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.

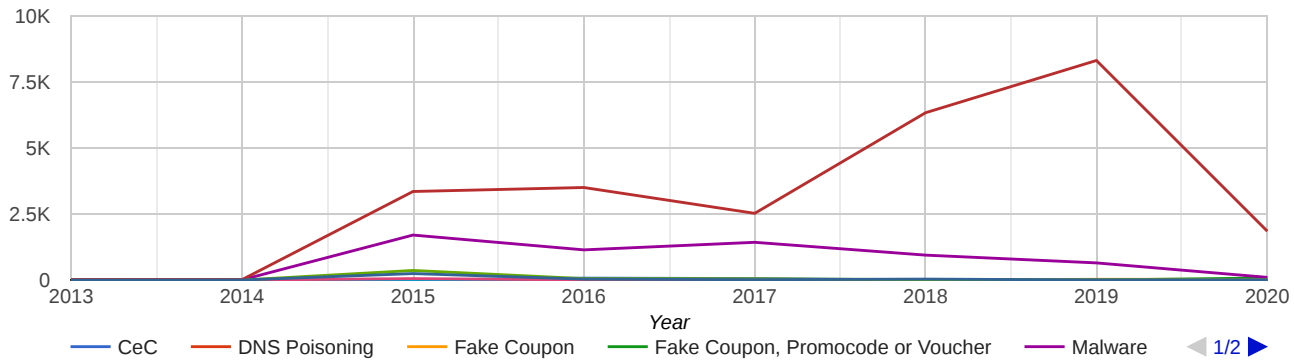
Los datos han sido recabados de algunas organizaciones colaboradoras y de fuentes propias.

Incidentes

Incidentes por Año

Esta gráfica muestra los incidentes anualizados que fueron notificados al WARP desde otras organizaciones.

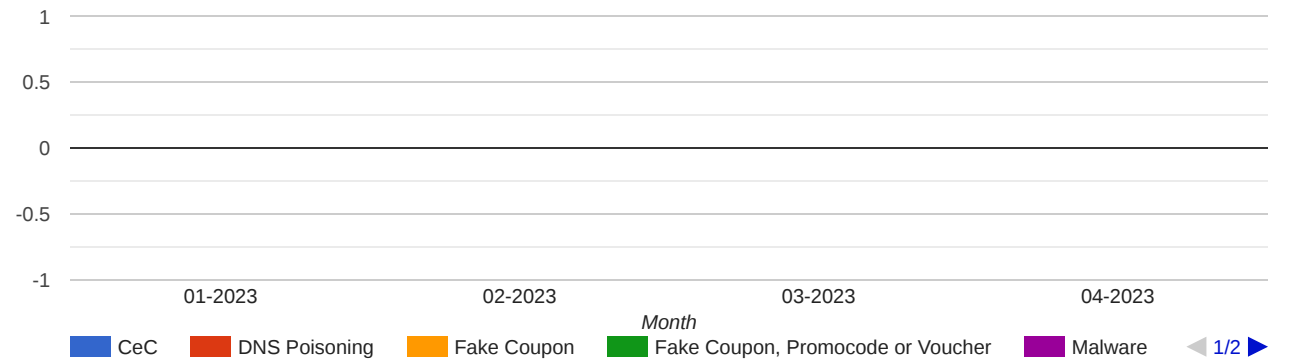
Year Choose year...



