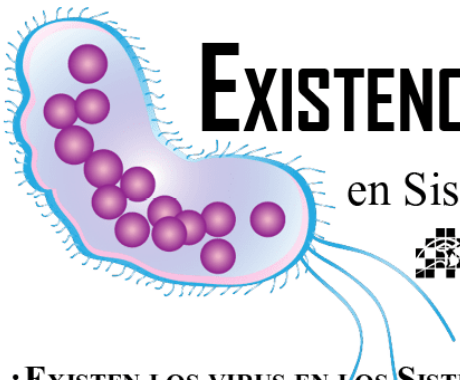
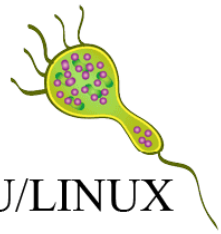


Existencia de Virus



en Sistemas Operativos GNU/LINUX

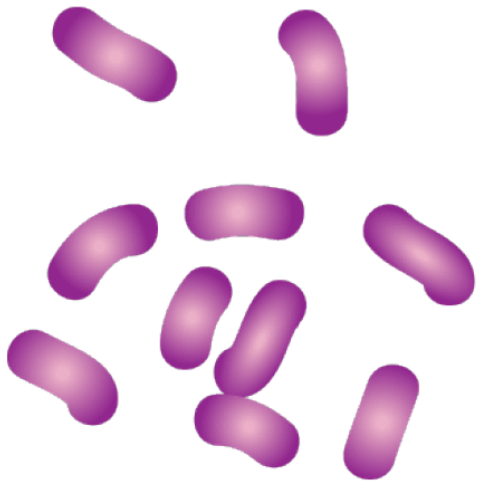
Samuel Pavón / samuel.pavon@ucv.ve

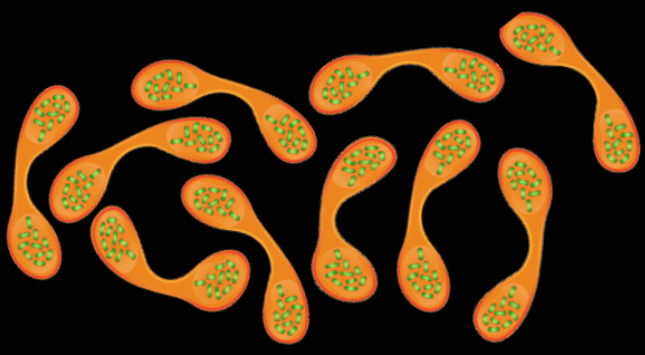
¿Existen los virus en los Sistemas Operativos GNU/Linux?

El debate sobre los sistemas operativos libres y los virus no es algo nuevo, en reiteradas ocasiones dentro de los foros de tecnología y listas de correos, se ha formulado la pregunta: ***¿Existen virus para linux?***, la verdad es que, ni administradores de sistemas, ni desarrolladores, inclusive las personas que responden afirmativamente en los foros y listas de correos han experimentado alguna vez la existencia de virus en un sistema ***Linux***, lo cual hace del tema todo un mito que ha sido difícil de desmontar; principalmente por la presencia de intereses económicos.

Existen personas interesadas en transmitir una idea que establezca que ***Linux*** no tiene este tipo de problemas porque muy poca gente lo utiliza, argumento que pudo haber tenido sustento hace algún tiempo; pero que en nuestros días es totalmente desfasado y carece de credibilidad porque la mayoría de los servidores a nivel mundial, así como una gran proporción de los dispositivos móviles y de escritorios funcionan actualmente bajo la combinación ***GNU/Linux***.

Tomando en cuenta lo expuesto anteriormente, la verdadera discusión pareciera estar enmarcada en esclarecer técnicamente si es o no es posible que existan virus para ***Linux***. En la actualidad no hay pruebas concluyentes que evidencien su existencia, aún cuando estos sistemas son muy difundidos. Sin embargo, antes de argumentar es necesario que primero se conozcan algunos términos relacionados con el tema.





¿Qué es un virus?

