TREND MICRO™

Organization of American States

Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas

Contenido

Mensaje del Secretario General Adjunto de la OEA

Embajador Albert R. Ramdin

La Organización de los Estados Americanos (OEA) colabora con nuestros Estados Miembros para forta-lecer sus capacidades de seguridad informática, particularmente para proteger su infraestructura crítica. En 2004, la Asamblea General de la OEA aprobó por unanimidad la Estrategia Interamerica-na Integral de Seguridad Cibernética. Al reconocer que debido a que las amenazas cibernéticas han crecido de manera persistente, los gobiernos de los países americanos firmaron la declaración de "Fortalecimiento de la Seguridad Cibernética de las Américas" (2012), y más recientemente el Comité Interamericano contra el Terrorismo (CICTE) de la OEA adoptó la "Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes" (2015).

Estos instrumentos son críticos para la promoción de las políticas de seguridad cibernética que buscan mejorar la seguri-dad cibernética de la infraestructura crítica en el continente.

Los Estados Miembros dependen de su infraestructura crítica para brindar servicios y productos imprescindibles, y gracias a que los países de América han experimentado un crecimiento del número de infraestructuras que operan sobre las redes de Internet, también ha aumentado el número de ataques cibernéticos a dichas infraestructuras, lo que podría com-prometer la infraestructura crítica de un país así como su capacidad de proveer servicios imprescindibles para sus ciuda-danos.

Las explotaciones que pueden afectar a la infraestructura de los países son normalmente introducidas por herramientas sencillas o sofisticadas que pueden tener acceso a los dispositivos móviles u otros dispositivos personales para penetrar a sectores de alto valor, como son los de transporte, energía o sistemas financieros. Para enfrentar estas amenazas cibernéticas, la OEA procedió a fortalecer sus capacidades de seguridad cibernética en la infraestructura crítica al brindar capacitación a la medida a los funcionarios de nivel directivo, legisladores y técnicos de seguridad que trabajan en la infraestructura crítica de los países.

A través de los años, estos esfuerzos han evolucionado para también representar mejor las actuales tendencias de los ataques a la infraestructura crítica. Entender las capacidades de seguridad cibernética de los Estados Miembros y las tendencias de los ataques cibernéticos es el primero paso hacia el fortaleci-miento de la capacidad de respuesta. Considerando esto, el presente reporte se preparó con el propósito de ser un documento integral del cual los Estados Miembros, los operadores de la infraestructura crítica y otros pueden sacar conclusiones útiles y entender mejor las principales amenazas cibernéticas que afectan a la infraestructura crítica en América. Por ejemplo, los datos reunidos revelaron que 53% de los encuestados advirtieron un aumento de los ataques a sus sistemas de cómputo en 2014, y 76% aseguró que los ataques cibernéticos contra la infraestructura con cada vez más sofisticados.

Vale la pena mencionar que fue posible reunir dichos datos gracias a la cooperación que la OEA fomenta entre los sectores público y privado. Los gobiernos deben trabajar conjuntamente con el sector privado y las organizaciones de la sociedad civil y reconocer que la seguridad cibernética es una responsabilidad compartida. Este reporte es un excelente ejemplo de la participación de las múltiples partes que la OEA ha promovido en sus políticas de seguridad cibernética, combinando las contribuciones de los gobiernos de los Estados Miembros, del sector privado, de la academia y de la sociedad civil. Esperamos que esta infor-mación sirva como guía a nuestra región para brindar un espacio cibernético más seguro y mejorar la seguridad cibernética para proteger nuestra infraestruc-tura esencial.

Prólogo

Organización de los Estados Americanos

Adam Blackwell

Secretario de Seguridad Multidimensional | *Organización de los Estados Americanos*

El mundo nunca ha sido más pequeño, somos mucho más los que nos podemos conectar a velocidades mucho más altas. El Internet de Todo ha cambiado la forma en que interactuamos, ha revolucionado los procesos de negocio, y ha modificado la forma en que se administran los países y su infraestructura crítica. No hay duda de que esta hiperconectividad es una poderosa herramienta de desarrollo y una oportunidad de crecimiento, para gobiernos, empresas e individuos por igual. Una herramienta que debe ser abierta y accesible a pesar de los riesgos inherentes. La manera en que equilibremos y enfrentemos estos riesgos es el desafío que tenemos en el futuro inmediato; y es esta apertura y facilidad de acceso también lo que ha abierto la puerta a los emprendedores criminales.

Pueden participar en actividades ilícitas desde casi cualquier lugar lo que le dificulta aún más a las fuerzas de seguridad vincular el crimen con el responsable y la jurisdicción.

Por consiguiente, todos debemos trabajar juntos; gobiernos, organizaciones internacionales, el sector privado y la sociedad civil, reforzando la colaboración y reconociendo que la seguridad cibernética es una responsabilidad compartida. El cribercrimen afecta a la sociedad en su conjunto, no sólo amenazando la privacidad de los individuos, sino también comprometiendo potencialmente a la infraestructura crítica de un país y su capacidad de brindar servicios imprescindibles a sus ciudadanos. La globalización de las economías también representa una amenaza de escala internacional. Esto destaca la necesidad de actuar en cuatro niveles distintos: Internacional, nacional, sector privado e individual, pues los individuos también tienen la misma responsabilidad y deben estar conscientes de sus propias vulnerabilidades y de su participación en la higiene cibernética.

Actualmente, América Latina y el Caribe tienen una de las poblaciones de Internet de más rápido crecimiento del mundo, lo que da origen a una serie de retos importantes en cuanto a la seguridad cibernética. En respuesta al aumento de las amenazas, la Organización de los Estados Americanos (OEA), a través del Comité Interamericano Contra el Terrorismo (CICTE), ha desarrollado un programa regional de seguridad cibernética que busca fortalecer la seguridad y mejorar la protección de la infraestructura de información crítica en todo el continente. Reconociendo la importancia de la colaboración, el Programa de Seguridad Cibernética de la OEA gira en torno a la implementación del siguiente plan de siete puntos:

[1] **Participación de la sociedad civil y del sector privado:** Más de 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por éste. Por esta razón la OEA se ha asociado con compañías privadas como Trend Micro, con quien tenemos el placer de colaborar en este reporte, Microsoft, Symantec, así como organizaciones sin fines de lucro que incluyen al Foro Económico Mundial, PARA.PIENSA.CONECTATE[1], y el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC).

[2] **Crear conciencia:** Con el desarrollo del Internet de las Cosas, la gente se conecta a Internet de diferentes maneras. Esta nueva tendencia destaca la importancia de diseñar políticas para crear conciencia entre los usuarios finales de Internet acerca de las medidas de seguridad cibernética. La OEA ha lanzado un programa agresivo de concientización para asegurar que los individuos entienden los riesgos y la necesidad de adoptar medidas adecuadas para su propia seguridad cibernética.

1 http://stopthinkconnect.org/

[3] **Desarrollo de estrategias nacionales:** Una estrategia nacional de seguridad cibernética permite que los países definan una visión completa de la seguridad cibernética y establecer responsabilidades claras, coordinando acciones entre los gobiernos y los interesados relevantes. La OEA promueve el desarrollo de estrategias y marcos nacionales de seguridad cibernética en todos los Estados Miembros, y ha trabajado anteriormente con Colombia, Panamá y Trinidad y Tobago, y trabaja actualmente con Dominica y las Bahamas.

[4] **Brindar capacitación:** Es fundamentar permanecer actualizados en el entorno de seguridad cibernética que está en constante evolución. Se ha comprobado que brindar capacitación técnica a los funcionarios es un medio bastante exitoso para mejorar la seguridad cibernética a escala nacional y regional. En particular, la OEA ha ayudado a los Estados Miembros a establecer Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs) nacionales y gubernamentales, los cuales han aumentado de seis a diecinue-ve en la última década.

[5] **Ejercicios de Gestión de Crísis:** En paralelo con la capacitación técnica y el desarrollo de equipos de respuesta, la OEA también realiza ejercicios de manejo de crisis. Esto le permite a los Estados Miembros diseñar ejercicios de acuerdo con sus necesidades al tiempo de fortalecer la colaboración a nivel técnico dentro de otros países para responder a las amenazas.

[6] **Misiones de asistencia técnica:** La OEA responde a las necesida-des de los países al desarrollar y realizar misiones de asistencia técnica diseñadas para atender las preocupaciones cibernéticas. Esto normalmente involucra visitas, revisiones de las políticas y presentaciones de las autorida-des locales, culminando en una serie de recomendaciones de expertos.

[7] **Compartir información y experiencia:** La OEA está trabajando en el desarrollo de una red de CSIRTs nacionales y otras autoridades relacionadas con la seguridad cibernética, lo que busca facilitar la comunicación en tiempo real y compartir información.

Trend Micro

En Trend Micro, nuestra misión de hacer un mundo seguro para intercambiar información nos ha llevado a desarrollar y cultivar asociaciones privadas y públicas con organizaciones de todo el mundo. Nunca ha sido más importante que las organizaciones públicas y privadas colaboren y compartan información en un esfuerzo por combatir el cibercrimen. Para lograrlo, nos enorgullece habernos asociado con la OEA para desarrollar este reporte que examina las amenazas del crimen cibernético que afectan a las infraestructuras críticas de América.

Los datos recopilados en este reporte incluyen información de todos los países americanos que reportaron un aumento importante del nivel de ataques a sus sistemas de cómputo durante el año pasado. El aumento de la actividad criminal no sorprende, pues el aumento de los ataques cibernéticos en América Latina se documentó en nuestro reporte de 2013 de Tendencias de Ciberseguridad y Respuestas de los Gobiernos en la región.[2]

2 http://www.oas.org/cyber/documents/OASTrendMicroLAC_ENG.pdf

Además, el Resumen Anual de Seguridad 2014 de TrendLabsSM reporta que numerosas organizaciones de todo el mundo, incluyendo a bancos y servicios públicos, perdieron millones de registros de clientes y credenciales en 2014.[3] El sector de infraestructura crítica ha surgido como un vector de ataque particularmente vulnerable, debido a instalaciones antiguas y el predominio de “medidas a medias e improvisadas”, en lugar de sistemas de seguridad integrales.[4]

Con este reporte los lectores tendrán entenderán mejor los tipos de ataques que ha sufrido este sector en América y enfoca la atención en la necesidad de una mejor colaboración entre las organizaciones de infraestructura crítica y los gobiernos. Como lo atestiguamos en 2014, el gobierno de Estados Unidos ha reconocido las vulnerabilidades de este sector y las posibles graves consecuencias si las industrias no se aseguran adecuadamente a nivel nacional, como las redes eléctricas, el suministro de agua y combustibles fósiles y las telecomunicaciones.

Este reporte tiene el propósito de aclarar la actividad cibercriminales y las tendencias que se han observado en el sector de infraestructura crítica de América. También busca informar sobre cómo promover la colaboración entre estas industrias y cómo sus gobiernos pueden fortalecer su capacidad de combatir los ataques cibernéticos.

3 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf
4 http://blog.trendmicro.com/breaking-down-old-and-new-threats-to-critical-infrastructure/

Resumen Ejecutivo

Los ataques a la infraestructura crítica se han convertido en una importante preocupación para los gobiernos y proveedores privados de todo el mundo – ya sean ataques cometidos por criminales cibernéticos que buscan tener ganancias financieras o por hackers como actos políticos que buscan socavar la credibilidad de los gobiernos y las compañías.

La agitación alrededor de estas amenazas está justificada, ya que la investigación demuestra que los ataques a la infraestructura crítica se han vuelto más comunes y sofisticados y continuarán creciendo en el futuro inmediato.

La gestión y el monitoreo de los sitios ha mejorado en las instalaciones de la infraestructura crítica gracias a que éstas se conectan cada vez más agresivamente a Internet. Sin embargo, la conveniencia de la conectividad ha convertido la superficie de ataques una vez limitada de estas industrias en un campo fértil para los ataques cibernéticos. Debido a los efectos de alto perfil de los ataques a los sistemas de la infraestructura crítica, estas industrias se han convertido en blancos más atractivos para los criminales.

Aprovechando el éxito de nuestro estudio de 2013 “Tendencias de la Seguridad Cibernética y las Respuestas de los Gobiernos de América Latina y el Caribe”, la OEA y Trend Micro se han unido para brindar otra visión del estado de la seguridad de los miembros de la OEA.[5] Esta encuesta sin precedente de más de 20 Estados Miembros de la OEA ofrece un panorama del estado actual de la seguridad cibernéti-ca alrededor de la infraestructura crítica de la región y de las tendencias de las amenazas que enfrentan estas organizaciones clave.

La información reunida ofrece una importante perspectiva de los ataques cibernéticos sufridos por las organizaciones de infraestructura crítica en la región, así como de las medidas y políticas de seguridad cibernética de las organizaciones; de la colaboración con los gobiernos locales; y de su preparación para enfrentar los ataques cibernéticos.
Muchos de los hallazgos de la encuesta se correlacionan con nuestra investigación actual sobre los ataques a la infraestructura crítica, y los nuevos conocimientos ayudarán a guiar nuestra investigación en el futuro para proteger esta industria contra los ataques cibernéticos.

Los participantes en la encuesta pertenecen a agencias de gobierno, así como a industrias críticas como las comunicaciones, banca y finanzas, manufactura, energía y seguridad, entre otras. También dijeron que los atacantes están cada vez más interesados en robar datos para provocar caos y confusión mediante el hackeo de los sistemas de control (SCADA).

No sorprende que todos los miembros encuestados citaran a las tácticas de spear-phishing como el método de ataque más grande contra el que tuvieron que defenderse, seguido por la explotación de vulnerabilidades de software sin parches. Esto refleja el papel problemático que el spear-phishing juega en los incidentes de seguridad cibernética, especialmente en los ataques dirigidos.

5 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Los entrevistados dejaron claro que los ataques dirigidos a la infraestructura son un peligro claro y presente mientras que sólo un menor porcentaje de ellos pudo decir que no habían visto este tipo de ataques.

Cuando se les pidió hacer una descripción del panorama de amenazas, los participantes aseguraron que éstas están siendo muy severas, mientras que algunos calificaron como desalentador el futuro de asegurar estas infraestructuras. Para la mayoría de los encuestados, la frecuencia de los ataques está aumentando o se mantiene constante, en tanto que los ataques son cada vez más sofisticados.

Entre los factores positivos, los entrevistados indicaron que estaban preparados o algo preparados para enfrentar un ataque cibernético. Asimismo, las organizaciones han implementado tecnologías, políticas y procedimientos que pueden ayudar a proteger su entorno.

Este reporte también revela la falta de asociación proactiva entre los gobiernos y las organizaciones privadas de esta región. Una escueta mayoría de los encuestados de la industria privada y del gobierno reportó que no hay un diálogo o sólo hay diálogos informales entre estos socios clave.

Una conclusión notable es que el hecho de que no exista una asociación pública privada, lo cual representa una oportunidad perdida histórica, no obstante que el nivel de confianza para que los gobiernos logren avances en una agenda de ciberseguridad alrededor de la infraestructura crítica es muy alto para todos los entrevistados.

Otro impedimento para enfrentar estas amenazas en evolución son los bajos presupuestos. La mayoría de los encuestados dijo que existen desafíos que pueden dificultar la defensa continua contra los ataques dirigidos a sus infraestructuras críticas.

Si bien las organizaciones de América han hecho un buen trabajo para proteger la infraestructura crítica contra los ataques, se acerca un punto crítico. Debido a que la frecuencia y la sofisticación de los ataques continuarán o se agravarán y se enfocarán no sólo en afectar a la infraestructura crítica sino también en comprometer la información vital que pudiera usarse en el futuro, los defensores pronto podrían no tener el apoyo necesario para prevenirlos. La falta de financiamiento y de liderazgo gubernamental en esta área deja a los defensores sintiéndose cada vez más solos. Más que eso, los gobiernos de la región necesitan tender la mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial.

Análisis y Comentario sobre el Estado de la Seguridad Cibernética de la Infraestructura Crítica en las Américas

Esta sección incluye una serie de ensayos cortos escritos por colaboradores expertos que analizan y comentan el estado de la seguridad cibernética y de la infraestructura crítica.

Información proporcionada por Trend Micro

Trend Micro Forward-looking Threat Research observó varias tendencias durante el año pasado, entre las que destaca el uso de malware para comprometer los sistemas de control de supervisión y de adquisición de datos (SCADA), incluyendo el Sistema de Información de Gestión Personas sin Hogar (HMIS), procesamiento histórico y otros dispositivos conectados.

Esta tendencia se ha manifestado de dos maneras: malware que se hace pasar por aplicaciones SCADA válidas, y malware que se utiliza para analizar e identificar protocolos SCADA específicos. En la primera, el malware se ha hecho pasar por aplicaciones válidas para Siemens, Allen Bradley y varios otros proveedores. En la segunda manifestación, hemos observado malware específico que detecta OPC y Modbus. Si bien la razón para este análisis aún no se ha determinado, el propósito probablemente es la reunión de inteligencia para el espionaje industrial o realizar un ataque futuro. Hemos observado un creciente interés en los protocolos SCADA, ataques y malware, y se espera que esta tendencia continúe.

Lo que distingue a esta tendencia es que parece haber un crecimiento notable del conocimiento que los atacantes tienen de la tecnología SCADA. Estos atacantes no sólo han demostrado tener un conocimiento de los nombres de las aplicaciones, de los nombres de los proyectos, etc., también conocen muy bien los protocolos de SCADA. Este conocimiento ha crecido mes con mes, y se prevé que esta tendencia aumente considerablemente en 2015 y 2016, y es probable que se revele más funcionalidad en el malware y los grupos adicionales que atacan a SCADA.

