Módulo de información de seguridad en MiLACNIC

Proyectos que nutren esta información y cómo pueden estos datos ayudar a los administradores en sus redes y/o sistemas.

Guillermo Pereyra
Analista en Seguridad LACNIC CSIRT

lacnic Csirt
Centro de Respuesta a Incidentes de Seguridad

lacnic csirt

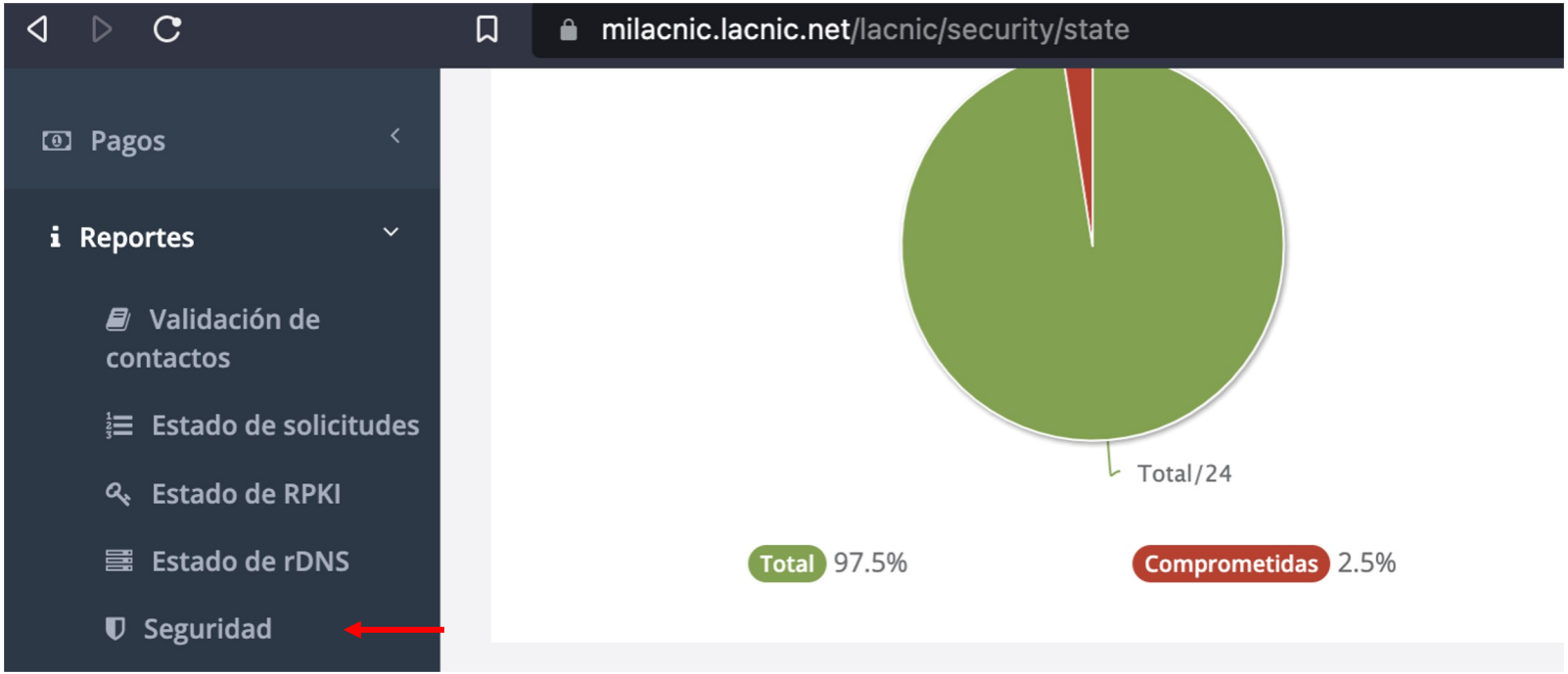
- Comunidad objetivo
- Rol
- Autoridad
- Punto de reporte - formulario web
  - https://csirt.lacnic.net/reportar-incidente
  - https://csirt.lacnic.net/solicitar-informacion-leas
- Cursos CAMPUS
  - Curso básico para creación de CSIRTS
  - Gestión de la información en investigaciones

Fuentes de Información

- Honeynet
- Open Resolvers IPv6
- Open Resolvers IPv4
- Actividades maliciosas
  - IoC Botnets (Mirai, Gamut)
  - Malware
  - Phishing
  - SPAM

→ milacnic

Módulo seguridad MiLACNIC



Módulo seguridad MiLACNIC

Funcionamiento de este módulo

Estadísticas / Alertas de Seguridad

Este módulo de Mi LACNIC provee información sobre eventos de seguridad informática donde se encuentran involucrados recursos pertenecientes a la región de LACNIC.

Dichas alertas de seguridad se procesan diariamente y se publican desde CSIRT (https://csirt.lacnic.net), son recibidas desde diversas fuentes de información: organizaciones con las cuales se tiene acuerdo de cooperación, datos propios recabados de nuestra Honeynet y del proyecto DNS Open Resolvers con IPv6.

Información Importante

Se debe tomar en cuenta que la información presentada se actualiza cada 24 hs.

En caso de existir alertas repetidas, significa que más de una fuente de información detectó el mismo evento.

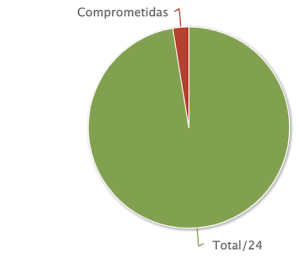
MÁS INFORMACIÓN SOBRE LOS PROYECTOS

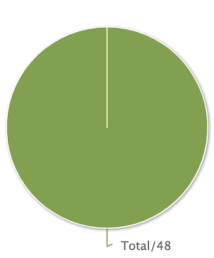
LACNIC Honeynet

Es una iniciativa de LACNIC CSIRT con la cual buscamos conocer de primera mano los tipos de ataques de seguridad más frecuentes en América Latina y el Caribe.

Para ello desplegamos una red de honeypots de interactividad media que nos permite visualizar los eventos de seguridad en tiempo real y conocer el modus-operandi de los ataques más comunes en la región, con el objetivo de generar inteligencia a partir de los

Módulo seguridad MiLACNIC





Reporte seguridad

A continuación verá una lista de todas las IPs que han sido comprometidas:

Filter:

Fecha	OrgId	IP	Tipo de ataque	Detalles	Más información
2022/09/28 21:27			botnet - gamut	Remote IP: - Remote Port: 25 - Protocolo: TCP	https://csirt.lacnic.net/glosario/#botnet_gamut
2022/09/29 00:00			Malicious activity	Malicious activity detected	https://csirt.lacnic.net/glosario/#malicious
2022/09/29 00:25			Phishing	hxxp://phishing.lacnic.net/	https://csirt.lacnic.net/glosario/#phishing

Info ofuscada

lacnic csirt
Centro de Respuesta a Incidentes de Seguridad

Posibles soluciones a los distintos reportes

Botnets - Distintas medidas dependiendo de la botnet

Open Resolvers - Restringir redes a las que se brinda el servicio, corrección de Firmware, bloqueos de puertos en CPE

Actividad maliciosa - Distintas medidas dependiendo del host

https://antispam.br/en/#4

Resumen

Conocer el estado actual de problemas de seguridad que puedan afectar a las actividades de las organizaciones, permite adoptar decisiones adecuadas para identificarlos y/o prevenirlos.

¡GRACIAS!

csirt@lacnic.net
https://csirt.lacnic.net/