https://info.nodo50.org/116-horas-de-ataques-continuados-de-denegacion-de-servicio-contra-medios-de.html

Análisis técnico

116 horas de ataques continuados de denegación de servicio contra medios de comunicación

- Noticias - Noticias Destacadas -

Fecha de publicación en línea: Martes 30 de noviembre de 2021

Entre los días 19 y 23 de noviembre de 2021 se produjo un ataque continuado de denegación de servicio que tuvo como objetivo siete sitios web alojados en los servidores de Nodo50. Todos ellos medios de comunicación independientes de poderes económicos. Una semana después y tras el análisis de, entre otras cosas, 107 GB de logs con 428 millones de líneas, esto es lo que hemos averiguado sobre el ataque.

Nodo50 es un proveedor de servicios de Internet sin ánimo de lucro y enfocado a los movimientos sociales. Los medios de comunicación que han sido víctimas del ataque son:

- *La Marea*, que es una publicación en papel y digital surgida del cierre de la edición en papel del diario Público en 2012. Es un medio independiente de poderes empresariales y políticos ya que su financiación proviene de sus lectores/as.
- *El Salto* es un medio de comunicación creado en 2016, producto de la evolución del periódico *Diagonal* y de la convergencia de varias decenas de medios de comunicación. Se rige por principios democráticos, de propiedad colectiva, descentralizado y financiado por la gente, no por grandes corporaciones, para asegurar su independencia informativa.
- *Kaos en la Red* fue creado en 2001 y se define como un medio de contrainformación plural, de alcance mundial y de enfoque anticapitalista.
- *AraInfo* es un diario libre fundado en 2010. Se define como un proyecto cooperativista que trabaja por la soberanía de la comunicación desde principios solidarios, colaborativos, de honestidad y feministas.
- Y también el propio sitio web de *Nodo50*, donde, además de ofertar sus servicios como proveedor de internet, publica cada día una pequeña selección de noticias.

Los sitios web afectados durante el ataque fueron:

- www.elsaltodiario.com y tienda.elsaltodiario.com
- www.lamarea.com y kiosko.lamarea.com
- www.kaosenlared.net
- www.arainfo.org
- info.nodo50.org

Los ataques duraron 116 horas, comenzando el 19 de noviembre a las 12:21 UTC y por un periodo de 4 días y medio hasta el martes 23 de noviembre a las 22:13 UTC.

Desde el primer día el atacante utilizó dos tipos principales de ataques:

- Ataques de capa de aplicación (L7) contra cada uno de los sitios utilizando más de 27.000 direcciones IP. El atacante inundó los sitios con solicitudes falsas por turnos o inundando varios sitios simultáneamente.
- Ataques de inundación de tráfico UDP mediante tráfico reflejado, principalmente usando los servicios NTP y DNS.

Durante la fase inicial de los ataques, el atacante realizó varias comprobaciones online para verificar la eficacia de sus estrategias. Utilizó el servicio check-host.net, utilizado con frecuencia por "booters" o "IP stressers" de pago (servicios para realizar ataques).
[https://info.nodo50.org/local/cache-vignettes/L319xH400/check-host_elsalto_down-2dee0.png]

Al no tener éxito, el atacante añadió más potencia a sus ataques, añadiendo otras botnets compuestas por proxies abiertos, la red Tor y docenas de dispositivos del servicio VPN vpngate.com.
[https://info.nodo50.org/local/cache-vignettes/L319xH400/check-host_lamarea_up-40b39.png]

Una gran parte de las botnets proceden de India, Vietnam, Túnez y Rusia. Muchos de los bots están dentro de redes domésticas, lo que sugiere que el atacante compró acceso a una infraestructura de ataque que tiene el control de dispositivos de IoT (Internet de las cosas) o de dispositivos infectados por malware.

Casi 9.000 direcciones IP participantes en el ataque están asociadas a los proveedores de India AS55836 Reliance Jio Infocomm Limited y a los de Vietnam AS131429 MOBIFONE-VN y AS7552 Viettel Corporation.

Autoría del ataque

Estos ataques rara vez son reivindicados, pero en este caso alguien que reclamaba la autoría se puso en contacto por Twitter con los medios atacados y con Nodo50. Desde la cuenta de Nodo50 se le pidió una prueba de la autoría, cosa que hizo anunciando la interrupción del ataque contra www.kaosenlared.net, lo que efectivamente sucedió.