"Un reporte del Equipo de Respuesta a Emergencias Cibernética de los Sistemas de Control Industrial (ICS-CERT) de Estados Unidos señala que los sistemas de control industrial fueron blanco de los ataques cibernéticos por lo menos 245 veces en un periodo de 12 meses, de octubre de 2013 a septiembre de 2014. Cerca de 32% de las industrias fueron del sector energético, mientras que el de manufactura crítica comprendió el 27%. El ICS-CERT reveló que 55% de los incidentes investigados mostraron señales de que se han utilizado amenazas persistentes avanzadas, o ataques dirigidos, para violar los sistemas."

Referencias:

http://www.v3.co.uk/v3-uk/news/2399334/us-industrial-control-systems-attacked-245-times-in-12-months

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

A menudo es complicado, si no es que imposible, establecer el origen de estos grupos cibercriminales. Sin embargo, la mayoría de los grupos que utilizan malware dirigido contra los sistemas SCADA provienen de Rusia. Aún se desconoce su motivación; por tanto, es difícil determinar si estos ataques están siendo realizados por criminales individuales o por aquellos respaldados por el gobierno.

Dos notables ataques a la Infraestructura Crítica de 2014

De acuerdo con la firma de seguridad CrowdStrike, un grupo de hackers rusos denominado "Oso Energético" provocó estragos importantes en empresas del sector energético de los Estados Unidos[6]. El grupo utilizó un malware altamente efectivo y recientemente creado que se conoce como "Havex" para penetrar en el sistema de control industrial (ICS)/sistemas SCADA de sus compañías objetivo. Una vez que este malware infecta el ICS de una compañía, envía datos e información sensibles a los hackers a través de los servidores de comando y control (C&C). De acuerdo con Mike Assante, Director de ICS del SANS Institute, "los módulos de malware (Havex y BlackEnergy II) capaces de afectar a los ICS indican una inversión importante de tiempo y dinero".

A finales de 2014, un ataque lanzado contra una planta de acero alemana provocó daños físicos, de acuerdo con un reporte de la Oficina Federal para la Seguridad de la Información de Alemania, o la BSI.[7] Aparentemente los atacantes habían comprometido primero la red de la oficina de la planta siderúrgica mediante el uso de correos electrónicos con spear-phishing e ingeniería social inteligente. A partir de ahí, lograron penetrar a la red de producción y a otros sistemas, incluyendo los sistemas que controlan el equipo de la planta.

Este compromiso generó fallas frecuentes de los componentes de control individuales y de varios sistemas, y finalmente provocó que los operadores no pudieran regular adecuadamente y cerrar rápidamente un alto horno. El resultado fue un "daño masivo a la planta", informó la BSI.[8]

Las organizaciones pueden implementar las siguientes prácticas para defenderse contra los ataques a los ICS en 2015:

- Implementar software anti-malware donde sea posible en el entorno de ICS
- Utilizar un servidor bastión para prevenir el acceso no autorizado a ubicaciones seguras a lo largo del entorno de ICS
- Aplicar listas blancas de aplicaciones en el entorno de ICS para evitar que se ejecuten las aplicaciones no autorizadas
- Implementar un sistema de detección de brechas
- Habilitar el bloqueo de USB en todos los entornos SCADA. Esto evita que el malware entre físicamente al entorno
- Implementar medidas básicas de seguridad entre los segmentos de la red, como firewalls/IPS, entre la red de negocio y la red ICS

6 http://www.infosecurity-magazine.com/news/energetic-russian-bear-attacking-western-energy/
7 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile
8 http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html

Caltech Smart Grid Research: Amenazas Cibernéticas Potenciales y Mitigación

Steven Low

Profesor de Ciencias de la Computación y de Ingeniería Eléctrica | Instituto de Tecnología de California

La transformación histórica de nuestros sistemas de energía ha alcanzado la cúspide. La red eléctrica, desde la generación y transmisión hasta la distribución y el consumo, experimentará el mismo tipo de transformación arquitectónica en las próximas décadas por la que la red de cómputo y comunicación ha pasado en los dos últimos años. Imaginamos una red futura con cientos de millones de recursos de energía distribuidos (DERs) como paneles solares, aerogeneradores, vehículos eléctricos, dispositivos de almacenamiento de energía, edificios inteligentes, dispositivos inteligentes, inversores inteligentes y otros sistemas electrónicos. Estos endpoints inteligentes no serán cargas pasivas únicamente, como son actualmente la mayoría de los endpoints, sino también podrán generar sentido, calcular, comunicarse y accionar. Nos darán una tremenda oportunidad para generar y utilizar la electricidad de forma más eficiente y flexible, pero también traerán varios riesgos debido al potencial de ataques cibernéticos y otras vulnerabilidades.

Nuestra investigación incluye algunos de los desafíos de ingeniería y económicos más fundamentales y difíciles para ayudarnos a entender y guiarnos en esta transformación histórica, así como reducir su riesgo y alcanzar su potencial. A continuación, ofrecemos un ejemplo de los resultados de nuestra investigación.

Ataque y propagación de las fallas y mitigación

La red eléctrica transformada será la integración más grande y más compleja de las redes cibernéticas y físicas de la historia. La inteligencia se integrará en todas partes, desde los paneles solares y los vehículos eléctricos hasta los dispositivos inteligentes y el almacenamiento de energía, desde los hogares y las micro-redes hasta las subestaciones. Si bien es indispensable para la estabilidad, la confiabilidad y la eficiencia de la red, esto también creará una nueva fragilidad ante las amenazas a la seguridad cibernética. Cada DER se convertirá en un punto de entrada potencial para un ataque cibernético. La red cibernética que controla y optimiza la red física también ampliará considerablemente la escala, la velocidad y la complejidad de un ataque. Asimismo, puede acelerar y ampliar la propagación de fallas en la red física, lo que dificultará mucho la mitigación de los apagones.

Hemos estudiado este proceso para entender su dinámica y desarrollar las estrategias de mitigación.

"Si bien es indispensable para la estabilidad, la confiabilidad y la eficiencia de la red, también esto creará una nueva fragilidad para las amenazas a la seguridad cibernética. Cada recurso distribuido de energía se convertirá en un punto de entrada potencial para un ataque cibernético. La red cibernética que controle y optimice la red física también ampliará considerablemente la escala, la velocidad y la complejidad de un ataque".

Supongamos que un ataque a la red cibernética o física ocasiona la falla de una serie de dispositivos de la red. ¿Cómo se propagaría esta falla? ¿La falla ocasionaría un apagón de gran escala? Para contestar estas preguntas es necesario entender la redistribución del flujo eléctrico en la red cuando falla una serie de dispositivos de la red.

Hemos descubierto propiedades de monotonicidad con respecto a la falla de la conexión que nos permiten entender sistemáticamente las dinámicas de la distribución de electricidad conforme la falla se propaga por la red. Utilizando estas propiedades de monotonicidad, hemos diseñado estrategias de desbordamiento de carga que puedan aminorar la sobrecarga de la red y los apagones cuando los dispositivos de la red fallan, y aislar los ataques cibernéticos potenciales.

Optimización del flujo de energía

El flujo de energía óptimo (OPF) busca reducir ciertas funciones de costos, como la electricidad perdida en una red, el costo del combustible para la generación de electricidad, o las limitaciones de seguridad. El OPF es fundamental para las operaciones y la planeación del sistema de energía ya que constituye la base de numerosas aplicaciones como el compromiso de las unidades (qué generadores utilizar), el despacho económico (cuánto deben producir estos generadores), la estimación del estado (estimación del estado de la red completa a partir de mediciones parciales), la evaluación de la estabilidad y la fiabilidad (¿la red convergirá en un nuevo equilibrio estable en caso de una contingencia?), el control de Voltios-VAR (provisión de la energía reactiva para estabilizar los voltajes) y la respuesta a la demanda (adaptación de la carga a la oferta fluctuante).

La red óptima es flexible, con recursos que tienen índices dinámicos que varían con el tiempo y que reflejan su capacidad bajo diversas condiciones de operación. Asimismo, también está configurada de manera óptima; así, abrir o cerrar las líneas de transmisión se convierte en una variable de decisiones, o acción de control, en lugar ser la entrada para un problema, o estado. Cuando es posible, las limitaciones de seguridad son correctivas en lugar de preventivas. Con las limitaciones de seguridad preventivas, el sistema se opera de manera conservadora para sobrevivir a la pérdida de cualquier elemento de transmisión o generador. En contraste, las limitaciones correctivas reconfiguran el sistema de inmediato después de la pérdida de un generador o de un elemento de transmisión, como nuestras estrategias de desbordamiento de cargas, para mitigar los ataques cibernéticos potenciales.

En los últimos años, hemos estado desarrollando un nuevo modelo de OPF a través de la relajación semidefinitiva. Este método brinda la capacidad de determinar si una solución es óptima a escala global. Si no lo es, la solución ofrece un límite inferior sobre el costo mínimo, y por tanto, un límite en la brecha subóptima de cualquier solución factible. Hemos probado nuestros métodos en varios sistemas de referencia y en sistemas de distribución reales, y descubrimos que ofrecen con éxito soluciones globales óptimas en más de 95% de los casos analizados.

Control ubicuo de la frecuencia de la carga

A diferencia de las redes de datos, la oferta y la demanda de electricidad debe equilibrarse siempre y en todos los puntos de la red, lo cual se logra a través del control de frecuencia. Mantiene la frecuencia de nuestro sistema de energía de corriente alterna (CA) alrededor de su valor nominal (por ejemplo, 60Hz en Estados Unidos, 50Hz en Europa) cuando la demanda o la oferta fluctúan. Las dinámicas del sistema son impulsadas principalmente por grandes máquinas giratorias en los generadores. Las frecuencias a las que estas máquinas rotan determinan la frecuencia de la red de electricidad. Cuando la demanda supera a la oferta, estas máquinas se hacen más lentas y cae la frecuencia del sistema.

Por otro lado, cuando la demanda es menor a la oferta, estas máquinas se aceleran, y aumenta la frecuencia del sistema. Por tanto, la desviación de la frecuencia mide el desbalance instantáneo de la energía.
Tradicionalmente es en la parte de la generación donde se implementa el control de frecuencia, por ejemplo, la generación se ajusta respondiendo a las fluctuaciones de la demanda. Hemos estado estudiando la posibilidad del control de frecuencias continuo y ubicuo en la parte de la carga. A diferencia del control tradicional en la generación, el control de frecuencias en la carga responde más rápidamente y no consume combustible extra ni emite gases invernadero extra.

La necesidad y las tecnologías para implementar el control de frecuencias en la parte de la carga han madurado durante la última década. El problema radica en saber cómo diseñar los algoritmos de control de retroalimentación en tiempo real para al control de frecuencias ubicuo y continuo en el extremo de la carga.

Recientemente desarrollamos una serie de algoritmos distribuidos que son estables, eficientes y equitativos, y pueden escalar a millones de cargas inteligentes. Las simulaciones han demostrado que trabajan en armonía con el control de los generadores, y mejoran el comportamiento estático y transitorio sobre el control únicamente del lado del generador. Conforme transformemos nuestra red eléctrica con DERs integrados, podemos modificar estos algoritmos para ajustarlos a las fallas de las conexiones que pudieran ser provocadas por los ataques cibernéticos.

Conclusión

La integración de redes informáticas y físicas promete un suministro eficiente, confiable y flexible de la electricidad en harmonía con las necesidades de energía que aumentan rápidamente. Los DERs inteligentes crearán oportunidades tremendas, pero también introducirán riesgos potencialmente serios.

Al entender los desafíos de ingeniería y los riesgos que traen consigo estas oportunidades, es posible reducir las amenazas potenciales a la seguridad cibernética. Las propiedades de monotonicidad de las fallas de la red provocadas por posibles ataques cibernéticos pueden utilizarse para desarrollar estrategias de desbordamiento de cargas. Las limitaciones de seguridad pueden incluirse en las fórmulas del OPF para mantener la eficiencia de la red. Además, el control ubicuo de frecuencias en el lado de las cargas puede utilizarse para conservar la estabilidad de la red a través de algoritmos distribuidos que se ajusten a los ciberataques potenciales.

El vital papel de la Protección de la Infraestructura de Información Crítica (CIIP) en la Seguridad Cibernética

Peter Burnett

Coordinador de Meridian | CiviPol Consultant

Quarter House Ltd

Intercambio de Información sobre Seguridad Cibernética

La CIIP es una derivación del concepto más ampliamente conocido de Protección de la Infraestructura Crítica (CIP), o la protección de las infraestructuras de energía, telecomunicaciones, suministro de agua, transporte, finanzas, salud y otras que permiten que funcione una nación. Estas infraestructuras críticas necesitan ser protegidas contra eventos accidentales y deliberados que no les permitirían operar correctamente y que impactarían severamente a la economía y al bienestar social de esa nación.

Estas infraestructuras se han protegido contra los ataques físicos y el sabotaje durante muchas décadas y hasta los inicios de este siglo. Sin embargo, varios países se dieron cuenta de que muchas de estas infraestructuras críticas también tenían algo en común: dependían en mayor o menor medida de las infraestructuras de información (redes de telecomunicaciones y sistemas de cómputo, ITC). Y debido a esta dependencia nació la disciplina de Protección de la Infraestructura de Información Crítica (CIIP). Los gobiernos y la industria ha comprendido rápidamente esto, y ha surgido el concepto más amplio de seguridad cibernética que incluye la CIIP.

La CIP (incluyendo la CIIP) es esencialmente un problema que deben resolver los gobiernos, pero no poder ofrecer una CIP es un problema para todos pues todos dependemos de esa infraestructura. La CIP a menudo es una responsabilidad nacional, y puede ser manejada principalmente como un asunto de seguridad nacional, pero la CIIP es casi siempre un asunto internacional o global. Son pocos los países (si los hay) cuya infraestructura de telecomunicaciones no va más allá de sus fronteras, y en el espacio cibernético existe frontera con todos los países, no sólo con los países vecinos.

En muchos países, y en particular en los occidentales, las infraestructuras críticas pertenecen al sector privado y son administradas por operadores privados, y con frecuencia las infraestructuras de información son administradas por corporaciones multinacionales que se encuentran fuera de las fronteras. Esto significa que los gobiernos deben colaborar de manera estrecha con aquellos operadores de infraestructuras del sector privado para asegurar la continuidad del servicio al construir infraestructuras robustas.

El Internet se concibió intencionalmente para ser una red resistente, y fundamentalmente lo sigue siendo. Nunca fue diseñado para ser esa infraestructura de información crítica vital en la que hoy se ha convertido, especialmente para las pequeñas empresas, cuya dependencia del correo electrónico, de los sitios web, del acceso a otros recursos en línea se incrementa cada día. El impacto de una pérdida seria del acceso a Internet durante un periodo prolongado es incalculable debido a la complejidad de nuestras dependencias. ¡Sólo intente prescindir del ancho de banda algunas semanas!

Por lo tanto, es esencial que los gobiernos trabajen muy de cerca con el sector privado, a menudo en Asociaciones Públicas-Privadas (PPPs) para ayudar a enfrentar las amenazas para estas Infraestructuras de Información Críticas (CCIs) y hallar soluciones. Con frecuencia el sector privado es el primero en detectar estas amenazas, pero los CERTs del gobierno también pueden jugar un papel vital para coordinar la respuesta. Los modelos específicos de PPPs han evolucionado para asegurar que este intercambio de información sea oportuno y efectivo, incluyendo el modelo de Intercambio de Información y Centro de Análisis (ISAC) desarrollado en Estados Unidos hace 20 años, el modelo de Intercambio de Información (IE) y recientemente la Asociación de Intercambio de Información sobre Seguridad Cibernética (CISP) ambos desarrollados en el Reino Unido, y la variante Duch ISAC, por nombrar algunos.

Los gobiernos también necesitan hablar entre sí sobre estos asuntos, bilateralmente, y algunas veces de forma confidencial para que puedan compartir experiencias y soluciones, y crear redes de contactos gubernamentales internacionales confiables sin presiones comerciales de los socios del sector privado. Un foro global de este tipo se proporciona de forma única por las Conferencias Meridian, las cuales se realizan en diferentes países y regiones cada año; la 11ª conferencia anual se llevará a cabo en España en octubre de 2015, patrocinado por la Agencia Española de CIIP, CNPIC, y después de la conferencia que se realizó en Argentina en 2013, Meridian planea regresar a las Américas en el 2016.

El gran problema que está reuniendo a los operadores de la CIP y la CIIP y a los gobiernos es el área de cruce conocida como la seguridad de los sistemas de Control de Supervisión y Adquisición de Datos (SCADA), o la seguridad de los Sistemas de Control Industrial (ICS). Estos incluyen sistemas que controlan las defensas contra inundaciones, las represas, las instalaciones de generación de electricidad, los oleoductos, los controles de plantas químicas y muchos otros componentes de la infraestructura crítica. Antes de este siglo, eran controles manuales, o eran controlados por hardware y software especiales oscuros, y que sólo algunos ingenieros y especialistas entendían.

Actualmente, un mayor número de estos sistemas se están computarizando con controles de comunicación remotos, y casi siempre están conectados a Internet de alguna forma. Eso significa que deben protegerse contra el mismo malware y contra las explotaciones que pueden afectar a los sistemas de cómputo de los hogares y de las pequeñas empresas, y significa también que dependemos aún más de la resistencia del Internet. Sólo imagine una interrupción prolongada de Internet que no sólo lo privaría de su ancho de banda, sino que también detendría la estación encargada de bombear agua, el sistema que genera la electricidad, el centro de logística para distribuir materia prima a las fábricas de alimentos y supermercados, el oleoducto que lleva el combustible a las refinerías y a las gasolineras; la pesadilla sería interminable.

