

Incidencia de vulnerabilidad

Organizacion	BANVIVIENDA
Fecha	Abril 04, 2018
Seguridad nivel	Medium

Descripción

En nuestro sistema de monitoreo (GOC), hemos detectado lo siguiente:

La IP 172.16.230.66, tiene una actividad inusual y persistente a la DMZ-BANVIVIENDA, específicamente hacia las direcciones IPs 10.100.201.161, 10.100.201.129 y 10.100.201.169 al puerto 443/tcp.

Recomendamos verificar el equipo con esa IP y los intentos de accesos.

Adjuntamos imagen de lo mencionado.

Event
<163>1 2018-03-27T18:18:15-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39335 to DMZ-Banvivienda:10.100.201.161/443
<163>1 2018-03-27T18:18:15-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39334 to DMZ-Banvivienda:10.100.201.161/443
<163>1 2018-03-27T18:16:58-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39337 to DMZ-Banvivienda:10.100.201.129/443
<163>1 2018-03-27T18:16:57-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39336 to DMZ-Banvivienda:10.100.201.129/443
<163>1 2018-03-27T18:16:56-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39335 to DMZ-Banvivienda:10.100.201.129/443
<163>1 2018-03-27T18:16:55-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39334 to DMZ-Banvivienda:10.100.201.129/443
<163>1 2018-03-27T18:16:16-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39333 to DMZ-Banvivienda:10.100.201.169/443
<163>1 2018-03-27T18:16:16-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39332 to DMZ-Banvivienda:10.100.201.169/443
<163>1 2018-03-27T18:16:10-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39333 to DMZ-Banvivienda:10.100.201.161/443
<163>1 2018-03-27T18:16:10-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39333 to DMZ-Banvivienda:10.100.201.129/443
<163>1 2018-03-27T18:16:09-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 172.16.230.66/39332 to DMZ-Banvivienda:10.100.201.179/443

En GLESEC, nuestro GOC y nuestro equipo de Servicios Profesionales están dispuestos a apoyarlos, como siempre, en remediar estas situaciones. Por favor, no dude en contactarnos si este es el caso.

Saludos Cordiales y reiterándole siempre nuestra disposición en prestarle un servicio de alta calidad y acorde a sus expectativas, se despide;

GLESEC OPERATION CENTER – GOC.