apropiadas tanto para los esquemas de evaluación de la conformidad basados en la atestación como en la evaluación por parte de terceros.

Nombre de la tarea: Definir la línea de base de la capacidad de seguridad básica

Número de acción: 1.1

Resumen de la tarea: Comparar/analizar diferentes documentos de referencia para identificar las "capacidades básicas de seguridad" ampliamente aceptadas y aplicables que podrían ser respaldadas por toda la gama de esquemas de evaluación. Como mínimo, la línea de base de capacidades abordaría la seguridad de los dispositivos y los datos. El NIST publicará la línea de base consensuada como un libro blanco del NIST o un informe interinstitucional (NISTIR) para su referencia y uso en futuras tareas.

Colaborador(es): NIST (líder), propietarios de líneas de base, proveedores de kits de desarrollo, consorcios de consumidores, Consejo para la Seguridad de la Economía Digital (CSDE)5/Asociación de Tecnología de [Consumo] (CTA) Tareas previas: N/A

Inicio previsto6: 1T19 Finalización prevista: 3Q19

Establecer un mercado sólido para dispositivos IoT domésticos y de confianza

Las siguientes tareas están diseñadas para establecer una base de capacidad de seguridad ampliamente adoptada para los productos del IoT de consumo/doméstico con una alta disponibilidad de productos y un fuerte reconocimiento de los clientes. Estas tareas comienzan por aumentar la base de capacidades de seguridad básicas con requisitos específicos para el mercado del IoT de consumo/doméstico. Para fomentar el desarrollo y el despliegue de dispositivos conformes, se crea un sistema de certificación o evaluación junto con herramientas educativas y de concienciación que ayudarán a los clientes a tomar decisiones informadas sobre las compras de IoT.

Nombre de la tarea: Desarrollar una línea de base de seguridad de IoT para el consumidor y el hogar

Número de acción: 1.1

Resumen de la tarea: Construir sobre las capacidades básicas para identificar la línea de base de seguridad apropiada para el IoT de los consumidores/del hogar.

Colaborador(es): Industria del IoT, sociedad civil, NIST, CSDE/CTA Tareas previas: Publicar la línea de base de la capacidad de seguridad básica Inicio previsto: 2Q19

Finalización prevista: 1Q20

Nombre de la tarea: Establecer o apoyar programas de evaluación para los dispositivos IoT de los consumidores/del hogar

Número de acción: 5.1

Resumen de la tarea: Establecer o apoyar programas ágiles de evaluación o certificación para dispositivos IoT de consumo/domésticos que cumplan con la línea de base mencionada.

Contribuyente(s): Industria, sociedad civil, CTIA, NIST, otras partes interesadas del gobierno estadounidense (USG), CSDE/CTA

Tareas previas: Desarrollar la línea de base de la seguridad del consumidor/del hogar de IoT Inicio previsto: En curso

Finalización prevista: 2Q20

Nombre de la tarea: Explorar el etiquetado para el IoT de los consumidores/del hogar

Número de acción: 5.1

Resumen de la tarea: Explorar la utilidad de un enfoque de etiquetado voluntario, u otras opciones informativas, para mejorar el conocimiento de los consumidores/dispositivos IoT domésticos.

Contribuyente(s): Comisión Federal de Comercio (FTC), NTIA, otros socios federales, industria de la IO, minoristas, sociedad civil, academia, CSDE/CTA

Tareas previas: N/A Inicio previsto: 4Q19 Finalización prevista: 4Q20

Nombre de la tarea: Implementar estrategias de concienciación para dispositivos IoT domésticos/de consumo de confianza

Número de acción: 5.1

Resumen de la tarea: Desarrollar herramientas informativas, como el etiquetado o la marca, que ayuden a los consumidores motivados a identificar los productos de consumo/domésticos de IO conformes.

Contribuyente(s): Industria del IoT, minoristas, CSDE/CTA

Tareas previas: Establecer un programa de evaluación para los dispositivos IoT de los consumidores/del

hogar; explorar el etiquetado para el IoT de los consumidores/del hogar
Inicio previsto: 2T20
Finalización prevista: 2T21

Nombre de la tarea: Apoyo federal a la línea de base y evaluación de la seguridad de los consumidores/del IoT en el hogar Número de acción: 5.5

Resumen de la tarea: Aumentar el compromiso del SGA con las comunidades de usuarios seleccionadas y la sociedad civil para promover la concienciación y la aceptación de la línea de base de la seguridad de la IO de los consumidores/del hogar y los programas de evaluación de apoyo; aprovechar las actividades de concienciación existentes del DHS, como STOP.THINK.CONNECT.

Contribuyente(s): DHS, Comercio, FTC, sociedad civil

Tareas previas: Desarrollar una línea de base de seguridad para el consumidor/el IoT doméstico; establecer un programa de evaluación para los dispositivos del IoT doméstico.

Inicio previsto: 2Q20

Finalización prevista: 1Q23

Establecer un mercado sólido para los dispositivos industriales del IoT de confianza

Las siguientes tareas están diseñadas para establecer una base de capacidad de seguridad ampliamente adoptada para los productos del IoT industrial con una alta disponibilidad de productos y un fuerte reconocimiento de los clientes. Estas tareas comienzan por aumentar la línea de base de la capacidad de seguridad básica con requisitos específicos para el mercado del IoT industrial. Para fomentar el desarrollo y el despliegue de dispositivos conformes, se crean uno o varios esquemas de evaluación junto con herramientas educativas y de concienciación para informar a los clientes.

Nombre de la tarea: Desarrollar la línea base de seguridad del IoT industrial
Número de acción: 1.1
Resumen de la tarea: Aprovechar las capacidades básicas para identificar la línea de base de seguridad apropiada para los entornos industriales/SCADA.
Contribuyente(s): Industria del IoT, laboratorios nacionales, DHS, agencias sectoriales, consejos de coordinación sectorial (por ejemplo, Energía, Salud, Transporte)
Tareas previas: Publicar la línea de base de la capacidad de seguridad básica
Inicio previsto: 2Q19
Finalización prevista: 4Q19

Nombre de la tarea: Establecer un programa de evaluación para los dispositivos industriales del IoT
Número de acción: 5.2
Resumen de la tarea: Establecer uno o varios programas de evaluación rentables para los dispositivos industriales del IoT que cumplan los requisitos básicos.
Contribuyente(s): Industria del IoT, laboratorios nacionales, DHS, agencias sectoriales, consejos de coordinación sectorial (por ejemplo, Energía, Salud, Transporte)
Tareas previas: Desarrollar la línea de base de la seguridad del IoT industrial
Inicio previsto: 4Q19
Finalización prevista: 2Q20

Nombre de la tarea: Explorar el etiquetado u otro esquema de transparencia para los dispositivos industriales del IoT

Número de acción: 5.2
Resumen de la tarea: Trabajar para desarrollar un enfoque de etiquetado voluntario, u otro esquema de transparencia de la información, como opción para informar a los clientes de las empresas industriales.
Contribuyente(s): Industria del IoT, laboratorios nacionales, DHS, agencias sectoriales, consejos de coordinación sectorial (por ejemplo, Energía, Salud, Transporte)
Tareas previas: Desarrollar la línea de base de la seguridad del IoT industrial
Inicio previsto: 4Q19
Finalización prevista: 4Q20

