Ciberseguridad y ataques dirigidos

Graciela Martínez
Coordinadora WARP

Latin American and Caribbean Network Information Center

LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe

Es una organización no gubernamental internacional establecida en Uruguay en el año 2002.

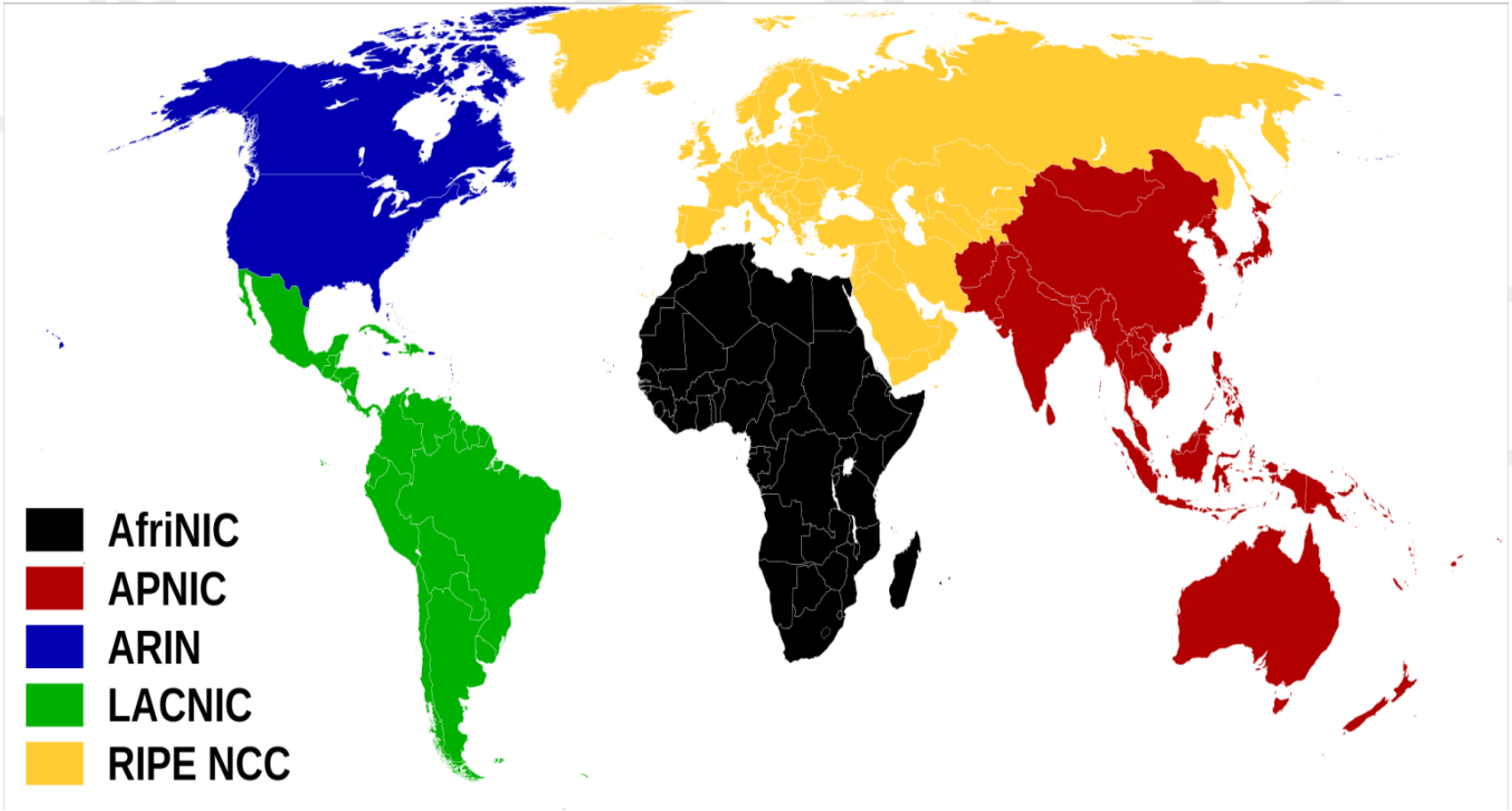
Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, para la región de América Latina y el Caribe.

