NISTIR 8192

Mejora de la resistencia de Internet y Ecosistema de comunicaciones

Actas de un taller del NIST

Tim Polk

Esta publicación está disponible de forma gratuita en https://doi.org/10.6028/NIST.IR.8192

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8192

Mejora de la resistencia de Internet y Ecosistema de comunicaciones

Actas de un taller del NIST

Tim Polk
División de Ciberseguridad Aplicada
Laboratorio de Tecnologías de la Información

Esta publicación está disponible de forma gratuita en https://doi.org/10.6028/NIST.IR.8192

Septiembre de 2017

Departamento de Comercio de los Estados Unidos

Wilbur L. Ross, Jr., Secretario

Instituto Nacional de Normas y Tecnología
Kent Rochford, Director en funciones del NIST y Subsecretario de Comercio para Normas y Tecnología

Informe interno 8192 del Instituto Nacional de Normas y Tecnología
33 páginas (septiembre de 2017)

Esta publicación está disponible de forma gratuita en
https://doi.org/10.6028/NIST.IR.8192

Los comentarios sobre este tema pueden presentarse hasta el 5 de febrero de 2018 a:

Instituto Nacional de Normas y Tecnología
Attn: División de Ciberseguridad Aplicada, Laboratorio de Tecnología de la Información
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Correo electrónico: distributed.threats@nist.gov

Consulte la sección 5 de este documento para obtener más detalles.

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología de la Información (ITL) del Instituto Nacional de Normas y Tecnología (NIST) promueve la economía y el bienestar público de los Estados Unidos proporcionando liderazgo de la infraestructura de medición y normalización del país. El ITL desarrolla pruebas, ensayos métodos, datos de referencia, aplicaciones de prueba de concepto y análisis técnicos para avanzar en la desarrollo y uso productivo de las tecnologías de la información. Las responsabilidades del DIT incluyen desarrollo de normas y directrices de gestión, administrativas, técnicas y físicas para la seguridad y la privacidad rentables de la información no relacionada con la seguridad nacional en el ámbito federal sistemas de información.

Resumen

Estas actas documentan el 11 y 12 de julio de 2017 "Mejora de la resiliencia de Internet y Taller "Ecosistema de Comunicaciones" dirigido por el Instituto Nacional de Normas y Tecnología. Orden Ejecutiva 13800, "Fortalecimiento de la ciberseguridad de las redes federales y Infraestructura Crítica" exigía a los Secretarios de Comercio y Seguridad Nacional que "conjuntamente liderar un proceso abierto y transparente para identificar y promover la acción de las partes interesadas para mejorar la resistencia del ecosistema de Internet y las comunicaciones y fomenter colaboración con el objetivo de reducir drásticamente las amenazas perpetradas por los ataques distribuidos (por ejemplo, botnets)". El taller se diseñó para que las partes interesadas pudieran explorer una serie de soluciones actuales y emergentes que abordan las amenazas automatizadas y distribuidas en una y transparente. El taller atrajo a 150 participantes de diversas partes interesadas comunidades y se llevó a cabo bajo las reglas de Chatham House.

Palabras clave

Botnet; amenaza distribuida; ataque de denegación de servicio distribuido (DDoS); Internet de las cosas; resistencia; raíz de confianza; actualización segura

Agradecimientos

Aunque el Instituto Nacional de Normas y Tecnología (NIST) convocó este taller, su
El éxito de la conferencia se debe a las valiosas contribuciones de los 150 participantes de la industria, el mundo académico, las organizaciones de normalización, las organizaciones no gubernamentales y las agencias gubernamentales. Apreciamos especialmente las contribuciones de nuestros presidentes y panelistas; su pensamiento los debates que provocaron fueron fundamentales para el éxito de las sesiones de trabajo que siguieron.
Por último, este informe del taller no habría sido posible sin el extraordinario apoyo que recibido del Centro Nacional de Excelencia en Ciberseguridad (NCCoE) del NIST y de The MITRE Corporation, el operador del NCCoE. El NCCoE es una colaboración público-privada para acelerar la adopción generalizada de herramientas y tecnologías de ciberseguridad integradas, y es copatrocinado por el Estado de Maryland y el Condado de Montgomery, Md. El NCCoE y MITRE proporcionó expertos en la materia para captar las contribuciones de nuestros participantes y realizó un análisis detallado después del taller, identificando las áreas clave de interés y preocupación. Los expertos en la materia que apoyaron este proceso fueron:

- Brian Abe (NCCoE)
- Drew Allensworth (NCCoE)
- Brittany Biondo (Mitre)
- David Dandar (Mitre)
- Lura Danley (Mitre)
- Zachary Furness (NCCoE)
- Diane Khula (Mitre)
- Susan Prince (NCCoE)
- Julie Steinke (NCCoE)
- Caroline Tan (NCCoE)
- Aaron Temin (NCCoE)
- Teresa Thomas (NCCoE)
- Mary Yang (NCCoE)

Resumen ejecutivo

Orden ejecutiva 13800, "Fortalecimiento de la ciberseguridad de las redes federales y de las Infraestructura" fue emitido el 11 de mayo de 2017. En la sección 2 (d), la orden ejecutiva requiere los Secretarios de Comercio y de Seguridad Nacional "dirigirán conjuntamente una proceso para identificar y promover la acción de las partes interesadas adecuadas para mejorar la resiliencia de el ecosistema de Internet y las comunicaciones y fomentar la colaboración con el objetivo de reduciendo drásticamente las amenazas perpetradas por ataques automatizados y distribuidos (por ejemplo, botnets)". La Orden Ejecutiva ordena a los Departamentos publicar un informe preliminar en enero de 2018 y presentar el informe final al Presidente antes del 11 de mayo de 2018.[1]

Estas actas documentan el 11 y 12 de julio de 2017 "Mejora de la resiliencia de Internet y Taller "Ecosistema de Comunicaciones" dirigido por el Instituto Nacional de Normas y Tecnología. El taller fue uno de los varios flujos de trabajo que llevaron a cabo simultáneamente varios componentes de los departamentos para involucrar a las partes interesadas e identificar las acciones apropiadas. La página web el taller atrajo a 150 participantes de diversas comunidades interesadas y se llevó a cabo bajo las reglas de Chatham House.

En los debates del taller surgieron seis temas generales:

1. La naturaleza global del problema: La mayoría de los dispositivos comprometidos que component las redes de bots están ubicadas geográficamente fuera de Estados Unidos. La acción coordinada con internacionales serán necesarios para aumentar la resistencia del ecosistema contra estas amenazas.
2. La disponibilidad de herramientas eficaces: Las herramientas, procesos y prácticas necesarias para mejorar significativamente la resiliencia del ecosistema están ampliamente disponibles, y rutinariamente aplicados en determinados sectores del mercado, pero generalmente infrautilizados.
3. La importancia de asegurar los productos durante todo el ciclo de vida: Los dispositivos que se vulnerables en el momento del despliegue, carecen de medios para parchear las vulnerabilidades después de su descubrimiento, o que permanezcan en servicio una vez finalizado el soporte del proveedor, hacen que el montaje de botnets y la distribución de amenazas demasiado fáciles.
4. El impacto de las lagunas en la educación y la concienciación: Lagunas de conocimiento en el hogar y la empresa clientes, desarrolladores de productos y operadores de infraestructuras impiden el despliegue de la herramientas, procesos y prácticas que harían que el ecosistema fuera más resistente. En mecanismos particulares y fáciles de usar para identificar opciones más seguras análogas a el programa Energy Star o las calificaciones de choque de los vehículos son necesarios para informar sobre la adquisición decisiones.
5. Conflictos entre los incentivos del mercado y los objetivos de resiliencia: Los incentivos de mercado percibidos no no se ajusta al objetivo de "reducir drásticamente las amenazas perpetradas por los ataques distribuidos". Los incentivos del mercado motivan a los desarrolladores y vendedores de productos a minimizar el coste y el tiempo de comercialización, en lugar de incorporar la seguridad u ofrecer una seguridad eficiente actualizaciones.

[1] El texto completo de la Orden Ejecutiva está disponible en https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

6. La necesidad de una acción intersectorial coordinada: Ninguna comunidad de partes interesadas es de abordar el problema de forma aislada. Las contribuciones de todos los sectores serán necesario para aumentar significativamente la resistencia del ecosistema contra las redes de bots y amenazas distribuidas automatizadas.

El taller proporcionó información crítica que, junto con la información pública recibida en respuesta a la solicitud de comentarios de la Administración Nacional de Telecomunicaciones e Información y una informe del Comité Consultivo de Telecomunicaciones de Seguridad Nacional, informará al desarrollo del proyecto de informe. Las implicaciones para el informe de enero de 2018 incluyen:

- Las acciones propuestas en el informe abordarán cada uno de los temas generales extraídos de participantes en el taller.
- El informe recomendará una o más acciones propuestas para cada una de las partes interesadas grupos (es decir, proveedores de infraestructuras, desarrolladores de productos, empresas, usuarios domésticos, académico y gubernamental).
- Las partes interesadas no gubernamentales esperan que el gobierno federal predique con el ejemplo y Promover las acciones de otras partes interesadas a través de incentivos en lugar de la regulación.
- Muchas acciones dependerán de acciones asignadas a otras partes interesadas, por lo que los mecanismos de colaboración tendrán que ser identificados también en el informe.
- Las recomendaciones incluirán probablemente acciones inmediatas para aumentar la concienciación y despliegue de las tecnologías actualmente disponibles, las acciones a medio plazo para crear un mercado incentivos (especialmente para asegurar el ciclo de vida completo del producto) y promover la coordinación y colaboración, y acciones a largo plazo para desarrollar nuevas tecnologías.

