CSRIC III

Communications Security, Reliability and Interoperability Council

Marzo de 2012

Informe final

Código de Conducta Anti-Bot (ABC) de los Estados Unidos para los proveedores de servicios de Internet (ISP)

(Un código voluntario)

"Este Código de Conducta sería un gran paso adelante y un importante complemento a los esfuerzos más amplios de la Administración contra las botnets".

Presidente de la FCC Julius Genachowski 22 de febrero de 2012

GRUPO DE TRABAJO 7 - Remediación de botnets

Índice de contenidos

1 Resultados en resumen

1.1 Resumen ejecutivo

Un "bot" malicioso es un programa que se instala en un sistema para que éste realice automáticamente una tarea o conjunto de tareas, normalmente bajo el mando y control de un nefasto administrador remoto. El crecimiento de los dispositivos de usuario final infectados por bots1 representa una amenaza significativa para la vitalidad y resistencia de Internet y para la economía en línea.
Las redes de bots son redes de dispositivos informáticos de usuario final conectados a Internet e infectados con malware de bots, que son controlados a distancia por terceros con fines nefastos. Los bots y las redes de bots pueden dar lugar a robos de información personal, ataques contra redes públicas y privadas, y la explotación de la capacidad informática y el acceso a Internet de los usuarios finales.

El CSRIC III encargó al Grupo de Trabajo 7, Remediación de Botnets, que propusiera un conjunto de prácticas voluntarias consensuadas que constituyeran el marco de un modelo de implementación optativo que los ISP pudieran seguir para mitigar la amenaza de los botnets. En respuesta, se desarrolló el Código de Conducta Anti-Bot de Estados Unidos para los ISP con el fin de hacer frente a la amenaza de los bots y botnets en las redes de banda ancha residenciales a través de la participación voluntaria. Al desarrollar el Código se determinó que los componentes de todo el ecosistema de Internet tienen importantes funciones que desempeñar para hacer frente a la amenaza de los botnets y que los ISP dependen del apoyo de las demás partes del ecosistema.

El Código anima a los ISP a participar en actividades de apoyo a la educación de los usuarios finales para prevenir las infecciones de bots, la detección de bots, la notificación de posibles infecciones de bots, la reparación de bots y la colaboración y el intercambio de información de la participación en el Código. El Código se incluye en el Apéndice.

El Grupo de Trabajo propuso un conjunto de prácticas voluntarias acordadas que constituirían el marco de un modelo de aplicación opcional para que los ISP ayuden a hacer frente a la amenaza de las redes de bots. El Grupo de Trabajo recomienda acciones que los ISP que ofrecen acceso a Internet de banda ancha residencial pueden llevar a cabo si deciden adoptar el Código. El Grupo de Trabajo recomienda además que los ISP y otros proveedores de servicios indiquen su acuerdo para participar en el Código voluntario poniéndose en contacto con la organización de la industria que finalmente administre la participación en el Código. Inicialmente se sugiere que los ISP y otros proveedores de servicios participantes notifiquen a la entidad de su elección su participación en el código o se autoafirmen en su propio sitio web. El trabajo futuro que se ha identificado incluye la determinación de la administración a largo plazo de la participación en el Código, las actualizaciones periódicas del mismo, la identificación de las barreras a la participación en el Código, la definición de métricas y la identificación de las mejores prácticas y las lecciones aprendidas entre los participantes en el Código y los colaboradores del ecosistema de apoyo.

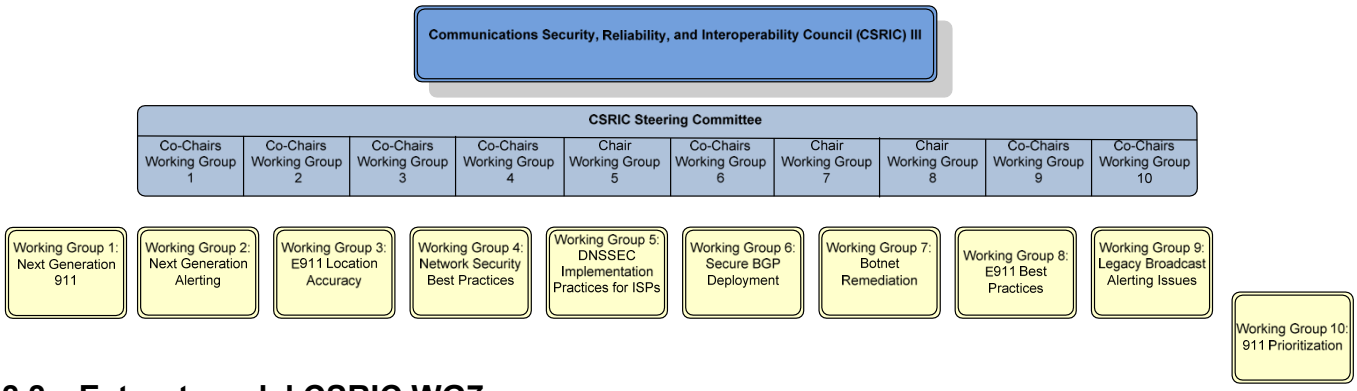
[1] En este documento se utilizan indistintamente los términos bot e infección bot.

2 Introducción

El CSRIC III creó el Grupo de Trabajo 7 (WG7) para abordar la reparación de botnets en las redes de banda ancha. El WG7 investigó los trabajos sobre remediación de bots que se están llevando a cabo en el IETF, Japón, Australia, Finlandia, Alemania y otros países para determinar el mejor enfoque para hacer frente a la amenaza de los bots en las redes de banda ancha de Estados Unidos.

El resultado de este trabajo es el Código de Conducta Anti-Bot de Estados Unidos para Proveedores de Servicios de Internet, de carácter voluntario, que puede encontrarse en el Apéndice.

2.1 Estructura del CSRIC



2.2 Estructura del CSRIC WG7

El WG7 está presidido por Michael O'Reirdan, Presidente del Grupo de Trabajo contra el Abuso de la Mensajería (MAAWG), y vicepresidido por el Dr. Peter Fonash, Director de Tecnología de la Oficina de Ciberseguridad y Comunicaciones del Departamento de Seguridad Nacional. Entre los miembros del WG7 se encuentran representantes de ISP, proveedores de software y equipos de red, del mundo académico, así como de otras organizaciones que forman parte del ecosistema de Internet.

2.3 Miembros del equipo del Grupo de Trabajo 7

El Grupo de Trabajo 7 está formado por los miembros que se indican a continuación.

