REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	BANVIVIENDA
Fecha	10/08/2018
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 9 de agosto de 2018, a las 2:56 PM se detectó un archivo malicioso en un dispositivo terminal de la red interna de su Organización, este está asociado a la dirección IP 172.16.207.138, en el cual se accedió a la dirección URL "http://post.securestudies.com/packages/IR/PackageI2.exe", el cual descarga un archivo malicioso. Este dominio resuelve a la dirección IP 165.193.78.234 y es catalogado como Malicioso o Inseguro por 44 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 Adware/Agent. El sha256 generado de este archivo malicioso es: ec11448a5d4d50c36f20d018059da6c2b1ba69cd5f633f29 5663ddb66063c13f.

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.

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

COMENTARIOS Y RECOMENDACIONES

Se recomienda agregar a una lista negra, la dirección pública **165.193.78.234** y/o el URL **"http://post.securestudies.com/packages/IR/PackageI2.exe"**. También, agregar el archivo con sha256:**ec11448a5d4d50c36f20d018059da6c2b1ba69cd5f633f295663ddb66063c13f** MD5:**6a3147ced47a6c7fd8cb4ae45843f420** y sha1: **06b54a7e5c1d4e7c0b4f50037c4c66cbf088aa3f** 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 este tipo de amenazas es muy importante ya que siempre es mejor prevenir cuando se trata de archivos maliciosos.

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).