Se agradecen otras contribuciones públicas sobre este tema, que pueden enviarse a distributed.threats@nist.gov. Las contribuciones presentadas antes del 15 de octubre de 2017 serán consideradas para su inclusión en el informe preliminar, que se compartirá con la comunidad en o antes de 5 de enero de 2018.

Las contribuciones y comentarios públicos sobre el informe preliminar se aceptarán hasta febrero 5, 2018. Una vez cerrado el periodo de comentarios, se celebrará un taller público en febrero para discutir la resolución prevista de los comentarios. Sobre la base de los comentarios del público y los debates mantenidos en el segundo taller, los Departamentos completarán el informe para presentarlo al Presidente el 11 de mayo de 2018 o antes.

Índice de contenidos

Lista de apéndices

Lista de figuras

1. Introducción

Orden ejecutiva 13800, "Fortalecimiento de la ciberseguridad de las redes federales y de las Infraestructura" fue emitido el 11 de mayo de 2017. En la sección 2 (d), la orden ejecutiva requiere los Secretarios de Comercio y de Seguridad Nacional "dirigirán conjuntamente una proceso para identificar y promover la acción de las partes interesadas adecuadas para mejorar la resiliencia de el ecosistema de Internet y las comunicaciones y fomentar la colaboración con el objetivo de reduciendo drásticamente las amenazas perpetradas por ataques automatizados y distribuidos (por ejemplo, botnets)". La Orden Ejecutiva ordena a los Departamentos publicar un informe preliminar en enero de 2018 y presentar el informe final al Presidente antes del 11 de mayo de 2018.[2]

Estas actas describen el 11 y 12 de julio de 2017 "Mejora de la resiliencia de Internet y Taller "Ecosistema de Comunicaciones" dirigido por el Instituto Nacional de Normas y Tecnología (NIST) como paso inicial en este proceso. El taller se llevó a cabo bajo Normas de Chatham House. Se animó a los participantes a compartir las opiniones y la información de los participantes en el taller, pero se les pidió que se abstuvieran de identificar a los ponentes o sus afiliación. De acuerdo con las normas, este informe no asocia las cuestiones planteadas en el taller con organizaciones o sectores industriales.

El taller complementó varias líneas de trabajo que se desarrollan simultáneamente en varios components de los departamentos para involucrar a las partes interesadas e identificar las acciones apropiadas, incluyendo una solicitud para los comentarios publicados por la Administración Nacional de Telecomunicaciones e Información (NTIA)[3] y del Departamento de Seguridad Nacional (DHS) para la Seguridad Nacional y Consejo Asesor de Telecomunicaciones (NSTAC). [4]

Las Actas constan de cinco componentes principales: esta introducción; un breve recuento de el proceso empleado para organizar el taller y desarrollar las actas; un taller resumen en el que se destacan los temas comunes del taller; los impactos previstos por el información obtenida de los participantes en el taller sobre el proyecto público del informe que comercio y el DHS publicarán en enero de 2018; y las oportunidades para continuar el compromiso sobre este tema.

[2] El texto completo de la Orden Ejecutiva está disponible en https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[3] La Administración Nacional de Telecomunicaciones e Información (NTIA) publicó la "Solicitud de comentarios sobre Promover la acción de las partes interesadas contra las redes de bots y otras amenazas automatizadas" el 8 de junio. Información adicional, incluyendo los comentarios públicos recibidos por la NTIA están disponibles en https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoción de la acción de las partes interesadas contra las redes de robots y otras amenazas automatizadas.

[4] Para más información sobre el NSTAC, véase https://www.dhs.gov/national-security-telecommunications-advisory-comité.

2. Planificación, ejecución y análisis del taller

Planificación de talleres

Inmediatamente después de la publicación de la O.E. 13800, y de forma simultánea a estos esfuerzos, el NIST comenzó a planificar un taller público, junto con nuestros socios de la NTIA y el DHS, como una paso inicial para involucrar a las partes interesadas en la elaboración del informe. El taller fue diseñado para que las partes interesadas puedan explorar de forma abierta y transparente una serie de soluciones emergentes para mejorar la resistencia del ecosistema de Internet y las comunicaciones (el ecosistema) contra las amenazas automatizadas y distribuidas. El taller se anunció el 6 de junio de 2017 con sólo cinco semanas de antelación para que las contribuciones pudieran reflejarse en el proyecto público. A pesar del tiempo de espera, el taller logró rápidamente una inscripción completa de 150 participantes que representan a diversas comunidades de interesados. El equipo de planificación del taller agradece especialmente las numerosas adaptaciones realizadas por nuestros panelistas, ponentes y facilitadores a participar dado el poco tiempo de espera y las interrupciones inesperadas de los viajes aéreos. [5]

Resumen del taller

El orden del día se estructuró en una serie de paneles moderados y sesiones de trabajo en las que se exploró el contribuciones potenciales de cinco comunidades de actores clave: infraestructura de Comunicaciones proveedores, desarrolladores de productos, clientes, investigadores y gobiernos. Además de ofrecer los paneles tenían como objetivo estimular el debate en los grupos de trabajo. sesiones. Los facilitadores de los grupos de trabajo se encargaron de orientar el debate hacia la identificación de una amplia de opciones para una comunidad de interesados específica (por ejemplo, proveedores de infraestructuras, productos desarrolladores o propietarios de redes) para mejorar la resistencia del ecosistema frente a los amenazas distribuidas. Se pidió a los facilitadores que aplazaran el debate sobre las opciones específicas de otros comunidades a la sesión correspondiente, pero el debate que destaca las dependencias entre se fomentó la realización de posibles acciones por parte de las diferentes comunidades de interesados. Los facilitadores fueron Se ha indicado que no es necesario que los participantes en la mesa redonda lleguen a un consenso con respecto a una opción, o establecer una ordenación o priorización de estas opciones.

Análisis y preparación de las actas

El Centro Nacional de Excelencia en Ciberseguridad (NCCoE) del NIST proporcionó información sobre ciberseguridad expertos en la materia (PYMES) para que sirvieran de escribas en las sesiones de trabajo y realizaran la análisis técnico de las aportaciones recogidas. Aproximadamente 787 contribuciones se clasificaron en diez categorías principales; 313 contribuciones también se clasificaron como pertenecientes a una de las cinco categorías menores ortogonales.

[5] Véase https://www.washingtonpost.com/news/dr-gridlock/wp/2017/07/10/hazmat-incident-at-air-traffic-control-center-delays-flights-around-the-washington-region/?utm_term=.d009260f400e.

Las principales categorías
fueron:

- Concienciación
- Retos empresariales
- Desarrollo y ciclo de vida de los productos
- Complejidad del ecosistema
- Papel del consumidor
- Gobernanza
- Intercambio de información, colaboración y privacidad
- Datos
- Métricas
- Tecnologías fundamentales y emergentes

Los escribas clasificaron los temas de debate planteados en sus sesiones de trabajo de acuerdo con lo siguiente categorías, y se elaboraron porcentajes agregados. La distribución de las 787 contribuciones se representa en la Figura 1, a continuación. Casi la mitad de las contribuciones se caracterizaron como negocios desafíos o cuestiones de gobernanza.

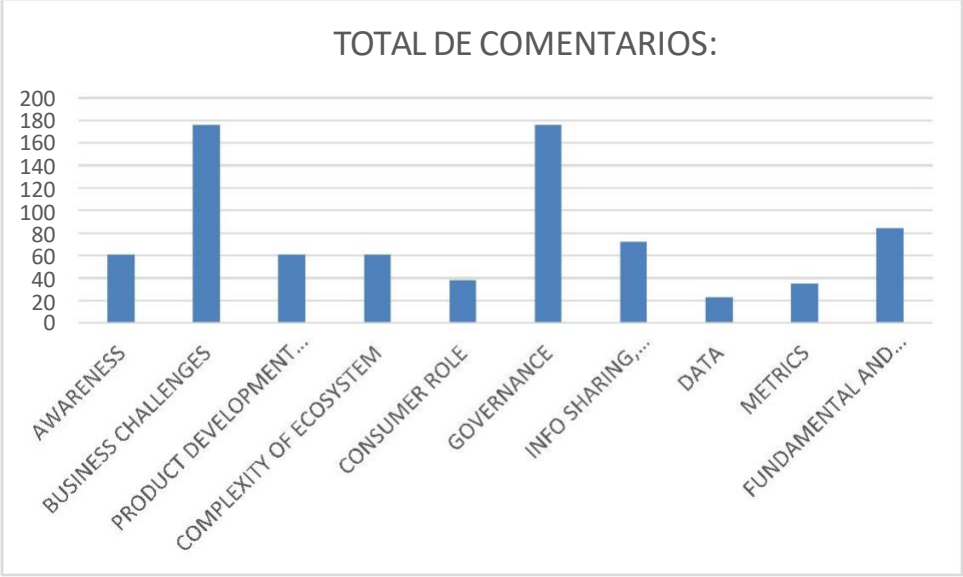

Figura 1. Distribución de las contribuciones según las características de los escribas

Las categorías menores
fueron:

- Adversarios
- Comunicación
- Ciberseguridad
- Lecciones y mejores prácticas
- Normas

Los escribas clasificaron los temas de debate planteados en sus sesiones de trabajo de acuerdo con lo siguiente categorías menores, y se elaboraron porcentajes agregados. La distribución de los 313 las contribuciones se representan en la figura 2. Más de la mitad de los comentarios asignados a las contribuciones menores categorías se consideraron cuestiones de ciberseguridad, con lecciones aprendidas, comunicación normas que reciben la mayor parte de los comentarios restantes.