Nombre	Empresa
Michael O'Reirdan - Presidente	MAAWG
Peter Fonash - Vicepresidente	Departamento de Seguridad Nacional
Neil Schwartzman - Secretario	CAUCE
Robert Thornberry - Editor	Bell Labs, Alcatel-Lucent
Paul Diamond - Editor	CenturyLink
Vernon Mosley - Enlace	FCC
Alex Bobotek	AT&T
Adam O'Donnell	Sourcefire
Alfred Huger	Sourcefire
Barry Greene	ISC
Bill McInnis	IID
Bill Smith	PayPal
Brian Done	Departamento de Seguridad Nacional
Chris Roosenraad	Time Warner Cable
Chris Sills	IID
Craig Spiezle	Alianza para la Confianza en Línea (OTA)
Daniel Bright	EMC
Eric Osterweil	Verisign
Gabe Iovino	REN-ISAC
Greg Holzapfel	Sprint
Gunter Ollmann	Damballa
James Holgerson	Sprint
Jay Opperman	Comcast
Joe St Sauver	Universidad de Oregón e Internet2
Johannes Ullrich	Instituto SANS
John Denning	Banco de América
John Griffin	Sistemas de Telecomunicación Inc.
John St. Clair	Verizon
Jon Boyens	Instituto Nacional de Normas y Tecnología
Kevin Sullivan	Microsoft
Kurian Jacob	FCC
Matt Carothers	Cox
Maxim Weinstein	StopBadware
Merike Kaeo	ISC
Michael Fiumano	Sprint
Michael Glenn	CenturyLink
Robert Mayer	USTelecom
Tice Morgan	T-Mobile
Tim Rohrbaugh	Intersecciones
Timothy Vogel	Verizon

Cuadro 1 - Lista de miembros del Grupo de Trabajo 7

3 Objetivo, alcance y metodología

2.3 Objetivo

El CSRIC encargó al Grupo de Trabajo 7, Remediación de Botnets, que propusiera un conjunto de prácticas voluntarias acordadas que constituyeran el marco de un modelo de aplicación opcional para que los ISP lo siguieran con el fin de mitigar la amenaza de los botnets. En respuesta, se desarrolló el Código de Conducta Anti-Bot de Estados Unidos para los ISP con el fin de hacer frente a la amenaza de los bots y botnets en las redes de banda ancha residenciales a través de la participación voluntaria.

2.4 Alcance

Esta sección identifica el planteamiento del problema, la descripción del grupo de trabajo y los resultados previstos en la carta del CSRIC III para el Grupo de Trabajo 7.

Planteamiento del problema: El crecimiento de los dispositivos de usuario final infectados por bots2 representa una amenaza significativa para la vitalidad y resistencia de Internet y para la economía en línea. Las redes de bots son redes de dispositivos informáticos de usuario final conectados a Internet e infectados con malware de bots, que son controlados a distancia por terceros con fines nefastos. Los bots y las redes de bots pueden dar lugar al robo de información personal, a ataques contra las redes públicas y privadas, y a la explotación de la capacidad informática de los usuarios finales y del acceso a Internet.

Con el fin de reducir las infecciones de bots en los dispositivos de los usuarios finales residenciales y mitigar la posible explotación de los bots, los miembros del Grupo de Trabajo 7 elaboraron el Código de Conducta Anti-Bot de Estados Unidos, de carácter voluntario, para los ISP.

Grupo de Trabajo 7 Descripción: Este Grupo de Trabajo revisará los esfuerzos realizados dentro de la comunidad internacional, como el Código de Prácticas de la Industria de Internet de Australia, y entre los grupos de partes interesadas nacionales, como el IETF y el Grupo de Trabajo Anti-Abuso de la Mensajería, para su aplicabilidad a los ISP de Estados Unidos. Basándose en el trabajo del Grupo de Trabajo 8 del CSRIC II sobre prácticas de protección de redes de ISP, el Grupo de Trabajo sobre Remediación de Botnets propondrá un conjunto de prácticas voluntarias acordadas que constituirían el marco para un modelo de implementación opcional para los ISP. El Grupo de Trabajo propondrá un método para que los ISP expresen su intención de optar por el marco propuesto por el Grupo de Trabajo. El Grupo de Trabajo también identificará las posibles barreras de implementación de los ISP al nuevo Código redactado e identificará los pasos que la FCC puede tomar para ayudar a superar estas barreras. Por último, el Grupo de Trabajo identificará métricas de rendimiento para evaluar la eficacia del Código a la hora de frenar la propagación de infecciones por bots.

[2] En este documento se utilizan indistintamente los términos bot e infección bot.

Resultados del informe:

1. Código de Conducta Anti-Bot de Estados Unidos para los ISP: 22 de marzo de 2012
2. Barreras para la participación en el código: 12 de septiembre de 2012
3. Métricas de rendimiento de la remediación de bots: 5 de diciembre de 2012

Este informe, el Código de Conducta Anti-Bot de Estados Unidos para los proveedores de servicios de Internet, es el primero de los tres informes que se entregarán al Grupo de Trabajo 7.

2.5 Metodología

El Grupo de Trabajo 7 comenzó su investigación sobre el desarrollo de un Código de Conducta Anti-Bot voluntario para los ISP de EE.UU. reuniendo a un equipo de expertos de la industria, el gobierno y el mundo académico, que representan a diversas partes interesadas en el desarrollo y la aplicación del Código. El Grupo de Trabajo 7 revisó los esfuerzos realizados dentro de la comunidad internacional, incluyendo el Código de Prácticas de la Industria de Internet de Australia y el Centro Cibernético Limpio de Japón, y entre los grupos de partes interesadas nacionales, incluyendo el Grupo de Trabajo de Ingeniería de Internet (IETF) y el Grupo de Trabajo Anti-Abuso de Mensajería, para su aplicabilidad a los ISP de Estados Unidos. Basándose en el trabajo del Grupo de Trabajo 8 del CSRIC II, Prácticas de Protección de la Red de los ISP, el Grupo de Trabajo 7 del CSRIC III estableció conferencias telefónicas quincenales entre sus miembros para debatir el desarrollo, el contenido y la relevancia de los esfuerzos relacionados con el establecimiento de un Código de Conducta Anti-Bot de Estados Unidos para los ISP. El Grupo de Trabajo 7 coordinó sus esfuerzos de desarrollo del Código con el Departamento de Comercio y el Personal de Seguridad Nacional de la Casa Blanca a través de conferencias telefónicas periódicas para discutir áreas de interés mutuo en materia de remediación de botnets. El Grupo de Trabajo 7 celebró dos reuniones presenciales con sus miembros, una en noviembre de 2011 para desarrollar la estructura y discutir el contenido de las secciones del proyecto de Código, y una última reunión presencial en febrero de 2012 para revisar el proyecto de Código definitivo. El Código de Conducta Anti-Bot de Estados Unidos resultante para los ISP se basa en las aportaciones colectivas de los miembros del Grupo de Trabajo 7, y en los debates que dichos miembros y sus empresas han mantenido con otras partes interesadas en la reducción de la incidencia de las infecciones bot.

