REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	11/09/2018
Servicio	MSS-EDR
Nivel de Severidad	Informativo
Nivel de Impacto	Informativo
Nivel de Vulnerabilidad	Informativo

DESCRIPCION DE INCIDENTE

Nuestro servicio MSS-EDR (Endpoint Detection and Response) detectó que en el servidor BPVEXCH01, se ejecutó un script, bajo el usuario *jorge.jarpa*, llamado "UACDisable.bat", cargado de un controlador de dominio.

La función de este script es modificar el registro de Windows, para deshabilitar el UAC (User Account Control). El UAC es una función de seguridad que solicita confirmación del usuario antes de realizar algún cambio en el sistema, esto es una medida preventiva para impedir cambios no autorizados en el sistema.

COMENTARIOS Y RECOMENDACIONES

Tenemos conocimiento que el usuario Jorge Jarpa es el encargado de hacer los cambios en los equipos para el Servicio de GLESEC MSS-EDR. Esta actividad se reporta con fines informativos.

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).