Nombre de la tarea: Concienciación de apoyo a los clientes de los dispositivos industriales del IoT
Número de acción: 5.2
Resumen de la tarea: Crear herramientas informativas, como etiquetas o marcas, que ayuden a los clientes de las empresas industriales a identificar los productos del IoT industrial que sean conformes.
Contribuyente(s): Industria del IoT, minoristas, DHS a través del Consejo Nacional de Centros de Análisis e Intercambio de Información (ISAC)
Tareas previas: Desarrollar la línea de base de la seguridad del IoT industrial
Inicio previsto: 2Q20
Finalización prevista: 4Q20

Nombre de la tarea: Promover la adopción del régimen de evaluación por parte de las infraestructuras críticas
Número de acción: 5.2
Resumen de la tarea: A través del Consejo ISAC, el DHS y la industria evaluarán el régimen o los regímenes de certificación comercial para los productos de IoT y TI a medida que surjan para su aplicabilidad a las infraestructuras críticas.
Contribuyente(s): DHS (Líder), industria de IoT, laboratorios nacionales, DHS, agencias específicas del sector, consejos de coordinación del sector (por ejemplo, Energía, Salud, Transporte)
Tareas previas: Establecer un programa de evaluación de los dispositivos industriales del IoT Inicio previsto: 3Q20
Finalización prevista: 2Q21

Establecer un mercado sólido para dispositivos federales de IoT de confianza

Las siguientes tareas están diseñadas para establecer una base de capacidad de seguridad ampliamente adoptada para los productos federales del IoT con una alta disponibilidad de productos y un fuerte reconocimiento de los clientes. Estas tareas comienzan por aumentar la línea de base de la capacidad de seguridad básica con requisitos específicos para el mercado federal del IoT.
Para fomentar la adquisición y el despliegue de dispositivos conformes, se establece una normativa federal de contratación que hace referencia a la línea de base federal.

Nombre de la tarea: Identificar los requisitos federales de seguridad del IoT
Número de acción: 2.3
Resumen de la tarea: Convocar a las principales partes interesadas en una serie de reuniones para identificar las capacidades de seguridad no esenciales que son comunes/específicas de los entornos federales.
Contribuyente(s): Oficina de Gestión y Presupuesto (OMB), Administración de Servicios Generales (GSA), Departamento de Defensa (DOD), DHS, NIST, Consejo Federal de Directores de Información (CIO), directores federales de seguridad de la información (CISO)
Tareas previas: Publicar la línea de base de la capacidad de

seguridad básica Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Especificar la línea de base de la capacidad de seguridad del IoT federal
Número de acción: 2.3
Resumen de la tarea: En colaboración con la industria y las agencias, desarrollar y publicar una línea de base de la capacidad de seguridad del IoT federal.
Colaborador(es): NIST (líder), DHS, Consejo Federal de CIOs, CISOs federales, industria, CSDE/CTA
Tareas previas: Identificar los requisitos federales de seguridad de la IO
Inicio previsto: 3T19
Finalización prevista: 1Q20

Nombre de la tarea: Establecer la normativa federal de contratación de la IO
Número de acción: 2.3
Resumen de la tarea: Establecer reglamentos de contratación pública federal para apoyar la adquisición de dispositivos de IoT coherentes con la línea de base de la capacidad de seguridad federal de IoT.
Colaborador(es): GSA (líder), OMB, Consejo Federal de CIOs, CISOs federales y oficiales de compras
Requisito previo Tareas: Especificar la línea de base de la capacidad de seguridad del IoT federal
Inicio previsto: TBD Finalización
prevista: TBD

Corriente de trabajo de IoT 2: Adopción y sostenibilidad de la seguridad de IoT

Esta línea de trabajo se centra en el desarrollo del ecosistema global de los dispositivos de la IO en general. Es decir, la cartera de acciones especificadas en esta corriente de trabajo mejora la seguridad de los productos de la IO y promueve la confianza en el mercado de la IO, independientemente de las tres líneas básicas de seguridad específicas del sector. Las tareas se centran en la colaboración entre las comunidades de ciberseguridad y de tecnología operativa, así como en la promoción de políticas internacionales, la armonización y las normas. Con la excepción del desarrollo de normas de IoT relevantes a nivel mundial, estas actividades tienen pocas dependencias. Un reto clave será priorizar las actividades para reflejar la disponibilidad de recursos.

Ampliación de la gestión de riesgos para el IoT

Muchos programas de ciberseguridad de las empresas han cambiado a enfoques basados en el riesgo, como el Marco de Ciberseguridad del NIST. Las normas, directrices y mejores prácticas que estas organizaciones aprovechan para gestionar el riesgo relacionado con la ciberseguridad utilizando el Marco y los enfoques relacionados se han centrado históricamente en la tecnología de la información (TI) y las redes de TI tradicionales. En esta serie de tareas, los enfoques de gestión de riesgos se amplían para ayudar a las organizaciones a comprender y gestionar mejor los riesgos de ciberseguridad y privacidad asociados a sus dispositivos IoT a lo largo de su ciclo de vida.

Nombre de la tarea: Habilitar el enfoque de gestión de riesgos para la seguridad del IoT
Número de acción: 1,5
Resumen de la tarea: Publicar NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" (Consideraciones para la gestión de los riesgos de la Internet de las cosas), para apoyar los enfoques de gestión de riesgos de la seguridad de la Internet de las cosas. Colaborador(es): NIST (líder), industria
Tareas previas: N/A Inicio previsto: En
curso Finalización prevista: 1Q19

Nombre de la tarea: Publicar las mejores prácticas para los fabricantes de dispositivos IoT
Número de acción: 1,5
Resumen de la tarea: Identificar las mejores prácticas que contribuyen a los resultados de los clientes identificados en el emergente NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" (Consideraciones para la gestión de los riesgos de ciberseguridad y privacidad de la Internet de las cosas) utilizando las capacidades de seguridad básicas.
Colaborador(es): NIST (líder), TBD
Tareas previas: Habilitar el enfoque de gestión de riesgos para la seguridad del IoT; publicar la línea de base de la capacidad de seguridad básica
Inicio previsto: 2Q19 Finalización prevista:
2Q20

Nombre de la tarea: Comercializar tecnologías de actualización seguras

Número de acción: 1,5
Resumen de la tarea: Promover normas y marcos comerciales para las actualizaciones seguras. Animar a los kits de desarrollo de IoT a incorporar mecanismos de actualización segura para minimizar el tiempo de comercialización de los desarrolladores. Publicar las especificaciones del Grupo de Trabajo de Ingeniería de Internet (IETF) para la actualización segura de los dispositivos del IoT con el fin de fomentar la compatibilidad con los parches de seguridad.
Colaborador(es): Participantes del IETF, NIST, NTIA, otros
Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 2T19

Nombre de la tarea: Alinear la usabilidad y la manejabilidad con las capacidades del cliente
Número de acción: 3.2
Resumen de la tarea: Dar prioridad a los procesos de despliegue y configuración simples y sencillos para los dispositivos comercializados para el hogar y las pequeñas empresas.
Colaborador(es): Asociación de Tecnología del Consumidor (CTA), industria de las TI y del
IoT Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: En curso

Establecer normas de IoT relevantes a nivel mundial

El informe sobre la red de bots señalaba que "el gobierno y la industria de Estados Unidos deberían colaborar con los desarrolladores de normas y especificaciones internacionales voluntarias dirigidas por la industria para establecer normas relevantes a nivel mundial". Esta serie de tareas anima al gobierno y a la industria de EE.UU. a buscar conjuntamente normas internacionales coherentes con las líneas de base de capacidades desarrolladas en la línea de trabajo anterior.

