Malware Calling

and how we call back

BotConf Nantes 2013

@maciekkotowicz

CERT POLSKA

$ w

Tomasz Bukowski + Maciej Kotowicz + Lukasz Siewierski

- IRT@CERT.pl since 2009
- botnet monitoring
- malware analyzis

- IRT@CERT.pl
- DragonSector CTF
- RE/Exploit dev
- Formal methods

- Security Projects Team at CERT Polska
- Windows/Android malware analysis
- Honeyspider

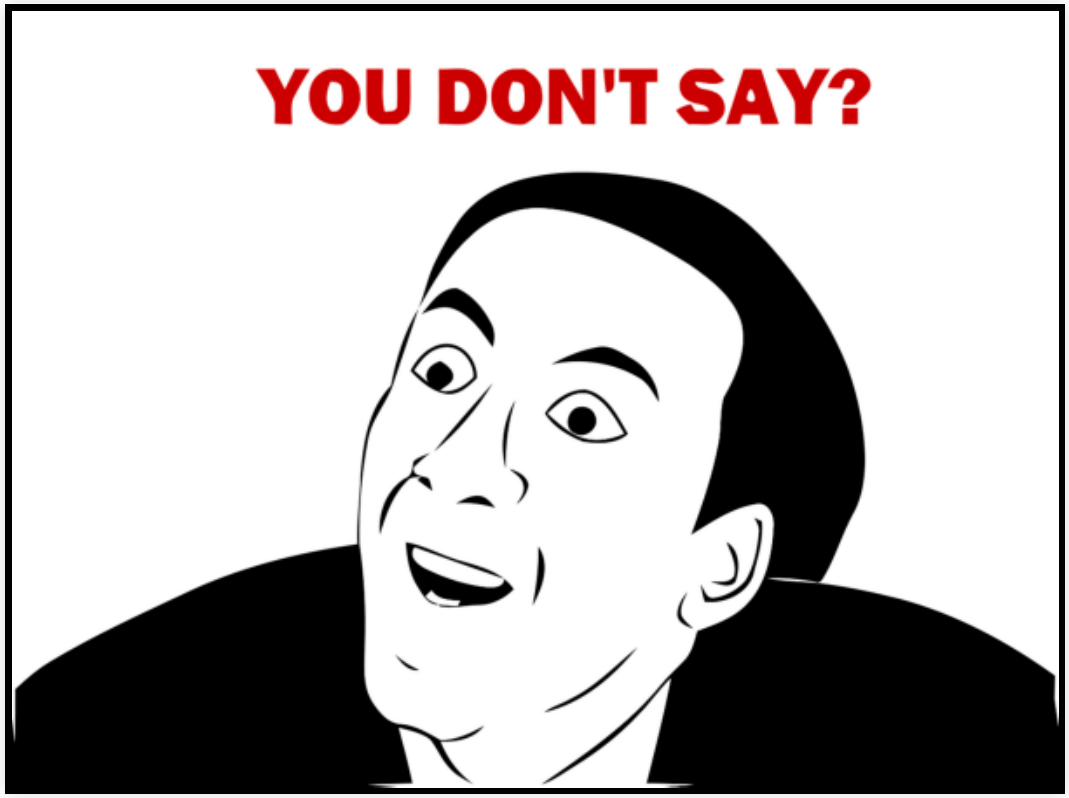
Intro

- Around 2011
- April 2013
- September 2013
- October 2013

PC-Malware

- Packed/Protected Manager
- RunTime DLLs
- Strange communication
- ZeuS as DLL...
- HTTPS

PowerZeus



PowerZeus

1. Alureon/PowerLoader (.exe)
    - x86/x64 in memory loading
    - RC4 everyware
    - 3 diffrent keys
    - 7 commands
2. Data Stealer (grabber.dll)
    - certs/cookies/email/password
3. ZeuS (bot{32/64}.dll)
    - SpyEye based modularization
    - ZeuS 2.0.8.9

```
[ DCT ]
mainver =15
[ modules ]
bot32 = qprtctolnnqqupg
bot64 = jfbmjigjwjiwppw
grabber = xbmxmnooivwfpgh
[ modconn ]
bot32 = none
bot64 = none
grabber = bot32
[ modparams ]
bot32 = empty
bot64 = empty
grabber = grab_ftps ; grab_certs ;
[ modrunm ]
bot32 =2
bot64 =2
grabber =0
[ modver ]
bot32 =6
bot64 =6
grabber =1
[ inject ]
*= bot32 ; bot64 ; grabber
```