La cuenta de usuario del atacante, @a66229952, fue eliminada el sábado 20, sin que haya vuelto a ponerse en contacto por otros medios. Ignoramos si la cuenta fue auto borrada o si Twitter la canceló por reportes de otros usuarios/as.
[https://info.nodo50.org/local/cache-vignettes/L284xH400/twitter_photo-e02e1.jpg]
[https://info.nodo50.org/local/cache-vignettes/L298xH400/twitter_2021-11-20_14.07.20-5f071.jpg]

Por la forma en que se desarrolló el ataque, por la forma en que reaccionaba a nuestras medidas de mitigación, y por la forma en que distribuía su potencia de ataque entre varios objetivos, nos parece que se trataba de una única persona, al menos en lo que se refiere a la parte técnica de ejecutar el ataque (“al teclado”).
[https://info.nodo50.org/local/cache-vignettes/L211xH400/twitter_2021-11-20_14.29.52-c5ae3.png]
[https://info.nodo50.org/local/cache-vignettes/L400xH187/twitter_2021-11-20_14.39.06-72868.png]

Además, por las horas de inicio y final de los ataques de flujos UDP (ver tabla mas abajo), podemos deducir que está en la zona horaria del estado español, o muy próximo, que está libre a partir de las 12 del mediodía para dedicarse a los ataques, y que detiene los ataques UDP antes de irse a dormir, no muy tarde, entre las 00:00 y las 01:00 AM. Quizás no tiene presupuesto para dejarlos toda la noche en automático, pues es muy probable que los ataques de inundación de tráfico UDP le salgan mas caros que los L7 al necesitar IP spoofing. Llegó a usar 152 horas de ataques UDP contra diferentes objetivos (suman mas que el total de horas del ataque porque se solapaban al atacar a varios objetivos a la vez).

Sobre la motivación del atacante se ha especulado con su ideología ultraderechista. No hemos encontrado nada que pueda confirmarlo, mas allá de la fecha elegida para comenzar el ataque (fin de semana del 20-N) y que los medios atacados forman parte de lo que un ultraderechista puede considerar medios antagonistas. Al contrario que en 2013, cuando el atacante se definió a sí mismo como falangista, el autor de este ataque no realizó proclamas ideológicas en el poco tiempo que estuvo activo en Twitter.

Vectores de ataque

L7 - Capa de aplicación (TCP) Algunas de las inundaciones contra los sitios web se realizaron abusando del KeepAlive (sesiones HTTPS persistentes), cuando un bot lograba establecer la primera sesión web cifrada (HTTPS)

con el sitio, una ráfaga de miles de solicitudes de inundación se canalizaban en la misma conexión activa.

Otro vector de ataque consistió en realizar peticiones Proxy CONNECT al puerto 80/443 de los sitios web que utilizan Apache como servidor web, para luego inundar el sitio con solicitudes de Proxy al puerto HTTPS cifrado.

Durante gran parte del ataque, las inundaciones tuvieron una media de 10.000 solicitudes por segundo con picos que alcanzaron las 30.000.

Los ataques L7 se lanzaron ininterrumpidamente durante los 4 días y medios del ataque, al contrario que los de inundación UDP que tuvieron interrupciones por las noches.

L4 - Ataques volumétricos (UDP) El atacante combinó los ataques de la capa de aplicación (L7) con los ataques de la capa 4 basados en UDP. Los ataques L4 se realizaron en su mayoría abusando de servidores públicos NTP (puerto 123) y DNS (puerto 53). También estuvieron presentes otras técnicas de amplificación de L4, como SynOptics SNMP (puerto 391) y el, recientemente descubierto, vector de amplificación DDoS Web Services Discovery (puerto 3702).
[https://info.nodo50.org/local/cache-vignettes/L400xH315/l4-1-941f5.png]

Los ataques volumétricos L4 tenían como objetivo generar una sobrecarga de la capacidad de los enlaces de tránsito entrantes al centro de datos.

