Una historia de éxito en ciberseguridad

Cinco años de gestión de incidentes de seguridad informática

2019

lacnicwarp

@LACNIC_Warp

Índice

Resumen ejecutivo

Las tecnologías de la información y las comunicaciones (TIC) son omnipresentes en la vida cotidiana de las personas. Los beneficios que aportan al bienestar de las sociedades modernas y al desarrollo económico son múltiples. Sin embargo, estas tecnologías se encuentran amenazadas por actividades maliciosas, cambiantes y en crecimiento continuo, que pueden provenir de cualquier lugar del mundo.

Este panorama exige una coordinación que pueda hacer frente a la complejidad de la interconexión de las redes informáticas y a la multiplicidad de dispositivos que hoy permiten acceder al ciberespacio. Contar con referentes confiables y especializados se ha vuelto un principio incuestionable para fortalecer el posicionamiento de las personas y las organizaciones frente a las TIC.

En este marco, LACNIC comenzó a gestar, durante 2014, la idea de crear un grupo especializado para la gestión de incidentes de seguridad, que inauguró en marzo de 2015, bajo la denominación LACNIC WARP, por las siglas de Warning, Advice and Reporting Point (Alertas, Recomendaciones y Punto de Reporte e Intermediación). Esta decisión se adopta en línea con su misión de velar por el uso debido y seguro de los recursos numéricos de Internet de América Latina y el Caribe y su registro.

Cabe destacar que se trata del único RIR que a la fecha ofrece este tipo de servicios a sus asociados. LACNIC brinda a sus miembros, sin costo adicional, servicios destinados a la gestión de incidentes, la intermediación basada en el conocimiento de las necesidades de aquellos a quienes atiende y la generación de alertas de seguridad, que publica en su sitio web.

Desarrolla también un esfuerzo importante para formar capacidades de prevención, detección y respuesta a incidentes en la región, a través de los talleres Amparo.

Para fortalecer la relación de confianza entre entidades de similar naturaleza de la región, creó y mantiene el grupo de equipos de respuesta LAC-CSIRTS.

En su vinculación internacional ha firmado numerosos acuerdos con reconocidas organizaciones internacionales que se dedican al combate de incidentes de seguridad informática y mantiene un estrecho contacto con equipos que, en el mundo, dan respuesta a incidentes.

LACNIC WARP recibe todo tipo de reportes de incidentes de su comunidad, si bien algunas categorías tienen una mayor presencia.

Cinco años después de su creación, el WARP sigue expandiendo sus servicios y aportando valor a los miembros de LACNIC. Además, ha logrado reconocimiento a nivel regional e internacional por su contribución a una Internet estable, abierta, en continuo crecimiento y, especialmente, más segura.

Introducción

La dimensión que han alcanzado las tecnologías de la información y las comunicaciones (TIC) en la vida cotidiana de las personas en las últimas tres décadas es impactante. El acceso casi inmediato a la información y al conocimiento, la inmediatez de los contactos y la atemporalidad y ubicuidad en el acceso a los servicios son algunas de las consecuencias más significativas de esta transformación.

Si cuarenta años atrás los dispositivos digitales disponibles se hubieran apagado de golpe, es probable que todo hubiera seguido funcionando sin mayores problemas. Hoy las consecuencias serían dramáticas, ya que el bienestar y el progreso individual y colectivo están indisolublemente ligados al desarrollo tecnológico.

Sin embargo, la confianza excesiva en el desarrollo tecnológico y las expectativas de bienestar basadas en los dispositivos digitales parecen haberse incrementado notoriamente, superando ampliamente las capacidades y habilidades desarrolladas para protegerse frente a usos indebidos de las TIC. Resulta dificultoso para los Estados, para las organizaciones y para las personas comprender la magnitud de los riesgos y, especialmente, saber cómo abordarlos y a quién recurrir. En otras palabras, no es sencillo encontrar instituciones referentes y especialistas confiables en condiciones de dar respuesta ante eventos que pueden afectar negativamente la información, las operaciones y los servicios que se brindan.

Las amenazas se diversifican y globalizan, y cada vez se requiere de mayor coordinación para hacer frente a la complejidad de la interconexión. Compartir información y estar preparados para responder a los incidentes se ha vuelto un imperativo de economía de recursos, que ayuda a fortalecer el posicionamiento de las personas y las organizaciones frente a las TIC, al brindar herramientas en un escenario que no reconoce fronteras temporales ni geográficas.

En este marco, LACNIC, como Registro de Direcciones de Internet para América Latina y el Caribe, empezó a delinear en 2014 la idea de formar un equipo de respuesta a incidentes, que inauguró en marzo de 2015 bajo la denominación de LACNIC WARP, siglas de Warning, Advice and Reporting Point (Alertas, Recomendaciones y Punto de Reporte e Intermediación, en español). Esta decisión se adoptó en línea con su misión de velar por el uso debido y seguro de los recursos

numéricos de Internet de América Latina y el Caribe y su registro, mediante iniciativas que los protejan frente a factores externos que puedan afectarlos.

A continuación se describirá la trayectoria de LACNIC WARP desde su creación, así como su proyección. Se detallará la evolución de los tipos de abuso que ha gestionado frente a un panorama de amenazas cambiante, creciente y de difícil predicción, y se identificarán sus principales aportes a la comunidad de miembros de LACNIC.

Reseña histórica de lacnic warp

Por su trayectoria y la importancia de su actividad, LACNIC mantiene desde su fundación, en 2002, una estrecha vinculación con sus asociados, comunidad que reúne a la fecha a unas 10.000 organizaciones distribuidas en los países de América Latina y el Caribe. Se encuentra vinculado también a otras organizaciones de la región y del mundo, como los otros cuatro Registros Regionales de Internet (RIR).

Este posicionamiento y cercanía con organizaciones de diversa naturaleza daba lugar a que, en su gestión cotidiana, LACNIC tomara conocimiento de información relacionada con potenciales incidentes de seguridad que podrían afectar a su membresía. Esto significaba una oportunidad y también un desafío: comunicar estos hechos en forma oportuna y certera para contribuir a mitigar sus efectos.

El WARP surge ante la urgencia de atender los eventos de seguridad reportados por los miembros de LACNIC, recibidos en su mayoría a través de una casilla de correo denominada «abuse». Sin embargo, por el volumen y magnitud de los eventos reportados y por carecer en ese momento de un grupo especializado en la gestión de incidentes de seguridad, no era posible atender ese tipo de requerimientos en tiempo y forma.

En 2014 se comenzó a gestar la idea de crear un grupo especializado en la gestión de incidentes de seguridad, conocidos internacionalmente como CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team).

Un año después, se creó LACNIC WARP, con la misión de llevar a cabo la coordinación necesaria para fortalecer las capacidades de respuesta a incidentes vinculados a los recursos de numeración de Internet (IPv4, IPv6), Números

Autónomos y Resolución Inversa de América Latina y el Caribe. Buscó contribuir a un objetivo mayor: el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento, en línea con la visión de LACNIC.

