https://info.nodo50.org/NOTA-Nueve-dias-de-ataque-contra.html

Ataque de denegación de servicio (DDoS) contra proyectos alojados en Nodo50

Doce días de ataque contra Nodo50

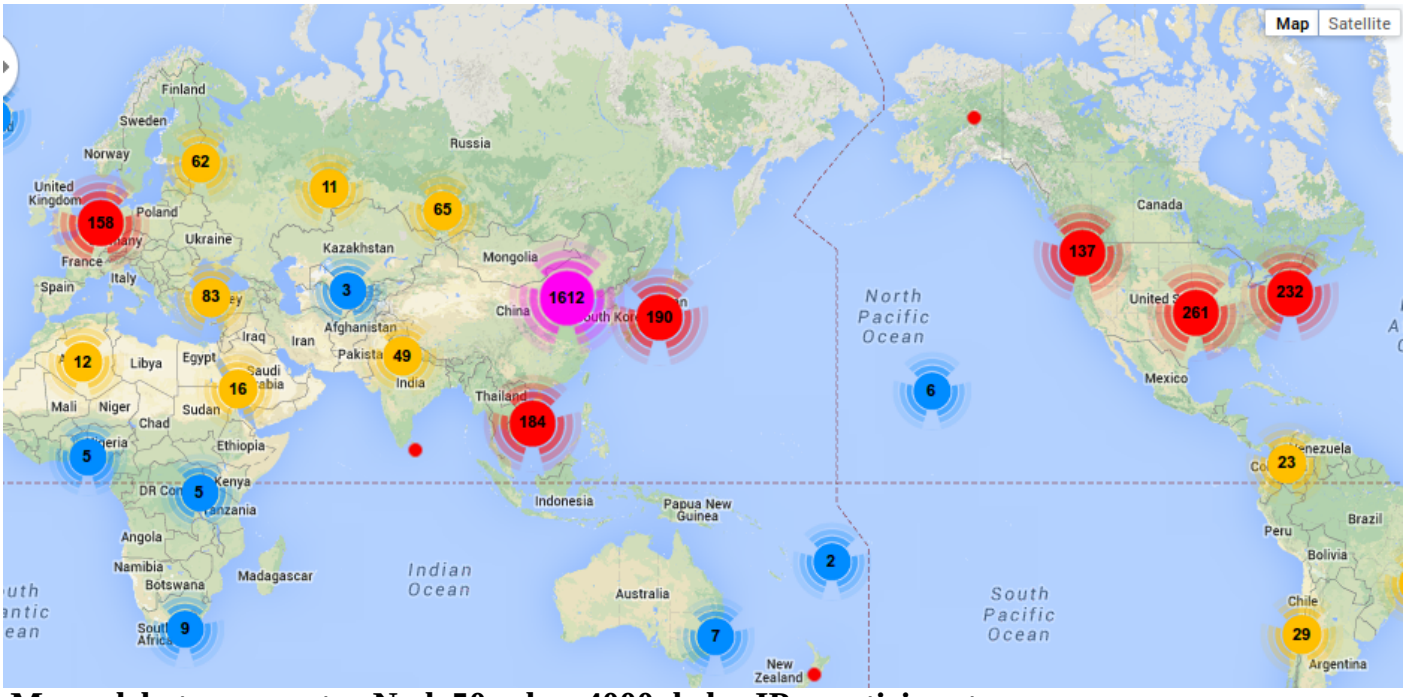
- Noticias - Noticias Destacadas -

Fecha de publicación en línea: Jueves 24 de octubre de 2013

ACTUALIZACIÓN 24 DE OCTUBRE

Sigue las reacciones e informaciones sobre el #ataquenodo50

24 de octubre: Nueve días de ataque de denegación de servicio (DDoS) contra proyectos alojados en Nodo50.



Mapa del ataque contra Nodo50 sobre 4000 de las IPs participantes

ACTUALIZACIÓN 24 de Octubre

Desde las 0:00 horas a las 2:00 horas del jueves 24 de octubre se ha registrado un nuevo ataque contra proyectos alojados en Nodo50.

ACTUALIZACIÓN 21 de Octubre

De nuevo ataques DDoS contra proyectos alojados en Nodo50.

ACTUALIZACIÓN 19 de Octubre

Se cumple una semana de ataques DDoS contra proyectos alojados en Nodo50.

ACTUALIZACIÓN 18 de Octubre

Sexto días de ataques DDoS contra proyectos alojados en Nodo50. En esta ocasión desde las 11:30 horas están lanzando distintos ataques contra el periódico Diagonal y otras webs alojadas de Nodo50.

Mismo atacante y tipo de ataque. Seguimos tomando medidas para minimizar las incidencias en el servicio.

