

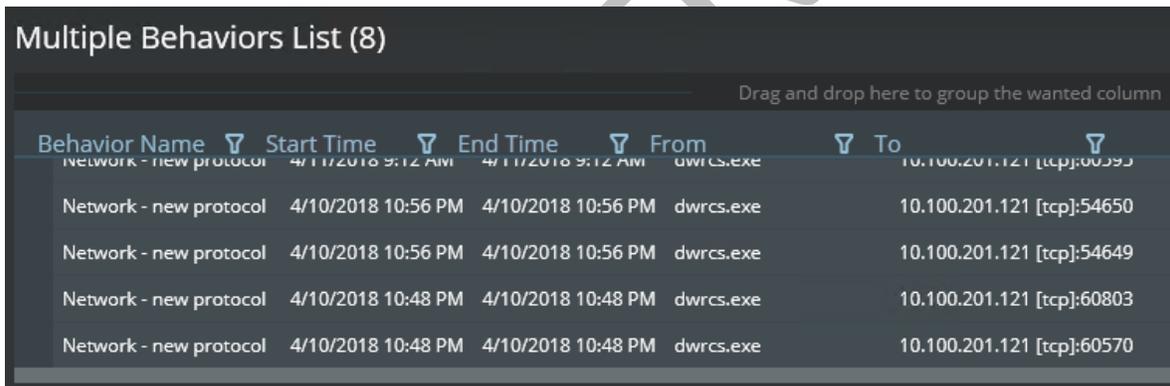
## Incidencia de vulnerabilidad

<b>Organizacion</b>	BANVIVIENDA
<b>Fecha</b>	Abril 11, 2018
<b>Seguridad nivel</b>	Medium

### Descripción

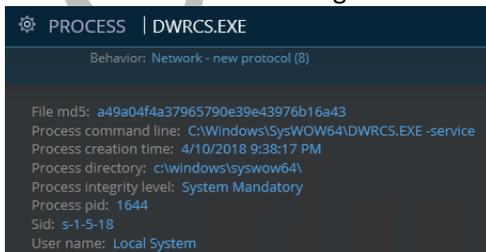
En nuestro sistema de monitoreo (GOC) y usando el servicio MSS-EIR hemos detectado lo siguiente:

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 "bvplwb2", estas conexiones se realizaron fuera de horas laborales el día 4/10/2018, como se muestra en la imagen a continuación:



Behavior Name	Start Time	End Time	From	To
Network - new protocol	4/11/2018 9:12 AM	4/11/2018 9:12 AM	dwrcs.exe	10.100.201.121 [tcp]:60593
Network - new protocol	4/10/2018 10:56 PM	4/10/2018 10:56 PM	dwrcs.exe	10.100.201.121 [tcp]:54650
Network - new protocol	4/10/2018 10:56 PM	4/10/2018 10:56 PM	dwrcs.exe	10.100.201.121 [tcp]:54649
Network - new protocol	4/10/2018 10:48 PM	4/10/2018 10:48 PM	dwrcs.exe	10.100.201.121 [tcp]:60803
Network - new protocol	4/10/2018 10:48 PM	4/10/2018 10:48 PM	dwrcs.exe	10.100.201.121 [tcp]:60570

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:



<b>PROCESS   DWRCs.EXE</b>
Behavior: Network - new protocol (8)
File md5: a49a04f4a37965790e39e43976b16a43
Process command line: C:\Windows\SysWOW64\DWRCs.EXE -service
Process creation time: 4/10/2018 9:38:17 PM
Process directory: c:\windows\syswow64\
Process integrity level: System Mandatory
Process pid: 1644
Sid: s-1-5-18
User name: Local System



CONFIDENTIAL

YOUR GLOBAL CYBER-SECURITY PARTNER

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.**

CONFIDENTIAL



USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR  
Tel: +1 (609)-651-4246 / +(507)-836-5355

