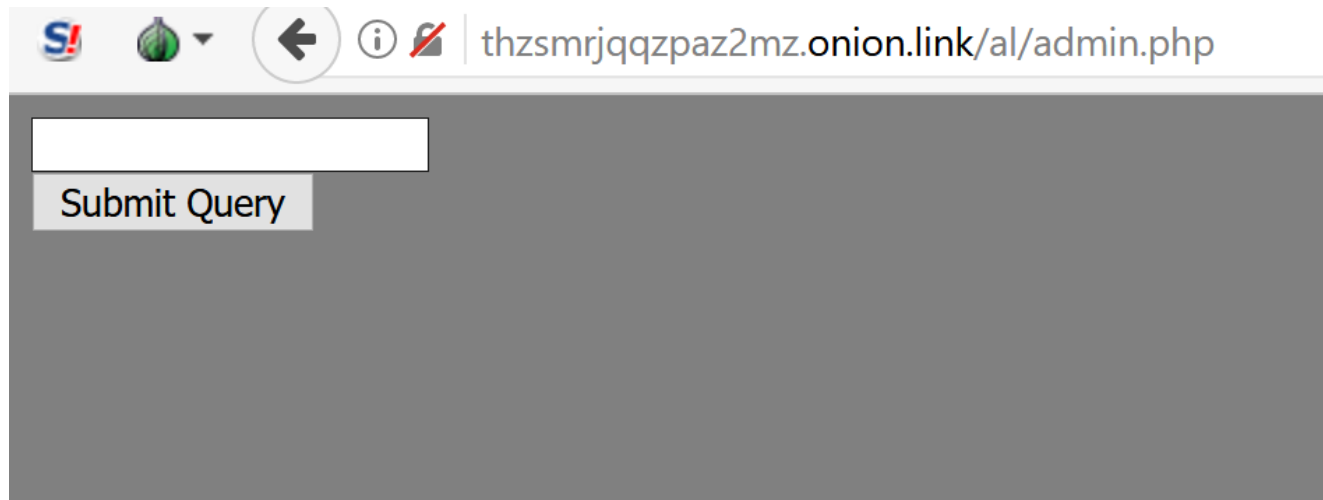


# Quick look at another Alina fork: XBOT-POS

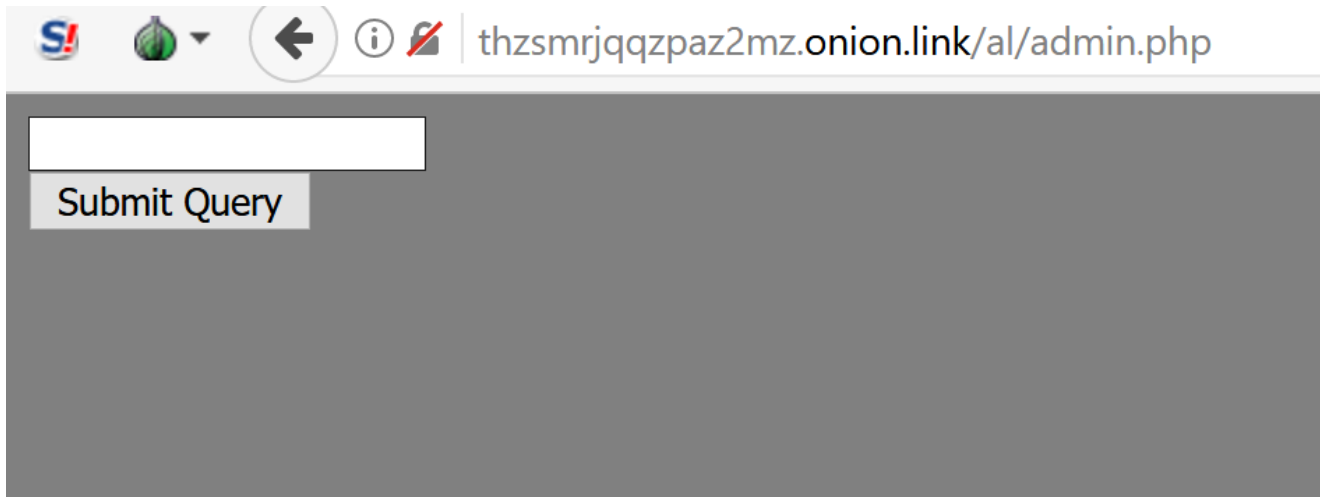
benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html



