Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos

NOTA: La información y los argumentos que se expresan en el presente informe no necesariamente reflejan los puntos de vista oficiales de la Organización de los Estados Americanos o de los gobiernos de sus Estados miembros.

Contents

Introducción

En un mundo interconectado, es necesario buscar un equilibrio entre disfrutar la comodidad que ofrecen las tecnologías de la información y minimizar las oportunidades que su uso les ofrece a los delincuentes cibernéticos, quienes pueden, por ejemplo, difundir amenazas complejas explotando los populares dispositivos móviles y las aplicaciones en la nube para infiltrarse en blancos de alto valor y han convertido el espacio cibernético en un medio para victimizar al público.

Durante todo 2012, las tendencias de las actividades cibernéticas ilícitas en todo el mundo demostraron cómo algunas amenazas antes desconocidas habían evolucionado hasta volverse omnipresentes y convertirse en un peligro para todo tipo de usuarios del internet. El uso de herramientas como el Blackhole Exploit Kit, los sistemas de transferencia automática y el ransomware se disparó, junto con el empleo de mejores estrategias de ingeniería social, técnicas de evasión y tácticas de amedrentamiento.[1] La muy difundida historia de la apropiación de una nueva tecnología para fines nefastos resurgió en 2012, cuando las amenazas móviles adquirieron dimensiones espectaculares y aumentaron a un ritmo mucho más acelerado que el que afectó a las computadoras normales.[2] El número de aplicaciones maliciosas para Android creció de mil a más de 350.000 en el transcurso de un solo año.

Los incidentes cibernéticos han puesto de manifiesto la importancia de mantenerse al día con respecto a las tendencias globales de la delincuencia cibernética, en especial en lo que toca al uso de aparatos móviles y dispositivos personales de cómputo. Los especialistas en seguridad informática y los analistas de amenazas cibernéticas deben producir, entonces, a partir de promedios globales, estadísticas específicas a organizaciones, industrias o regiones, a fin de determinar las mejores formas para proteger la información confidencial que resguardan. Si no se producen estos análisis específicamente focalizados de las amenazas, los datos críticos se distorsionarán e impedirán que los países y las empresas diseñen e implementen políticas y capacidades técnicas de seguridad cibernética eficaces, con lo que los ciudadanos seguirán siendo vulnerables.

El conocimiento de que se dispone sobre el panorama general de las amenazas cibernéticas y las respuestas de los gobiernos en América Latina y el Caribe es incompleto. Gran parte de lo que se conoce sobre el panorama de las amenazas cibernéticas en la región se basa en informes noticiosos esporádicos y sin fundamentos sólidos. Algunas fuentes señalan que el malware bancario fue el problema de delincuencia cibernética más importante en 2011, mientras que otras acusan como los mayores culpables a los programas maliciosos de propósitos múltiples que afectaron a los routers en América Latina en mayor escala que en cualquier otra parte del mundo.[3] La divergencia entre los distintos puntos de vista demuestra que se requieren datos más específicos para diagnosticar con precisión las amenazas que acosan a nuestros ciudadanos.

1 http://www.trendmicro.de/media/misc/blackhole-exploit-kit-research-report-en.pdf; http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf; http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf; http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf

2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf

3 http://blog.trendmicro.com/trendlabs-security-intelligence/latin-america-router-compromising-malware-found/

En colaboración con Trend Micro Incorporated, la Organización de los Estados Americanos (OEA) y su Secretaría de Seguridad Multidimensional (SMS) desea compartir este informe para ilustrar las tendencias en seguridad y delincuencia cibernética en América Latina y el Caribe. La información que aquí se presenta se recabó a través métodos tanto cuantitativos como cualitativos, a partir de datos extraídos de una encuesta entre los gobiernos de los Estados miembros de la OEA, así como de un análisis minucioso de inteligencia de las amenazas mundiales de honeypots y datos aportados por clientes y recogidos por Trend Micro. Excepto cuando se señala lo contrario, las figuras y cuadros emplean datos recopilados por Trend Micro. Los análisis y conclusiones del presente informe cubren solamente a aquellos países que participaron en la encuesta de la OEA.

Resultados de la encuesta de países de la OEA

Se invitó a los 32 Estados miembros de la OEA de América Latina y el Caribe a proporcionar voluntariamente información sobre los tipos y la extensión de los incidentes de seguridad cibernética que se enfrentaron en sus países en 2012, así como sobre sus respuestas a dichos incidentes. Trece de los 18 Estados miembros latinoamericanos y siete de los 14 Estados miembros del Caribe aportaron subsiguientemente contribuciones a este informe. Suministraron datos cualitativos una variedad de instituciones, entre las que destacan los Equipos Nacionales de Respuesta a Incidentes de Seguridad Cibernética (CSIRTs) y, en menor medida, las unidades policiales nacionales de delincuencia cibernética.

Buena parte de la información recogida se presenta aquí en forma conjunta, para mantener la confidencialidad de algunos hallazgos delicados. Además, al igual que con cualquier encuesta de gran escala sobre incidentes cibernéticos y actividades cibernéticas ilícitas, este esfuerzo para recopilar y analizar este tipo de datos para Américas y el Caribe adolece de limitaciones inherentes. Por un lado, ningún administrador de redes o equipo nacional de respuesta a incidentes sabe cuántos ataques están logrando su objetivo sin ser detectados. Las intrusiones a través de la red se descubren rutinariamente meses o incluso años después del inicio de la violación original. Además, los diálogos con los Estados miembros participantes revelaron que la ausencia de comunicación e intercambio de información eficaces dentro de los gobiernos para la notificación de incidentes cibernéticos sigue siendo un desafío clave. Ya sea debido a la competencia entre agencias, a la preocupación por no proyectar una imagen de ineficacia o a la simple falta de canales o mecanismos necesarios para compartir la información, la ausencia de este intercambio de información sobre incidentes cibernéticos o violaciones de seguridad en redes sigue siendo una realidad generalizada que debe tomarse en cuenta al analizar los datos sobre la conducta cibernética en la región.

Este estudio también sufrió limitaciones por la falta de una terminología definida y homogénea. En el análisis de los datos quedó claro que la frase “incidente cibernético” no se entiende ni se aplica uniformemente en toda la región, y cae fuera del alcance de este estudio exhortar a los Estados a integrar sus respectivas definiciones. Algunos gobiernos interpretan los incidentes cibernéticos como cualquier informe o queja enviado a un equipo nacional de respuesta, mientras que otros son más estrictos en su clasificación. Algunos resultados de la encuesta entre los Estados incluyeron incidentes contra los sectores público y privado, así como contra usuarios finales y el sector académico. Otros solamente incluyeron información relacionada con las redes gubernamentales, mientras que otros más solo describieron incidentes cibernéticos que involucraron a uno o dos ministerios clave. A pesar de las deficiencias que plantean los matices en taxonomía o clasificación, este informe ofrece una oportunidad para que los gobiernos presenten sus experiencias —tanto positivas como negativas—, con la esperanza de que estas permitan a las partes interesadas relevantes obtener una mejor comprensión de lo que está ocurriendo en la región y lo que falta por hacer.

Tendencias detectadas

Tendencias generales

En 2012, los gobiernos observaron un aumento general en la frecuencia de los incidentes cibernéticos en comparación con 2011, incluso cuando los datos cuantitativos definitivos eran incompletos o no estaban disponibles. El mínimo incremento evaluado en los incidentes cibernéticos durante el período de 2011 a 2012 registrado por un gobierno fue de entre el 8% y el 12%, mientras que en el extremo superior otros dos países registraron un incremento del 40%. La mayor parte de los gobiernos citaron aumentos en algún punto dentro de esta escala, aunque es interesante observar que varios informaron que, en términos globales, se detectaron menos incidentes.

Además de poner de relieve la diversidad de definiciones de los términos relacionados con la seguridad cibernética, la interpretación y el análisis de los datos recopilados arrojó luz sobre otras consideraciones importantes. Varios gobiernos aclararon que las cifras proporcionadas no necesariamente reflejaban cambios reales en la frecuencia de los ataques, sino mejoras en la vigilancia de sus redes y mayor capacitación de su personal, lo que les permitió a las organizaciones detectar más violaciones de los sistemas y otras actividades cibernéticas ilícitas. Es interesante que aquellos países donde los CSIRT nacionales se establecieron recientemente registraran algunos de los incrementos más significativos en los incidentes que manejaron. Esto reforzó la noción de que todo el tiempo había habido ataques, pero que sencillamente no se descubrieron o no se documentaron.

También cabe resaltar el hecho de que la mayor parte de los Estados no diferencian entre el tipo o la gravedad de los incidentes cibernéticos que registran. Esto plantea una deficiencia en los datos analizados, en vista de la variedad de consecuencias potenciales de los distintos tipos de incidentes o ataques: un ataque complejo y de gran escala a una infraestructura nacional crítica probablemente tendrá mayores repercusiones que la profanación de un sitio web gubernamental. Los datos en que sí se especificaron los tipos de ataques generalmente se presentaron en forma conjunta, aunque en el caso de algunos sitios hemos podido desplegar las frecuencias de los distintos tipos o la gravedad de los ataques sufridos. Una CISRT nacional incipiente, por ejemplo, señaló que manejó 45 incidentes en 2012 y que solamente consideró uno de ellos un caso “prioritario”.

Obviamente, los incidentes cibernéticos incluidos en los informes de los gobiernos de los Estados miembros de la OEA representan solamente una fracción del número total de incidentes y otras formas de delincuencia cibernética que se llevan a cabo en la región. Pero sigue siendo sencillamente imposible en este momento recopilar datos que permitan obtener una imagen verdaderamente exhaustiva y detallada de la extensión de todos estos incidentes y actividades en las Américas y el Caribe, o en cualquier otro sitio.

Como ya dijimos, el intercambio de información dentro de los gobiernos —incluso aquellos con la capacidad más avanzada en materia de seguridad cibernética— sigue quedando corto, en gran parte debido a las realidades prácticas de que múltiples organizaciones tengan que responder simultáneamente a una gama de amenazas y blancos en constante evolución. Y muchas empresas privadas y otras entidades no gubernamentales siguen mostrándose reacias a reportar ataques o violaciones. Contabilizar el número de incidentes que afectan a los ciudadanos individuales plantea un desafío incluso mayor, en vista del porcentaje incluso más alto de ellos que pasan desapercibidos y no se reportan. Por último, la falta de colaboración generalizada y persistente entre las partes interesadas en todos los niveles dificulta todavía más recoger información sobre violaciones de datos. Las consecuencias netas de todos estos factores son una conciencia menos que adecuada del problema y la continua vulnerabilidad de redes y sistemas de información críticos.

