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
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/andromeda-gamarue-loves-json
  - http://blog.fortinet.com/post/andromeda-2-7-features
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

```c
bb_flag = 0;
v6 = GetKeyboardLayoutList(0, 0);
v21 = v6;
if ( v6 )
{
  v7 = sub_7FF92329(4 * v6 + 4);
v8 = v7;
  if ( v7 )
  {
    GetKeyboardLayoutList(v21, (HKL *)v7);
    for ( _DWORD *v8; *i; ++i )
    {
      v10 = *i & 0xFFFF;
      if ( v10 == 1049 || v10 == 1058 || v10 == 1059 || v10 == 1087 )// Russian | Ukrainian | Belarusian | Kazakh
        bb_flag = 1;
    }
  }
  sub_7FF92358(v8);
}
sub_7FF94280();
sub_7FF94745();
return 1;
```
Evolution of Andromeda

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

- Binary
  - Anti-analysis
    - Newer versions
      - Just blacklisted processes (CRC32)
## Evolution of Andromeda

<table>
<thead>
<tr>
<th>Hex</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 44 DD 99</td>
<td>hash_blacklist</td>
<td>Added in 2.07</td>
</tr>
<tr>
<td>B4 9D 85 2D</td>
<td>Added in 2.08/2.09</td>
<td></td>
</tr>
<tr>
<td>CE OD 34 64</td>
<td>Added in latest version</td>
<td></td>
</tr>
<tr>
<td>74 44 C5 63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8B 9C 9C 34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CE EE 46 34</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE B1 A9 5B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F3 BE E2 3C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2B F0 46 3D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F7 10 AE 77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5D E9 44 F3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6F 6D BE 2D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44 02 D1 A3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>91 ED 72 1D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE 6B 93 96</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58 DF 8C 27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>85 F8 FF 3B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D9 23 33 6D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4 C6 EB 92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D2 AC 18 DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D4 F7 44 30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 00 00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Version 2.06**
- `dd 9DD4432h` (DATA XREF: AntiAnalysis+C8\r
AntiAnalysis+DD\r
vmwareuser.exe)
- `dd 2D859DB4h` (vmwareservice.exe)
- `dd 64340DCEh` (vboxservice.exe)
- `dd 63C54474h` (vboxray.exe)
- `dd 3495C68Bh` (sandboxedcomlaunch.exe)
- `dd 3446E7CEh` (sandboxiercss.exe)
- `dd 5BA9B1FEh` (procmon.exe)
- `dd 3CE2BEF3h` (regmon.exe)
- `dd 3D46F02Bh` (filemon.exe)
- `dd 77AE10F7h` (wireshark.exe)
- `dd 0F344E95Dh` (netmon.exe)

**Added in 2.07**
- `dd 2DE6D6F7h` (prl_tools_service.exe (Parallels))
- `dd 0A3D10244h` (prl_tools.exe (Parallels))
- `dd 1D72ED91h` (prl_cc.exe (Parallels))
- `dd 96936BEEh` (sharedintapp.exe (Parallels))
- `dd 278CDF58h` (vmtoolsd.exe)
- `dd 3BBFF885h` (vmsrv.exe)
- `dd 6D3223D9h` (vmusrv.exe)
- `dd 0D2EF06C4h` (python.exe (New!))
- `dd 0D1BACD2h` (perl.exe (New!))
- `dd 304DF7D4h` (New)
Evolution of Andromeda