Nombre de la tarea: Establecer normas de IoT relevantes a nivel mundial
Número de acción: 1.2
Resumen de la tarea: El gobierno y la industria de EE.UU. deberían, a través de procesos de debate inclusivos, identificar conjuntamente un conjunto clave de lugares para el desarrollo de normas internacionales voluntarias de seguridad del IoT e iniciar la actividad normativa. Los participantes pueden introducir la línea de base de la capacidad de seguridad básica como una contribución una vez que la línea de base se haya completado.
Colaborador(es): NIST, NTIA, DHS, IICSWG, industria
del IoT Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: 4Q19

Nombre de la tarea: Identificar los incentivos para la adopción de normas de seguridad en el IoT
Número de acción: 2.3
Resumen de la tarea: Identificar los incentivos existentes y necesarios para la adopción por parte del sector privado de las normas y líneas de base de seguridad de la IO, que pueden ser adoptadas por el GEEUU.
Contribuyente(s): Industria de la IO, DHS, Comercio, FTC, agencias específicas del sector, consejos de coordinación del sector
Tareas previas: Establecer normas de IoT relevantes a nivel mundial Inicio

Línea de esfuerzo de la empresa

La línea de esfuerzo de la empresa se centra en las acciones que se pueden llevar a cabo a nivel de gestión empresarial para reducir el riesgo general para la empresa y el ecosistema de las redes de bots y los ataques automatizados y distribuidos.

La Línea de Esfuerzo Empresarial tiene cuatro líneas de trabajo complementarias:

- Perfiles del LCR para la mitigación y la protección
- Migración a arquitecturas de red empresariales avanzadas
- Adopción federal de las mejores prácticas empresariales
- Tecnología operativa

Línea de trabajo de la empresa 1: Perfiles de los MCA para la mitigación y la protección

El Marco de Ciberseguridad del NIST se ha convertido en una herramienta esencial para las empresas y organismos que emplean un enfoque basado en el riesgo para lograr resultados de seguridad adecuados. Esta serie de tareas establece perfiles CSF consensuados por la industria para mitigar las amenazas de denegación de servicio distribuidas (DDoS) y combatir las redes de bots. Una vez completados los perfiles liderados por la industria, el gobierno federal adapta estos perfiles para el entorno federal.

Nombre de la tarea: Desarrollar un perfil de LCR para la mitigación de DDoS
Número de acción: 2.2
Resumen de la tarea: Trabajar con la industria para desarrollar un perfil consensuado de CSF para la mitigación de DDoS. Colaborador(es): Cybersecurity Coalition (líder),[7] industria del ecosistema digital, NIST, NTIA, DHS, sociedad civil
Tareas previas: N/A Inicio previsto: En
curso Finalización prevista: 1Q19

Nombre de la tarea: Publicar el perfil federal del LCR para la mitigación de DDoS
Número de acción: 2.3
Resumen de la tarea: Publicar el perfil federal de CSF para la mitigación de DDoS como una publicación especial del NIST. Colaborador(es): NIST (líder), DHS, agencias federales, partes interesadas del ecosistema digital, sociedad civil Requisito previo Tareas: Desarrollar el perfil del CSF para la mitigación de DDoS
Inicio previsto: 2Q19 Finalización
prevista: 3Q19

Nombre de la tarea: Desarrollar un perfil de LCR para la mitigación de amenazas de botnets
Número de acción: 2.2
Resumen de la tarea: Desarrollar perfiles CSF consensuados por la industria para la mitigación de amenazas de botnets. Colaborador(es): Cybersecurity Coalition (líder), partes interesadas del ecosistema digital, NIST, NTIA, DHS, sociedad civil
Tareas previas: N/A Inicio
previsto: En curso Finalización
prevista: 2Q19

[7] *Véase* Cybersecurity Coalition, *disponible en* https://www.cybersecuritycoalition.org/

Nombre de la tarea: Publicar el perfil federal del LCR para la mitigación de amenazas de botnets
Número de acción: 2.3
Resumen de la tarea: Publicar el perfil federal de la CSF para la mitigación de amenazas de botnets como una publicación especial del NIST.
Colaborador(es): NIST (líder), DHS, agencias federales, partes interesadas del ecosistema digital, sociedad civil Tareas previas: Desarrollar un perfil de CSF para la mitigación de amenazas de botnets
Inicio previsto: 2Q19 Finalización
prevista: 3Q19

Nombre de la tarea: Concienciar a la empresa sobre la mitigación de DDoS
Número de acción: 3.3
Resumen de la tarea: Establecer campañas de asociación y actividades de compromiso estratégico para mejorar el conocimiento de los usuarios y las empresas sobre las amenazas distribuidas automatizadas y las mejores prácticas de seguridad.
Colaborador(es): Cybersecurity Coalition, NTIA, DHS, NIST, sociedad civil
Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: TBD

Línea de trabajo de la empresa 2: Avanzar en las arquitecturas de red de la empresa

Las empresas deben migrar a arquitecturas de red que faciliten la detección, interrupción y mitigación de las amenazas automatizadas y distribuidas. También deben considerar cómo sus propias redes ponen en riesgo a los demás. En esta línea de trabajo, una serie de actividades concurrentes identifican las mejores prácticas actuales y exploran las tecnologías emergentes para las arquitecturas de redes empresariales.

Nombre de la tarea: Mejorar y evolucionar las mejores prácticas en la gestión del tráfico de la red empresarial
Número de acción: 3.1
Resumen de la tarea: Mejorar y hacer evolucionar las políticas constructivas y las mejores prácticas sobre la gestión del tráfico de la red empresarial en los sectores del ecosistema objetivo, teniendo en cuenta los requisitos de las pequeñas empresas. Evolucionar las mejores prácticas a medida que avanzan las tecnologías y las arquitecturas, y abordar las lagunas en las mejores prácticas para los nuevos actores y participantes.
Contribuyente(s): CSDE /CTA (líder), grupos de coordinación de la industria, operadores de redes empresariales, grupos de operadores de redes (NOG), ingenieros de redes, NIST, NTIA, DHS, DOD, proveedores de servicios de Internet, proveedores de infraestructuras, empresas del ecosistema digital global, sociedad civil Tareas previas: N/A.
Inicio previsto: En curso. Finalización
prevista: 2Q2019

Nombre de la tarea: Promover arquitecturas de redes empresariales que mitiguen los riesgos de las amenazas automatizadas y distribuidas
Número de acción: 3.3
Resumen de la tarea: Promover la implementación y adopción de arquitecturas de red empresariales avanzadas que mitiguen el riesgo de amenazas automatizadas y distribuidas. Identificar dónde proliferan las lagunas en la adopción por parte de las empresas, y emprender

esfuerzos para comprender las barreras políticas y de mercado para la integración y el despliegue.
Contribuyente(s): CSDE, organismos de coordinación de la industria, ingenieros y operadores de redes empresariales, NOGs, NTIA, NIST, DHS, Comité de Sistemas de Seguridad Nacional (CNSS), academia, sociedad civil

Tareas previas: Mejorar y evolucionar las mejores prácticas en la gestión del tráfico de la red
Inicio previsto: 2Q2019
Finalización prevista: TBD