El hactivismo, o el haqueo por motivos políticos, recibió amplia atención de los medios de comunicación en 2012, y la información suministrada por los Estados miembros sugiere que esta forma de incidentes cibernéticos verdaderamente está aumentando en la región. Dos países reportaron campañas coordinadas de ataques cibernéticos como respuesta a iniciativas legislativas para fortalecer la aplicación de leyes de derechos de autor y reformar códigos tributarios. En ambos casos, conforme se acercaba la ratificación de los respectivos proyectos de ley, los foros de hackers se saturaron con planes para emprender ataques cibernéticos de gran escala contra infraestructuras gubernamentales excepto si se vetaban los proyectos de ley. Ambos CSIRTs nacionales recibieron advertencias previas de los ataques inminentes, gracias a lo cual lograron mantener los daños al mínimo. Las investigaciones de estos dos incidentes no fueron concluyentes; una de ellas no arrojó pruebas enjuiciables y la otra se estancó a la larga, cuando se enfriaron las pistas iniciales.

Es interesante observar que en algunos casos estas campañas de hactivismo generaron beneficios imprevistos. En dos de los países que contribuyeron a este informe, grupos no identificados amenazaron con lanzar ataques contra múltiples instituciones gubernamentales. En uno de estos países amenazados, este fue su primer caso de advertencia explícita de haqueo por motivos políticos. Las amenazas motivaron a ambos gobiernos a implementar planes de acción para mitigar y responder a ataques potenciales. Aunque los incidentes en cuestión nunca se materializaron plenamente, sí provocaron una mayor colaboración entre las partes interesadas clave, entre ellas las agencias policíacas, los proveedores de servicios de internet (ISP) y un operador de infraestructura. La información que proporcionaron los Estados miembros señala que la capacidad que se obtuvo y las lecciones aprendidas de la planeación y, en algunos casos, la respuesta proactiva ante estos incidentes se han convertido en un motor central para aumentar la resiliencia cibernética nacional de esos países.

También se reportaron otras importantes tendencias en la seguridad cibernética. En por lo menos un país se detectó spyware en servidores de las fuerzas policiales. Numerosos Estados suministraron información que sugiere que los sindicatos tradicionales de la delincuencia organizada han recurrido cada vez más al internet para obtener y lavar fondos, lo cual concuerda bastante bien con las tendencias que se observan a nivel mundial. Un país informó que más del 80% de los delitos investigados en 2012 involucraron algún aspecto de delincuencia electrónica o el uso ilícito de tecnologías de la información. Y aunque las tecnologías de la información y las comunicaciones pueden no ser todavía el principal vehículo para la mayoría de los delitos, ciertamente han pasado a formar parte integral de todas las investigaciones, lo que destaca la necesidad de instrumentos legislativos adecuados, investigadores y fiscales capacitados y una mayor cooperación internacional en materia cibernética.

A pesar de su mayor visibilidad, el hactivismo no sustituyó a los beneficios pecuniarios como la motivación primaria que subyace al haqueo y al uso ilícito del internet en la región. Los hackers siguieron buscando datos personales y financieros y alimentando los mercados negros en línea en todo el mundo. Sin embargo, es imposible medir con precisión en términos cuantitativos el impacto y las pérdidas económicas que causó el haqueo en las Américas y el Caribe en 2012. La cifra es extraordinariamente alta, muy probablemente superior a las pérdidas provocadas por cualquier otra forma de delincuencia, incluido el narcotráfico.

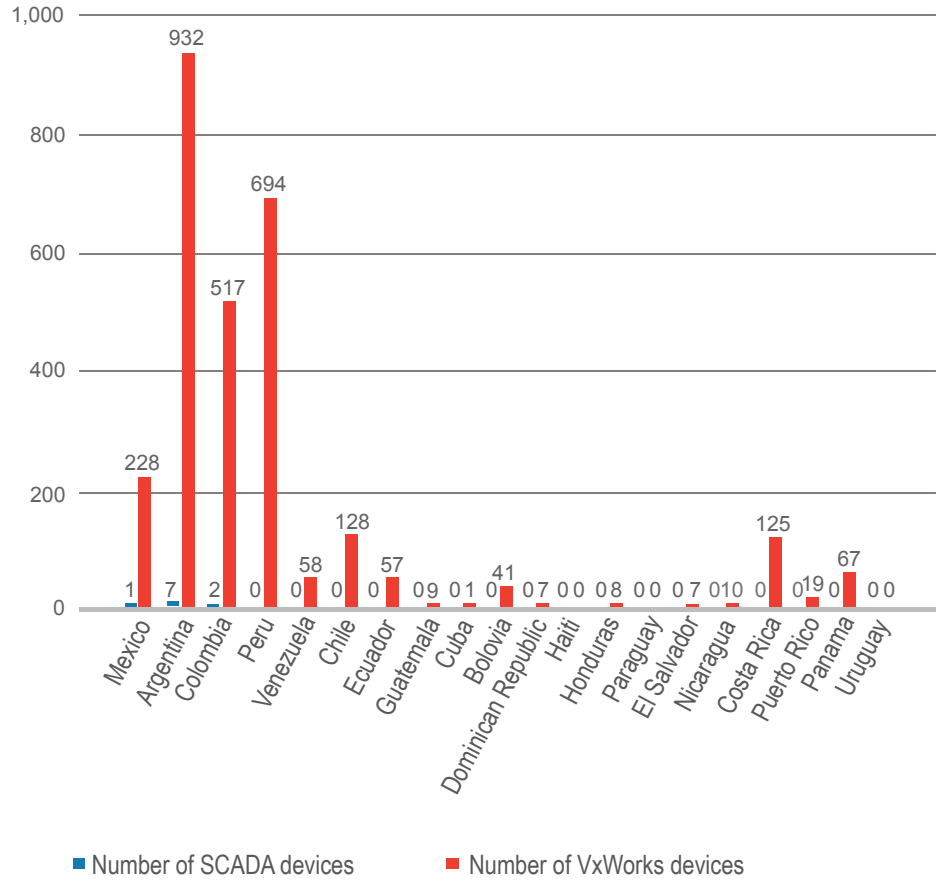
Preocupaciones sobre los sistemas de control industrial

Tanto los datos de la OEA como los de Trend Micro indicaron un aumento en el número de ataques contra infraestructuras críticas. Muchas infraestructuras críticas, incluidas las que manejan los sectores financiero, de transporte, de energía y de atención de la salud, dependen de sistemas de control industrial. Muchos de estos sistemas, a su vez, utilizan el internet, lo que les permite a las infraestructuras críticas operar de manera eficiente y barata. A pesar de que facilita la prestación barata y oportuna de servicios críticos, la conectividad de los sistemas de control industrial también les presenta a delincuentes y terroristas oportunidades de atacar a países donde se sentirá más.

Numerosos estudios de casos en el último año ilustran el carácter apremiante de estas amenazas para los sistemas de control industrial. Un servicio público nacional de electricidad en cierto país experimentó una avalancha de ataques cibernéticos, aunque el CSIRT nacional logró minimizar los daños provocados por las violaciones. Otro gobierno reportó ataques extensos contra instituciones financieras que formaban la base de su zona económica especial. En este caso, los ataques podrían tener el potencial de causar daños especiales, considerando que la zona económica especial representa un alto porcentaje del producto económico del país y buena parte de su inversión extranjera directa. El proveedor principal de servicios de telecomunicaciones de un país también sufrió ataques, que provocaron una interrupción breve, pero extendida, del servicio celular. A diferencia de la mayoría de los ataques, los perpetradores de este último incidente fueron atrapados y condenados.

Estos incidentes resaltan los peligros que plantean los ataques bien coordinados a infraestructuras críticas para el bienestar público y el desarrollo económico. Aunque no ha habido todavía ataques relacionados con infraestructura crítica que provoquen pérdidas catastróficas o daños físicos en las Américas y el Caribe, sí se recalca la necesidad de mantener la vigilancia y de mejorar la resiliencia, pues muchos sistemas críticos en la región siguen estando expuestos.

En 2012, 51 proveedores de la comunidad de seguridad de sistemas de control industrial registraron 171 vulnerabilidades en diversos sistemas de control industrial expuestos al internet, y el problema es especialmente agudo en las Américas. Al analizar los dos tipos de sistemas de control industrial más populares en la región, Trend Micro concluyó que muchos de estos dispositivos estaban conectados al internet.



Number of Internet-Facing SCADA and VxWorks Devices in the Americas and the Caribbean
Fuente: http://www.shodanhq.com/

Aunque el uso de sistemas de control industrial conectados al internet no es peligroso en sí, muchos de los sistemas que se muestran en la Figura 1 no tenían protección por contraseña ni mantenían actualizados los parches de seguridad más recientes, lo cual los dejaba expuestos a ataques. Un estudio realizado por Trend Micro indicó que los sistemas de control industrial conectados al internet sufren ataques diariamente. Los datos demuestran que en un lapso de 28 días se registró un total de 39 ataques de 14 países distintos. De estos 39 ataques, 12 fueron únicos y podrían clasificarse como "focalizados", mientras que 13 fueron repetidos por varios de los mismos agentes en el transcurso de varios días y podrían considerarse "focalizados" o "automatizados."[4]

4 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf

Informes de los países sobre delincuencia cibernética

Toda la información contenida en esta sección provino de informes presentados por Estados miembros de la OEA.