3 Antecedentes3

Un "bot" malicioso o potencialmente malicioso se refiere a un programa que se instala en un sistema con el fin de permitir que ese sistema realice automáticamente (o de forma semiautomática) una tarea o conjunto de tareas normalmente bajo el mando y control de un nefasto administrador remoto, o "bot master". Los bots también se conocen como "zombis". Dichos bots pueden haber sido instalados subrepticiamente, sin que el usuario entienda lo que el bot hará una vez instalado, sin saberlo como parte de otra instalación de software, bajo falsos pretextos, o de una variedad de otras formas posibles.

Los dispositivos utilizados por los usuarios de Internet pueden estar infectados con programas maliciosos que pueden contener o instalar uno o más bots en un dispositivo. Pueden representar un problema importante por varias razones. En primer lugar, estos bots pueden utilizarse para enviar spam, en algunos casos volúmenes muy grandes de spam. Este spam puede suponer un coste adicional para los ISP en términos de desperdicio de recursos de red, servidores o personal, entre otros.

[3] Véanse las recomendaciones para remediar los bots en las redes de los ISP, http://tools.ietf.org/rfc/rfc6561.txt

muchos otros costes y efectos secundarios potenciales. Este tipo de spam también puede afectar negativamente a la reputación del ISP, a sus clientes y a la reputación del correo electrónico del espacio de direcciones IP utilizado por el ISP (a menudo denominado simplemente "reputación IP").

Además, estos bots pueden actuar como plataformas para dirigir, participar o realizar ataques a infraestructuras críticas de Internet. Los bots se utilizan con frecuencia como parte de ataques coordinados de denegación de servicio distribuido (DDoS) por motivos criminales, políticos o de otro tipo.

El papel de los ISP en la prestación de servicios a los usuarios de Internet, coloca a los ISP en posición de poder intentar detectar y observar las redes de bots que operan en sus redes. Además, los ISP también pueden estar en condiciones de notificar a sus clientes la infección real, potencial o probable de los bots.

Desde el punto de vista de los usuarios finales, recibir una notificación de que pueden tener un dispositivo infectado en su red proporciona información importante. Una vez que lo saben, pueden tomar medidas para eliminar los bots, resolver cualquier problema que pueda derivarse de la infección por bots y protegerse contra futuras amenazas.

El Grupo de Trabajo 7 desarrolló el Código de Conducta Anti-Bot de Estados Unidos para los ISP con el fin de hacer frente a la amenaza de los bots y botnets, descrita anteriormente, en las redes de banda ancha residenciales. La adopción del Código por parte de los ISP es voluntaria. No es obligatoria.

4 Recomendaciones

4.1 Recomendaciones

El Grupo de Trabajo propuso un conjunto de prácticas voluntarias acordadas que constituirían el marco de un modelo de aplicación opcional para que los ISP ayuden a hacer frente a la amenaza de las redes de bots. El Grupo de Trabajo recomienda acciones que los ISP que ofrecen acceso a Internet de banda ancha residencial pueden llevar a cabo si deciden adoptar el Código. El Grupo de Trabajo recomienda, además, que los ISP y otros proveedores de servicios indiquen su acuerdo para participar en el Código voluntario poniéndose en contacto con la organización de la industria que en última instancia administra la participación en el Código. Al ser un Código de Conducta voluntario desarrollado por la industria y para la industria, el objetivo es que un foro neutral de la industria reciba y coteje los informes relativos a la participación en el Código.
Inicialmente, para indicar la participación, se sugiere que los PSI y otros proveedores de servicios participantes notifiquen a la entidad de su elección su participación en el Código o se autoafirmen en su propio sitio web.

5.1.1 Trabajo futuro

Este informe, el Código de Conducta Anti-Bot de los Estados Unidos para los ISP, es el primero de los tres informes que el Grupo de Trabajo 7 debe entregar. Aún queda por resolver la administración a largo plazo del Código y las actualizaciones periódicas. A continuación, el Grupo de Trabajo identificará los posibles obstáculos a la participación en el Código. Como último paso, el Grupo de Trabajo identificará posibles métricas de rendimiento para la reparación de bots.

Se recomienda trabajar en el futuro para abordar los mecanismos de entrega de infecciones de bots desde sitios web y servicios de alojamiento infectados y nefastos para que los esfuerzos del WG7 sean omnipresentes y, por tanto, eficaces.

5.1.2 Agradecimientos

El WG7 desea agradecer a Yurie Ito, del CERT de Japón, su presentación informativa y el debate sobre las lecciones aprendidas del Japan Cyber Clean Center, el programa anti-botnet de Japón. También agradecemos a Ari Schwartz del National Institute of Standards (NIST) su presentación sobre la amenaza de las botnets y las estrategias de mitigación. Además, el WG7 agradece a Microsoft, al MAAWG y a la FCC por acoger las reuniones presenciales del WG7.

El Grupo de Trabajo 7 desea agradecer especialmente a los siguientes miembros del grupo, cuyos esfuerzos incansables han contribuido enormemente al proceso de desarrollo del Código:

Robert Thornberry, de Bell Labs, Alcatel-Lucent (Editor) Paul
Diamond, CenturyLink (Editor)
Joe St Sauver, Universidad de Oregón e Internet2 (Glosario) Neil
Schwartzman, CAUCE (Secretario)

5 Conclusiones

En respuesta al encargo del CSRIC III al Grupo de Trabajo 7, se desarrolló el Código de Conducta Anti-Bot de Estados Unidos para los ISP, de carácter voluntario, con el fin de hacer frente a la amenaza de los bots y las botnets en las redes de banda ancha residenciales mediante la participación voluntaria. Al desarrollar el Código se determinó que los componentes de todo el ecosistema de Internet tienen importantes funciones que desempeñar para hacer frente a la amenaza de los botnets y que los ISP dependen del apoyo de las demás partes del ecosistema.

Este informe del 22 de marzo de 2012, el Código de Conducta Anti-Bot de Estados Unidos para los ISP, es el primero de los tres informes que entregará el Grupo de Trabajo 7. A continuación, el Grupo de Trabajo identificará los posibles obstáculos a la participación en el Código, con un informe que se publicará en septiembre de 2012. Como último paso, el Grupo de Trabajo identificará las métricas de rendimiento de la reparación de botnets y presentará su informe sobre este tema en diciembre de 2012.

6 Anexo

Código de Conducta Anti-Bot (ABC) para Proveedores de Servicios de Internet (ISP) que abordan la actividad de los bots en las redes de banda ancha
Final 22 de
marzo de 2012

1. Introducción

El crecimiento de los dispositivos de usuario final* *infectados por bots representa una amenaza significativa para la vitalidad y resistencia de Internet y para la economía en línea. Obsérvese que en este documento se utilizan los términos "infección por bot" y "bot" como sinónimos para referirse a un dispositivo de usuario final infectado por un malware bot.
Las redes de bots son redes de dispositivos informáticos de usuario final conectados a Internet e infectados con malware de bots*que son controlados a distancia por terceros con fines nefastos.