<table>
<thead>
<tr>
<th>Version 2.06</th>
<th>Added in 2.07</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash_blackList</td>
<td>dd 9DD4432h</td>
</tr>
<tr>
<td></td>
<td>DATA XREF: AntiAnalysis+C8\r</td>
</tr>
<tr>
<td></td>
<td>AntiAnalysis+DD\r</td>
</tr>
<tr>
<td></td>
<td>vmwareuser.exe</td>
</tr>
<tr>
<td></td>
<td>vmwareservice.exe</td>
</tr>
<tr>
<td></td>
<td>vboxservice.exe</td>
</tr>
<tr>
<td></td>
<td>vboxtray.exe</td>
</tr>
<tr>
<td></td>
<td>sandboxedcomlaunch.exe</td>
</tr>
<tr>
<td></td>
<td>sandboxierpcss.exe</td>
</tr>
<tr>
<td></td>
<td>procmem.exe</td>
</tr>
<tr>
<td></td>
<td>dd 2D859DB4h</td>
</tr>
<tr>
<td></td>
<td>vboxservice.exe</td>
</tr>
<tr>
<td></td>
<td>vboxtray.exe</td>
</tr>
<tr>
<td></td>
<td>sandboxedcomlaunch.exe</td>
</tr>
<tr>
<td></td>
<td>sandboxierpcss.exe</td>
</tr>
<tr>
<td></td>
<td>procmem.exe</td>
</tr>
<tr>
<td></td>
<td>dd 3C2BEF3h</td>
</tr>
<tr>
<td></td>
<td>regmon.exe</td>
</tr>
<tr>
<td></td>
<td>filemon.exe</td>
</tr>
<tr>
<td></td>
<td>dd 77AE10F7h</td>
</tr>
<tr>
<td></td>
<td>wireshark.exe</td>
</tr>
<tr>
<td></td>
<td>netmon.exe</td>
</tr>
<tr>
<td></td>
<td>dd 0F344E95Dh</td>
</tr>
<tr>
<td></td>
<td>prl_tools_service.exe (Parallels)</td>
</tr>
<tr>
<td></td>
<td>prl_tools.exe (Parallels)</td>
</tr>
<tr>
<td></td>
<td>prl_cc.exe (Parallels)</td>
</tr>
<tr>
<td></td>
<td>sharedintapp.exe (Parallels)</td>
</tr>
<tr>
<td></td>
<td>vmtoolsd.exe</td>
</tr>
<tr>
<td></td>
<td>vmsrv.exe</td>
</tr>
<tr>
<td></td>
<td>vmsrv.exe</td>
</tr>
<tr>
<td></td>
<td>dd 0DE2FC64h</td>
</tr>
<tr>
<td></td>
<td>python.exe (New!)</td>
</tr>
<tr>
<td></td>
<td>perl.exe (New!)</td>
</tr>
<tr>
<td></td>
<td>dd 3044F7D4h</td>
</tr>
<tr>
<td></td>
<td>New</td>
</tr>
</tbody>
</table>

avpui.exe (Kaspersky)
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

```c
j_seg004_ws2_32_WSAStrtup(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);
```
Evolution of Andromeda

- Binary
  - They want to fool you
    - Fake URLs
      - thisshitismoresafethanpentagonfuckyoufedsbecausethisisasf.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

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
ret     4

RemoveCode endp
```

; CODE XREF: sub_7FF91A2C+1D9+p
; DATA XREF: RemoveCode+24+w
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

```assembly
loc_30001031:
    ; CODE
    ; Begin

    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
```
Evolution of Andromeda

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

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

RC4_Loop:

```
36 8A 94 29 00 FF FF FF
02 C2
02 04 33
36 8A B4 28 00 FF FF FF
36 88 B4 29 00 FF FF FF
36 88 94 28 00 FF FF FF
FE C1
74 08
43
3B 5D 0C
74 CF
EB CF
```