Para su creación e implementación se contó con el apoyo de las gerencias de LACNIC. A través del área Comunicaciones, se realizó una planificación detallada para llegar a toda la membresía con la información de este nuevo servicio.

La comunidad objetivo, es decir, el conjunto de destinatarios de los servicios del WARP, está formada por los miembros de LACNIC, a quienes asiste en la gestión de incidentes sin costos adicionales. Un formulario en línea para su reporte y una serie de canales alternativos de comunicación permiten informar al equipo especializado sobre cualquier actividad sospechosa que detectan en sus redes informáticas.

Sin embargo, es importante aclarar que el WARP no tiene autoridad para actuar sobre las operaciones de los sistemas de su comunidad. En otras palabras, queda a discreción de la organización afectada la decisión de cómo gestionar el incidente y el WARP adopta un rol de asesoramiento y de asistencia, si se requiere.

Desde su creación, WARP publica alertas de seguridad en su sitio web ‹https://warp.lacnic.net/›, además de información de contacto, oferta de capacitaciones y estadísticas sobre los incidentes tratados. Cabe acotar que LACNIC es el único RIR que ofrece este tipo de servicios a sus miembros.

Servicios ofrecidos

Como la mayoría de los CSIRT, ofrece tanto servicios proactivos como reactivos, los que se describen someramente a continuación.

Gestión de incidentes

Como un CSIRT más, el principal servicio que ofrece LACNIC WARP es la gestión de los incidentes de seguridad. Se ubica así como un punto de confianza para el reporte de los eventos sospechosos o información sensible que se detecta en las redes de las organizaciones afectadas.

Actúa también en un rol coordinador, pues eleva a otros centros de naturaleza similar aquellos incidentes que no pueden ser gestionados por el propio WARP. Toda esta actividad se desarrolla bajo niveles estrictos de confidencialidad.

A lo largo de la existencia del WARP, el volumen y la variedad de incidentes tratados se ha ido ampliando de forma paulatina, dada la diversidad y la evolución constante de las amenazas. Además, el proceso para su gestión se ha ido perfeccionando en un ciclo de mejora continua.

LACNIC WARP nació como una respuesta a la necesidad de atender reportes de eventos de seguridad que afectaban a los asociados, los que llegaban mayormente a la casilla de correo abuse. Sin embargo, el aumento en volumen, la complejidad de los reportes recibidos y la carencia de un grupo especializado hacía imposible la debida atención.

Una de las primeras acciones al conformarse el WARP fue un estudio de la información recibida para categorizarla, lo que también dio lugar a una recopilación estadística. Se decidió entonces definir una casilla de correo específica para el reporte de incidentes de seguridad: info-warp@lacnic.net.

Poco después, una vez publicado el sitio en Internet, se incorporó el formulario web que permite, hasta hoy, reportar cualquier incidente. De este modo, se provee un ambiente seguro y anónimo de intermediación para facilitar la identificación, caracterización, análisis y respuesta, con el fin de mitigar los efectos y contribuir al restablecimiento de los servicios afectados.

Todos los reportes recibidos a través del formulario y la casilla mencionados se someten a un procedimiento de triage, habitual en este tipo de actividad, para decidir si se trata de un incidente que amerita gestión o si, por el contrario, es un simple evento que no requiere tratamiento.

Si se identifica como un incidente de seguridad a gestionar, se procede a su categorización, se le asigna una prioridad y se crea un ticket con el cual se hace un seguimiento hasta el cierre.

LACNIC WARP recibe todo tipo de reportes de su comunidad. Los más habituales corresponden a ataques de phishing y malware. En la sección de Estadísticas se explicará con mayor detalle la evolución de cada uno de estos incidentes.

Advertencias de seguridad y boletines informativos

LACNIC WARP publica en su sitio web alertas de seguridad. Las más actuales o relevantes aparecen destacadas en «Noticias» y luego se van recopilando en la sección «Advertencias de Seguridad». La sección «Artículos» presenta documentos con temas informativos que se consideran relevantes para la comunidad atendida por el WARP. Estas novedades también se distribuyen a los miembros a través de boletines informativos de envío periódico.

De esta manera, el WARP alerta a su comunidad —y en muchos casos al público en general— para que cuente con información técnica oportuna y actualizada y, si es del caso, adopte medidas de prevención.

Con los reportes que se generan de la gestión de incidentes y con la información que se obtiene de los vínculos con entidades dedicadas a la investigación de estos temas, se elaboran las estadísticas que se publican mensualmente, como hacen equipos de naturaleza similar. Más adelante se hará referencia específica a los tipos de incidentes gestionados.

Adicionalmente, aprovechando que LACNIC cuenta con un sistema denominado MILACNIC —en el que cada organización miembro administra su propia información— se difunde a través de este canal información de interés vinculada a cuestiones de ciberseguridad.

Por ejemplo, en 2018 se llevó a cabo un proyecto de identificación de problemas de Open Resolvers en IPv6 en la región con el fin de hacer llegar a los miembros información sobre cómo configurar correctamente sus DNS. Esta iniciativa surgió a partir de los numerosos reportes recibidos en la casilla de correo abuse sobre este tipo de problemas que, en muchos casos, estaban siendo utilizados para realizar ataques a otras infraestructuras.

De este modo, se asistió a los potenciales afectados para mitigar un riesgo para la seguridad de sus recursos. Una vez que el sistema quedó automatizado, esa información se integró a MILACNIC para que cada miembro pudiera identificar problemas en sus recursos y solucionarlos.

Entre los planes del WARP está continuar agregando a este sistema la información referida a otros tipos de alertas que puedan estar afectando recursos de su membresía.

Incorporar más información sobre mejoras en la configuración de servicios críticos o alertas sobre problemas detectados es indispensable para el desarrollo de una infraestructura segura y estable, preparada para prevenir o detectar a tiempo incidentes con alto riesgo de propagación.

Capacitaciones

Para el fomento de una cultura de la ciberseguridad y la difusión de buenas prácticas, LACNIC WARP lleva adelante una importante iniciativa vinculada a la formación de capacidades de respuesta a incidentes. Con ese fin funciona en su ámbito el taller Amparo, que busca capacitar al personal de las organizaciones que integran la comunidad atendida por el WARP para que formen sus propios centros de respuesta.

En estos talleres también se abordan buenas prácticas vinculadas a la seguridad en redes y a la gestión de incidentes, como la seguridad en DNS y el despliegue de DNSSEC, el enrutamiento seguro a través de la difusión de mejores prácticas, la certificación de recursos y el uso de RPKI.

Los talleres se dictan en español e inglés e incluyen aspectos técnicos, organizativos, procedimentales y de actualidad, vinculados a la gestión de incidentes de seguridad. Estas actividades se acompañan de presentaciones abiertas a sectores vinculados a esta disciplina, con las que se generan espacios de concientización para decisores y especialistas, lo que contribuye a una atención más precisa de los riesgos del ciberespacio.

Recursos

En LACNIC, el equipo cuenta con dos profesionales altamente calificados que se dedican, a tiempo completo, a la gestión de incidentes, docencia e investigación. Durante 2019, se contó con la asistencia de otra persona y se conformó así un equipo

multidisciplinario para el abordaje de tareas específicas para la mejora de sus sistemas.