PowerZeus - Tools

1. Loader
    - aluGetCfg.py
    - aluCommunicate.py
2. Zeus
    - getCfg.py

```
class WorkDbg(vtrace.Breakpoint):
    def notify(self,ev,tr):
        print '[*] Trying to find config data'
        esp = tr.getRegisterByName('esp')
        reta = unpack('I',tr.readMemory(esp,4))[0]
        print '[*] OpenProcess called from ' + hex(reta)
        for hit in tr.searchMemory("\x00\x00\x5b"):
            if hit >= reta-0x10000 and hit<= reta+0x10000:
                if tr.readMemory(hit+3,1) not in ['\x00','\x25']:
                    print self.decodecf(tr,hit+2)

    def decodecf(self,tr,addr):
        key,size = unpack('II',tr.readMemory(addr-12,8))
        mem = tr.readMemory(addr,size)
        print '[+] Found Config[0..%d] @ 0x%x with key: %X' % (size,addr,key
        return ''.join([chr(ord(mem[i]) ^ (key % (i+1))) for i in range(0,si


bp = WorkDbg(t.parseExpression('kernel32.OpenProcess'))
t.addBreakpoint(bp)
```

```
C:\Documents and Settings\[redacted]\Pulpit>C:\Python27\python.exe alu_getCf
ceadecac.exe
[*] Trying to find config data
[*] OpenProcess called from 0x4048aa
[+] Found Config[0..223] @ 0x40c00c with key: 8FF1B3BC
[DCT]
srvurls=https://myonlinevideo.ru/dropvideo/data.php;https://viewonlinevideo.
ropvideo/data.php;https://viewonlinevideo.ru/dropvideo2/data.php
srvdelay=3
srvretry=6
buildid=main
fpicptr=GetKeyboardLayoutList
```

```
if args.dll:

    pe = pefile.PE(args.dll)
    rc4_xor  = args.rc4_xor
    size_xor = args.len_xor

    for s in pe.sections:
        if s.Name.strip("\x00") == '.text':
            data = s.get_data()
            off1 = data.find("\x81\x34") # rc4key
            off2 = data.find("\x81\x75") # size-key
            if not rc4_xor:
                rc4_xor = struct.unpack('I',data[off1+3:off1+7])[0]
                print "rc4: XOR: 0x%x" % rc4_xor
            if not size_xor:
                size_xor = struct.unpack('I',data[off2+3:off2+7])[0]
                print "size XOR 0x%x" % size_xor
            sec = pe.sections[pe.FILE_HEADER.NumberOfSections-1]
            data =Stream(sec.get_data())
            rc4_key  = ''
            for i in range(0,256,4):
                rc4_key += struct.pack('I',data.int32() ^ tryhex(rc4_xor))
                with open('rc4.key','w') as f:
                    f.write(rc4_key)
            configSize = data.int32()  ^ tryhex(size_xor)
            dd = visDecry(rc4crypt(data.read(configSize),rc4_key))
            with open('config.dump','w') as f:
                f.write(dd)
            config = Stream(dd)
```

```
rc4: XOR: 0x5b9e07b9
size XOR 0x21fb3635
################################
ID: CFGID_URL_SERVER_0 FLAGS: ITEMF_IS_OPTION
 size: 0x00000031 realSize: 0x00000031
https://viewonlinevideo.ru/logsfilms/getadobe.php
--------------------------------
ID: CFGID_NOTIFY_SERVER FLAGS: ITEMF_IS_OPTION
 size: 0x00000033 realSize: 0x00000033
https://viewonlinevideo.ru/logsfilms/notifygate.php
--------------------------------
ID: CFGID_HTTP_FILTER FLAGS: ITEMF_IS_OPTION | ITEMF_COMPRESSED
 size: 0x000000ac realSize: 0x0000010b
@*bnpparibas.pl*
@*aliorbank.pl*
@*ebgz.pl*
@*centrum24.pl*
@*citibankonline.pl*
@*ebank.db-pbc.pl*
@*pocztowy24.pl*
@*ingbank.pl*
@*bankmillennium.pl*
@*mbank.pl*
@*polbank24.pl*
!https://*porno*
!https://*chat*
!https://*forum*
!https://*msn.*
!https://*facebook*
```