Nombre de la tarea: Acelerar la disponibilidad nacional de los servicios de Internet IPv6
Número de acción: 3.4
Resumen de la tarea: El gobierno trabaja con las partes interesadas para apoyar la transición completa a IPv6 por parte de los proveedores de servicios de Internet (ISP) identificando las lecciones aprendidas de la industria y de otros países, identificando tanto los impedimentos para la transición como los posibles incentivos.
Colaborador(es): NTIA (Líder), Registros Regionales de Internet (RIRs), ISPs, Industria de TI y IoT
Tareas Previas: N/A
Inicio previsto: 4T19
Finalización prevista: 2T20

Nombre de la tarea: Acelerar la transición a las redes empresariales IPv6
Número de acción: 3.4
Resumen de la tarea: Demostrar el impacto y la viabilidad del despliegue de TI empresarial sólo con IPv6. Colaborador(es): NIST (líder), industria
Tareas previas: N/A Inicio
previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Establecer los requisitos para las redes de confianza cero (ZTN)
Número de acción: 3.3
Resumen de la tarea: El Grupo de Trabajo de Redes de Confianza Cero del Consejo Federal CIO desarrollará los requisitos iniciales para el despliegue de redes de confianza cero (ZTN) por parte de las agencias. A partir de estos requisitos, los departamentos y las agencias estarán en condiciones de incorporar estas características a medida que surjan las tecnologías de respuesta.
Contribuyente(s): Grupo de Trabajo de la Red de Confianza Cero del Consejo Federal de Directores de Informática (líder)[8]
Tareas previas: N/A Inicio previsto: En
curso Finalización prevista: 4Q18

Nombre de la tarea: Evaluar la viabilidad actual de la ZTN
Número de acción: 3.3
Resumen de la tarea: El Centro Nacional de Excelencia en Ciberseguridad (NCCoE) y los colaboradores de la industria llevarán a cabo un estudio de viabilidad para los requisitos de la ZTN identificados por el Grupo de Trabajo de la ZTN del Consejo CIO utilizando tecnologías comerciales y emergentes.
Colaborador(es): NIST (líder), DHS, CIO Council Zero Trust Networking Working Group Tareas previas: Establecer los requisitos para las redes de confianza cero
Inicio previsto: En curso Finalización
prevista: 4Q19

Nombre de la tarea: Identificar las mejores prácticas para la gestión de la red IoT
Número de acción: 1,5

Resumen de la tarea: Utilizando los resultados del proyecto NCCoE Mitigating IoT-Based DDoS y el estudio de viabilidad de la ZTN, el NIST identificará las mejores prácticas actuales para la gestión de la red empresarial cuando los entornos incluyan dispositivos IoT.

Colaborador(es): NIST (líder), DHS, industria del ecosistema digital y partes interesadas de la sociedad civil Tareas previas: Evaluar la viabilidad actual de la ZTN; mitigar los DDoS basados en el IoT Inicio previsto: 3Q19
Finalización prevista: 2Q20

Línea de trabajo empresarial 3: Adopción federal de las mejores prácticas empresariales

Las partes interesadas indicaron que la adopción por parte del gobierno federal de prácticas de "buena vecindad" proporcionaría una base en todo el ecosistema 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. En esta serie de tareas, el gobierno federal realiza actividades para garantizar que estas mejores prácticas se reflejen adecuadamente en las políticas, normas, directrices y supervisión de las agencias federales.

Nombre de la tarea: Adopción federal de los perfiles federales del LCR para las amenazas automatizadas y distribuidas

Número de acción: 2.3
Resumen de la tarea: La OMB emite orientaciones a las agencias, incluyendo plazos para la adopción y la presentación de informes, en relación con la adopción de perfiles federales de LCR para las amenazas distribuidas automatizadas. El NIST crea o identifica herramientas de medición para cuantificar el progreso.
Contribuyente(s): OMB e-Gov (líder), NIST, DHS, otras agencias del Gobierno de Estados Unidos
Tareas previas: Perfil Federal CSF para la mitigación de DDoS; Perfil Federal CSF para la prevención y mitigación de botnets
Inicio previsto: En curso Finalización
prevista: 2T20

Nombre de la tarea: Implementar el filtrado de entrada/salida en todas las redes de las agencias federales de EE.UU.

Número de acción: 2.3
Resumen de la tarea: Las agencias federales garantizan que las redes de las agencias y los servicios de información de red suministrados comercialmente toman medidas activas para evitar el tráfico con direcciones de origen de red falsificadas.
Contribuyente(s): DHS (líder), GSA, OMB, otras agencias federales, proveedores de servicios contratados por el gobierno federal
Tareas previas: N/A Inicio
previsto: En curso Finalización
prevista: 3Q19

Nombre de la tarea: Desarrollar directrices federales de seguridad para los reflectores

Número de acción: 2.3
Resumen de la tarea: Complementar las directrices existentes del NIST para el funcionamiento de los servidores y resolvedores DNS con una publicación especial del NIST que establezca directrices generales para el funcionamiento del Protocolo de Tiempo de Red (NTP) y otros recursos basados en el Protocolo de Datagramas de Usuario (UDP) ampliamente desplegados.
Colaborador(es): NIST (líder), DHS
Tareas previas: N/A Inicio
previsto: En curso

Finalización prevista: 2Q19

Nombre de la tarea: Aplicar las directrices federales de seguridad para los reflectores
Número de acción: 2.3
Resumen de la tarea: Obligar a todos los organismos federales a aplicar las directrices del NIST sobre recursos reflexivos.
Contribuyente(s): DHS (codirector), OMB (codirector), NIST
Tareas previas: Desarrollar directrices federales de seguridad para los reflectores Inicio previsto: 2Q19
Finalización prevista: 2Q20

Nombre de la tarea: Rastrear y remediar los recursos vulnerables en las agencias federales
Número de acción: 2.3
Resumen de la tarea: Elaborar una lista de los organismos federales con recursos de reflexión que no cumplen las directrices del NIST y hacer un seguimiento de los progresos realizados.
Contribuyente(s): DHS (líder), OMB, departamentos y agencias de Estados Unidos
Tareas previas: Adopción de los perfiles federales del LCR para las amenazas automatizadas y distribuidas Inicio previsto: 2Q20
Finalización prevista: En curso

Línea de trabajo empresarial 4: Tecnología operativa

A continuación se especifican una serie de tareas que pretenden cerrar las brechas de entendimiento entre las comunidades de ciberseguridad y de tecnología operativa (OT). Los expertos en ciberseguridad suelen tener un conocimiento limitado de las limitaciones y restricciones impuestas por las preocupaciones específicas de la OT (por ejemplo, la seguridad), mientras que la comunidad de la tecnología operativa tiene un conocimiento limitado de los riesgos y las capacidades de ciberseguridad.