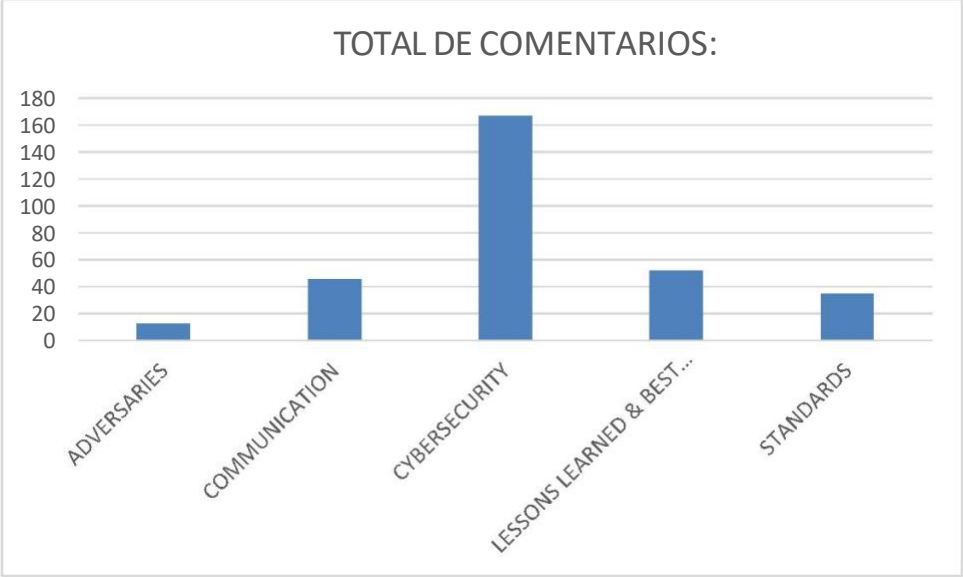

Figura 2. Caracterización de las contribuciones según las áreas temáticas menores

Los expertos en la materia del NIST se basan en las notas sin procesar proporcionadas por el NCCoE de los escribas, las listas con viñetas de los aspectos más destacados preparadas por los escribas y el análisis suministrado por el NCCoE, como así como las propias notas personales de las PYMES del NIST.

3. Resumen del taller

Esta sección resume las cuestiones planteadas por los ponentes y los participantes en los talleres a lo largo del de la jornada y se presenta en dos subsecciones.

- La primera subsección presenta seis temas generales que surgieron de los debates. Estos temas se aplican a múltiples sectores, y fueron planteados por diferentes participantes en múltiples ocasiones. Aunque no se juzgó el consenso y no debe suponerse, pocos habló en contra de estos conceptos.

- La segunda subsección ofrece información específica del sector (es decir, específica de una comunidad de interesados) cuestiones y observaciones. En algunos casos, esto representa una visión más detallada del temas generales, pero en otros los conceptos son simplemente exclusivos de ese sector. La página web las observaciones sectoriales se organizan por grupos de trabajo.

Aunque el ámbito del taller incluía toda la gama de amenazas distribuidas de forma automatizada, hay que observó que la conversación se centraba con frecuencia en el Internet de las cosas. Estaba claro que el Mirai La red de bots estaba en la mente de muchos participantes, y proporcionó un contexto compartido para las discusiones sobre asegurar el ciclo de vida de los productos, la educación y la concienciación, y muchos otros temas. El contexto de la IO sólo se reitera en los resúmenes que siguen cuando las cuestiones u observaciones eran específicas de IoT (a diferencia del encuadre ilustrativo.)

Como se ha señalado anteriormente, el taller se llevó a cabo bajo las normas de Chatham House, y los facilitadores se centró en la presentación de opciones de actuación más que en alcanzar un consenso o obtener medidas objetivas de apoyo. En este resumen se utilizan las frases "varios participantes,"un número de participantes" y "muchos participantes" para denotar nuestra evaluación subjetiva de niveles crecientes de apoyo o interés más allá de la línea de base normal.

Temas generales

A lo largo de los debates del taller se encontraron seis temas generales[6]:

1. El carácter global del problema;
2. La disponibilidad de herramientas eficaces;
3. La importancia de asegurar los productos durante todo el ciclo de vida;
4. El impacto de las lagunas en la educación y la concienciación;
5. Conflictos entre los incentivos del mercado y los objetivos de resiliencia; y
6. La necesidad de una acción intersectorial coordinada.

Los participantes en el taller señalaron repetidamente que las redes de bots y las amenazas distribuidas son un problema mundial. Aunque hay excepciones, la mayoría de los dispositivos comprometidos que conforman las redes de bots son geográficamente ubicados fuera de los Estados Unidos. Acciones que aumentan la seguridad de los dispositivos vendidos en Estados Unidos, o que protegen contra las amenazas de las telecomunicaciones nacionales

[6] Obsérvese que los participantes en el taller no se pusieron de acuerdo ni establecieron una prioridad. En consecuencia, el orden de los seis temas es no es significativo.

tráfico, sólo puede abordar una parte del problema. Acción coordinada con los socios internacionales será necesario para aumentar la resistencia del ecosistema frente a estas amenazas. Aunque la resolución requerirá un enfoque global, hubo un amplio acuerdo en que Estados Unidos podría y debe liderar la lucha contra estas amenazas, actuando con el ejemplo y promoviendo normas de comportamiento adecuadas.

También hubo un amplio acuerdo sobre las posibilidades de actuación inmediata. Para citar un orador, "no partimos de una hoja en blanco". Al aplicar un conjunto de medidas bien herramientas, procesos y prácticas conocidas y efectivas, podemos mejorar significativamente la resiliencia del ecosistema. Estas herramientas han demostrado su valor en el ámbito de la informática personal. Sin embargo, estas tecnologías y procesos no están incluidos en las prácticas comunes de los productos desarrollo y despliegue en muchos otros sectores. Un conjunto (o conjuntos) de normas mínimas o requisitos debe establecerse, aunque tal vez no formalmente, para garantizar que las mejores prácticas se aplican en todos los sectores.

Abordar todo el ciclo de vida del producto/red con estas herramientas, procesos y prácticas fue otro tema general. La importancia de incorporar la seguridad desde el principio, en lugar de que atornillarlo después, era una creencia ampliamente compartida. Demasiados productos se envían con vulnerabilidades conocidas; estos productos pueden ser detectados, atacados y comprometidos en minutos de despliegue. Se necesitan mecanismos de actualización seguros para hacer frente a las vulnerabilidades descubiertos durante la vida útil normal del producto. Procesos claros y eficaces para abordar el fin de también se necesitan cuestiones relacionadas con la vida útil, ya que no se pueden abordar las vulnerabilidades de los productos obsoletos, lo que garantiza que los adversarios tengan un punto de partida fiable a la hora de penetrar en una empresa o establecer una botnet.

Los participantes señalaron un problema sistémico de educación y concienciación. Casi el 6 % de los recomendaciones/comentarios durante las sesiones de trabajo del taller se centraron en la importancia de educación y concienciación. Muchos asistentes citaron la seguridad en el transporte, donde el uso del cinturón de seguridad y las calificaciones de las pruebas de choque han dado lugar a mejores resultados, como una historia de éxito de la educación y la concienciación. Otros citaron el mismo sector como un ejemplo de precaución, con largos plazos antes de la generalización aceptación de los cinturones de seguridad y otras mejoras tecnológicas. Energy Star también fue objeto de discusión repetida, con métricas sencillas para los consumidores. Un organismo independiente para probar y certificar las características relevantes para la seguridad y ofrecer un esquema de calificación más accesible, fue citado con frecuencia como un paso importante hacia la identificación por parte del consumidor de productos con fuertes características de seguridad.

Los incentivos percibidos por el mercado no se ajustan a nuestros objetivos de seguridad y resiliencia, según muchos participantes en los talleres. Los desarrolladores y vendedores de productos minimizan el coste y el tiempo de comercialización, en lugar de incorporar seguridad u ofrecer actualizaciones de seguridad eficientes. Gran parte del debate se centró en en técnicas para crear incentivos de mercado, como la certificación independiente de productos, pero algunos consideraron que sería necesaria una intervención más activa del gobierno (por ejemplo, la regulación) para superar los fallos del mercado. Sin embargo, los participantes señalaron que el cumplimiento de la normativa también puede ser a de los objetivos de seguridad y resiliencia. [7]

[7] Por ejemplo, varios asistentes citaron la reticencia histórica del sector sanitario a poner parches a los dispositivos médicos para evitar la recertificación por parte de la Administración de Alimentos y Medicamentos. Tenga en cuenta que las directrices actuales de la FDA abordan esta cuestión, permitiendo parches sin requerir una nueva certificación en algunos casos. Véase "Gestión de la ciberseguridad después de la comercialización en el sector médico".

Otro tema fue la incapacidad de un sector en particular para influir en la resistencia del ecosistema de forma aislada. Los proveedores de infraestructuras pueden mejorar la eficacia de los mecanismos anti-DDoS, pero siempre pueden ser superados por un mayor número de dispositivos. Los fabricantes de dispositivos pueden mejorar la calidad de sus productos, pero no disponemos de la tecnología necesaria para construer productos, por lo que algunos dispositivos siempre serán vulnerables a las amenazas. Del mismo modo, los propietarios de empresas pueden aumentar sus inversiones en seguridad, pero algunos de sus sistemas serán vulnerables, y los adversarios disponen de todo Internet para lanzar ataques contra la empresa. Los investigadores pueden desarrollar mejores tecnologías, pero las mejoras en la seguridad sólo se consiguen si los proveedores incluyen estas tecnologías en los productos, los clientes compran estos productos y los despliegan adecuadamente. Se necesitarán contribuciones de todos los sectores para aumentar significativamente la resistencia del ecosistema contra las redes de bots y las amenazas distribuidas automatizadas.

Resúmenes sectoriales

En esta sección se repasan las cuestiones y observaciones del taller desde la perspectiva de cada comunidad de interesados a su vez. En algunos casos, esto representa una visión más detallada o matizada de los temas generales, pero en otros los conceptos son simplemente exclusivos de ese sector.