ACTUALIZACIÓN 17 de Octubre

Continua el ataque contra proyectos alojados en Nodo50. En esta ocasión desde las 16:49 horas están lanzando distintos ataques contra el periódico Diagonal y colectivos anticapitalistas, además de la portada de Nodo50.

Los ataques provienen de la misma red botnet de alquiler que en anteriores ocasiones.

ACTUALIZACIÓN 16 de Octubre

Hoy, 16 de octubre, se repite el ataque de DDoS contra Nodo50, una copia de los anteriores. El ataque ha comenzado a las 14:00 horas y ha durado 4 horas.

Como en anteriores ocasiones estaba compuesto por tres *sub-ataques*:

1. Una inundacion de trafico UDP reflejado usando servidores de nombres abiertos.
2. Una inundacion de paquetes SYN con cabeceras falsas.
3. Trafico fragmentado UDP y ICMP.

Hemos detectado la firma digital de la red botnet usada y la fecha en que se puso en el mercado, el 23 Septienbre 2013, arrancando su funcionamiento el 1 de Octubre de 2013.

Esta firma digital es identica a los ataques que hemos recibido los ultimas días, podemos afirmar que proviene del mismo atacante.

La repetición y tipo de ataque corresponde con el modelo habitual utilizado por organizaciones criminales en internet, que prestan este tipo de servicio bajo pago.

Sigue sin haber una reivindicación ni mensaje del atacante sobre los motivos para intentar silenciar los proyectos alojados en Nodo50.

En esta ocasión se ha mitigado más rápido los efectos del ataque que en anteriores intentos, apenas sintiéndose sobre el normal servicio de las webs afectadas.

El escaso impacto sobre el servicio no minimiza la importancia de los hechos. El ataque contratado está destinado a impedir el funcionamiento de nuestros servidores y con ello impedir la visibilidad en internet de los proyectos

alojados en Nodo50.

COMUNICADO

14 de octubre de 2013

El pasado 12 de Octubre, a las 0:00 horas, comenzaba un ataque de denegación de servicio (DDoS) contra Kaosenlared.net, organización alojada en Nodo50.

Este tipo de ataques buscan invisibilizar la web víctima mediante la saturación del servidor. Los atacantes amplificaron su tráfico usando servidores de terceros y excediendo la capacidad del servicio. En el ataque que hemos sufrido han participado más de 32.000 máquinas distintas y generado más de 3Gbps.

Por el número de servidores atacantes empleados y su distribución (ver el gráfico de 4000 de esas IPs) parecen haber sido alquiladas a alguna red de botnet. En internet existen mercenarios del hack que revenden este tipo de infraestructuras para que personas sin capacidad puedan lanzar ataques DDoS.

El domingo 13 de octubre los efectos del ataque se han dejado sentir impidiendo el normal acceso a Kaosenlared.net. Esta mañana, 14 de octubre, hemos logrado mitigar el ataque y tanto el proyecto atacado como otras webs afectadas funcionan desde entonces con normalidad.

Posteriormente el atacante ha decidido atacar la web de nodo50, info.nodo50.org, sin grandes incidencias en el servicio.

En el momento de escribir el comunicado los atacantes han desistido.

Kaosenlared ha recibido un mensaje de autoria, aunque no aporta ningún dato que permita contrastar la autenticidad. Como en otras ocasiones resulta imposible determinar con certeza el origen del ataque. El único mensaje cierto es el intento de silenciar un medio de comunicación.

Queremos agradecer una vez más la solidaridad mostrada con nodo50 y el compromiso mutuo con las organizaciones que integran el proyecto. Seguimos peleando por la libertad de expresión y el derecho a informar.

Asamblea de Nodo50

Distribución de los operadores de máquina

Distribución de los operadores de máquina que participaron en el ataque del 13 y 14 de octubre.

CN **620** CHINANET-BACKBONE No.31,Jin-rong Street
CN **375** CHINA169-BACKBONE CNCGROUP China169 Backbone
KR **154** KIXS-AS-KR Korea Telecom
KR **107** LGDACOM LG DACOM Corporation
CN **82** CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd.
KR **76** HANARO-AS Hanaro Telecom Inc.
US **47** COMCAST-7922 - Comcast Cable Communications, Inc.
CN **43** CHINANET-SH-AP China Telecom (Group)
TW **39** ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information Center
CN **37** CNIX-AP China Networks Inter-Exchange
CN **36** CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
US **36** CABLE-NET-1 - Cablevision Systems Corp.
US **35** CMCS - Comcast Cable Communications, Inc.
US **33** CHARTER-NET-HKY-NC - Charter Communications
CN **33** DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.
KR **21** KRNIC-ASBLOCK-AP KRNIC
CN **21** ERX-CERNET-BKB China Education and Research Network Center
CN **18** CNCGROUP-SH China Unicom Shanghai network