El equipo se apoya en los servicios y recursos de LACNIC en todo lo referente al relacionamiento institucional, instrumentos jurídicos e infraestructura tecnológica. Puede contratar a especialistas de los países de la región para el dictado de aspectos específicos incluidos en los talleres Amparo y para el desarrollo de documentos técnicos. La totalidad del presupuesto de funcionamiento del WARP proviene de LACNIC.

Relacionamiento con la comunidad

Los servicios del WARP se centran en los miembros de LACNIC. Para optimizar esta vinculación, se relaciona con otras organizaciones de similar naturaleza o con objetivos complementarios. Por ejemplo, con organizaciones internacionales, como ICANN, FIRST, OEA, otros RIR y con entidades reconocidas internacionalmente, como Team Cymru, M3AAWG, APWG, entre otras. Además, mantiene contacto con los CERT/CSIRT, especialmente los de Latinoamérica, muchos de los cuales surgieron a partir de los talleres Amparo.

A iniciativa de WARP, LACNIC ha firmado acuerdos de cooperación con la mayoría de estas entidades. Por ejemplo, con Stop, Think & Connect (STC), la cual lleva adelante una importante iniciativa de concientización de seguridad destinada a la población y aúna globalmente a Estados, entidades regionales como LACNIC, organizaciones no gubernamentales y empresas privadas de la industria de las TIC del mundo.

En el marco del memorando de entendimiento firmado con el FIRST en 2015 y renovado en 2017, se han iniciado varias líneas de trabajo para apoyar el desarrollo de capacidades de respuesta a incidentes cibernéticos en la región. Como parte de este acuerdo, FIRST puso a disposición de LACNIC sus programas de formación para su despliegue con equipos regionales. Desde 2018 y junto al Cert.br, CERT coordinador del Brasil, se realiza en Latinoamérica un simposio anual del FIRST, que incluye una conferencia plenaria y varias jornadas de entrenamiento.

lac-csirt

En el seno de las actividades de seguridad desarrolladas por LACNIC, se detectó la ausencia de un espacio de relacionamiento entre equipos de respuesta a incidentes de seguridad en la región. Como consecuencia, durante el evento de LACNIC 21 de Cancún (México), realizado en 2014, se propuso la creación del grupo LAC-CSIRTS, lo que luego reforzó la red de contacto entre los CSIRT de la región.

Esta grupo tiene entre sus objetivos el incremento y la mejora de las relaciones con los miembros de la comunidad regional, el establecimiento de una red de confianza para compartir información y experiencias, y el compromiso de trabajar en forma coordinada en temas de seguridad de interés común.

Los eventos anuales que organiza LACNIC brindan a estos equipos la oportunidad de realizar reuniones presenciales y se consolidan como un espacio de trabajo e intercambio de experiencias. Así se busca fortalecer a los países para la prevención y mitigación del impacto de incidentes de seguridad. LACNIC WARP realiza la tarea de secretaría del grupo.

El ADN del WARP: la situación internacional de ciberseguridad

Al tiempo que los procesos y los datos de las personas y las organizaciones se mudan inexorablemente al ciberespacio, aumentan significativamente los riesgos a los que se exponen. Algunos son menores y pueden pasar desapercibidos, mientras que otros tienen un impacto tan notorio que llegan a afectar fuertemente a toda una organización o incluso a una parte importante de la sociedad o de la economía de un país.

El año 2014 será recordado por un incremento notable en los ciberataques sufridos por grandes empresas, mayormente ubicadas en Estados Unidos y Europa, caracterizados por la exposición de los datos personales y financieros de millones de personas. Ese mismo año, LACNIC se preparó para lanzar el WARP, incorporando a quien es su actual líder. En octubre de ese año se presentó la iniciativa en Santiago de Chile, durante un coloquio técnico de FIRST, que fue muy bien recibida por los asistentes.

Marzo de 2015 fue el mes elegido para el lanzamiento del WARP y en octubre se incorporó un analista especializado. También se dictó en San José de Costa Rica el primer taller Amparo y se firmó el primer memorando de entendimiento con FIRST. Este reconocimiento por parte del FIRST, organización de primer nivel que reúne a los principales CERT y CSIRT del mundo, es una evidencia temprana de la importancia que tendría con los años el WARP y de la necesidad de contar con este tipo de servicios en la región.

Ese mismo año, un importante operador de telefonía móvil europeo sufrió un ataque por el cual se accedió ilegítimamente a los registros de quince millones de clientes y dos hackers consiguieron tomar el control de la electrónica de un vehículo en movimiento, obligando al fabricante a retirar más de un millón de autos potencialmente vulnerables.

Al año siguiente se publicaron en el sitio web del WARP las primeras estadísticas de incidentes gestionados en la región y se dictó en Belice el primer taller Amparo en inglés.

En 2016, el mundo presenció el robo de más de un millón de registros de un gigante europeo de las comunicaciones y se utilizó el código malicioso Mirai para infectar millones de dispositivos. Esto causó un ataque distribuido de denegación de servicios sobre la infraestructura de uno de los líderes mundiales en la provisión de servicios de DNS, que terminó afectando a una parte importante de Internet a nivel global.

WannaCry, código malicioso del tipo ransomware, sorprendió al mundo, en mayo de 2017, como el primer ataque de escala internacional. Afectó de forma directa a servicios hospitalarios, empresas de telecomunicaciones, gobiernos y aeropuertos, entre otros e, indirectamente, a organizaciones de todo tipo. Durante ese año, LACNIC WARP renovó su acuerdo con el FIRST, firmó un convenio con el APWG y fortaleció su relación con el M3AAWG.

Durante 2018, el WARP lanzó el proyecto de identificación de Open Resolvers en Ipv6, como mecanismo a disposición de los miembros de LACNIC, para evitar que sus servidores mal configurados acepten peticiones recursivas de información sin importar su origen, y sean inadvertidamente parte de un ataque de denegación de servicio.

También organizó junto al Team CYMRU el Evento Regional de Seguridad de Internet en Montevideo (el segundo de este tipo en Sudamérica).

Ese año, grandes empresas responsables de redes sociales mostraron graves fallas en sus mecanismos de privacidad. Como consecuencia, más de 30 millones de personas sufrieron las consecuencias de la exposición de sus datos personales y de contacto. Además, la ciudad de Atlanta, en Estados Unidos, vio inhabilitados sus sistemas por más de una semana debido al ataque de un ransomware. Por otra parte, instituciones bancarias en Latinoamérica sufrieron el robo de los datos financieros de sus clientes, lo que causó preocupación en los gobiernos de esos países.

El año 2019 volvió a traer grandes filtraciones de datos personales y ataques de ransomware y continúan apareciendo en los medios internacionales noticias de acciones cibernéticas encaradas por organizaciones delictivas de alcance global y grupos terroristas. Incluso se acusa a gobiernos de algunos países de ser el origen de estas.