```
mov  dl, ss:[ecx+ebp+var_100]
add  al, dl
add  al, [ebx+esi]
mov  dh, ss:[eax+ebp+var_100]
mov  ss:[ecx+ebp+var_100], dh
mov  ss:[eax+ebp+var_100], dl
inc  cl
jz   short loc_7FFA0EDD
inc  ebx
cmp  ebx, [ebp+arg_4]
jz   short loc_7FFA0EAA
jmp  short RC4_Loop
```
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
Evolution of Andromeda
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
The Dark Side of Andromeda

- Prices

<table>
<thead>
<tr>
<th>Product</th>
<th>Old price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot v1.*</td>
<td>$300</td>
</tr>
<tr>
<td>Bot v2.*</td>
<td>$500</td>
</tr>
<tr>
<td>Socks4</td>
<td>Included</td>
</tr>
<tr>
<td>Formgrabber</td>
<td>$500</td>
</tr>
<tr>
<td>Keylogger</td>
<td>$200</td>
</tr>
<tr>
<td>Ring3 Rootkit</td>
<td>$300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product</th>
<th>Current price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot v2.*</td>
<td>$500</td>
</tr>
<tr>
<td>Rebuild (bot)</td>
<td>$10</td>
</tr>
<tr>
<td>Socks5</td>
<td>Free</td>
</tr>
<tr>
<td>Formgrabber</td>
<td>$500</td>
</tr>
<tr>
<td>Keylogger</td>
<td>$200</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>$500</td>
</tr>
</tbody>
</table>
Statistics

# Samples per version

- 1.06: 438
- 2.06: 1855
- 2.07: 50
- 2.08: 28
- 2.09: 4651
- 2.10: 3722
Statistics

Versions vs Time

1.06  2.06  2.07  2.08  2.09  2.10
Statistics

![Bar Chart: Botnets vs Versions]

- **Versions**: 1.06, 2.06, 2.07, 2.08, 2.09, 2.10
- **Number of Botnets**: 0, 10, 20, 30, 60, 70

*Note: The exact number of botnets for each version is not specified in the diagram.*
Statistics

Active botnets vs Time

InTELL BY FOX IT
Statistics

Spread malware types

- Bots
- Ransomware
- Clickfraud
- Loaders
- Bankers
- Infectors
- Spammers
- DDoS
- RATs
Statistics

Spread malware families

- Lethic
- Neutrino
- Cryptowall
- Fleercivet
- BetaBot
- Sality
- DorkBot
- PonyLoader
- Expiro
- Gozi-ISFB
- KINS
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
Interesting use cases
Interesting use cases

- Andromeda loving AV industry

<table>
<thead>
<tr>
<th>Function</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>c&amp;c</td>
<td><a href="http://avastsupport.net/base/gate.php">http://avastsupport.net/base/gate.php</a></td>
</tr>
<tr>
<td>c&amp;c</td>
<td><a href="http://avastsecure.com/base/gate.php">http://avastsecure.com/base/gate.php</a></td>
</tr>
<tr>
<td>binary_distribution</td>
<td><a href="http://nortonsecure.net/avbases/serv/an2510.pack">http://nortonsecure.net/avbases/serv/an2510.pack</a></td>
</tr>
<tr>
<td>c&amp;c</td>
<td><a href="http://nortoncenter.net/newstyle/topview.php">http://nortoncenter.net/newstyle/topview.php</a></td>
</tr>
<tr>
<td>c&amp;c</td>
<td><a href="http://nortonsecure.net/avbases/linuxttl.php">http://nortonsecure.net/avbases/linuxttl.php</a></td>
</tr>
</tbody>
</table>
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
### Messages

<table>
<thead>
<tr>
<th>Title</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>[38] System</td>
<td></td>
</tr>
<tr>
<td>[8] pharma-replica</td>
<td></td>
</tr>
<tr>
<td>[41] scam</td>
<td></td>
</tr>
<tr>
<td>[9] adult</td>
<td></td>
</tr>
<tr>
<td>[8] webcams</td>
<td></td>
</tr>
<tr>
<td>[8] ChipDale</td>
<td></td>
</tr>
<tr>
<td>[8] rus</td>
<td></td>
</tr>
<tr>
<td>[2] Casino</td>
<td></td>
</tr>
<tr>
<td>[13] dating</td>
<td></td>
</tr>
<tr>
<td>be_message</td>
<td>(665) [be-text-becho] [FR_redirect] ...</td>
</tr>
<tr>
<td>dating2</td>
<td>(35) [dating-try] [dating-try1] ...</td>
</tr>
<tr>
<td>es_dating</td>
<td>(17) [dating_es_links] ...</td>
</tr>
<tr>
<td>fr_dating</td>
<td>(64) [regarder_tous] [les_filles_en_1] ...</td>
</tr>
<tr>
<td>il_dating</td>
<td>(10) [il_links] ...</td>
</tr>
<tr>
<td>it_dating</td>
<td>(28) [provarre_questo] [it_links] ...</td>
</tr>
<tr>
<td>sa_msg</td>
<td>(19) [sa_try] [sa_links] ...</td>
</tr>
<tr>
<td>sc_de_html</td>
<td>(1522) [Hallo] [GutenTag] [Hej], main fl...</td>
</tr>
<tr>
<td>sc_en</td>
<td>(2393) [Hello] [Hi] [Hey] [Good morning] [Goo...</td>
</tr>
<tr>
<td>sc_html</td>
<td>(2240) [Hi] [Hello] [Salut] [Hey there] [Howd...</td>
</tr>
<tr>
<td>sc_it</td>
<td>(2038) [Ciao] [Buongiorno] [Salute] [Save] ...</td>
</tr>
<tr>
<td>sc_it_html</td>
<td>(2032) [Ciao] [Buongiorno] [Salute] [Save] ...</td>
</tr>
<tr>
<td>test</td>
<td>(5) [test] ...</td>
</tr>
<tr>
<td>test</td>
<td></td>
</tr>
<tr>
<td>test</td>
<td></td>
</tr>
<tr>
<td>[10] test</td>
<td></td>
</tr>
<tr>
<td>[4] loans</td>
<td></td>
</tr>
<tr>
<td>[2] pharma</td>
<td></td>
</tr>
<tr>
<td>[1] hosting</td>
<td></td>
</tr>
<tr>
<td>[1] job</td>
<td></td>
</tr>
</tbody>
</table>
Botnet total

Online
24h
Total

Bots

910
4920

New bots

Current
24h

5
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
Thanks!!

Jose Miguel Esparza
http://eternal-todo.com
@EternalTodo