Nombre de la tarea: Las comunidades de ciberseguridad y OT colaboran para mejorar la comprensión de los retos de ciberseguridad de OT
Número de acción: 4,5
Resumen de la tarea: La comunidad de ciberseguridad trabaja con la comunidad de OT para mejorar la comprensión de los desafíos de ciberseguridad.
Colaborador(es): DHS (líder), agencias sectoriales, laboratorios nacionales, consejos de coordinación sectorial Tareas previas: N/A
Inicio previsto: 2T19 Finalización
prevista: 3Q21

Nombre de la tarea: Ampliar el intercambio de información sobre OT y ciberseguridad
Número de acción: 4,5
Resumen de la tarea: Ampliar los compromisos federales actuales que promueven el intercambio de información entre las comunidades de OT y ciberseguridad.
Colaborador(es): DHS (líder), agencias sectoriales, laboratorios nacionales, consejos de coordinación sectorial Tareas previas: N/A
Inicio previsto: 2T19 Finalización
prevista: 3Q21

Nombre de la tarea: Promover la adopción por parte de las OT de la tecnología de seguridad informática
Número de acción: 4,5

Resumen de la tarea: Ampliar los compromisos federales actuales que promueven la adopción de tecnología de seguridad informática por parte de las OT.
Colaborador(es): NIST (líder), DHS, agencias específicas del sector, consejos de coordinación del sector
Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 3Q21

Línea de esfuerzo en infraestructuras

La Línea de Esfuerzo de Infraestructura se centra en acciones que requerirán la coordinación entre la gran diversidad de actores del ecosistema digital, o que afectan a las capacidades funcionales básicas de la infraestructura digital global.

La Línea de Esfuerzo de Infraestructura tiene cuatro líneas de trabajo complementarias:

- Mejoras en la seguridad de las rutas
- Compartir información en la práctica
- Protocolos de intercambio de información
- Investigación y desarrollo

Línea de trabajo de infraestructura 1: Mejoras en la seguridad de las rutas

Internet se diseñó para facilitar las comunicaciones resistentes entre puntos finales, y prestó menos atención a los servicios básicos de seguridad. Como resultado, el estado de la seguridad del enrutamiento en Internet está muy por debajo de lo que puede lograrse tanto con las herramientas y prácticas comunes como con las más recientes. Esta serie de tareas avanza en el despliegue de tecnologías anti-spoofing de larga data y de tecnologías más nuevas para proteger contra el secuestro y la filtración de rutas.

Nombre de la tarea: Eliminar las barreras legales y políticas para la adopción de la Infraestructura de Clave Pública de Recursos (RPKI)
Número de acción: 2.3
Resumen de la tarea: Establecer una estrategia legal consensuada para abordar las barreras a la adopción de RPKI, incluyendo la emisión de certificados RPKI para los titulares de direcciones heredadas, los problemas de responsabilidad y las barreras a los modelos de despliegue alternativos.
Colaboradores: Academia, ingenieros de Internet, NIST, NTIA, DOD, registros regionales y locales de Internet
Tareas previas: N/A Inicio
previsto: 2Q19 Finalización
prevista: 1Q20

Nombre de la tarea: Las agencias federales adoptan la RPKI
Número de acción: 2.3
Resumen de la tarea: Los titulares de direcciones federales y los proveedores de servicios crean autorizaciones de origen de ruta (ROA) para los recursos de direcciones y aplican las ROA a las decisiones de enrutamiento de Internet para mitigar los secuestros de rutas.
Contribuyente(s): DHS (líder), OMB, DOD, agencias federales
Tareas previas: Eliminar las barreras legales y políticas para la adopción de RPKI

Inicio previsto: 1Q20
Finalización prevista: 1Q21

Nombre de la tarea: Aumentar la escalabilidad y robustez de los mecanismos antispoofing
Número de acción: 2.3
Resumen de la tarea: El gobierno y la industria continúan investigando para hacer que el anti-spoofing sea más escalable y robusto, y esté disponible en todos los niveles de Internet.
Colaborador(es): DHS (Líder), incubadoras de tecnología federales, NIST, ingenieros de Internet, academia
Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 4Q19

Nombre de la tarea: Ampliar la adopción, el conocimiento y la aplicación de los mecanismos anti-spoofing
Número de acción: 2.3
Resumen de la tarea: Promover la adopción y ampliar la implementación de mecanismos anti-spoofing, según corresponda, en toda la infraestructura de Internet.
Colaborador(es): Propietarios y operadores de infraestructuras de Internet, sociedad civil, NIST, NTIA, DHS Tareas previas: Aumentar la escalabilidad y robustez de los mecanismos anti-spoofing Inicio previsto: 4Q19
Finalización prevista: 4Q20

Nombre de la tarea: Establecer un observatorio de normas mutuamente acordadas para la seguridad de las rutas (MANRS) y un panel de control para las métricas de seguridad de las rutas
Número de acción: 2.5
Resumen de la tarea: Desarrollar métricas y un sitio web para evaluar la seguridad y la resistencia del sistema de enrutamiento de Internet a lo largo del tiempo.
Colaborador(es): Internet Society, RIRs Tareas
previas: N/A
Inicio previsto: En curso
Finalización prevista: 4Q18

Nombre de la tarea: Desarrollar requisitos de seguridad para los servicios de Internet
Número de acción: 3.3
Resumen de la tarea: Publicar el SP 800-189, "Secure Inter-Domain Traffic Exchange: Robustez de BGP y mitigación de DDoS".
Colaborador(es): NIST (líder)
Tareas previas: N/A Inicio
previsto: En curso Finalización
prevista: 2Q19

Nombre de la tarea: Explorar la evolución de las amenazas y las soluciones emergentes en torno a la seguridad de las rutas
Número de acción: 3.3
Resumen de la tarea: Involucrar a las partes interesadas y a los actores de la infraestructura de Internet para comprender los beneficios y los límites de las soluciones de seguridad de enrutamiento existentes y emergentes, captando las preocupaciones de las partes

interesadas y las posibles mitigaciones.
Colaborador(es): NTIA, propietarios y operadores de infraestructuras de Internet, sociedad civil, NIST, DHS Tareas previas: N/A
Inicio previsto: 3Q19
Finalización prevista: 3Q20

Línea de trabajo de infraestructura 2: Compartir información en la práctica

Los grandes proveedores de redes comparten actualmente las técnicas de gestión de redes y las tácticas defensivas que son eficaces contra determinadas amenazas. Las fuerzas del orden dependen de la información del sector privado para iniciar las investigaciones. Esta serie de tareas se centra en ampliar el intercambio de información a los PSI más pequeños y a los proveedores de redes extranjeros, y en garantizar que las fuerzas del orden sean alertadas en la fase más temprana posible, respetando al mismo tiempo las directrices y la normativa en materia de privacidad.

Nombre de la tarea: Aumentar el acceso de los ISP más pequeños a la información sobre amenazas compartida por el sector

Número de acción: 2.1
Resumen de la tarea: Ampliar el intercambio de información nacional para mejorar la participación de los PSI más pequeños. Colaborador(es): Proveedores de infraestructuras, DHS a través del ISAC de comunicaciones
Tareas previas: N/A Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Ampliar el intercambio de información sobre amenazas a nivel mundial y regional

Número de acción: 2.1
Resumen de la tarea: Mejorar los mecanismos de intercambio de información para facilitar un mayor intercambio global y regional.
Contribuyente(s): Equipos globales de respuesta a incidentes de seguridad informática (CSIRT), DHS, NOGs, ISACs, proveedores de infraestructura
Tareas previas: N/A Inicio
previsto: 1Q19 Finalización
prevista: TBD

Nombre de la tarea: Ampliar los acuerdos de intercambio de información

Número de acción: 2.1
Resumen de la tarea: El gobierno de EE.UU. aprovecha los ISAC, las asociaciones NOG, el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST), y trabaja con sus homólogos internacionales para ampliar los acuerdos de intercambio de información.
Contribuyente(s): DHS, NOGs, Consejo ISAC, ISACs, FIRST, asociaciones de fuerzas de seguridad, centros cibernéticos/centros de fusión
Tareas previas: N/A Inicio
previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Compartir información oportuna y procesable con las fuerzas de seguridad

