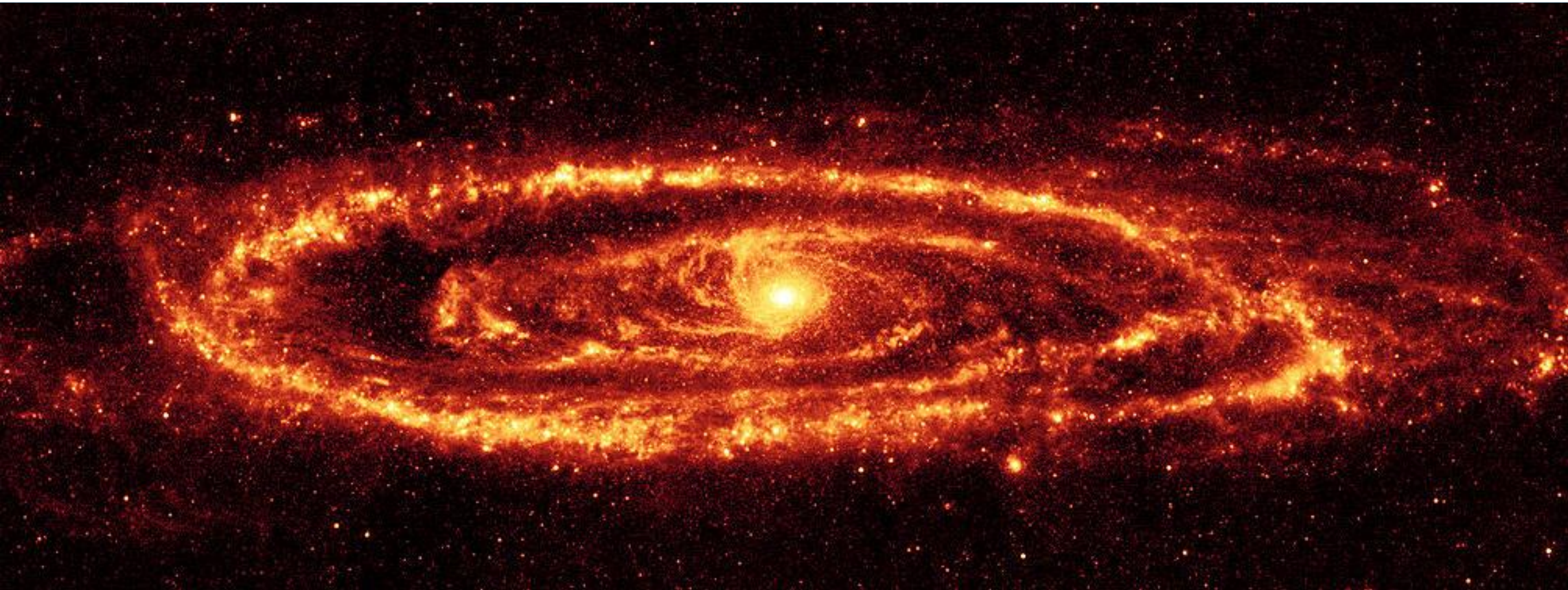
Travelling to the far side of Andromeda

Jose Miguel Esparza



$ whoami

- Jose Miguel Esparza
- Lead Threat Analyst at Fox-IT InTELL (NL)
  - Malware, Botnets, C&Cs, Exploit Kits, …
- Security Researcher at home ;)
  - peepdf, NFC, malware (again)
- http://eternal-todo.com
- @EternalTodo on Twitter

InTELL
BY FOX IT

Agenda

- Introduction
- Evolution of Andromeda
- The Dark Side of Andromeda
- Statistics
- Interesting use cases
- Conclusions

Introduction

- Developed during 2011 (probably 2010 too)
- First advertised in July 2011
- Modular and versatile bot
- Pings C&C periodically asking for “tasks”
  - Executes additional malware (and updates)
  - Executes plugins
  - Capability to send tasks to specific countries/bots/build_ids
- Spread via spam campaigns, loaders and Exploit Kits
- Current version: 2.10

Evolution of Andromeda

- Binary
- Plugins
- Panel

Evolution of Andromeda

- Binary
  - Request parameters
  - Response encryption
  - Plugins decryption
  - Anti-analysis (and bypass!)

Evolution of Andromeda

- Binary
  - References
    - http://eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis
    - http://eternal-todo.com/blog/andromeda-gamarue-loves-json
    - http://blog.fortinet.com/post/andromeda-2-7-features
    - http://blog.fortinet.com/post/new-anti-analysis-tricks-in-andromeda-2-08
    - http://stopmalvertising.com/spam-scams/cve-2013-2729-and-andromeda-2.9-a-massive-hsbc-themed-email-campaign/andromeda-botnet.html

Evolution of Andromeda

- Binary
  - Request parameters
    - **<= 2.06**
      - **id:%lu|bid:%lu|bv:%lu|sv:%lu|pa:%lu|la:%lu|ar:%lu**
    - **2.07/2.08**
      - **id:%lu|bid:%lu|bv:%lu|os:%lu|la:%lu|rg:%lu**
    - **2.09**
      - **id:%lu|bid:%lu|os:%lu|la:%lu|rg:%lu**
    - **2.10**
      - **{"id":%lu, "bid":%lu, "os":%lu, "la":%lu, "rg":%lu}**
      - **{"id":%lu, "bid":%lu, "os":%lu, "la":%lu, "rg":%lu, "bb":%lu}**

Evolution of Andromeda

```
80   bb_flag = 0;
81   v6 = GetKeyboardLayoutList(0, 0);
82   v21 = v6;
83   if ( v6 )
84   {
85     v7 = sub_7FF92329(4 * v6 + 4);
86     v8 = v7;
87     if ( v7 )
88     {
89       GetKeyboardLayoutList(v21, (HKL *)v7);
90       for ( i = (_DWORD *)v8; *i; ++i )
91       {
92         v10 = *i & 0xFFFF;
93         if ( v10 == 1049 || v10 == 1058 || v10 == 1059 || v10 == 1087 )// Russian | Ukrainian | Belarusian | Kazakh
94           bb_flag = 1;
95       }
96       sub_7FF92358(v8);
97     }
98   }
99   sub_7FF94280();
100  sub_7FF94745();
101  return 1;
102 }
```

InTELL
BY FOX IT

Evolution of Andromeda

- Binary
  - Anti-analysis
    - Previous versions
      - BP detection
      - Custom exception handler
      - Comodo / Sandboxie
      - Process blacklist (custom hash)
      - VM detections
      - Time check (RDTSC)

```
push    [ebp+var_178]
call    [ebp+var_34]
cmp     [ebp+var_184], 'awmw'
jz      short loc_A1746
cmp     [ebp+var_184], 'xobv'
jz      short loc_A1746
cmp     [ebp+var_184], 'umeq'
jz      short $+2
```

InTELL BY FOX IT

Evolution of Andromeda

- Binary
  - Anti-analysis
    - Newer versions
      - Just blacklisted processes (CRC32)

Evolution of Andromeda

```
32 44 DD 99

B4 9D 85 2D
CE 0D 34 64
74 44 C5 63
8B 9C 9C 34
CE EB 46 34
FE B1 A9 5B
F3 BE E2 3C
2B F0 46 3D
F7 10 AE 77
5D E9 44 F3
6F 6D BE 2D
44 02 D1 A3
91 ED 72 1D
BE 6B 93 96
58 DF 8C 27
85 F8 FF 3B
D9 23 33 6D
C4 C6 EF D2
D2 AC 1B DE
D4 F7 44 30
00
00
00
00
```

```
hash_blacklist  dd 99DD4432h            ; DATA XREF: AntiAnalysis+C8↓r
                                        ; AntiAnalysis+DD↓r
                                        ; vmwareuser.exe
                dd 2D859DB4h            ; vmwareservice.exe
                dd 64340DCEh            ; vboxservice.exe
                dd 63C54474h            ; vboxtray.exe
                dd 349C9C8Bh            ; sandboxiedcomlaunch.exe
                dd 3446EBCEh            ; sandboxierpcss.exe
                dd 5BA9B1FEh            ; procmon.exe
                dd 3CE2BEF3h            ; regmon.exe
                dd 3D46F02Bh            ; filemon.exe
                dd 77AE10F7h            ; wireshark.exe
                dd 0F344E95Dh           ; netmon.exe
                dd 2DBE6D6Fh            ; prl_tools_service.exe (Parallels)
                dd 0A3D10244h           ; prl_tools.exe (Parallels)
                dd 1D72ED91h            ; prl_cc.exe (Parallels)
                dd 96936BBEh            ; sharedintapp.exe (Parallels)
                dd 278CDF58h            ; vmtoolsd.exe
                dd 3BFFF885h            ; vmsrvc.exe
                dd 6D3323D9h            ; vmusrvc.exe
                dd 0D2EFC6C4h           ; python.exe (New!)
                dd 0DE1BACD2h           ; perl.exe (New!)
                dd 3044F7D4h            ; New
                db    0
                db    0
                db    0
                db    0
```