E-Security

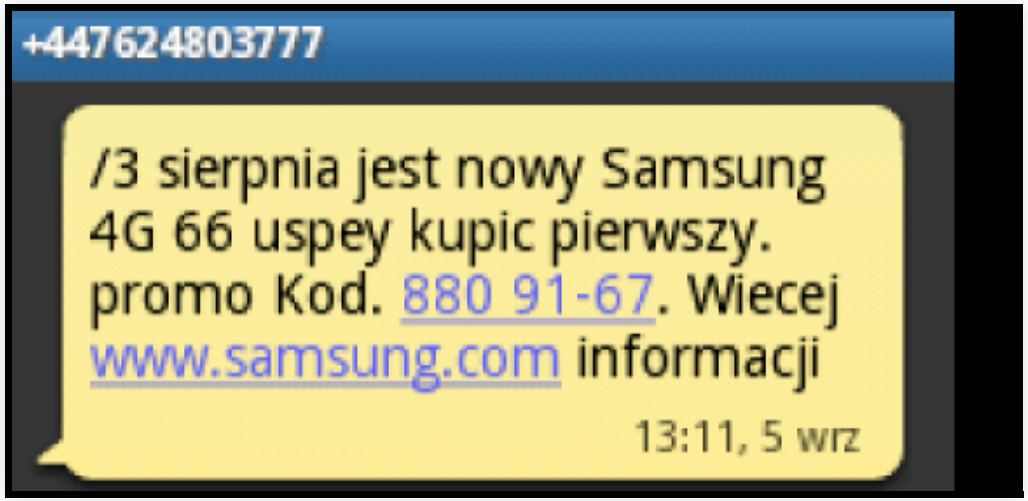
1. Mobile Malware
    - Android/BlackBerry/Symbian
2. Steales OTP password
    - and any other sms
3. 4 Commands
    - !
    - #
    - /
    - ,
4. Post-Own hosting

```
advernia.eu                                allegro.plocku.pl
blachymetalex.pl                           datajet.warszawa.pl
dlagolebia.pl                              edruk.net
emtom.linuxpl.info                         gimnazjumscinawa.pl
globalltd.pl                               grh7dak.linuxpl.info
megareklamy.pl                             multiline.com.pl
mm304.vot.pl                               moto.linuxpl.eu
myrta.art.pl                               nadobrejstronie.pl
number-one.xaa.pl                          plocku.pl
pparchetyp.pl                              prywatnestudium.pl
przewoz-niepelnosprawnych.com.pl           rowneszansescinawa.pl
roletykutno.pl                             rozoweokulary.edu.pl
rozoweok.linuxpl.info                      taramka.pl
smarttank.org                              w.plocku.pl
telemar.linuxpl.info                       www.zks.nq.pl
wmd6.linuxpl.info
```

```
403952.apk 448300.apk 980312.apk a{\d+}-signed.apk app.apk e-sec.apk
e-security.apk index.apk install.apk polska.apk poland.apk
```

```php
<?php
//$name = "polska_".rand(1 ,10000);
$name = "polska";
$file_ending = "apk";
//header("Content -type: application/octet -stream");
header("Content -type: application/vnd.android.package -archive") ;
header("Content -Disposition: attachment; filename={$name}.{$file_ending}");
header("Pragma: no-cache") ;
header("Expires: 0");
$myFile = "logo.jpg";
$handle = fopen($myFile , 'r');
while (!feof($handle))
{
  $data = fgets($handle , 512) ;
  echo $data;
}
fclose($handle);
$r=rand(1 ,1024) ;
for($i=0;$i<$r;$i++)
  echo rand() ;
?>
```

E-Security - redirection



E-Security - redirection

```
public String ExtractNumberFromMessage(String paramString)
  {
    String str = "+";
    Matcher localMatcher = Pattern.compile("\\d+").matcher(paramString);
    for (int i = 0; ; i = 1)
    {
      if (!localMatcher.find())
      {
        if (i == 0)
          str = "";
        return str;
      }
      str = str + localMatcher.group();
    }
  }
```