Afortunadamente existen muchas organizaciones comerciales, operadores privados y agencias de gobierno que trabajan para asegurar que las infraestructuras de información crítica estén protegidas y sean resistentes, y para asegurarse de que esta pesadilla no suceda, y están trabajando juntos de la mejor manera posible.

Centro de Intercambio y Análisis de Información de Servicios Financieros (FS-ISAC) de Estados Unidos

Los ataques de DDoS de 2012 y 2013 contra el sector financiero son un excelente ejemplo de la respuesta coordinada de los sectores a través del Centro de Intercambio y Análisis de Información de Servicios Financieros (FS-ISAC). Bajo el Compendio de Todos los Riesgos de FS-ISAC, creamos un equipo de acción ante incidentes integrado por 37 instituciones que estaban siendo atacadas. La comunicación que se dio entre el grupo fue fenomenal. Después tomamos la información, la englobamos y la hicimos anónima y la compartimos con el resto de los socios del sector como el Centro Nacional de Seguridad Cibernética y de Integración de Comunicaciones (NCCIC) y otros ISACs.

La información compartida incluyó IOCs, mejores prácticas, scripts y estrategias de mitigación y lecciones aprendidas. Asimismo, trabajamos muy de cerca con los ISPs y mitigadores y nos reunimos con ellos para compartir y desarrollar las mejores tácticas y estrategias de mitigación. El IAT también desarrolló un punto de vista de las amenazas sobre DDoS que actualizamos tres veces cuando las tácticas cambiaron, y se compartieron con el sector y los socios. El esfuerzo tuvo tanto éxito que los atacantes persiguieron a otras instituciones cuando sus tácticas se volvieron menos efectivas. El último día de la última de las tres fases, fue atacada una institución que no había sufrido ataques pero sin sufrir ningún daño. Nos dijeron que gracias a la comunicación que se había dado anteriormente pudieron implementar las estrategias de mitigación que esencialmente frustraron el ataque. Este es el mejor ejemplo del intercambio de información.

América Latina y la Ciberseguridad Industrial

El interés de la comunidad de la seguridad para analizar y descubrir nuevas vulnerabilidades de los sistemas de automatización industrial, en particular de las infraestructuras críticas, ha crecido rápidamente. Si bien este interés comenzó en casi todas las conferencias de seguridad importantes de 2013 y 2014, se ha hablado mucho de los ataques perpetrados contra los sistemas de control y automatización. También se ha publicado mucho sobre este tema; asimismo, los proveedores están adaptando sus tecnologías para brindar "nueva" protección a estos sistemas. Sin embargo, lo más importante es el hecho de que los principales medios de comunicación han reportado un número importante de ataques que afectan principalmente a la producción y distribución de petróleo, gas y energía.

Y América Latina no ha sido la excepción; existe un gran interés por investigar las posibles debilidades y los ataques sufridos. Los países latinoamericanos han estado siguiendo esos temas muy de cerca, aunque tienen menores presupuestos que los de los países europeos y Estados Unidos.

Mediante el análisis de los tres países más representativos de la región, como son Argentina, Brasil y Colombia, podemos observar tres maneras distintas de abordar la ciberseguridad industrial, a partir de problemas totalmente diferentes y las características particulares de cada país, lo que los enriquece con sus propias experiencias.

En el caso de Argentina, las definiciones "cerradas" o las políticas multinacionales sobre seguridad no se han aplicado directamente debido a que los sistemas industriales implementados en el país son obsoletos (no todos ellos), híbridos o se han desarrollado localmente. La política económica ha impulsado el desarrollo de sistemas de control y monitoreo industrial, sin embargo, los desarrollos locales no siempre se han aplicado al mismo "paquete de políticas" creado para otras plataformas. En este contexto, y de acuerdo con la idea de proyectos de hardware abierto como el de Raspberry-Pi, Argentina dio a conocer un proyecto denominado CIAA, (Computadora Industrial Abierta Argentina)[9]. A través de este proyecto se busca proporcionar computadoras que puedan trabajar en tiempo real y que puedan utilizarse en los sistemas industriales de las pequeñas y medianas empresas (PyMEs) de ese país, pues estas empresas no tienen la capacidad de adquirir marcas internacionales, las cuales también son escasas. Por su parte, las instituciones educativas como las universidades también pueden utilizar estas computadoras.

9 http://www.proyecto-ciaa.com.ar

En cuanto al contexto político en torno a este tema, Argentina creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)[10], cuyo objetivo es "…impulsar la creación y la adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones".

Este programa del gobierno nacional realiza tareas para sustituir y monitorear las infraestructuras críticas del país. Desafortunadamente, la integración de las organizaciones del sector público y privado a este marco de control establecido por el ICIC es voluntario y no obligatorio, por lo que su evolución no ha sido tan rápida o ágil como se esperaba. Sin embargo, con el apoyo y la convicción de quienes apoyan este tema, se han realizado acciones periódicas que incluyen la capacitación sobre la ciberseguridad industrial para los representantes de las compañías miembro, así como ejercicios a escala nacional para responder a los incidentes cibernéticos (Programa ENRIC), y en el que se involucran representantes del gobierno como las fuerzas de seguridad o el CERT.

Por otro lado, Colombia fue el primer país de la región en tomar muy en serio este tema, y ha captado la atención mundial. Pero aunque esta información podría ser curiosa no lo es, debido a que Colombia ha estado luchando contra las Fuerzas Armadas Revolucionarias de Colombia (FARC) durante varias décadas, una lucha que hace que las Fuerzas Militares y la Policía, en coordinación con el sector privado, defiendan y protejan la infraestructura crítica física y virtual del país. Por tanto, en la etapa final de su Política Nacional de Ciberseguridad y Ciberdefensa (CONPES 3701/2011), se han formado grupos de trabajo y se incluyen a las Instituciones del Gobierno Nacional (Ministerio de Defensa Nacional, MINTIC, la Policía Nacional, etc.) y a las organizaciones del sector privado (representantes de los sectores de energía y comunicaciones, administradores de los dominios .co, universidades, etc.) para crear un marco serio y coordinado que busca proteger las infraestructuras críticas del país.

Su implementación será liderada por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) con la ayuda del sector privado español. ColCERT identificará, dará prioridad y clasificará la infraestructura crítica del país. También servirá como la plataforma informática que clasifique la infraestructura crítica y que conecte a las organizaciones de seguridad nacional para que puedan brindar una protección efectiva. Finalmente, se hará cargo de la planeación y creación de una Estrategia Nacional de Defensa de la Infraestructura Crítica.

Brasil, el país más grande de América Latina, también es el más digitalizado, y ha hecho la mayor inversión en TI de la región. También es el cuarto país con el mayor número de usuarios de Internet del mundo con más de 100 millones de personas conectadas a Internet, gracias a los incentivos del gobierno. La presidencia de la República aprobó el Marco Civil de Internet en abril de 2014, el cual plantea las reglas, los derechos y las obligaciones del uso de Internet, así como la protección de los datos.

Las organizaciones privadas y estatales han incluido a la ciberseguridad en su agenda desde la planeación de la Copa Mundial FIFA 2014, y se están preparando para organizar los Juegos Olímpicos de 2016 en Río de Janeiro. Desde entonces se han estado organizando eventos sobre SCADA y seguridad en dicha ciudad.

10 www.icic.gob.ar

De acuerdo con distintos reportes, los ejecutivos brasileños creen que la mayoría de los incidentes de ciberseguridad son causados por los hackers, los competidores, los ciberactivistas y los empleados, actuales y antiguos. El número de incidentes de seguridad industrial están creciendo considerablemente – tan sólo los incidentes en Brasil están aumentando en cantidad, gravedad y sofisticación. Desde el hacktivismo de LulzSec y LulzSecBrasil en 2014, los sitios del Ministerio del Deporte, el Ministerio de Asuntos Exteriores y la Presidencia han sido blancos de ataques distribuidos de negación de servicio (DDoS). También fue robada información sobre puestos públicos. Debido a las noticias frecuentes sobre corrupción e inestabilidad social y política, podemos esperar un año plagado de incidentes de ciberseguridad, especialmente de incidentes relacionados con la ciberseguridad industrial.

Los datos de Brasil, Chile y México revelan que la mayoría de las vulnerabilidades se relacionan con las configuraciones erróneas de los sistemas, seguidas por versiones obsoletas y problemas con las aplicaciones.

Además de las iniciativas individuales de cada país de la región, Perú y Chile, entre otros, han estado realizando un trabajo muy interesante en materia de ciberseguridad. Organizaciones como la Unión de Naciones Suramericanas (UNASUR)[11] y los Estados Miembros han incluido a la ciberseguridad y a la ciberdefensa en su agenda. De igual manera, han organizado también conferencias militares en distintas ciudades, y han analizado alianzas e iniciativas de cooperación. Sin embargo, más allá del trabajo que haya realizado cada país o las organizaciones, no hay información oficial sobre los incidentes de seguridad en los sistemas industriales o las infraestructuras críticas de la región.

Evolución de los incidentes

La mitad de las compañías de América Latina y del Caribe sufrieron ataques en los años recientes, al igual que las instituciones gubernamentales, las administraciones y las organizaciones políticas. Y los ataques siguen al alza.

Argentina es uno de los países con la actividad criminal cibernética más alta del mundo. Las amenazas cibernéticas en Colombia también son numerosas pues casi la mitad de los ataques de phishing en América Latina ocurren en este país. Estos ciberataques incluyen los fraudes, los ataques dirigidos, el secuestro de computadoras, el hacktivismo, el robo de información pública y privada y de identidad (especialmente en el sector financiero), el terrorismo y la guerra y el espionaje militar. Los ciberataques en la región incluyen también ataques de alto perfil y robo de identidad, similar a lo que sucedió con el correo electrónico del Presidente Santos, que tuvo una gran repercusión en los medios.

A escala global, las dos principales tendencias en el crimen cibernético son el fraude con motivaciones económicas, y los ataques contra la confidencialidad, la integridad y la disponibilidad.

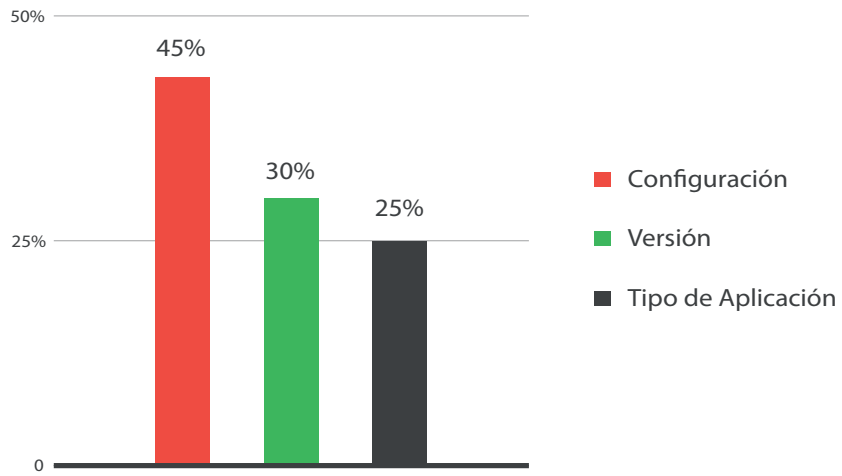
Vulnerabilidades

El aumento de los ataques dirigidos, en particular los ataques dirigidos a los sectores o infraestructuras que brindan servicios críticos para la sociedad y el Estado, fomenta el crecimiento de los servicios de detección de vulnerabilidades. Se hace esto para ayudar a establecer prioridades, solucionar los problemas de seguridad y cumplimiento para prevenir ataques, y facilitar la implementación de políticas y estrategias adecuadas en cada caso.

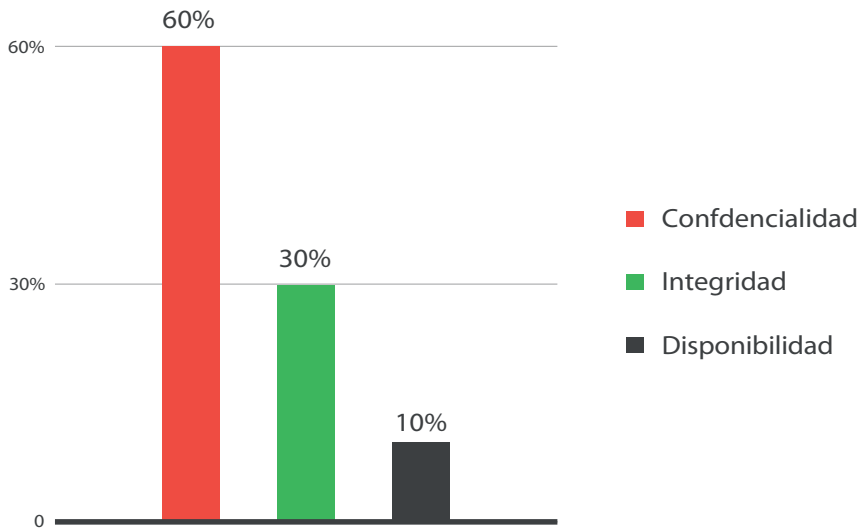
Los datos de Brasil, Chile y México revelan que la mayoría de las vulnerabilidades se relacionan con las configuraciones erróneas de los sistemas, seguidas por versiones obsoletas y problemas con las aplicaciones. Sin embargo, esos problemas se asocian con un nivel de riesgo más alto.

60% de las vulnerabilidades que dejan al descubierto los agujeros podrían afectar a la confidencialidad de la información. En tanto, 30% de las vulnerabilidades representan una amenaza para la integridad, mientras que 10% de las vulnerabilidades son debilidades que pueden aprovechar los ataques contra la disponibilidad de la información y de los servicios.

11 http://www.unasurs.org/node/13



Tipos de vulnerabilidades



Alcance de la vulnerabilidad

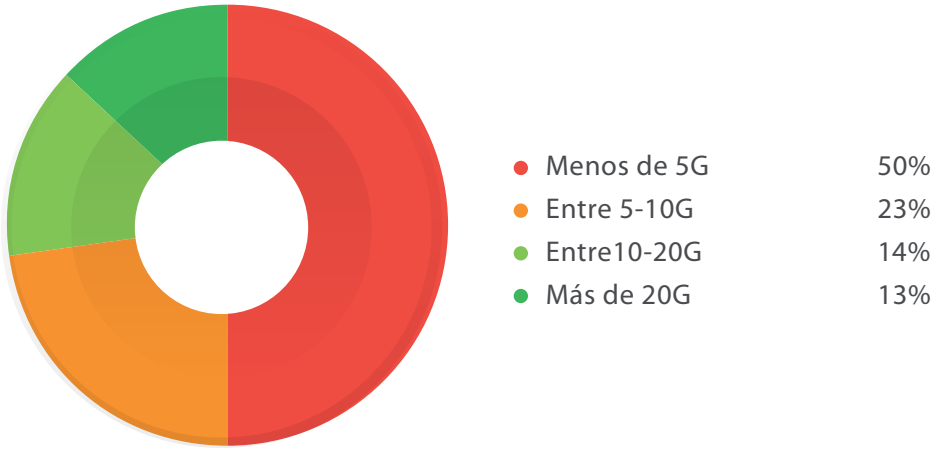
Distributed Denial of Service (DDoS)

Los ataques "DDoS-for-hire" y los ataques de reflexión y de múltiples vectores son una tendencia que aumenta en cuanto al número y volumen de los incidentes. Las víctimas de estos ataques incluyen a proveedores de servicios financieros, compañías de comercio electrónico, instituciones gubernamentales, medios digitales, centros de datos, etc.

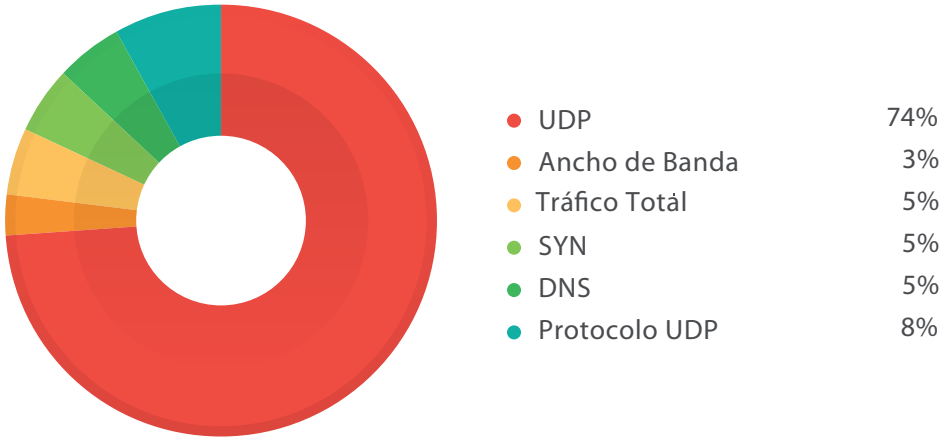
En Chile, una sola víctima sufrió hasta 35 ataques DDoS en un mes durante 2014. 50% de los ataques observados tuvieron un ancho de banda menor a los 5Gbps; mientras que 25% de los ataques tuvieron anchos de banda entre 5 y 10Gbps; y el 25% restante incluyó accidentes con volúmenes entre 10 y 20Gbps. Los ataques más frecuentes tuvieron anchos de banda superiores a 20Gbps. Los ataques de 50Gbps son cada vez más comunes. La información es similar al resto de los países de la región.