Version 2.06

Added in 2.07

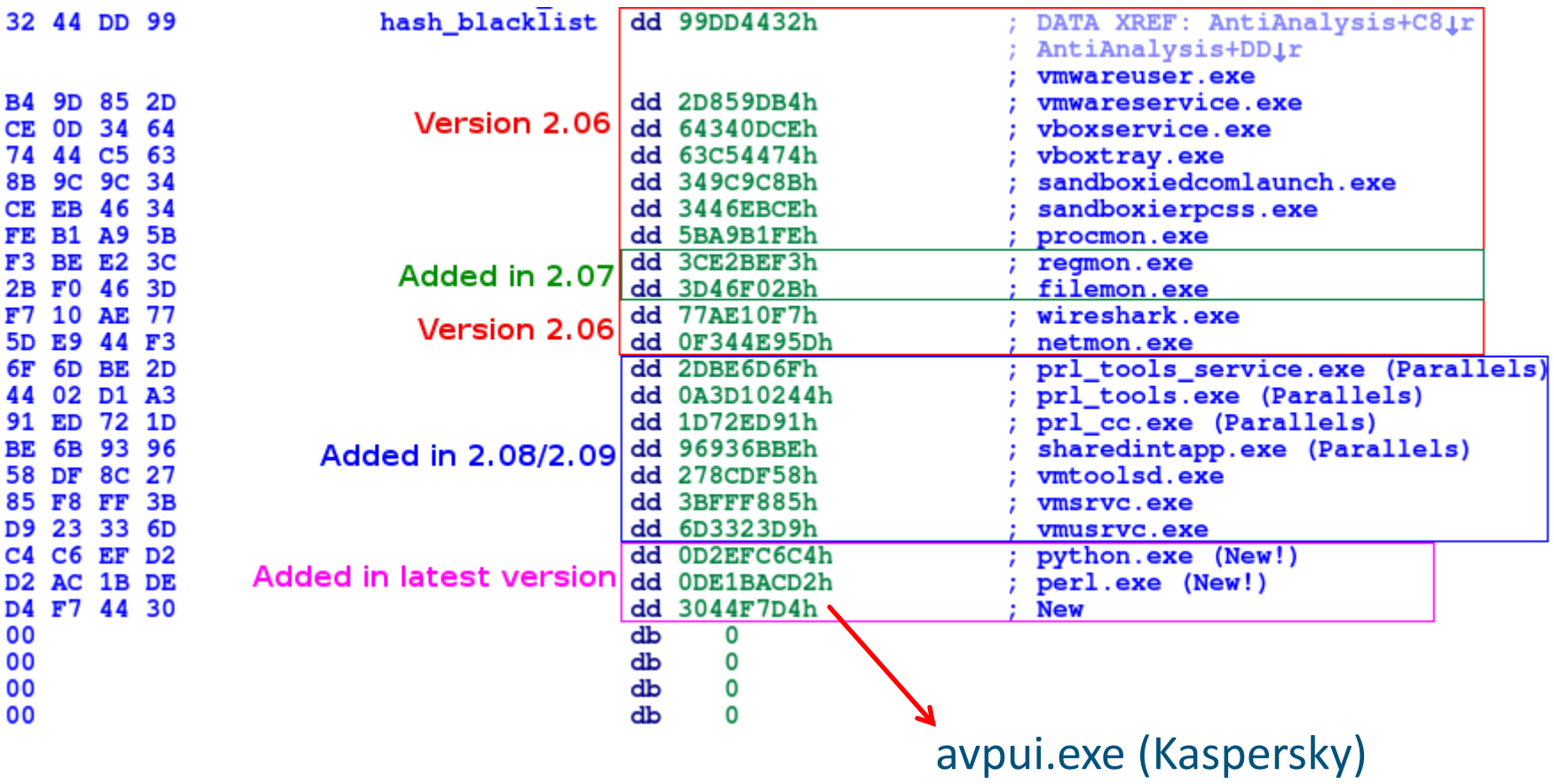
Version 2.06

Added in 2.08/2.09

Added in latest version

InTELL
BY FOX IT

Evolution of Andromeda



InTELL
BY FOX IT

Evolution of Andromeda

- Binary
  - Bypassing anti-analysis
    - Hardcoded system drive volume hash (previous versions)
      - **0x20C7DD84 (CKF81X)**
    - Special registry key (current version)
      - *HKEY_LOCAL_MACHINE\SOFTWARE\Policies*
        - ***is_not_vm =botid***

Evolution of Andromeda

- Binary
  - They want to fool you
    - Fake payload (old versions)
    - Fake URL
    - Overwritten code
    - RC4 algorithm modified
    - Fake RC4 key

Evolution of Andromeda

- Binary
  - They want to fool you
    - Fake payload (old versions)
      - Cmd.exe in port 8000

Evolution of Andromeda

```
j_seg004_ws2_32_WSAStartup(257, &unk_200002C4);
v11 = 2;
v12 = j_seg004_ws2_32_htons(8000);
v13 = 0;
v14 = j_seg004_ws2_32_WSASocketA(2, 1, 6, 0, 0, 0);
if ( v14 != -1 && j_seg004_ws2_32_bind(v14, &v11, 16) != -1 && j_seg004_ws2_32_listen(v14, 5) != -1 )
{
  while ( 1 )
  {
    memset(&v5, 0, 0x44u);
    v2 = j_seg004_ws2_32_accept(v14, 0, 0);
    v5 = 68;
    v8 = v2;
    v9 = v2;
    v10 = v2;
    v7 = 0;
    v6 = 257;
    j_seg004_kernel32_CreateProcessA(0, "cmd.exe", 0, 0, 1, 0, 0, 0, &v5, &v4);
  }
 }
}
return j_seg004_kernel32_ExitProcess(0);
```

InTELL
BY FOX IT

Evolution of Andromeda

- Binary
  - They want to fool you
    - Fake URLs
      - thisshitismoresafethanpentagonfuckyoufedsbecausethisisaf.com/image.php (2.06)
      - http://www.chudakov.net/goto.php?num=146897 (2.07)
      - http://s28.postimg.org/wmsgw5s23/image.jpg (2.08)
      - http://img4.joyreactor.cc/pics/post/... (2.08)

Evolution of Andromeda

- Binary
  - They want to fool you
    - Code to decrypt URLs removed (since 2.07)

Evolution of Andromeda

```
RemoveCode      proc near               ; CODE XREF: sub_7FF91A2C+1D9↓p
                                        ; DATA XREF: RemoveCode+24↓w
                push    ebp
                mov     ebp, esp
                push    esi
                push    edi
                lea     edi, CreateKeyDecryptURLs
                lea     esi, sub_7FF93093
                mov     ecx, 7FF910F6h
                sub     ecx, edi
                rep movsb
                mov     dword ptr ds:CreateKeyDecryptURLs, 0CC0004C2h
                mov     dword ptr ds:RemoveCode, 0CC0004C2h
                pop     edi
                pop     esi
                pop     ebp
                retn    4
RemoveCode      endp
```

InTELL
BY FOX IT

Evolution of Andromeda

- Binary
  - They want to fool you
    - RC4 algorithm modified (2.07/2.08)
      - Replacing 1 byte (add/sub)
      - Craziness trying to decrypt

Evolution of Andromeda

```
loc_30001031:                                   ; CODE
                                                ; Decr
                lea     eax, RC4_Substraction
                mov     byte ptr [eax], 2
                lea     esi, unk_300007BD
                lea     edi, loc_30000FE1
                mov     ecx, 6Ah
                rep movsb
                pop     ebx
                pop     edi
                pop     esi
                leave
                retn    4
DecryptURLs     endp
```

InTELL
BY FOX IT

Evolution of Andromeda

```
                                RC4_Loop:                                       ; CODE XR
36 8A 94 29 00 FF FF FF                         mov     dl, ss:[ecx+ebp+var_100]
02 C2                                           add     al, dl

                                RC4_Substraction:                               ; DATA XR
2A 04 33                                        sub     al, [ebx+esi]
36 8A B4 28 00 FF FF FF                         mov     dh, ss:[eax+ebp+var_100]
36 88 B4 29 00 FF FF FF                         mov     ss:[ecx+ebp+var_100], dh
36 88 94 28 00 FF FF FF                         mov     ss:[eax+ebp+var_100], dl
FE C1                                           inc     cl
74 08                                           jz      short loc_30000EED
43                                              inc     ebx
3B 5D 0C                                        cmp     ebx, [ebp+arg_4]
74 CF                                           jz      short loc_30000EBA
EB CF                                           jmp     short RC4_Loop
```

