BOLETÍN DE ALERTA

Boletín Nro.: 2017-11
Fecha de publicación: 27/07/2017
Tema: Solicitudes de auditoría de software a instituciones gubernamentales
Fecha de actualización: 27/09/2017

Actualización:

Recientemente fuimos contactados por representante de Autodesk, quienes acreditaron ser representante oficiales de dicha empresa. Los mismos nos explicaron que dicho requerimiento fue enviado de forma errónea a instituciones que no son clientes de Autodesk; la auditoría debería haber sido solicitado únicamente a aquellas instituciones clientes de Autodesk.
Las instituciones que son clientes de Autodesk, ya sea de forma directa o a través de un partner autorizado, volverán a recibirán una solicitud de auditoría de software por nota oficial de Autodesk, amparados en las cláusulas del contrato que dicha institución haya firmado con Autodesk Inc. Cualquier institución que haya adquirido alguno de los siguientes productos es considerado cliente de Autodesk, y por ende estará sujeto al cumplimiento del contrato:

- Autodesk Autocad
- Autodesk Autocad LT
- Autodesk Revit
- Autodesk Revit LT
- Autodesk 3ds Max
- Autodesk BIM
- Autodesk Fusion
- Autodesk ReCap
- Autodesk InfraWorks
- Autodesk Inventor
- Autodesk Maya

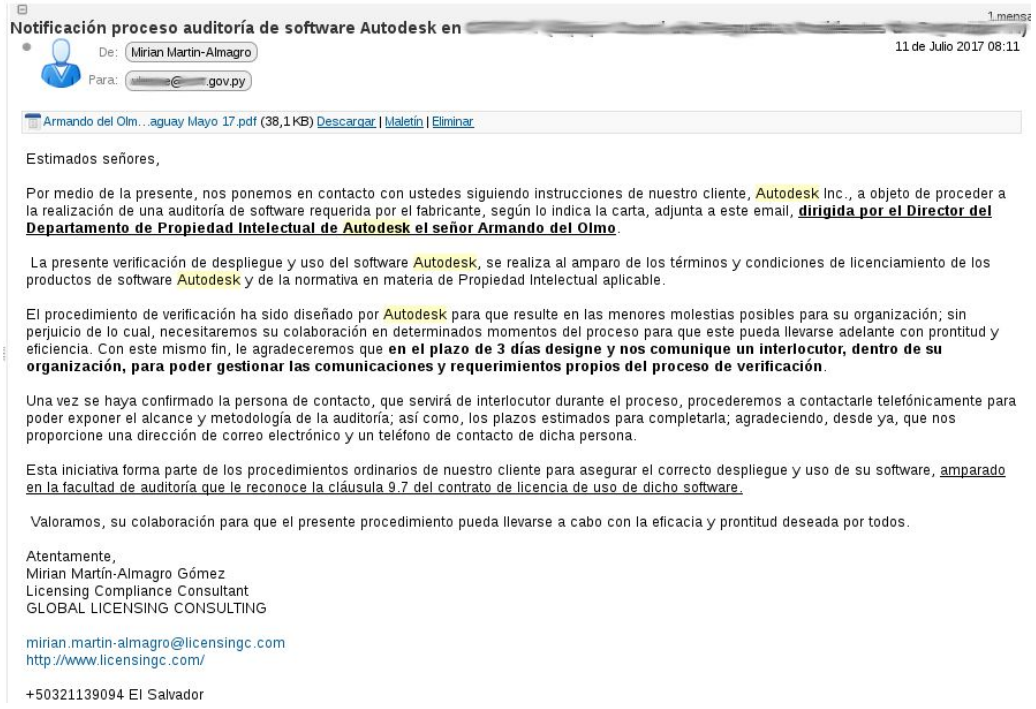
De acuerdo a lo manifestado por los representante de Autodesk, las solicitudes se realizarán de forma directa a través de Autodesk, y no a través de terceros.
Las instituciones que no son clientes de Autodesk no recibirán dicha solicitud de auditoría y no deberán realizar ninguna acción adicional, pudiendo desestimar las solicitudes previas que hayan recibido de manera errónea por correo electrónico.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Descripción:

Recientemente hemos recibido reportes de unos correos electrónicos que habían llegado a funcionarios de varias instituciones públicas, en los que se requería realizar una auditoría de software. Los correos electrónicos decían ser de empleados de una empresa GLOBAL LICENSING CONSULTING, un supuesto partner autorizado por la empresa Autodesk Inc., ésta última una empresa estadounidense real, dedicada al software de diseño en 2D y 3D, propietaria entre otros productos, del software AutoCAD.