La mayoría de los ataques con un volumen más alto que utilizaron el protocolo UDP se dirigieron a los puertos NTP, DNS, SNMP, HTTP y HTTPS, lo que implica el uso potencial de mecanismos de reflexión/amplificación para crear tráfico.

También se ha observado un aumento importante en el volumen de ataques contra SSL/TLS.



Tipos de ataques "UDP": ataques de inundación usando el protocolo UDP.



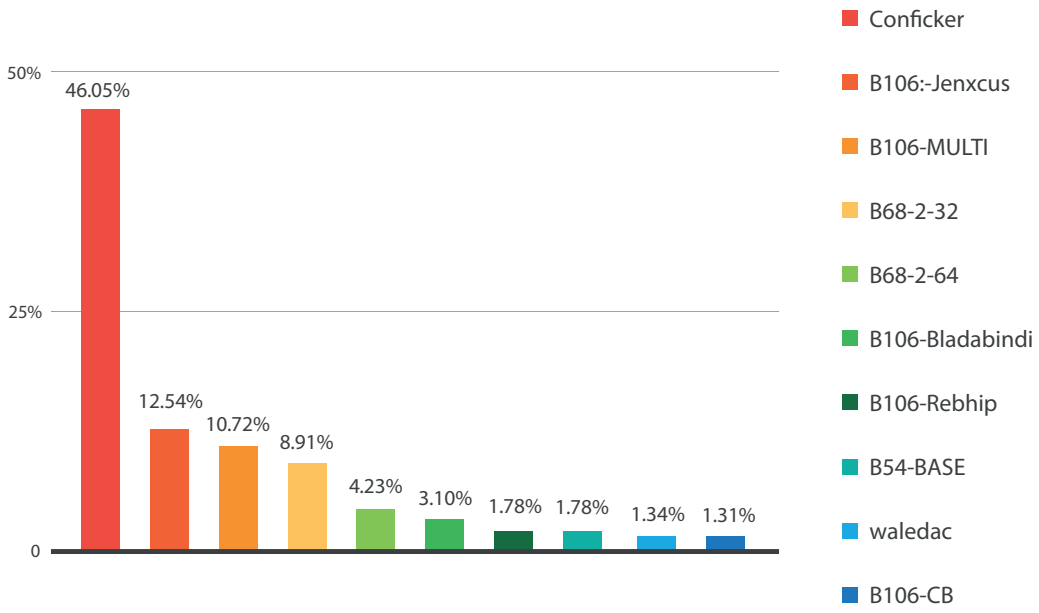
Tipos de ataques del "Protocolo UDP": ataques que utilizan las anomalías del protocolo UDP

Spam y malware

El robo de información confidencial sigue siendo la principal motivación para quienes utilizan el correo electrónico para propagar amenazas. También los medios sociales siguen siendo el medio perfecto para esta categoría de cibercrimen.

Por su parte, el fraude contra las instituciones financieras utiliza el spam para ocultar el phishing, el malware y el robo de datos. De acuerdo con los proveedores de servicios y contenido brasileños, cerca de dos millones de correos electrónicos basura son enviados diariamente, de los cuales un porcentaje importante se hacen pasar por notificaciones de tarjetas de crédito.

De acuerdo con información acerca del malware en la región de habla hispana, se reportan alrededor de 1.5 millones de intentos de conexión desde las computadoras infectadas a sus respectivos C&Cs. De igual manera, se identifican alrededor de 10,000 IPs diariamente, y se infectan 7,000 diferentes IPs a la semana con malware, lo que corresponde a la actividad de cerca de 50 botnets diferentes, incluyendo a DOWNAD/Conficker[12], ZACCESS/ZeroAccess[13] y la familia de malware B106[14].



Información sobre la principal actividad del malware a febrero de 2015

Conficker: *Gusano botnet,* ***B106:*** *Robo de identidad/ fraude financiero/ invasión de la privacidad,* ***B68: ZeroAccess: p****ublicidad/ fraude de clics,* ***B54: Citadel:*** *robo de identidad/ fraude financiero,* ***Waledac:*** *Spam.*

Todos estos indicadores apuntan hacia la consolidación de la idea de que la ciberseguridad es una necesidad apremiante para la alta administración de las organizaciones públicas y privadas así como para los ciudadanos en general de los países.

Capacidades y retos

Argentina

El sector de las TICs de Argentina contribuye de manera importante al PIB, alrededor de 4.5% y su crecimiento continúa; este país es el tercero que más apoya a este sector, junto con Brasil y México. Los sectores público y privado habrían invertido €7,400 millones en las TIC tan sólo en 2013.

La ciberseguridad de las infraestructuras críticas padece de una colaboración limitada entre los sectores público y privado, regulaciones específicas insuficientes y de la carencia de una mejor conciencia entre algunos profesionales del sector, para quienes la ciberseguridad sirve únicamente para proteger sus redes SCADA (Primera Conferencia de Concientización para la Protección de Infraestructuras Críticas y Ciberseguridad, octubre 2012).

12 http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_downad
13 http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/rtkt_zaccess
14 https://csirt.cesnet.cz/_media/cs/services/x4/botnet_b106.pdf

Los retos más relevantes son los que se relacionan con la toma de decisiones y la adopción de medidas organizacionales, además de reforzar la coordinación de todas las organizaciones públicas, y entre éstas y el sector privado.

Brasil

"Tanto los gobiernos como las empresas deben promover una cultura de ciberseguridad en todos los niveles que propicie la prevención de las amenazas. La colaboración internacional y nacional entre los sectores público y privado juega un papel vital para el fortalecimiento de los marcos de ciberseguridad nacionales."

El PIB del sector de las TIC brasileño creció 5.3% en 2013 en comparación con el año anterior, lo que representa el crecimiento más alto desde 2008. En 2013, la facturación de las ITC en Brasil creció alrededor de 30% a €103,000 millones. Gran parte del gasto en investigación y desarrollo de América Latina se presenta en Brasil. Además, Brasil es el primer país de la región, y el séptimo del mundo, que más invierte en las ITC; la inversión alcanzó los €48,200 millones en 2013.

La seguridad es una de las prioridades de la Estrategia de Defensa Nacional. Este documento es de carácter inclusivo, y no cubre solamente las cuestiones militares sino también la protección de las infraestructuras críticas del espacio, ITC y las industrias nucleares, y busca reducir la dependencia de otros países. Brasil cuenta con una amplia red de centros de alerta temprana y equipos de respuesta contra incidentes de seguridad.

Los desafíos que enfrenta Brasil pueden clasificarse en tres categorías: Presupuestos para la investigación, el desarrollo y la innovación (I&D&I); organización y control de los actuales sistemas de ciberseguridad; y la reducción de la dependencia de países extranjeros en cuanto a los suministros y adquisiciones.

Colombia

Los ingresos del sector de las ITC de Colombia alcanzaron los €14,000 millones en 2012, 6% del PIB con un crecimiento anual de 9%. La industria de las ITC creó 110,000 empleos directos y reporta un crecimiento superior al de otros sectores. La inversión en el sector de las ITC alcanzó los €5,900 millones de euros en 2013, por lo que Colombia se coloca como el cuarto país de América Latina después de Brasil, México y Argentina.

El plan de ciberseguridad será la hoja de ruta para la administración y se aplicará a las infraestructuras críticas y al sector privado; sus aspectos más importantes incluyen: una estructura de doble defensa y ciberseguridad contra las amenazas externas e internas, el crecimiento de los recursos tecnológicos; revisión y endurecimiento del actual marco regulatorio; y el reforzamiento de las capacidades de inteligencia, tanto técnicas como humanas.

Colombia enfrenta varios desafíos: educativos, para promover y consolidar una cultura de la ciberseguridad en todos los ámbitos; y regulatorios, para establecer un marco claro que se adecue a la realidad del país y sus recursos críticos, con la capacidad de verificar el cumplimiento.

Conclusión

Tanto los gobiernos como las empresas deben promover una cultura de ciberseguridad en todos los niveles que propicie la prevención de las amenazas. La colaboración internacional y nacional entre los sectores público y privado juega un papel vital para el fortalecimiento de los marcos de ciberseguridad nacionales. Es necesario realizar más trabajo legislativo y regulatorio si se desea ver un progreso. El intercambio de información y la respuesta operativa también deben ser determinantes.

Resultados de la Encuesta de los Países de la OEA

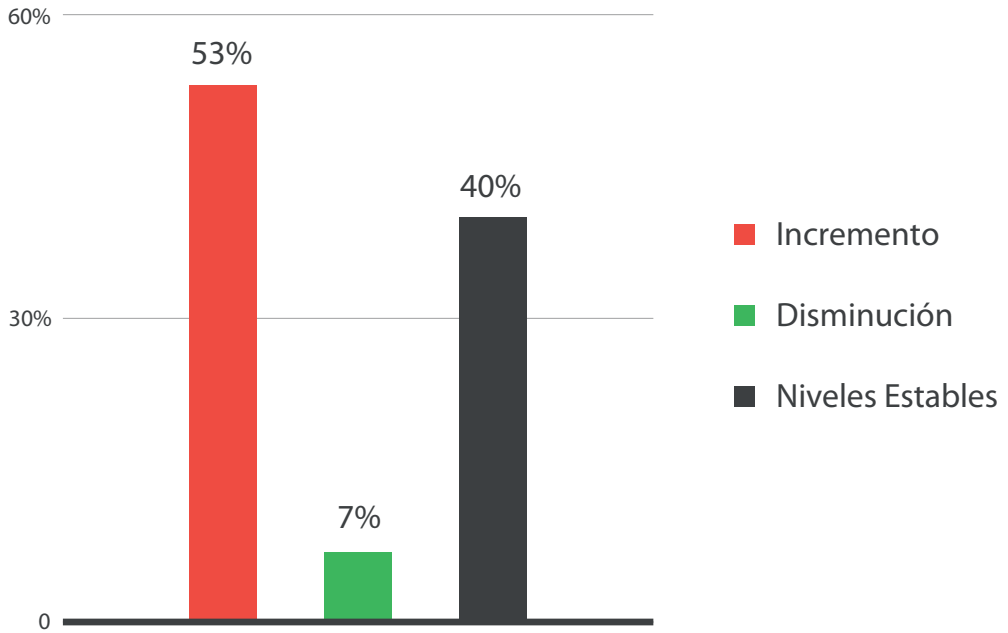
Esta sección da cuenta de los factores más destacados y analiza las respuestas de la encuesta que ofrecieron los Estados Miembros a las preguntas sobre ciberseguri-dad, ataques, preparación y la infraestructura crítica.

La OEA y Trend Micro realizaron una encuesta cuantitativa en línea en enero de 2015 entre los Jefes de Seguridad de las principales infraestructuras críticas de los Estados Miembros en todos los países de América. Asimismo, se incluyeron organi-zaciones privadas que gestionan la infraestructura crítica en sus países. El objetivo de la encuesta es darnos una visión del estado de la seguridad de la infraestructura crítica dentro de estos Estados Miembros para ayudarnos a identificar las fortalezas y las debilidades que deben reforzarse.

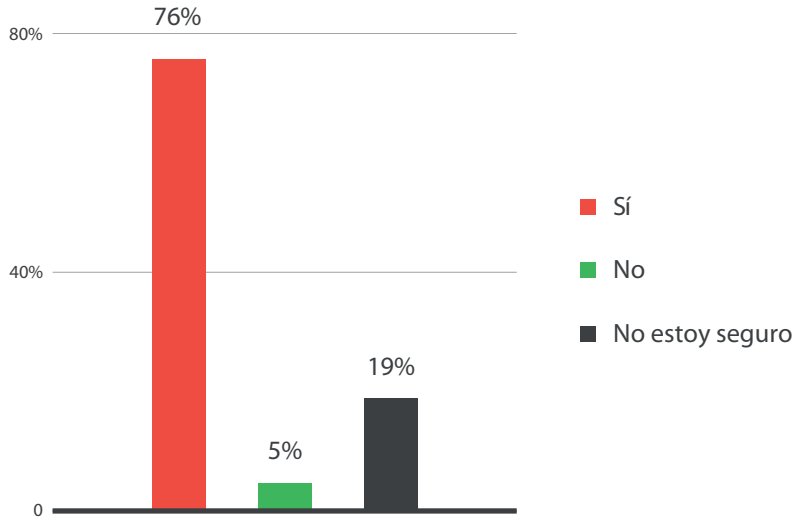
La primera parte de la encuesta evalúa el estado del panorama de las amenazas en estas regiones y cómo se perpetran los ataques prevalentes y sofisticados.

Nivel de Incidentes en el Sistema de Cómputo durante el año pasado

¿Ha observado un incremento, disminución o un nivel estable de los incidentes en sus sistemas de cómputo durante al año pasado?



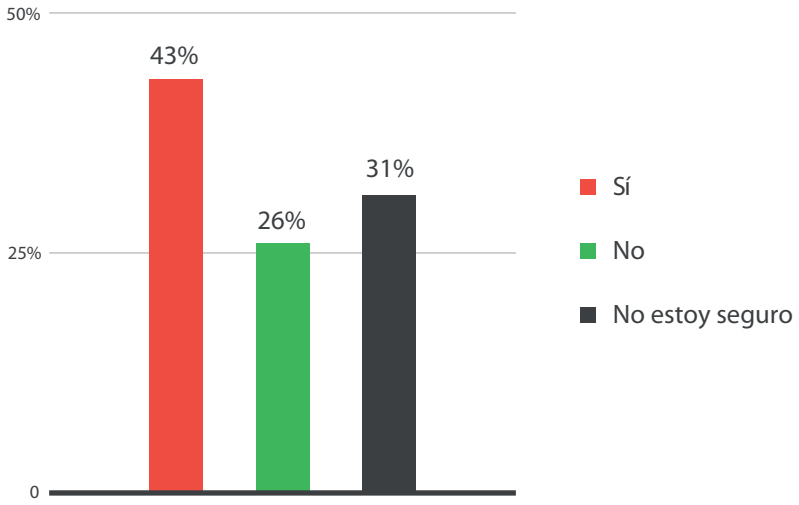
¿Los incidentes contra las infraestructuras se están volviendo más sofisticados?



Los resultados mostrados anteriormente indican que los incidentes están a aumentando o se están volviendo más sofisticados ya que los creadores de amenazas podrían estar apuntando a infraestructuras críticas más vulnerables en el futuro. Estos resultados indicarían la necesidad de establecer mejores protecciones así como mejores procesos de respuesta a incidentes en las regiones para asegurar la reducción efectiva de futuros ataques. Ya que sólo 5% de los encuestados dijeron que los ataques no se están volviendo más sofisticados, esto nos dice que los atacantes están esforzándose por entender cómo comprometer la infraestructura crítica y la necesidad de mejorar las herramientas y técnicas que utilizan en los ataques. Estamos observando un fenómeno similar con los ataques a los sistemas de punto de venta (PoS) que ocurrieron en los Estados Unidos el año pasado.

Ataques a la Infraestructura

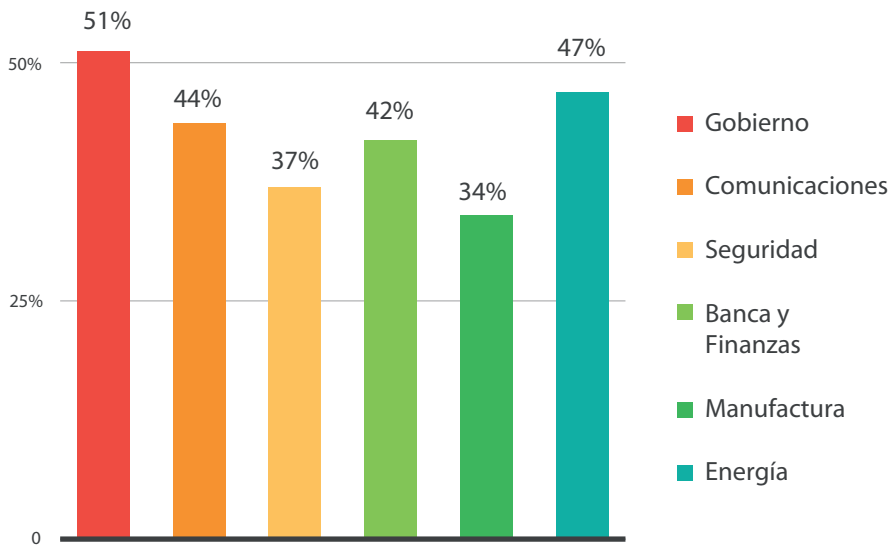
¿Ha detectado algún ataque/incidente/instrucciones dirigido específicamente a la infraestructura que su organización opera/mantiene/administra?



Los datos anteriores muestran un incremento específico de los ataques a la infraestructura crítica (43%) mientras que un alarmante 31% dijo que no estaban seguros de haber sido atacados. Sin duda, un desafío importante al día de hoy es la sofisticación de los ataques (76% dicen que se están volviendo más sofisticados) los cuales son difíciles de detectar. Ya que casi una tercera parte de los encuestados entran en esta categoría, es evidente que se requieren controles de monitoreo continuo en la mayoría de las organizaciones para que éstas puedan advertir mejor la presencia de los atacantes en sus redes.