Estos ataques tienen como blanco a importantes sectores económicos, infraestructuras críticas de información y organismos públicos. El concepto de debido cuidado (due dilligence) respecto a las medidas que deben adoptar los países para evitar que las redes y demás recursos informáticos ubicados en sus territorios puedan ser utilizados como medio para atacar las infraestructuras tecnológicas localizadas en otras naciones, empieza a discutirse en los organismos internacionales.

En este contexto, LACNIC WARP se prepara para expandirse y continúa ofreciendo servicios a la comunidad de miembros de LACNIC.

El siguiente gráfico muestra los hitos del WARP desde su creación.

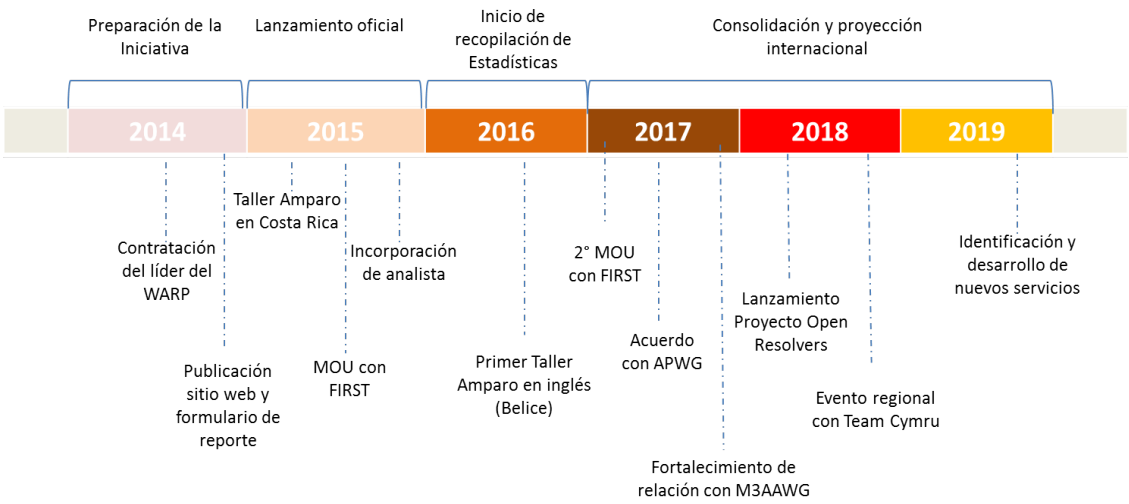


Gráfico 1: HITOS DEL WARP

Evolución de los tipos de abusos

La denominada respuesta a incidentes, como un proceso de aseguramiento de la información, nació hace aproximadamente 30 años, cuando los especialistas entendieron que era necesario prevenir posibles desastres en el ecosistema de las redes informáticas —y particularmente Internet— y mejorar así los objetivos internos vinculados a la protección de la información dentro de la organización.

Fue en 1988, a partir de la aparición del gusano Morris, primer malware autorreplicable que infectó a un diez por ciento de los servidores conectados a ARPANET (antecesora de lo que hoy conocemos como Internet), que apareció el primer centro de respuesta a incidentes de seguridad, en la Universidad Carnegie Mellon de los Estados Unidos.

Un año después se fundó el FIRST, como respuesta a la necesidad de compartir información y cooperar en materia de gestión de incidentes de seguridad por parte de los equipos especializados. Esta organización reúne hoy a unos 500 equipos de todas partes del mundo y es la mayor red global de confianza en la materia.

Con el paso del tiempo y la creciente conectividad entre múltiples entidades, el foco en la expansión de servicios superó ampliamente la preocupación por los posibles riesgos. Actualmente puede observarse la espectacular variedad de servicios y despliegues que permite el desarrollo tecnológico, pero también un número creciente de incidentes que, cada vez con más frecuencia, llegan a oídos del público general.

En este sentido, la infraestructura de recursos que da soporte a los servicios —provista por la mayor parte de las organizaciones que integran la comunidad de LACNIC en la región— se vuelve un eslabón crítico en la cadena de valor del desarrollo tecnológico y los CSIRT emergen como ámbitos especializados que asisten en la prevención de problemas y en su contención y mitigación si se materializan.

Entre los servicios que brindan estos equipos, quizá el de mayor beneficio para el ecosistema sea el de compartir información sobre incidentes, recomendación que se considera hoy como una de las buenas prácticas más importantes en cualquier decálogo de ciberseguridad.

La posibilidad de que las organizaciones estén mejor preparadas para proteger su información tiene implícita la necesidad de conocer cuáles son las amenazas que las acechan, ante un panorama que muestra una mayor frecuencia de incidentes y un mayor impacto. Una consideración importante es que muchos de esos incidentes se repiten a lo largo de los años, como por ejemplo el phishing, al que se hará referencia más adelante.

En este contexto, LACNIC WARP, como los equipos de respuesta a incidentes que han proliferado en el mundo, es una entidad preeminentemente técnica y su fortaleza, sin dudas, está en el reconocimiento de las características que estas amenazas y sus potencialidades adversas representan para los miembros de LACNIC y, fundamentalmente, cómo se gestionan.

Incidentes y aportes directos del WARP hacia la comunidad

Entre los incidentes que pueden afectar de manera directa a la comunidad del WARP se encuentran los relacionados con el protocolo BGP. El BGP Hijacking o el anuncio de prefijos de red no autorizados se origina cuando un participante en el routing en Internet anuncia un prefijo que no le está autorizado. En consecuencia, las tablas de ruteo se corrompen.

WARP clasifica este tipo de incidentes de seguridad como «Anuncio no autorizado de ruta». Si bien no se presentan con demasiada frecuencia, a lo largo de estos años ha recibido varios reportes, que ha atendido a través del servicio de intermediación

entre las partes. La ocurrencia de este tipo de incidentes constituye un gran riesgo debido a su fuerte impacto. Los problemas con los enrutamientos pueden originarse por acciones deliberadas o por debido a malas configuraciones. Sin embargo, en ambos casos los efectos son, inicialmente, iguales.

La causa más común suele ser un error de tipeo al configurar o realizar actualizaciones en los sistemas. En estos casos, al detectarse y comunicarse el error, las organizaciones responden casi de inmediato y corrigen el problema, minimizando rápidamente el impacto. El valor agregado del WARP es la recepción del reporte del problema, su evaluación y la inmediata comunicación a los involucrados para que realicen las acciones correctivas lo antes posible. Actúa como intermediario entre las partes afectadas.

Si bien este tipo de casos se registra desde fines de 1997, fue durante 2017 que —a partir del análisis de una serie de incidentes gestionados—, el área de I+D del WARP tomó la determinación de generar un artículo específico con una serie de recomendaciones de carácter general, destinadas a prevenir incidentes cuyos efectos podían ser potencialmente gravísimos. Estos problemas se evidencian a través de fallas en la conectividad, quejas de los usuarios por inconvenientes para acceder a ciertos sitios y también a partir de otras consecuencias más serias.

En este tipo de casos resulta sumamente eficiente contar con un punto confiable de asistencia y coordinación, a fin de compartir información sobre el incidente —tanto en los primeros momentos como durante su esclarecimiento— para luego realizar las acciones necesarias para evitar que vuelvan a ocurrir.