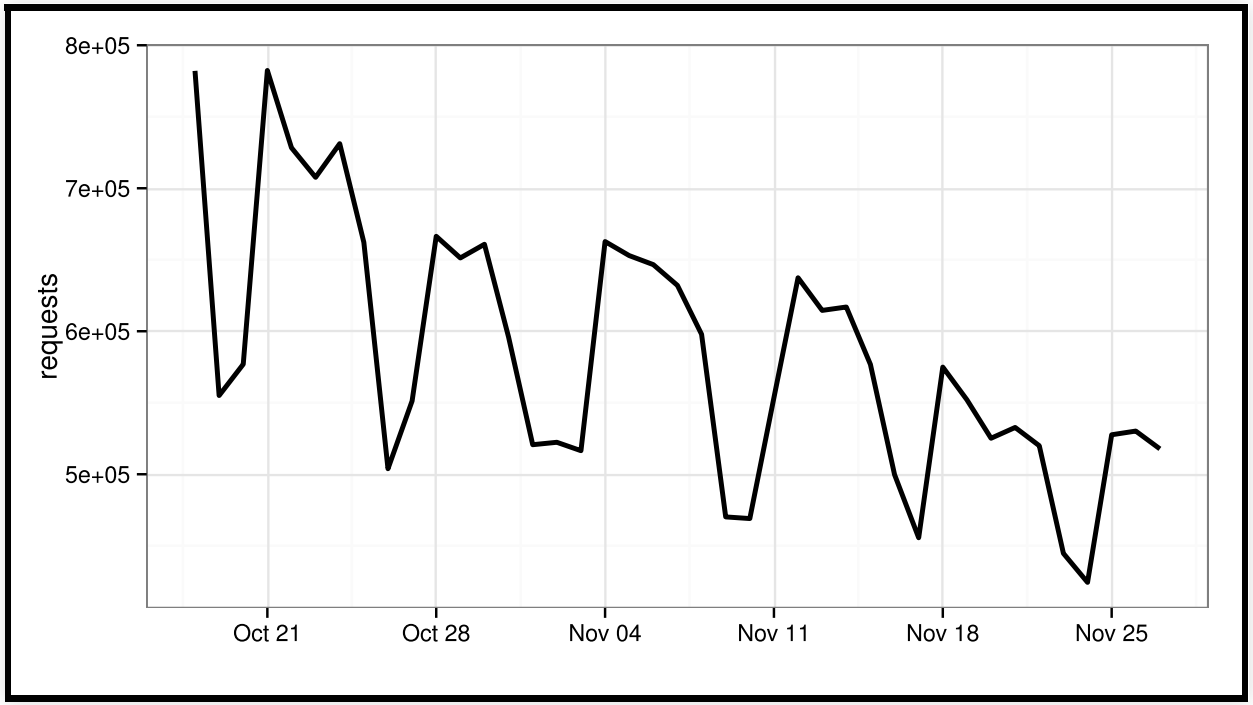
FonYou.com

```
fonYou has developed a proprietary technology platform, the OMT-9000,
which is connected to the mobile operators' existing core networks
and enables them to offer Cloud Telephony Services to their end customers.
These services put the end customers in total control of their mobile
phone service as they allow them to configure advanced control settings
for blocking, filtering or redirecting traffic; set up different voicemail
greetings per contact or  contact group; and access a complete
history of their call records, SMS and voicemails from anywhere and in
real-time.
```