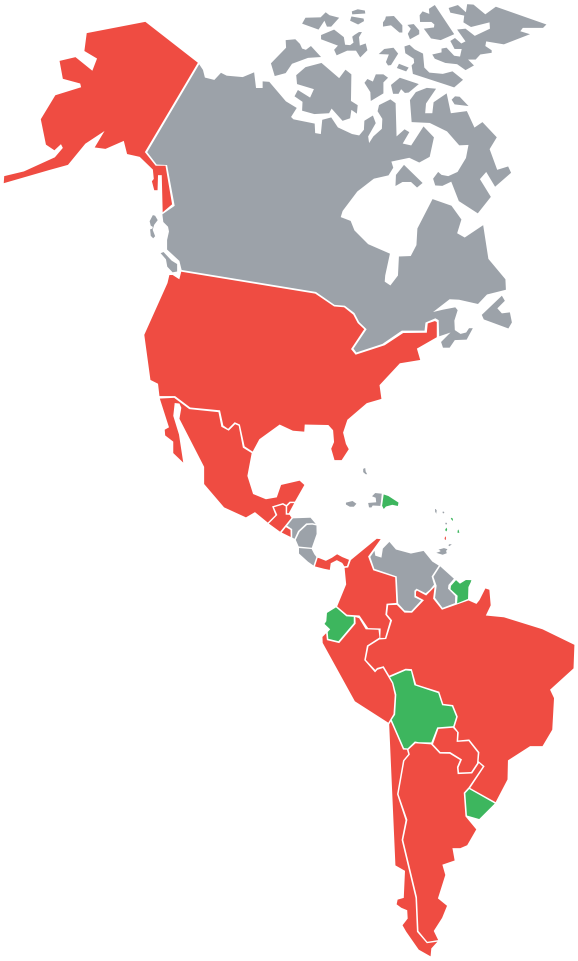
Experiencia con Varios Incidentes

Porcentaje de Organizaciones que experimentaron intentos de eliminar o destruir información por tipo



De acuerdo con los resultados de la encuesta, los sectores de gobierno y energía son las dos principales industrias que sufren ataques destructivos por amenazas, seguidos por los de comunicaciones y de banca y finanzas.

Las Instituciones Gubernamentales que experimentaron intentos de manipulación de su equipo a través de una red/sistema de control por País



SÍ

Argentina
Belice
Brasil
Chile
Colombia
El Salvador
Granada
Guatemala
México
Panamá
Paraguay
Perú
Estados Unidos

NO

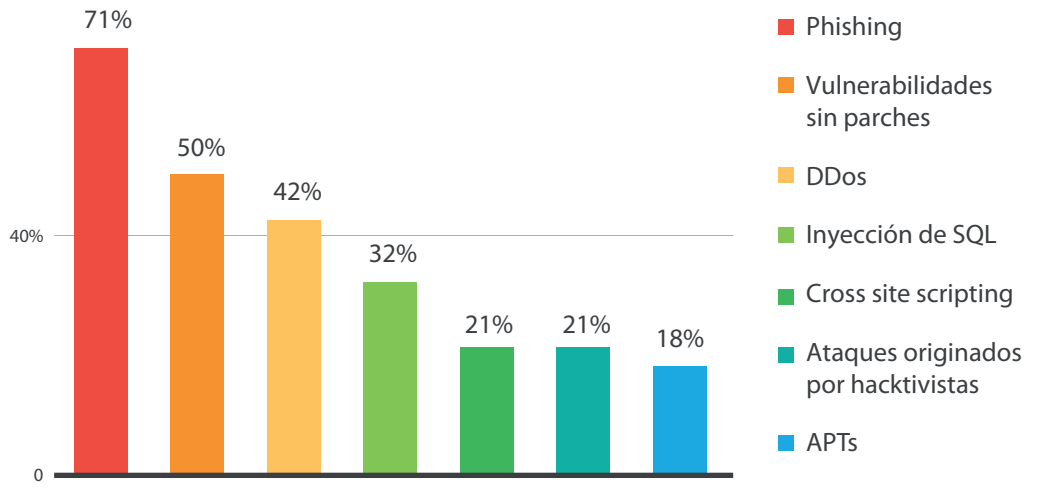
Barbados
Bolivia
Mancomunidad de Dominica
República Dominicana
Ecuador
San Vicente y las Granadinas
Surinam
Uruguay

NO PARTICIPÓ/NO HAY RESPUESTA

La mayoría de las regiones en las que se aplicó la encuesta indicaron que su equipo ICS/SCADA estaba siendo atacado, lo que revela una gran cantidad de actividad por parte de los creadores de amenazas. Si bien muchos de estos ataques podrían ser para reunir inteligencia sobre sus objetivos, se puede prever que más regiones reportarán esto en el futuro conforme sus infraestructuras críticas se vuelvan más conectadas o mejoren su capacidad de identificar la presencia de un ataque.

Tipos de Métodos para Ataques Cibernéticos

¿Qué tipo de ataques cibernéticos se han utilizado contra su organización?



A partir de los resultados anteriores, podemos observar que la mayoría de las regiones están enfrentando ataques de phishing contra sus organizaciones.

Actualmente es el phishing la primera amenaza que se utiliza en los ataques dirigidos y podría ser un indicador del estado real de las actividades relacionadas con los ataques dirigidos aunque esta fue la amenaza más baja señalada en los resultados de la lista anterior. Esto también indicaría que los intentos iniciales de los atacantes es penetrar en una organización para tratar de moverse lateralmente a otros sistemas, como sus dispositivos ICS/SCADA.

Los criminales cibernéticos a menudo utilizan vulnerabilidades que no tienen parche en sus rutinas de infección pues reconocen que la aplicación de parches es un proceso difícil para muchas organizaciones. Asimismo, muchos dispositivos de la infraestructura crítica utilizan versiones antiguas de los sistemas operativos y de las aplicaciones, y son más propensos a ser vulnerables ya que muchas ya no reciben soporte.

Como lo vimos anteriormente, los ataques se están volviendo más prevalentes y sofisticados, lo que exigirá que las organizaciones estén mejor preparadas. Enseguida, le pedimos a las regiones identificar si están preparadas actualmente en caso de que sufrieran un ataque.

Percepción de la Preparación para los Incidentes Cibernéticos

¿Cuán preparada está su organización para un incidente cibernético?

NO PREPARADA

Dominica
Ecuador
El Salvador
Granada
Nicaragua

ALGO PREPARDA

Argentina
Barbados
Belice
Brasil
Colombia
Costa Rica
Guatemala
México
Panamá
Paraguay
Perú
San Vicente y las Granadinas
Estados Unidos
Uruguay

PREPARADA

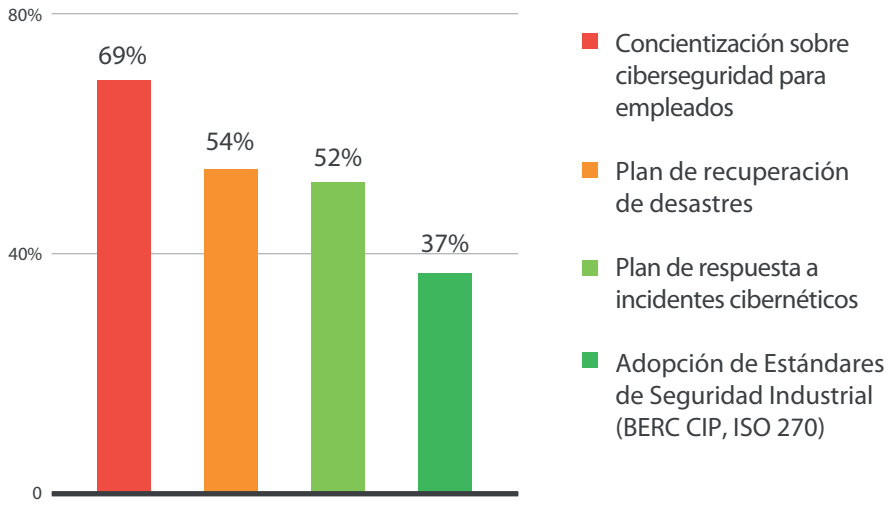
Chile
República Dominicana

NO PARTICIPÓ/
NO HAY RESPUESTA

La mayoría de los países consideran que están algo preparados para un incidente cibernético, lo cual es una buena noticia, pero los resultados de la siguiente encuesta sugieren que el esfuerzo por mejorar su preparación podría ser más complicado de lo que parece. Asimismo, el aumento en el número y sofisticación de los ataques significa que los países que no están preparados o que están algo preparados deben considerar de inmediato mejorar sus capacidades de detección, protección y respuesta.

Políticas de Ciberseguridad

¿Su organización tiene políticas y/o planes de ciberseguridad?



La preparación comienza con un plan, y si únicamente poco más de la mitad (52%) de los encuestados dijeron tener un plan de respuesta a los incidentes cibernéticos, no es un buen presagio si ocurriera un incidente. No se han implementado los controles industriales (ICS/SCADA) con las medidas de seguridad necesarias y por tanto muchas regiones han añadido regulaciones y estándares para éstos. Únicamente 37% de las organizaciones han adoptado esos estándares, lo que incrementa el riesgo de comprometer sus dispositivos.

Presupuesto para la Ciberseguridad

Las Instituciones de gobierno cuyo presupuesto para la ciberseguridad aumentó en el último año

NO HA AUMENTADO

Argentina
Barbados
Brasil
Colombia
Mancomunidad de Dominica
Ecuador
El Salvador
Granada
Guatemala
México
Nicaragua
Panamá
Paraguay
Perú
Estados Unidos

HA AUMENTADO

Belice
Chile
República Dominicana
Uruguay

NO ESTÁ SEGURO

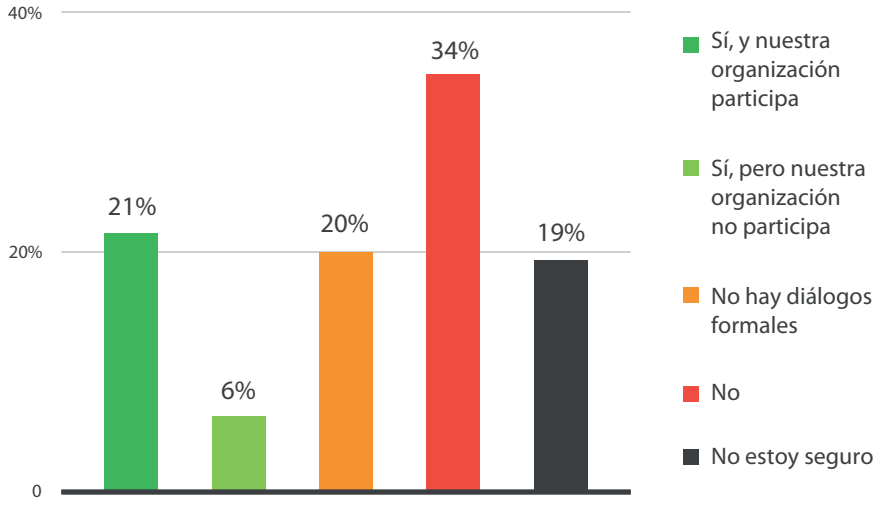
Costa Rica
San Vicente y las Granadinas

NO PARTICIPÓ/
NO HAY RESPUESTA

Ya que más de la mitad de los encuestados dijo que sus presupuestos no han aumentado en el último año, la capacidad de detectar intrusiones se verá seriamente comprometida pues la mayoría de los ataques de hoy no pueden descubrirse utilizando las medidas de seguridad tradicionales. Los sistemas utilizados para detectar las brechas pueden ayudar a mejorar esta tarea, pero hemos visto que éstos requieren de un presupuesto adicional para implementarse.

Discusión con el Gobierno acerca de resistencia cibernética de los Sistemas de Infraestructura Crítica

¿Hay una discusión/diálogo con el gobierno sobre la resistencia cibernética de los sistemas de infraestructura crítica?

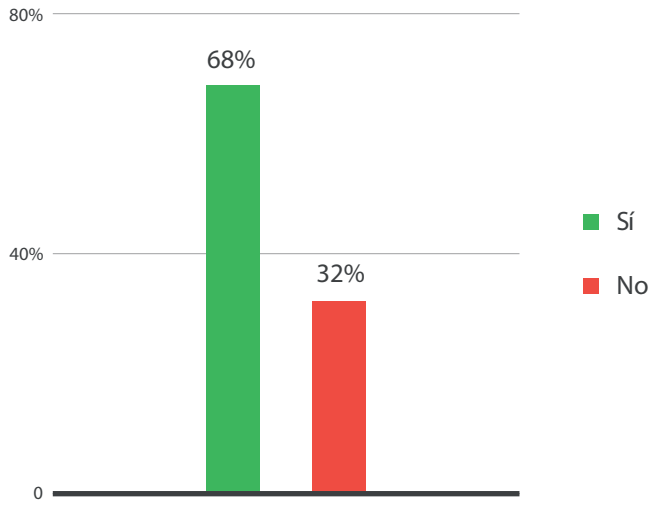


Ya que la infraestructura crítica afecta a todos en una región, las Asociaciones Público-Privadas (PPPs) son vitales para la gestión adecuada de la amenaza asociada a sus creadores que buscan comprometer estos sistemas. Ya que únicamente uno de cada cinco encuestados (21%) dijo que existía un diálogo activo, aún deben hacerse mejoras para enfrentar efectivamente a una amenaza.

Si los encuestados confían en el Gobierno para impulsar una Agenda de Ciberseguridad en las Industrias de Infraestructura Crítica

La buena noticia es que la mayoría de los encuestados (68%) aseguran que confían en que su gobierno apoye los avances para enfrentar la amenaza. Esto podría indicar que la barrera para tener un mejor diálogo está más baja de lo que parecía, y simplemente se requiere que las organizaciones públicas y privadas se pongan en contacto e inicien el proceso.

¿Confía en que el gobierno impulse una agenda de ciberseguridad en las industrias de infraestructura crítica? ¿Está dispuesto a trabajar con ellos?



Análisis Global de la Inteligencia de Amenazas de Trend Micro

Malware

En 2014, América fue afectada por diferentes tipos de malware, y cada uno de ellos tenía distintas características que podrían ayudar a los potenciales atacantes a llevar a cabo sus explotaciones. Estas van desde gusanos (DUNIHI y DOWNAD/Conficker), troyanos (AGENT y FAKEAV) explotaciones de navegadores (CONDUIT, SAFNUT y CROSSRDR) hasta herramientas de hackeo/rompimiento de aplicaciones (KEYGEN, ACTIVATOR y PRODUKEY). Como se ha observado en los últimos años, los dispositivos de almacenamiento removibles que no están lo suficientemente asegurados, los sistemas operativos y/o aplicaciones sin parches, y el comportamiento indiscriminado de los usuarios en línea son algunos de los factores determinantes que ponen en riesgo a los usuarios y organizaciones.

Las Principales Familias de Malware de 2014

FAMILIA DE MALWARE	DESCRIPCIÓN
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente.
DUNIHI	Esta familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades removibles; puede llegar como un archivo anexo del correo no deseado.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla manualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afectado. Esta herramienta de hackeo puede ser instalada manualmente por el usuario.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosas, que van desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectados podrían requerirse procedimientos además del análisis con un programa antivirus.
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Principales Familias de Malware en América por Trimestre

1Q	2Q	3Q	4Q
DUNIHI	DUNIHI	KEYGEN	KEYGEN
DOWNAD	KEYGEN	ACTIVATOR	VOBFUS
KEYGEN	VOBFUS	CONDUIT	ACTIVATOR
PASSVIEW	PRODUKEY	SAFNUT	DUNIHI
VOBFUS	DOWNAD	DOWNWARE	PRODUKEY
FAKEAV	FAKEAV	DUNIHI	DOWNAD
PRODKEY	ACTIVATOR	CROSSRDR	UPATRE
PRODUKEY	PRODKEY	NIXAX	KULUOZ
VARNEP	EXPLOIT	AGENT	CONDUIT
FORUCON	CHECK	KILIM	AGENT

Spam

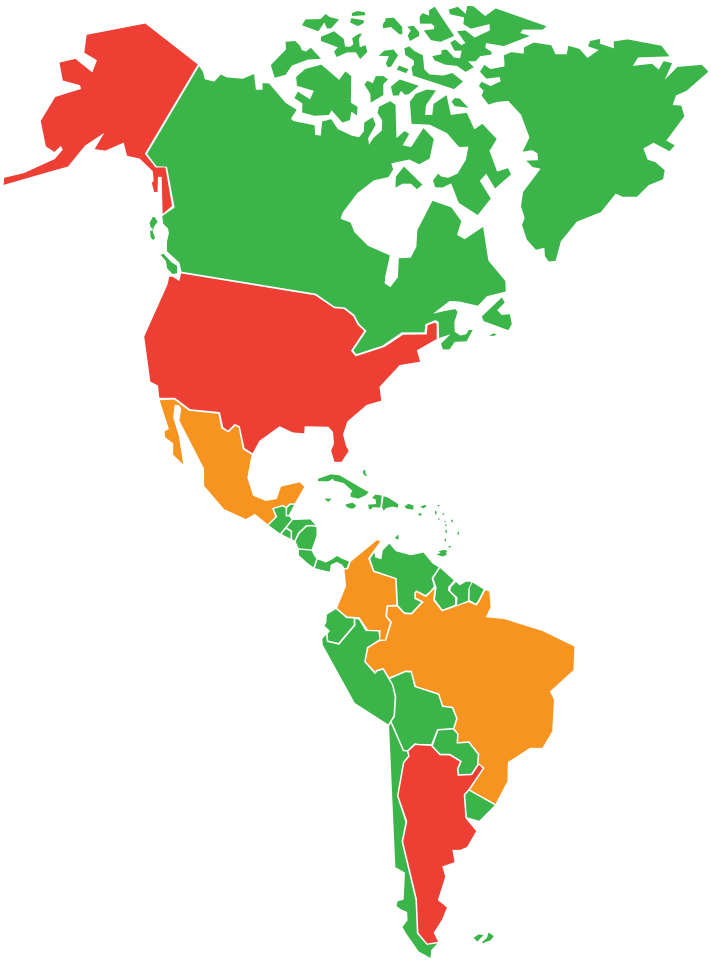
En los dos últimos años se ha incrementado el volumen del spam en todo el mundo.[15,16] Este aumento puede atribuirse a la prevalencia del malware como los programas para descargar troyanos, que normalmente entran a las computadoras como archivos adjuntos de los correos electrónicos que son enviados por los botnets. A pesar de este aumento, el correo electrónico como un vector de infección sigue a la baja. Esto podría ser debido a que los criminales cibernéticos siguen explorando y explotando otros vectores de infección como los sitios de las redes sociales y los dispositivos móviles.

