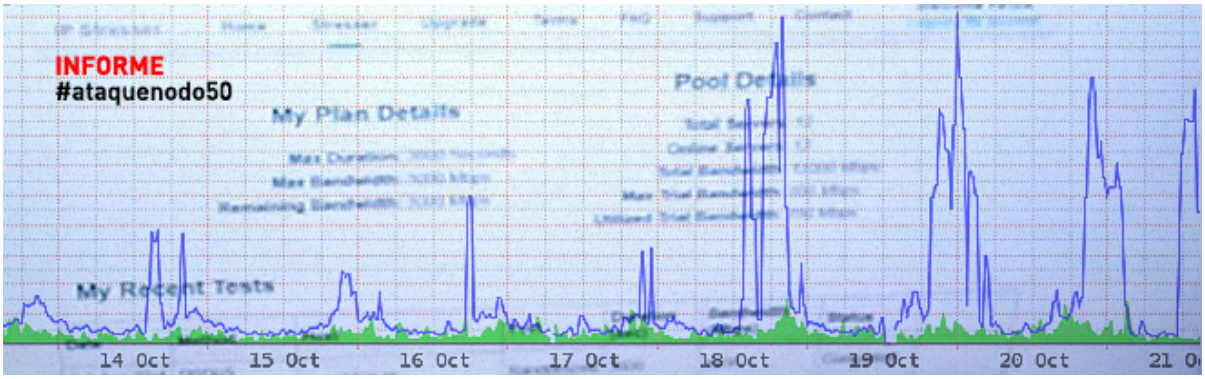
https://info.nodo50.org/ESPECIAL-Informe-sobre-los-ataques.html

Informe sobre los ataques de Octubre del 2013 contra Nodo50 y sus organizaciones alojadas

- Noticias - Noticias Destacadas -

Fecha de publicación en línea: Jueves 31 de octubre de 2013



Resumen

Durante octubre de 2013 se han producido una serie de ataques de denegación de servicio y reivindicaciones anónimas vía correo electrónico y twitter contra la organización Nodo50 (ORG-NA403-RIPE). El siguiente informe detalla la naturaleza del ataque y las identidades y organizaciones vinculadas al mismo.

La principal conclusión de este análisis forense es que el requisito más importante 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 (con remitente manipulado) dentro de su red. Hemos sido capaces de rastrear el tráfico de los ataques hasta el Amsterdam Internet Exchange (AMS-IX) 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 basándose en el uso de servidores o servicios alojados en Ecatel. Nuestro análisis apunta a que se ha descargado y empleado código disponible en el foro www.hackforums.net en servidores de Ecatel, en los Países Bajos, para la ejecución del ataque.

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 Torrevieja y que se hace conocer en los foros de juegos en red con más de media docena de nombres de usuario distintos.

El atacante, usando la identidad de D.V.G., pudo contratar los servicios del ataque a terceros, como www.ipstresser.com, escondido tras Cloudfare y que hace uso de los servidores de Ecatel para lanzar ataques de DDoS, a sabiendas de que ese proveedor de alojamiento era conocido por permitir la generación de tráfico con remitente falseado desde su red.

Análisis

Entre el 13 de octubre de 2013 a las 23:00 PM (CET) y el 24 de octubre de 2013 a las 2:00 AM (CET) una serie de ataques de denegación de servicio fueron lanzados contra la organización RIPE ORG-NA403-RIPE (Nodo50, Altavoz por la libertad de expresión y comunicación) con número AS197772. Durante los 12 días de ataque se identificaron las siguientes firmas del ataque.

Firma de ataque 1: Ataque de reflexión Chargen UDP

El atacante envió tráfico con remitente falso (spoofed) contra servidores públicos con el servicio “chargen UDP/19”. El remitente falsificado de los paquetes era la IP de la víctima, con lo que la respuesta de los servidores chargen llegaba al objetivo del ataque. Durante estos ataques observamos hasta 3 Gbps de este tipo de tráfico reflejado proveniente de 8000 servidores, lo que indica que el atacante solo necesitó generar menos de 200 Mbps de tráfico para el ataque.