Los bots y las redes de bots pueden provocar el robo de información personal, ataques contra redes públicas y privadas y la explotación de la capacidad *informática y el acceso a Internet de los usuarios finales. La conciencia pública sobre los bots, su impacto y los problemas de seguridad y privacidad resultantes es escasa. Este código de conducta voluntario ("Código") proporciona un conjunto de principios y actividades recomendadas que los proveedores de servicios de Internet pueden adoptar para ayudar a hacer frente a las amenazas presentadas por la presencia de bots y botnets en las redes residenciales de banda ancha.

Hay que reconocer que los bots afectan a todo el ecosistema de Internet *y que para reducirlos o mitigar su impacto será necesaria la acción colectiva de todas las partes de ese ecosistema, incluidos los usuarios finales, los desarrolladores de software, los proveedores de búsquedas, los sitios web, los sitios de comercio electrónico y otros. Los dispositivos de los usuarios finales están fuera del control de los proveedores de servicios de Internet, por *lo que todos los participantes en el ecosistema de Internet deben trabajar juntos para abordar este problema. Este Código pretende sentar las bases para una futura coordinación entre las distintas partes interesadas, definiendo un conjunto de acciones adecuadamente dirigidas al limitado papel que pueden desempeñar los PSI para ayudar a resolver esta importante cuestión.
El Código reconoce la sustancial variabilidad en el tamaño, los recursos, los modelos de negocio y los entornos, la experiencia y las capacidades de los ISP en Estados Unidos. El éxito de las actividades de los ISP depende de los esfuerzos similares de otras partes interesadas en Internet.

Los requisitos básicos para participar en este Código se exponen en la sección 5. Las demás secciones de este documento contienen información de fondo o material explicativo adicional.

---

* Definición encontrada en el Glosario

2. Definiciones de términos clave

Nota para el lector:

Cualquier discusión sobre bots implica inevitablemente un vocabulario técnico único. Reconociendo que muchos lectores pueden no estar familiarizados con algunos de esos términos especializados, el Código incluye un glosario como Apéndice 2. Cualquier término que aparezca en el glosario se marcará con un asterisco "*" en el cuerpo del texto del Código la primera vez que aparezca como forma de alertar al lector de que hay una definición disponible en el glosario.

3. Objetivos y principios

a. Los objetivos de este Código son:

1. Proporcionar un marco inicial para que los proveedores de servicios de Internet comprendan mejor y ayuden a abordar el problema de los bots; y

2. Animar a los ISP a

• Informar a los usuarios finales de la amenaza que suponen los bots y de las medidas que pueden tomar para ayudar a prevenir las infecciones por bots;

• Detectar actividades de bots u obtener información, incluso de terceros creíbles, sobre infecciones de bots entre su base de usuarios finales;

• Notificar a los usuarios finales las sospechas de infecciones por bots o ayudar a los usuarios finales a determinar si están potencialmente infectados por bots; y

• Proporcionar información y recursos, directamente o por referencia a otras fuentes, a los usuarios finales para ayudarles a remediar las infecciones por bots.

b. La aplicación del Código se guiará por los siguientes principios:

1. Voluntario - la participación es voluntaria y fomenta los tipos de acciones que deben tomar los ISP, sin embargo este Código no requiere ninguna actividad en particular.

2. Tecnología neutra: este Código no prescribe ningún medio o método en particular.

3. Neutralidad del enfoque: este Código no prescribe ningún enfoque particular para aplicar cualquier parte de este Código.

4. Respeto a la privacidad: los proveedores de servicios de Internet deben abordar las cuestiones relativas a la privacidad de forma adecuada y conforme a la legislación vigente.

5. Cumplimiento legal: las actividades deben cumplir con la legislación aplicable.

6. Responsabilidad compartida: los ISP, actuando solos, no pueden hacer frente por completo a la amenaza que suponen los bots. Otros participantes del ecosistema de Internet también deben hacer su parte.

7. Sostenibilidad - Los PSI deben buscar actividades que sean rentables y sostenibles en el contexto de sus modelos de negocio.

8. Intercambio de información - Los PSI deben indicar cómo participan en el Código y compartir las lecciones aprendidas de sus actividades con otras partes interesadas. Todo intercambio de información entre los PSI y otras partes implicadas debe realizarse de acuerdo con las leyes aplicables, incluyendo, pero sin limitarse a, las leyes antimonopolio y de privacidad.

9. Eficacia - Hay que animar a los PSI a realizar actividades que hayan demostrado ser adecuadas y eficaces.

10. Comunicación eficaz - La comunicación con los* clientes debe tener en cuenta diversas cuestiones, como el idioma, y asegurarse de que la información se proporciona de una manera que se espera razonablemente que sea entendida y accesible por los destinatarios.

4. Alcance y funciones

Este Código se ha redactado específicamente para los PSI y otros proveedores de servicios que ofrecen servicios de acceso a Internet de banda ancha a usuarios finales residenciales. Las actividades de este Código pueden ser adaptadas para su uso por otros proveedores y participantes de Internet.

Este Código no pretende ser un enfoque global de la seguridad en línea, sino que pretende coexistir con otros esfuerzos actuales y futuros. Prevé un papel importante para otros participantes en el ecosistema de Internet, entre otros:

- Proveedores de software de seguridad
- Desarrolladores de sistemas operativos
- Organizaciones centradas en el usuario final
- Proveedores de contenidos, aplicaciones y servicios de Internet

La seguridad en línea debe incluir un enfoque polifacético y flexible que utilice consejos y herramientas de diversas fuentes acreditadas.

a. Definición de éxito

El éxito inicial de este Código se evaluará en función de la participación de la comunidad de ISP. Sin embargo, el apoyo del ecosistema de Internet en general se considera primordial para el éxito final en la lucha contra los bots.

b. Beneficios de la participación en el Código

Los siguientes beneficios de alto nivel pueden resultar de la participación significativa de los PSI en este Código:

- Aumento de la seguridad de la información y los dispositivos de los usuarios finales y de las infraestructuras de Estados Unidos;

- Una mayor concienciación sobre la amenaza de los bots y cómo abordarla entre los usuarios finales, los ISP y otros participantes del sector relacionados con Internet;

---

* Definición encontrada en el Glosario

- Notificación* y corrección* de la actividad de los bots en los dispositivos de los usuarios finales infectados por bots;
- Creación de un entorno en las redes residenciales de banda ancha de EE.UU. aún más hostil al despliegue y utilización de bots; y
- Desarrollo y uso más amplio de arquitecturas y herramientas efectivas de notificación y remediación entre los usuarios finales y los ISP.

Algunos ISP que participan en el proceso de desarrollo del Código y que han aplicado previamente algunos aspectos del mismo han experimentado resultados beneficiosos en áreas tales como un menor volumen de llamadas a los servicios de asistencia por parte de los clientes con máquinas infectadas, una reducción del consumo de ancho de banda ascendente por ataques de denegación de servicio y spam*un aumento de la buena voluntad de los clientes y una menor rotación de los mismos, así como una reducción de las quejas relacionadas con el spam por parte de otros ISP. Aunque los resultados individuales pueden variar, se anima a los ISP a buscar formas específicas en las que la participación en el Código refuerce su negocio de banda ancha en general, y a compartir esas experiencias con otros ISP. Además, la participación de los ISP en este Código puede permitir a los ISP generar métricas tangibles relacionadas con el impacto de actividades específicas en las operaciones generales del negocio de banda ancha de los ISP, lo que a su vez puede apoyar el desarrollo o el despliegue de más actividades anti-bot.