Como lo muestran estos datos, entre los países de América, Estados Unidos representa más de una cuarta parte de número total de mensajes basura enviados en 2014. Argentina le sigue muy de cerca, mientras que Colombia, Brasil y México encabezan la lista de países que envían spam en 2014. Estos países representan más de 75% del número total en América.

15 http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/

16 http://blog.trendmicro.com/trendlabs-security-intelligence/1h-2014-spam-attacks-and-trends/

Países que más envían spam



> 20%

Argentina
Estados Unidos

10-20%

Brasil
Colombia
México

< 10%

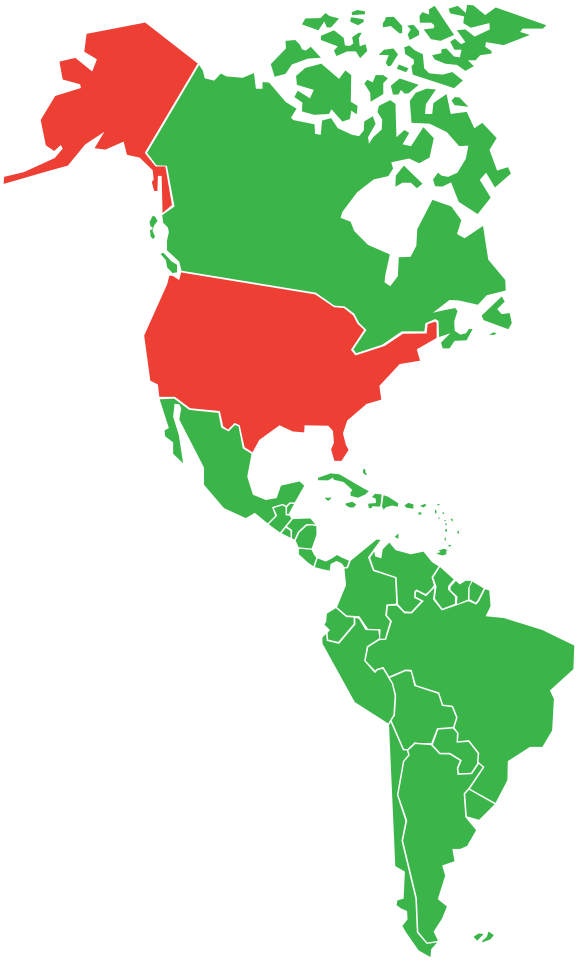
Anguilla
Antigua y Barbuda
Aruba
Bahamas
Barbados
Belice
Bermuda
Bolivia
Canadá
Islas Caimán
Chile
Costa Rica
Dominica
Republica Dominicana
Ecuador
El Salvador
Islas Malvinas
Guyana Francesa
Groenlandia
Granada
Guadalupe
Guatemala
Guyana
Haití
Honduras
Jamaica
Martinica
Montserrat
Nicaragua
Nicaragua
Panamá
Paraguay
Perú
Puerto Rico
San Cristóbal y Nieves
Santa Lucía
San Martín
San Pedro y Miquelón
San Vincente y las Granadinas
Surinam
Trinidad y Tobago
Islas Turcas y Caicos
Uruguay
Venezuela
Islas Vírgenes Británicas
Islas Vírgenes de Estados Unidos

Sitios Maliciosos y de Phishing

Los sitios maliciosos, como aquellos conocidos como watering holes (abrevaderos), hospedados en América siguen siendo una epidemia. Entre los países que se analizan en este reporte, Estados Unidos no sólo encabezó la lista sino también tuvo el nivel más alto de tráfico hacia sitios maliciosos. Estos sitios maliciosos son considerados vectores de trastornos. Estos URLs normalmente están vinculados a mensajes basura y pueden descargar otras amenazas como malware en los sistemas afectados cuando tienen acceso a ellos.

Así mismo, Estados Unidos también superó a otros países de América en términos de phishing.

Países con los mayores niveles de Phishing



> 20%

Estados Unidos

< 10%

Brasil
Anguilla
Antigua y Barbuda
Argentina
Aruba
Bahamas
Barbados
Belice
Bolivia
Canadá
Islas Caimán
Chile
Colombia
Islas Cook
Costa Rica
Dominica
Republica Dominicana
Ecuador
El Salvador
Islas Malvinas
Guyana Francesa
Grenada
Guadalupe
Guatemala
Guyana
Haití
Honduras
Jamaica
Kiribati
Martinica
México
Montserrat
Antillas Holandesas
Nicaragua
Panamé
Paraguay
Perú
Puerto Rico
San Cristóbal y Nieves
Santa Lucía
San Vincente y las Granadinas
Islas Georgias del Sur y Sandwich del Sur
Trinidad y Tobago
Islas Turcas y Caicos
Uruguay
Venezuela
Islas Vírgenes Británicas
Islas Vírgenes de Estados Unidos

Actividad Clandestina

Amenazas Notables y Tendencias de las Amenazas

Estados Unidos fue víctima de ataques dirigidos y de brechas relacionadas con el malware PoS. Los atacantes robaron millones de datos de los clientes de tiendas, bancos, servicios públicos y varias organizaciones. Y más que pérdidas monetarias, el robo de datos en el país provocó un daño enorme a la marca y reputación de las organizaciones; por ejemplo, en Code Spaces el daño fue irreparable pues su sitio fue totalmente derribado, y el atacante logró borrar las bases de datos de los clientes y los respaldos del sitio.[17] P.F. Chang's tuvo que volver a utilizar dispositivos manuales para tomar la impresión de las tarjetas de crédito después de haber sufrido una brecha.[18] Target y Home Depot, por su parte, han sufrido las brechas de datos más grandes de la industria en términos del volumen de información de tarjetas de crédito robadas y gastos por demandas. Antes de que terminara el año, el ataque dirigido del que más se habló fue el realizado contra Sony Pictures. Probablemente este incidente demostró cuánto puede perder una compañía como consecuencia de una brecha de seguridad, incluso las compañías de la marca Sony han sido víctimas de ataques masivos. Se obligó a la compañía a cerrar temporalmente su red después de que fuera comprometida por los denominados Guardianes de la Paz (GOP).[19]

Por otro lado, el robo bancario en línea sigue siendo un problema serio en América Latina y el Caribe, pues los criminales cibernéticos siguen encontrando nuevas formas de infectar a los usuarios y socavar las medidas de seguridad. Un ejemplo de esto es el BANLOAD Trojan, una familia de troyanos bancarios que afecta en particular a los bancos brasileños.[20] En 2014 se descubrió que una variante de BANLOAD evitaba ser detectada y limitaba su propagación a otras regiones. Esto lo hacía al comprobar primero los plug-ins de seguridad específicos antes de intentar realizar sus rutinas maliciosas.

Otra táctica que se utiliza para comprometer las credenciales para la banca en línea es el uso de archivos maliciosos del panel de control (CPL).[21] En términos de análisis, si se observa un archivo CPL se podría advertir que es esencialmente idéntico a un archivo DLL. Sin embargo, a diferencia del último, se ejecuta automáticamente al dar doble clic. Esto lo hace similar a los archivos EXE; sin embargo, los usuarios no capacitados tienen más probabilidades de intentar ejecutar los archivos CPL.

También se han utilizado las extensiones maliciosas de los navegadores para infectar a los usuarios de la región.[22] En lugar de iniciar un archivo ejecutable, se instruye a los usuarios para que instalen una extensión maliciosa de un navegador, o se les engaña para que lo hagan, la cual, si se instala con éxito, secuestra las cuentas de redes sociales de las víctimas para enviar una copia de sí mismo.

17 http://www.networkcomputing.com/cloud-infrastructure/code-spaces-a-lesson-in-cloud-backup/a/d-id/1279116
18 http://www.usatoday.com/story/money/business/2014/08/04/pfchang-credit-debit-card-data-breach/13567795/
19 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf
20 http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/
21 http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-cpl-malware/

Clandestinidad Cibercriminal en América

Trend Micro sigue observando muy de cerca los mercados clandestinos en diferentes países del mundo.[22] En 2014, los investigadores de la compañía analizaron la economía subterránea brasileña,[23] que parecía estar madurando continuamente a pesar de la falta de desarrollo en las herramientas y las tácticas que ofrecen.

Algunos de los mercados clandestinos cibercriminales identificados poseen características únicas. Una de las cuales es el uso de plataformas populares de medios sociales para cometer fraudes en lugar de ocultarse en los profundos recovecos de la Web con herramientas a las que los usuarios ordinarios normalmente no tienen acceso. Los criminales cibernéticos de estas áreas utilizan medios populares, como son las redes sociales como Facebook, YouTube, Twitter, Skype y WhatsApp, pues éstas se han convertido en lugares efectivos.

En algunos casos los criminales son jugadores que comercializan generadores de números y verificadores o probadores para algo más que tarjetas de crédito. Ofrecen herramientas creadas para realizar ataques contra productos y servicios exclusivos de un país particular así como servicios de capacitación para aspirantes a convertirse en criminales cibernéticos. Entre los productos que se ofrecen, además de los troyanos bancarios, se incluyen credenciales de cuentas para las aplicaciones de negocio populares, páginas de phishing y listas de números telefónicos.

22 http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/

23 http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-underground-market-for-cybercriminal-wannabes

Casos Prácticos

Argentina

Con más 32.9 millones de usuarios de Internet, esto es más de 76% de la población total, y más de 22 millones de computadoras personales, la República de Argentina se encuentra entre los primeros países de la región en términos de adopción de las Tecnologías de Información y Comunicación (ITC).[24] Además, las conexiones móviles que incluyen computadoras y tabletas conectadas, así como teléfonos inteligentes y otros aparatos celulares con paquetes de servicio de datos o Wi-Fi gratuito han crecido a una tasa exponencial, llegando a 20 millones de conexiones a finales de 2014. Un componente importante de este rápido crecimiento ha sido el número de políticas y programas estatales como “Argentina Conectada” y “Conectar Igualdad”, que buscan elevar la conectividad del ancho de banda en todo el país y promover la inclusión digital entre los estudiantes y profesores de las escuelas públicas sin importar su condición socioeconómica. Ya que la sociedad Argentina se conecta cada vez más a Internet, se vuelve imperativo que los ciudadanos entiendan los riesgos que acompañan al hecho de que la información “sensible” circule, como características identificables, tarjetas de crédito, estados de cuenta bancarios y otro tipo de información personal.

Además del crecimiento de las ITC en la sociedad argentina, las instituciones gubernamentales también han digitalizado mucha de su infraestructura crítica. Por ejemplo, la Administración Nacional de la Seguridad Social (ANSES) y la Administración Federal de Ingresos Públicos (AFIP) han digitalizado muchos de sus servicios. Además, una gran cantidad de procedimientos y transacciones del Estado se realizan actualmente por Internet.

24 Datos proporcionados por el estudio "mercado total", realizado por Prince Consulting, Diciembre 2014. www.princeconsulting.biz

Estos cambios no sólo se reflejan en el gobierno sino también en el sector privado. Actualmente, en el país existen 758 proveedores de servicios de Internet (ISP)[25] y la industria de la telefonía móvil ha cuadriplicado su tamaño desde 2003, cuando superó a las líneas fijas, con 43 millones de líneas activas. Dichos desarrollos han aumentado el riesgo del país de ser un blanco para el crimen cibernético y otras actividades criminales maliciosas; durante el año pasado, las autoridades nacionales observaron un aumento en el robo de identidad y el fraude a través de las redes sociales, el correo electrónico y la banca electrónica, deformaciones de sitios web y amenazas persistentes avanzadas (ATPs).[26]

"Actualmente, en el país existen 758 proveedores de servicios de Internet (ISP) y la industria de la telefonía móvil ha cuadriplicado su tamaño desde 2003, cuando superó a las líneas fijas, con 43 millones de líneas activas. Dichos desarrollos han aumentado el riesgo del país de ser un blanco para el crimen cibernético y otras actividades criminales maliciosas; durante el año pasado, las autoridades nacionales observaron un aumento en el robo de identidad y el fraude a través de las redes sociales, el correo electrónico y la banca electrónica, deformaciones de sitios web y amenazas persistentes avanzadas (ATPs)."

Y para enfrentar estas amenazas, en 2011 el Gobierno Nacional, a través del Jefe del Gabinete de Ministros, creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), el cual está diseñado para apoyar la creación y adopción de un marco regulatorio que identifique y proteja a las infraestructuras estratégicas y críticas que requiere el Sector Público Nacional, las organizaciones interjurisdiccionales, la sociedad civil y el sector privado.

Entre los objetivos que planteo el ICID se encuentran:

- Sensibilizar a los ciudadanos y las instituciones acerca del riesgo que plantean las nuevas tecnologías y alentarlas a proteger su información.
- Fortalecer los niveles de seguridad cibernética en el Sector Público Nacional mediante la creación de estrategias comunes para proteger la información y las infraestructuras críticas.
- Fomentar la colaboración entre los diferentes sectores de la sociedad (empresas, industrias, organizaciones de la sociedad civil, universidades, etc.) con el objetivo de adoptar un marco común de lineamientos para fortalecer los niveles de ciberseguridad e infraestructuras de información críticas de sus organizaciones.
- Contribuir al mejoramiento de la ciberseguridad y la infraestructura de información crítica a escala internacional.

Hasta 2014, el ICIC ha logrado lo siguiente: [27]

- Ha ayudado a aprobar la legislación actual relacionada con el crimen cibernético, lo que ha permitido la investigación y persecución exitosas de varios casos de criminales cibernéticos.
- Ha desarrollado la iniciativa conocida como Internet Sano, que promueve y brinda material educativo sobre el uso responsable de las ITC y el Internet.
- Desde 2012, ha llevado a cabo ejercicios de respuesta a incidentes cibernéticos denominados ENRIC, y sigue impartiendo capacitación para identificar, analizar,

25 Fuente: Comisión Nacional de Comunicaciones http://www.cnc.gob.ar/Fuente: :
26 Organización de los Estados Americanos, Tendencias de Ciberseguridad de América Latina + Caribe, junio de 2014.
27 Fuente: Organización de los Estados Americanos, Tendencias de Ciberseguridad de América Latina + Caribe, junio de 2014.

Desde 2011, el ICIC se ha aliado con varias organizaciones tanto nacionales como internacionales, y ha logrado despertar un mayor interés dentro de Argentina para abordar temas de ciberseguridad. El ICIC ha tenido una participación activa en los eventos patrocinados por la Organización de los Estados Americanos (OEA), el Instituto de Estudios de Seguridad de la Unión Europea (UEISS), la Agencia Internacional de Energía Atómica (IAEA), Meridian Process, entre otros. Asimismo, varias instituciones de educación superior del país ofrecen ahora programas de certificación y licenciaturas en muchos ámbitos de la seguridad cibernética, incluyendo la investigación forense digital.

Si bien la capacidad de Argentina para enfrentar a las amenazas cibernéticas ha mejorado considerablemente desde que se fundó el ICIC, un reporte de la OEA descubrió tres impedimentos para los esfuerzos continuos que aún existen: una falta consistente de conciencia entre los interesados de todos los niveles, problemas y preocupaciones respecto a la privacidad, y financiamiento insuficiente. Estos desafíos deben superarse si se quiere asegurar el éxito de las iniciativas de seguridad cibernética de Argentina.

Trinidad yTobago

Representando cuarenta por ciento (40%) del producto interno bruto (PIB) del país, el sector energético es la principal fuente de ingresos para Trinidad y Tobago. Así, los componentes de este sector son considerados como recursos de la infraestructura crítica. Desde los controladores lógicos programables (PLC) hasta las redes de control como los Sistemas de Control Industrial (ICS) y el Control de Supervisión y Adquisición de Datos (SCADA), se hace un amplio uso de las tecnologías de la información y comunicaciones (ITCs) en el sector energético del país que lo hace vulnerable a las amenazas cibernéticas. Las interrupciones que podrían provocar estas vulnerabilidades tendrían un efecto devastador en la economía nacional.

Cabe destacar también que los componentes de la infraestructura crítica de Trinidad y Tobago se pueden encontrar en otros sectores como los de finanzas, telecomunicaciones, servicios públicos y salud. Sin embargo, al igual que el de energía, el sector financiero tiene una importancia particular en términos de ciberseguridad y protección de la infraestructura crítica (CIP), pues los ataques a cualquier institución de este sector pueden tener un efecto debilitante en el sector financiero general.

Al reconocer la necesidad de proteger la infraestructura crítica mediante el desarrollo de un marco de ciberseguridad robusto, el Gobierno de Trinidad y Tobago estableció en 2011 un Comité Interministerial (IMC) para desarrollar una estrategia de seguridad integral en el país. Integrado por varios ministerios clave (incluyendo a los Ministerios de Ciencia y Tecnología, Administración Pública, Fiscalía General, Servicios Públicos, Finanzas, Energía y Asuntos Energéticos, el IMC se encarga, entre otras cosas, de:

- Desarrollar una estrategia coordinada de ciberseguridad y un plan de acción
- Facilitar, guiar y asegurar la promulgación de una Ley Nacional contra el Cibercrimen
- Facilitar, guiar y asegurar la implementación del Equipo Nacional de Respuestas a Incidentes de Seguridad Informática (CSIRT)
- Establecer un mecanismo de implementación que haría que la autoridad legislativa desarrolle y aplique regulaciones de ciberseguridad
- Crear un mecanismo/marco que asegure que se realicen con regularidad evaluaciones de riesgos/vulnerabilidades de cada infraestructura cibernética y plan de ciberseguridad del Ministerio.