Es uno de los 5 Registros Regionales de Internet en el mundo.

Coordina el desarrollo de las políticas

¿Cómo se asignan las direcciones IP?

Se asignan a través de los Registros Regionales de Internet: RIRs



¿Que rol cumple LACNIC?

Lo que no hace LACNIC:

- No tiene poder de policía en Internet
- No puede filtrar redes, ni arma listas de acceso
- No cancela la posesión de recursos por mal uso
- No sanciona a los ISPs

¿Que rol cumple LACNIC?

Lo que *si* hace LACNIC:

- Mantiene un WHOIS actualizado
- Sirve como organismo de coordinación en la región
- Brinda capacitaciones y formación a sus miembros
- Aconseja sobre mejores prácticas
- Decide políticas (reglas para la administración de los recursos de Internet) en base a propuestas de sus miembros

Hacia una gestión de incidentes de seguridad efectiva

LACNIC WARP

- Equipo coordinador y facilitador del manejo de incidentes de seguridad informática para los miembros de la LACNIC
- Sitio web: https://warp.lacnic.net/
- En línea con la misión de LACNIC tendiente a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento
- La comunidad objetivo está constituida por todas las organizaciones miembros de LACNIC

¿ COMO REPORTAR UN INCIDENTE ?

- WARP provee a los miembros un punto de contacto de confianza para el reporte de incidentes de seguridad u otra información sensible.
- Las organizaciones no miembros también podrán reportar incidentes de seguridad.
- El reporte de incidentes podrá realizarse:
  - Correo electrónico a la casilla: info-warp@lacnic.net
  - Formulario web: http://warp.lacnic.net/servicios/#reportar-incidente

INTERNET SECURITY

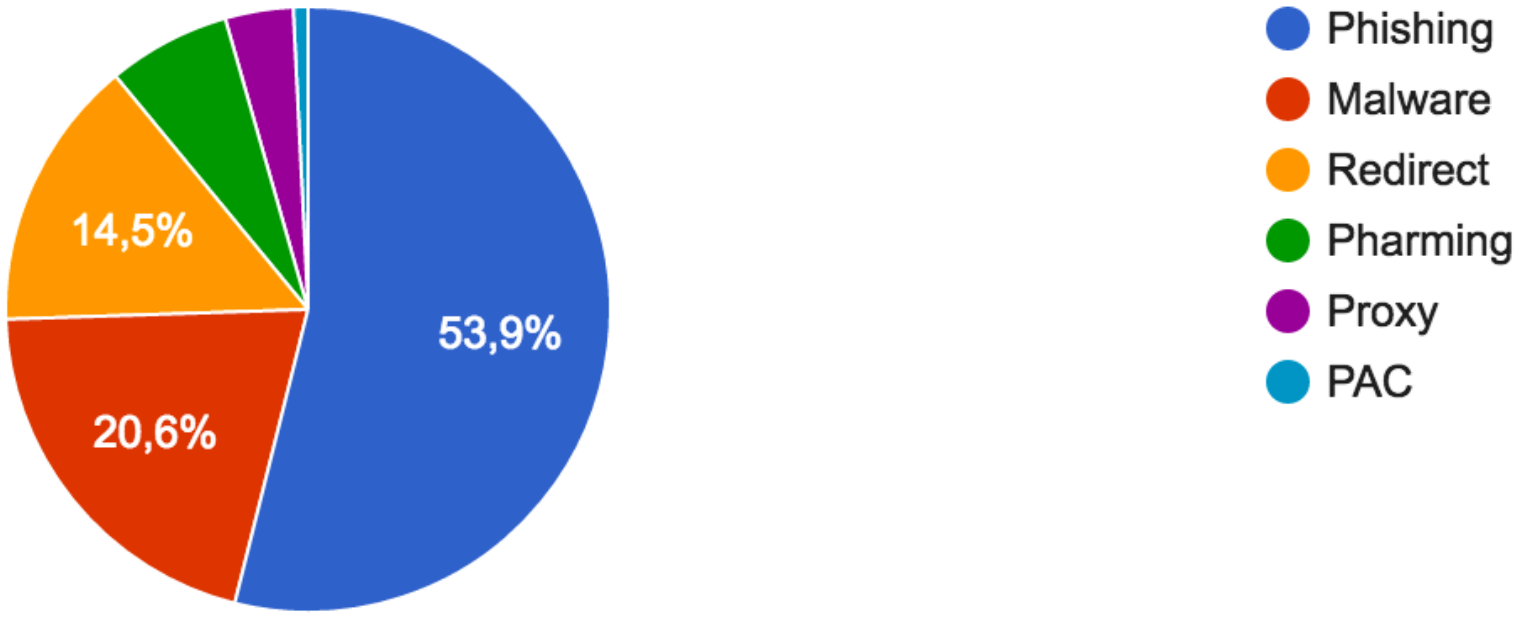
A tener en cuenta:

- Los criminales se han enfocado donde está el dinero.
  - Los estudios muestran que la economía de Internet genera anualmente entre $2 trillion - $3 trillion, y se calcula que el cybercrime se lleva entre 15% y 20%
- El espionage se enfoca donde está la información clasificada confidencial
- La infraestructura crítica está cada vez mas conectada a Internet

REPORTE de INCIDENTES

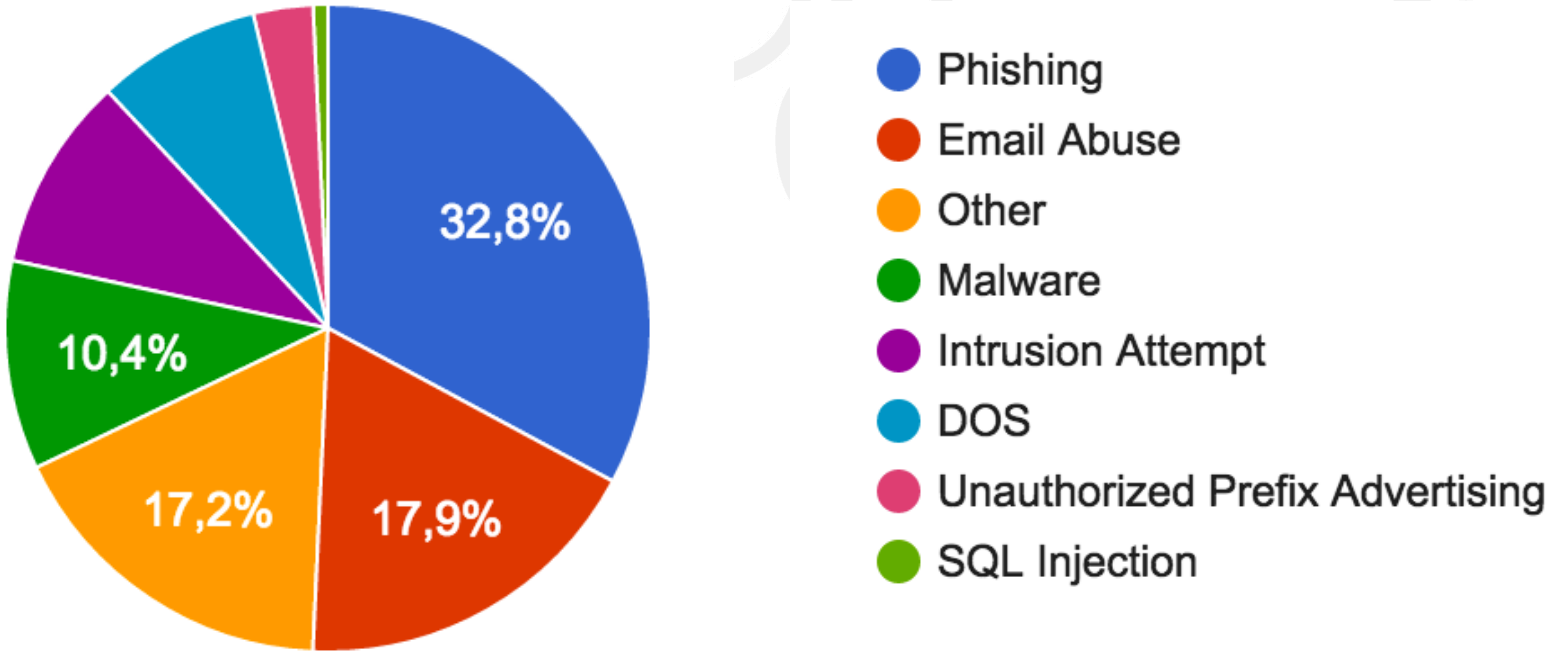
Esta gráfica muestra los incidentes notificados al WARP desde otras organizaciones diferenciados por tipo.