Si bien el protocolo BGP tiene debilidades sobre las que puede trabajarse, durante los últimos años también se han conocido incidentes originados en acciones de gobiernos que han ocasionado problemas más allá de sus fronteras, cuyo origen es importante conocer.

Otro caso de acción directa es el de la identificación de los servidores DNS Open Resolver. En IPv4, esta actividad resulta sencilla por el tamaño del espacio de direcciones. Sin embargo, IPv6 presenta un escenario distinto. Es así que a comienzos de 2018 el WARP inició un proyecto para su identificación en esta versión del protocolo.

A continuación se muestran los resultados obtenidos en este proyecto:

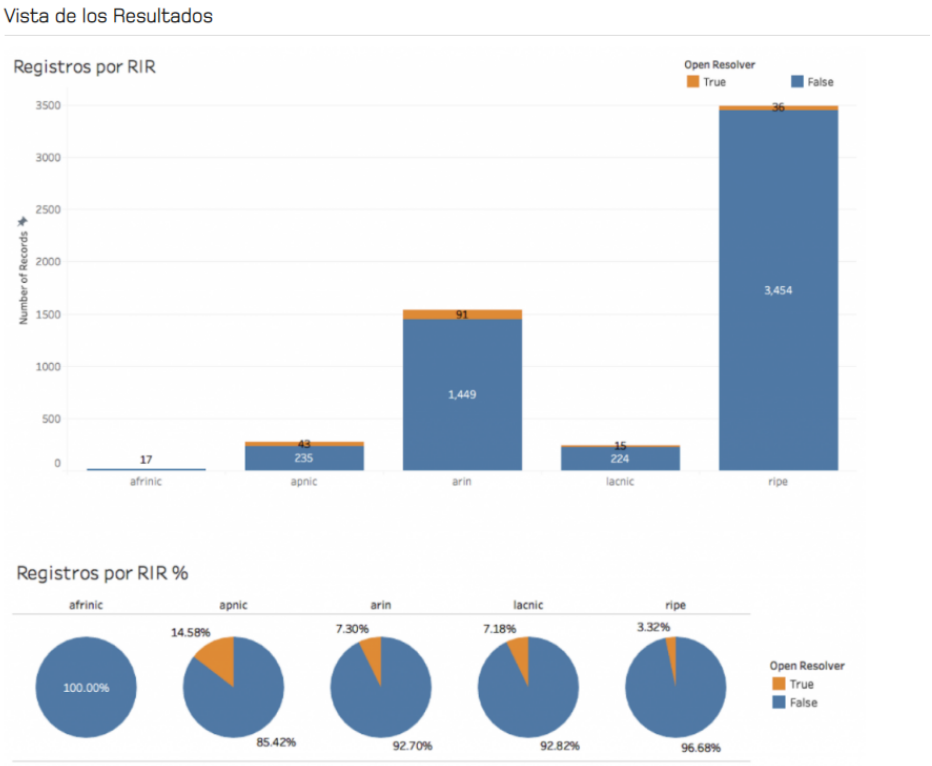


Gráfico 2: Resultados del proyecto Open Resolver

Fuente ‹http://bit.ly/warp-openresolvers›

El trabajo para brindar información sobre los orígenes de este tipo de incidentes y las recomendaciones —mediante boletines y/o capacitaciones— que fortalezcan posibles debilidades en el funcionamiento de esquemas relacionados con el direccionamiento IP son aportes de valor directo a la comunidad.

Estadísticas

La información estadística de incidentes de seguridad brindada por una fuente confiable e independiente proporciona información de gran valor para fines de investigación, así como también para conocer el estado de situación y proponer medidas para mejorar la respuesta y contribuir a la prevención.

Además de la recepción de notificaciones de incidentes de la propia comunidad atendida, desde los inicios de la actividad del WARP se han establecido acuerdos con organizaciones del ecosistema para acceder a información acerca del uso abusivo de

los recursos de Internet que administra LACNIC, de manera de poder asistir en la respuesta a incidentes y, también, formar una sólida base estadística.

En este sentido, surge —fundamentalmente del análisis de las estadísticas y de los tipos de incidentes detectados más relevantes— la identificación de nichos para planificar estrategias de concientización y formación de capacidades en la región. Como se mencionó, de los tipos de incidentes registrados por el WARP desde 2015, los de mayor presencia son los relativos al phishing y al malware.

Entre los incidentes más antiguos tratados por el WARP, se encuentran el phishing y un conjunto de piezas de código malicioso que se denomina, en forma genérica, malware. Estos han mostrado persistencia a lo largo del tiempo, no solo en la región sino en el mundo (hecho que puede verse claramente en las estadísticas del WARP).

Esta premisa está directamente relacionada con la veloz y creciente circulación de amenazas y con el reconocimiento por parte del WARP y de la comunidad de especialistas de que ninguna organización se encuentra a salvo. Por lo tanto, compartir información sobre las amenazas, tipos de incidentes y sus modalidades entre los integrantes de una comunidad con características similares representa una ventaja mayor y un valor agregado para cualquier organización.

En el caso del phishing, mencionado por primera vez en 1996 y popularizado en 2003 —cuando comenzó a hacerse rentable como modalidad fraudulenta— no ha parado de crecer. Tampoco ha parado de crecer el malware, que aglutina todo tipo de código que accede a un dispositivo, sin autorización.

Un componente esencial en estas modalidades es la vulnerabilidad humana, de la que la ingeniería social hace uso para lograr sus fines maliciosos. De ahí la importancia de las actividades que desarrolla el WARP para formar recursos humanos capaces de transformarse en eslabones fuertes a la hora de proteger la información.

El malware, código diseñado para adaptarse y mutar y así transgredir las barreras que se le presenten a su objetivo, busca desde el espionaje industrial al robo de credenciales, la captura de dispositivos para botnets, el control de sensores o cualquier acción que pueda aportar beneficios de distinta naturaleza a las organizaciones delictivas. Las actividades que en su momento podrían ser consideradas como daños menores, que afectaban a una organización o a unos pocos

individuos, hoy afectan al conjunto de la sociedad y traspasan las fronteras geográficas y temporales sin mayores dificultades.

