Estadísticas

Estas estadísticas publicadas han sido generadas con el propósito de dar a conocer la situación de los recursos de Internet bajo la administración de LACNIC, que han sido utilizados con fines maliciosos, ya sea como origen o destino.

Algunas gráficas muestran cuáles son los tipos de ataques mas comunes que han sido gestionados por algún centro de respuesta a incidentes de seguridad.

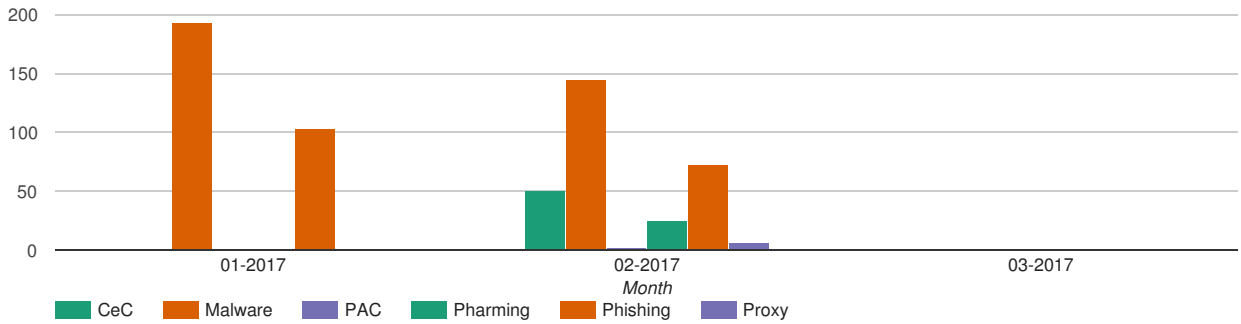
Los datos han sido recabados de algunas organizaciones colaboradoras y de fuentes propias.

Incidentes

Incidentes por Mes

Esta gráfica muestra los incidentes notificados al WARP discriminados por mes desde otras organizaciones.

Year x 2017



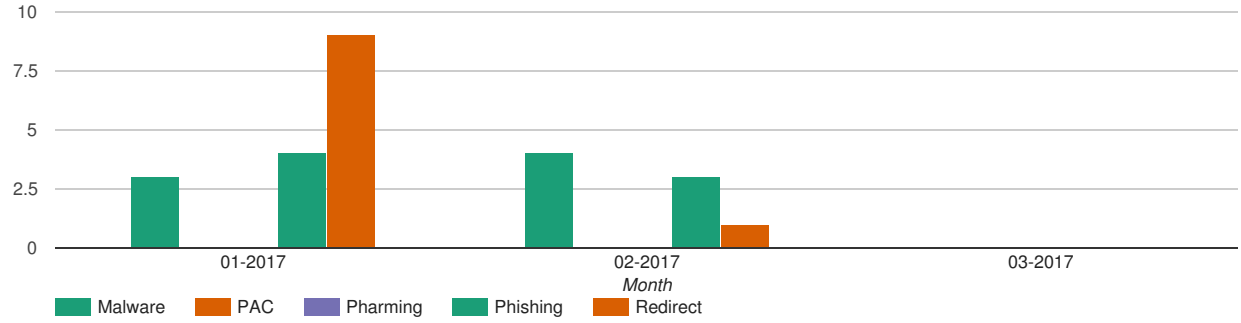
Tipos de Incidentes

Esta gráfica muestra el porcentaje de cada tipo de incidente notificados al WARP desde otras organizaciones.

Incidentes por Mes - Recursos LACNIC

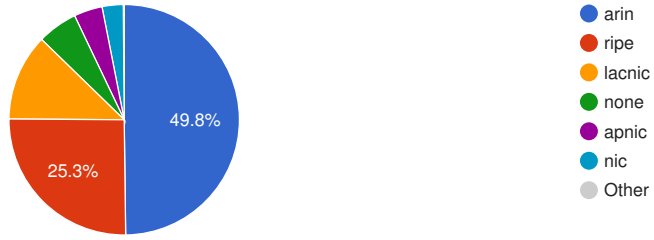
Esta gráfica muestra los incidentes notificados al WARP desde otras organizaciones que involucran recursos de la región de LACNIC como origen del ataque.