PAC – Proxy automatic configuration



REPORTE de INCIDENTES

Esta gráfica muestra los incidentes gestionados por WARP diferenciados por tipo.



OTROS TIPOS DE INCIDENTES

- Sextorsion – es una forma de explotación sexual a través de Internet
  - Chantaje:
    - Fines económicos
    - Otros fines – pornografía
  - No necesariamente es realizada por desconocidos
  - Fuentes: cámara web, fotos de dispositivos, etc.

OTROS TIPOS DE INCIDENTES

Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

OTROS TIPOS DE INCIDENTES

- RANSOMWARE – un tipo de malware que encripta archivos digitales y pide una recompensa a cambio de la clave para desencriptarlos.
- Ejemplos: CryptoLocker (2013), Locky (Feb. 2016), CryptoXXX (Mar. 2016)
- Notas:
  - $325 millones de ganancias al año
  - Utilizan la red TOR para el anonimato
  - Bitcoins – divisa electrónica – dificulta la trazabilidad
  - Pagar la recompensa no garantiza obtener la clave
  - Todo tipo de organización ha sido víctima de este ataque

OTROS TIPOS DE INCIDENTES

- Advanced Persistent Threats – APT
  - Malware altamente sofisticado
  - Requiere individuos altamente calificados, con expertise en diferentes tecnologías
  - Recursos financieros
  - Utilizados en contra de organizaciones estatales, industriales y militares.
  - Las técnicas utilizadas para atacar por lo general son “Zero-Day exploit” para la comunidad de seguridad

OTROS TIPOS DE INCIDENTES

- Ejemplos:
- Stuxnet – Activo Junio 2009 (2005) – Detectado Junio 2010
  - Pensado para atacar sistemas de control industrial. Se presume para sabotear el programa nuclear iraní.
  - Infección inicial: desconocida
  - Propagación: Red, dispositivos removibles
- Duqu – Activo desde Nov. 2010 – Detectado Set. 2011
  - Objetivo: espionaje
  - Infección inicial: MS Word
  - De acuerdo a lo que se sabe no infectó mas de 50 objetivos a lo largo del mundo
  - Desde la infección inicial, se mantuvo vivo por 36 días hasta su autodestrucción
  - Contenía keylogger para recolectar información sensible

OTROS TIPOS DE INCIDENTES

- Ejemplos (II):
- Flame – Activo desde Mayo 2012 (2006) - Detectado en Mayo 2012
  - Objetivo: robo de información. Infectó miles de sistemas Windows, en su mayoría del Medio Oriente. Contenía keylogger, interceptaba mensajes, capturaba pantallas, accedía al micrófono de las máquinas, etc.
  - Infección inicial: Desconocida
- Red October – Activo desde Mayo 2007– Detectado en Octubre 2012
  - Objetivo: recolección de información de agencias diplomáticas, gubernamentales y científicas.
  - Infección inicial: MS Excel / Word, Java