Infraestructura

El sector de los proveedores de infraestructuras fue objeto del primer panel del taller y sesión de trabajo. El panel se centró en el estado actual de la infraestructura, las tendencias y enfoques prometedores para mitigar las amenazas distribuidas automatizadas, como los DDoS, con especial atención a las redes de bots y al IoT.

Varios participantes señalaron que la infraestructura de Internet es mucho más resistente hoy en día, y resiste ataques DDoS de una magnitud impensable hasta ahora de forma casi diaria. Este demuestra tanto la eficacia de las herramientas actuales como la naturaleza de la carrera armamentística de los DDoS protección.

Los participantes identificaron explícitamente una serie de herramientas y técnicas para la protección contra DDoS; éstas son que se enumeran a continuación con un breve análisis de los puntos fuertes y las limitaciones. (El orden de presentación no tiene importancia).

- Filtrado de entrada/salida: Muchos participantes se refirieron a la tarea de ingeniería de Internet Force (IETF) Best Current Practice (BCP) 38, "Network Ingress Filtering", y BCP 84, "Filtrado de entrada para redes multihomed". Históricamente, los ataques DDoS se han basado en la suplantación de direcciones de red, en la que los sistemas comprometidos afirman direcciones de origen que no no existe en la red local, para ocultar la ubicación de los recursos de los atacantes. [8] Por tráfico filtrar en los límites de la empresa y descartar el tráfico que es claramente ilegítimo, es posible para limitar la eficacia y el alcance de estos ataques.

---

[1] Dispositivos https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[8] Algunos ataques DDoS recientes, como Mirai, han afirmado direcciones de origen legítimas.

BCP 38 y BCP 84 se publicaron en 2000 y 2004, respectivamente, pero su adopción y El despliegue ha sido lento y desigual. Aunque el nivel de apoyo actual se debatió en el taller, hubo un apoyo generalizado al despliegue ubicuo del filtrado de tráfico para las redes de borde. Se debatió brevemente sobre las limitaciones del filtrado dentro de la Red troncal de Internet, donde el enrutamiento asimétrico (donde el tráfico entre dos puntos finales sigue caminos separados en cada dirección) complica la diferenciación del tráfico legítimo de eso con direcciones de red falsas.

- Servicios de protección DDoS fuera de las instalaciones: Los ISP están ofreciendo protección DDoS fuera de las instalaciones servicios para los clientes, en los que el tráfico se redirige y filtra antes de su entrega al red del cliente. Los servicios de protección DDoS requieren el aprovisionamiento de importantes recursos (en términos de sistemas especializados y ancho de banda extra) para absorber y procesar la el tráfico adicional proyectado. Estos servicios han demostrado su eficacia en numerosos casos, pero los proveedores de servicios se ven obligados a aumentar continuamente el nivel de recursos adicionales a medida que las redes de bots crecen y el ancho de banda total de los ataques aumenta.

  La eficacia de estos servicios está limitada en parte por el conocimiento de los clientes. DDoS servicios de protección requieren la provisión de importantes recursos adicionales (en términos de sistemas especializados y ancho de banda extra) por lo que no figuran en la red básica ofertas de servicios. Los clientes pueden no ser conscientes de los riesgos que presentan los ataques DDoS hasta que se conviertan en víctimas, o que estos servicios estén siquiera disponibles. Incluso cuando un empresa tiene el conocimiento y el deseo de adquirir servicios anti-DDoS, la arquitectura pueden ser necesarios cambios para optimizar el nivel de seguridad alcanzado.

  (Nota: Las comunicaciones entre los clientes y los proveedores de servicios presentan otra desafío a la eficacia de los servicios de protección DDoS fuera de las instalaciones. Ver en tiempo real señalización, abajo).

- Protección DDoS in situ: Cuando los ataques DDoS se adaptan a los objetivos de una empresa recursos críticos, como las aplicaciones clave o el firewall corporativo, la protección local mecanismos pueden ser más eficaces. Estos servicios "On-Premise" están ahora disponibles como complemento de los servicios tradicionales de protección DDoS del proveedor de servicios (fuera de las instalaciones) ofrecidos por los ISP. Como en el caso anterior, el conocimiento de los clientes sobre los riesgos y las tecnologías disponibles es como precursor de la mejora de la resiliencia a través de estas tecnologías.

- Señalización en tiempo real: Como se ha señalado anteriormente, las comunicaciones con los servicios de protección DDoS y dispositivos durante los ataques puede ser problemático. Varios asistentes destacaron que Internet Grupo de Trabajo de Señalización de Amenazas Abiertas DDoS (DOTS) de la Engineering Task Force como fuente prometedora de soluciones en un futuro próximo. DOTS está desarrollando actualmente un conjunto de normas para la señalización en tiempo real de la telemetría relacionada con el DDoS y la gestión de las amenazas solicitudes a través de enlaces que pueden estar congestionados por el tráfico de ataque.

- Coordinación global: Internet es una infraestructura global, al igual que la amenaza.

Los enfoques basados en las infraestructuras exigen una estrecha cooperación y coordinación. Participantes indicaron que la cooperación entre pares nacionales se ha vuelto bastante sólida, pero la comunicación y la cooperación internacionales han sido desiguales. Hay esfuerzos para establecer normas y codificar las prácticas, pero estos esfuerzos están retrasando el problema.

Los participantes señalaron que casi cincuenta empresas han aceptado las Normas mutuamente acordadas para la Seguridad del Enrutamiento (MANRS), y este acuerdo podría considerarse un modelo de esfuerzo específico para botnets. Otros señalaron el Código de Conducta Anti-Bot de Estados Unidos para Internet Proveedores de Servicios (ABC para los ISP) desarrollado por la Federal Communications Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones de la Comisión ("CSRIC"). [9]

- Complejidad: Los problemas de infraestructura se ven agravados por la creciente complejidad del Internet: no solo la llegada del IoT, sino también la expansión de la infraestructura multiusuario. Las normas y prácticas que se aplican ampliamente a los PC y servidores no han sido uniformemente al espacio de la IO, con consecuencias desafortunadas, y los ISP más pequeños hacen no tienen la capacidad de aplicar las mismas normas y prácticas que los grandes ISP. Incluso cuando una empresa tiene el conocimiento y el deseo de adquirir servicios anti-DDoS, pueden ser necesarios cambios arquitectónicos para optimizar el nivel de seguridad alcanzado.
- Métricas: Se carece de métricas utilizables para caracterizar los ataques y documentar su gravedad. Uno de los participantes señaló que la Oficina Federal de Investigación había desarrollado un 75 marco de atributos para describir los ataques distribuidos, pero que completar esta descripción tardaban tanto que los ataques solían terminar. Las métricas utilizables y ampliamente reconocidas son necesarios para facilitar la coordinación y la cooperación.
- Interdependencias: Los participantes señalaron una serie de dependencias con otros sectores. Deficiente los atributos de seguridad de los dispositivos de borde, y especialmente de los dispositivos IoT, hacen que sea extremadamente difícil que la infraestructura se proteja contra estos ataques.
- Educación y concienciación: La educación y la concienciación de los clientes es una necesidad urgente; cuando los proveedores de servicios de Internet se ponen en contacto con las empresas para alertarlas de los problemas, pero las empresas suelen estar mal equipadas para comprender el problema o ejecutar sus propias responsabilidades. Generalmente asumen que su ISP "iba a encargarse de eso", sea lo que sea "eso".
- La educación y la concienciación del personal operativo también se consideraron problemáticas. En particular, algunos consideraron que el escaso despliegue del filtrado BCP 38 en los ISP extranjeros, los más pequeños ISPs domésticos, y los routers BGP mantenidos por las empresas fue en gran parte el resultado de la falta de habilidades dentro de esas organizaciones.

Fabricante del producto

El segundo panel y la sesión de trabajo exploraron los esfuerzos actuales y las oportunidades futuras para fabricantes de componentes de red y dispositivos (incluidos los proveedores de soluciones de IoT) para abordar la causas fundamentales de las recientes redes de bots

[9] Consejo de Fiabilidad e Interoperabilidad de la Seguridad de las Comunicaciones (CSRIC) III, Código de Conducta Anti-Bot de los Estados Unidos (ABC) para Proveedores de servicios de Internet (PSI), Informe final, GT 7 (mar. 2012), http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

(acceso no restringido a la red, contraseñas codificadas y software). El debate incluyó productos desarrollados tanto para la empresa como para el hogar.

Hay dos caracterizaciones generales del problema del desarrollo de productos. La más La caracterización prevalente indicó que el número de vulnerabilidades en los productos debe ser significativamente reducido para dificultar el compromiso de los dispositivos en masa y el lanzamiento de grandes ataques. Por otro lado, los productos nunca serán perfectos, por lo que algunos participantes consideraron que deberíamos concentrarse en tecnologías que limiten los daños de los dispositivos comprometidos. Las dos caracterizaciones no están en conflicto, y la mayoría parecía pensar que debían seguirse ambas vías.

En cuanto a dificultar la puesta en peligro de los sistemas, muchos participantes destacaron que esto era una cuestión de ciclo de vida del producto. En su opinión, es fundamental gestionar la vulnerabilidad de dispositivos desde el envío inicial del producto, pasando por su uso, hasta el final de su vida útil. Una serie de técnicas que reducir la vulnerabilidad de los productos:

- Para reducir la vulnerabilidad de los productos en su despliegue inicial, los participantes sugirieron una mayor aplicación de una serie de herramientas complementarias y mejores prácticas. Por ejemplo, es más probable que los procesos de desarrollo seguros por diseño den lugar a configuraciones que son generalmente seguras y evitan las contraseñas administrativas codificadas y otros escollos comunes. Las cadenas de herramientas de desarrollo de software sensibles a la seguridad pueden eliminar errores de codificación comunes, como la mayoría de los desbordamientos de búfer.