En los correos, una persona que dice ser empleado de GLOBAL LICENSING CONSULTING solicita que la institución designe una persona de contacto para realizar una auditoría de software en nombre de Autodesk, amparados en una cláusula de un supuesto contrato de licencia de uso de software Autodesk.



Notificación proceso auditoría de software Autodesk en [redacted]

De: Mirian Martin-Almagro
Para: [redacted].gov.py

11 de Julio 2017 08:11

Armando del Olm...aguay Mayo 17.pdf (38,1 KB) Descargar | Maletín | Eliminar

Estimados señores,

Por medio de la presente, nos ponemos en contacto con ustedes siguiendo instrucciones de nuestro cliente, Autodesk Inc., a objeto de proceder a la realización de una auditoría de software requerida por el fabricante, según lo indica la carta, adjunta a este email, **dirigida por el Director del Departamento de Propiedad Intelectual de Autodesk el señor Armando del Olmo**.

La presente verificación de despliegue y uso del software Autodesk, se realiza al amparo de los términos y condiciones de licenciamiento de los productos de software Autodesk y de la normativa en materia de Propiedad Intelectual aplicable.

El procedimiento de verificación ha sido diseñado por Autodesk para que resulte en las menores molestias posibles para su organización; sin perjuicio de lo cual, necesitaremos su colaboración en determinados momentos del proceso para que este pueda llevarse adelante con prontitud y eficiencia. Con este mismo fin, le agradeceremos que **en el plazo de 3 días designe y nos comunique un interlocutor, dentro de su organización, para poder gestionar las comunicaciones y requerimientos propios del proceso de verificación**.

Una vez se haya confirmado la persona de contacto, que servirá de interlocutor durante el proceso, procederemos a contactarle telefónicamente para poder exponer el alcance y metodología de la auditoría; así como, los plazos estimados para completarla; agradeciendo, desde ya, que nos proporcione una dirección de correo electrónico y un teléfono de contacto de dicha persona.

Esta iniciativa forma parte de los procedimientos ordinarios de nuestro cliente para asegurar el correcto despliegue y uso de su software, amparado en la facultad de auditoría que le reconoce la cláusula 9.7 del contrato de licencia de uso de dicho software.

Valoramos, su colaboración para que el presente procedimiento pueda llevarse a cabo con la eficacia y prontitud deseada por todos.

Atentamente,
Mirian Martín-Almagro Gómez
Licensing Compliance Consultant
GLOBAL LICENSING CONSULTING

mirian.martin-almagro@licensingc.com
http://www.licensingc.com/

+50321139094 El Salvador

Figura 1: Correo electrónico de notificación de un supuesto proceso de auditoría de software

En los siguientes correos electrónicos, un supuesto empleado de GLOBAL LICENSING CONSULTING envía unos instructivos en formato pdf y un enlace a un subdominio de autodesk.com, desde el cual se descarga un archivo .zip, que contiene unos instructivos y un archivo ejecutable.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

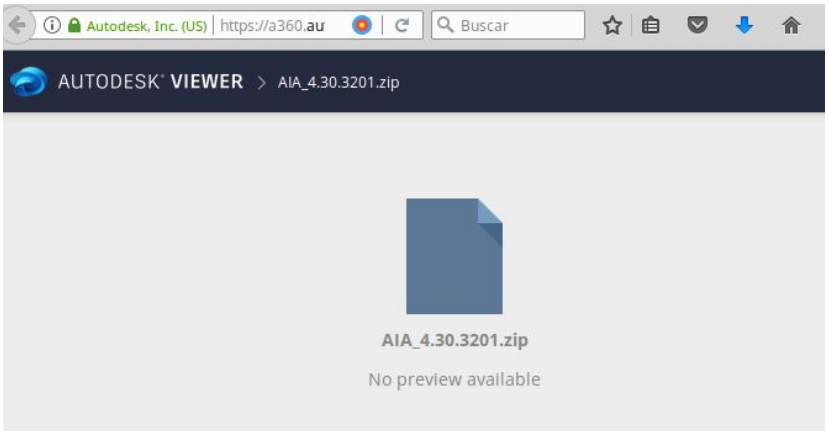


Figura 2: Enlace de descarga a un archivador zip

El análisis realizado por el CERT-PY de dichos archivos indica que, aparentemente, se trata de un software de auditoría legítimo de la empresa Autodesk, el cual, de por sí, no es malicioso. Igualmente, los instructivos en pdf aparentemente no ocultan ningún código malicioso.
Sin embargo, cabe resaltar que, al tratarse de un programa de auditoría de software, aunque fuera legítimo, el mismo, al ser ejecutado, escanea toda la red con privilegios de administrador y recoge una enorme cantidad de información sensible: nombres de equipos de la red, sistema operativo, listado completo de programas instalados con sus versiones, información de red, entre otras.