Tendencias de la delincuencia cibernética en Chile

En 2012, el número de incidentes cibernéticos que condujeron a investigaciones y respuestas en Chile se redujo en un 33%, según lo informó la unidad de delincuencia cibernética de la policía federal. El número de incidentes de fraude electrónico basados en el internet —a menudo ataques tipo phishing y pharming— se redujo en un 122% en términos globales. Las autoridades atribuyeron la reducción en este tipo de incidentes, que constituyeron una alta proporción del tráfico delictivo en la web del país, al desmantelamiento de un notorio sindicato responsable de la distribución a gran escala de programas maliciosos utilizados a menudo para defraudar a bancos y personas individuales. Chile observa que muchos delitos involucran ahora elementos de explotación del internet, pues los narcotraficantes y otros delincuentes emplean la web para facilitar sus actividades. La prevalencia de delitos basados en el internet en ese país saca a relucir las dificultades en la cooperación internacional, que se citó en Chile como el mayor obstáculo para responder, investigar y disuadir los incidentes cibernéticos.

Tendencias de la delincuencia cibernética en Colombia

De acuerdo con el colCERT —el CSIRT nacional de Colombia— ese país registró menos incidentes cibernéticos en 2012 que en 2011, lo que lo coloca junto con Chile como uno de los pocos países latinoamericanos con esa distinción. No obstante, no es claro si esto se debió a una reducción real en el número de incidentes, a una mejor gestión de la seguridad por parte de las agencias gubernamentales atendidas por los CSIRT o a la implementación de políticas que cambiaron la cobertura de la asistencia prestada por los equipos de respuesta de Colombia.

Sea como fuere, el fraude fue el tipo de incidente cibernético más común reportado por el colCERT en 2012. Contribuyó notablemente a esta cifra la captura en Colombia, el año pasado, de un prolífico delincuente cibernético, Jorge Maximiliano Pachón Viola. Apodado el “zar de la clonación”, Viola había cometido fraudes en por lo menos siete países latinoamericanos y finalmente fue arrestado con más de 8.000 tarjetas de crédito clonadas a la mano y tras amasar más de US$9 millones.[5]

La lista de incidentes cibernéticos de Colombia contiene además distintos tipos de haqueo y spoofing de páginas web. Más de uno de los equipos de respuesta del país reportó ataques de hactivistas, dirigidos en su mayoría contra entidades estatales y militares e instituciones financieras.

El gobierno colombiano reportó bajos niveles de conciencia de la seguridad cibernética, lo que precipitaba hábitos de navegación inseguros y había provocado la defraudación de usuarios del internet vulnerables. Además, la insuficiente capacitación de la policía sobre ataques avanzados, las dificultades para preservar y examinar evidencias digitales y la falta de cooperación de los proveedores de servicios de internet y otras organizaciones privadas constituyeron impedimentos importantes para poner freno a la delincuencia cibernética en Colombia.

5 http://latinamericacurrentevents.com/head-of-major-credit-card-cloning-ring-arrested-in-colombia/18040/

Tendencias de la delincuencia cibernética en Jamaica

El gobierno jamaiquino reportó un incremento del 14% en el número de incidentes cibernéticos en 2012, la mayoría dirigidos contra instituciones públicas. No obstante, las instituciones financieras y un prominente proveedor de servicios de infraestructura crítica también fueron objeto de incidentes de haqueo de alto perfil. La encuesta reveló que, al igual que en Chile, la tecnología de la información y las comunicaciones fue un componente de muchos delitos en Jamaica en 2012. La frecuencia creciente de incidentes cibernéticos en Jamaica se complica por la ausencia de personal capacitado para responder a ellos o para investigación digital, la inadecuada cooperación interna e internacional y una falta de medidas proactivas para frenar a hackers y atacantes.

La conciencia sobre la seguridad cibernética en Jamaica sigue siendo baja en general, aunque el gobierno ha emprendido una campaña de sensibilización a gran escala dirigida a los estudiantes.

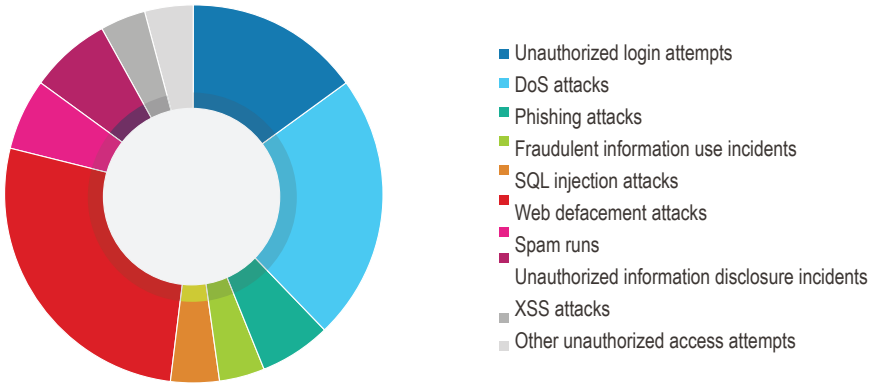
Tendencias de la delincuencia cibernética en México

Las autoridades mexicanas registraron un incremento del 40% en el número de incidentes cibernéticos en 2012, en buena parte debido a ataques de hactivistas. A pesar de disponer de varias unidades encargadas de responder y analizar incidentes cibernéticos, el país todavía cita la ausencia de normas legislativas y conciencia del público como las razones de la falta de seguridad cibernética.

Los ataques más graves en 2012 se dirigieron contra infraestructuras gubernamentales creadas y empleadas específicamente para apoyar las elecciones presidenciales en julio. Los hackers lanzaron ataques distribuidos de denegación de servicio (DDoS), vandalizaron páginas web y llevaron a cabo ataques de secuencias de comandos en sitios cruzados (XSS) e inyecciones SQL. Los técnicos de respuesta a incidentes estaban bien equipados para abordar estos ataques, ya que fueron semejantes a otros incidentes de hactivistas que habían ocurrido a lo largo de 2012.

Tendencias de la delincuencia cibernética en Panamá

El principal tipo de incidente cibernético registrado en Panamá fue el vandalismo de páginas web, con un 27% de todos los casos que manejó el CSIRT-PANAMÁ —el equipo nacional de respuesta a incidentes del país— seguido cercanamente por los ataques de DDoS (23%) y los intentos de inicio de sesión no autorizado (15%).



Most Dominant Cyber-Incident Types Reported in Panama
Fuente: Encuesta de la OEA.

Los casos de phishing (6%), uso fraudulento de información (4%), inyección de SQL (4%), spamming (6%), divulgación de información no autorizada (7%), uso de XSS (4%) y otros intentos de acceso no autorizado (4%) completaron el gráfico de ataques. La mayoría de los incidentes en Panamá se registraron durante el tercer trimestre de 2012. Las autoridades relacionan este hecho con la introducción de la Ley 510 en agosto, con la que se intentó ampliar los mecanismos de aplicación jurídica contra violaciones de derechos de autor y que produjo respuestas ruidosas y muy publicitadas de hactivistas.

A estos incidentes cibernéticos se vincularon informes de las autoridades panameñas en el sentido de que los centros de servicio al cliente con frecuencia tenían más acceso del necesario a la información personal de sus clientes, situación que expone innecesariamente a las personas a amenazas internas. Los centros de servicio también con frecuencia estaban expuestos a ataques de DDoS, lo que complica los riesgos para la información delicada, que a menudo también se almacena en forma precaria.

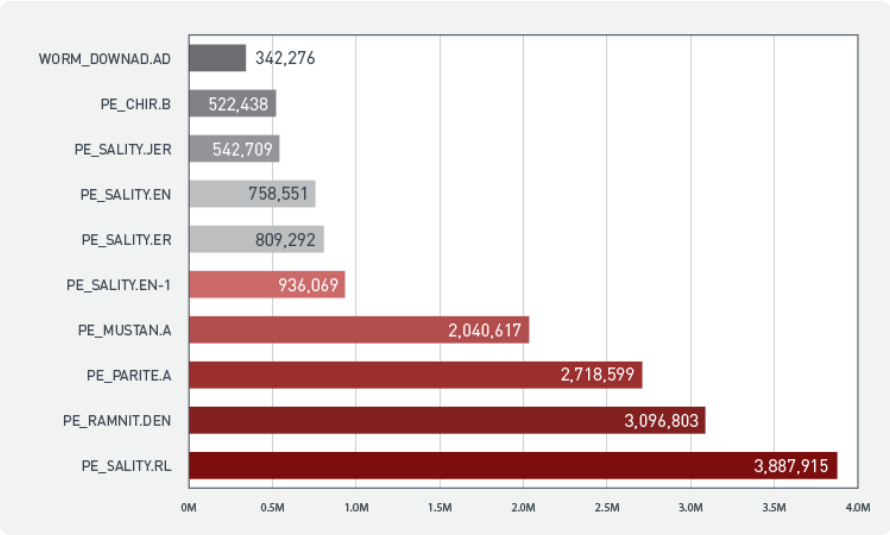
Panamá citó la falta de especialistas forenses digitales y de respuesta a incidentes calificados como el principal obstáculo en la lucha contra la delincuencia cibernética. Las autoridades culpan de muchos incidentes cibernéticos a la falta de conciencia a gran escala, incluso después de las investigaciones, pues muchas veces se determinó que los ataques eran evitables. Esto se debe al hecho de que los usuarios del internet se resisten a aprender sobre seguridad cibernética, pues consideran que los hábitos de computo seguros son demasiado complejos o técnicos para aprenderlos bien. Aunque varias instituciones financieras difundieron materiales educativos, estas actividades estuvieron mal coordinadas y las campañas de sensibilización pequeñas no lograron el impacto deseado. Para combatir las actitudes laxas hacia la seguridad en el uso del internet, el gobierno está planeando actualmente más iniciativas de sensibilización en 2013.