Year x 2017



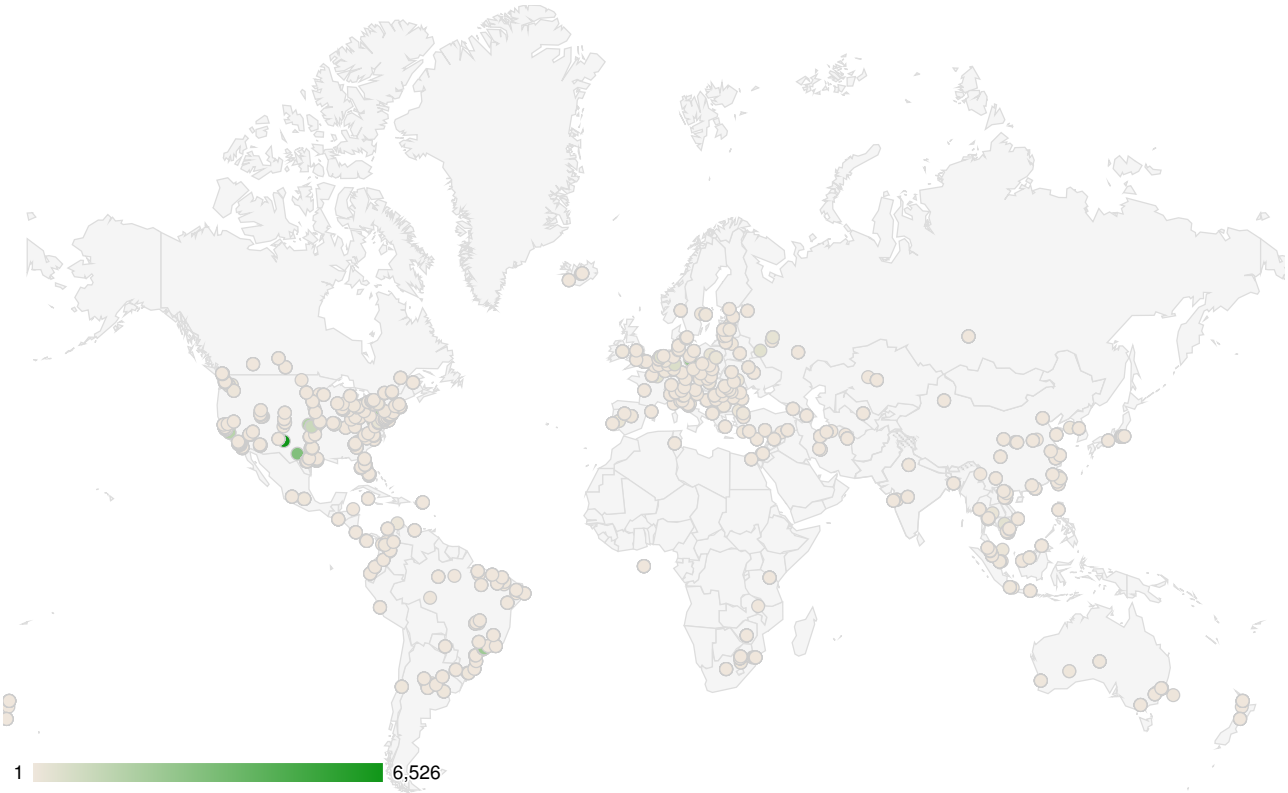
Incidentes por RIR

Esta gráfica muestra los incidentes notificados al WARP desde otras organizaciones, agrupados por regiones según el origen del ataque.



Geolocalización de Incidentes

Esta gráfica muestra los incidentes de seguridad notificados al WARP desde otras organizaciones geolocalizados según el origen del ataque.