Edit: In fact after looking at the sample it's a pure copy pasta of Tiny Nuke :) - cd025523e3aec57f809552b9d1adc4b89526cc632f6d4c481aa2c8c3501dda6b Hi, it's time for a new post. Today I'll try to have a look at the "Team NZMR" I've found this funny team by hazard on Twitter via the bot [@ScumBots](#)

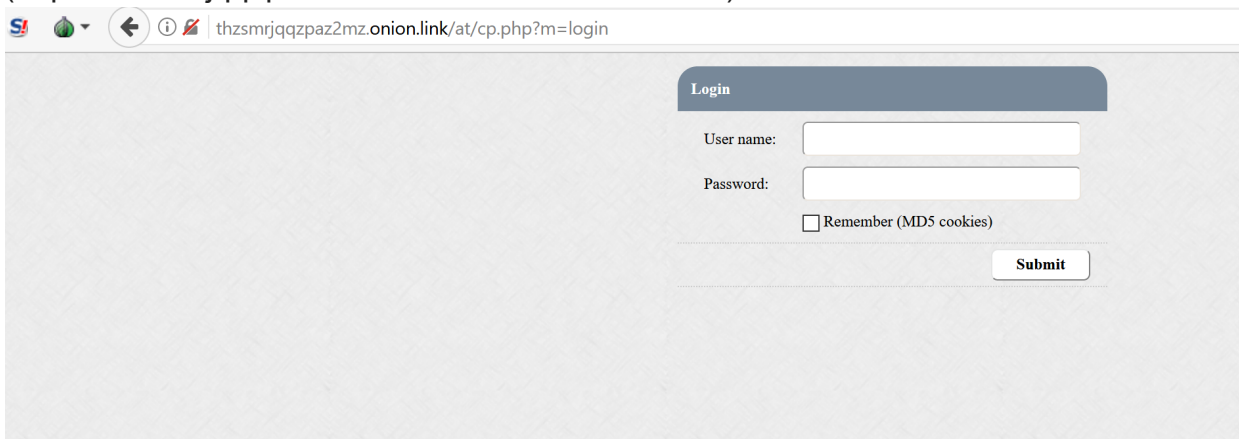
Alina: <https://t.co/ttyh5aEJDX>  
C2:thzsmrjqqpaz2mz[.]onion[.]link/al/loading[.]php,t[.]ht/al/loading[.]php,  
— ScumBots (@ScumBots) [15 août 2017](#)

I would like to write this little blog post because I think that this is interesting to see an Alina panel behind a .onion domain and as you can see later, I like look at some weird panels :D. Let's have a look on this server. As we know, we have an Alina (Well known POS malware) panel at [thzsmrjqqpaz2mz.onion.link/al/loading.php](http://thzsmrjqqpaz2mz.onion.link/al/loading.php) . Samples: [26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298](http://thzsmrjqqpaz2mz.onion.link/al/Spark.exe) (<http://thzsmrjqqpaz2mz.onion.link/al/Spark.exe>)



In the same boring way, we can find:

- a Fareit/Pony panel at <https://thzsmrjqqpaz2mz.onion.link/pn/admin.php> (I don't have sample)
- an Atmos at <https://thzsmrjqqpaz2mz.onion.link/at/cp.php> : Sample e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525 (<https://thzsmrjqqpaz2mz.onion.link/at/files/us.exe>)



Thanks to CCAM we can get 2 new servers used by this team:

- <http://netco1000.ddns.net/at/file.php>
- <http://22klzn6kzjwlm2.onion.link/at/file.php>

Those guys really want your creds and your credit card numbers :D They also try to deal with ransomware (NZMR Ransomware) at <https://thzsmrjqqpaz2mz.onion.link/ed2/> without success...