* Definición encontrada en el Glosario

5. Parámetros de participación

La participación en este Código es voluntaria.

Requisitos de participación en el Código de Conducta Voluntario

Para participar en este Código, un PSI realizará al menos una actividad (es decir, emprenderá una acción significativa) en cada una de las siguientes áreas generales:

- Educación - una actividad destinada a ayudar a aumentar la educación y la concienciación de los usuarios finales sobre los problemas de las redes de bots y cómo ayudar a prevenir las infecciones de bots;
- Detección: actividad destinada a identificar la actividad de las redes de bots en la red del ISP, obtener información sobre la actividad de las redes de bots en la red del ISP o permitir a los usuarios finales determinar por sí mismos posibles infecciones de bots en sus dispositivos de usuario final;
- Notificación - una actividad destinada a notificar a los clientes de presuntas infecciones de bots o permitir a los clientes determinar si pueden estar infectados por un bot;
- Remediación - una actividad destinada a proporcionar información a los usuarios finales sobre cómo pueden remediar las infecciones de bots, o para ayudar a los usuarios finales a remediar las infecciones de bots.
- Colaboración - una actividad para compartir con otros PSI los comentarios y la experiencia aprendida de las actividades del Código de los PSI participantes.

El concepto de realizar "al menos una actividad" en cada una de estas áreas generales pretende fomentar cierto nivel de actividad en cada una de las cinco áreas señaladas anteriormente como parte de un proceso general a nivel nacional de creación de un entorno en las redes residenciales de banda ancha de Estados Unidos que sea aún más hostil al despliegue y la utilización de bots. Se pretende apoyar y fomentar una amplia gama de esfuerzos flexibles para experimentar e innovar con diversos métodos de educación, detección*detección, notificación y corrección. En esa misma línea, el requisito de compartir la información con otros ISP no pretende dictar ningún medio o método específico para compartir dicha información.

* Definición encontrada en el Glosario

6. Educación del usuario final

a. Resumen

Los usuarios finales son, en última instancia, los responsables de la protección de sus dispositivos y de remediar un dispositivo infectado. Los proveedores de servicios de Internet, al igual que muchos otros participantes de Internet y actores gubernamentales, pueden ayudar a educar a los usuarios finales sobre las amenazas que presentan los bots y los pasos que los usuarios finales pueden tomar para proteger sus dispositivos y remediar las infecciones.

b. Acción recomendada:

1. Educación sobre la prevención de bots*:

Los ISP deben poner a disposición de los usuarios información sobre la prevención de infecciones por bots y cuestiones relacionadas. Como mínimo, dicha información debería incluir:

- Cómo y por qué los usuarios finales deben mantener su software actualizado para ordenadores y dispositivos con actualizaciones de software fácilmente disponibles.
- La importancia de utilizar un software de seguridad eficaz y actual de un proveedor de confianza.
- La importancia de hacer copias de seguridad de los datos y el software de los usuarios y cómo hacerlo eficazmente.
- Acciones básicas del usuario final para minimizar la exposición a las infecciones de bots mientras usa Internet.

Se espera que muchos PSI puedan cumplir este objetivo proporcionando esta información directamente a sus abonados o enlazando con fuentes existentes y disponibles públicamente de dicha información.

2. Apoyo a los esfuerzos de remediación de los bots de los usuarios finales:

Junto con la información sobre la prevención, los ISP deberían poner a disposición (por ejemplo, a través de publicaciones de los ISP, publicaciones de terceros o enlaces web) información sobre cómo los usuarios finales pueden remediar en general las infecciones de bots. En este ámbito, se espera que los ISP puedan cumplir este objetivo enlazando con fuentes de información existentes y disponibles públicamente o creando nuevas fuentes de información, ya sea individualmente o en colaboración con otros.

En relación con las actividades de notificación a los usuarios finales de un ISP, los ISP deben incluir en dichos avisos o de otro modo, información sobre dónde puede acudir el destinatario para obtener información y asistencia adicional. Dicha información podría incluir enlaces a información en línea disponible públicamente, herramientas de seguridad o sugerencias para buscar ayuda de un profesional de la informática. Otros temas y referencias que un ISP podría incluir son:

---

* Definición encontrada en el Glosario

- Riesgos para el usuario final y la comunidad de Internet por el uso de un dispositivo que se cree que está infectado,
- Cómo identificar y eliminar las formas más comunes de infecciones por bots,
- Herramientas o servicios disponibles públicamente (gratuitos o de pago) para ayudar a la detección y eliminación de infecciones de bots, y
- Orientación sobre dónde encontrar asistencia adicional (gratuita o de pago).

3. Directrices:

Al abordar los requisitos anteriores, los PSI deben tener en cuenta estas directrices:

- Ofrecer información y recursos educativos directamente o mediante la remisión a servicios de terceros.
- Mantenga el contenido educativo conciso y centrado en las cosas más importantes que los usuarios necesitan saber.
- Garantizar que las instrucciones puedan ser seguidas por un público de usuarios no técnicos.
- Utilice múltiples medios, por ejemplo, imágenes, vídeos, texto, subtítulos, etc., y, cuando sea útil, varios idiomas para maximizar la comprensión y la accesibilidad del cliente.
- Ayudar a los usuarios finales a determinar si tienen una infección de bots proporcionando información o señalando recursos que describan comportamientos anómalos de los dispositivos infectados por bots y la disponibilidad y uso de herramientas o servicios de software de detección de bots.

7. Detección de bots

a. Resumen

A medida que los bots evolucionan, también deben hacerlo las herramientas y técnicas utilizadas para detectarlos. El reto de la detección radica en la versatilidad que ha alcanzado el tráfico de bots para evitar muchas técnicas singulares utilizadas para los mecanismos de detección, como la simple coincidencia de patrones. La detección puede complicarse por el hecho de que algunas aplicaciones de Internet, como las redes de distribución de contenidos con caché distribuida, las aplicaciones de juegos en línea y otros servicios de este tipo pueden mostrar un comportamiento similar al de los bots maliciosos, y pueden utilizar tecnologías similares. Los ISP deben tener cuidado al identificar a las partes afectadas para notificarlas y remediarlas.

b. Acción recomendada:

Los ISP pueden descubrir la actividad maliciosa y los dispositivos de usuario final comprometidos por bots de varias maneras:

1. Recibir notificaciones de entidades externas, en particular las destinadas a ayudar a la comprensión general y a la difusión en tiempo real de los datos relacionados con los robots. En el Apéndice 2 se incluye una lista de recursos.