Figura 3: Ejecución del ejecutable que se encuentra en el archivador

El supuesto empleado de GLOBAL LICENSING CONSULTING exige que dicho programa sea ejecutado y que se le envíe los resultados de dicho escaneo. Como alternativa, menciona que es posible utilizar cualquier software de inventario, siempre y cuando se le brinde la siguiente información: nombre de los equipos, software de Autodesk instalado (producto, versión, edición, serial).

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

En algunos casos, un supuesto empleado de GLOBAL LICENSING CONSULTING incluso ha contactado telefónicamente a las instituciones, de modo a averiguar quién es la persona encargada de las licencias de software de la institución.

En la gran mayoría de los casos reportados, las instituciones que recibieron el requerimiento manifestaron que **no han firmado nunca ningún contrato ni acuerdo con Autodesk,** que no son clientes directos ni indirectos de Autodesk ni han adquirido nunca los productos de Autodesk, en ninguna de sus formas.

Desde el CERT-PY se ha contactado a Autodesk Inc., sin embargo, no se ha obtenido respuesta, por lo que no podemos afirmar ni descartar la legitimidad de GLOBAL LICENSING CONSULTING ni su relación con Autodesk. En este orden, el CERT-PY advierte sobre las imprecisiones que existen en estas comunicaciones, en las que no se ha podido comprobar la existencia efectiva de la empresa GLOBAL LICENSING CONSULTING, ni su vinculación con la empresa AUTODESK INC., y lo que es más importante, que la empresa no se encuentra radicada en Paraguay, ni cuenta con representante legal debidamente acreditado que realice estas intervenciones en nombre y por mandato de la empresa, todo lo cual resta legitimidad a la solicitud recibida y por ende, no impone ninguna obligación a que las personas que reciban esta comunicación, deban responder y/o dar cumplimiento a lo que se solicita.

La Dirección Nacional de Propiedad Intelectual (DINAPI), el ente rector en cuanto a propiedad intelectual y lucha contra la piratería, nos ha informado por su parte que no cuenta con ningún acuerdo ni está avalando ningún tipo de proceso de auditoría con la empresa Autodesk ni terceros.

En cualquiera de los casos, no existe obligación de obedecer a la solicitud de auditoría de software o de intercambio de información remitida por un remitente no acreditado por parte de la empresa licenciataria, así como que no se presenta por un representa legal debidamente acreditado, invocando derechos que legítimamente posea como Titular de las licencias del software objeto.

En caso de que una institución tuviera licencias adquiridas o algún contrato o acuerdo con Autodesk y/o un tercero y/o haya adquirido productos de Autodesk, deberá estarse a lo acordado, siendo no obstante necesario, para el cumplimiento de cualquier compromiso contractual, que las partes estén debidamente acreditadas y actúen en nombre propio, lo que en el presente caso no se da.

Impacto:

Al compartir los resultados de una auditoría de software con personas no autorizadas, las mismas tendrán acceso a información sensible sobre la red de la institución, entre ellas: nombres de equipos, sistemas operativos utilizados, programas o software instalados, versiones, información de red, entre otras. Esta información puede ser utilizada en un futuro con fines maliciosos, tales como un ataque dirigido mediante un exploit específico para un determinado software vulnerable.

Recomendaciones:

En caso de haber recibido una solicitud similar a la descrita, se recomienda no responder a las mismas. En caso de ser contactados telefónicamente, se recomienda no revelar información de ningún tipo. Se recomienda además no abrir, descargar ni ejecutar ningún archivo y/o programa que les sea enviado.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

En caso de haber ejecutado el programa de auditoría de software que fue indicado por la supuesta empresa GLOBAL LICENSING CONSULTING, recomendamos no enviar ni compartir los resultados de dicha ejecución. Adicionalmente, a pesar de que no tenemos evidencia de que se trate de un software malicioso (malware), recomendamos analizar su red con su antivirus u otra solución de seguridad, de modo a determinar el impacto que pudo ocasionar.

En caso de haber compartido dicha información, recomendamos contactar al CERT-PY, de modo a analizar las acciones correctivas a tomar.

En caso de que su institución haya firmado un contrato o acuerdo con la empresa Autodesk y/o con un asociado de la misma, recomendamos consultar con el área jurídica de su institución antes de acceder a la auditoría de software solicitada. En caso de duda, puede recurrir también a la DINAPI.

No obstante, una comunicación no identificada como del tipo que aquí hemos tratado, no sería adecuada para exigir el cumplimiento de compromisos contractuales asumidos, por no haberse acreditado suficientemente la calidad de Titular de las licencias respectivas y por ende, de los derechos respectivos.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py