## Bitcoin Address

Addresses are identifiers which you use to send bitcoins to a

| Summary  |  | Transactions     |       |
|----------|--|------------------|-------|
| Address  | <a href="#">1Dh6zY9U1V3XJELDh8hQdox3eR765XyR4H</a>       | No. Transactions | 0     |
| Hash 160 | <a href="#">8b372656bc83a0238ac5abbec5e3e22da68ae338</a> | Total Received   | 0 BTC |
| Tools    | <a href="#">Related Tags - Unspent Outputs</a>           | Final Balance    | 0 BTC |

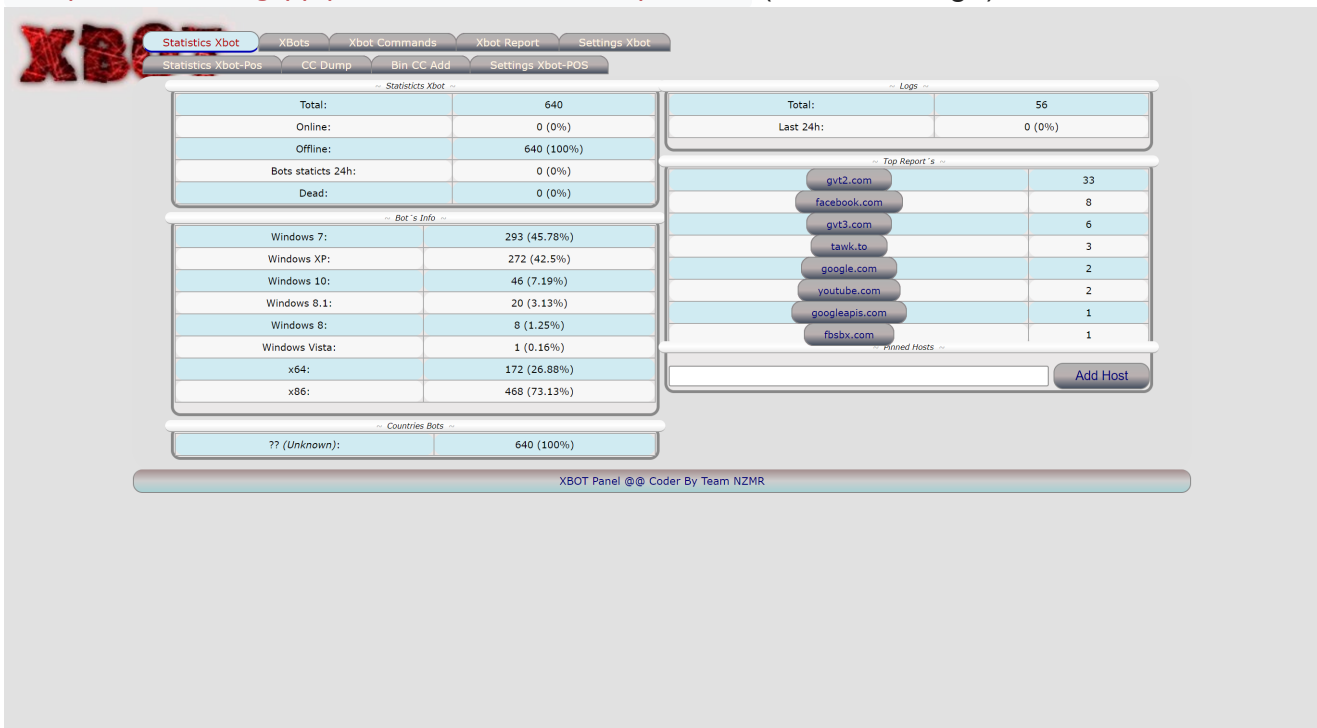
Request Payment Donation Button

### Transactions [\(Oldest First\)](#)

No transactions found for this address, it has probably not been used on the network yet.

But I've write this quick blog post for the last panel, Let me introduce you XBOT panel \o/:

<https://thzsmrjqzpzaz2mz.onion.link/panel/> (click to enlarge)



The bot ad: Selling xbot ,new bank trojan -- Modules -- Webinject -- Formgrabber -- Socket4/5 -- Hidden VNC New bot bank xbot is available for rent (800\$/monthly) -- server on tornetwork/clearnet Customized programming service and web developer/c/c++/Python/NET/others Team Coder/NZMR xbot costs 3k \$ modules available >webinject -- formgrabber -- Socket4/5 -- Hidden VNC When buying xbot what do you get? You will get the builder,bin/exe+socket.exe/server.exe hvnc [+] - Free installation on your server in tornetwork or clearnet, you choose [+] - monthly support paid 100