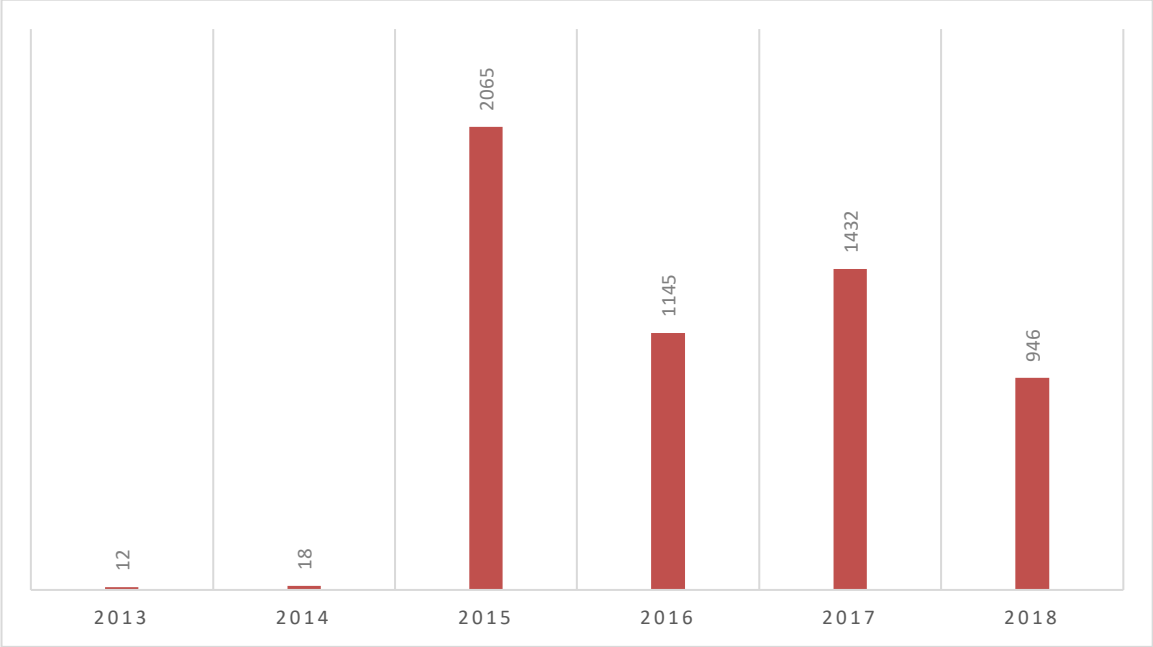
Los incidentes que solían presentarse de manera segmentada o aislada hoy se presentan de manera sofisticada en complejas combinaciones. Por ejemplo, históricamente el envío masivo de correos tenía como objetivo distribuir publicidades o propagandas. Sin embargo, desde hace un tiempo se vienen utilizando botnets para distribuir malware, ya sea mediante archivos adjuntos o incluyendo enlaces que llevan a sitios para engañar a los usuarios. Esto dio origen a que las publicaciones especializadas hablen del malspam (apócope de malware spam o malicious spam).

Asimismo, el phishing, que en sus principios utilizaba técnicas de ingeniería social para que un usuario revelara información confidencial propia —como datos de tarjetas de crédito o información de acceso a homebanking— se utiliza hoy de la misma manera pero con mayor potencialidad, dado que los servicios digitales se han extendido y ampliado hacia muchos otros canales y ámbitos de la vida social. Como ejemplos pueden señalarse las aplicaciones de citas, el acceso a sistemas médicos o los servicios ofrecidos por gobiernos, tanto de impuestos como de otros tipos.

Por otro lado, el phishing resulta en la actualidad el método de acceso para los ataques de mayor impacto y el primer paso en los ataques de tipo APT (Advanced Persistent Threat o Amenazas Persistentes Avanzadas, en español). Este último es planificado y ejecutado durante lapsos de tiempo prolongados y sus características principales son una baja probabilidad de ocurrencia y su alto impacto.

Generalmente se inicia con un correo engañoso que, cuando logra su objetivo, permite acceder a un dispositivo de manera no autorizada o ilegítima y finaliza con el robo de un gran número de datos, usualmente financieros. En este sentido, incidentes que observados a nivel micro podrían indicar que son los mismos de siempre, a nivel general se combinan, se complejizan y causan mayores impactos.

Los siguientes gráficos permiten observar la evolución a lo largo de los años de los reportes de malware y phishing según LACNIC WARP.



Gräfico 3 - Evolución del reportes de malware en warp lacnic

Como puede apreciarse en el gráfico 3, 2015 fue uno de los años con mayor incidencia del malware en la región. En el caso del phishing, 2018 marcó un crecimiento notorio, acompañando las tendencias mundiales, como se desprende del gráfico 4. Efectivamente, a pesar de todas las iniciativas que se llevan adelante para prevenirlo, este tipo de fraude, lejos de disminuir, muestra un crecimiento alarmante y, como se mencionó, es base de muchos ataques a sistemas bancarios, con impacto en los países de la región.

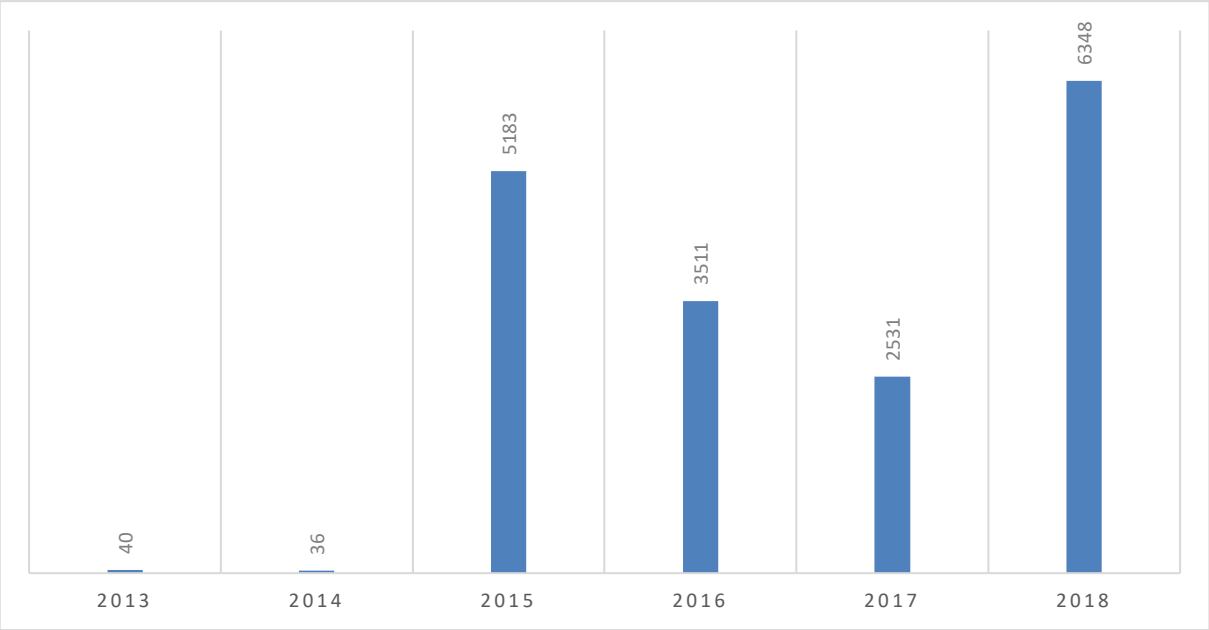


Gráfico 4: Evolución de reportes de Phishing en el warp lacnic

Es importante también señalar la cantidad de incidentes registrados por LACNIC WARP sobre redirect, método de ataque utilizado para redireccionar a un usuario que cree acceder a una dirección de Internet mientras es remitido a otra (incluso puede formarse una cadena de redirects). Por lo general, esta modalidad es utilizada para desviar el tráfico hacia un sitio fraudulento. Combinada con otras técnicas, puede tener un grave impacto para el público. El siguiente gráfico muestra la evolución de estos ataques recopilados por el WARP.

