

<https://info.nodo50.org/NOTA-Analisis-de-los-ataques-de.html>



# Análisis de los ataques de Octubre del 2013 contra Nodo50 y sus organizaciones alojadas

- Noticias - Noticias Destacadas -

Fecha de publicación en línea: Miércoles 30 de octubre de  
2013

---

Copyright © Nodo50 - Todos derechos reservados

---

Durante el mes de octubre de 2013, una serie de ataques distribuidos de denegación de servicio y amenazas anónimas a través del correo electrónico y Twitter se lanzaron en contra de la organización sin ánimo de lucro Nodo50 (ORG-NA403-RIPE). Estamos finalizando un informe que presentará una descripción detallada de la naturaleza de los ataques y de las identidades y organizaciones que están vinculadas a ellos.

Adelantamos que la principal conclusión de este análisis forense es que el principal requisito, para que estos ataques pudieran ser efectivos, es la capacidad del atacante para comprar alojamiento y/o el acceso al alquiler de servidores y herramientas en un proveedor de hosting que permite la generación y encaminamiento de tráfico de Internet falso dentro de su red. Hemos sido capaces de rastrear el tráfico de los ataques hasta el Amsterdam Internet Exchange (AMSIX) y pudimos determinar que **el atacante estaba lanzando los ataques desde Ecatel**, un proveedor de alojamiento en los Países Bajos. Nuestras simulaciones de laboratorio indican que el atacante podría generar los ataques con el uso de tres servidores dedicados alojados en Ecatel.

Gracias a las muestras obtenidas de los ataques, hemos podido localizar un anuncio en un foro de Internet donde un persona de buyddos.com proporciona instrucciones detalladas para la implementación de ataques basandose en el uso de servidores o servicios alojados en Ecatel.

También, hemos podido correlacionar los e-mails que recibimos del atacante y la revisión de la información disponible en varios sitios públicos donde el atacante reivindicada y documenta los ataques, y así determinar que el agresor es o hace uso de la identidad de D.V.G., una persona que puede operar desde Torre Vieja y que se hace conocer en los foros de juegos en red como -----.

La conclusión de nuestro análisis apunta a un solo atacante usando la identidad de D.V.G. que pudo descargar e instalar código disponible en el foro [www.hackforums.net](http://www.hackforums.net) en servidores Ecatel, en los Países Bajos. El atacante pudo también contratar dichos servicios a terceros a sabiendas de que ese proveedor de alojamiento era conocido por permitir el tráfico falso proviene de su red.

*En las próximas horas publicaremos el informe técnico ampliando la información.*

## Más noticias en prensa

- [InfoLibre: La Policía detiene a un miembro de Falange por los ataques a infoLibre y otros medios digitales](#)
- [Diagonal: Detenido un ultraderechista como presunto autor de los ataques a medios digitales de izquierdas](#)
- [La Marea: Detenido un joven nazi por amenazas y ataques a medios de comunicación digitales](#)
- [El Plural: Un falangista, detenido como responsable del ataque a ELPLURAL.COM y otros medios progresistas](#)
- [El Diario: Detenido un hacker ultraderechista por ataques informáticos a varios medios](#)
- [El País: Detenido por atacar a medios en Internet en nombre de un comando fascista](#)