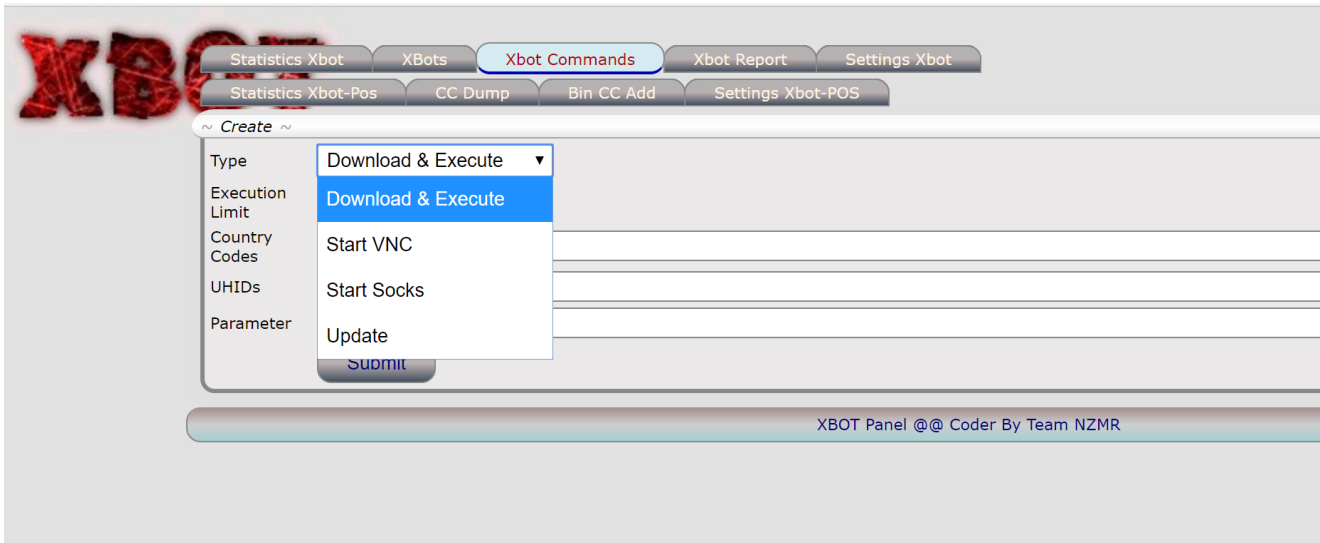
\$ (you choose,with or without support) [+] - Update bot for new version 400 \$ [+] Rent xbot Panel access (Clearnet/Tornetwork) Bin (exe) Socket.exe/hvnc.exe Price 800 \$ monthly (First 6 customers, others 1k \$) Support monthly 100 \$ (btc) I don't have any sample yet but if you have one, i'm REALLY interested :D. Thanks to Xylitol this panel looks like a mix between Alina and Dexter. For example the URI scheme "/front/stats.php", the successtatuscode 666 or this page "Version Control":

The screenshot displays the XBOT control panel. At the top, there are navigation tabs: Statistics Xbot, XBots, Xbot Commands, Xbot Report, Settings Xbot, and Statistics Xbot-Pos. Below these are sub-tabs: CC Dump, Bin CC Add, and Settings Xbot-POS. The main content area is titled 'Overall: 59 XBot-Pos (0 online, 2 online in last 12 hours)'. It includes a 'Version Control' section with a table for updating bots and a 'Bot Control' section listing online and offline bots with their last seen timestamps.

| Version           | Update URL           | Delete                   |
|-------------------|----------------------|--------------------------|
| Mozilla/4.0 (com) | <input type="text"/> | <input type="checkbox"/> |
| Mozilla/5.0 (com) | <input type="text"/> | <input type="checkbox"/> |