2. Desplegar capacidades dentro de sus redes que ayuden a identificar posibles infecciones de bots.

3. Dirigir a los clientes a herramientas, un portal web u otros recursos que permitan a los clientes autoidentificar una posible infección por bots.

8. Notificación al usuario final de una posible infección de bots

a. Resumen:

Muchos usuarios finales no son conscientes de que sus dispositivos están infectados y funcionan como bots. Como resultado, esos usuarios y sus datos permanecen en riesgo, y los bots pueden permanecer activos indefinidamente. Los ISP deben aprovechar los esfuerzos de detección descritos en la sección 7 para que los clientes sean conscientes de las infecciones activas.

Las notificaciones deben estar diseñadas para ayudar a mitigar los bots y el daño que causan. Las notificaciones pueden incluir información sobre lo que es un bot, los medios de infección, que los bots pueden no tener síntomas visibles y el significado de la notificación. Las notificaciones también pueden contener o identificar otros recursos como herramientas, guías y servicios que faciliten la prevención, verificación y mitigación de la infección*. También pueden proporcionar información sobre cualquier bot específico detectado.

La notificación al usuario final puede adoptar diferentes formas. Puede ser realizada directamente por el ISP o por terceros en nombre del ISP. Los ISP pueden alertar directamente a los usuarios finales o proporcionar mecanismos que permitan a los usuarios finales solicitar y recibir información sobre su estado de infección. Del mismo modo, los PSI pueden llegar a acuerdos que permitan que las notificaciones sean enviadas a los usuarios finales por otros participantes del ecosistema con los que el usuario final tenga una relación, como un proveedor de una aplicación o servicio de Internet.

El ISP debe considerar mecanismos que garanticen que el cliente pueda autenticar fácilmente las notificaciones como auténticas y que dichas notificaciones sean difíciles de falsificar.

Cuando sea posible, el ISP puede querer hacer un seguimiento de la recepción de las notificaciones. Esto puede ayudar al ISP a comprender mejor la eficacia de los distintos mecanismos de notificación.

Cada ISP tendrá que evaluar diferentes métodos de notificación para encontrar el más adecuado para el ISP en particular y la amenaza bot concreta. El método de notificación elegido puede tener que integrarse con los procesos empresariales existentes y con la red existente

* Definición encontrada en el Glosario

infraestructura. Puede ser necesario investigar y analizar para desarrollar y mantener sistemas y políticas de notificación adecuados.

b. Acción recomendada:

Comunicar al cliente la sospecha de infección por bots o ayudar a los clientes a determinar si están potencialmente infectados por bots. Muchos de los métodos de notificación se describen en las referencias del Apéndice 2; sin embargo, se pueden utilizar otros métodos.

9. Remediación de bots

a. Resumen

La mitigación y reparación de bots es el objetivo final de cualquier programa de notificación de infecciones de bots y es, en última instancia, responsabilidad del usuario final. La notificación por sí sola puede ser suficiente para los usuarios técnicos, pero la mayoría de los usuarios suelen necesitar algún tipo de ayuda para eliminar el malware bot de sus dispositivos infectados. Sin embargo, la remediación puede ser difícil y puede implicar otras funciones complejas, como aislar el origen de la infección entre muchos dispositivos que comparten una conexión a Internet; hacer una copia de seguridad de todos los datos y del software del sistema con antelación, de manera que se preserve la capacidad de recuperación de los usuarios finales (pero sin hacer también una copia de seguridad de los archivos o programas infectados); y asegurarse de que el usuario final tenga discos de origen y otros materiales a partir de los cuales reconstruir la imagen de su dispositivo si es necesario durante el proceso de remediación.

Se entiende que algunos ISP pueden no tener los recursos para proporcionar este nivel de servicio, ni ser capaces de apoyar tales actividades de forma gratuita o incluso por una tarifa. En muchos casos, los usuarios finales pueden necesitar ser remitidos a proveedores de servicios profesionales de soporte informático para remediar completamente sus máquinas. Las notificaciones de los ISP pueden anticiparse a este hecho y sugerir a los clientes que busquen la ayuda de terceros para evitar frustrar a los usuarios finales con servicios de asistencia limitados o líneas de apoyo que no son capaces o no están equipadas para abordar plenamente los problemas de reparación.

b. Acción recomendada:

1. Los bots están diseñados para ser sigilosos y difíciles de eliminar. Como parte de la notificación, los proveedores de servicios de Internet deben ofrecer orientación, como se ha descrito anteriormente. Esto puede incluir enlaces a una variedad de fuentes de información, software y herramientas disponibles en línea y de terceros. También puede incluir enlaces a servicios profesionales. No es necesario que sean ofrecidos por el propio ISP, sino que pueden ser ofrecidos por terceros.

2. Un ISP puede proporcionar herramientas de corrección al usuario final, ya sea durante o después del proceso de notificación. Sin embargo, el ISP no debe obligar al usuario final a ejecutar las herramientas de corrección. Si el ISP proporciona herramientas al usuario final, éste debe poder salir del proceso sin ejecutar ninguna de las herramientas o procedimientos sugeridos.

3. Como parte del proceso de notificación, los proveedores de servicios de Internet pueden incluir una guía (dependiendo de la naturaleza del bot en cuestión) que indique que los ajustes en los equipos de red propiedad del cliente, como las puertas de enlace y los routers domésticos, pueden tener

ha sido alterado y debe ser restaurado a un estado seguro, dependiendo de la naturaleza de la infección del bot.

c. Directrices:

1. Las herramientas y servicios de eliminación de bots deben respetar la privacidad del usuario.

2. Los posibles métodos de remediación de la infección se describen en las mejores prácticas del CSRIC II WG 8 y en la RFC del IETF sobre remediación de bots a la que se hace referencia en el Apéndice 2.

10. Colaboración con el ISP

a. Resumen:

La mitigación y la gestión de los bots son actividades en las que intervienen los ISP, los proveedores de búsquedas, los usuarios finales, los departamentos de TI, las empresas de alojamiento, los proveedores de blogs, los vendedores de seguridad, los investigadores, el gobierno, las empresas de servicios financieros, los proveedores de servicios en la nube y otras partes. Con las aportaciones y la colaboración de las múltiples partes interesadas, los resultados superarán a los posibles con acciones independientes por sí solas. Cabe esperar que la participación de los ISP en este código, junto con los enfoques complementarios y de colaboración adoptados por otros segmentos del ecosistema de Internet, impulse una mitigación sustancial de la amenaza que suponen las redes de bots.

b. Acción recomendada:

La participación en el código requiere la colaboración en el seno de los PSI, de la industria o de foros más amplios a través de actividades de colaboración, de las cuales las siguientes son ejemplos:

1. Compartir los métodos de detección, notificación o mitigación previstos o desplegados en las redes de los proveedores de servicios de Internet y, en su caso, una evaluación de su eficacia.

