

Noticias, comentarios y anuncios tecnológicos

**En esta edición:**

**Ataques DDoS**

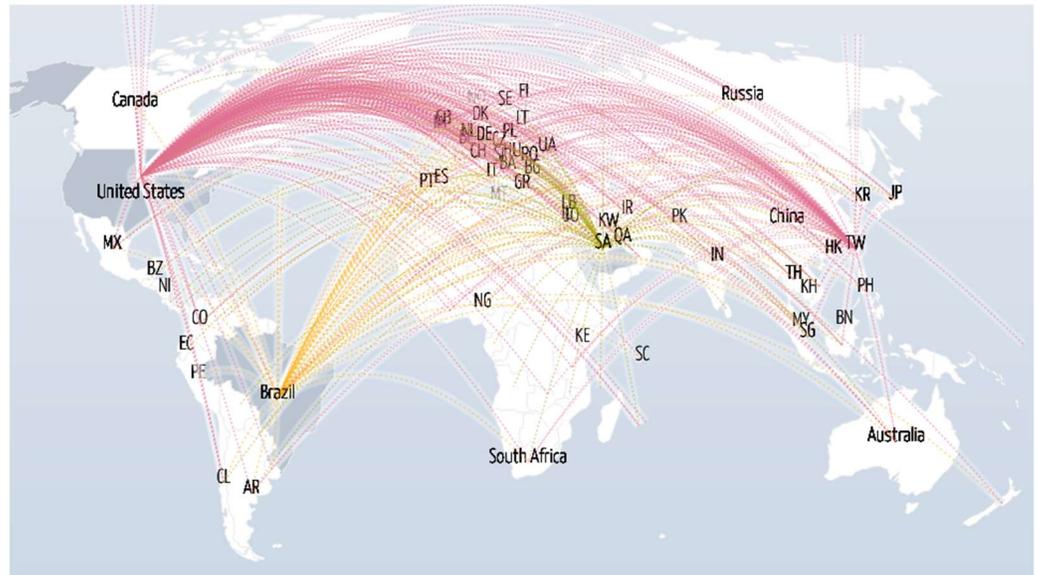
Inundación y afectación de los servicios de red

**Botnet**

Red compuesta por miles de zombies

**Malware**

Software malicioso: virus y gusanos



**Representación de un ataque distribuido en tiempo real**

## Ataques DDoS

**Los ataques de denegación distribuida de servicio (DDoS) son ataques informáticos que generalmente son llevados a cabo por un grupo de computadores infectados con software malicioso, ubicados alrededor del mundo.**

Generalmente, el ataque consiste en inundar en un momento determinado y de forma coordinada, uno o varios sitios web con miles de visitas de forma simultánea, afectando de forma parcial o completa el funcionamiento de estos servicios.

El aumento significativo de las solicitudes de servicio recibidas termina sobrepasando la capacidad de los servidores que brindan los servicios web respectivos, haciendo imposible responder de forma inmediata la demanda de acceso provocada por el atacante, así como las solicitudes de servicios ordinarias del público en general.

También, puede provocar el bloqueo temporal del ancho de banda de internet de una organización, afectando por completo todas las facilidades que dependen de este servicio en particular.

Este tipo de ataque es dirigido específicamente contra objetivos previamente seleccionados. En muchos casos, la persona ignora que su computador forma parte de una actividad de este tipo.



## Malware

**El malware es un concepto que agrupa a varios tipos de software malicioso, hostil, intrusivo y no autorizado. Entre ellos tenemos gusanos (worms), caballos de troya, virus informáticos, software espía (spyware), software de rescate (ransomware), entre otros.**

La medida para protegerse contra este fenómeno es la instalación de un **software antimalware**.

### Virus

La palabra proviene del latín **virus**, que hace referencia al veneno, o alguna sustancia nociva.

Un virus informático es un software que altera o destruye los datos almacenados en un computador. Tienen la capacidad de propagarse en los sistemas infectados mediante el intercambio de archivos contaminados, llegando a contaminar programas o documentos almacenados en un dispositivo electrónico.

### Gusano

Un gusano informático es una subclase de un virus informático. Son segmentos de software que se duplican a sí mismos en un computador infectado, propagándose de forma autónoma entre computadores o redes informáticas existentes.

## Botnet

Botnet es el término utilizado para referirse a un conjunto de computadores infectados con un software malicioso, los cuales forman parte de una red bajo el control de un **Bot Master**.

El Bot Master es el principal recurso de administración de la Botnet a cargo de un atacante, el cual a través de equipos denominados servidores de **Comando y Control** (C&C) infectan a otros computadores, con el fin de integrarlos a la Botnet.

Una Botnet es una red distribuida que puede estar formada por miles - o millones - de equipos de cómputo contaminados, ubicados por todo el mundo.

Los equipos infectados pasan a ser llamados Bots o robots. También, se les denomina **Zombies**.

El objetivo de la Botnet es llevar a cabo ataques del tipo **DDoS**, el ejecutar envíos masivos de correo electrónico no deseado (**spam**), o infiltrar equipos de cómputo mediante la búsqueda de vulnerabilidades existentes en el software instalado en estos equipos, entre otros.

También, se utiliza para llevar a cabo **minería de criptomonedas** sin el conocimiento de la persona afectada.

Debe evitarse la instalación de software de origen dudoso o desconocido, y la apertura de mensajes o enlaces sospechosos recibidos por medio del correo electrónico.