**Bot Control**  
 Its 16 August 2017 19:28:12  
 Online:  
 Last 12 hrs:  
 IaRzVW@JOHN-PC (Mozilla/5.0 (com)) - last seen on 16 August 2017 09:50:05  
 rzDATA@DESKTOP-TPP91TT (Mozilla/5.0 (com)) - last seen on 16 August 2017 08:24:10  
 Offline for more than 12 hrs:  
 uAGmz@HACKER0X0-PC423432424230 (Mozilla/4.0 (com)) - last seen on 13 August 2017 01:29:01  
 PscGF2424234@ME2034234234234234 (Mozilla/4.0 (com)) - last seen on 13 August 2017 01:32:16  
 alOmdr2234@EQU01-PC4324234234 (Mozilla/4.0 (com)) - last seen on 13 August 2017 01:31:11  
 DloX@EDARA-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:02  
 Jncck@MHMOHD-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:01  
 MVQh@KIZANA-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:00  
 bQOOJ@FIX-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:58  
 rzDATA@SERVIDOR-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:58  
 rzDATA@ALEX (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:57  
 GcITa@TECH85 (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:53  
 PiePC@USER-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:52  
 RlvFV@DESKTOP-2TOEC1C (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:47  
 JBLU@TATAKDWI-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:45  
 wainaw@DESKTOP-N67PR0 (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:45  
 tiBudy@DELL-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:44  
 tizYI@SSC-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:10  
 aF5bP@ASUS-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:15  
 YPvBB@THANHTU (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:20  
 HamATA@KLAYANAN-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:46:33  
 bQZSM#3 (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:43:15  
 BkCGV@DAPHILA-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:43:01  
 WYzvVQ@UROS-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:42:32  
 tXcGq@LYAS-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:40:35  
 oLjGz@IASUS (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:40:16  
 ZmsSag@ZMH-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:40:01  
 jPWGwa@CREATIVE (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:40:00  
 FksXDD@BK-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:34  
 TzUja@ISMABEL (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:39:20  
 gDAhG@DESKTOP-J84CPM (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:42  
 HCGze@MEDION-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:37  
 dkInX@MIMI-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:26:26  
 TSUWIP@ALFA-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:48  
 sossca@ANDRIAMAHEFA-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:22  
 HODnO@EMBO (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:20  
 KteE@ELVIS-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:19  
 Ynelus@UNBCO-222 (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:14  
 KxULtX@KO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:11  
 pLHtd@KB-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:09  
 eFKC@NAMCAN-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:09  
 foHlqM@DESKTOP-TKNQCT (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:08  
 tcvUaj@EMMAPORTATL (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:08  
 aKtCa@TREVON (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:05  
 VcGhJ@RODRIGO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:27:16  
 dEAvGm@LAPTOP-9KPS04UH (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:29:10  
 xisaT@LENOVO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:35  
 mZvWlq@PC4-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:34  
 UmHcoX@PC-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:34  
 XwGaYf@YOLO (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:27  
 mwxkX@SUSARIO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:25  
 bshay@ARL-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:24  
 MWHTW@TORRESDARIO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:17  
 dITLd@LENOVO-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:13  
 bYhY@ESBURGERS-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:10  
 xBTW@GONGGONG1-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:08  
 XcvFvH@SHAHMRAD-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:38:02  
 QMwQjs@ENGAMHAD-PC (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:29:11  
 BPKCq@SERVIDORMANIA (Mozilla/5.0 (com)) - last seen on 15 August 2017 20:25:01

This panel looks designed for Banking stuff (webinjects) and POS malware. From XBOT panel you can DL/Exec, Start VNC sessions, socks sessions and update bots:



We can also found some strange "webinjects" stuff:

The image shows the XBOT Panel interface. At the top, there are navigation tabs: Statistics Xbot, XBots, Xbot Commands, Xbot Report (selected), and Settings Xbot. Below these are sub-tabs: Statistics Xbot-Pos, CC Dump, Bin CC Add, and Settings Xbot-POS. The main area is titled "Search Report Datas WebInject ~". It contains search filters for Date (12/08/2017 to 12/08/2017), URL, Content, UHIDs, WebInject (checkbox), Contains (checkbox), and CC (checkbox). There is a "Submit" button and an "Order By" dropdown set to "Receive" with a "Descending" sort order.

Below the search filters is a "Reports ~" section containing a table with the following columns: URL, Browser, UHID, Received, View Content, and Bot Info. The table lists numerous reports, all received 4 days ago. The URLs are primarily from beacons.gvt2.com and beacons.gcp.gvt2.com, with some from facebook.com and youtube.com. The browsers used are Firefox and Chrome. The UHID values are either 14BED1FF2CBB2936050476 or 6B02A11D4DE9232415574.

At the bottom of the table, there are navigation buttons: First, Previous, 1 / 2, Next, Last. Below the table, it says "XBOT Panel @@ Coder By Team NZMR".

where "view content" leads to these kinds of data:

```
POST /domainreliability/upload HTTP/1.1
Host: beacons.gvt2.com
Connection: keep-alive
Content-Length: 1067
Content-Type: application/json; charset=utf-8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8,km;q=0.6
```

q=0.6

Some settings (look at the Alinas 666 status code):

The image shows two screenshots of the XBOT Panel interface. The top screenshot is the 'Settings Xbot' page, and the bottom screenshot is the 'Settings Xbot-POS' page.