2. Compartir datos de inteligencia o de ataques operativos que puedan ser útiles para la prevención, defensa o reparación de bots.

3. Identificación de datos clave o recursos técnicos que se necesitan de sistemas o actores más allá de la red del ISP.

4. Participación en la definición, el desarrollo o el funcionamiento de estrategias o sistemas de defensa integrados que se extienden más allá de los límites de la red ISP.

5. Otras actividades de colaboración que impliquen compartir información con partes ajenas al ISP o datos con sistemas ajenos a la red del ISP.

Todo intercambio de información entre los proveedores de servicios de Internet y otras partes implicadas se realizará de acuerdo con la legislación aplicable, incluidas, entre otras, las leyes antimonopolio y de privacidad.

11. Desarrollo posterior de este Código

Este Código evolucionará con el tiempo debido a la naturaleza dinámica de la amenaza de los bots y a la experiencia y evaluación de los ISP.

12. Información y recursos adicionales

Apéndice 1 - Glosario Apéndice 2
- Referencias

Apéndice 1 - Glosario:

1. Bot

La siguiente definición se basa en gran medida en las "Recomendaciones para la reparación de bots en las redes de los ISP" (referenciadas en el Apéndice 2):

Un "bot" malicioso (o potencialmente malicioso) (derivado de la palabra "robot", en lo sucesivo denominado simplemente "bot") se refiere a un programa que se instala en un sistema con el fin de permitir que ese sistema realice automáticamente (o de forma semiautomática) una tarea o conjunto de tareas normalmente bajo el mando y control de un administrador remoto (a menudo denominado "bot master" o "bot herder").

Los sistemas informáticos y otros dispositivos de usuario final que han sido "botteados" también suelen ser conocidos como "zombis".

Los bots maliciosos se instalan normalmente de forma subrepticia, sin el consentimiento del usuario, o sin que éste sepa lo que podría hacer el sistema del usuario una vez instalado el bot.

Los bots se utilizan a menudo para enviar correo electrónico no deseado ("spam"), para reconocer o atacar otros sistemas, para espiar el tráfico de la red o para alojar contenidos ilegales como software pirata, material de explotación infantil, etc.

Muchas jurisdicciones consideran que la infección involuntaria de hosts de usuarios finales es un ejemplo de intrusión informática ilegal.

2. Botnet

Las redes de bots son redes de dispositivos informáticos de usuario final conectados a Internet e infectados con malware de bots, que son controlados a distancia por terceros con fines nefastos.
Una red de bots está bajo el control de un determinado "molestador" o "botmaster". Una red de bots puede tener sólo un puñado de hosts bots, o millones.

3. Cliente (o "Cliente directo")

La parte que contrata el servicio con un ISP. Hay que distinguir entre "cliente" y "usuario autorizado": por ejemplo, una cafetería puede contratar el servicio de Internet de un ISP. La cafetería sería el cliente del ISP. La cafetería puede optar por ofrecer el uso gratuito de su conexión (si lo permite la política de uso aceptable del ISP) a quienes le compren café: los compradores de café serían entonces usuarios autorizados de la conexión adquirida por la cafetería, pero no el cliente directo del ISP.

4. Detección

La detección es el proceso por el que un proveedor de servicios o un usuario final se da cuenta de que un determinado sistema o dispositivo ha sido infectado con software malicioso. Un proveedor de servicios puede detectar que un sistema se ha infectado de muchas maneras diferentes, incluso como resultado de recibir quejas de terceros sobre el spam, el escaneo de la red o los ataques que se han originado en ese sistema. Los usuarios finales pueden detectar las infecciones del sistema mediante herramientas de software u otros medios.

5. Ecosistema

Este término se utiliza a menudo para describir la interrelación de varios participantes en Internet: fabricantes de hardware, desarrolladores de software, proveedores de servicios de Internet y proveedores de diversos contenidos, aplicaciones y servicios de Internet que hacen que la red funcione y sea útil para los usuarios finales.

El ecosistema de Internet incluye proveedores de sistemas operativos, organizaciones centradas en el usuario final, proveedores de contenidos, aplicaciones y servicios de Internet, proveedores de servicios de Internet, proveedores de búsquedas, usuarios finales, departamentos de TI, empresas de alojamiento, proveedores de blogs, proveedores de seguridad, investigadores, gobiernos, empresas de servicios financieros y otras partes.

La llamada "economía sumergida" también se describe a menudo como un "ecosistema", con múltiples participantes que desempeñan diversas funciones especializadas. Por ejemplo, algunos participantes pueden especializarse en la escritura de malware, mientras que otros pueden "cosechar" direcciones de correo electrónico de páginas web y listas de correo, mientras que otros pueden especializarse en la distribución de malware a esas direcciones de correo electrónico cosechadas.
El ecosistema de los programas maliciosos también incluirá normalmente a la población de víctimas potenciales y a las fuerzas del orden que trabajan en la lucha contra la ciberdelincuencia.

6. Usuario final

Usuario final: En un contexto informático y de redes, el usuario final es la persona que, en última instancia, hace un uso autorizado de un producto o servicio.

A menudo, el usuario final puede no ser la misma persona que ha comprado el producto o servicio. Por ejemplo, el propietario de una cafetería puede comprar la conectividad para que la utilicen sus clientes; en ese caso, los clientes de la cafetería, y no el propietario, representan los verdaderos "usuarios finales", aunque no hayan contratado directamente a un ISP para la conectividad que utilizan.

Una parte, como un hacker/cracker que hace uso de un producto o servicio sin la autorización del comprador, se consideraría normalmente un intruso cibernético y no un "usuario final" per se.

7. ISP

Un proveedor de servicios de Internet (PSI) es una empresa que proporciona acceso a Internet al público, a las empresas y a otras organizaciones. Estas conexiones pueden ser por cable, DSL, satélite, inalámbricas, de acceso telefónico u otras tecnologías. Los ISP a veces se conocen también como "proveedores de acceso".

Una empresa que proporciona acceso a Internet únicamente a sus propios empleados no se consideraría normalmente un PSI. Del mismo modo, un operador de red que sólo proporciona acceso a Internet al por mayor para otros ISP se consideraría normalmente un proveedor de servicios de red (NSP), en lugar de un ISP.

8. Malware

"Malware" es la abreviatura de "software malicioso".

Los bots maliciosos son un tipo de malware. Otras formas de malware incluyen categorías de software conocidas como virus, troyanos, gusanos, rootkits, crimeware, registradores de pulsaciones de teclas, dialers, spyware, adware, etc. Los factores que distinguen esos diferentes tipos de malware son menos importantes que la comprensión de por qué el malware puede ser visto como "malicioso".

El malware suele violar uno o varios de los siguientes principios fundamentales:

(a) Consentimiento: El malware puede instalarse aunque el usuario no lo haya pedido conscientemente.

(b) Honestidad: El malware puede pretender hacer una cosa, mientras que en realidad hace algo completamente diferente.