InTELL
BY FOX IT

Evolution of Andromeda

```
                                RC4_Loop:                                ; CODE XR
36 8A 94 29 00 FF FF FF                  mov     dl, ss:[ecx+ebp+var_100]
02 C2                                    add     al, dl
02 04 33                                 add     al, [ebx+esi]
36 8A B4 28 00 FF FF FF                  mov     dh, ss:[eax+ebp+var_100]
36 88 B4 29 00 FF FF FF                  mov     ss:[ecx+ebp+var_100], dh
36 88 94 28 00 FF FF FF                  mov     ss:[eax+ebp+var_100], dl
FE C1                                    inc     cl
74 08                                    jz      short loc_7FFA0EDD
43                                       inc     ebx
3B 5D 0C                                 cmp     ebx, [ebp+arg_4]
74 CF                                    jz      short loc_7FFA0EAA
EB CF                                    jmp     short RC4_Loop
```

InTELL
BY FOX IT

Evolution of Andromeda

- Binary
  - They want to fool you
    - Fake RC4 key
      - MD5("go fuck yourself")
      - 754037e7be8f61cbb1b85ab46c7da77d

Evolution of Andromeda

- Base plugins (older versions)
  - Socks4
  - Formgrabber
  - Keylogger
  - Ring3 Rootkit

Evolution of Andromeda

- Base plugins
  - Socks5
  - Formgrabber
  - Keylogger
  - TeamViewer

Evolution of Andromeda

- Additional plugins
  - Tutorial/Help on how to write your own plugins

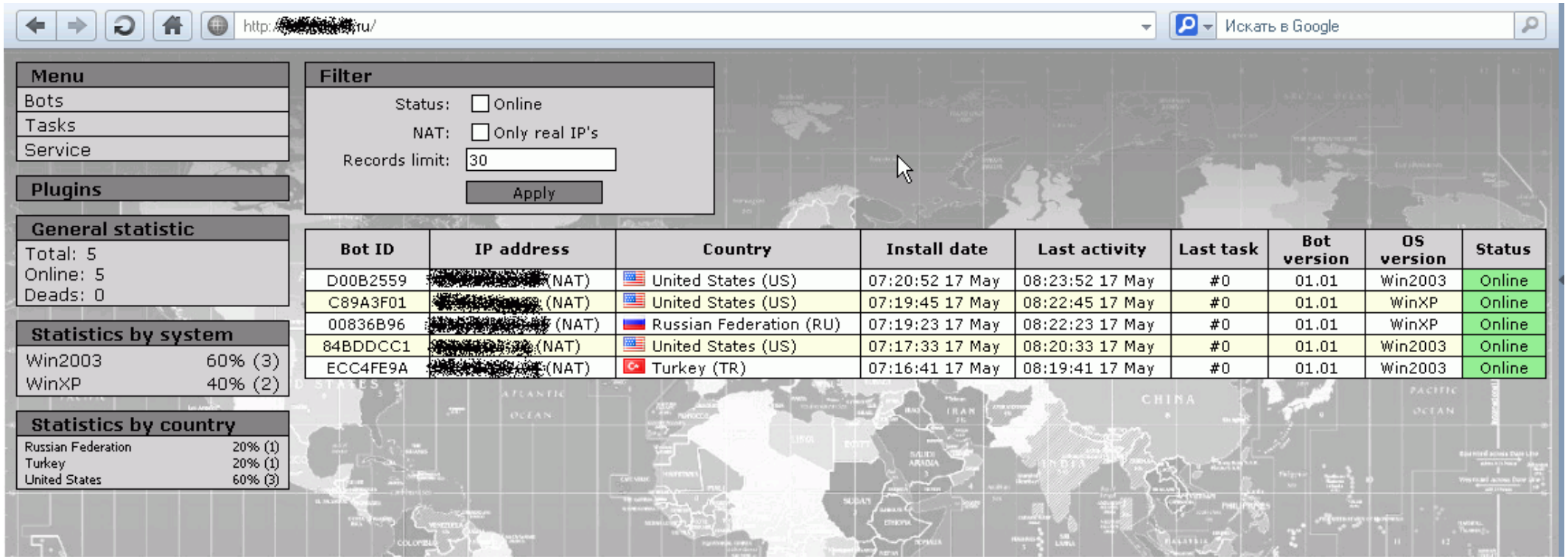
Evolution of Andromeda

- Additional plugins
  - Pony
  - Powershell + Embedded dlls
  - Spam
  - Proxy
  - …

Evolution of Andromeda

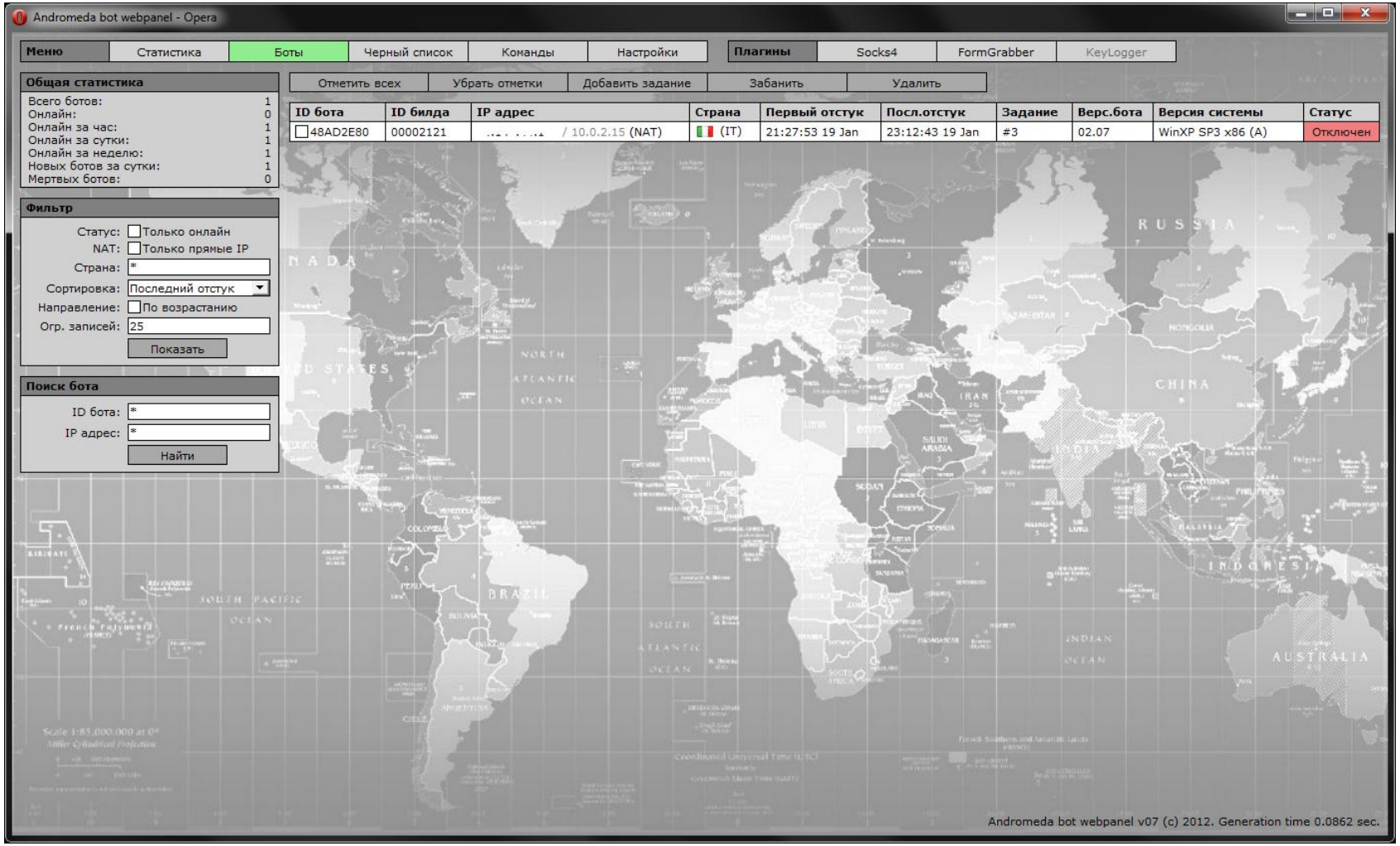
- Panel
  - Show bot information / stats
  - Create tasks
  - Check received logs (Formgrabber / Keylogger)