Número de acción: 4.1
Resumen de la tarea: Proporcionar información aún más oportuna y procesable para facilitar, apoyar y acelerar las acciones de las fuerzas del orden, incluidas las que afectan a las redes de bots distribuidas por todo el mundo.
Contribuyente(s): Departamento de Justicia (DOJ)/Oficina Federal de Investigaciones (FBI), FTC, ISACs, DHS, NOGs, CSIRTs globales, grandes empresas y proveedores de infraestructura
Tareas previas: N/A Inicio
previsto: TBD Finalización

Nombre de la tarea: Mejorar el intercambio de información del Gobierno de EE.UU. con la industria

Número de acción: 4.1
Resumen de la tarea: Mejorar la puntualidad y la pertinencia de la información compartida por el gobierno de EE.UU. con la industria.
Contribuyente(s): Centros Cibernéticos del Gobierno de los Estados Unidos, DHS, Agencias Sectoriales, ISAC/organizaciones de intercambio y análisis de información (ISAOs)
Tareas previas: N/A Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Mejorar la precisión de los recursos de datos críticos para la seguridad
Número de acción: 4.1
Resumen de la tarea: Las bases de datos WHOIS, que comprenden la información de registro de los recursos de denominación y numeración de Internet (por ejemplo, direcciones IP y nombres de dominio), se mejoran para que sean más precisas y faciliten la atribución de los malos actores. Se desarrollan mecanismos que preservan la información de WHOIS en el momento oportuno, a la vez que satisfacen las regulaciones de protección de la privacidad (por ejemplo, el Reglamento General de Protección de Datos de la UE [GPDR]) y apoyan el trabajo de investigación de botnets.
Colaboradores: Registros/registradores de nombres de dominio, NTIA, la Corporación para la Asignación de Nombres y Números en Internet (ICANN), RIRs, Fuerzas de Seguridad, academia y sociedad civil
Tareas previas: N/A Inicio
previsto: En curso Finalización
prevista: En curso

Línea de trabajo de infraestructura 3: Protocolos de intercambio de información

Este conjunto de tareas se centra en la estandarización de los protocolos de intercambio de información para aumentar la velocidad y permitir una respuesta automatizada. La mejora de la utilidad de los protocolos de intercambio de información complementa las tareas del proceso de intercambio de información al aumentar el valor de la información que se comparte.

Nombre de la tarea: Apoyar la automatización del intercambio de información
Número de acción: 2.1
Resumen de la tarea: Mejorar los protocolos de intercambio de información para aumentar la velocidad y apoyar la respuesta automatizada.
Contribuyente(s): DHS, ISAOs, industria, sociedad civil, consorcios Tareas
previas: N/A
Inicio previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Apoyar la respuesta colaborativa a los incidents Acción: 4.4
Resumen de la tarea: El IETF finaliza el protocolo de señalización de amenazas abiertas DDoS (DOTS). Las empresas con estrategias de mitigación de DDoS multipartitas implementan y despliegan DOTS para facilitar la acción coordinada.
Colaborador(es): IETF, empresas del ecosistema digital, Sociedad
civil Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: TBD

Nombre de la tarea: Mejorar los protocolos de intercambio de información para facilitar el intercambio de información global

Número de acción: 2.4
Resumen de la tarea: El gobierno y la industria de Estados Unidos revisarán y mejorarán los protocolos de intercambio de información, como el Structured Threat Information Expression (STIX) y el Trusted Automated Exchange of Indicator Information (TAXII), para facilitar el intercambio global de información con respecto a las amenazas automatizadas.
Contribuyente(s): DHS (líder), ISAOs, centros de investigación y desarrollo financiados por el gobierno federal (FFRDCs), industria
Tareas previas: N/A Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Establecer normas internacionales para facilitar el intercambio de información

Número de acción: 2.4
Resumen de la tarea: La industria, con el apoyo del gobierno de Estados Unidos, establecerá normas internacionales para el intercambio de información con el fin de facilitar la coordinación mundial.
Colaborador(es): Industria (líder), DHS, ISAC/ISAOs, sociedad civil Tareas
previas: N/A
Inicio previsto: TBD
Finalización prevista: TBD

Infraestructura Línea de trabajo 4: Investigación y Desarrollo

Nombre de la tarea: Incorporar las mejores prácticas de infraestructura en el marco de ciberseguridad del NIST

Número de acción: 3.3
Resumen de la tarea: Evaluar continuamente los avances en las mejores prácticas y tecnologías de seguridad para su inclusión en el Marco de Ciberseguridad del NIST.
Colaborador(es): NIST (líder), proveedores de infraestructura
Tareas previas: N/A
Inicio previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Desbaratar el ecosistema de los atacantes mediante la transparencia y la trazabilidad

Número de acción: 4.4
Resumen de la tarea: El ecosistema de las amenazas automatizadas y distribuidas favorece al atacante. Esta tarea desarrolla métodos para interrumpir los ecosistemas que tradicionalmente se explotan para lanzar botnets, como la comunidad de jugadores, y aumentar el riesgo para los atacantes mediante la transparencia y la responsabilidad. La industria y el gobierno abogan conjuntamente en los foros pertinentes de las múltiples partes interesadas por una aplicación más amplia de las medidas que alteran las herramientas y los incentivos de los atacantes.
Colaborador(es): ICANN, RIRs, NTIA, Aplicación de la ley, FTC Tareas
previas: N/A
Inicio previsto: TBD
Finalización prevista: TBD

Línea de esfuerzo de desarrollo y transición tecnológica

La Línea de Esfuerzo de Desarrollo y Transición Tecnológica tiene tres líneas de trabajo complementarias:

- Establecer un mercado de software seguro
- Coordinación internacional
- Investigación y desarrollo

Línea de trabajo de desarrollo y transición tecnológica 1: Establecimiento de un mercado de software seguro

Esta serie de tareas establece un mercado sólido y sostenible para los sistemas y aplicaciones desarrollados mediante prácticas de desarrollo de software seguro. Las tareas establecen directrices ampliamente aceptadas para el desarrollo de software seguro, aumentan la eficiencia y la eficacia de las herramientas para el desarrollo de software seguro con el fin de aumentar el rendimiento de la inversión, y muestran estos avances en los foros tecnológicos patrocinados por el gobierno.