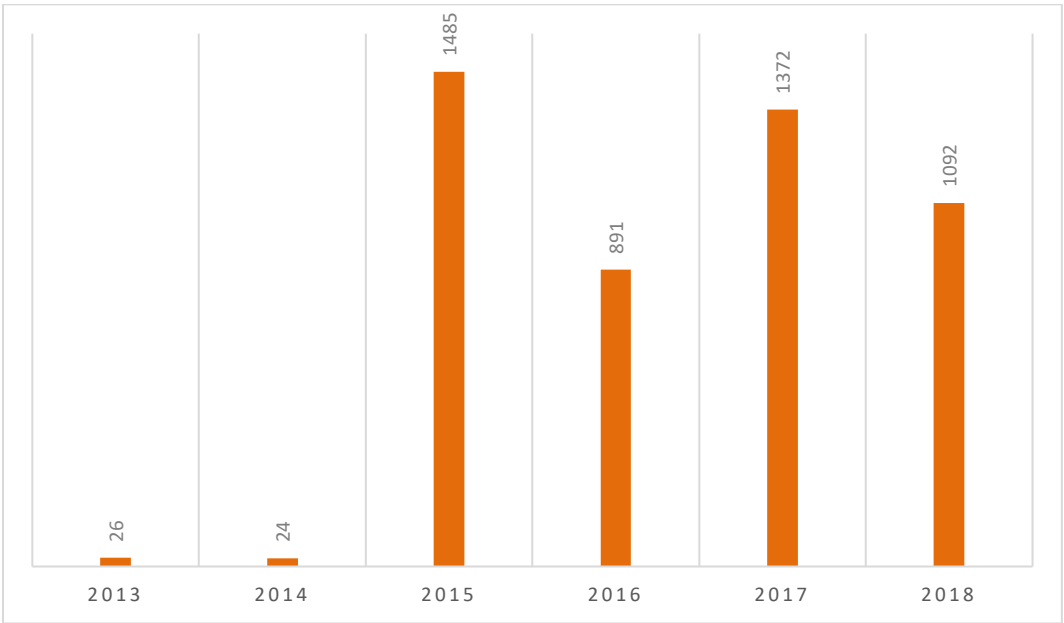


Gráfico 5: Evolución de reportes de Redirect según lacnic warp

Valor aportado por el WARP a los asociados

En la actualidad, los incidentes de seguridad se dan en todas las capas que habilitan la prestación de los servicios de la sociedad de la información. Pero es sin duda la capa de infraestructura la que constituye, de muchas formas, uno de los eslabones más críticos. Una vulnerabilidad detectada, informada y resuelta a tiempo implica un ahorro significativo de recursos —tanto económicos como humanos— y limita el daño, dado que la prestación de servicios solo es posible a partir de la infraestructura tecnológica plenamente operativa en sus servicios esenciales.

Como se ha mencionado, el WARP mantiene una observancia permanente de la aparición y evolución de los incidentes que pueden afectar a los asociados de LACNIC como base para planificar sus actividades, tanto en lo que refiere a la asistencia para la respuesta como a las capacitaciones y actividades de concientización y prevención que realiza.

Mantiene, asimismo, un estrecho vínculo con entidades de naturaleza similar o complementaria de la región y del mundo, utilizando la información que recopila para que su comunidad prevenga, mitigue y eventualmente resuelva de modo rápido y efectivo los problemas de seguridad que la pueden afectar.

Contar con un servicio de alertas, una fuente confiable y especializada de recomendaciones y un punto de reporte e intermediación en LACNIC brinda una ventaja notoria a sus miembros que, por su naturaleza y razón de ser, desarrollan actividades intrínsecamente enlazadas al desarrollo tecnológico en América Latina y el Caribe.

La excelente vinculación con los CSIRT y CERT de la región y del mundo permiten el acceso a las últimas tendencias en materia gestión de incidentes. Al fortalecer los vínculos de confianza con estos actores, aumenta la eficacia de sus servicios de gestión de incidentes, ya que, de ser necesario, se puede solicitar la colaboración de otros equipos o elevar un incidente de manera oportuna.

En este punto, el refuerzo de la seguridad y, aún más, la resiliencia de la infraestructura tecnológica resultan beneficiosos para toda la comunidad de organizaciones a las que el WARP brinda servicios, pero también para sus clientes y usuarios y para la región en su conjunto. Habilita una respuesta coordinada y, eventualmente, un mejor posicionamiento para mitigar los efectos de un ataque.

Conclusiones

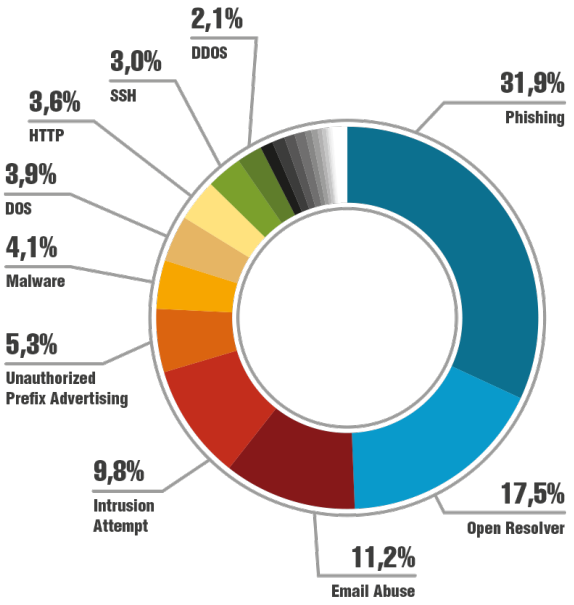
Gran parte del desarrollo económico, el funcionamiento de los Estados y las comunicaciones en la región de Latinoamérica y el Caribe se lleva adelante sobre la infraestructura de Internet. Por lo tanto, la asignación y administración de los recursos de numeración, los sistemas de números autónomos y los procesos de resolución inversa resultan esenciales para el continuo desarrollo de Internet.

En este marco, el WARP y la expansión de sus servicios a los miembros de LACNIC en estos cinco años de gestión han tenido reconocimiento a nivel regional e internacional por el fomento de las capacidades de prevención, detección y respuesta a incidentes de seguridad en la región.

Cotidianamente se reportan incidentes de seguridad que requieren de sus profesionales una rápida y efectiva respuesta para minimizar el impacto. En este sentido, está comprobado que la velocidad con la que se actúe limita el daño y disminuye los recursos necesarios para la recuperación de los servicios afectados.

Uno de los factores críticos para el éxito del WARP ha sido la calidad y dedicación de su personal, claramente comprometido con la labor desarrollada. Esta consideración aplica de lleno a quienes trabajan de forma exclusiva en la gestión de incidentes, pero puede extenderse al resto de las áreas de LACNIC que prestan asistencia y al cuerpo de docentes e investigadores que apoyan en forma permanente las actividades del WARP.