Durante el ataque se utilizó el dominio fak.dk en la amplificación de tráfico DNS. Nuestras pruebas arrojaron una respuesta de 10 KB por cada consulta de DNS. El nombre de dominio fak.dk utilizado por la infraestructura de estrés corresponde a las páginas del "Royal Danish Defense College", pero eso no implica que dicha institución esté implicada en el ataque, solo que su dominio fue elegido para las consultas DNS a amplificar.
[https://info.nodo50.org/local/cache-vignettes/L400xH224/l4-2-96c75.png]

Relación de ataques de UDP (según los flujos que hemos registrado)

```
67 ataques
 152 horas en total

 Web atacada | fecha | hora de inicio UTC  | duración en horas
 ========================================
 www.kaosenlared.net | 2021-11-19 | 12:28:21 | 1.0
 www.kaosenlared.net | 2021-11-19 | 15:19:20 | 1.0
 www.kaosenlared.net | 2021-11-20 | 09:19:05 | 2.0
 www.elsaltodiario.com | 2021-11-20 | 09:19:19 | 2.0
 www.arainfo.org | 2021-11-20 | 09:33:23 | 1.0
 info.nodo50.org | 2021-11-20 | 10:18:15 | 1.4
 www.arainfo.org | 2021-11-20 | 11:30:25 | 0.9
 www.elsaltodiario.com | 2021-11-20 | 11:56:33 | 1.0
 www.kaosenlared.net | 2021-11-20 | 12:34:07 | 2.4
 info.nodo50.org | 2021-11-20 | 12:47:47 | 5.6
 www.arainfo.org | 2021-11-20 | 15:07:57 | 1.0
 tienda.elsaltodiario.com | 2021-11-20 | 15:58:16 | 2.5
 info.nodo50.org | 2021-11-20 | 17:54:02 | 1.0
 info.nodo50.org | 2021-11-20 | 18:03:32 | 1.0
 info.nodo50.org | 2021-11-20 | 18:48:30 | 1.0
 info.nodo50.org | 2021-11-20 | 18:48:45 | 1.0
 info.nodo50.org | 2021-11-20 | 18:51:37 | 1.0
```

info.nodo50.org | 2021-11-20 | 20:12:03 | 3.8
tienda.elsaltodiario.com | 2021-11-20 | 20:52:13 | 3.1
info.nodo50.org | 2021-11-20 | 21:04:37 | 1.0
info.nodo50.org | 2021-11-21 | 00:00:01 | 0.1
tienda.elsaltodiario.com | 2021-11-21 | 00:00:01 | 0.1
tienda.elsaltodiario.com | 2021-11-21 | 11:14:32 | 12.8
info.nodo50.org | 2021-11-21 | 11:16:40 | 12.7
www.lamarea.com | 2021-11-21 | 11:29:55 | 1.0
www.lamarea.com | 2021-11-21 | 11:30:07 | 2.4
kiosco.lamarea.com | 2021-11-21 | 12:24:30 | 1.0
kiosko.lamarea.com | 2021-11-21 | 13:04:31 | 2.2
www.lamarea.com | 2021-11-21 | 13:12:28 | 1.0
kiosco.lamarea.com | 2021-11-21 | 14:36:08 | 1.0
www.lamarea.com | 2021-11-21 | 15:55:53 | 1.0
kiosco.lamarea.com | 2021-11-21 | 17:01:57 | 4.9
www.lamarea.com | 2021-11-21 | 18:01:04 | 0.9
www.lamarea.com | 2021-11-21 | 19:05:19 | 0.8
www.elsaltodiario.com | 2021-11-21 | 22:12:35 | 1.0
kiosco.lamarea.com | 2021-11-21 | 23:02:41 | 1.0
www.lamarea.com | 2021-11-21 | 23:02:54 | 1.0
kiosco.lamarea.com | 2021-11-22 | 00:00:02 | 1.1
info.nodo50.org | 2021-11-22 | 00:00:03 | 1.1
tienda.elsaltodiario.com | 2021-11-22 | 00:00:03 | 1.1
www.elsaltodiario.com | 2021-11-22 | 00:02:37 | 1.0
www.elsaltodiario.com | 2021-11-22 | 00:02:54 | 1.0
www.elsaltodiario.com | 2021-11-22 | 12:45:09 | 1.0
www.elsaltodiario.com | 2021-11-22 | 12:46:17 | 1.0
www.lamarea.com | 2021-11-22 | 12:47:04 | 1.0
www.lamarea.com | 2021-11-22 | 12:47:32 | 1.0
www.lamarea.com | 2021-11-22 | 12:48:01 | 1.0
kiosco.lamarea.com | 2021-11-22 | 12:48:29 | 1.0
tienda.elsaltodiario.com | 2021-11-22 | 12:49:10 | 3.0
kiosko.lamarea.com | 2021-11-22 | 12:55:24 | 2.9
kiosko.lamarea.com | 2021-11-22 | 12:55:36 | 0.1
www.elsaltodiario.com | 2021-11-22 | 14:36:40 | 5.2
www.lamarea.com | 2021-11-22 | 14:48:18 | 5.0
www.lamarea.com | 2021-11-22 | 14:48:27 | 1.0
www.elsaltodiario.com | 2021-11-22 | 14:48:37 | 5.0
www.elsaltodiario.com | 2021-11-22 | 14:48:44 | 1.0
kiosco.lamarea.com | 2021-11-22 | 14:49:08 | 2.0
info.nodo50.org | 2021-11-22 | 14:49:28 | 5.1
www.elsaltodiario.com | 2021-11-22 | 16:50:09 | 6.0
kiosco.lamarea.com | 2021-11-22 | 17:50:44 | 5.0
tienda.elsaltodiario.com | 2021-11-22 | 18:48:26 | 4.0
kiosko.lamarea.com | 2021-11-22 | 18:49:03 | 4.0
www.lamarea.com | 2021-11-22 | 18:49:32 | 4.0
www.elsaltodiario.com | 2021-11-22 | 20:50:04 | 2.0
www.lamarea.com | 2021-11-22 | 20:50:46 | 2.0
www.elsaltodiario.com | 2021-11-22 | 20:51:08 | 2.0
tienda.elsaltodiario.com | 2021-11-22 | 20:51:09 | 2.0

