LACNIC WARP
Respuesta a Incidentes de Seguridad

A.C. Graciela Martínez
Head of LACNI WARP
Security Incident Response

LACNIC WARP

- Llevar a cabo las funciones de coordinación necesarias para la respuesta a incidentes de seguridad vinculados a recursos de Internet de América Latina y el Caribe.

- La comunidad objetivo está constituida por todas las organizaciones miembros de LACNIC

Servicios de LACNIC WARP (I)

- Servicios a prestar por LACNIC ***WARP***

  - Filtered ***Warnings***: envío de advertencias de seguridad relevantes para la comunidad.

  - Intermediación (***Advice brokering*****):** se provee un ambiente seguro y anónimo de intermediación para la búsqueda, discusión e intercambio de información de incidentes de seguridad y buenas prácticas .

Servicios de LACNIC WARP (II)

- Reporte de incidentes (***Reporting Point***)
  - LACNIC 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, LACNIC WARP colaborará para redirigirlos según convenga.

¿ Cómo reportar un incidente de seguridad ?

El reporte de incidentes podrá realizarse a través de:

– Correo electrónico a la casilla: info-warp@lacnic.net

– Formulario web

www.lacnic.net/web/warp/form

Servicios de WARP

Los ejes de trabajo de un centro de respuesta pueden agruparse en tres tipos de servicios:

- Reactivos – Coordinación de incidentes de seguridad.
- Proactivos – Advertencias de seguridad, análisis de datos de spam, recursos de internet usados para phishing y malware, con fines estadísticos y de toma de acciones. Cooperación regional.
- Awareness – Fomentar la cultura del uso correcto de las TICs, buenas prácticas y capacitaciones.

Veamos entonces lo realizado en este sentido.

Capacitación y Awareness

- Con el proyecto AMPARO, instruimos a nuestra comunidad en cómo formar sus propios centros de respuesta. En esta año realizamos:
  - Dos talleres Amparo: Costa Rica y Paraguay
  - Se formaron 71 profesionales entre ambos talleres
  - Un taller Amparo Avanzado, en el marco de B-Sides.co Colombia, donde se formaron 15 personas
- Participamos en ICANN 53 donde brindamos un Taller Sobre Abuso de DNS y Mejores Prácticas Operacionales en conjunto con ICANN-OEA-INTERPOL
- II Foro de CiberSeguridad y Ciberdefensa 2015
- Tercer Taller Práctico para Centros de Respuesta a Incidentes de Seguridad – Bogotá Colombia.

Cooperación regional

Nosotros creemos que la seguridad es responsabilidad de todos los involucrados de alguna manera con Internet.

En particular LACNIC en este sentido seguimos realizando una serie de actividades:

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

Incidentes

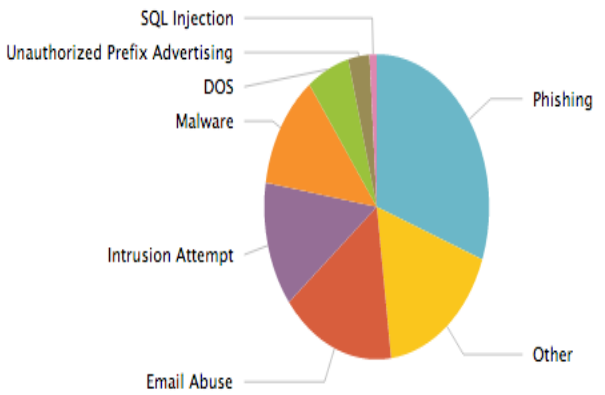
11m ago

	IncidentType	count	percent
1	Phishing	30	30.612245
2	Other	17	17.346939
3	Email Abuse	16	16.326531
4	Intrusion Attempt	13	13.265306
5	Malware	12	12.244898
6	DOS	6	6.122449
7	Unauthorized Prefix Advertising	3	3.061224
8	SQL Injection	1	1.020408

Tipos de Incidentes

11m ago

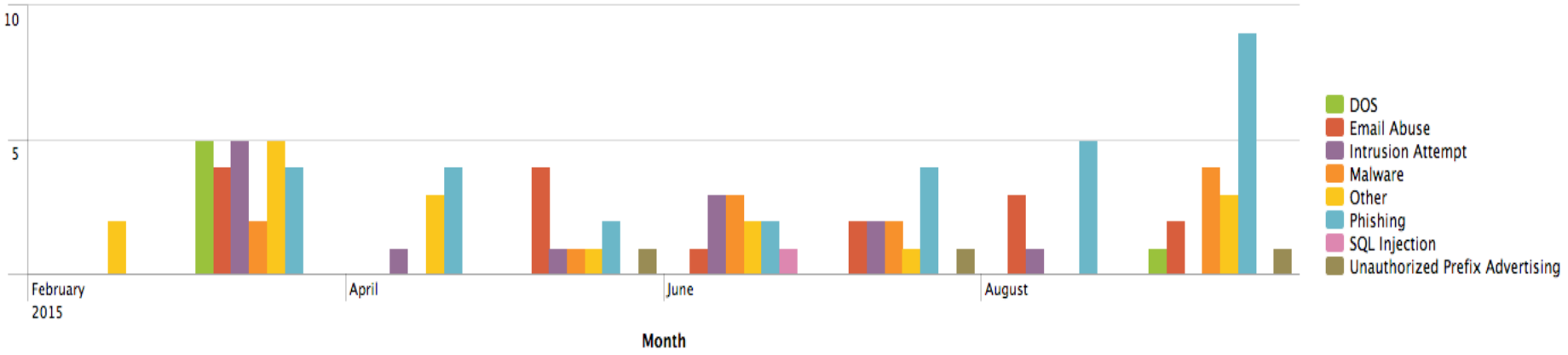
Tipos de Incidentes



Ticket Recibidos por Mes

11m ago

Ticket Recibidos por Mes



Próximos pasos

- Taller Amparo en La Habana – Cuba del 17 al 20 de diciembre
- Análisis de información y estadísticas, con la herramienta SPLUNK, utilizada por varios CSIRTS y recomendada por colegas en la conferencia anual del FIRST.
  - Splunk
    - Software para monitorizar y analizar Big Data
    - Captura, indexa y correlaciona en Tiempo Real
    - Interfaz web muy amigable
    - Gráficos, alertas y paneles que permiten
      - Identificación de patrones
      - Realizar mediciones
      - Diagnostico de problemas

Seguimos avanzando

En el marco de las metas específicas establecidas por la misión de LACNIC tendientes a lograr el fortalecimiento constante de una Internet *segura, estable, abierta* y en continuo crecimiento

lacnic24
lacnog
28/9 - 2/10
bogotá, colombia

Preguntas

Muchas Gracias...