- Incluso cuando se desarrollan utilizando metodologías de diseño seguro y centradas en la seguridad cadenas de herramientas, es probable que se detecten vulnerabilidades en el software, continuando durante meses o años después de que el producto se despliegue por primera vez. El malware que se dirige a estas vulnerabilidades suele ser ampliamente disponibles en días o semanas después de su detección. Para gestionar la vulnerabilidad de estos productos, muchos participantes afirmaron que la actualización segura y preferiblemente automática es absolutamente esencial. Además, afirmaron que los fabricantes deberían comprometerse a parchear las vulnerabilidades de seguridad durante un periodo mínimo después de la implantación.

- Las raíces de la confianza son una tecnología complementaria que fue citada por numerosos participantes.

Al proporcionar un conjunto de funciones básicas y de alta confianza, podemos aumentar la garantía de que el software y el firmware no se han modificado o sólo se han modificado mediante una actualización segura mecanismos. El módulo de plataforma de confianza (TPM) es un ejemplo ampliamente disponible, pero puede ser demasiado costoso para los dispositivos de bajo coste. Nuevos esfuerzos, como el Trusted Computing Group (TCG) Device Identity Composition Engine (DICE) puede ampliar el alcance de productos que incorporan estas tecnologías proporcionando una base para la identidad del dispositivo y verificar que se han instalado las actualizaciones de software. Los dispositivos necesitan una identidad emitida por el fabricante para que haya una manera de saber qué tipo de dispositivo es y qué configuración, software y los parches están destinados al dispositivo. El proyecto de publicación NIST SP 800-193 del 30 de mayo de 2017 describe las raíces de la confianza para la protección, detección y recuperación que podrían aplicarse en el espacio del IoT como bloques de construcción para recuperar dispositivos a distancia. Personas es poco probable que gestionen individualmente los dispositivos IoT, por lo que se necesita una recuperación automatizada.

- Cuestiones relacionadas con el fin de la vida útil y el software sin licencia. Los participantes también destacaron la vulnerabilidades asociadas a los dispositivos que no son compatibles con su fabricante. En estos casos, las actualizaciones ya no se publican (o quizás nunca se publicaron) por lo que las vulnerabilidades persisten indefinidamente. Esto tiene un paralelismo con el software sin licencia, donde las actualizaciones de seguridad no suelen estar disponibles.

  Los participantes alabaron la decisión de Microsoft de actualizar Windows XP para mitigar el WannaCry, a pesar de haber finalizado el soporte tres años antes, pero consideró que era una caso excepcional. Los participantes consideraron que las propuestas anteriores de soluciones generales al final de la vida problemas, como la liberación de software para productos no soportados al código abierto comunidad, como poco práctico.

Los participantes señalaron que las técnicas mencionadas son ampliamente conocidas y bien comprendidas. So aplicada ampliamente en algunos sectores (por ejemplo, los sistemas operativos) pero casi nunca en otros (por ejemplo, la Internet de las cosas). Se sugirieron una serie de impedimentos y causas fundamentales, entre ellos:

- Educación y concienciación del consumidor: Los fabricantes de productos están motivados por las ventas, y los consumidores no tienen la perspectiva necesaria para priorizar la seguridad ni la capacidad de identificar los productos con mayor garantía. Los consumidores pueden no estar motivados de forma natural para elegir este tipo de productos, dado que los productos comprometidos suelen seguir funcionando su función determinada mientras participan en ataques distribuidos. La educación del consumidor debe centrarse en las posibles consecuencias para la seguridad y el rendimiento, más que en las redes de bots prevención: puede que a los usuarios no les importe que su nanny cam ataque a un gran banco, pero sí les importará sobre extraños que invaden la privacidad de su familia.

  Una vez motivados, los consumidores seguirán necesitando ayuda para seleccionar los productos que puedan tienen menos vulnerabilidades a lo largo del ciclo de vida del despliegue. Ningún mecanismo satisfactorio para transmitir información a los consumidores sobre la seguridad de los productos existe hoy en día. Energy Star para la eficiencia energética y la National Highway Traffic Safety Las calificaciones de seguridad de 5 estrellas de la Administración Nacional de Seguridad del Transporte (NHTSA) para la seguridad de los vehículos fueron citadas como ejemplos importantes y exitosos.

- Educación y concienciación de los desarrolladores de productos: Como el espacio entre la TI y la tradicional de productos, educar a los desarrolladores de productos en materia de seguridad se ha convertido en una necesidad. Los diseñadores de electrodomésticos saben cómo mantener los alimentos a temperatura, limpiar tejidos o tostar pan. A medida que estos productos pasan a formar parte de la ecosistema, pedimos a estos diseñadores que incorporen nuevos requisitos de seguridad que son ajenos a ellos. En particular, la industria debe reconocer que la actualización segura los mecanismos son un requisito para "todo".

- Desajuste con los incentivos del mercado: Muchos desarrolladores de productos temen que la inversión en seguridad encarecerá sus productos y retrasará el despliegue de la innovadora nuevas funcionalidades que construyen la cuota de mercado. Los proveedores más grandes tienen un desarrollo más sólido procesos, pero las nuevas empresas y las más pequeñas a menudo dependen de procesos menos maduros.

- Responsabilidad poco clara: También se debatió sobre la responsabilidad: quién debe ser responsable de la seguridad de los productos? ¿Los propietarios? ¿Los vendedores? Para los usuarios domésticos y las pequeñas empresas, parece poco práctico hacerles responsables si su DVR doméstico o la cámara de seguridad de su tienda está comprometida y se añade a una red de bots. Para

usuarios industriales, podemos tener mayores expectativas, pero a medida que se multiplican los dispositivos IoT también puede haber limitaciones en este sentido. En ambos entornos, los protocolos como el Descripción de uso del fabricante (MUD, véase la segmentación de la red virtual más abajo) puede ayudar a trasladar parte de la responsabilidad a los fabricantes de forma escalable.

El segundo punto de vista era que los productos nunca serán perfectos, y los incentivos simplemente no centrarse en la seguridad. Esto refuerza la idea de que la actualización segura es una seguridad fundamental requisito, pero también tenemos que encontrar formas de limitar los daños de los dispositivos comprometidos. Se propusieron varias direcciones hacia adelante, entre ellas:

- Segmentación de la red virtual: Históricamente, los sistemas conectados a Internet han gozado de conectividad total en las capas de red y transporte. [10] Las necesidades de los usuarios humanos son imprevisible, por lo que restringir el tráfico de forma significativa sería inmanejable. Las implicaciones de la conectividad total son significativas: cualquier dispositivo de Internet puede ser utilizado para lanzar un ataque a cualquier otro dispositivo; una vez comprometido, el dispositivo se convierte en un lanzamiento de movimiento lateral, tanto dentro de la empresa como en los ataques a otros dispositivos conectados. Con la aparición de la Internet de las cosas (IoT), las Comunicaciones necesidades de muchos dispositivos se vuelven más predecibles y las implicaciones de seguridad de la conectividad inaceptable. Por ejemplo, un termostato IoT puede necesitar comunicarse con el sitio web del fabricante para las actualizaciones, pero probablemente no necesita comunicarse con una bolsa de valores.

  El estándar MUD que se está desarrollando actualmente en el IETF ofrece una vía potencial hacia adelante. Cuando los dispositivos se unen a la red, solicitan una dirección IP a través de la función Dynamic Protocolo de configuración de host (DHCP). Cuando se utiliza el MUD, el dispositivo también indica cómo para obtener de forma segura una descripción de los requisitos de comunicación del dispositivo del fabricante. Los proveedores de equipos de red aprovechan el archivo MUD y sus capacidad para aplicar el filtrado de paquetes por dispositivo. Si se compromete, el atacante no podía utilizar el termostato IoT para desplazarse lateralmente por la cafetera o atacar el bolsa de valores.

- La señalización de amenazas ofrece un enfoque alternativo para restringir el acceso a la red. Tercero los servicios de terceros identifican los sistemas de host o los dominios que presentan una amenaza relativa para la ecosistema (o algún sector de la industria). Esta información se transmite a los suscriptores redes empresariales, que establecen filtros de ruta apropiados y descartan las tráfico perjudicial. Mientras que el MUD está adaptado para soportar dispositivos con de las comunicaciones, la señalización de amenazas mejora la seguridad de los dispositivos informáticos con necesidades de comunicación impulsadas por el usuario (e imprevisibles).

Clientes: Empresas, usuarios domésticos y administraciones públicas

El tercer panel y la sesión de trabajo exploraron cómo los clientes, particularmente en la empresa, pueden ambos se protegen de los ataques distribuidos -incluyendo DDoS, ataques a

[10] Más tarde, los administradores de red podían restringir el acceso mediante reglas de cortafuegos que se aplicaban en toda la empresa, pero había generalmente no hay limitaciones dentro de la empresa.

y el fraude, y evitar ser parte del problema. Se pidió a los participantes que destacaran las capacidades y limitaciones de las mejores prácticas actuales y las tecnologías emergentes, y considerer el potencial de colaboración intersectorial.

Muchos participantes diferenciaron a los clientes en tres grandes clases: usuarios domésticos, empresas y gobierno. En algunos debates, las empresas se diferenciaron además por su tamaño, ya sea como grandes frente a las pequeñas y medianas empresas (PYMES), o las nuevas empresas frente a las empresas establecidas. Los participantes tenían expectativas muy diferentes para las distintas clases de clientes en términos de sensibilización, mejores prácticas, aplicabilidad de las tecnologías y colaboración.