La siguiente muestra del 13 de Octubre de 2013 contra la IP 91.226.117.72 muestra una respuesta UDP amplificada proveniente de 97.92.14.191, incluyendo tráfico fragmentado UDP.
20:33:32.445088 IP 97.92.14.191.19 > 91.226.177.72.50729: UDP, length 1164 20:33:33.658298 IP 97.92.14.191.19 > 91.226.177.72.29198: UDP, length 1941 20:33:34.174633 IP 97.92.14.191.19 > 91.226.177.72.5398: UDP, length 2291 20:33:34.628270 IP 97.92.14.191.19 > 91.226.177.72.64260: UDP, length 2620 20:33:34.628625 IP 97.92.14.191 > 91.226.177.72: udp 20:33:35.212909 IP 97.92.14.191.19 > 91.226.177.72.32164: UDP, length 3025 20:33:35.324992 IP 97.92.14.191.19 > 91.226.177.72.5325: UDP, length 3101 20:33:35.325767 IP 97.92.14.191.19 > 91.226.177.72.12758: UDP, length 3101 20:33:35.334463 IP 97.92.14.191.19 > 91.226.177.72.45524: UDP, length 3113 20:33:35.335225 IP 97.92.14.191 > 91.226.177.72: udp

Firma de ataque 2: ICMP inalcanzable (ICMP unreachable)

El 14 de octubre de 2013 las víctimas recibieron grandes cantidades de tráfico ICMP. Este tráfico fue generado por el mismo tipo de ataque de reflexión Chargen UDP, pero el tráfico ICMP aparece cuando los servidores públicos chargen que fueron usados en el ataque 1 ya no están disponibles.
00:09:54.264936 IP 210.96.179.168 > 91.226.177.72: ICMP 210.96.179.168 udp port 19 unreachable, length 40
00:09:54.264969 IP 94.77.195.131 > 91.226.177.72: ICMP 94.77.195.131 udp port 19 unreachable, length 40
00:09:54.265018 IP 203.156.244.2 > 91.226.177.72: ICMP 203.156.244.2 udp port 19 unreachable, length 40
00:09:54.265026 IP 203.156.244.2 > 91.226.177.72: ICMP 203.156.244.2 udp port 19 unreachable, length 40
00:09:54.265031 IP 211.170.1.178 > 91.226.177.72: ICMP host 210.216.253.95 unreachable, length 40
00:09:54.265037 IP 94.77.195.131 > 91.226.177.72: ICMP 94.77.195.131 udp port 19 unreachable, length 40
00:09:54.265153 IP 218.248.235.194 > 91.226.177.72: ICMP time exceeded in-transit, length 36 00:09:54.265162 IP 202.103.212.176 > 91.226.177.72: ICMP 202.103.212.176 udp port 19 unreachable, length 40 00:09:54.265166 IP 220.180.10.211 > 91.226.177.72: ICMP 220.180.10.211 udp port 19 unreachable, length 40 00:09:54.265225 IP 198.64.249.42 > 91.226.177.72: ICMP 198.64.249.42 udp port 19 unreachable, length 40 00:09:54.265231 IP 222.240.201.136 > 91.226.177.72: ICMP 222.240.201.136 udp port 19 unreachable, length 40

Firma de ataque 3: Ataque de reflexión DNS (DNS reflection attack)

El 14 de octubre de 2013, las víctimas recibieron una gran cantidad de tráfico UDP desde servidores DNS públicos. Para realizar este ataque se envían consultas DNS a servidores DNS abiertos poniendo como dirección IP de origen

de las consultas la IP de la víctima o víctimas. Para lograr la amplificación del tráfico, el atacante realiza una consulta DNS que implique una respuesta larga, de muchos bytes, que serán enviados a la víctima.