Análisis de inteligencia sobre amenazas globales de Trend Micro

Malware

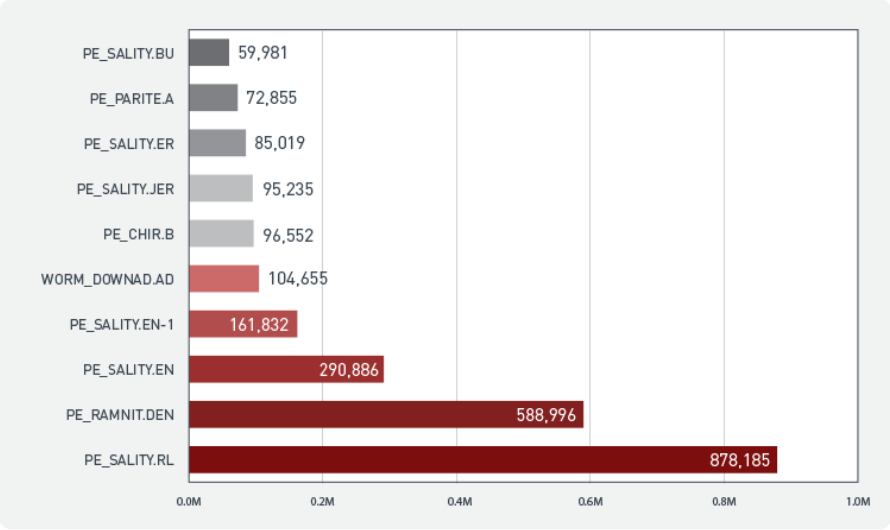
En 2012, América Latina y el Caribe se vieron afectados más por infecciones de archivos que por cualquier otro tipo de software malicioso, lo que a menudo indica la prevalencia de dispositivos de almacenamiento portables insuficientemente asegurados y la falta de parches en los sistemas operativos o aplicaciones.

Los 10 principales programas maliciosos en las Américas y el Caribe en 2012



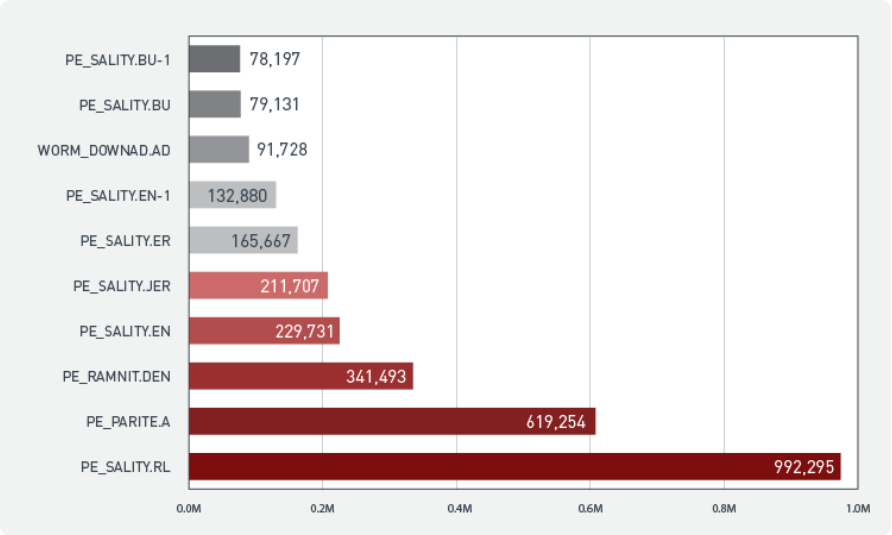
Fuente: Trend Micro Smart Protection Network.

Los 10 principales programas maliciosos en las Américas y el Caribe en el primer trimestre de 2012



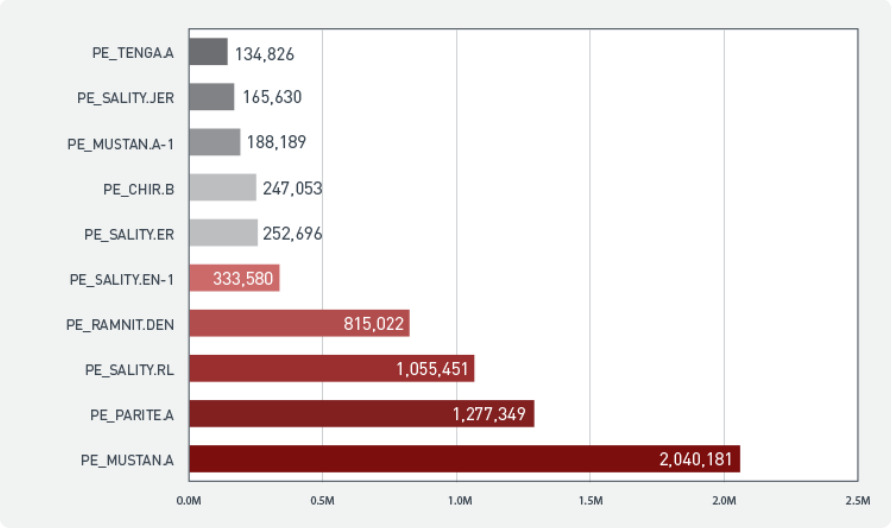
Fuente: Trend Micro Smart Protection Network.

Los 10 principales programas maliciosos en las Américas y el Caribe en el segundo trimestre de 2012



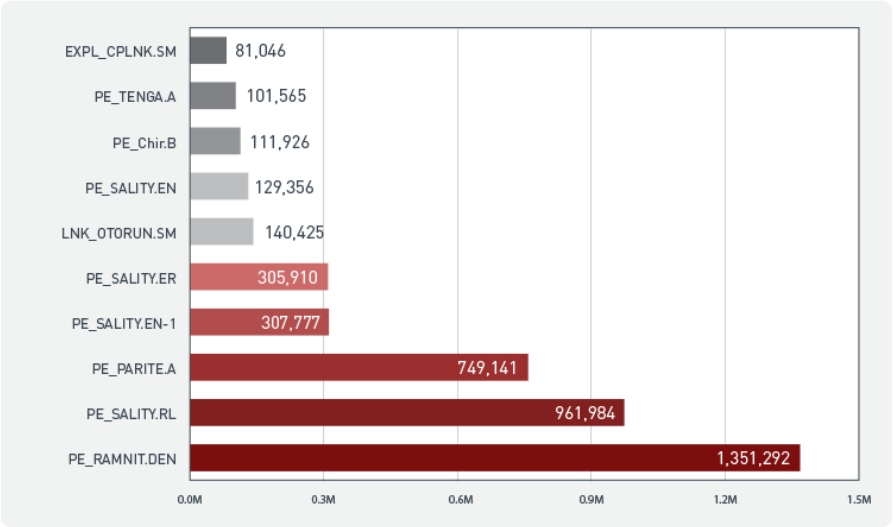
Fuente: Trend Micro Smart Protection Network

Los 10 principales programas maliciosos en las Américas y el Caribe en el tercer trimestre de 2012



Fuente: Trend Micro Smart Protection Network

Los 10 principales programas maliciosos en las Américas y el Caribe en el cuarto trimestre de 2012



Fuente: Trend Micro Smart Protection Network

Spam

El volumen mundial de spam (o "correos basura") se ha ido reduciendo desde 2011 debido a enormes desmantelamientos de botnets y otras operaciones policiales relacionadas con este tipo de mensajes de correo. Sin embargo, falta mucho para que el volumen de spam toque fondo. En 2012, entre los países de América Latina y el Caribe cubiertos por este informe, el principal país originador de spam fue México, seguido por Argentina y Colombia.

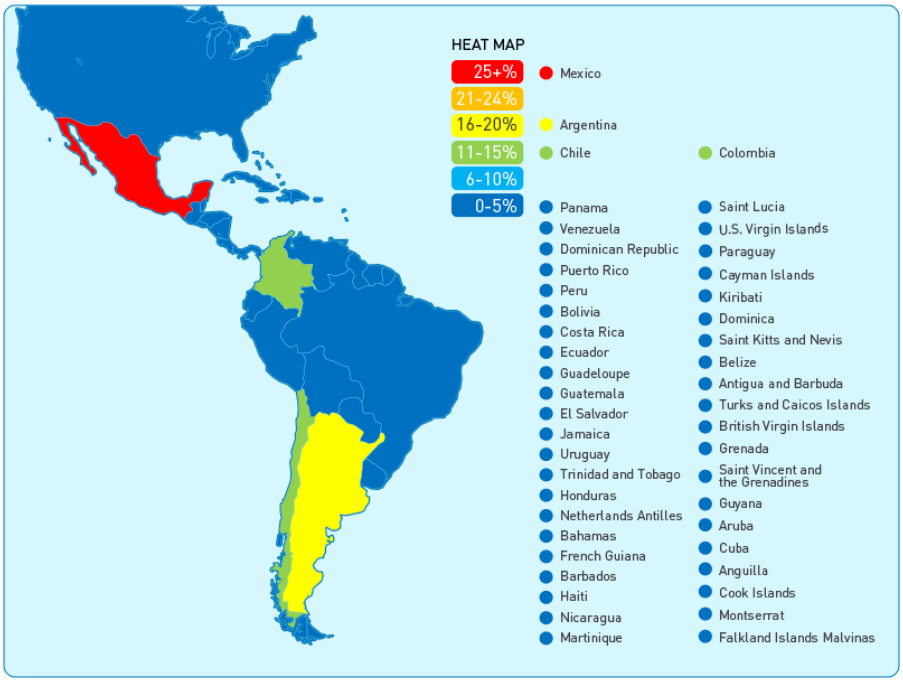
Desglose de países originarios de spam en América Latina y el Caribe (sin incluir a Brasil)

Fuente: Trend Micro Smart Protection Network

URLs maliciosos

El hospedaje de sitios maliciosos es un grave problema en las Américas y el Caribe. Los dos principales países originarios de spam también ocupan los primeros lugares en la lista de países que albergaron el mayor número de URLs maliciosos. Colombia—país que ocupó el tercer lugar en envío de spam— fue reemplazado por Chile en la lista de principales alojadores de URLs maliciosos.

Desglose de países que hospedan URLs maliciosos en América Latina y el Caribe (sin incluir a Brasil)



Fuente: Trend Micro Smart Protection Network

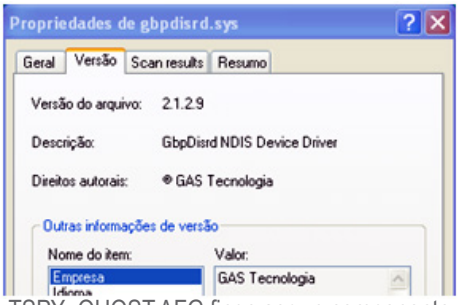
Actividades clandestinas

Robos bancarios en línea y uso de crimeware

El robo bancario en línea se ha reportado ampliamente en América Latina. Estas actividades tienen características distintivas, que dependen del país o banco al que están orientadas y de la naturaleza de las medidas de autentificación y seguridad que protegen sus datos financieros.