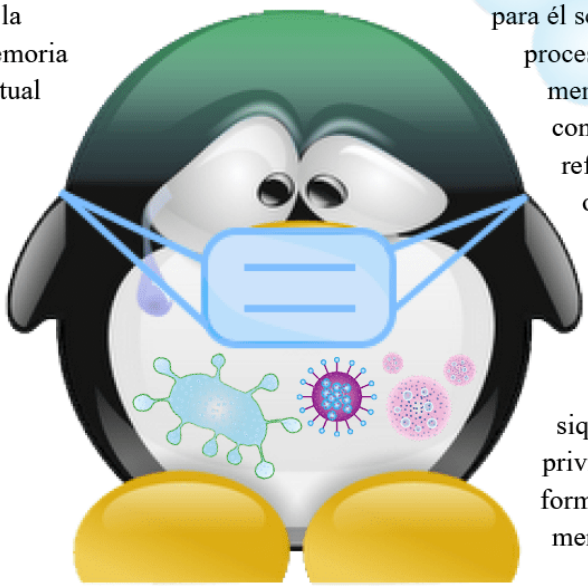
Es un programa que se copia y se ejecuta automáticamente, sin permiso o conocimiento del usuario, con el objetivo de alterar el normal funcionamiento de un computador. Para ello, los virus reemplazan archivos ejecutables por otros infectados con su código. El virus se instala solo y esa es la característica que lo diferencia del resto del **malware.**

La transmisión de los virus en *Linux*

El mecanismo de propagación de un virus, es lo que realmente lo define como tal, y es la base de la existencia de los mismos. Los virus tienen exclusivamente sólo dos métodos de transmisión:

1. Replicándose accediendo a la memoria de otros procesos, durante su ejecución:

En este método se puede indicar que la arquitectura de la memoria virtual de ***Linux*** no permite a ningún proceso ejecutarse en el mismo nivel de procesamiento que el ***kernel***, porque son dos instancias separadas; el ***kernel*** se ejecuta en una instancia del procesador y los procesos del sistema en otra instancia, lo cual mantiene a estos dos componentes aislados.



El ***kernel*** mediante el uso de la memoria virtual hace creer a cada proceso que tiene toda la memoria para él sólo, de esta forma, un proceso sólo puede ver la memoria virtual que le han configurado y no es capaz de referenciar la memoria de otro proceso. En efecto, la arquitectura de memoria virtual impide este mecanismo de transmisión porque ningún proceso (ni siquiera los que tienen privilegios de ***root***) tienen forma de acceder a la memoria de otros.

2. Infectando ejecutables en *Linux*

Este otro método abre los ejecutables del sistema de archivos y añade su código a dicho ejecutable.

En ***Linux*** los procesos son limitados por el usuario efectivo y su grupo efectivo. Si nos fijamos donde están los ejecutables, veremos que solamente ***root*** tiene privilegios de escritura tanto en directorios, como en los ficheros contenidos, es decir, únicamente ***root*** puede modificar los archivos.

Por ende, la única forma de propagar el código de un virus es siendo ***root***. En este caso para que un virus funcione es necesario que los usuarios tengan siempre privilegios de administrador, pero para transmitir la infección necesita tomar otro ejecutable, mandarlo por correo a otro usuario que sólo emplee el equipo como ***root***, y que repita el proceso.■

Conclusión:

Los sistemas operativos **GNU/Linux** tienen vulnerabilidades, tales como: gusanos, troyanos y **rootkits**. Hay herramientas para explotar estas vulnerabilidades, pero esos instrumentos no se pueden definir como virus.

Un virus legítimo tendría que saltar una serie de dificultades que paradójicamente siempre se han puesto como un defecto/problema de **Linux** (por los defensores de Windows); estas dificultades son las que complican la existencia de virus reales en un sistema **Linux**.

Referencia

Este artículo es una síntesis del reportaje **"Mitos y realidades: Linux y los virus"** de la revista **Todo Linux Nº 90**, autor: David Santo Orcero.

Para visualizar la fuente original ingrese al siguiente link: http://blog.desdelinux.net/wp-content/uploads/2012/01/Mitos-y-realidades-Linux-y-los-virus.pdf