El equipo del WARP de LACNIC ha gestionado 600 incidentes informáticos de gran entidad en América Latina y el Caribe en sus primeros cinco años de gestión. Además, publicó más de 25 alertas de seguridad ante eventos considerados críticos, en coordinación con otras entidades dedicadas a la prevención de ciberataques.



Tipos de Incidentes Gestionados - Reportado WARP

En este primer quinquenio, el WARP organizó 19 talleres Amparo en la región, con el objetivo de fortalecer y promover Centros de Respuesta a Incidentes de Seguridad Informática, CSIRTS (por sus siglas en inglés), en lo cuales ha capacitado, en forma gratuita, a 800 profesionales expertos en ciberseguridad de la región.

Fruto de ese esfuerzo, se conformaron equipos de respuesta a incidentes en Costa Rica, Honduras, Bolivia, México y Ecuador y se fortalecieron los centros existentes en el resto de los países que recibieron a los expertos de LACNIC.

Países donde se han realizado talleres Amparo

El WARP cuenta con un mapeo actualizado de todos los equipos latinoamericanos dedicados a la prevención de ataques cibernéticos. Pueden encontrarse en ‹https://warp.lacnic.net/mapa-csirts›.

Los principales referentes de esos centros se han dado cita en las diez reuniones presenciales de LAC-CSIRT organizadas durante los eventos de LACNIC. Estos encuentros han servido para formar capacidades de prevención, detección y

respuesta a incidentes y han fortalecido la relación de confianza entre entidades de similar naturaleza de la región.

El trabajo profesional del equipo del WARP le ha permitido integrarse a la élite mundial de las entidades dedicadas a la seguridad informática. En ese sentido, LACNIC firmó acuerdos de cooperación con reconocidas organizaciones: FIRST, CERT.br, Message, Mobile, Malware Anti Abuse Working Group (M3AAWG), Anti-Phishing Working Group (APWG), Stop, Think & Connect (STC) y Team Cymru.

A la luz de estos datos, los objetivos iniciales fijados por el WARP pueden considerarse cumplidos, ya que este se ha transformado en un referente regional y ha obtenido reconocimiento internacional.

La gestión de estos cinco años del warp ha tenido como base la misión de LACNIC: contribuir a una Internet estable, abierta, en continuo crecimiento y, especialmente, más segura.

Pasos futuros

A partir de su rol en la gestión de incidentes de seguridad en América Latina y el Caribe, LACNIC WARP tiene como uno de sus principales objetivos a corto plazo ser aceptado como miembro del FIRST. Con este fin, se ha planificado la realización de un estudio interno, aplicando un modelo de madurez de procesos y capacidades, que permita determinar en qué nivel se encuentra actualmente el WARP y qué nivel busca alcanzar, lo que permitirá realizar las adaptaciones necesarias para corregir los desvíos y alcanzar el objetivo. Ingresar como equipo miembro del FIRST dará mayor visibilidad y brindará la posibilidad de integrar la mayor red mundial en gestión de incidentes de seguridad.

Sin embargo, la transformación digital, a la que no han escapado las organizaciones de la región, presenta un panorama creciente y cambiante de riesgos que es necesario enfrentar y gestionar. Esto, sin duda, exige la incorporación de nuevos profesionales que enriquezcan las múltiples actividades que hoy realiza el WARP.

La incorporación de nuevas herramientas de automatización para detectar fallas de configuración o de errores, así como la posibilidad de poner a disposición de los asociados de LACNIC y del público en general mayor información para la prevención,

puede resultar un camino interesante a explorar, especialmente si se puede realizar en forma personalizada, según las características de cada asociado.

En el mismo sentido, incrementar la oferta de servicios de seguridad en MILACNIC puede resultar valioso a la hora de contribuir a una mejora de la seguridad en la región.

La participación en eventos de seguridad a nivel internacional posiciona al WARP como referente en la materia, por lo que se espera continuar con estas actividades, así como concretar nuevos acuerdos.

En materia de servicios a la comunidad objetivo, durante los próximos años se continuarán personalizando las prestaciones según las características y necesidades de cada organización que compone nuestro ecosistema.

Glosario

APWG: Anti-Phising Working Group.

APT (Advanced Persistent Threat): tipo de ataque prolongado y dirigido, a partir del cual un intruso accede a una red y, sin ser detectado, permanece por un período extenso con la intención de robar datos o causar un daño en el momento más oportuno.

Botnet: conjunto de dispositivos que fueron capturados con un malware y que son controlados desde un centro de comando y control desde donde se les envían instrucciones para que ejecuten acciones no autorizadas. Afecta a dispositivos de todo tipo, incluso I0T.

Malware: código malicioso utilizado generalmente para robar información, destruir sistemas de forma total o parcial, o secuestrar información. Puede ser introducido en los sistemas mediante archivos adjuntos a correos electrónicos, descarga de aplicaciones y vulnerabilidades de los sistemas operativos.

M3AAWG – Messaging, Malware, Mobile and Anti-abuse Working Group.

Incidente de seguridad: todo evento que provoque un efecto adverso o amenace la disponibilidad, integridad y confidencialidad de los recursos de Internet, redes y los sistemas de información, incluyendo las transgresiones de políticas de uso o seguridad establecidas.

Pharming (Rogue DNS): es la explotación de una vulnerabilidad en el software de los servidores DNS o en los equipos de los usuarios que permite a un atacante redireccionar un nombre de dominio a otra máquina distinta.

Phishing: es un método de engaño a los usuarios diseñado para robar información sensible. Se presentan recursos fraudulentos como legítimos y, por lo general, apuntan a robar las credenciales de acceso de un usuario a un sistema, con el fin de llevar a cabo fraudes monetarios. Puede introducirse en los sistemas mediante correos electrónicos falsos o bien durante visitas a sitios de dudosa reputación.

Redirect: método de ataque utilizado para redireccionar a un usuario desde un enlace hacia otro (se puede formar una cadena de redirects). Por lo general, el usuario es redirigido hacia un sitio fraudulento.

RIR: Regional Internet Registry.

Triage: del francés trier, que significa clasificar o escoger. Es una de las etapas de la gestión de incidentes que comprende la recepción del reporte, la verificación, la clasificación inicial y la posterior asignación del caso para su resolución.

Unauthorized Prefix Advertising o BGP Hijacking: anuncios de prefijos de red no autorizados; anuncios de rutas desde orígenes no autorizados. Cuando un participante en el routing en Internet anuncia un prefijo que no está autorizado a anunciar, se produce un secuestro de ruta (route hijacking). Puede ser intencional o causado por error operacionales.

Siglas y abreviaturas

APWG Anti-Phishing Working Group

APT Advanced Persistent Threat

CERT Computer Emergency Response Team

CSIRT Computer Security Incident Response Team

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

ENISA European Network and Information Security Agency

FIRST Forum of Incident Response Teams

IOT Internet of Things

M^3AAWG Messaging, Malware and Mobile Anti-Abuse Working Group

OEA Organización de Estados Americanos

RIR Regional Internet Registry

RPKI Resource Public Key Infraestructure

TIC Tecnologías de la Información y las Comunicaciones

WARP Warning, Advice and Response Point

Listado de gráficos