Nombre de la tarea: Establecer directrices para el ciclo de vida del desarrollo de software seguro
Número de acción: 1.3
Resumen de la tarea: En colaboración con la industria, el NIST define las directrices del ciclo de vida del desarrollo de software seguro para su publicación como Publicación Especial del NIST.
Colaborador(es): NIST (líder), DHS, industria Tareas
previas: N/A
Inicio previsto: En curso
Finalización prevista: 2T20

Nombre de la tarea: Desarrollar directrices para la transparencia de los componentes de software
Número de acción: 1.3
Resumen de la tarea: Explorar cómo los fabricantes y vendedores pueden comunicar información útil y procesable sobre los componentes de software de terceros en los dispositivos modernos de software e IoT, y cómo estos datos pueden ser utilizados por las empresas para fomentar mejores decisiones y prácticas de seguridad.
Colaborador(es): NTIA (líder), sectores de infraestructuras críticas, partes interesadas del ecosistema digital Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 2T19

Nombre de la tarea: Llenar las lagunas de las herramientas de desarrollo de software
Número de acción: 1.3
Resumen de la tarea: El Programa de Investigación y Desarrollo de Redes y Tecnologías de la Información (NITRD) promoverá la financiación de la investigación dirigida y las actividades de transición tecnológica en colaboración para las herramientas de desarrollo de software necesarias para adoptar de forma eficiente y eficaz el ciclo de vida de desarrollo de software seguro (SSDLC).
Colaborador(es): NITRD (líder) Tareas
previas: N/A Inicio previsto: En curso
Finalización prevista: 1Q23

Nombre de la tarea: Mejorar las cadenas de herramientas de desarrollo de software

Número de acción: 1.3
Resumen de la tarea: Acelerar el desarrollo y la adopción de técnicas de desarrollo de software eficaces y eficientes mediante la gestión de un concurso abierto para cadenas de herramientas de desarrollo de software.
Colaborador(es): NIST (líder), DHS Tareas
previas: N/A Inicio previsto: En curso
Finalización prevista: 1Q22

Nombre de la tarea: Mostrar los avances en las prácticas de codificación segura y compartir información sobre los riesgos de seguridad
Número de acción: 5.3
Resumen de la tarea: Mostrar los avances en las prácticas y herramientas de codificación segura desarrolladas por el mundo académico y los investigadores de seguridad y compartir información sobre los riesgos de seguridad en la conferencia anual PrivacyCon.
Colaborador(es): FTC (Líder) Tareas
previas: N/A Inicio previsto: 3Q19
Finalización prevista: En curso

Nombre de la tarea: Las agencias exigen un desarrollo seguro para el software gubernamental disponible (GOTS)
Número de acción: 2.3
Resumen de la tarea: Se establecen reglamentos federales de adquisición para los contratos de desarrollo de software GOTS que fomentan o exigen la aplicación del SSDLC. Colaborador(es):
GSA, OMB, DOD, otros departamentos y agencias estadounidenses
Tareas previas: Definir la línea de base de la capacidad de seguridad básica
Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Las agencias adquieren software comercial disponible desarrollado de forma segura (COTS)
Número de acción: 2.3
Resumen de la tarea: Se han establecido normas federales para la adquisición de software COTS que prefieren o requieren el desarrollo mediante el SSDLC.
Contribuyente(s): GSA (líder), OMB, DHS (Programa de Diagnóstico y Mitigación Continua), DOD, otros departamentos y agencias de los Estados Unidos
Tareas previas: Definir la línea de base de la capacidad de seguridad básica Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Desarrollar las mejores prácticas para el software al final de su vida útil
Número de acción: 1,5
Resumen de la tarea: Desarrollar una serie de procesos de fin de vida para software y dispositivos muertos y huérfanos que equilibren los requisitos del cliente y de la empresa.
Colaborador(es): CTA, NTIA, otros participantes del gobierno y de la industria
Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: 4Q19

Desarrollo tecnológico y transición Línea de trabajo 2: Coordinación internacional

Nombre de la tarea: Mejorar la coordinación existente entre el gobierno de EE.UU. y las normas internacionales
Número de acción: 4.2
Resumen de la tarea: Basarse en el trabajo del Grupo de Trabajo Interinstitucional sobre Normalización de la Ciberseguridad (IICSWG) para seguir mejorando la coordinación del GEEUU en su compromiso con los organismos internacionales de normalización. Identificar estrategias para la promoción del desarrollo de normas impulsadas por la industria dentro de esos organismos.
Colaborador(es): NIST (líder), organismos miembros del IICSWG Tareas
previas: N/A
Inicio previsto: En curso Finalización
prevista: En curso

Nombre de la tarea: Optimizar la coordinación de las normas entre la industria y el USG
Número de acción: 4.2
Resumen de la tarea: Establecer un marco y una estrategia para continuar la coordinación entre las entidades industriales estadounidenses y las agencias federales que participan en el desarrollo de normas internacionales. Colaborador(es): NIST, NTIA, Estado, IICSWG, industria, CSDE, asociaciones comerciales
Tareas previas: N/A Inicio previsto: En curso
Finalización prevista: En curso

Nombre de la tarea: Promover la adopción internacional de las mejores prácticas mediante el compromiso internacional bilateral y multilateral
Número de acción: 4.2
Resumen de la tarea: Promover la adopción de las mejores prácticas reconocidas internacionalmente a través de la participación bilateral, multilateral y de múltiples partes interesadas, aprovechando la experiencia de los organismos del Gobierno de Estados Unidos.
Colaborador(es): Estado, NTIA, NIST, industria, sociedad civil
Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: TBD

Nombre de la tarea: Promover el conocimiento y la adopción de herramientas, protocolos y mejores prácticas específicas establecidas a escala mundial
Número de acción: 3.3
Resumen de la tarea: Promover la implementación y adopción de herramientas, protocolos y mejores prácticas establecidas que aborden los riesgos cibernéticos automatizados a escala. Desarrollar guías de implementación fáciles de entender y trabajar con las partes interesadas de todo el mundo. Desarrollar la capacidad de medir el impacto de esta implementación.
Colaborador(es): Global Cyber Alliance, organismos de coordinación de la industria, NTIA, NIST, DHS Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: En curso

Colaborador(es): NTIA (líder), participantes gubernamentales y del sector privado de múltiples partes interesadas Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: En curso

Desarrollo y transición de la tecnología Línea de trabajo 3: Investigación y desarrollo

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- se necesitan urgentemente para adelantarse a los actores maliciosos. Se necesitan actividades de investigación dirigidas por la industria para desarrollar y desplegar tecnologías innovadoras. 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.

Nombre de la tarea: Acelerar la I+D financiada por el gobierno federal para mitigar las amenazas distribuidas

Número de acción: 1.4
Resumen de la tarea: Promover la financiación de la investigación dirigida y las actividades de transición tecnológica en colaboración para las tecnologías que mitigan las amenazas distribuidas automatizadas.
Colaborador(es): NITRD (líder), DHS, departamentos y agencias de Estados
Unidos Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: En curso

Nombre de la tarea: Acelerar el desarrollo y el despliegue de tecnologías innovadoras para la prevención y mitigación de las amenazas distribuidas
Número de acción: 1.4
Resumen de la tarea: La industria, el mundo académico y el gobierno deben acelerar el desarrollo y el despliegue de tecnologías innovadoras para la prevención y la mitigación de las amenazas distribuidas. Colaborador(es): Actores del ecosistema en un entorno competitivo
Tareas previas: N/A Inicio previsto:
En curso Finalización prevista: En
curso

Nombre de la tarea: Aumentar la responsabilidad en la gestión del tráfico
Número de acción: 2.5
Resumen de la tarea: Examinar en qué medida los acuerdos de sistemas interautónomos, de interconexión de redes y de tránsito pueden mejorar la responsabilidad de la gestión del tráfico.
Colaborador(es): NOGs, incubadoras tecnológicas federales, DHS, sociedad civil, academia
Tareas previas: N/A
Inicio previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Acelerar la I+D de la industria para mitigar las amenazas distribuidas
Número de acción: 1.4
Resumen de la tarea: Acelerar el desarrollo y despliegue de tecnologías innovadoras para la prevención y mitigación de las amenazas distribuidas.
Contribuyente(s): Consorcios y laboratorios de la industria, sector académico