Evolution of Andromeda



InTELL BY FOX IT

Evolution of Andromeda



InTELL
BY FOX IT

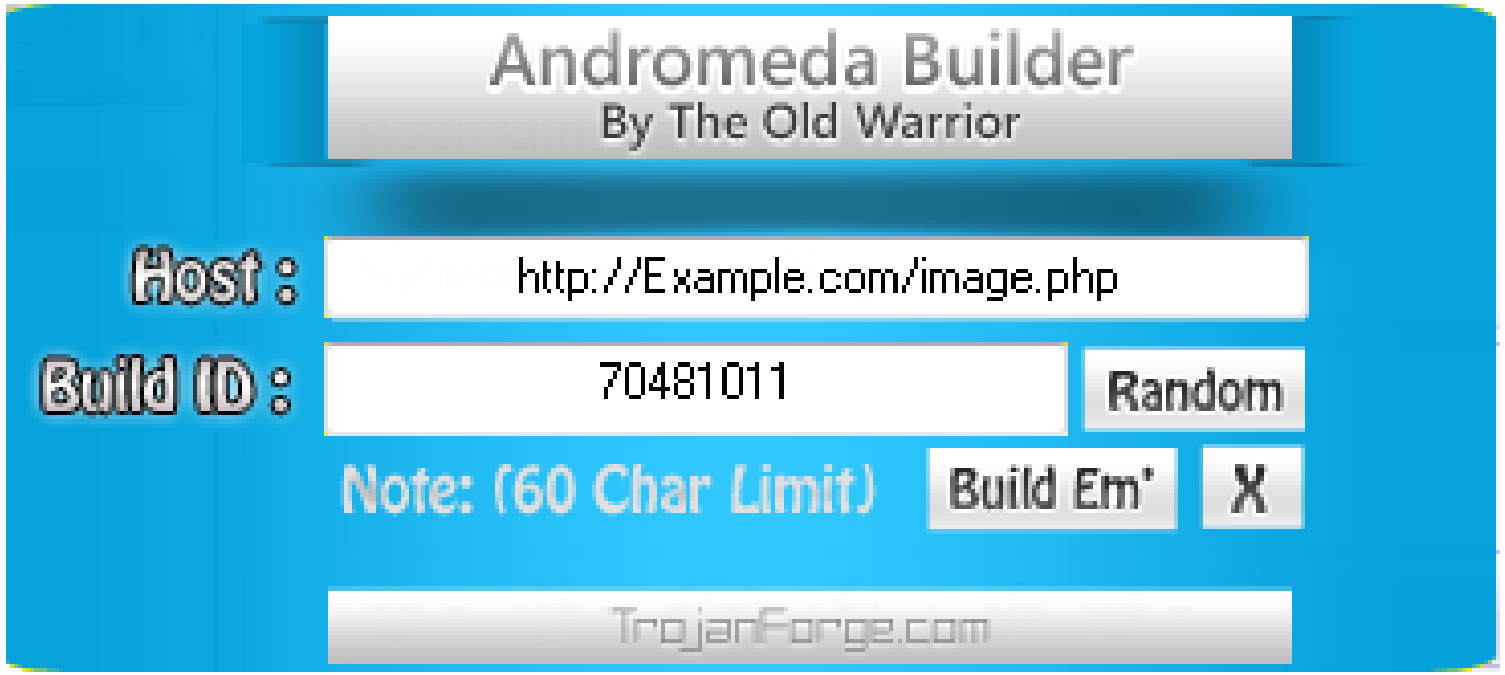
Evolution of Andromeda

- Panel
  - No too many changes in last version
  - Just added support for:
    - TeamViewer
    - JSON

The Dark Side of Andromeda

- Who is behind Andromeda?

The Dark Side of Andromeda



d40e75961383124949436f37f45a8cb6

The Dark Side of Andromeda

- Business model
  - Selling bot licenses
  - Charging per rebuild (bot)
  - Payment
    - BTC, Perfect Money

The Dark Side of Andromeda

- Builder
  - Used to create the binaries
    - URLs
    - RC4 key
    - Builder id

The Dark Side of Andromeda

- Jabber bot
  - Fully active since Feb 2012
  - Connected to customer DB
  - Refill credit
  - Build binaries
    - Command sent to bot
    - Bot responds with links to the binaries

The Dark Side of Andromeda

- Jabber bot
  - **resident**: If the bot will remain installed in the system or not
  - **plugins**: Can be disabled if you do not plan on using plug-ins
  - **integrity**: Add privilege elevation
  - **services**: Add functionality to stop and disable security services
  - **vm**: Add functionality to detect the virtual machines and "bad" software
  - **dns**: Specifies if the bot will use Google DNS servers to resolve domains
  - **relocs**: Relocation of sections in the executable

The Dark Side of Andromeda

- Jabber bot
  - ! set | resident | off
  - ! build | 123ABC | http://first.com/gate.php | http://second.com/gate.php

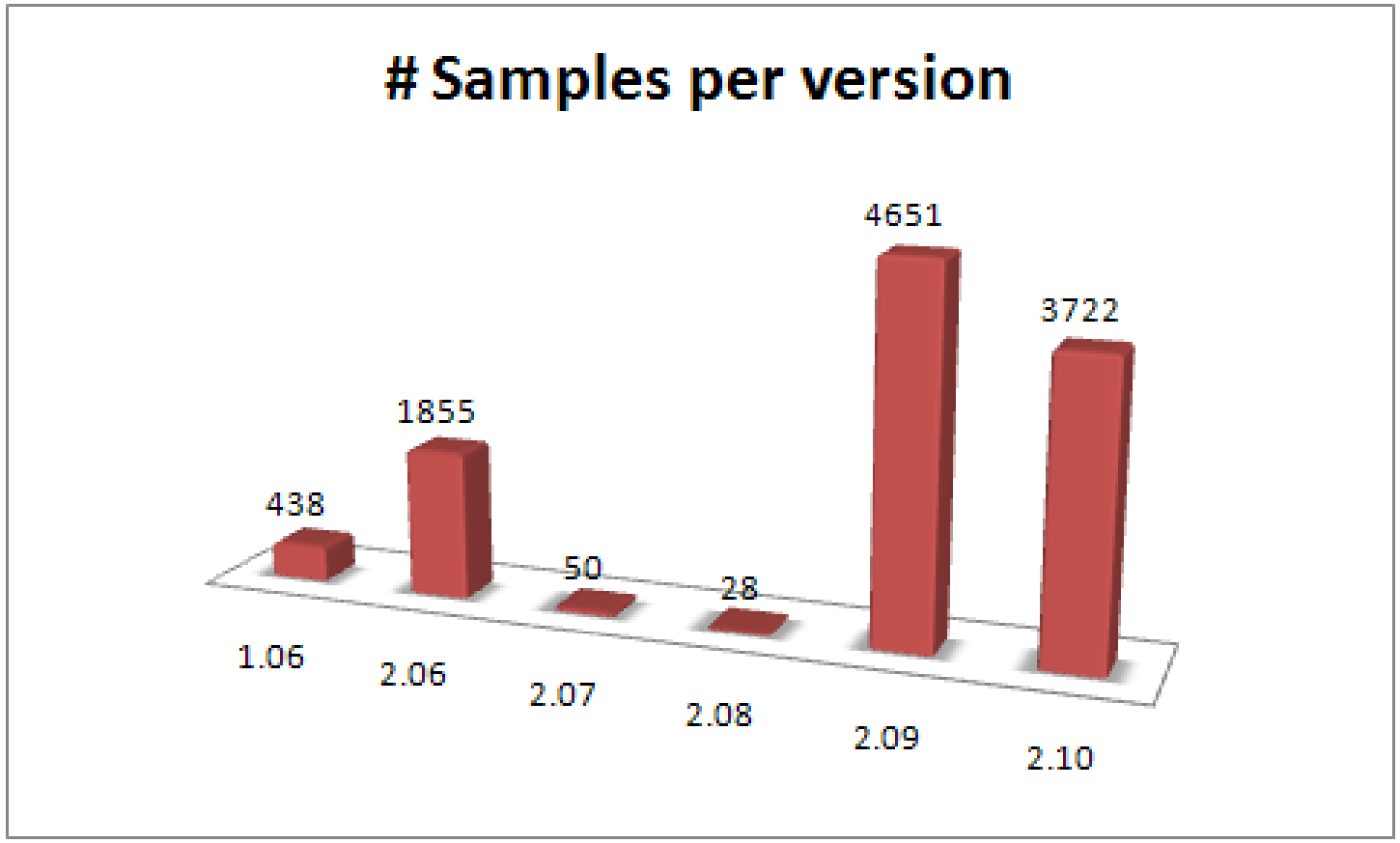
The Dark Side of Andromeda

- Prices

Product	Old price
Bot v1.*	$300
Bot v2.*	$500
Socks4	Included
Formgrabber	$500
Keylogger	$200
Ring3 Rootkit	$300