Los participantes identificaron una serie de mejores prácticas actuales y emergentes:

- Como se ha señalado anteriormente, muchos participantes identificaron la actualización segura de todos los dispositivos conectados a la red, incluyendo tanto un mecanismo de actualización adecuado como el compromiso del proveedor de proporcionar parches, como la mejor práctica actual más importante. Los detalles de una "adecuada". El mecanismo de actualización dependía del cliente al que se dirigía. Por ejemplo, los participantes sugirió que los usuarios domésticos sólo se beneficiarían de la actualización segura si el mecanismo automática y desatendida. Las grandes empresas exigirían un mayor nivel de control a través de herramientas de gestión centralizadas. Las necesidades y expectativas de las PYMES pueden variar dependiendo de la arquitectura de la red y la experiencia.

- El intercambio de información en tiempo real fue identificado como la mejor práctica actual para el gobierno y las grandes empresas. Compartir la información, tanto dentro de la empresa como a través de la ecosistema, permitirá a las empresas proteger mejor los recursos. Los participantes observaron que los actores maliciosos son mejores que nosotros en esto.

  Sin embargo, la información debe compartirse en una forma procesable, en lugar de hacerlo en forma no formateada texto. Actualmente existen múltiples soluciones para la ciberseguridad general de información. En particular, los participantes identificaron la amenaza estructurada Information eXpression (STIX™) y Trusted Automated eXchange of Indicator Información (TAXII™) como mejor práctica actual. La señalización de amenazas abiertas DDoS (DOTS) que se está desarrollando actualmente en el IETF proporcionará un estándar específico para DDoS solución.

- Arquitecturas de red que restringen los flujos de tráfico para limitar los posibles vectores de ataque y también se habló de los ataques de constreñimiento que se pueden lanzar desde los sistemas comprometidos. Tecnologías emergentes que establecen redes virtuales segmentadas, como el MUD (véase Fabricante de productos, más arriba) proporcionaría información procesable para redes domésticas y empresariales de forma escalable. Para los dispositivos heredados, la red los equipos podrían aprovechar la "señalización de amenazas" (por ejemplo, el intercambio de información para identificar sistemas comprometidos y sistemas o dominios externos sospechosos) y restringir el tráfico adecuadamente.

Dado que gran parte de la tecnología necesaria es ampliamente conocida, se debatió mucho dedicado a los impedimentos percibidos y a los posibles impulsores de la adopción.

- El impacto actual y potencial del ciberseguro fue ampliamente debatido. Experiencia de otros sectores demuestra que los seguros pueden impulsar la adopción de tecnologías. Por ejemplo, se fomentan los descuentos en el seguro del automóvil por los frenos antibloqueo y los airbags los consumidores a dar prioridad a estas características. Los seguros para edificios suelen exigir que el humo detectores y pueden ofrecer descuentos para los aspersores u otras medidas activas. Sin embargo, las ofertas de ciberseguros suelen ser incoherentes y se consideró que tenían un mínimo impacto hasta la fecha en el despliegue de la tecnología de ciberseguridad.

- Algunos participantes sugirieron que se necesitarán datos actuariales adicionales para posicionar impacto en el mercado. Una vez que se disponga de datos para imponer requisitos uniformes y ofrecer descuentos por opciones beneficiosas, el ciberseguro podría influir positivamente en la empresa propietarios.

- La educación y la concienciación son un problema sistémico, especialmente para las PYME y los usuarios domésticos. En media, las administraciones públicas y las grandes empresas debían tener un conocimiento significativo y un conocimiento relativamente profundo de los requisitos de seguridad para apoyar la selección de productos y aplicación de las mejores prácticas. Por otro lado, la reserva nacional de ciberseguridad expertos es insuficiente para imponer estas expectativas a las PYMES, y los usuarios domésticos no pueden ser se espera que se conviertan en expertos en ciberseguridad.

  Mientras se ahogan en información, los clientes no tienen forma de diferenciar el aceite de serpiente del tecnologías eficaces. Por ejemplo, un participante recibió 32 correos electrónicos de productos que afirmaron proteger contra WannaCry el día después de que se lanzara ese ataque. Pocos los clientes tendrían la posibilidad de evaluar sus reclamaciones, por lo que la mayoría no toma ninguna medida.

  Para facilitar la toma de decisiones productivas en materia de adquisición e implantación, los clientes necesitan datos accesibles. Los participantes destacaron la importancia de la certificación de los productos y debatido el impacto de los distintos regímenes de certificación. La calificación de seguridad de 5 estrellas de la NHTSA y la tarjeta de puntuación ENERGY STAR del DOE se citaron como ejemplos de certificación de envases datos en forma accesible. Los participantes tienen grandes esperanzas en las iniciativas en curso en Underwriters' Laboratories y Consumer Reports, aunque los criterios de estos esfuerzos no estaba claro. Proyectos de demostración en el NCCoE y sus guías prácticas asociadas ofrecen otra opción prometedora.

- Los participantes expresaron una serie de opiniones sobre las posibilidades de un sistema estrictamente voluntario adopción. Aunque todos los participantes expresaron su preferencia por las medidas voluntarias, hubo la preocupación de que la lentitud en la adopción obligue al gobierno a intervenir, sobre todo en los sectores que ya están regulados. La perspectiva de las regulaciones a nivel estatal fue particularmente que preocupa a los participantes. La posibilidad de 50 reglamentos ligeramente diferentes sería contraproducente, complicando la oferta de productos y servicios. Sin embargo, la imposición de mayores requisitos a las propias entidades gubernamentales, para predicar con el ejemplo y crear un mercado inicial, se recomendó con frecuencia.

- La claridad de la normativa (si se impone) se consideró esencial para evitar imprevistos consecuencias. Cuando se les obliga a deducir, a menudo se imaginan obstáculos reglamentarios que limitan o impedir la aplicación de mecanismos de seguridad adecuados.

- Los participantes también expresaron su preocupación por el coste. Sin incentivos gubernamentales, los costes para mejorar la ciberseguridad debe repercutir en los consumidores. En una economía global de la UE, la imposición de requisitos a nivel nacional puede obstaculizar la competitividad de negocios en el extranjero.

En resumen, los participantes estuvieron de acuerdo en que se necesitarán cambios culturales antes de que los usuarios domésticos y las empresas estadounidenses maximizan su contribución a la resistencia del ecosistema.

Investigación y academia

El segundo día del taller comenzó con el panel de Direcciones de Investigación, y el tema fue también se abordó en la única sesión de trabajo del segundo día, esa misma mañana. El objetivo de estas el objetivo de los debates era identificar y explorar las carencias en materia de resistencia de la red, y resaltar las oportunidades para abordar esas lagunas.

Los participantes identificaron una amplia gama de direcciones de investigación que podrían tener un impacto positivo en la resiliencia del ecosistema, incluyendo:

- Métricas y clasificación: Métricas y metodologías de clasificación para la automatización Las amenazas distribuidas podrían mejorar la priorización de los recursos para los esfuerzos de mitigación y la ley acciones de aplicación.
- Modelización de botnets y DDoS: Modelos robustos para botnets y otras amenazas automatizadas que abarcar la detección, el paso de datos y la aplicación de la ley podría permitir una y respuestas coordinadas.
- Comportamiento de los actores maliciosos: Los cambios en el comportamiento de los actores DDoS tendrán un impacto negativo en el eficacia de muchas técnicas actuales. Estos cambios incluyen la nacionalización de los mafias y organizaciones criminales cibernéticas; el cambio de "recursos robados" a infraestructura"; y el paso del tráfico impulsado por el usuario a los sistemas automatizados/IoT. Investigación es necesario para predecir el impacto de estos cambios en las tecnologías anti-DDoS actuales.
- Cuestiones sociotécnicas: La resiliencia, al igual que muchos aspectos de la ciberseguridad, tiene aspectos sociales dimensiones y no pueden ser abordadas únicamente a través de la tecnología. Los participantes destacaron la importancia de los enfoques de investigación que tienen en cuenta los aspectos humanos, sociales y organizativos, factores económicos y técnicos, y su repercusión en el despliegue y funcionamiento de un infraestructura resistente. Las interfaces hombre-máquina (véase más adelante) fueron un foco de atención específico. La investigación también es necesaria para entender cómo diseñar organizaciones que sean más resistentes ante un ciberataque y más eficientes en su recuperación de incidentes o desastres procesos.
- Interfaces hombre-máquina: Dados los retos de nuestra fuerza de trabajo en ciberseguridad, es urgente mejorar las interfaces hombre-máquina. La relación entre las tecnologías operativas (por ejemplo, los componentes SCADA) y sus operadores fue de interés particular. La automatización ofrece potencialmente numerosas ventajas de seguridad, pero los operadores necesitarán una mayor transparencia en los algoritmos antes de confiar decisiones de la máquina.

Los usuarios domésticos suponen otro reto para la interfaz de la máquina. Ingeniería del comportamiento del usuario, en lugar de asumir cambios improbables, puede aumentar la eficacia de las tecnologías actuales.

- Aprendizaje automático/inteligencia artificial (IA): Las técnicas de aprendizaje automático e IA pueden ofrecen nuevas vías para la detección precoz y la adaptación a las tensiones, incluidas las distribuidas amenazas. Investigación adicional en la toma de decisiones por parte de máquinas, modelización de escenarios hipotéticos, y el uso de big data (de los sensores de la red y del sistema) para establecer líneas de base normales podría contribuir a la resiliencia del ecosistema.

- Atribución: La atribución de los incidentes de seguridad informática es problemática, y podría decirse que más difícil para las redes de bots y las amenazas distribuidas. La identificación del actor malicioso y la sistemas comprometidos contribuiría positivamente a la mitigación durante los ataques, y permitir acciones policiales que puedan disuadir a los actores posteriores.

- Pruebas de eficacia: Al igual que con otros aspectos de la seguridad informática, las pruebas de que las herramientas y la eficacia de las técnicas es necesaria para justificar la continuidad de las inversiones.