L3 - Ataques (SYN-ACK)

A lo largo del lunes 22 de noviembre de 2021 los ataques alcanzaron su punto máximo a última hora de la noche,

alcanzando varios millones de conexiones por segundo en los servidores. Durante ese tiempo detectamos otro vector de ataque capa 3 (L3) conocido como amplificación SYN-ACK: el atacante envía paquetes SYN falsificados a servidores de terceros que devuelven tráfico SYN-ACK legítimo a nuestros servidores.

Los atacantes utilizan con frecuencia esta técnica para eludir las técnicas de mitigación especializadas que necesitan mantener el estado del 3WHS (TCP three-way handshake, o protocolo de establecimiento de la comunicación TCP) para verificar las conexiones legítimas. El ataque, cuando se diseña correctamente, puede proporcionar hasta un 770% de amplificación del tráfico cuando se inundan los reflectores con paquetes SYN de 40 bytes. Un buen artículo presentado en WOOT14 se puede encontrar aquí: https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf

Origen de los ataques

Botnets móviles Mas del 20% de las IP atacantes en el ataque L7 pertenecen al mayor proveedor 4G de India, Jio, lo que parece indicar que se trata de una botnet formada por teléfonos y dispositivos móviles que han sido comprometidos por la instalación de aplicaciones maliciosas. Este tipo de botnet es una novedad respecto a los anteriores ataques de 2013 y 2015.

Como ejemplo del tipo de aplicaciones maliciosas que se usan para construir estas botnets de móviles tenemos:

- Hola VPN, que recientemente ha sido retirada de las mas importantes tiendas de aplicaciones y de complementos de navegadores. http://adios-hola.org
- Aplicaciones falsas que simulan ser oficiales del proveedor indio Jio. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/malicious-android-apps-india-jio
- Con la progresiva expansión de las redes 5G este tipo de botnets tomarán mas protagonismo.

Stressers o booters De nuevo los stressers son una herramienta primordial en este tipo de ataques. Son servicios que ofrecen la realización pruebas de estrés a redes y servidores, ofreciendo al cliente un panel de control en el que elegir distintas “pruebas” y a que objetivo dirigirlas. La realidad es que se usan para realizar ataques DDoS a cambios de dinero, por un precio que es muy bajo en las versiones menos potentes de esos ataques.

Stressers VIP Los stressers hacen uso de redes de bots para realizar sus ataques. Pero una botnet que participa en muchos ataques es identificada, bloqueada y pierde efectividad (se quema rápidamente). Es por eso que los stressers reservan fragmentos de sus botnets, o botnets independientes, menos utilizadas para clientes especiales, que pagan mas o que son revendedores de sus servicios de ataque. Esos clientes tendrán acceso a un panel de control mas avanzado y se les garantizará mas posibilidades de éxito en sus ataques. En el otro lado, para las pruebas gratuitas que ofrecen en sus webs, se usarán las IP mas quemadas.

Fin de la primera parte del informe sobre el ataque DDoS de noviembre de 2021.