Una firma importante en este ataque fue la zona DNS utilizada. El dominio utilizado en las consultas DNS fue pkts.asia, un dominio registrado recientemente que contiene un fichero de zona muy grande. El dominio pkts.asia fue registrado el 1 de octubre de 2013 en el registrador de dominios Internet.bs, y sus dos servidores DNS, ns1.pkts.asia y ns2.pkts.asia están alojados en Ecatel. Los servidores de nombres del dominio se han movido de 69.42.219.74 to 89.248.168.94
00:10:01.155946 IP 178.248.70.26.53 > 91.226.177.72.58153: 53016 243/2/1 NS ns2.pkts.asia., NS ns1.pkts.asia., A 1.1.1.1, A 1.1.1.2, A 1.1.1.3, A 1.1.1.4, A 1.1.1.5, A 1.1.1.6, A 1.1.1.7, A 1.1.1.8, A 1.1.1.9, A 1.1.1.10, A 1.1.1.11, A 1.1.1.12, A 1.1.1.13, A 1.1.1.14, A 1.1.1.15, A 1.1.1.16, A 1.1.1.17, A 1.1.1.18, A 1.1.1.19, A 1.1.1.20, A 1.1.1.21, A 1.1.1.22, A 1.1.1.23, A 1.1.1.24, A 1.1.1.25, A 1.1.1.26, A 1.1.1.27, A 1.1.1.28, A 1.1.1.29, A 1.1.1.30, A 1.1.1.31, A 1.1.1.32, A 1.1.1.33, A 1.1.1.34, A 1.1.1.35, A 1.1.1.36, A 1.1.1.37, A 1.1.1.38, A 1.1.1.39, A 1.1.1.40, A 1.1.1.41, A 1.1.1.42, A 1.1.1.43, A 1.1.1.44, A 1.1.1.45, A 1.1.1.46, A 1.1.1.47, A 1.1.1.48, A 1.1.1.49, A 1.1.1.50, A 1.1.1.51, A 1.1.1.52, A 1.1.1.53, A 1.1.1.54, A 1.1.1.55, A 1.1.1.56, A 1.1.1.57, A 1.1.1.58, A 1.1.1.59, A 1.1.1.60, A 1.1.1.61, A 1.1.1.62, A 1.1.1.63, A 1.1.1.64, A 1.1.1.65, A 1.1.1.66, A 1.1.1.67, A 1.1.1.68, A 1.1.1.69, A 1.1.1.70, A 1.1.1.71, A 1.1.1.72, A 1.1.1.73, A 1.1.1.74, A 1.1.1.75, A 1.1.1.76, A 1.1.1.77, A 1.1.1.78, A 1.1.1.79, A 1.1.1.80, A 1.1.1.81, A 1.1.1.82, A 1.1.1.83, A 1.1.1.84, A 1.1.1.85, A 1.1.1.86, A 1.1.1.87, A 1.1.1.88,[|domain] 00:10:01.156024 IP 178.248.70.26 > 91.226.177.72: udp 00:10:01.156040 IP 178.248.70.26 > 91.226.177.72: udp

La zona DNS de este dominio, que contiene registros A de 1.1.1.1 a 1.1.1.241 es similar a la zona DNS de irlwinning.com que estaba alojada originalmente en 69.42.219.74. Ambos servidores DNS han sido denunciados por observatorios de ataques reflejos DNS como servidores maliciosos (http://d.hatena.ne.jp/ytakano/20131002/1380697169 y http://dnsamplificationattacks.blogspot.com.es/2013/10/domain-pktsasia.html).

El servidor DNS 69.42.219.74 alojado en Awknet Communications LLC todavía resuelve pkts.asia. Actualmente Ecatel aloja los servidores de nombres de pkts.asia.
[https://info.nodo50.org/local/cache-vignettes/L400xH201/buyddos_forum-58b23.jpg]

Imagen: En buyddos.com se explica cómo llevar a cabo un ataque de reflexión utilizando pkts.asia. Ref.: http://www.hackforums.net/showthread.php?tid=3823299