- Remediación: Después de detectar el compromiso, los usuarios a menudo se enfrentan a opciones desagradables: intentar limpiar el sistema; o desechar el dispositivo. La limpieza del sistema suele ser poco fiables; los procesos de reparación pueden ser complejos, y las amenazas persistentes avanzadas (APT) están diseñados para sobrevivir a la remediación. Descartar los dispositivos es caro y poco práctico en la mayoría de los escenarios. Investigación que hace que la reparación sea más sencilla y fiable para los usuarios aclararía estas opciones y aumentaría la resistencia tras un compromiso detectado.

- Diseño de redes para la resiliencia: El diseño de las redes puede influir en la resiliencia y limitar opciones de mecanismos anti-DDoS. Investigación sobre el diseño de la red para maximizar de resiliencia y preservar las opciones es necesario.

- Gran parte de la investigación reciente sobre la resistencia de la red se ha centrado en aumentar la visibilidad de redes de borde, pero pueden existir oportunidades para aprovechar los nuevos sensores y hacer que Internet "más inteligente" en su núcleo. Para hacer posible estas arquitecturas de próxima generación, es necesario investigar que identifica los tipos de sensores, dónde ubicarlos, qué información debe ser compartido, y con quién.

Los participantes también señalaron varios impedimentos a los esfuerzos centrados en la investigación para mejorar la resiliencia de la red, incluyendo:

- Educación y concienciación: Se introduce la física, la química y otros campos científicos mucho antes en el sistema educativo de Estados Unidos que la informática en general y ciberseguridad en particular. La exposición tardía al campo limita el interés, ya que muchos estudiantes han identificado un campo de estudio antes de ir a la universidad. Atraer a más de los mejores y más brillantes tendría probablemente un efecto dominó en cuanto a la propiedad intelectual agregada.

- Falta de recursos monetarios: Los presupuestos para la investigación se están reduciendo tanto en el sector público como en el privado sectores privados. La Fundación Nacional de la Ciencia financia una parte importante de tanto la investigación básica como la aplicada en este campo, pero el total de dólares disponibles es insuficiente para financiar todos los esfuerzos de investigación prometedores.

Gobierno y políticas públicas

El segundo panel del día 2 abordó las opciones de los gobiernos y de las políticas públicas para mejorar la resiliencia del ecosistema. El tema también se abordó, junto con las direcciones de investigación, como parte del Sesión de trabajo del segundo día por la mañana.

Al igual que en otros sectores, los participantes señalaron que muchas de las actividades en curso en el gobierno y políticas públicas ya están en marcha para mejorar la resiliencia del ecosistema, entre ellas:

- Acciones policiales: Los organismos encargados de la aplicación de la ley a todos los niveles están persiguiendo más delitos relacionados con la ciberseguridad, incluidos los que implican amenazas distribuidas de forma automatizada. En particular, los participantes señalaron que la Oficina Federal de Investigación ha retirado un número de botnets de alto perfil en los últimos años. Estos éxitos proporcionan una base para futuros casos y crear una medida de disuasión.

- Aplicación de la normativa: Los organismos reguladores están elaborando y aplicando políticas para ciberseguridad dentro de su ámbito tradicional. Por ejemplo, la Food and Drug, la Administración ha establecido unas directrices para los productos sanitarios que desvinculan la actualizaciones de seguridad de los regímenes de certificación de productos existentes, y la Comisión Federal de Comercio (FTC) ha tomado medidas en numerosos casos relacionados con la privacidad y la seguridad. IoT los dispositivos han figurado en algunas de estas acciones de aplicación.

- Iniciativas políticas: Los problemas de privacidad y seguridad de los datos de los dispositivos IoT han sido el centro de iniciativas políticas en varios departamentos y agencias. La serie de talleres sobre el IoT de la FTC centrada en dispositivos específicos de la IO (por ejemplo, drones, televisores inteligentes) y la FTC pública el concurso "IoT Home Inspector Challenge" fueron dos ejemplos destacados de una larga lista de actividades.

- Educación y concienciación: El gobierno federal se esfuerza por colmar las lagunas educativas a escala nacional a través de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE), que incluye muchas agencias gubernamentales. Las agencias reguladoras son independientes realizar actividades educativas complementarias, como la publicación de guías y blogs puestos, que se dirigen a sus grupos de interés.

- Coordinación y colaboración internacional: Otros gobiernos también están respondiendo a automatizadas distribuidas al ecosistema, y están llegando a sus socios y aliados para coordinar e intercambiar información.

Al igual que en otros sectores, estos esfuerzos son significativos, pero se necesita más para mitigar la evolución amenaza. Los participantes identificaron varios vectores diferentes para que el gobierno afecte a la resiliencia de la red, incluyendo:

- Adquisiciones: Aunque se reconoce que el poder adquisitivo del gobierno federal ya no es la fuerza dominante en el mercado de la tecnología de la información, los participantes alentaron de los gobiernos para utilizar el poder de la bolsa en concierto con una técnica bien especificada de los requisitos como un paso hacia los objetivos clave y para liderar el sector privado. Por ejemplo, al exigir a los proveedores que apoyen las actualizaciones de seguridad automáticas, el gobierno podría aumentar la resistencia de los componentes del ecosistema de propiedad y gestión federal y ampliar la gama de opciones disponibles para las entidades del sector privado centradas en la seguridad.

- Investigación básica: Los participantes señalaron que el gobierno federal sigue siendo el principal fuente de financiación de la investigación básica en la mayoría de las disciplinas científicas. La industria es comprensiblemente, se centran en la fase posterior de la I+D, por lo que el gobierno federal debe garantizar que la financiación es suficiente y está bien orientada.

- Cooperación y coordinación internacional: Como se ha señalado anteriormente, el ecosistema es global, y combatir eficazmente las amenazas distribuidas requerirá la cooperación de y coordinación con proveedores de servicios, fabricantes y usuarios empresariales no estadounidenses. En algunos casos, estas entidades están estrechamente vinculadas a los Estados nacionales. El gobierno federal es de la cooperación y la coordinación con estos organismos entidades.

- Aplicación de la ley: Los esfuerzos de las fuerzas de seguridad para desmantelar las redes de bots y mitigar estas las amenazas tuvieron un amplio apoyo entre los participantes. Un apoyo prudente a la revisión y se expresó la necesidad de revisar las políticas que impiden el enjuiciamiento, con la advertencia de que las revisions debe equilibrar las preocupaciones de aplicación de la ley con los derechos de privacidad y propiedad.

- Creación de incentivos de mercado: Varios participantes identificaron el proyecto de document comunicar la capacidad de actualización de la seguridad de los dispositivos IoT para mejorar la transparencia de consumidores, desarrollado a través del proceso de múltiples partes interesadas de la NTIA sobre la Internet de los objetos actualizaciones y parches de seguridad, como ejemplo que podría crear incentivos de mercado para las mejoras de seguridad. [11]

- Regulación e incentivos de mercado: Los participantes prefirieron los incentivos de mercado a los amplios iniciativas reguladoras, pero expresó cierto pesimismo ante los fallos del mercado en el pasado. los participantes señalaron que las nuevas normativas centradas en la ciberseguridad en los sectores podrían ser apropiados y tener un impacto positivo si se consideran cuidadosamente. Médico de la industria, y las recientes declaraciones de la FDA en relación con los parches se citaron como ejemplo de regulación reflexiva y equilibrada. los reglamentos también podrían tener un impacto positivo al aclarar las responsabilidades y la rendición de cuentas en diferentes etapas del ciclo de vida del producto o del proceso de respuesta a incidentes.

    - Se sugirió que siguiendo un modelo como el utilizado por la Internacional Unión de Telecomunicaciones - Sector de Radiocomunicaciones (UIT-R) para la gestión del espectro radioeléctrico internacionalmente podría ser un buen enfoque para establecer cómo cooperar en ciberespacio a nivel internacional.

[11] Para el proyecto de documento, véase https://www.ntia.doc.gov/files/ntia/publications/draft_communicating_iot_security_update_capability_-_jul_14_2017_-ntia_multistakeholder_process.pdf. Para más información sobre el esfuerzo de la NTIA en materia de IoT, véase https://www.ntia.doc.gov/category/internet-cosas.

- Educación y concienciación: Ya hay muchas orientaciones sobre ciberseguridad defensiva disponibles y no se conocen o se ignoran. Tal vez habría que hacer más hincapié en conseguir una aplicación más generalizada de las protecciones básicas.

    - Si vamos a confiar en los consumidores para que se encarguen de la ciberseguridad, tenemos que facilitar y proporcionar más educación, mucho antes de lo que se imparte actualmente, en modelos para ayudar a la gente a entender la ciberseguridad.

- Agilizar la remediación: Tal vez el Gobierno pueda hacer más para facilitar la remediación después de una brecha. ¿Pueden los ciudadanos obtener ayuda para recuperarse de las violaciones, como por ejemplo, hacer que más fácil notificar a las personas y organizaciones que se están estableciendo nuevas cuentas y las antiguas las cuentas son nulas.

- Establecer orientaciones: Los participantes sugirieron que el gobierno federal en general, y el NIST en particular, podrían ayudar a la industria mediante orientaciones adicionales para apoyar acción voluntaria. Varios participantes citaron el proceso que el NIST utilizó para desarrollar la Marco para mejorar la ciberseguridad de las infraestructuras críticas (Cybersecurity Framework) como modelo de construcción de consenso hacia una orientación útil y aceptada. Los participantes sugirieron explícitamente ampliar el Marco de Ciberseguridad para abordar IoT. [12]

- Predicar con el ejemplo: Los participantes señalaron que relativamente pocos dispositivos de las recientes redes de bots eran localizados en los Estados Unidos, validando los enfoques de seguridad nacionales. Esta historia de éxito es en gran parte se pasa por alto y no se reproduce. Crear incentivos para que los que están fuera de los EE.UU. tomen medidas de seguridad, debemos demostrar nuestro éxito y luego publicitarlo a nivel internacional, compartiendo nuestra solución. Gracias a este éxito, nosotros, como comunidad, pudimos convencer al personas para actuar y tomar decisiones de gasto en ciberseguridad.