Hasta ahora, el IMC ha logrado lo siguiente:

- Desarrollar una Estrategia Nacional de Ciberseguridad (aprobada en diciembre de 2012)
- Desarrollar una Política Nacional de Cibercrimen (aprobada en febrero de 2013)
- Desarrollar una Política para el Establecimiento de una Agencia de Ciberseguridad en Trinidad y Tobago (aprobada en agosto de 2013)
- Un Acuerdo Administrativo entre el Ministerio de Seguridad Nacional y la Unión Internacional de Telecomunicaciones (ITU) para ayudar a establecer un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) (Febrero de 2014)
- La aprobación para los Proyectos de Leyes titulados “La Ley de Cibercrimen 2014” y “La Ley de la Agencia de Ciberseguridad de Trinidad y Tobago, 2014”. La Ley de Cibercrimen fue sometida a discusión en el Parlamento el viernes 21 de marzo de 2014.

Además de la Estrategia Nacional de Ciberseguridad que satisface las necesidades de los sectores público y privado, el gobierno también estableció una Iniciativa de Seguridad para el Sector Energético (ESSI), que busca brindar una dirección estratégica para la seguridad del sector energético de Trinidad y Tobago. La ESSI es una Asociación Público-Privada que se formó mediante la colaboración entre el Gobierno de Trinidad y Tobago y organismos de los sectores público y privado y los operadores de la infraestructura energética. En foco principal de la iniciativa es crear un mecanismo sustentable para prevenir, mitigar, prepararse, responder y recuperarse de todas las posibles amenazas y vulnerabilidades que tengan el potencial de interrumpir o destruir el sector energético del país.

El objetivo estratégico de la ESSI es la prevención y mitigación de incidentes no deseados dentro del sector energético. Así, la iniciativa pretende asegurar que los recursos energéticos de Trinidad y Tobago se protejan de manera efectiva contra las actividades que podrían provocar interrupciones importantes debido a intentos deliberados, accidentes o desastres naturales.

Uruguay

"Desde su creación, el CERTuy ha coordinado e implementado la respuesta al análisis de los incidentes de seguridad, ha apoyado y coordinado los procesos de recuperación de desastres, ha realizado pruebas de penetración y auditorías de seguridad."

La República Oriental de Uruguay ha visto un aumento en el desarrollo nacional de las Tecnologías de Información y Comunicación (ITC). Tal vez no sea sorpresa, pero los datos sugieren que los incidentes cibernéticos, en particular el phishing, también han aumentado considerablemente. Dichas amenazas tienen serias ramificaciones para los recursos de información críticas del Estado, por ejemplo, aquellas que son vitales para las operaciones económicas y del gobierno, como los servicios de emergencia, los servicios de salud, el orden público, la energía, las telecomunicaciones, el transporte, el abasto de agua potable, los servicios bancarios y financieros o cualquier otro servicio que afecte a más de 30% de la población, y por tanto la seguridad y el bienestar de la sociedad.

En 2008, con el apoyo de la Agencia Nacional para el Desarrollo del Gobierno Electrónico y la Sociedad de la Información (AGESIC), se constituyó por ley el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy). Desde su creación, el CERTuy ha coordinado e implementado la respuesta al análisis de los incidentes de seguridad, ha apoyado y coordinado los procesos de recuperación de desastres, ha realizado pruebas de penetración y auditorías de seguridad. Asimismo, ha desarrollado y difundido normas, políticas y mejores prácticas que aumentan los niveles de seguridad. Asimismo, ha trabajado en el desarrollo de capacidades y la difusión del conocimiento a través de campañas de concientización, creación de capacidad para los operadores de la infraestructura crítica mediante ejercicios de manejos de crisis cibernéticas y particularmente para la creación e CSIRTs especializados. Los objetivos y obligaciones del CERTuy incluyen:

- Promover la confianza entre los usuarios de las TIC y crear conciencia sobre las amenazas cibernéticas entre la sociedad.
- Regular y proteger los recursos de información críticos del Estado.
- Consolidar a todas las organizaciones de servicios públicos bajo un criterio común para la clasificación de los sitios web (como ".gub.uy" y ".mil.uy") y mejorar los estándares de seguridad para las bases de datos, el correo electrónico y los nombres de dominio.
- Incorporar a todos los actores nacionales y regionales (Poder Judicial, Poder Legislativo, el Ministerio de Defensa Nacional, los sectores privado y financiero, la academia, los proveedores de servicios de Internet, la sociedad civil, los CSIRTs y las organizaciones internacionales, entre otros).

Desde sus inicios, el CERTuy ha logrado lo siguiente:

- Ha detectado intrusiones de distintos niveles de complejidad y severidad a los sistemas críticos que pudieron ser contenidos sin tener un impacto mayor.

- En caso de que se presentaran incidentes cibernéticos, se ofrecieron respuestas rápidas y efectivas para determinar los sistemas afectados y se realizaron esfuerzos de recuperación eficientes, lo cual se logró al incorporar metodologías de manejo de incidentes, la intervención de especialistas en seguridad de la información, redes de confianza nacionales e internacionales y el desarrollo constante de capacidades específicas.

- En noviembre de 2013 se anunció el inicio de la campaña “Conéctate de Forma Segura”, que busca crear conciencia sobre las amenazas que acompañan el uso de las ITC, y se adoptó la campaña STOP. THINK. CONNECT iniciada en Estados Unidos.

- Se impartió capacitación técnica al personal de varias autoridades que luchan contra el cibercrimen, incluyendo a la Unidad de Crímenes Informáticos de la Policía Nacional.

Como se dijo anteriormente, el CERTuy entiende que las alianzas y la participación de todos los actores de la ciberseguridad, públicos y privados, son fundamentales para poder contrarrestar el crecimiento y sofisticación de las amenazas a la ciberseguridad. Por lo tanto, la AGESIC y el CERTuy han colaborado regularmente con sus colegas de otros países y se han asociado con organismos internacionales con el fin de fomentar la comunicación y la colaboración entre los centros de respuesta como OAS/CICTE, LACNIC, FIRST e ITU.

El éxito futuro de Uruguay para combatir el cibercrimen y otras amenazas a la ciberseguridad dependerá, en parte, de su capacidad de resolver los tres problemas principales que han obstaculizado su progreso: falta de conciencia sobre la seguridad en las instituciones gubernamentales, recursos financieros y materiales insuficientes para llevar a cabo las iniciativas necesarias, y la falta de personal capacitado. [28] No obstante, el CERTuy ha seguido trabajando de forma ardua, continua y colaborativa para proteger la infraestructura crítica de Uruguay contra las amenazas cibernéticas y contribuir a la ciberseguridad a nivel internacional.

28 Fuente: Organización de los Estados Americanos, Tendencias de Ciberseguridad de América Latina + Caribe, junio de 2014.

Conclusión

Este reporte brinda una perspectiva única de los ataques cibernéticos que sufrieron las infraestructuras críticas de América. Los 500 encuestados destacaron el aumento radical de la sofisticación de los ataques cibernéticos. Lo más alarmante fue que el inquietante fenómeno descrito por al aumento considerable de los ataques destructivos, o ataques cibernéticos, que fueron concebidos para “eliminar o destruir” los sistemas back-end. Sin duda, existe ahí un peligro claro y directo que ilustra la dramática evolución de las capacidades cibernéticas que poseen los actores no estatales de la región. Estos grupos han adoptado los ataques cibernéticos contra las infraestructuras con propósitos criminales, activistas y geopolíticos. Debido a esta cruda realidad, los presupuestos para la ciberseguridad y la creación de capacidad deben elevarse así como facilitarse un mayor intercambio de información.

En conclusión, este reporte destaca que aunque se han realizado algunos esfuerzos, aún se requiere de una asociación proactiva entre los gobiernos y las organizaciones privadas en el hemisferio occidental. Ante la ausencia de una asociación público-privada formal estos criminales electrónicos prosperarán. Esto representa una oportunidad histórica que se ha desaprovechado. El Programa de Ciberseguridad de la OEA/CICTE juega un papel fundamental para fomentar la colaboración pública/privada que aún está madurando en la región. Y es por la filosofía de dicha colaboración público-privada que la OEA y Trend Micro unieron fuerzas para brindarle esta perspectiva única de los ataques a la infraestructura crítica que ha tenido impacto en 25 naciones. Sin duda, se necesita una acción colectiva.

“Ni todos los ejércitos del mundo pueden detener una idea cuya hora ha llegado”. – Víctor Hugo.

Apéndice: Encuesta sobre la Infraestructura Crítica

Metodología

- Se realizó una encuesta cuantitativa en línea en enero de 2015 entre los directores de Seguridad de los CIO de las principales infraestructuras críticas en todos los países de América.
- Un total de 575 participantes respondieron la encuesta.

Resultados de la Encuesta

Países Participantes

Un total de 26 países miembros de la OEA participaron en la encuesta. Estos son:

- Argentina
- Barbados
- Belice
- Bolivia
- Brasil
- Canadá
- Chile
- Colombia
- Costa Rica
- Mancomunidad de Dominica
- República Dominicana
- Ecuador
- El Salvador
- Granada
- Guatemala
- Honduras
- México
- Nicaragua
- Panamá
- Paraguay
- Perú
- San Vicente y las Granadinas
- Surinam
- Estados Unidos de América
- Uruguay
- RepúblicaBolivariana de Venezuela

¿En qué país trabaja actualmente?

Organización Vertical

- La industria que más se reportó es el gobierno, seguido por el sector de telecomunicaciones.

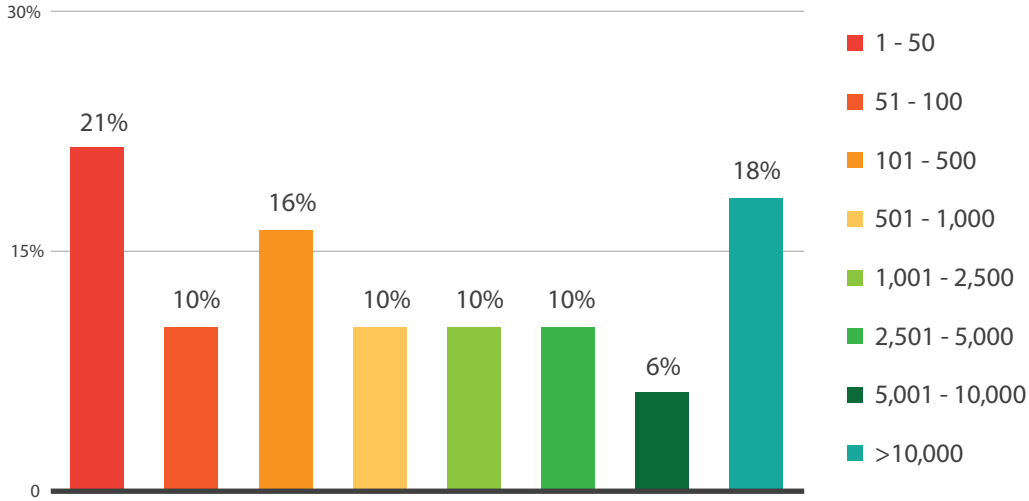
¿A qué industria pertenece su organización?

Gobierno	32%
Comunicaciones	17%
Seguridad	12%
Banca y Finanzas	11%
Manufactura	9%
Energía	8%
Transporte	4%
Salud	3%
Química y Minería	2%
Agricultura	2%
Servicios de Emergencia	1%
Manejo de Agua y Desechos	1%

Tamaño de la Organización

- Las organizaciones que participaron en la encuesta están distribuidas en varios tamaños. Los dos grupos que tienen el mayor número de empleados son de “1-50 empleados” (21%) y “> 10,000 empleados” (18%)

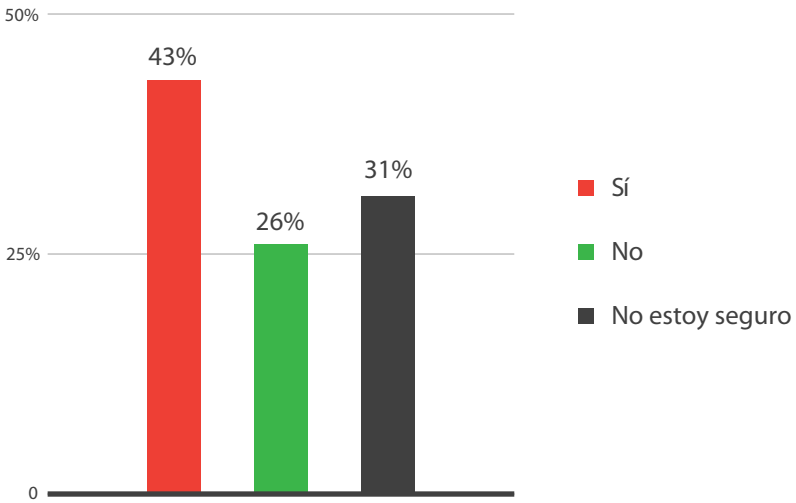
¿Cuántas personas su organización emplea en todo el mundo?



Nivel de Ataques al Sistema Informático durante el Año Pasado

- Más de la mitad de los encuestados reportaron un incremento en el nivel de ataques a sus sistemas informáticos el año pasado, mientras que cuatro de cada diez dijeron que el nivel de ataques no tuvo cambios.
- Muy pocos reportaron una disminución del nivel de ataques el año pasado.

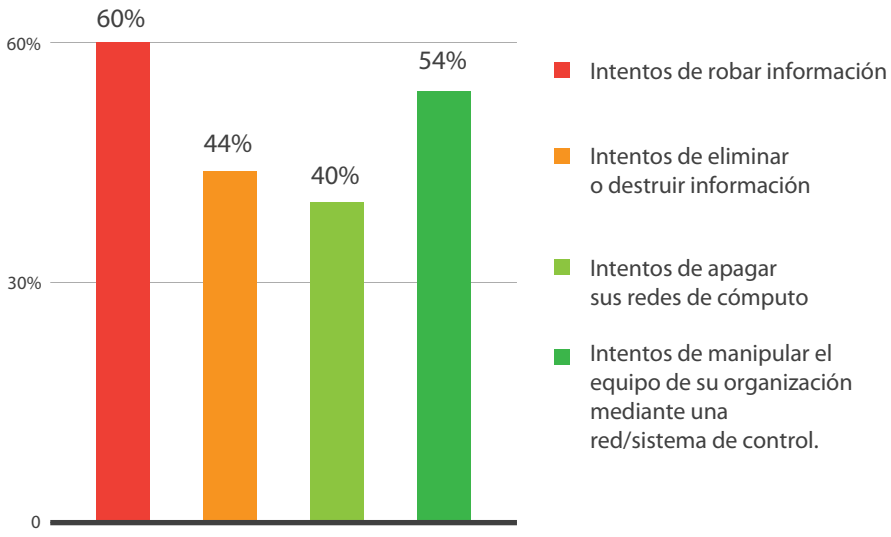
¿Ha notado un incremento, disminución o nivel estable de ataques a sus sistemas informáticos durante el año pasado?



Experiencias con Ataques Varios

- La mayoría de las organizaciones encuestadas han experimentado intentos de robar su información. Más de la mitad han experimentado intentos de manipular sus equipos mediante una red/sistema de control.

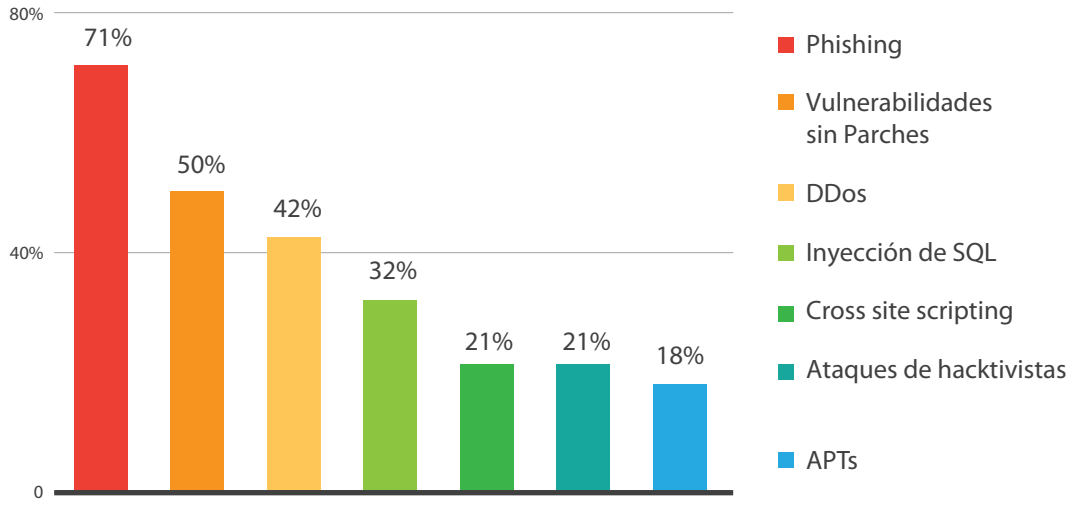
¿Su organización ha experimentado algunos de las siguientes?