Los delincuentes cibernéticos constantemente han encontrado formas de socavar las medidas de seguridad bancaria en cuanto se mejoran o actualizan, lo que convierte en una tarea especialmente difícil y en continua evolución mantener la seguridad de las redes financieras. Si un banco emplea un mecanismo simple de autentificación que implica solamente un nombre de usuario y una contraseña, se utilizan dispositivos de registro de teclado para obtener acceso. Los bancos que usan sistemas de contraseñas de un solo uso se inyectan con secuencias de comandos de sistemas de transferencia automatizados que ocultan las transacciones ilícitas.[6] Al igual que los sistemas de transferencia automatizados, también se usan objetos de ayuda del explorador contra sistemas complejos que implementan autentificación de dos o tres factores. Estas técnicas demuestran el ingenio de los delincuentes cibernéticos, que para cada avance en la seguridad bancaria en línea encuentran una forma igualmente innovadora para evadirlo.

La mayoría de los paquetes de crimeware sofisticados utilizan troyanos populares de banca en línea derivados de la familia de paquetes delictivos de la familia de BANCOS. El software malicioso BANCOS a menudo funciona como los rootkits, eliminando los componentes de seguridad en las computadoras víctimas que usan para obtener acceso a cuentas bancarias. Aunque estos kits se han utilizado ampliamente durante años, apenas se empezaron a considerar como una amenaza significativa en las Américas y el Caribe debido a la laxitud de la seguridad y a la falta de conciencia.[7]



TSPY_QHOST.AFG finge ser un componente de un plug-in de un sitio bancario legítimo para introducirse en las computadoras de las víctimas.

TSPY_QHOST.AFG es un ejemplo de un troyano de BANCOS. / A diferencia de la mayoría de las cepas, no solamente cambia el archivo host de una computadora infectada, sino que además utiliza funciones avanzadas singulares para evitar la detección de los programas de eliminación de malware.

Address	Length	Type	String
.rdata:00010D80	00000054	unicode	_BB_F=_ZLQGRZV_v|vwhp65_gulyhuv_hwf_krvwv
.rdata:00010DD8	0000004C	unicode	_BB_F=_surjudp#ilohv_jesoxjlq_lvj1jsf
.rdata:00010E28	0000005C	unicode	_BB_F=_dutxlyrv#gh#surjudpdv_jesoxjlq_lvj1jsf
.rdata:00010E88	00000056	unicode	_BB_F=_surjudp#ilohv_jesoxjlq_jelhklvj1goo
.rdata:00010EE0	00000066	unicode	_BB_F=_dutxlyrv#gh#surjudpdv_jesoxjlq_jelhklvj1goo
.rdata:00010F48	00000070	unicode	_BB_F=_ZLQGRZV_Grzqordghg#Surjudp#Ilohv_JeSoxjlqlvj1lqi
.rdata:00010FB8	0000005C	unicode	_BB_F=_zlqgrzv_v|vwhp65_gulyhuv_jesqglvug1v|v
.rdata:00011018	0000006A	unicode	_BB_F=_zlqgrzv_Grzqordghg#Surjudp#Ilohv_vfsvvvk51lqi
.rdata:00011088	0000004A	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsYlvwd1h{h
.rdata:000110D8	0000004A	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsvvvk51goo
.rdata:00011128	00000046	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsOLE1goo
.rdata:00011170	00000046	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsPLE1goo
.rdata:000111B8	00000050	unicode	_BB_F=_surjudp#ilohv_Vfsdg_vfsvvvk51goo
.rdata:00011208	0000004C	unicode	_BB_F=_surjudp#ilohv_Vfsdg_vfsOLE1goo

TSPY_QHOST.AFG encripta cadenas para evitar la detección y complicar los análisis.

6 http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf
7 http://blog.trendmicro.com/trendlabs-security-intelligence/new-crimeware-in-bancos-paradise/

Los delincuentes cibernéticos en las Américas y el Caribe también utilizan cambiadores del Sistema de Nombres de Dominio (DNS) y troyanos de acceso remoto (RAT). Cambian las configuraciones del proxy o añaden información al archivo host para violar los sistemas de banca en línea.

Las herramientas que acabamos de describir se transmiten con mayor frecuencia incrustando vínculos maliciosos en mensajes de correo spam o en sitios web convincentes de phishing.

Cybercriminal Underground

El desmantelamiento a gran escala de botnets en todo el mundo en los últimos años, incluido el de Esthost en 2011, han obligado a los delincuentes cibernéticos a modificar sus tácticas.[8] Ahora se esfuerzan por configurar sus propios servidores en centros de datos en todo el mundo en lugar de usar servidores secuestrados para hospedar sus infraestructuras, herramientas de spam y otros componentes operativos para comando y control. Evitan registrar nombres de host o dominios para sus servidores y usan solamente direcciones del Protocolo de Internet (IP) para evitar ser indexados por los motores de búsqueda, como Google.

En contraste con la preferencia por servidores pagados y de proxy que manifiestan los delincuentes en Europa Oriental, los de América Latina prefieren usar servicios de hospedaje gratuitos.[9] El software malicioso, los servidores de comando y control, las páginas de phishing y otros contenidos maliciosos que emplean los delincuentes cibernéticos en América Latina a menudo se alojan en Dot TK u otros sitios de hospedaje gratuito en la web con sede en Europa Oriental. Los delincuentes cibernéticos aprovechan los servicios que ofrecen lapsos de evaluación gratuita para registrar dominios maliciosos y robar información de los usuarios. Con ello no solamente obtienen acceso durante una semana cuando mucho, sino que también pueden ocultar pruebas y encubrir su huella digital. Los paquetes de crimeware y los datos que roban a menudo se comercian y comparten en sitios de redes sociales. Orkut, y no Facebook, es el mercado líder en América Latina.

8 http://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/

9 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

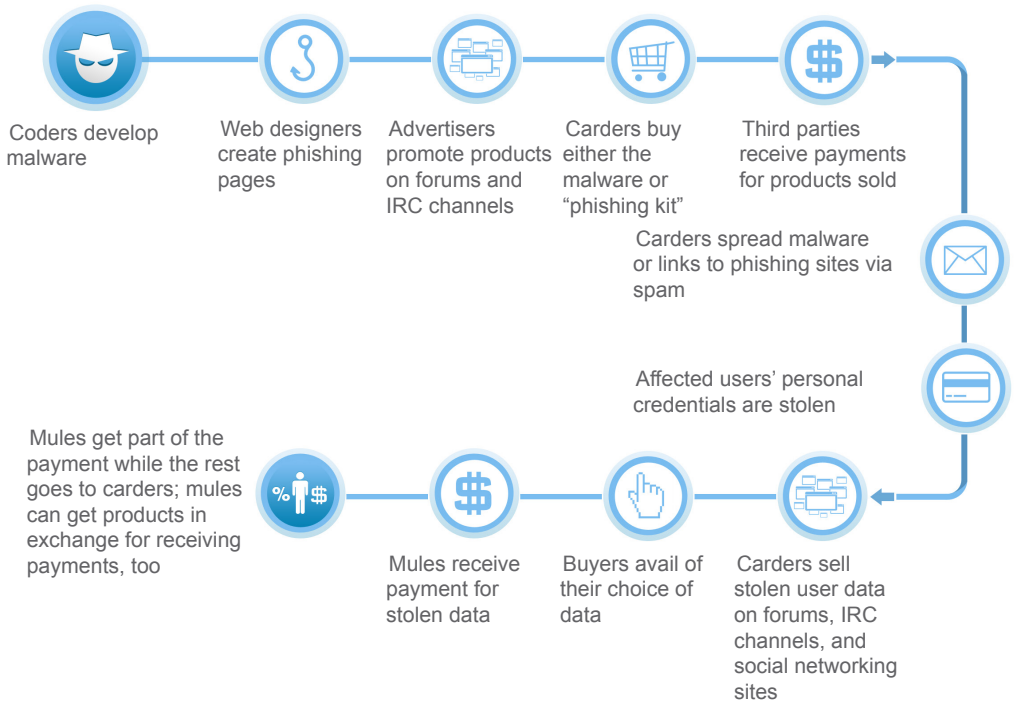
Son frecuentes los mensajes en Orkut que ofrecen diversos productos de software para actividades ilícitas en América Latina.

Al igual que en muchas regiones, los servidores de Internet Relay Chat (IRC), los foros de hackers y otros canales se usan para comprar y vender información sobre tarjetas de crédito, paquetes de crimeware y demás información de identificación personal.

También son comunes en los foros los mensajes relacionados con actividades de delincuencia cibernética

En contraste con las normas mundiales, los delincuentes cibernéticos en América Latina usan servicios de transferencia de dinero comunes para pagar los bienes y servicios de los delincuentes cibernéticos. Puesto que esto puede conducir a su identificación por parte de las autoridades, los delincuentes cibernéticos contratan mulas para llevar a cabo las transacciones. Además, sistemas como Webmoney se están usando mucho más ampliamente, como lo comprueba la creciente colaboración internacional entre los delincuentes cibernéticos que operan en América Latina y en Europa Oriental.