- Incentivar las acciones no comerciales: Desde el punto de vista de los proveedores de servicios de Internet, hay costes asociados con ciertas tareas que aumentan la resistencia de la red pero que no benefician directamente el cliente o el ISP. (La puesta en cuarentena y la notificación a los clientes se citó como una ejemplo). El gobierno podría incentivar estas acciones no comerciales proporcionando financiación o que permita a las empresas recuperar los costes.

[12] La ampliación del MCA a la IO implicaría muy probablemente el desarrollo de un perfil del sector de la IO, muy parecido al esfuerzo del CSRIC IV para la sector de las comunicaciones. Véase CSRIC IV, Cybersecurity Risk Management and Best Practices, Informe Final, WG 4 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

4. Conclusiones e implicaciones

La Orden Ejecutiva 13800 ordenó a los Departamentos de Comercio y Seguridad Nacional que presentar un informe al Presidente que "identificará y promoverá la acción de los partes interesadas para mejorar la resistencia del ecosistema de Internet y las comunicaciones y para fomentar la colaboración con el objetivo de reducir drásticamente las amenazas perpetradas por los y ataques distribuidos (por ejemplo, botnets)".

El taller proporcionó una aportación fundamental que, junto con la solicitud de comentarios de la NTIA y el informe del NSTAC servirá de base para la elaboración del proyecto de informe. Implicaciones para el mes de enero
informe incluyen:

- Las acciones propuestas en el informe abordarán cada uno de los temas generales extraídos de participantes en el taller.

- El informe recomendará una o más acciones propuestas para cada una de las partes interesadas grupos (es decir, proveedores de infraestructuras, desarrolladores de productos, empresas, usuarios domésticos, académico y gubernamental).

- Las partes interesadas no gubernamentales esperan que el gobierno federal predique con el ejemplo y promover las acciones de otras partes interesadas a través de incentivos en lugar de la regulación.
- Muchas acciones dependerán de acciones asignadas a otras partes interesadas, por lo que los mecanismos de colaboración tendrán que ser identificados también en el informe.

- Las recomendaciones incluirán probablemente acciones inmediatas para aumentar la concienciación y despliegue de las tecnologías actualmente disponibles, las acciones a medio plazo para crear un mercado incentivos (especialmente para asegurar el ciclo de vida completo del producto) y promover la coordinación y colaboración, y acciones a largo plazo para desarrollar nuevas tecnologías.

5. Próximos pasos y oportunidades de

Paralelamente a la publicación de este informe, la NTIA publicará un resumen de las declaraciones presentado en respuesta a la solicitud de comentarios de junio de 2017. [13] Comercio e Interior Seguridad comenzará a elaborar el informe basándose en los comentarios del público a y se incorporarán las aportaciones adicionales que se reciban. Paralelamente, el NSTAC seguirá trabajando en su informe para su publicación el 31 de octubre de 2017.

Se agradecen otras contribuciones públicas sobre este tema, que pueden enviarse a distributed.threats@nist.gov. Los comentarios enviados antes del 15 de octubre de 2017 se tendrán en cuenta para inclusión en el informe preliminar, que se compartirá con la comunidad en o antes de 5 de enero de 2018.

Las contribuciones y comentarios públicos sobre el informe preliminar se aceptarán hasta febrero 5, 2018. Una vez cerrado el periodo de comentarios, se celebrará un taller público en febrero para discutir la resolución prevista de los comentarios. Sobre la base de los comentarios del público y los debates mantenidos en el taller, los Departamentos completarán el informe para presentarlo al Presidente el o antes del 11 de mayo de 2018.

[13] Véase https://www.ntia.doc.gov/federal-register-notice/2017/report-responses-ntia-s-request-comentarios-que-promueven-la-acción-de-los-actores

A. Agenda

En las siguientes páginas se presenta el orden del día público del taller tal y como se publicó antes del mismo.
Hubo dos cambios en el orden del día "del día": Carlos Morales de Arbor Networks participó en el primer panel (Infraestructura de comunicaciones) en nombre de Arabella Harrington; y Craig Hyps, de Cisco, participó en el segundo panel (Productos) en lugar de Eric Wenger.

Mejora de la resistencia del ecosistema de Internet y las comunicaciones

Centro Nacional de Excelencia en Ciberseguridad del NIST, Rockville MD

11 y 12 de julio de 2017

Objetivo del taller**:** El objetivo de este taller es explorar una serie de temas actuales y emergentes soluciones para mejorar la resistencia de Internet frente a las amenazas distribuidas automatizadas, como botnets. El despliegue de estas soluciones dependerá de la capacidad y la voluntad de las distintas partes de tomar medidas. Dependiendo de la solución específica, los proveedores de infraestructura pueden requerir acciones, fabricantes de dispositivos, propietarios de sistemas y redes, comunidad investigadora, gobierno y/o desarrolladores de normas. Al explorar el espacio de soluciones con una amplia sección de participantes, el NIST espera identificar vías prometedoras para que todas las partes mejoren la resistencia de Internet.

Resultados del taller: El NIST elaborará un documento de actas del taller que resuma la sesión Los debates, las conclusiones y la identificación de oportunidades para los próximos pasos. Los resultados de este taller serán también sirven como aportación a las actividades de aplicación relacionadas con la Orden Ejecutiva 13800, *Fortalecimiento de la Ciberseguridad de las redes federales e infraestructuras críticas*.

Agenda Martes 11 de julio de 2017

7:30	**Registro de entrada**
8:30	**Bienvenida y resumen del taller**
8:45	**Preparando el escenario** *Esta sesión plenaria resumirá el espacio del problema (por ejemplo, el ecosistema de botnets), identificará las partes interesadas (desarrolladores de normas/protocolos, proveedores de infraestructuras, consumidores, fabricantes, reguladores) en la mitigación de botnets, y revisar los enfoques y resultados anteriores.*
9:30	**Perspectiva de los proveedores de infraestructuras: Normas actuales y emergentes, mejores prácticas, y tecnologías (panel 1)** *En esta sesión plenaria se analizarán los esfuerzos actuales y las oportunidades futuras para mejorar la resistencia de la infraestructura (por ejemplo, Internet). En este panel se debatirá el estado actual, tendencias y enfoques actuales y prometedores para mitigar las amenazas distribuidas automatizadas como el DDOS, con especial atención a las redes de bots y al IoT* **Russ Housley, Vigil Security (moderador)** **Richard Barnes, Cisco** **Arabella Hallawell, Arbor Networks** **Danny McPherson, VeriSign** **Ari Schwartz, Venable** **Brian Rexroad, AT&T**

10:15	**Romper**
10:30	**Sesión 1 Breakout (asignado)**
12:00	**Almuerzo**
1:00	**Desarrollo de productos (panel 2)** *En esta sesión plenaria se analizarán los esfuerzos actuales y las oportunidades futuras de la red fabricantes de componentes y dispositivos (incluidos los proveedores de soluciones de IoT) para abordar la raíz causas de las recientes redes de bots (acceso a la red sin restricciones, contraseñas codificadas y software). El ámbito de la sesión incluye tanto el uso empresarial como el doméstico.* **Yolonda Smith, Pwnie Express (moderadora)** **Anura S. Fernando, Underwriters Laboratory** **Jeff Greene, Symantec** **Rob Spiger, Microsoft** **Eric Wenger, Cisco**
1:45	**Sesión 2 Breakout (asignado)**
3:00	**Romper**
3:15	**Perspectiva del cliente: Enfoques actuales (Panel 3)** *En esta sesión plenaria se analizará cómo los usuarios de Internet, especialmente en la empresa, pueden protegerse y evitar ser parte del problema. Los panelistas comenzarán con una visión general de los retos a los que puede enfrentarse una empresa a causa de los ataques distribuidos, incluyendo DDoS, aplicaciones web y fraude. El debate destacará las capacidades y limitaciones de las mejores prácticas actuales y de las tecnologías emergentes, y el potencial de las colaboración.* **Nadya Bartol, Boston Consulting Group (moderadora)** **Steve Curren, Oficina del Subsecretario de Preparación y Respuesta del HHS** **Matt Eggers, Cámara de Comercio de Estados Unidos** **Bradley Nix, Director Adjunto de US-CERT en el NCCIC, DHS** **Spencer Wilcox, Exelon**
4:00	**Sesión 3 Breakout (asignado)**
5:00	**Levantar la sesión del día 1**

12 de julio de 2017

7:30	**Registro de entrada**
8:30	**Bienvenida y discurso de apertura**
8:45	**Direcciones de investigación** *Este panel identificará y explorará las áreas de brecha en los enfoques para mitigar las redes de bots, y destacar las oportunidades para abordar esas lagunas.* **Pat Muoio, Cybertech Consulting (moderador)** **David Dagon, Ga Tech** **Keith Marzullo, Univ. de MD** **Phil Reitinger, Global Cyber Alliance**
9:30	**El papel del Gobierno** *En esta sesión plenaria se debatirán los esfuerzos actuales y las oportunidades futuras de los gobiernos para mejorar la resistencia de la infraestructura, lo que puede incluir políticas y normativas enfoques, incentivos y motivadores del mercado, impactos económicos y consideraciones.* **Grace Koh, NEC (moderadora)** **Andi Arias, FTC** **Tom Grasso, FBI** **John Nicholson, Embajada del Reino Unido** **Malikah (Mikki) Smith, HHS/ONC**
10:15	**Romper**
10:30	**Grupos de investigación y papel del gobierno**
11:15	**Romper**
11:30	**Resumen de las sesiones de trabajo del primer día**
12:00	**Debate abierto**
12:30	**Cierre y próximos pasos (DOC/DHS)**
12:45	**Aplazar**