Incidentes por Mes

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

Year Choose year... × 2023



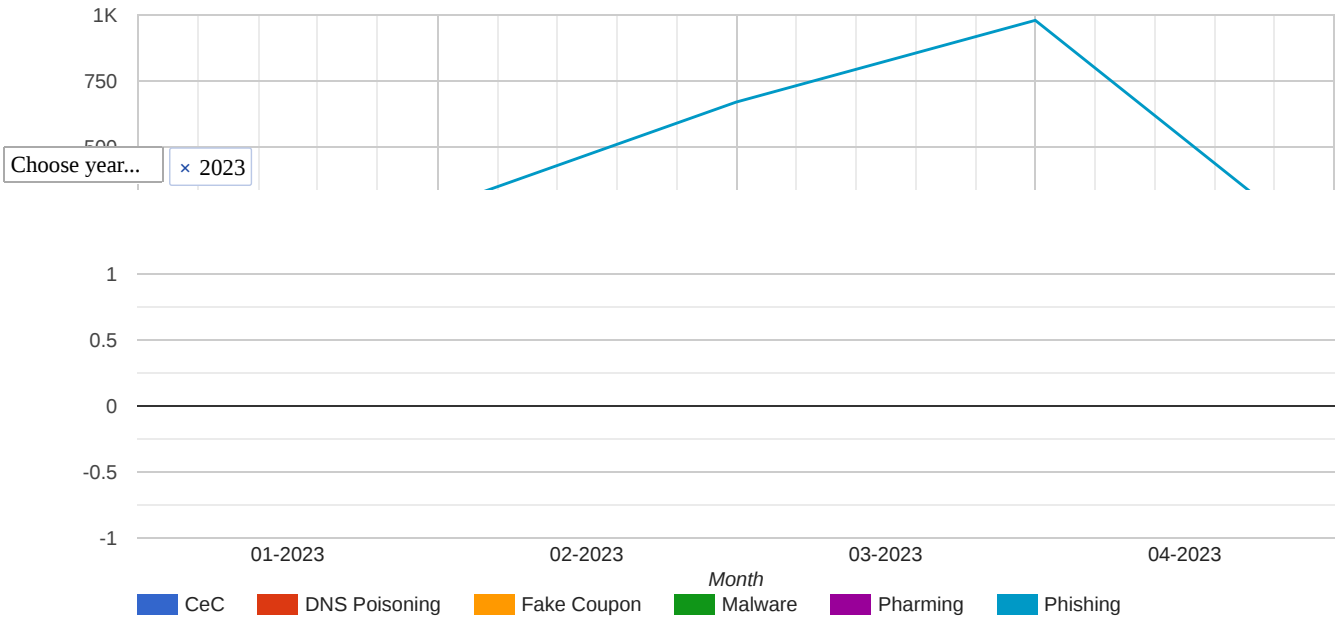
Tipos de Incidentes

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

Incidentes por Año - Recursos LACNIC

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

Year Choose year...


1K
750
Choose year...
× 2023
1
0.5
0
-0.5
-1
01-2023
02-2023
03-2023
04-2023
Month
CeC
DNS Poisoning
Fake Coupon
Malware
Pharming
Phishing

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

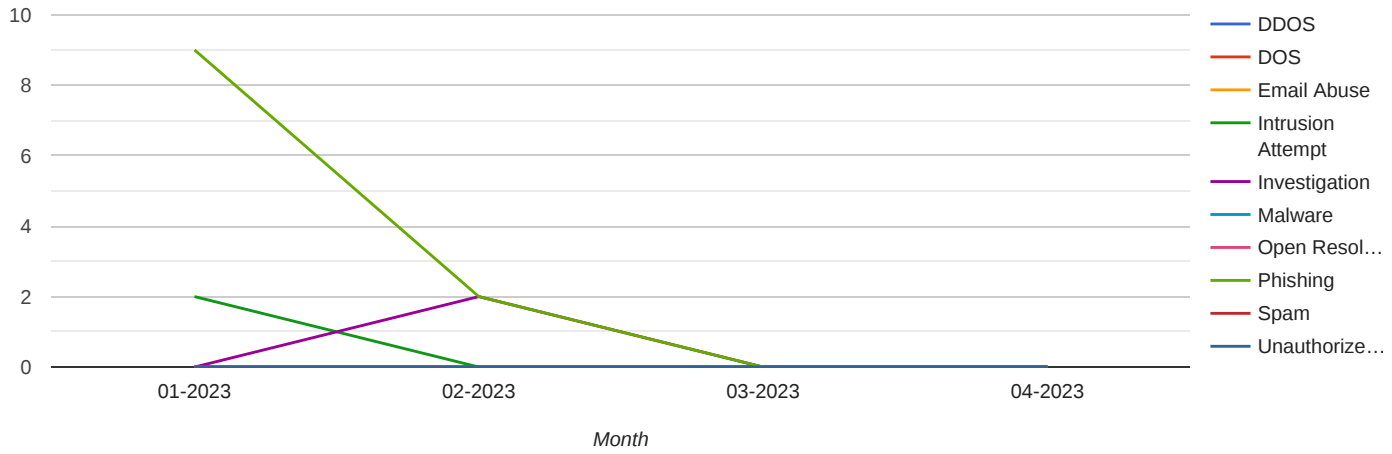
Esta gráfica muestra los incidentes de seguridad notificados al WARP desde otras organizaciones geolocalizados según el origen del ataque.

Incidentes Gestionados por WARP

Incidentes por Mes

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

Year Choose year... × 2023



Tipos de Incidentes

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

Botnets

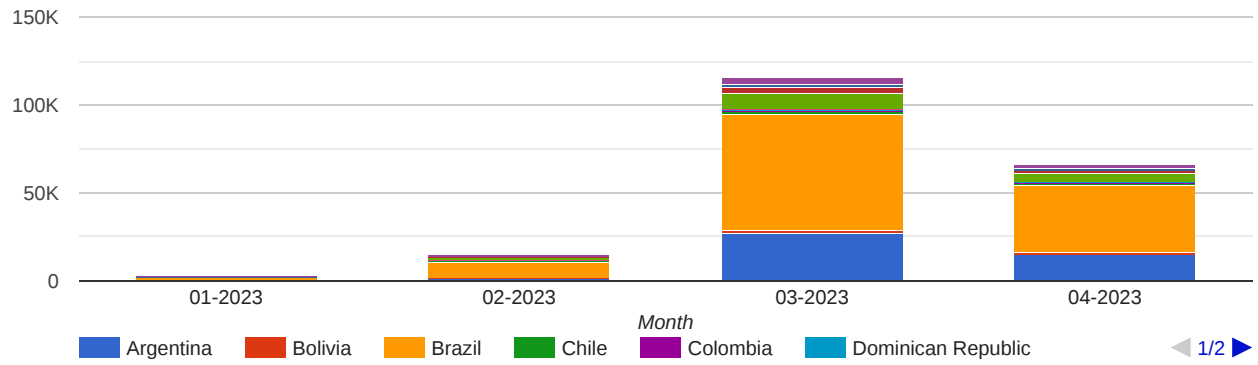
Tipos de Botnet

Esta gráfica muestra los tipos de botnet más comunes que afectan a recursos de la región.

