REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	BANVIVIENDA
Fecha	16/08/2018
Servicio	MSS-SIEM
Nivel de Severidad	Medium
Nivel de Impacto	Medium
Nivel de Vulnerabilidad	Medium

DESCRIPCION DE INCIDENTE

Nuestro centro de operaciones pudo detectar que el día 15 de agosto de 2018, a las 5:57 PM y nuevamente el 16 de agosto de 2018, a las 11:13 AM, se detectó un archivo malicioso en un dispositivo terminal de la red interna de su Organización, este fue encontrado en el endpoint con dirección IP local 172.16.230.216, en el cual se accedió a la dirección URL "http://update.cloudnetworktools.com/kits/autoupdate/1/SSE/pdfforgeExtension.exe", lo que descarga un archivo malicioso. Las direcciones IP públicas 52.85.107.220 y 13.32.81.224 fueron registradas como direcciones destino en cada uno de los eventos respectivamente; dicho archivo es catalogado como Malicioso o Inseguro por 24 casas de antivirus. También se muestra que el archivo no fue puesto en cuarentena, pero fue bloqueado por el dispositivo de seguridad de Fortinet, el cual lo reconoce como virus Malicious_Behavior.SB. El sha256 generado de este archivo malicioso es: 753cbae11a881b871e3295d65449954817061db5dec53df7b379fee9f21c33d1.

ACCIONES A TOMAR

Revisar este evento en el dispositivo terminal en el cual ocurrió para verificar que, efectivamente, el archivo ya no se encuentre en el endpoint; en el caso de encontrarlo, eliminar cualquier rastro de este archivo y/o archivos adicionales generados por el mismo.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

COMENTARIOS Y RECOMENDACIONES

No se puede determinar si este evento es o no un falso positivo desde el Centro de Operaciones debido al nivel de visibilidad que tenemos de los dispositivos que se encuentran en la red interna de su organización.

Se recomienda agregar el archivo con sha256: **753cbae11a881b871e3295d6544995481706 1db5dec53df7b379fee9f21c33d1,** MD5:**3b2e52bcee1538f26f2688ccf3eb5740** o sha1: **51838f4be589efc63eebb010103ea47ebdbd4be9** a la lista de archivos no permitidos/bloqueados/puestos en cuarentena en la configuración de antivirus o Endpoint protection system que se tenga para los dispositivos terminales. Además, la concientización de los usuarios sobre el impacto que puede provocar descargar archivos maliciosos de internet es muy importante ya que siempre es más beneficioso para la organización tomar acciones preventivas que tomar acciones de remediación.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

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