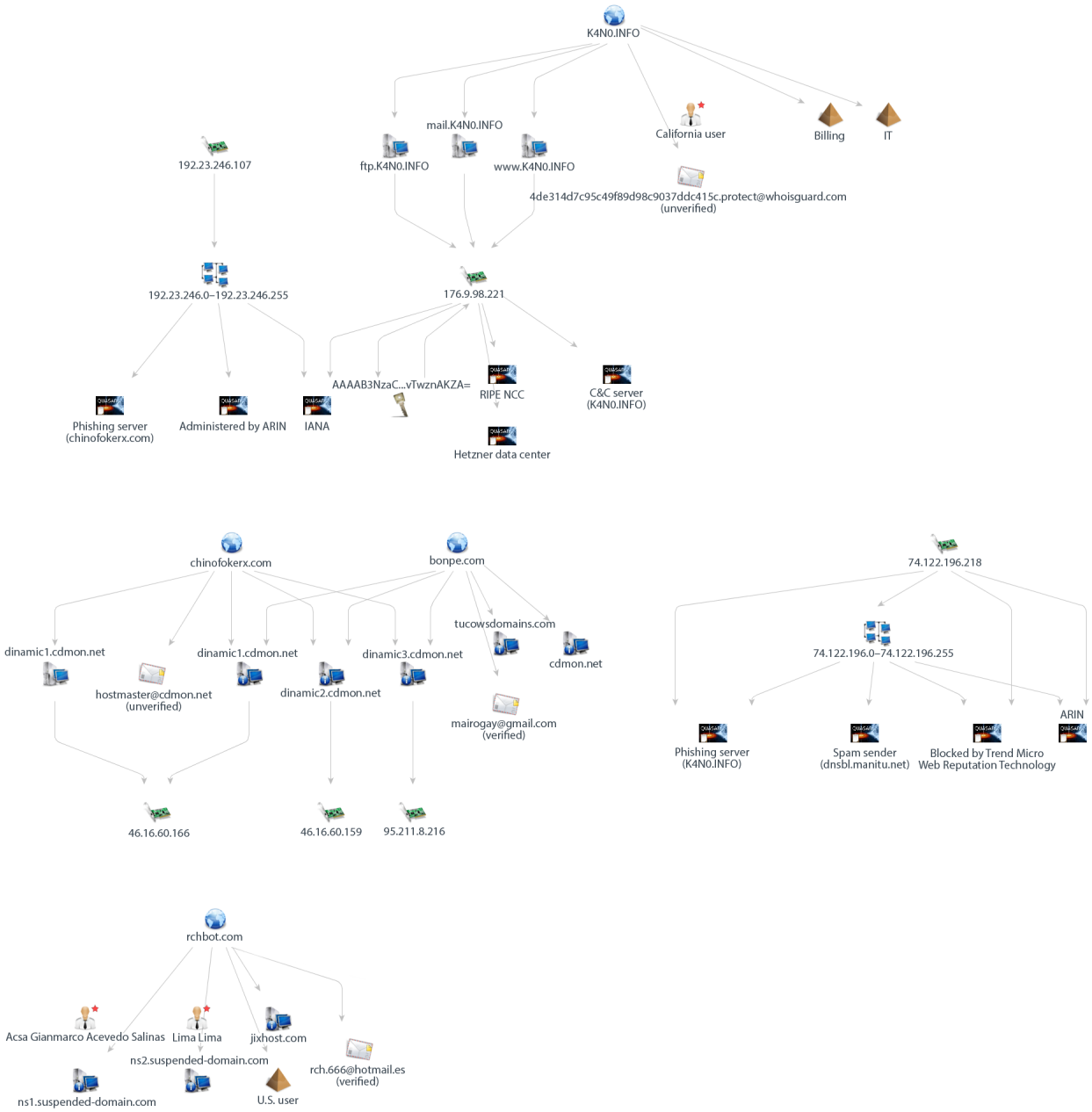
Cybercriminal Business Model in Latin America



PiceBOT

Los delincuentes cibernéticos en los Estados miembros de la OEA están teniendo cada vez mayor éxito en el diseño y la construcción a la medida de sus propios paquetes de crimeware. En diciembre de 2012 se introdujo en América Latina PiceBOT, un nuevo equipo de crimeware con un costo de US$140. El malware asociado con PiceBOT —que fue producido en la región— roba información financiera de usuarios desprevenidos. PiceBOT anunció una nueva era de sofisticación en las amenazas cibernéticas en las Américas y el Caribe. El software malicioso se producirá cada vez más en casa y se usará contra los gobiernos, el sector privado y los ciudadanos. La mayor prevalencia de equipos de crimeware que emplean nuevos códigos maliciosos significa que ahora más que nunca los sistemas de seguridad tendrán que luchar para mantenerse actualizados, identificar y parchar vulnerabilidades y en general seguirles el ritmo a los delincuentes cibernéticos.

Botnet Estructura de PiceBOT



Fuente: Trend Micro

Situación de la seguridad cibernética en las Américas

Cada país aborda de manera distinta la seguridad cibernética, dependiendo de su panorama económico, político y cultural imperante. Algunos países consideran la seguridad cibernética principalmente como un asunto de seguridad nacional y defensa. Otros opinan que tiene un mayor impacto en el desarrollo económico o en la competitividad internacional. Otros más la ven como un factor clave para la educación, la interacción social y la gobernanza centrada en los ciudadanos, aunque, sabiamente, muchos países están tratando de incorporar todas estas consideraciones en sus regímenes de seguridad cibernética. A pesar de la variedad de enfoques, están surgiendo estudios de casos que ayudarán más eficientemente a todos los países a mejorar sus políticas de seguridad cibernética.

Muchos gobiernos están enfrentando avances tecnológicos rápidos con burocracias que se adaptan con lentitud, lo que les suministran a los hackers y a las organizaciones ilícitas vías para operar sin preocuparse mucho por ser perseguidos o capturados. Uno de los principales impedimentos para frenar las actividades cibernéticas ilícitas en 2012 fue la falta de legislación adecuada y políticas robustas de seguridad cibernética. Conjuntamente con la falta de experiencia de los investigadores de delincuencia cibernética y la escasez de fiscales especializados en delitos relacionados con tecnologías, muchos países están encontrado dificultades para frenar y procesar judicialmente a los hackers y a otros delincuentes cibernéticos.

En las encuestas que se le devolvieron a la OEA, los países hablaron invariablemente de la necesidad de profesionales altamente capacitados que puedan asegurar las redes, diagnosticar intrusiones y manejar eficazmente los incidentes cibernéticos cuando ocurren. Este problema se manifiesta en la región en las bajas tasas de matrícula en programas de formación técnica. Dado el tiempo que se requiere para adquirir habilidades y experiencia práctica en seguridad cibernética, esta tasa baja de matrícula podría tener un impacto tangible en los próximos años.

Las dificultades que enfrentan quienes responden a los incidentes, al igual que los investigadores, fiscales y administradores de redes, se complican por el nivel persistentemente bajo de conciencia sobre la seguridad cibernética entre los usuarios del internet. Los gobiernos opinaron que el interés público en la seguridad cibernética seguía siendo volátil y desigual, y la mayoría no han implementado campañas de sensibilización eficaces y de gran escala.

En cualquier caso, la mayor frecuencia de los ataques y la publicidad asociada que recibieron generaron modificaciones en las actitudes y mejoras concretas en la seguridad cibernética en la región. Aunque los usuarios del internet siguen desentendiéndose en gran medida de los riesgos que plantean las amenazas cibernéticas, los gobiernos se están viendo motivados a actuar y a obtener resultados positivos de sus esfuerzos. Varios países han adoptado marcos integrales contra la delincuencia cibernética, tomando en cuenta tanto las disposiciones procesales como de derecho sustantivo. Otros han expresado interés por adoptar este tipo de marcos y han empezado a reunir recursos y voluntad política para ello. Incluso los países que disponen de marcos jurídicos sólidos, empero, siguen enfrentando dificultades para implementar e institucionalizar nuevas normas, lo que subraya el efecto devastador de los bajos niveles de experiencia en seguridad de la información.

* Favor de tomar nota de que la información contenida en esta sección proviene de las encuestas de países de la OEA.

Políticas gubernamentales de seguridad cibernética

Muchos Estados miembros de la OEA iniciaron sus esfuerzos en materia de seguridad cibernética con el establecimiento de CSIRTs. De hecho, la mayoría de los países, exceptuando a algunos del Caribe, disponen ya de capacidad de respuesta a incidentes a nivel nacional. Estos CSIRTs presentan todo un espectro en cuanto a su desarrollo. Algunos prestan servicios distintos de respuesta y prevención de incidentes, mientras que otros todavía están enfrentando dificultades para proteger sus redes. Los problemas que enfrenta este último grupo se complican por las dificultades para obtener recursos humanos y financieros, lo que impide que mejoren sus operaciones. Incluso los Estados del Caribe que no han establecido todavía un CSIRT nacional reconocen la importante función que desempeña la seguridad cibernética en el desarrollo social y económico. Algunos tienen laboratorios cibernéticos forenses o pondrán en funcionamiento su CSIRT en un futuro cercano. Aun así, sigue habiendo obstáculos significativos, incluyendo algunos específicos de los pequeños estados insulares. Incluso cuando podría no parecer lógico operar un CSIRT, los países del Caribe están adoptando otras medidas prácticas para mitigar los riesgos a la seguridad cibernética, como aumentar la conciencia del problema o fortalecer las unidades policiales de delincuencia cibernética, aunque la mayor parte de los gobiernos están de acuerdo en que es necesario hacer más.[10]

La respuesta a incidentes representa solamente un área de la seguridad cibernética en que los Estados de América Latina y el Caribe han exhibido progresos significativos. Muchos están siguiendo la tendencia reciente establecida por países como Canadá, Estonia, Alemania, Japón, el Reino Unido y Estados Unidos y han empezado a redactar políticas y estrategias nacionales integrales de seguridad cibernética. Con el apoyo de la OEA, Colombia se convirtió en el primer país latinoamericano en adoptar una estrategia nacional integral de ciberseguridad y ciberdefensa. Países como Chile, Perú, México, Trinidad y Tobago, Uruguay y otros se están esforzando por hacer lo mismo. Las estrategias de América Latina y el Caribe emulan las adoptadas por los gobiernos de Norteamérica y Europa, identifican a las partes interesadas clave, delinean funciones y responsabilidades, establecen mecanismos de coordinación e intercambio de información y formulan planes de acción estratégicos para las actividades nacionales de seguridad cibernética.

10 Se alcanzaron algunos acuerdos en un taller de capacitación en materia de delito cibernético y seguridad cibernética para el Caribe en agosto de 2012, así como durante la reunión de la Comisión de Seguridad Hemisférica del Consejo Permanente de la OEA sobre "Preocupaciones especiales de seguridad de los pequeños estados insulares del Caribe" en 2013.