Tipos de Métodos de Ataques Cibernéticos

- La gran mayoría de las organizaciones reportó que se había utilizado el phishing contra sus organizaciones. La mitad reportó que se habían utilizado vulnerabilidades sin parches contra su organización.

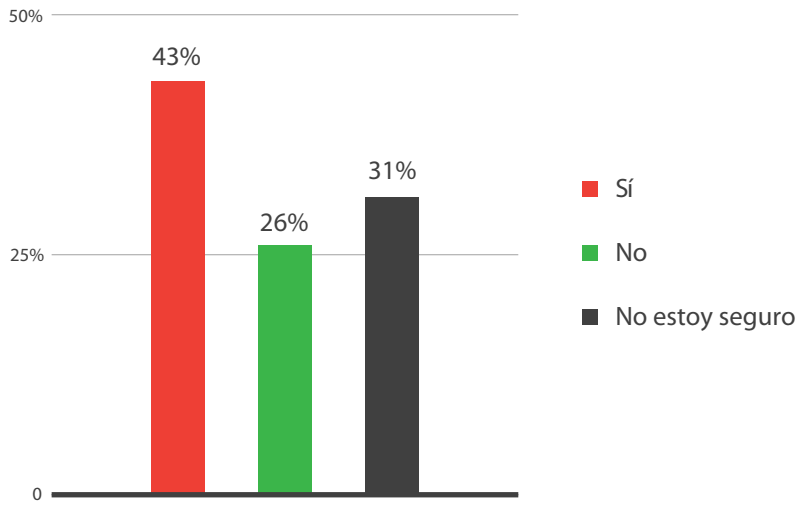
¿Qué tipos de métodos de ataques cibernéticos se han utilizado contra su organización?



Ataques a la Infraestructura

- Más de cuatro de diez organizaciones han detectado ataques dirigidos particularmente a la infraestructura que operan. En tanto, tres de diez dijeron que no estaban seguros.

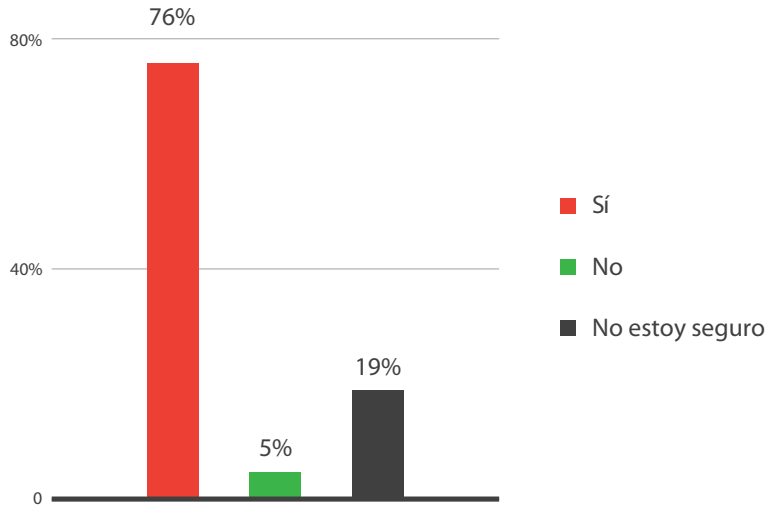
¿Ha detectado ataques/incidentes/intrusiones dirigidos particularmente a la infraestructura que su organización opera/mantiene/administra?



Sofisticación de los Ataques

- Hay un consenso universal de que los ataques contra la Infraestructura se están volviendo más sofisticados en todos los países encuestados

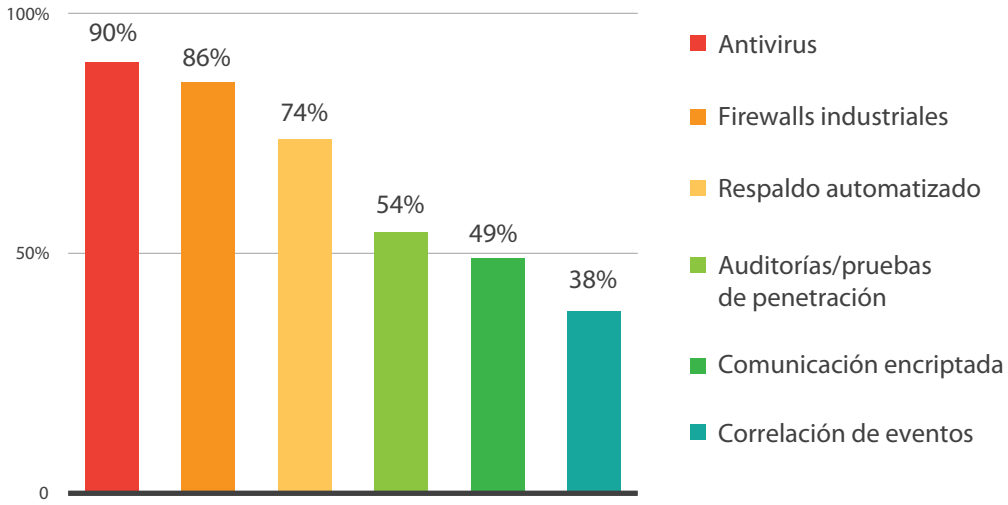
¿Los ataques contra las infraestructuras se están volviendo más sofisticados?



Medidas Adoptadas para Proteger los Sistemas de Información Críticos

- Las organizaciones utilizaron una variedad de controles de ciberseguridad para proteger los sistemas de información críticos, las medidas más comunes que se implementaron fueron: antivirus, firewalls industriales y respaldo automatizado.

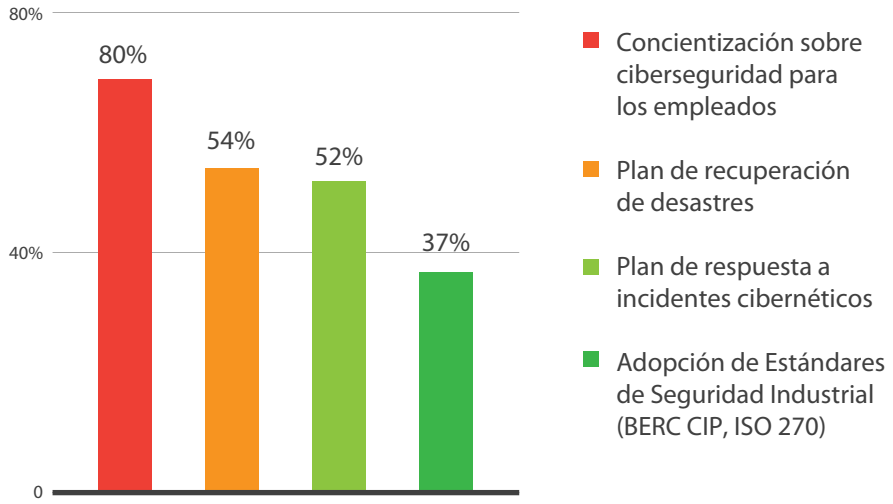
¿Qué tipo de medidas técnicas de ciberseguridad ha implementado su organización para proteger los sistemas de información críticos?



Políticas de Ciberseguridad

- Casi 70% de los participantes en la encuesta cuentan con Programas de Concientización sobre Ciberseguridad para sus empleados. Más de la mitad tienen un Plan de Recuperación de Desastres y/o un Plan de Respuesta a Incidentes Cibernéticos.

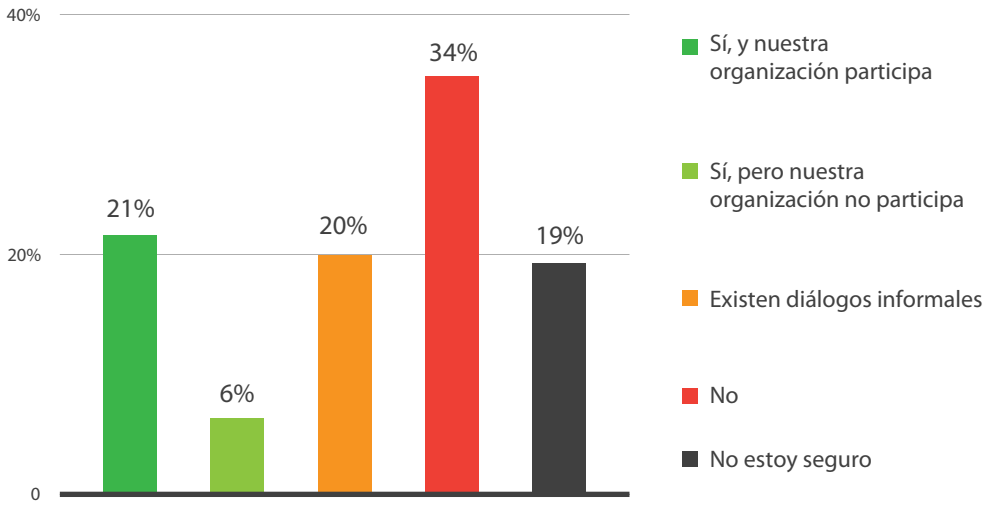
¿Su organización tiene políticas y/o planes de ciberseguridad?



Discusión con el Gobierno sobre la Resistencia Cibernética de los Sistemas de Infraestructura Crítica

- Casi la mitad de las organizaciones reportó que hay discusiones o diálogos informales con el gobierno sobre la resistencia cibernética de los sistemas de infraestructura crítica.

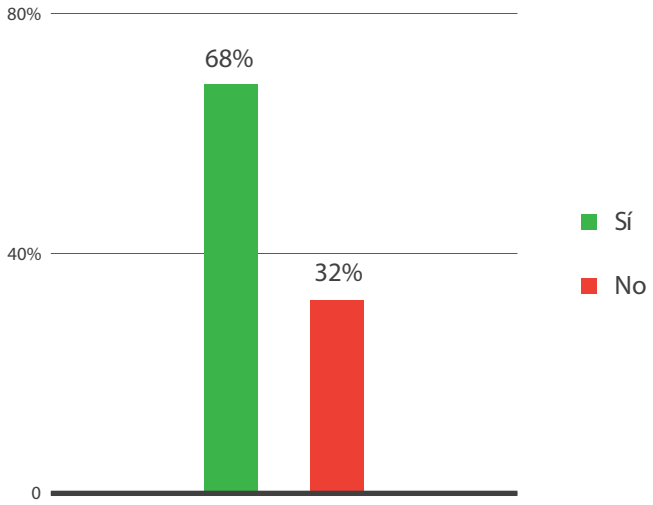
¿Existe una discusión/diálogo con el gobierno sobre la resistencia cibernética de los sistemas de infraestructura crítica?



Si los Encuestados Confían en que el Gobierno Impulse una Agenda de Ciberseguridad en las Industrias de Infraestructura Crítica

En general, la mayoría de las organizaciones encuestadas confían en que el gobierno impulse una agenda de ciberseguridad en las industrias de infraestructura crítica, y están dispuestas a trabajar con el gobierno.

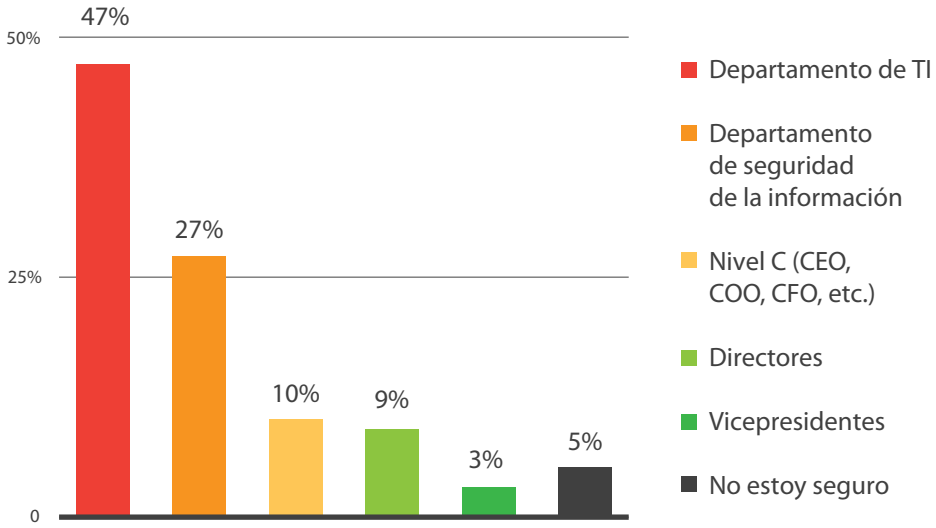
¿Confía en que el gobierno impulse una agenda de ciberseguridad en las industrias de infraestructura crítica? ¿Está dispuesto a trabajar con ellos?



Nivel de Administración que Supervisa la Ciberseguridad

- En general, los departamentos de TI se encargarán de supervisar la ciberseguridad organizacional, particularmente en Brasil.

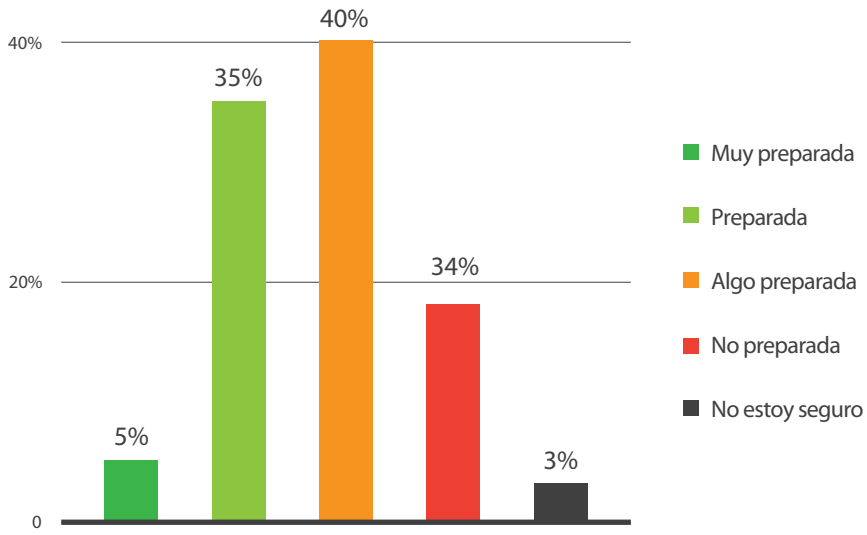
¿Qué nivel de administración supervisa la ciberseguridad organizacional?



Preparación para un Ataque Cibernético

- Casi la mitad de las organizaciones reportó que hay discusiones o diálogos informales con el gobierno acerca de la resistencia cibernética de los sistemas de infraestructura crítica.

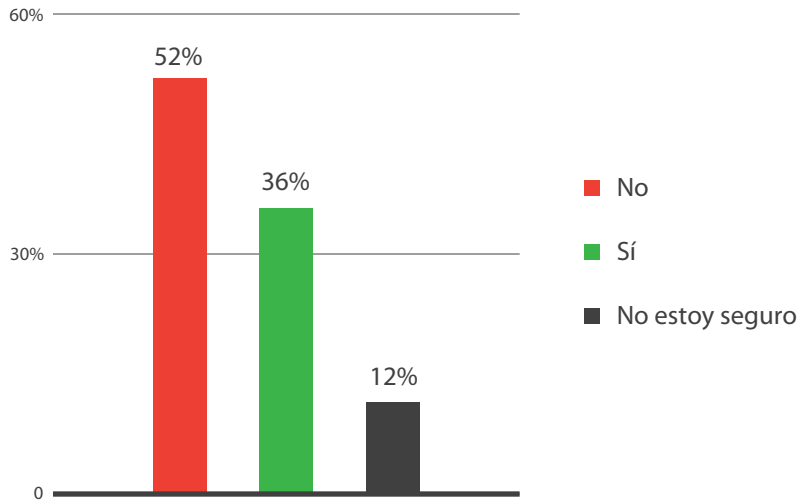
¿Cuán preparada está su organización para un incidente cibernético?



Presupuesto para la Ciberseguridad

- La mayoría de los encuestados reportó que su presupuesto para la ciberseguridad no se incrementó durante el año pasado.

¿El presupuesto para la ciberseguridad se ha incrementado durante el año pasado?



April 2015 / Abril de 2015

1889 F Street, N.W., Washington, D.C., 20006

United States of America

www.oas.org/cyber/

Organization of American States

Secretary General

José Miguel Insulza

Assistant Secretary General

Albert R. Ramdin

Secretary for Multidimensional Security

Adam Blackwell

Report on Cybersecurity and Critical Infrastructure in the Americas

Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas

Executive Secretary of the Inter-American Committee against Terrorism

Neil Klopfenstein

Editors

Tom Kellermann

Pablo Martinez

Belisario Contreras

Barbara Marchiori

Contributors

Kerry-Ann Barrett

Diego Subero

Gonzalo García-Belenguer

Emmanuelle Pelletier

Francisco Javier Villa

Geraldine Vivanco

Kyle Wilhoit

Christopher Budd

Ina Li

Paul Oliveria

Danielle Veluz

Trend Micro Incorporated, líder global en software de seguridad, se esfuerza por hacer del mundo un lugar seguro para el intercambio de información digital. Nuestras soluciones innovadoras para los usuarios finales, las empresas y los gobiernos proporcionan seguridad de contenidos en capas protegiendo la información en los dispositivos móviles, endpoints, gateways, servidores y la nube. Todas nuestras soluciones son potenciadas por inteligencia de amenazas global basada en la nube, Trend Micro™ Smart Protection Network™ y estan respaldadas por más de 1,200 expertos en amenazas. Para obtener más información, visite www.trendmicro.com.

TREND MICRO™

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569,8900