REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	10/09/2018
Servicio	MSS-EDR
Nivel de Severidad	Medio
Nivel de Impacto	Medio
Nivel de Vulnerabilidad	Medio

DESCRIPCION DE INCIDENTE

Nuestro servicio MSS-EDR (Endpoint Detection and Response) detectó que en el servidor BPVBLWB1, está instalado un software con nombre "dwrcs.exe" que fue ejecutado bajo el usuario "Bvpvblwb1\nt authority – system". Este software está ubicado en la siguiente ruta "c:\windows\syswow64\dwrcs.exe".

Según el hash calculado a partir de este ejecutable, este software se conoce también como DameWare Remote Access Software, un software de escritorio remoto.

COMENTARIOS Y RECOMENDACIONES

Favor confirmar si este software es parte de los programas permitidos en sus servidores.

Estamos a sus órdenes para apoyarlos con cualquier consulta.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTES DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimento con el protocolo de Semáforo (TLP) del Departamento de Seguridad de Estado de Estados Unidos (DHS): TLP -Blanco (Divulgación no limitada), TLP-Verde (Divulgación Limitada, Restringida, solo para la comunidad), TLP-Ámbar (Divulgación Limitada, Restringida, Para los participantes de la Organización) y TLP-Rojo (No Divulgación, Restringida/Confidencial – Solo compartida con el US DHS).

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