Basándonos en la firma del ataque pudimos encontrar un mensaje en www.hackforums.net (http://www.hackforums.net/showthread.php?tid=3819995) donde el usuario BitchGotRaped del sitio web www.buyddos.com ofrece el código fuente de un programa (en lenguaje C) e instrucciones detalladas sobre como lanzar un ataque de amplificación DNS usando pkts.asia y recomienda Ecatel como proveedor desde donde lanzarlo. El código fuente proporcionado en ese foro reutiliza código originalmente escrito por twbooter2, una plataforma que proporciona servicios para lanzar ataques DDoS.
[https://info.nodo50.org/local/cache-vignettes/L400xH101/buyddos_recomendando_ecatel-df83f.jpg]

Imagen: Mensaje en el foro recomendando Ecatel para los ataques

Firma de ataque 4: Inundación de paquetes SYN (SYN flooding)

Después de varios ataques de amplificación UDP que fueron mitigados con éxito, el atacante decidió lanzar una serie de ataques SYN flooding directamente contra los sitios web de las víctimas.

Se pudieron identificar dos firmas diferentes en estos ataques: SYN floodings usando el puerto 80 como origen y SYN floodings utilizando números de puertos aleatorios. En ambos casos usando una tamaño de venta fijo de 5840.
19:27:32.679974 IP 143.4.178.229.22589 > 91.226.177.73.22589: Flags [S], seq 0, win 5840, length 0
19:27:32.679982 IP 72.253.123.26.27933 > 91.226.177.73.27933: Flags [S], seq 0, win 5840, length 0
19:27:32.679989 IP 193.102.123.172.59724 > 91.226.177.73.59724: Flags [S], seq 0, win 5840, length 0
19:27:32.679996 IP 215.90.94.215.2147 > 91.226.177.73.2147: Flags [S], seq 0, win 5840, length 0
19:27:32.680003 IP 99.46.188.49.42933 > 91.226.177.73.42933: Flags [S], seq 0, win 5840, length 0
19:27:32.680011 IP 63.130.121.12.48104 > 91.226.177.73.48104: Flags [S], seq 0, win 5840, length 0
19:27:32.680018 IP 209.246.145.155.30543 > 91.226.177.73.30543: Flags [S], seq 0, win 5840, length 0
11:22:02.607843 IP 212.4.177.225.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0 11:22:02.607855 IP 80.140.239.234.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0 11:22:02.607873 IP 133.42.165.79.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0 11:22:02.607886 IP 4.139.187.48.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0 11:22:02.607901 IP 220.152.90.64.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0 11:22:02.607910 IP 8.61.254.31.80 > 91.226.177.73.80: Flags [S], seq 0, win 5840, length 0

Un análisis de los valores TTL del tráfico mostraba un valor fijo de 248, lo que indicaba la posibilidad de unos sola fuente/red de origen del ataque.
21:35:20.645556 IP (tos 0x0, ttl 248, id 12336, offset 0, flags [none], proto TCP (6), length 40

Verificando que Ecatel es el origen del tráfico

Como resultado de la forma en que el tráfico de datos en Internet es encaminado y de que un solo proveedor puede intercambiar tráfico por múltiples salidas, fue difícil rastrear el origen del ataque reflejo UDP/DNS y determinar donde fue generado el tráfico original. No fue hasta el 18 de octubre, cuando el atacante comenzó a lanzar frenéticamente SYN floodings contra la infraestructura de Nodo50 (AS197772), que pudimos relacionar los ataques con un único proveedor de origen.

Al correlacionar el tráfico entrante desde Ecatel en el AMS-IX (punto neutro de intercambio de tráfico entre proveedores en Amsterdam) y el tráfico que llegaba a las víctimas pudimos confirmar plenamente que Ecatel alojaba los puntos de origen del ataque.
[https://info.nodo50.org/local/cache-vignettes/L400xH368/trafico_ecatel-37aa9.jpg]

Imagen: Correlación entre el tráfico de AMS-IX hacia Ecatel y el tráfico entrante en el router central de AS197772

Se envió un mensaje a abuse@ecatel.info informando del problema. El 23 de octubre de 2013 se recibió como respuesta este breve mensaje:

> hello!
>
> problem should be solved by now.
> We are already receiving your routes from route-servers but prefer direct peering. Please let us know.
>
> thanks!!!
>
> Mykola Mitrokhin
> ECATEL LTD.