Tareas previas: N/A Inicio previsto: TBD
Finalización prevista: TBD

Nombre de la tarea: Priorizar la transición tecnológica
Número de acción: 2.5
Resumen de la tarea: Hacer hincapié en las estrategias de transición tecnológica como componente clave de los planes de investigación de nuevas herramientas y prácticas para la gestión del tráfico de red.
Colaborador(es): Coalición TBD de la industria, el gobierno y la sociedad civil Tareas
previas: N/A
Inicio previsto: TBD Finalización
prevista: TBD

Nombre de la tarea: Promover las mejores prácticas emergentes
Número de acción: 1.4
Resumen de la tarea: Ampliar los esfuerzos de investigación y transición tecnológica a medida que las tecnologías maduran y surgen las mejores prácticas.
Colaborador(es): Sociedad civil TBD Tareas
previas: N/A Inicio previsto: En curso
Finalización prevista: En curso

Línea de esfuerzo de sensibilización y educación

La Línea de Esfuerzo de Concienciación y Educación tiene dos líneas de trabajo complementarias:

- Fomentar la confianza de los consumidores
- Educar a los trabajadores

Línea de trabajo de concienciación y educación 1: Promover la confianza de los consumidores

La falta de confianza de los consumidores en la seguridad de los dispositivos IoT puede estar obstaculizando su adopción. Esta serie de tareas se centra en fomentar la confianza de los consumidores para que puedan identificar productos que satisfagan sus necesidades, se adhieran a las afirmaciones de seguridad de los vendedores y ofrezcan una protección real mediante la aplicación de tecnologías de ciberseguridad disponibles en el mercado.

Nombre de la tarea: Promover el despliegue adecuado de los productos
Número de acción: 4.3
Resumen de la tarea: Educar a los consumidores sobre las diferentes líneas de base y programas de evaluación que mostrarán que los productos desplegados utilizan la seguridad adecuada.
Colaborador(es): Agencias sectoriales, sociedad civil, grupos de consumidores, FTC, DHS, NTIA, CTA Tareas previas: Establecer un programa de evaluación para los dispositivos del IoT doméstico; establecer un programa de evaluación para los dispositivos del IoT industrial; especificar la línea de base de la capacidad de seguridad del IoT
Inicio previsto: 1T20 Finalización
prevista: 3Q23

Nombre de la tarea: Disuadir las prácticas ilegales de comercialización
Número de acción: 4.3

Resumen de la tarea: Detener y disuadir las prácticas ilegales de comercialización por parte de los proveedores de IoT y TI mediante acciones de aplicación.
Colaborador(es): FTC (líder)
Tareas previas: N/A Inicio
previsto: En curso Finalización
prevista: En curso

Nombre de la tarea: Mitigación de DDoS basados en IoT
Número de acción: 1,5
Resumen de la tarea: Demostrar el impacto y la viabilidad de combinar las descripciones de uso del fabricante (MUD), la señalización de amenazas, las actualizaciones seguras y la ciber higiene básica para proteger los dispositivos IoT y mitigar el impacto de los dispositivos IoT comprometidos.
Colaborador(es): NIST (líder), sociedad civil, ingenieros de Internet
Tareas previas: N/A
Inicio previsto: En curso
Finalización prevista: En curso

Sensibilización y educación Línea de trabajo 2: Educación de la mano de obra

A medida que toda la gama de productos y servicios se pone en línea, surgen amenazas de ciberseguridad en nuevas clases de productos. Los diseñadores de productos están profundamente impregnados de los riesgos tradicionales asociados a sus productos, pero a menudo no son conscientes de los nuevos riesgos que pueden introducirse cuando los productos se conectan a la red. Esta serie de tareas se centra en la educación de la mano de obra existente y emergente, independientemente de la disciplina de ingeniería, en materia de ciberseguridad básica.

Nombre de la tarea: Preparar la mano de obra de programación
Número de acción: 1.3
Resumen de la tarea: Incorporar los principios de seguridad por diseño y las herramientas de apoyo en los cursos de programación a lo largo de la carrera.
Contribuyente(s): Academia, comunidad de desarrollo de software seguro, proveedores de formación y certificación, organismos de acreditación, gobierno
Tareas previas: N/A Inicio previsto: En
curso Finalización prevista: 2Q20

Nombre de la tarea: Preparar la mano de obra de ingeniería
Número de acción: 5.4
Resumen de la tarea: Incorporar los principios de ciberseguridad en los cursos de todas las disciplinas de ingeniería.
Contribuyente(s): Academia, gobiernos federal y estatal Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 2T20

Nombre de la tarea: Alinear el plan de estudios con las necesidades de la mano de obra
Número de acción: 5.3

Resumen de la tarea: Seguir promoviendo el Marco de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) como herramienta de referencia para el desarrollo de los contenidos de los cursos, en particular con respecto al desarrollo de software.
Contribuyente(s): NIST (líder), Academia, organismos de acreditación, sociedades profesionales, proveedores de certificación

Tareas previas: N/A Inicio
previsto: En curso
Finalización prevista: 4Q18

Nombre de la tarea: Establecer un programa educativo de ciberseguridad para ingenieros
Número de acción: 5.4
Resumen de la tarea: Establecer la ciberseguridad como un requisito fundamental en todas las disciplinas de la ingeniería, y crear o aprovechar la formación en línea sobre ciberseguridad existente para los ingenieros.
Colaborador(es): NIST, comunidad educativa de ciberseguridad, programas de acreditación
Tareas previas: N/A
Inicio previsto: En curso Finalización
prevista: 1Q21

III. Próximos pasos

Los Departamentos de Comercio y Seguridad Nacional trabajarán con otras agencias gubernamentales de Estados Unidos y con el sector privado para coordinar y seguir las actividades de la hoja de ruta. El Departamento de Seguridad Nacional se coordinará entre los organismos específicos del sector y con las organizaciones de infraestructuras críticas. El Departamento de Comercio coordinará las actividades técnicas y de normalización a través del NIST, y coordinará las actividades de todo el gobierno y de la economía digital a través de la NTIA.

También proporcionaremos actualizaciones periódicamente, incluyendo:

- Reunirse y comunicarse periódicamente con las partes interesadas del sector privado que lideran iniciativas clave para compartir información y avances.
- Convocar a las partes interesadas a medio plazo (aproximadamente seis meses después de la publicación de la hoja de ruta), mediante un taller u otra sesión, para debatir los avances en la aplicación de la hoja de ruta.
- Presentar al Presidente un informe de situación de 365 días sobre la aplicación, que deberá presentarse un año después de la publicación de la hoja de ruta definitiva, tal como se detalla en el Informe sobre redes de bots. Esta actualización revisará el progreso de la comunidad en su conjunto, reevaluará la amenaza en la medida de lo posible, y discutirá las actividades clave en el próximo año.

Como se ha comentado en el Informe sobre redes de bots y en la Sección II de este documento, el problema de los ataques automatizados y distribuidos no puede ser resuelto por una sola entidad, y requerirá la acción, la coordinación y el aprovechamiento de la innovación en toda la administración y el sector privado (incluyendo la industria, el mundo académico y la sociedad civil). Los Departamentos

esperan trabajar con el sector privado y otras entidades gubernamentales durante el próximo año y más allá para mejorar la seguridad del ecosistema de Internet.