El reciente reconocimiento de las vulnerabilidades en la infraestructura crítica ha instado a varios Estados miembros de la OEA a adoptar iniciativas orientadas a fortalecer la seguridad de sus sistemas de control industrial. Argentina, por ejemplo, será en 2013 el primer país latinoamericano sede de una Conferencia Meridian sobre protección de infraestructuras críticas.[11] El desarrollo de una estrategia nacional por parte de Panamá también hizo hincapié en la importancia de proteger sistemas de control industrial importantes, en especial aquellos que en caso de verse comprometidos pueden tener efectos negativos a escala global. México también ha reconocido los graves riesgos que plantean las amenazas a los sistemas de control industrial y ha apoyado la capacitación especializada para muchos de sus técnicos en respuesta a incidentes. Estos tres países son solamente algunos de los que están actuando para asegurar los crecientemente importantes pero todavía vulnerables sistemas de control industrial en la región. Muchos otros están analizando medidas técnicas o de política para proteger su infraestructura más importante.

Esfuerzos interamericanos en seguridad cibernética

En términos globales, los Estados miembros de la OEA han mostrado unidad cuando se trata de asuntos de seguridad cibernética. Mientras que la Unión Europea (UE) adoptó una Estrategia de Seguridad Cibernética en febrero de 2013, los Estados miembros de la OEA ya habían adoptado por unanimidad la Estrategia Interamericana Integral de Seguridad Cibernética nueve años antes, en 2004. Conforme fueron evolucionando el panorama de las amenazas y los esfuerzos de los gobiernos, también aprobaron una declaración sobre "Fortalecimiento de la Seguridad Cibernética en las Américas" en marzo de 2012. La adopción de estos documentos prueba que aunque todavía queda mucho por hacer y los Estados comulgan con distintas opiniones sobre la mejor forma de lograr la seguridad cibernética, existe un consenso político sólido en el Hemisferio Occidental, lo que ayuda a facilitar la cooperación regional y el intercambio de información. Trabajando con la OEA y a través de ella, los Estados miembros han logrado llegar a un acuerdo sobre un tema difícil. Los acuerdos han generado un entorno colaborativo y en última instancia han permitido que la Secretaría General de la OEA suministre asistencia técnica y mejore la seguridad cibernética de los Estados miembros en múltiples niveles.

Estudios de casos

Argentina

El gobierno argentino estableció la Oficina Nacional de Tecnologías de Información (ONTI) para evaluar y poner en marcha un sistema de modernización y uso eficiente de los recursos digitales. A través de esta Oficina se estableció en 2005 el Equipo de Respuesta ante Emergencias Informáticas (ArCERT), que hizo de Argentina uno de los primeros países en América Latina en operar un CSIRT nacional. Los primeros esfuerzos se enfocaron en la inclusión digital y el acceso universal y en la sensibilización sobre seguridad cibernética.

Para mitigar las amenazas emergentes a los sistemas de control industrial, en 2012 Argentina creó el ICIC —Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad—, al que se le ha encargado específicamente la protección de la infraestructura crítica del país.

11 https://www.meridian2012.org/pages/the-conference

La ONTI está trabajando actualmente en el segundo borrador del Plan Nacional de Ciberseguridad y Protección de Infraestructura Crítica 2013-2015. Este plan se basa en cuatro pilares: sensibilización, protección de los activos digitales, promoción de la comprensión judicial y académica de la seguridad de la información y la infraestructura de información crítica y fomento de alianzas de seguridad duraderas entre el gobierno, las empresas y las organizaciones de la sociedad civil.

Colombia

A mediados de febrero de 2012, Colombia encabezó la operación Unmask, una operación multinacional dirigida a desmantelar una banda transnacional de delincuentes cibernéticos y hactivistas, que se integró como respuesta a ataques persistentes contra infraestructura crítica en Chile y Colombia. Esta operación se caracterizó por depender de la colaboración entre equipos de respuesta a incidentes y cuerpos policiales de Argentina, Chile, Colombia y España. De hecho, se llevaron a cabo redadas simultáneamente en 40 sitios en 15 ciudades distintas. En total, la operación Unmask condujo al arresto de 25 delincuentes y al decomiso de 250 dispositivos informáticos, junto con numerosas tarjetas de crédito y efectivo producto de robos.[12]

En 2011, Colombia adoptó una estrategia integral de ciberseguridad y ciberdefensa conocida como el "CONPES 3701". Los aspectos técnicos de la ciberseguridad y la ciberdefensa del CONPES están a cargo de tres instituciones:

- **El Centro Cibernético Policial (CCP),** responsable de asegurar la integridad de las redes policiales y de la sociedad civil y que mantiene una vigorosa capacidad de investigación.
- **El Comando Conjunto Cibernético (CCOC),** una unidad militar que responde a ataques contra los bienes militares de la nación.
- **El colCERT,** la entidad coordinadora a nivel nacional que supervisa todos los aspectos de la ciberseguridad y la ciberdefensa.

Colombia solicitó recientemente su adhesión a la Convención sobre la Delincuencia Cibernética del Consejo de Europa y espera unirse a este tratado en 2013, lo que complementará su política y sus avances técnicos con un conjunto robusto de legislación sobre delincuencia cibernética.

Jamaica

En 2012, Jamaica revisó su legislación sobre delincuencia cibernética, amplió la capacidad de la Unidad de Comunicación Forense y Delincuencia Cibernética (CFCU) de la policía jamaiquina y avanzó en el establecimiento formal de un CSIRT. La CFCU demostró sus capacidades técnicas e investigativas cuando se encargó de la investigación y detención de un hacker de alto perfil que había atentado contra la infraestructura crítica del país. Para conservar la paridad con las amenazas emergentes, esta unidad mantiene un laboratorio digital forense sólido que constantemente se audita y actualiza.

El Ministerio de Ciencia, Tecnología, Energía y Minería jamaiquino ha encabezado los esfuerzos del gobierno para mejorar su estrategia y su política de seguridad cibernética. En 2012, este Ministerio supervisó la creación del Grupo de Trabajo de Seguridad Cibernética Nacional, que comprende a todas las dependencias gubernamentales correspondientes y otras partes interesadas.

12 http://www.interpol.int/News-and-media/News-media-releases/2012/PR014

México

El gobierno mexicano tenía inicialmente una sola unidad en la Secretaría de Seguridad Pública encargada de responder a las amenazas cibernéticas. La mayor frecuencia de los incidentes cibernéticos impulsó la creación de una nueva Coordinación para la Prevención de Delitos Electrónicos. Esta Coordinación es responsable del manejo de las respuestas a incidentes cibernéticos, la investigación de delitos electrónicos, el análisis de pruebas digitales, la protección de la infraestructura crítica y las respuestas a amenazas digitales que pudieran afectar la integridad de redes críticas.

Además se creó el Equipo Nacional Especializado Nacional de Respuesta a Incidentes Cibernéticos para aumentar la capacidad de respuesta gubernamental a estos incidentes. Los técnicos de este equipo son altamente calificados y se les imparte capacitación continua para asegurar su conocimiento de las herramientas y técnicas de haqueo emergentes. Este grupo monitorea y protege los activos digitales del gobierno federal.

Panamá

En marzo de 2013, Panamá adoptó oficialmente su Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, con lo que se unió a Colombia como el único país latinoamericano con un plan integral de seguridad cibernética. Esta estrategia se basa en seis pilares:

1. Asegurar la privacía y la confianza en el uso de las tecnologías de la información y las comunicaciones.

2. Eliminar el uso ilícito de las tecnologías de la información y las comunicaciones. Ensuring continuity of critical infrastructures.

3. Asegurar la continuidad de la infraestructura crítica.Promoting a culture of cybersecurity.

4. Desarrollar normas de seguridad cibernética benévolas para la industria.

5. Promover una cultura de seguridad cibernética.

6. Proteger las redes estatales.

La estrategia se implementará gradualmente a través de 43 tareas o procesos específicos, que incluyen el desarrollo de una campaña nacional de sensibilización a gran escala y la creación de CSIRTs para sectores específicos.

Panamá también presentó una solicitud formal para adherirse al Convenio de Budapest sobre el Cibercrimen del Consejo de Europa.

Conclusión

Estamos viviendo actualmente un período decisivo en materia de seguridad cibernética. Las noticias sobre incidentes cibernéticos de gran escala llenan los informes diarios y se están convirtiendo cada vez más en objeto de deliberaciones políticas y augurios apocalípticos. Nuestro mayor temor—de que ataques cibernéticos arrasen con la infraestructura o generen caos y depresión económica—afortunadamente no se ha hecho realidad todavía. Pero es necesario hacer más para seguirles el ritmo a quienes se proponen explotar las vulnerabilidades digitales. En las Américas y el Caribe, las personas necesitan tomar nota de la forma en que utilizan el internet y asegurarse de adoptar todas las precauciones posibles para proteger sus datos y sus aparatos contra abusos. El internet es un bien compartido, y la seguridad cibernética es una responsabilidad compartida, lo que significa que es necesario que los individuos adquieran un sentido de propiedad y pongan en práctica buenos hábitos de seguridad en línea. La dependencia de las tecnologías de la información y las comunicaciones seguramente seguirá creciendo incesantemente. Por lo tanto, es necesario que los gobiernos adopten las medidas pertinentes para proteger y asegurar sus infraestructuras críticas iniciando o promoviendo continuamente planes y legislación sobre seguridad cibernética, aumentando la cooperación internacional y obteniendo la participación de todas las partes interesadas pertinentes, incluido el sector privado.

Los datos recogidos por la OEA y por Trend Micro han llevado a conclusiones en cinco ámbitos principales:

- El estado de las respuestas gubernamentales a la delincuencia cibernética
- El estado del uso del internet
- El estado del panorama de las amenazas
- El estado del panorama de los ataques
- El estado de la delincuencia cibernética clandestina

El estado de las respuestas gubernamentales a la delincuencia cibernética

Las respuestas de los Estados miembros a la delincuencia cibernética siguen siendo desiguales. Muchos gobiernos empezaron a tomar medidas serias para fortalecer la seguridad cibernética tras la adopción de la Estrategia de Seguridad Cibernética de la OEA en 2004. En términos globales, los dirigentes políticos son conscientes de los peligros que plantean los hackers y los delincuentes cibernéticos para el desarrollo y la seguridad pública. Sin embargo, la voluntad política no siempre conduce a cambios en la situación imperante. En América Latina, dos factores bloquean comúnmente los esfuerzos: la falta de recursos dedicados al fortalecimiento de la capacidad en seguridad cibernética y la escasez de conocimientos especializados y experiencia práctica para la implementación de políticas o capacidad técnicas.