Traducción:

> ¡Hola!
> El problema ya debe estar resuelto.
> Nosotros ya estamos recibiendo sus rutas desde los servidores de rutado, pero preferimos el intercambio de tráfico directo. Por favor avísenos.
> ¡Gracias!
> Mykola Mitrokhin
> ECATEL LTD.

[https://info.nodo50.org/local/cache-vignettes/L260xH350/160mbps_syn_flooding-c5e2a.jpg]

Imagen: Gráfico de un SYN flooding de 160 Mbps

Mediante la observación de los ataques SYN flooding de 160 Mbps y la medición de sus cambios de rendimiento durante docenas de ataques, llegamos a la conclusión de que el ataque se estaba originando en no mas de 3 servidores alojados en Ecatel con 100 Mbps cada uno.
[https://info.nodo50.org/local/cache-vignettes/L400xH105/ofertas_ecatel-bea64.jpg]

Imagen: oferta de servidores en Ecatel

Ecatel no sólo ofrece servidores que pueden generar 100 Mbps de tráfico, sino también rutas para meter ese tráfico con origen falsificado en Internet, al precio de 62 €/mes.

Rastreando al atacante

Durante los 12 días de ataques, alguien utilizó la dirección de correo pandabear77@outlook.com para enviar una serie de mensajes a las organizaciones afectadas por los ataques. Utilizando los nombres de Twitter NacCiberCom7 y Nationalistnet7, esa persona se atribuyó la responsabilidad de los ataques. Durante la madrugada del 21 de octubre de 2013, el atacante anunció y realizó un grupo de ataques comentados en tiempo real en Twitter para probar su autoría. Envío sus mensajes al usuario @nodo50 e incluyó la etiqueta #ataquenodo50.

Durante los ataques del domingo 20 y lunes 21 de octubre de 2013, el autor publicó tres fotos personales en un perfil de Twitter.
[https://info.nodo50.org/local/cache-vignettes/L400xH378/conversacion_naccibercom7-2a214.jpg]

Imagen: Conversación via Twitter con atacante bajo idéntidad de @NacCiberCom7
[https://info.nodo50.org/local/cache-vignettes/L400xH300/carnets_dvg-bfffd.jpg]

Imagen: Imagen colgada por el perfil de twitter de @NacCiberCom7 para probar su autoría
[https://info.nodo50.org/local/cache-vignettes/L400xH378/perfil_naccibercom7-95aff.jpg]

Imagen: Imagen colgada por el perfil de twitter de @NacCiberCom7 para probar su autoría
[https://info.nodo50.org/local/cache-vignettes/L308xH400/perfil_nationalistnet7-0da7c.jpg]

Imagen: Perfil de Twitter @NetNationalism7 empleado por el atacante
[https://info.nodo50.org/local/cache-vignettes/L400xH267/pandabear-2705d.jpg]

Imagen: Imagen colgada por el atacante en el perfil de twitter de @NacCiberCom7 para probar su autoría.

Detención del atacante

El pasado 24 de octubre la policia detenía a D.V.G., trás la denuncia presentada por www.infolibre.es, por su relación con distintos ataques a medios de comunicación de izquierdas.

En el video de la operación policial contra PandaBear77, denominada "Bambu", se aprecia la herramienta que empleaba en ese momento el atacante, www.ipstresser.com, que coincide con la empleada en los ataques realizado a Nodo50 y sus proyectos alojados. También se aprecia parte del historial de ataques realizados (minuto 1:16 del video), los últimos parecen indicar que habría atacado antes de su detención a las asociaciones de periodistas que mostraron su solidaridad con quienes padecían DDoS y a la web www.psoe.es.
[https://info.nodo50.org/local/cache-vignettes/L400xH225/herramienta_ipstresser-5caf5.jpg]
https://info.nodo50.org/local/cache-vignettes/L400xH231/panda-23aba.png

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 Pais: Detenido por atacar a medios en Internet en nombre de un comando fascista