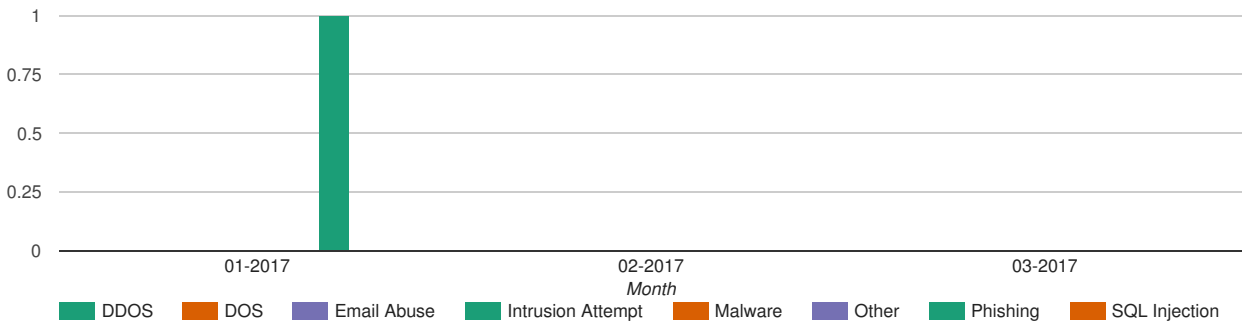


Incidentes Gestionados por WARP

Incidentes por Mes

Esta gráfica muestra los tipos de incidentes gestionados por WARP diferenciados por mes.

Year x 2017



Tipos de Incidentes

Esta gráfica muestra el pocentaje histórico de cada tipo de incidente gestionado por WARP.

Glosario

DoS

Denegación de servicio -Los ataques de Denegación de Servicio (DoS) consisten en realizar determinadas actividades con el fin de colapsar equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios autorizados. Por ejemplo: ping de la muerte, SYN Flood, etc.

Email abuse

Un ataque ejecutado a través de un mensaje de correo electrónico o un archivo adjunto al mismo, el cual contiene algún tipo de malware.

Fuerza Bruta

Método de prueba de ensayo y error. Por lo general se realiza a través de un software que utiliza un diccionario cargado de contraseñas comúnmente utilizadas, con el objetivo de descrifrar la clave de la víctima a través de comparaciones y pruebas sucesivas.

Intrusion attempt

Intento de acceso no autorizado – Ataque por fuerza bruta con el fin de obtener la clave de acceso a un sistema. El protocolo más común reportado para este tipo de ataques es el SSH.

MALWARE

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

PHARMING – (Rogue DNS)

Es la explotación de una vulnerabilidad en el software de los servidores DNS, o en el de los equipos de los propios 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. En el mismo se presentan recursos fraudulentos como legítimos, y por lo general apuntan a robar las credenciales de acceos de un usuario a un sistema, con el fin de llevar a cabo fraudes monetarios. Puede ser introducido a los sistemas mediante correos electrónicos falsos o bien mediante visitas a sitios de dudosa reputación.

Other

Corresponde al resto de los reportes de incidentes de seguridad que no pertenecen a las otras categorías.

Unauthorized Prefix Advertising

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 esta autorizado a anunciar se produce un “secuestro de ruta” (route hijacking). El mismo puede ser intencional o causado por error operacionales.

REDIRECT

Método de ataque utilizado para redireccionar a un usuario de un link hacia otro, pudiendo inclusive formar una cadena de “Redirects”. Por lo general el usuario es redirigido hacia un sitio fraudulento.

REDIRECT

Método utilizado para redirecionar o usuário de um link para outro, podendo inclusive formar uma cadeia de Redirects.

PAC – Proxy auto-config.

Un ataque PAC redirige el tráfico especificado en el script malicioso hacia un servidor proxy fraudulento. De esta forma el atacante puede visualizar todo el tráfico de los usuarios víctima, lo que le puede permitir capturar información confidencial, como por ejemplo usuario y contraseña, o secuestrar sesiones de autenticación ya realizadas mediante el robo de sus cookies.

PROXY

Es un servidor intermediario entre los requerimientos de un cliente y un servidor destino. Todas las solicitudes de conexión de los usuarios de una red son enviadas al destino deseado a través del mismo. Este mecanismo puede permitir la visualización de la información que pasa por él, como por ejemplo usuario/contraseña u otra información sensible.