(c) Privacidad-Respeto: El malware puede violar la privacidad de un usuario, quizás capturando sus contraseñas o la información de su tarjeta de crédito.

(d) No es intrusivo: El malware puede molestar a los usuarios mostrando anuncios, cambiando la página de inicio del navegador, haciendo que los sistemas sean lentos o inestables y propensos a fallar, o interfiriendo con el software de seguridad ya instalado.

(e) Inocuidad: El malware puede ser un software que perjudica a los usuarios (como el que daña nuestro sistema, envía correos electrónicos de spam o desactiva el software de seguridad).

(f) Respeto a la gestión del usuario: Si el usuario intenta eliminar el software, éste puede reinstalarse o anular las preferencias del usuario.

Todo se resume en "el software que los usuarios no quieren".

Los usuarios pueden instalar malware sin saberlo al abrir un archivo adjunto contaminado recibido por correo electrónico o al visitar una página web con contenido malicioso. Los sistemas también pueden ser infectados directamente por un atacante remoto como resultado de que los atacantes se dirijan a una vulnerabilidad conocida que pueda ser explotada de forma remota, o por el usuario que monta un CD, DVD o unidad de disco duro infectado.

9. Mitigación

La mitigación es el proceso de gestionar o controlar los efectos asociados a un bot. Por ejemplo, si un sistema está infectado con un bot de spam, y está arrojando correo electrónico comercial no deseado, la mitigación puede consistir en filtrar el spam que se está emitiendo desde ese dispositivo.

Hay que tener en cuenta que la mitigación no suele implicar el arreglo de la condición subyacente (eso sería "remediación"); la mitigación sólo maneja los síntomas asociados a una condición.

10. Notificación

La notificación es un proceso por el que los ISP se comunican con sus usuarios finales en relación con la posible infección del dispositivo del usuario final por un malware bot o con la forma en que un abonado puede prevenir o identificar dicha infección. La notificación también puede implicar un proceso por el que se dirige a los usuarios finales a herramientas que permitirán el autodescubrimiento de las infecciones por bots. La notificación puede adoptar diferentes formas, incluida la notificación directa por parte del ISP al usuario final, o la notificación indirecta a través de las herramientas de autodescubrimiento disponibles o de un tercero. La notificación puede hacerse a través de múltiples canales potenciales, incluyendo (pero no limitado a) el correo electrónico, el correo postal, una llamada telefónica, una notificación en el navegador, una herramienta de autodescubrimiento basada en la web o un mensaje SMS.

11. Prevención

La prevención es el proceso de endurecimiento de un sistema o servicio para que sea menos vulnerable al compromiso y la explotación. Por ejemplo, en muchos sistemas, la prevención puede implicar:

- Parchear el sistema operativo y todas las aplicaciones con las correcciones de seguridad disponibles
- Instalar o habilitar un cortafuegos
- Uso de software antivirus
- Asegurarse de que el sistema tiene una copia de seguridad periódica
- Utilizar contraseñas seguras
- Desactivar todos los servicios de red innecesarios
- Animar a los usuarios a utilizar de forma segura los servicios de Internet (por ejemplo, el correo electrónico, la navegación por la web, etc.)

12. Remediación

La remediación es el proceso por el que pasa un usuario final para limpiar un ordenador infectado para que deje de estarlo. En los casos fáciles, esto puede implicar la instalación y ejecución de un producto antivirus. En los casos más difíciles, la reparación puede implicar una intervención más sustancial hasta "destruir y pavimentar" el sistema, es decir, formatearlo y reinstalarlo desde cero, o al menos desde la última copia de seguridad limpia conocida. Una vez que el sistema esté limpio o se haya reinstalado, normalmente se endurecerá para protegerlo de una nueva infección.

13. Spam

Correo electrónico no deseado y no solicitado, a menudo de carácter comercial, que se envía normalmente a un gran número de destinatarios de forma prácticamente idéntica. El spam suele ser enviado por "afiliados" que reciben el pago de la persona que gestiona el programa de afiliación cuando los destinatarios compran el producto anunciado por el spam.

Apéndice 2 - Referencias

1. Recomendaciones sobre cómo gestionar los efectos de los ordenadores infectados con bots maliciosos: "Recomendaciones para remediar los bots en las redes de los ISP"

http://tools.ietf.org/rfc/rfc6561.txt

2. Grupo de Trabajo 8 del CSRIC II - Mejores prácticas de protección de la red del ISP

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PRO TECTION_20101213.pdf

3. icode - Código de prácticas de la industria australiana de Internet que aborda la

ciberseguridad http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. Centro de Limpieza Cibernética de Japón - Proyecto Anti-

Botnet https://www.ccc.go.jp/en_index.html

5. Centro Alemán de Asesoramiento Anti-Botnet - Proyecto Anti-Botnet

https://www.botfrei.de/en/

6. Equipo de Respuesta a Emergencias Informáticas de Japón

(CERT) http://www.jpcert.or.jp/english/

7. US CERT - Entendiendo las amenazas ocultas: Rootkits y Botnets

http://www.us-cert.gov/cas/tips/ST06-001.html

8. Alianza para las Soluciones de la Industria de las Telecomunicaciones

(ATIS) http://www.atis.org/

9. Departamento de Seguridad Nacional

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. Departamento de Seguridad Nacional - Equipo de Preparación para Emergencias Informáticas de los Estados Unidos

http://www.us-cert.gov/

11. Unión Internacional de Telecomunicaciones Botnet Mitigation Toolkit

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

12. Instituto Nacional de Normas y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos

http://www.nist.gov/index.html

13. Solicitud de información del Departamento de Comercio/Departamento de Seguridad Nacional - Modelos para promover la notificación voluntaria de las empresas a los consumidores en relación con el uso ilícito de equipos informáticos por parte de botnets y programas maliciosos relacionados

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. Comentarios recibidos en respuesta a la solicitud de información del Departamento de Comercio/Departamento de Seguridad Nacional - Modelos para promover la notificación corporativa voluntaria a los consumidores en relación con el uso ilícito de equipos informáticos por parte de botnets y programas maliciosos relacionados

http://www.nist.gov/itl/botnetcomments.cfm

15. Grupo de trabajo contra el abuso de la mensajería (MAAWG.org) - Código de conducta

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. Colección M3AAWG de Mejores Prácticas para ISPs y Operadores de Red

http://www.maawg.org/published-documents

17. Base de datos nacional sobre vulnerabilidad - Instituto Nacional de Normas y Tecnología

http://nvd.nist.gov/

18. Centro de Tormentas de

Internet

http://isc.sans.edu/index.html

19. Fundación Shadowserver

http://shadowserver.org

20. Lista de bloqueo de la política de

Spamhaus

http://www.spamhaus.org/pbl/

21. Lista de bloqueo compuesta

http://cbl.abuseat.org

22. OnGuard Online

http://www.onguardonline.gov/default.aspx

23. IETF BCP38 Network Ingress Filtering

http://tools.ietf.org/html/bcp38