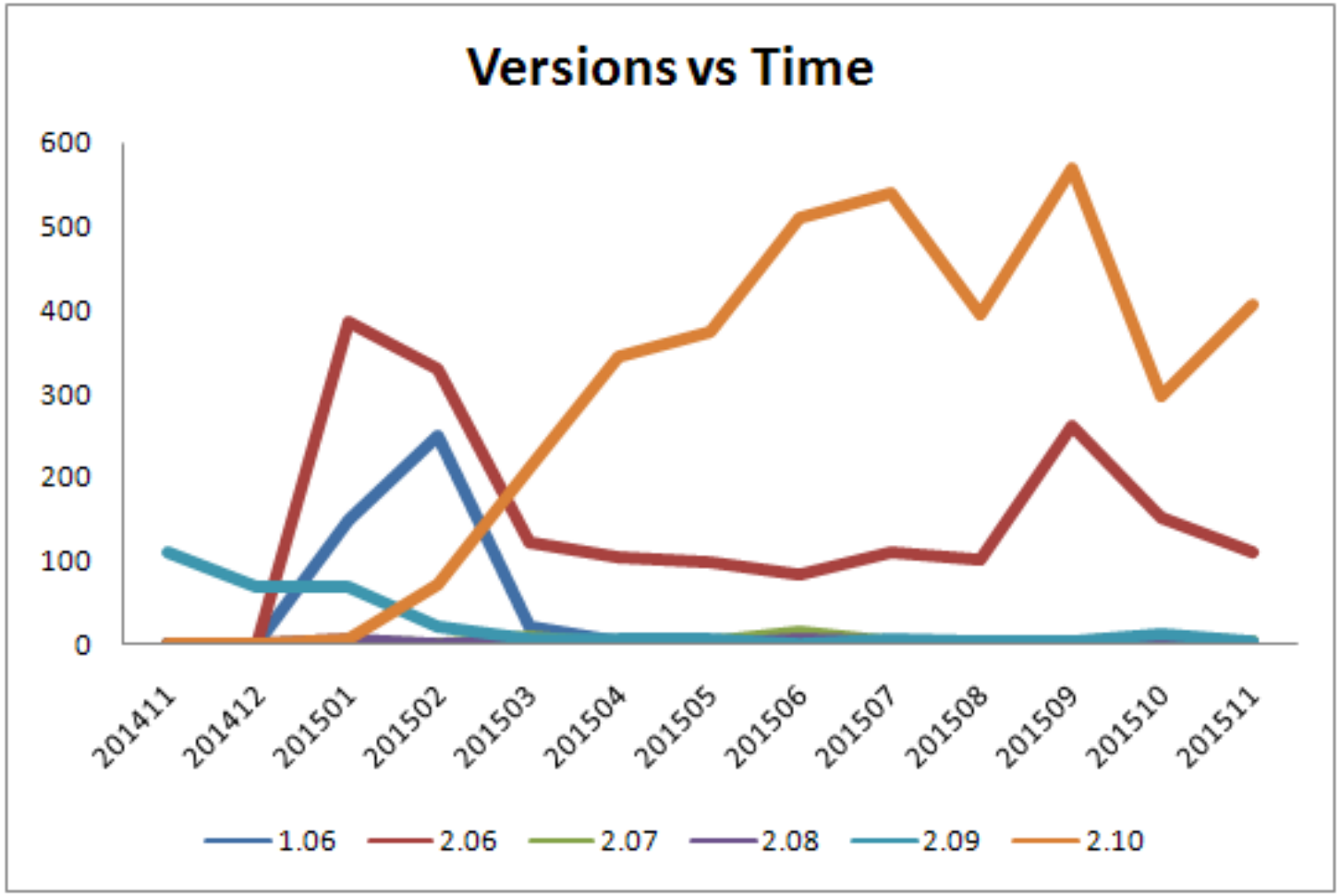
Product	Current price
Bot v2.*	$500
Rebuild (bot)	$10
Socks5	Free
Formgrabber	$500
Keylogger	$200
TeamViewer	$500