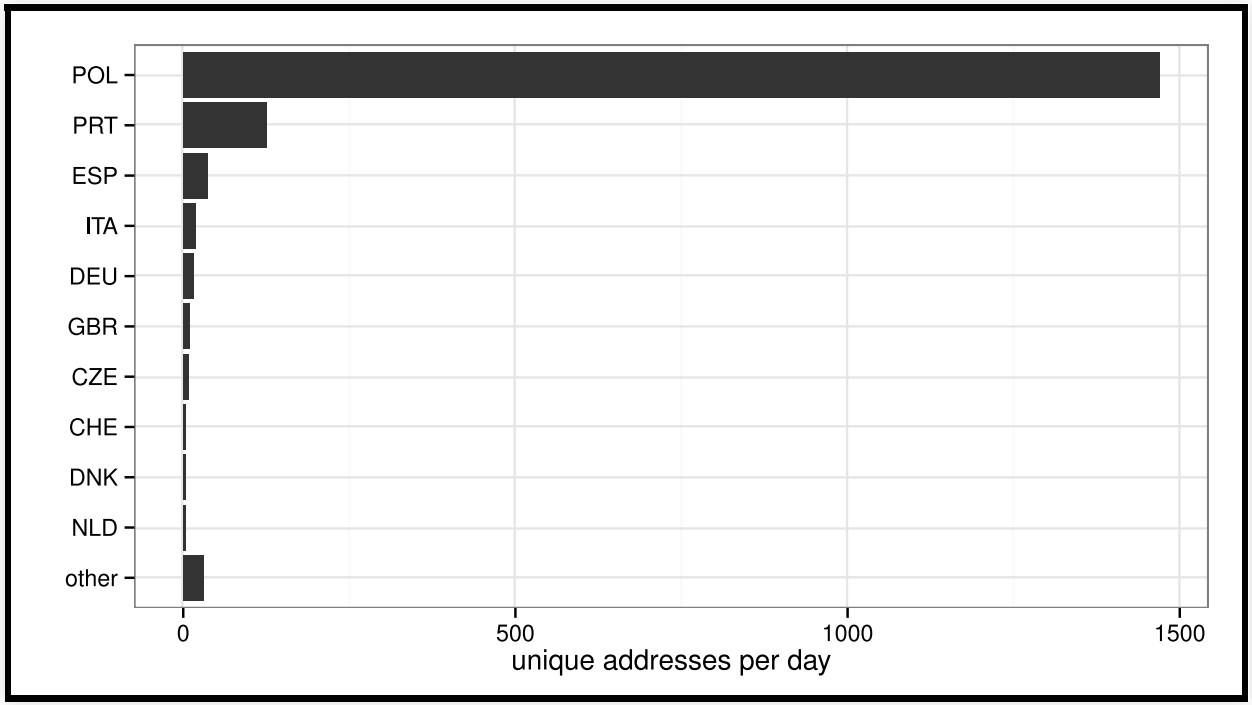
FonYou.com

1. Redirects
    - +34 668 830 ***
    - +34 668 809 ***
2. Commands
    - +44 762 480 *7 *7 - kown malicius number

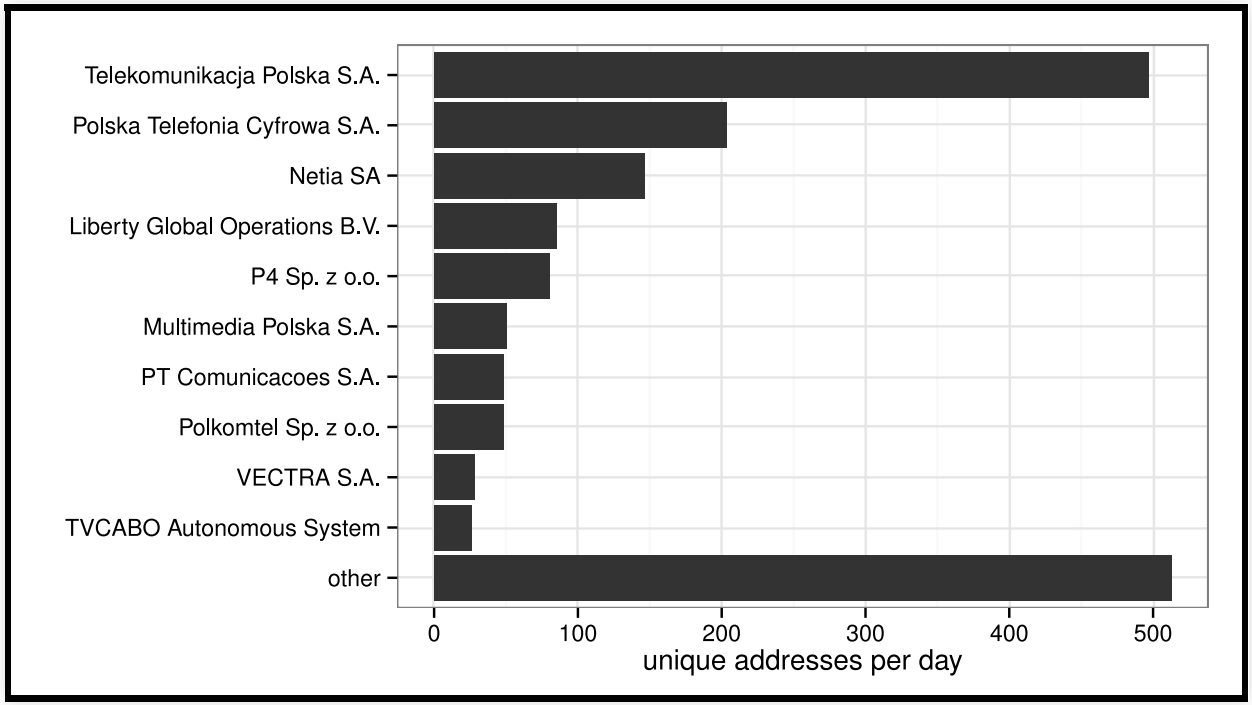
Sinkhole stats



Sinkhole stats



Sinkhole stats



Q & A

@maciekkotowicz
lokalhost.pl/talks/botconf2013 CERT Polska
@CERT_Polska_en