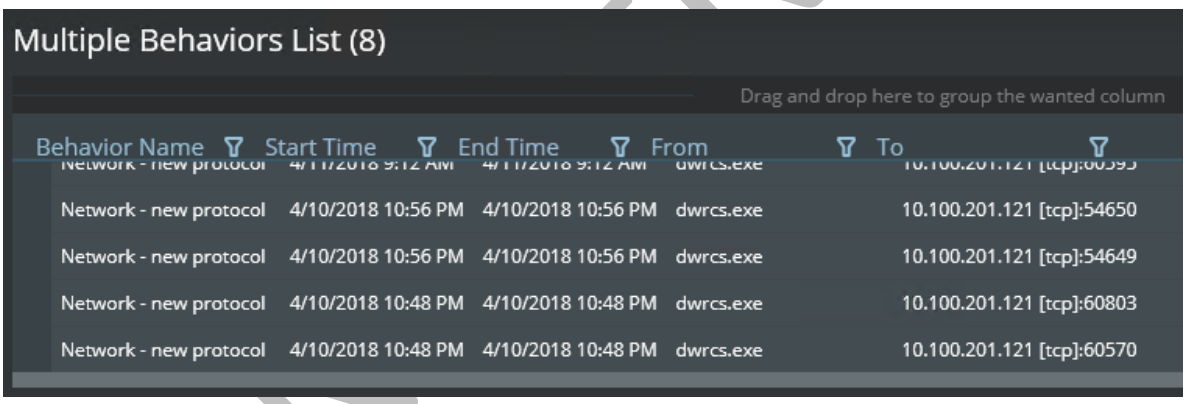
Incidencia de vulnerabilidad

Organizacion	BANVIVIENDA
Fecha	Abril 11, 2018
Seguridad nivel	Medium

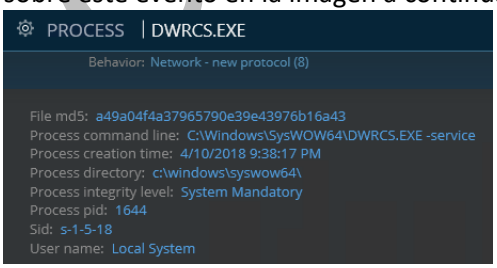
Descripción

En nuestro sistema de monitoreo (GOC) y usando el servicio MSS-EIR hemos detectado lo siguiente:

Desde un archivo que corresponde al agente de DameWare Mini Remote Client Agent, ubicado en dirección “C:\windows\SysWOW64\dwrcs.exe” se iniciaron conexiones de manera repetitiva a la dirección 10.100.201.121 en el equipo en donde está instalado el agente con identificador “bvpblwb2”, estas conexiones se realizaron fuera de horas laborales el día 4/10/2018, como se muestra en la imagen a continuación:



Es posible que esto forme parte de algún proceso normal y debidamente autorizado, sin embargo, de no ser así, se recomienda tomar las acciones necesarias para que esto no siga sucediendo.
Este agente es comúnmente utilizado para establecer conexiones remotas a dispositivos Windows, MAC OS X y Linux, es por este el nivel de severidad de este reporte de incidencia. Más información sobre este evento en la imagen a continuación:



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.