Statistics



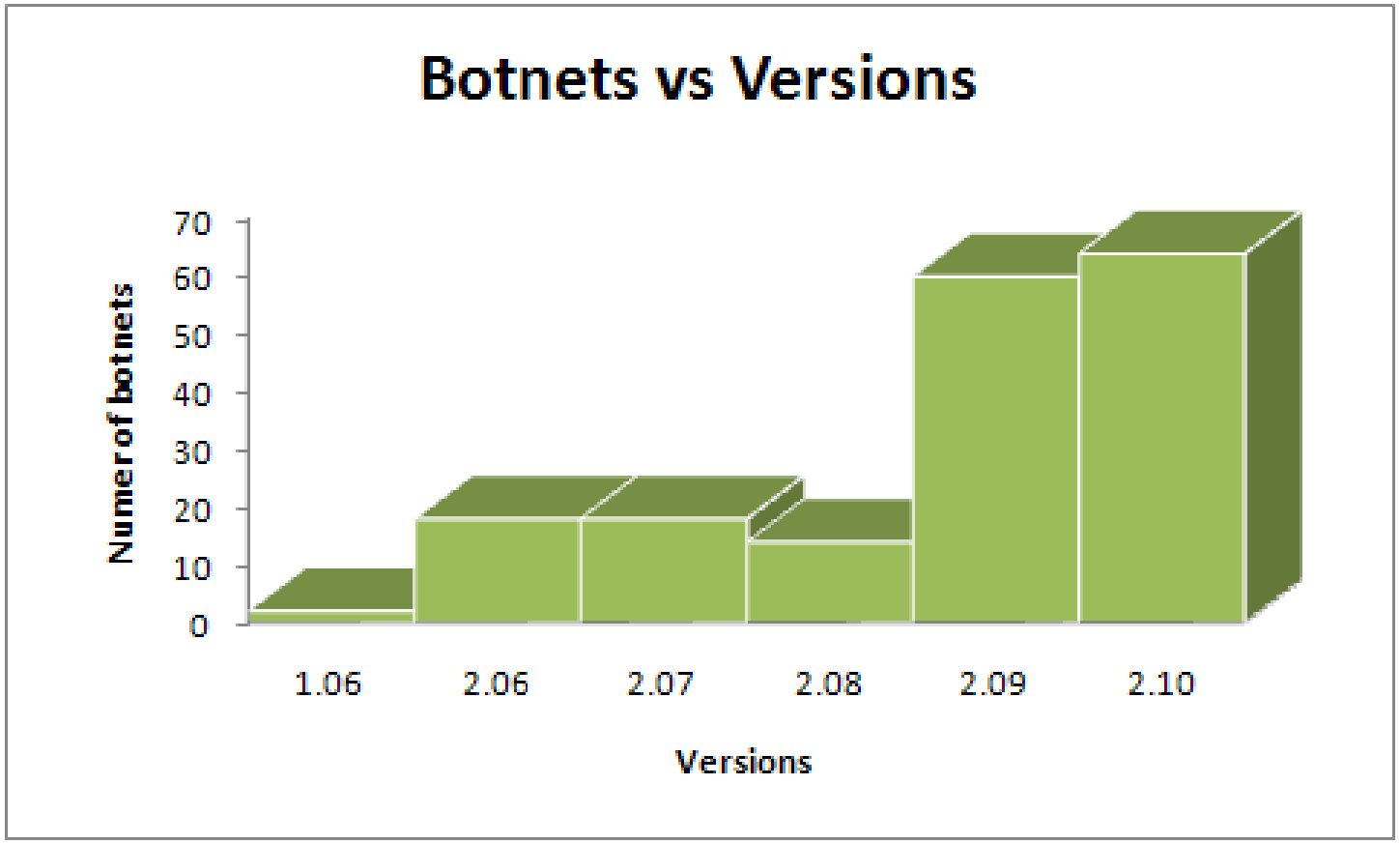
InTELL
BY FOX IT

Statistics



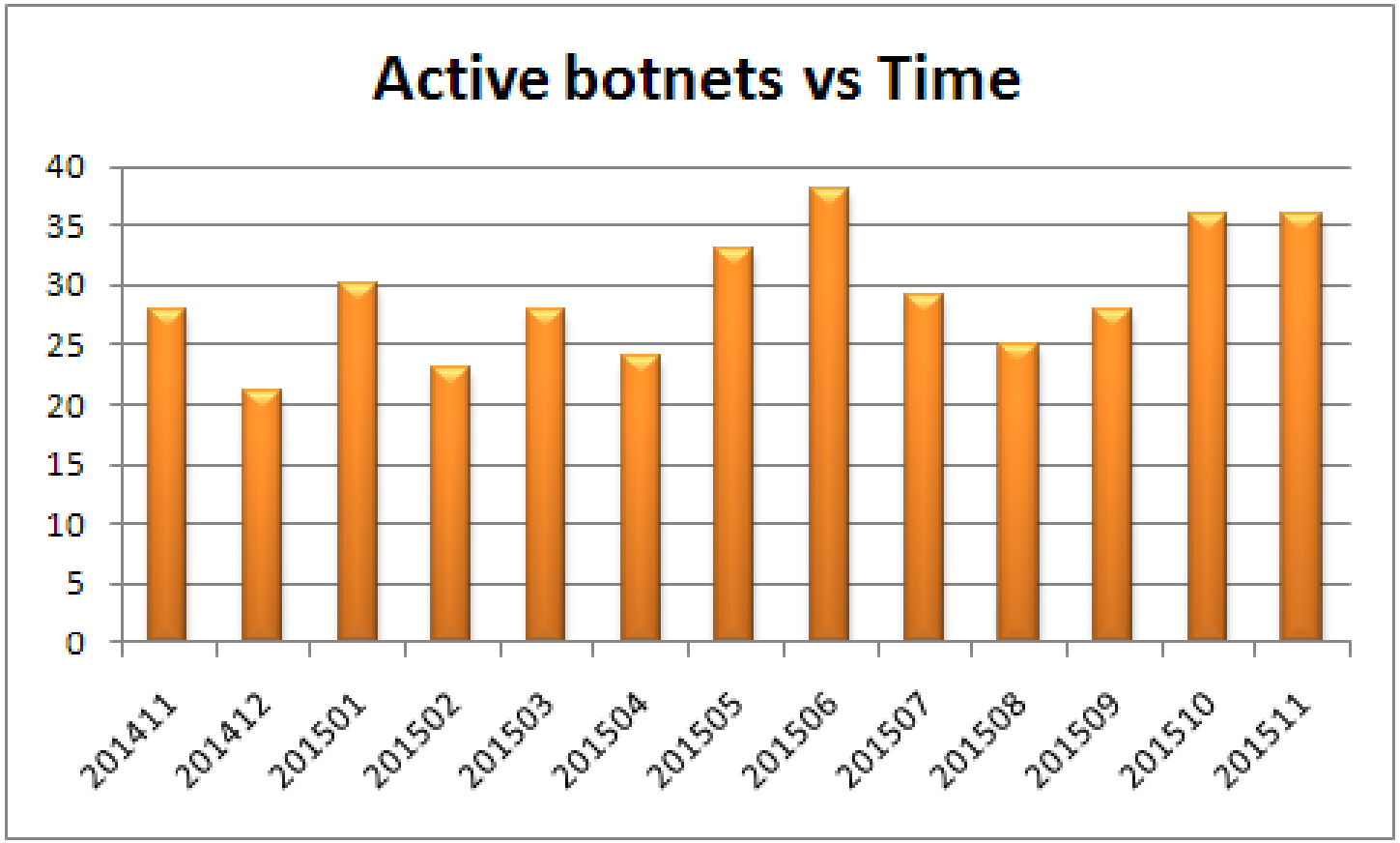
InTELL
BY FOX IT

Statistics



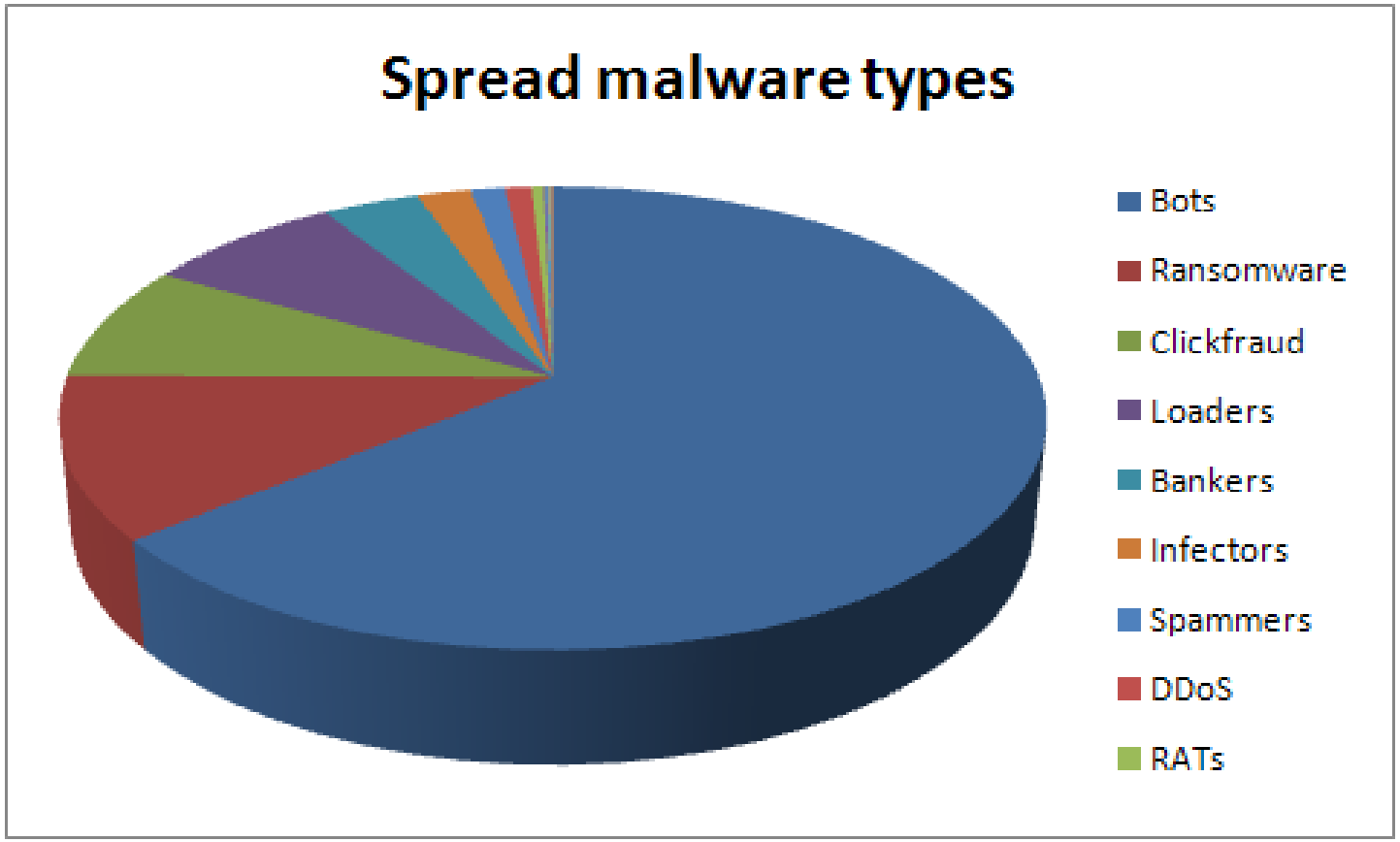
InTELL
BY FOX IT

Statistics



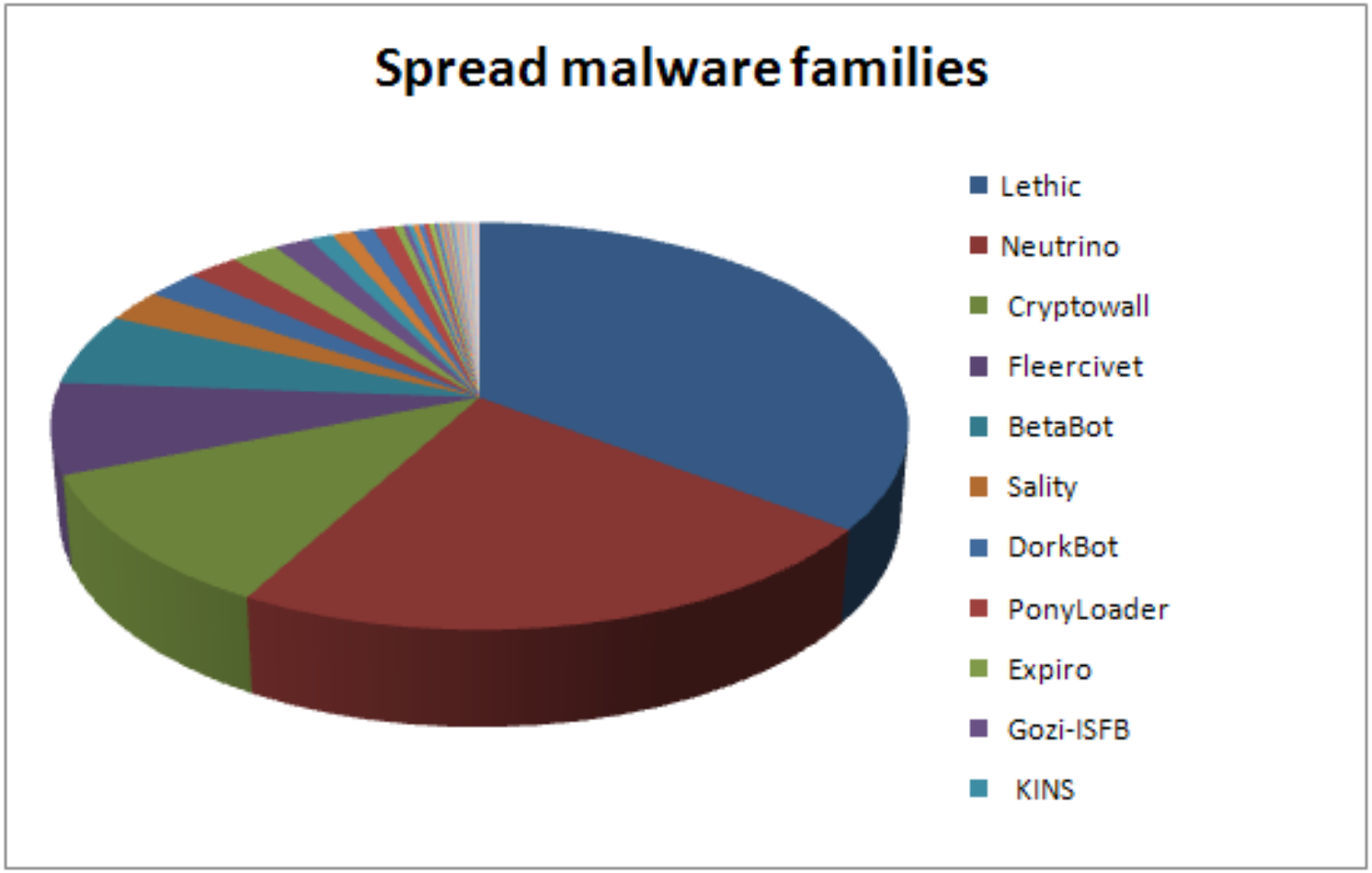
InTELL
BY FOX IT

Statistics



InTELL
BY FOX IT

Statistics



InTELL
BY FOX IT

Interesting use cases

- The Anunak group
- Smilex
- GamaPOS
- Andromeda + TOR
- Andromeda + PDF
- Andromeda loving AV industry

Interesting use cases

- The Anunak group
  - Report published in December 2014 (Fox-IT+GroupIB)
  - Russian banks and POS breaches
  - Andromeda botnet
    - Gozi/ISFB variant dropping Andromeda