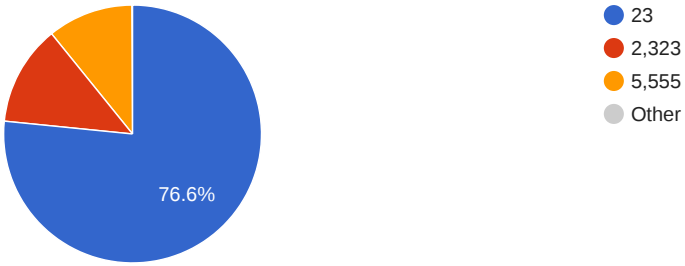
Mirai

Eventos Mensuales por País Esta gráfica muestra los incidentes de MIRAI notificados al WARP desde otras organizaciones discriminados por mes.

Year Choose year... × 2023



Top de Puertos Esta gráfica muestra los puertos más utilizados para ataques por la botnet mirai.



Glosario

Beta Bot (Neurevt)

Neurevt es un troyano que corre como un servicio del sistema operativo que infecta ordenadores con Windows. Este troyano ha sido diseñado para robar información sensible como credenciales de acceso a determinados servicios, datos del sistema operativo, de la computadora del usuario, entre otros.

CeC

Unidad de Comando y Control de diferentes malware. Son utilizados para la interacción entre el atacante y la máquina de la víctima, tanto para enviar como para recibir informaciones.

Conficker

Conficker es un malware de tipo gusano que afecta a ordenadores con sistema operativos Windows. Una vez infectado un ordenador pasa a ser parte de una red de bots, los cuales son controlados de forma remota por un nodo central. Este malware puede ser utilizado para realizar muchas actividades delictivas, sin embargo principalmente se ha usado para robar información de los sistemas infectados y realizar spam.

Cutwail (Pushdo)

Cutwail es un malware de tipo troyano que infecta ordenadores con sistemas operativos Windows, pasando a ser parte de una red de bots o botnet. Básicamente es utilizada para el envío de correo spam y descarga archivos con malware en el ordenador infectado para posteriormente ejecutarlos.

Fake Coupon

Cupones o Vouchers de descuento que se utilizan como cebo para obtener informaciones personales de los usuarios, normalmente compartidos vía WhatsApp.

DNS Poisoning

Servidor de DNS malicioso que tiene como objetivo re-dirigir a un usuario que desea acceder a un sitio legítimo para una sitio falso para robarle su información personal.

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.

Dyre

Dyre es un malware de tipo troyano que infecta ordenadores con sistema operativo Windows, pasando a ser parte de una red de bots o botnet. Entre las diferentes funcionalidades podemos destacar: robo credenciales, envío de correo spam o descarga e instalación de otros archivos con malware.

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.

Gamut

Gamut es un malware de tipo troyano que infecta ordenadores con sistema operativo Windows. Los ordenadores infectados pasan a ser parte de una red de bot o botnet, que son controladas de forma remota, y que son usadas para cometer delitos. Principalmente el objetivo de esta botnet ha sido la distribución de spam.

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.

Kelihos

Kelihos es el nombre de una botnet que utiliza comunicaciones de tipo P2P, dificultando de esta forma la detección de los centros de control. Algunas de las funciones de la Botnet son: ataques de DoS, spam, robo de monederos de Bitcoin o minería de Bitcoin.

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.

Mirai (iotmirai)

MIRAI es una botnet que afecta a Internet de la Cosas, conocida como IoT, por sus siglas (Internet of Things). Este malware explota vulnerabilidades de distintos dispositivos, como por ejemplo routers, grabadoras digitales de vídeo y cámaras IP de vigilancia. Esta botnet ha sido utilizada principalmente para realizar ataques de denegación de servicio (DoS).

Open Relay

Open Relay es un servidor SMTP configurado de tal manera que permite que cualquier usuario de Internet lo use para enviar correo electrónico a través de él.

Other

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

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.

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.

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.

Proxy Poisoning

Servidores en los que son hospedados sitios falsos, para donde son enviados los usuarios víctimas de Pharming.

RANSOMWARE

Aplicación maliciosa que infecta una computadora, cifrando ciertos archivos. De esta forma restringe el acceso del usuario a los mismos, hasta que se pague un rescate a cambio de la clave para descifrarlos.

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.

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.

ZeroAccess

ZeroAccess es un malware de tipo troyano que infecta ordenadores con sistema operativos Windows, pasando estos a ser parte de una red de bots o botnet. Estas redes de botnets, que son controladas de forma remota por un nodo central, pueden ser utilizadas para múltiples objetivos maliciosos. Los ordenadores infectados además de estar controlados por una unidad central, tienen como principal objetivo: Minería de Bitcoin o Fraude en campaña online de anuncios.