Latinoamérica sigue enfrentando restricciones presupuestales, y los planes de gastos a menudo no contemplan grandes inversiones en aspectos como la seguridad informática. Los fondos se invierten con mayor frecuencia en aspectos de 'seguridad propiamente dicha', aunque esto probablemente cambiará conforme los riesgos cibernéticos vayan planteando cada vez más amenazas contra el bienestar físico y económico y la estabilidad de los gobiernos. En cualquier caso, es importante observar que a pesar de las limitantes presupuestales, los países pueden dar grandes pasos en materia de seguridad cibernética. Uruguay, por ejemplo, estableció un CSIRT robusto y desarrolló capacidad general de seguridad cibernética con recursos financieros mínimos. Otros países han estudiado e implementado programas de sensibilización eficientes en términos de costos para educar a sus ciudadanos. Es asombrosa la cantidad de software gratuito de seguridad cibernética a que tienen acceso los países, aunque no siempre logran aprovechar las oportunidades.

La escasez de conocimientos especializados y experiencia práctica necesarios para implementar iniciativas técnicas podría atribuirse a las bajas tasas de matrícula en programas de formación técnica. La falta de expertos calificados en las Américas significa que los países prácticamente se están ahogando en un mar inservible de software libre de seguridad cibernética y materiales educativos. Algunos países experimentan esta deficiencia más que otros, pero este problema podría mitigarse mediante cooperación internacional. La OEA seguirá promoviendo las redes y facilitando el intercambio de prácticas óptimas y conocimientos profesionales dentro y entre sus Estados miembros. Asegurando el flujo de información, los países pueden seguir añadiendo valor a sus capacitaciones y lecciones aprendidas.

Dentro del contexto de estas deficiencias, los países están luchando para sensibilizar a sus ciudadanos y están enfrentando dificultades para mantener el impulso en la implementación de soluciones técnicas y de política para los problemas de seguridad cibernética. Algunos gobiernos no tienen un acervo centralizado de información sobre incidentes cibernéticos. Algunos no tienen capacidad para responder a incidentes. Incluso los que ya han dado algunos pasos adelante experimentan problemas con el intercambio de información entre ministerios y departamentos. Esta realidad se vio repetidamente en las encuestas de la OEA a los gobiernos.

Pero los países están avanzando en la dirección correcta. Los casos de éxito de que hemos hablado resaltan solamente unas cuantas iniciativas que han adoptado recientemente los Estados miembros. La conciencia sobre la seguridad cibernética está aumentando día a día, y los gobiernos se están esforzando para mejorar sus instrumentos de política. No obstante, queda mucho trabajo por hacer para seguirles el ritmo a quienes tratan de corromper redes críticas y abusar del intercambio de información personal.

El estado del uso del internet

El uso del internet en América Latina está aumentando a uno de los ritmos más acelerados en todo el mundo. Desgraciadamente, el número de ciudadanos digitales no se ha visto acompañado por un aumento proporcional en los protocolos e infraestructuras para proteger la seguridad de las personas en línea. Las respuestas a la encuesta de la OEA y los datos de Trend Micro demuestran que los hábitos cibernéticos inseguros han alimentado los altos niveles de delincuencia cibernética. El número de infecciones informáticas indica que los usuarios no están manteniendo actualizadas sus soluciones contra programas maliciosos y que siguen usando dispositivos de almacenamiento sin prestar mayor atención a inquietudes sobre seguridad. Los datos técnicos fueron confirmados por las opiniones de los gobiernos en el sentido de que los ciudadanos en general siguen ajenos y despreocupados con respecto a los peligros que plantean la delincuencia cibernética y el haqueo.

A pesar de todas estas deficiencias, hay señales alentadoras. Numerosas organizaciones no gubernamentales, como USUARIA y STOP. THINK. CONNECT.[13] están activas en la región y se han aliado con la OEA y con los Estados miembros para diseñar y difundir campañas de sensibilización a gran escala. Entre una plétora de ciberciudadanos vulnerables está naciendo un conjunto creciente de expertos y organizaciones preocupados por aumentar la resiliencia de las redes educando a los usuarios del internet. La OEA ha estado promoviendo activamente alianzas entre gobiernos y organizaciones no gubernamentales como USUARIA y STOP. THINK. CONNECT. con resultados positivos hasta ahora.

El estado del panorama de las amenazas

Los datos de los Estados miembros de la OEA y de la Smart Protection Network de Trend Micro mostraron que los delincuentes cibernéticos lanzaron en 2012 una combinación de ataques motivados política y financieramente. Los grupos de delincuencia organizada están adquiriendo capacidad cibernética y los sindicatos de hackers están aumentando en número y sofisticación. Así pues, es necesario que los gobiernos sigan fortaleciendo los mecanismos de coordinación e intercambio de información con agencias policíacas, proveedores de servicios de internet y el sector privado para desmantelar foros y proveedores de hospedaje blindado y establecer alternativas a los canales de pago que emplean actualmente los delincuentes cibernéticos.

13 http://stopthinkconnect.org/

Las técnicas y los programas maliciosos nuevos están permitiéndoles a los atacantes acometer contra sistemas de control industrial y otras infraestructuras críticas. De hecho, el número de ataques contra servicios, bancos, plantas purificadoras de agua y otros proveedores de servicios esenciales va en aumento. Se ha detectado mediante exploraciones que muchos sistemas de control industrial están conectados al internet y son vulnerables a ataques cibernéticos. Los operadores de infraestructura crítica tienen que aplicar normas y políticas que den cuenta de su seguridad, dado el importante papel que desempeñan sus servicios en la sociedad. La protección de los sistemas de control industrial plantea problemas particulares, pues la cuestión de las alianzas público-privadas a menudo está vinculada inextricablemente con la infraestructura crítica. Nuevamente, esto refuerza la necesidad de que todos los sectores y las partes interesadas clave permanezcan involucrados y colaboren en asuntos de seguridad cibernética. Los delincuentes cibernéticos no enfrentan problema alguno para el intercambio información ni para colaborar a través de distintos idiomas y fronteras; es necesario que nos esforcemos por ser como ellos.

El estado del panorama de los ataques

Uno de los puntos más importantes que Trend Micro descubrió en los datos es que las computadoras de la mayoría de los ciudadanos están plagadas de archivos infectados. A menudo esto indica la prevalencia de dispositivos de almacenamiento portables insuficientemente protegidos y la falta de parches en los sistemas operativos o aplicaciones. La continua viabilidad de infecciones de archivos refleja las dificultades que ha estado experimentando la región para protegerse de los programas maliciosos, lo que, nuevamente, evidencia la falta de conciencia entre los usuarios.

El estado de la delincuencia cibernética clandestina

Los delincuentes cibernéticos clandestinos en América Latina recurren mucho a troyanos bancarios, en comparación con otras regiones, donde se usan otros tipos de programas maliciosos, como ransomware y ATSs.

Es claro que los responsables de las amenazas en la región aprenden de los errores de sus colegas delincuentes en otras regiones, notablemente de Europa Oriental. Reconocieron que el uso de servidores secuestrados contribuyó al éxito de las operaciones policiales y, en consecuencia, cambiaron al uso de servicios de hospedaje gratuitos para llevar a cabo sus actividades maliciosas. Las agencias policíacas necesitan tomar nota de esta táctica específica de la región y ajustar sus propias tácticas de vigilancia e investigación en consecuencia.

Los responsables de las amenazas y sus operaciones económicas ilícitas han utilizado en gran medida los servicios de Orkut y IRC, que han fungido como bazares clandestinos para el intercambio de dinero y bienes y servicios ilícitos. Estos procesos a menudo son facilitados por mulas que efectúan pagos para ocultar las identidades de quienes organizan estos planes.

Recomendaciones

A partir de las observaciones de los Estados miembros de la OEA y de los datos recogidos por Trend Micro pueden formularse tres recomendaciones:

1. Aumentar la conciencia sobre los hábitos cibernéticos y la sensibilidad general hacia la seguridad cibernética entre los usuarios finales, los operadores de infraestructuras críticas y los funcionarios gubernamentales. Esto dificultará que los delincuentes cibernéticos perpetren ataques que han sido comunes contra estos tres grupos. La sensibilización puede ser una de las maneras más baratas y eficaces de minimizar los riesgos a la seguridad cibernética y cerrar las brechas de seguridad que siguen estando totalmente abiertas.

2. Invertir y promover la matriculación en programas de formación técnica. La protección de redes gubernamentales y privadas requiere conocimientos técnicos difíciles de adquirir a corto plazo. Junto con las campañas de sensibilización en las escuelas, las instituciones académicas necesitan esforzarse más para atraer estudiantes hacia los itinerarios formativos en ciencias informáticas y seguridad informática. Esto asegurará que se disponga de un gran acervo de candidatos calificados del cual extraer a los profesionales que se requerirán para cubrir el número creciente de carreras profesionales en seguridad informática.

3. Seguir fortaleciendo los mecanismos de política para asignar funciones y responsabilidades gubernamentales relacionadas con la seguridad cibernética y codificar mecanismos de intercambio de información y cooperación. Esta labor se ha iniciado ya, pero es hora de que todos los Estados reflexionen estratégicamente sobre cómo desarrollarán sus regímenes de seguridad cibernética, hacia dónde enfocarán sus esfuerzos y cómo convertirán sus visiones en realidades.

Referencias

- http://about-threats.trendmicro.com/malware.aspx?language=au&name=TSPY_QHOST.AFG
- http://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/
- http://blog.trendmicro.com/trendlabs-security-intelligence/latin-america-router-compromising-malware-found/
- http://blog.trendmicro.com/trendlabs-security-intelligence/new-crimeware-in-bancos-paradise/
- http://latinamericacurrentevents.com/head-of-major-credit-card-cloning-ring-arrested-in-colombia/18040/
- http://stopthinkconnect.org/
- http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf

- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf
- https://www.meridian2012.org/pages/the-conference

May 2013 / Mayo de 2013

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

Latin American and Caribbean Cybersecurity Trends and Government Responses

Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos

Executive Secretary of the
Inter-American Committee against Terrorism
CICTE
Neil Klopfenstein

Editors
Brian Dito
Belisario Contreras
Tom Kellermann

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

Securing Your Journey to the Cloud