    - Andromeda dropping Anunak

Interesting use cases

- Smilex
  - Dridex operator
  - Arrested some months ago in Cyprus
  - Using Andromeda to distribute spambot (FortDisco)
  - Spambot distributing Dridex via doc+macro

Interesting use cases

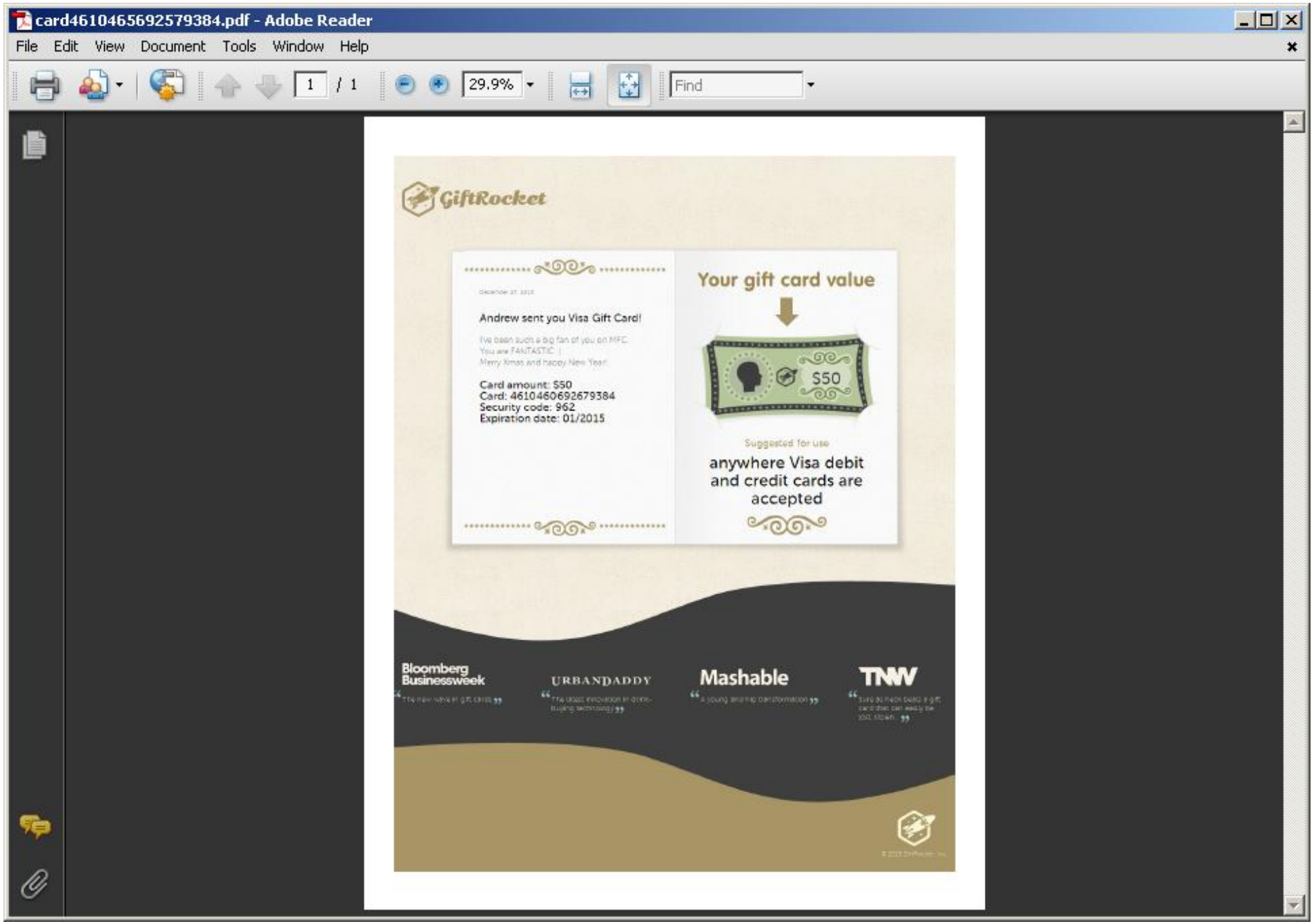
- GamaPOS
  - TrendMicro (July 2015)
  - Andromeda spread via DOC+Macro and Rig EK
  - PsExec & Mimikatz
  - GamaPOS in certain bots

Interesting use cases

- Andromeda + TOR
  - Weird case
  - Spotted by Jaime Blasco (AlienVault)
  - Dropper on Malwr
  - Setting up proxy in the registry…

Interesting use cases

- Andromeda + PDF
  - Curious case
  - Binary executing Andromeda
  - Opening decoy PDF file