OTROS TIPOS DE INCIDENTES

- Ejemplos (III):
- Mini Duke – Junio 2012 – Detectado en Febrero 2013
  - Atacó a organismos de gobierno de 23 países en su mayoría europeos
  - Infección inicial: PDF
- Propagación manual: Duqu, Flame, R.Oct y Mini Duke

Medidas

- Administración adecuada de patches
  - Sistemas Operativos
  - Aplicaciones
  - Efectos limitados ante Zero-Day exploits, pero previene que nuevos sistemas sean infectados
- Segregación de la red
  - Estaciones de trabajo – Hardening de Servidores
- Aplicar políticas estrictas de acceso a internet, por ejemplo utilizando una white list de sitios
- Inspección granular de tráfico entrante y saliente
- Control del software a instalar y ejecutar en un sistema
- Control de cambios de configuraciones mediantes hashes
- Capacitación de usuarios

Algunos Problemas

- Mala legislación – Vacío legal – nacional e internacional
- Medidas de seguridad no adecuadas – contraseñas
- DDoS – ISP´s no atacan el problema de las botnets de forma efectiva
- Falta de implementación de buenas prácticas
  - BCP 38 – antispoofing
  - Educación de los usuarios: entiendan los riesgos
  - DNSSEC
  - RPKI
  - Desarrolladores: no toman en cuenta la seguridad desde el diseño

PROBLEMAS

- Falta de cooperación entre organizaciones
- Muchos usuarios no reportan los incidentes de seguridad
- Conocimiento de cybercrimen
  - Dos mayores fuentes:
    - Exposición a través de terceros – se conoce a alguien que fue victima de hacking, fraude de tarjeta de crédito, etc
    - Exposición a través de los medios – artículos on-line, series de TV, películas, etc.
- Muchas veces las medidas se toman despues!

Iniciativas de seguridad de LACNIC

Como objetivo estratégico, para contribuir con nuestra visión de fortalecer una Internet abierta, estable y segura y en un continuo crecimiento desarrollamos el programa Security, Stability and Resiliency – S.S.R.

- Security/Seguridad
  - DNSSEC - (DNS Security Extensions) es un conjunto de extensiones al protocolo DNS que permiten validar criptográficamente las respuestas que envían los servidores de DNS.
  - RPKI - es una infraestructura de clave que sirve para verificar el derecho de uso de un recurso de Internet por parte de un cliente.
  - Talleres de capacitación AMPARO

Iniciativas de seguridad de LACNIC

- Stability/Estabilidad
  - IXPs
  - Root Servers - El objetivo principal de +Raíces es la instalación de copias anycast de los servidores raíz en los países de la región de LACNIC. Mediante la instalación de estos servidores en puntos estratégicos de la región como IXPs (Internet Exchange Points) y NAPs (Network Access Points) se busca lograr un acceso más directo a uno de los recursos críticos de Internet como es el DNS, mejorando la conectividad de usuarios y proveedores de Internet locales.
- Resiliency/Resiliencia
  - IXPs – puntos de intercambio de tráfico

Cooperación regional

Nosotros creemos que la seguridad es responsabilidad de todos los actores de Internet.

En este sentido seguimos realizando una serie de actividades:

- Reunión de CSIRTS de la región en nuestros eventos anuales
- LACNIC es hosting para el FIRST TECHNICAL COLLOQUIUM
- Todos los meses tenemos una reunión virtual de la lista de LAC-CSIRTS donde compartimos inquietudes, proyectos, etc.

Otras Actividades

Foro LAC-CSIRTs

Objetivo: construir red de confianza para compartir información y experiencias y producir trabajos en conjunto

– Procedimiento de ingreso

Amparo

– Contribuye a fortalecer la capacidad regional en seguridad informática formando a nuestros miembros para que puedan crear la función de respuesta a incidentes de seguridad.

Muchas Gracias...

gmartinez@lacnic.net