

Nodo De Tor Es Usado Para Infectar Gran Cantidad De Usuarios

Anteriormente compartimos algunos consejos para [usar](#)  [Tor](#), aunque los hayas leído de seguro no te hubieras salvado de la reciente infección que reportaron **usuarios de Tor** que estaban descargando **archivos desde la Deep Web**, quienes se llevaron una desagradable sorpresa recientemente. Un nodo de Tor de salida malicioso se ha descubierto, el cual estaba **añadiendo código malicioso** en las descargas binarias.

Estos archivos no eran necesariamente infectados desde lugares «oscuros». Josh Pitt de Leviathan Security Group, [vio](#) como archivos procedentes de varios proveedores de confianza, entre ellos [Microsoft](#) se infectaron durante el envío por el [ataque de hombre en el medio](#) en el nodo. Cuando el código ha sido descargado por completo, inmediatamente llama por teléfono a los servidores de C & C a través de HTTP y abre cierto **puerto para recibir instrucciones**.

Una vez que **Pitt** confirmó la actividad maliciosa, informó el nodo de infección al **proyecto Tor**. Rápidamente se marcan como malicioso para que el tráfico de otros usuarios, y así evitar otras infecciones. **Pitt** señaló que éste era el único nodo malicioso que se encontró durante su encuesta de más de 1.100 usuarios.

Sin embargo, es un recordatorio de que necesitas verificar y ver las descargas antes de ejecutarlas. Incluso cuando accedes a un archivo de un proveedor de confianza, está claro que es posible que la carga se modificará, y así modificar la estructura de tu sistema operativo. Pero, ¿Cual es la mejor defensa en este momento? Trate de seguir las descargas que se realicen a través de una [conexión SSL](#). Pitt recomienda usar un

plug-in como [HTTPS Everywhere](#), desarrollado por el grupo de EFF, con la **ayuda de nada menos que el proyecto Tor**.