InTELL BY FOX IT

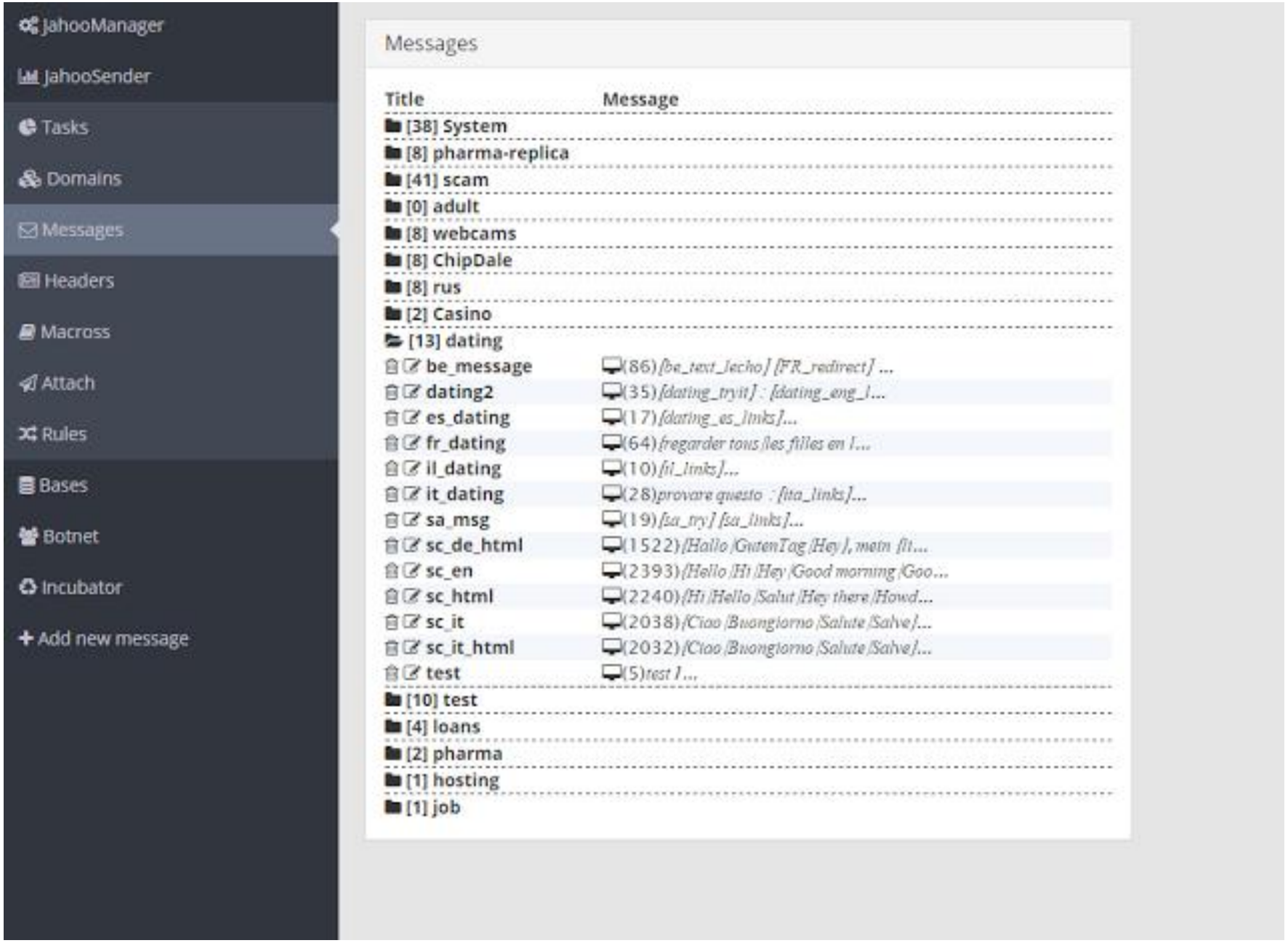
Interesting use cases

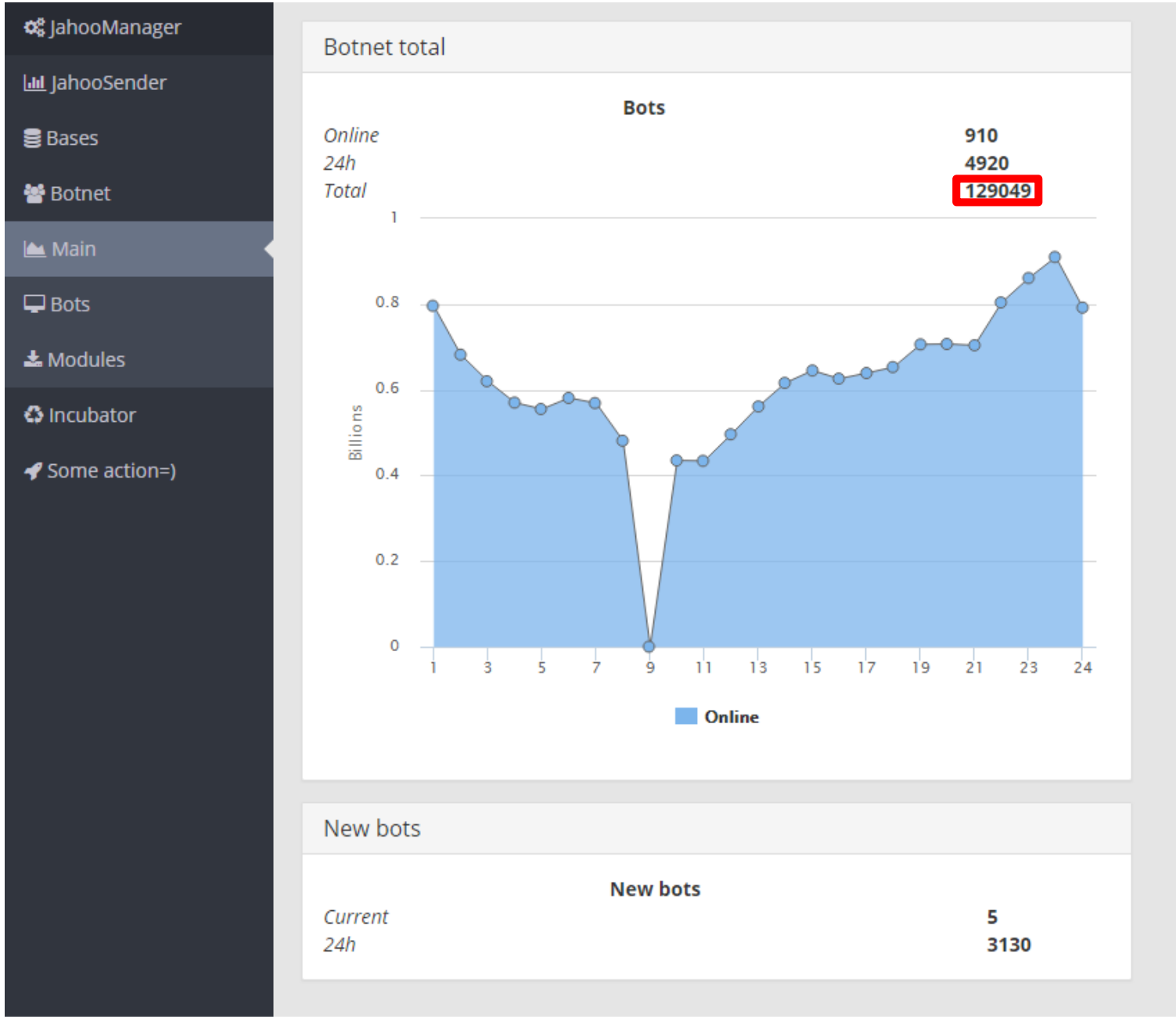
- Andromeda loving AV industry

Function	Data
c&c	http://avastsupport.net/base/gate.php
c&c	http://avastsecure.com/base/gate.php
binary_distribution	http://nortonsecure.net/avbases/serv/an2510.pack
c&c	http://nortoncenter.net/newstyle/topview.php
c&c	http://nortonsecure.net/avbases/linuxttl.php

Interesting use cases

- Veronica´s botnet ;)
  - Distributed same plugin, different hashes
  - Spam bot (Jahoo/Otlarda)
    - S:_src_bor_soft\JSS_kit\Jahoo\Release\Jahoo32.pdb
  - Documented by Kafeine 5 days ago


JahooManager
JahooSender
Tasks
Domains
Messages
Headers
Macross
Attach
Rules
Bases
Botnet
Incubator
+ Add new message
Messages
Title
Message
[38] System
[8] pharma-replica
[41] scam
[0] adult
[8] webcams
[8] ChipDale
[8] rus
[2] Casino
[13] dating
be_message (86) [be_text_lecho] [FR_redirect] ...
dating2 (35) [dating_tryit] : [dating_eng_l...
es_dating (17) [dating_es_links]...
fr_dating (64) regarder tous les filles en l...
il_dating (10) [il_links]...
it_dating (28) provare questo : [ita_links]...
sa_msg (19) [sa_try] [sa_links]...
sc_de_html (1522) [Hallo |GutenTag |Hey], mein [it...
sc_en (2393) [Hello |Hi |Hey |Good morning |Goo...
sc_html (2240) [Hi |Hello |Salut |Hey there |Howd...
sc_it (2038) [Ciao |Buongiorno |Salute |Salve]...
sc_it_html (2032) [Ciao |Buongiorno |Salute |Salve]...
test (5) test 1 ...
[10] test
[4] loans
[2] pharma
[1] hosting
[1] job


JahooManager
JahooSender
Bases
Botnet
Main
Bots
Modules
Incubator
Some action=)
Botnet total
Bots
Online 910
24h 4920
Total 129049
Billions
1
0.8
0.6
0.4
0.2
0
1 3 5 7 9 11 13 15 17 19 21 23 24
Online
New bots
New bots
Current 5
24h 3130

Conclusions

- Andromeda is far from dying
- Alive “project” and business
- Used by serious criminal gangs
- Interesting custom plugins

Acknowledgements

- Fox-IT InTELL
  - Ronaldo Vasconcellos
  - Alberto Ortega
  - Frank Ruiz
- The Honeynet Project
- Malware research community
  - Alexandru Maximciuc (Bitdefender)
- Botconf

InTELL
BY FOX IT

Thanks!!

Jose Miguel Esparza

http://eternal-todo.com

@EternalTodo