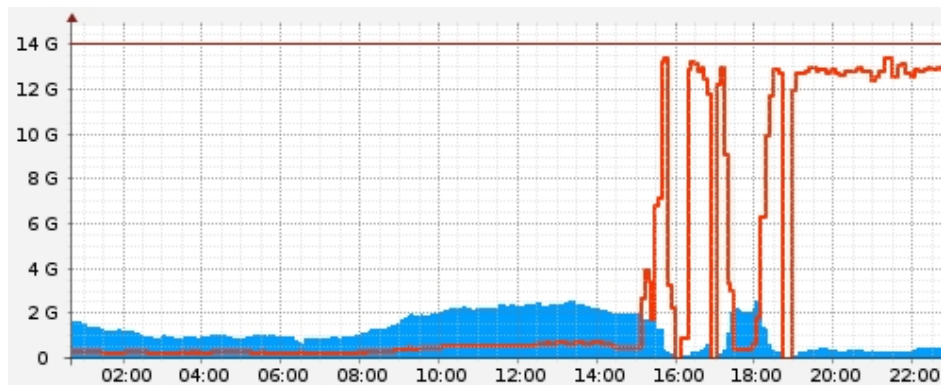


Un ataque masivo afecta a milleiros de usuarios e webs galegas.

Escrito por Redaccion @valminorinfo
Mércores, 24 Decembro 2014 18:54



Un ataque "masivo" DDoS aos servidores da empresa galega Dinahosting desde as 16 horas de onte afectou a milleiros de usuarios impedindo o acceso ás webs aloxadas nos servidores da empresa. A incidencia, coñecida como ataque "DDoS volumétrico", orixinouse pola chegada de decenas de peticións de gigabytes dende millóns de IPs distintas contra os servidores DNS da empresa ca fin de boicotear o acceso dos usuarios ás mesmas.

Os servizos lograron restablecerse definitivamente a primeira hora de esta mañá, tras unha esgotadora xornada de traballo segundo dá conta Dinahosting nun informe público na mañá de hoxe. Os motivos da agresión aínda se descoñecen máis a empresa sinala que baralla varias hipóteses e manterá "varias vías de acción que poñerá en coñecemento das autoridades competentes".

A gravidade do ataque quedou reflectida ao longo da xornada do martes cando centos de usuarios atoparon que era denegado o acceso ás súas webs. Inmediatamente a empresa respondeu ao ataque tentando filtrar as Ips atacantes, paralelamente ao soporte e atención aos seus clientes. Moitos deles propietarios de tendas virtuais que vían perder unha das xornadas máis importantes de vendas do ano. Portais como a do Instituto de Estudos Miñoranos, Praza Pública, Galicia Confidencial e outras de claro contido cultural ou informativo tamén sufriron as consecuencias do ataque aos servidores DNS.

"Para que vos fagades unha idea da magnitude do ataque. É tremendo: aproximadamente 30 veces o tráfico habitual" sinalaban sobre a pasada media noite dende Dinahosting. A empresa informaba ao seus clientes que a caída do servizo "está superando as nosas previsións", á vez que agradecía ás provedoras de conectividade e CPD pola súa colaboración no filtrado do "enorme volume de tráfico que estamos recibindo".

Un ataque masivo afecta a milleiros de usuarios e webs galegas.

Escrito por Redaccion @valminorinfo
Mércores, 24 Decembro 2014 18:54

Reporte das actuacións remitido por Dinahosting

23/12/2014 - 15:51

Os nosos sistemas de Monitorización detectan unha perda de conectividade que afecta a todos os segmentos de rede.

23/12/2014 - 16:00

O noso equipo técnico empeza a analizar a incidencia. Detectan que o problema é orixinado por un ataque que están recibindo os nosos DNS, tanto os que están na nosa rede, como externos internacionais.

23/12/2014 - 16:30

Vemos que o ataque é de tal magnitude que satura gran parte dos enlaces dos nosos carriers.

23/12/2014 - 16:45

Poñémonos inmediatamente en contacto con todos os nosos carriers para que nos dean información sobre o ataque, para intentar mitigarullo.

23/12/2014 - 17:15

O ataque cesa.

Un ataque masivo afecta a milleiros de usuarios e webs galegas.

Escrito por Redaccion @valminorinfo
Mércores, 24 Decembro 2014 18:54

23/12/2014 - 18:00

Detectamos que un novo ataque empeza a producirse con maior intensidade que o anterior.

23/12/2014 - 19:00

Intentamos configurar a Subred a donde está dirixido o ataque, para que o tráfico chegue filtrado ao noso sistema autónomo e deste xeito nosos enlaces non se vexan afectados.

23/12/2014 - 19:30

O noso equipo técnico do CPD ponse a traballar para aumentar en ancho de banda dos Sevidores DNS en 20 veces para soportar o ataque e redundar o tráfico.

23/12/2014 - 23:00

Solicitamos novamente a un dos nosos carriers que xestiona a maior parte do tráfico internacional o bloqueo do servizo DNS, coa intención de mitigar o ataque.

Seguimos traballando en redundar o tráfico dos nosos servidores e reforzar a medidas de filtrado do DNS

24/12/2014 - 1:20

Un ataque masivo afecta a milleiros de usuarios e webs galegas.

Escrito por Redaccion @valminorinfo
Mércores, 24 Decembro 2014 18:54

A maioría das provedoras nacionais de Internet xa se poden conectar correctamente aos servizos de Dinahosting (Movistar, Jazztel).

24/12/2014 - 6:00

Damos por controlado e estabilizado o ataque. O tráfico nacional esta case restablecido por completo.

24/12/2014 - 7:00

Solicitamos ao carrier que xestiona o tráfico internacional que permita o tráfico DNS.

Todos os servizos volven á normalidade.

Agradecementos

Trala a esgotadora xornada e cos servizos normalizados Dinahosting agradeceu aos usuarios pola súa “comprensión, paciencia e apoio nunhas circunstancias tan difíciles”, á colaboración das provedoras e partners e especialmente ao persoal da empresa “que de xeito voluntario e por iniciativa propia e sen excepción” acudiron a traballar na rehabilitación dos servizos.