**Settings Xbot Page:**

- Update Timeouts (Seconds):** Offline: 1000, Dead: 2592000. Update button.
- Update Database Credentials:** Host: 127.0.0.1, Name: panel, User: panel, Password: [empty]. Update button.
- Update Panel Credentials:** User: admin, Password: [empty], Password Verification: [empty]. Update button.
- Upload WebInjects:** File: Choisissez un fichier | Aucun fichier choisi. WebInjects button.
- Upload Binaries:** x64: Choisissez un fichier | Aucun fichier choisi; x86: Choisissez un fichier | Aucun fichier choisi. Upload button.
- Footer: XBOT Panel @@ Coder By Team NZMR

**Settings Xbot-POS Page:**

Setting Xbot-POS

| Key            | Value                            | Delete?                  |
|----------------|----------------------------------|--------------------------|
| log            | 1                                | <input type="checkbox"/> |
| updateinterval | 240                              | <input type="checkbox"/> |
| successcode    | 666                              | <input type="checkbox"/> |
| cardinterval   | 30                               | <input type="checkbox"/> |
| admin          | 21232f297a57a5a743894a0e4a801fc3 | <input type="checkbox"/> |
| key            | Password1\$                      | <input type="checkbox"/> |
| outkey         | Password1\$                      | <input type="checkbox"/> |

name: [empty] val: [empty]  
Add button

**Dlex**

http://... Currently executed by 0  
Set Delete buttons

Footer: XBOT Panel @@ Coder By Team NZMR

You can also add some bins in the panel database. Currently, they have 8472 Bins in the database. And finally the bot lists (~600 bots if I trust the bots list).

The image shows the XBOT Panel interface. At the top, there are navigation tabs: Statistics Xbot, XBots (selected), Xbot Commands, Xbot Report, Settings Xbot, Statistics Xbot-Pos, CC Dump, Bin CC Add, and Settings Xbot-POS. Below the tabs is a search section with fields for Country Codes, UHIDs, and IPs, and a Submit button. To the right of the search section, there are dropdown menus for Order By (Last Seer) and Descending. The main area is a table of results with the following columns: UHID, IP, Country, OS, Computer, Username, Last Seen, and First Seen. Each row represents a bot, and there is a Command button at the end of each row. The table contains 50 rows of data. At the bottom of the table, there are navigation buttons: First, Previous, 1 / 13, Next, Last. Below the table, there is a footer: XBOT Panel @@ Coder By Team NZMR.

| UHID                    | IP        | Country      | OS                 | Computer        | Username          | Last Seen            | First Seen | Command |
|-------------------------|-----------|--------------|--------------------|-----------------|-------------------|----------------------|------------|---------|
| 24833C8508C12778904926  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | PC2017051811ECK | Administrator     | 2 days ago (Offline) | 3 days ago | Command |
| A7D702CDDA193186266598  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | PC6-PC          | pc6               | 2 days ago (Offline) | 3 days ago | Command |
| D430FFCD6F193186266598  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | GC-20110411XULL | Administrator     | 2 days ago (Offline) | 3 days ago | Command |
| 7FCC06EA05CE3120641781  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | ILYAS-PC        | ILYAS             | 2 days ago (Offline) | 3 days ago | Command |
| 85802524C3383023011859  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | WIN7-PC         | WIN7              | 2 days ago (Offline) | 3 days ago | Command |
| 7C5BF25219F6574217965   | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | THUY-PC         | Thuy              | 2 days ago (Offline) | 4 days ago | Command |
| 899556C881BC3625698399  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | HOSSAM-1A23B6B9 | hossam            | 2 days ago (Offline) | 4 days ago | Command |
| 107D46A08ED42963495975  | 127.0.0.1 | ?? (Unknown) | Windows XP SP2 x86 | HAFID-DEDA7C65A | hafid             | 2 days ago (Offline) | 3 days ago | Command |
| 1CBFD94323DF1942779736  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | KLAYANAN-PC     | K. LAYANAN        | 2 days ago (Offline) | 4 days ago | Command |
| 781CC7ACAS801019693163  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | ASAS4EVER       | AsAs              | 2 days ago (Offline) | 3 days ago | Command |
| 71D3A00292263528003197  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | ENGHAMAD-PC     | Engahmad          | 2 days ago (Offline) | 3 days ago | Command |
| 0FF9222150CD244771074   | 127.0.0.1 | ?? (Unknown) | Windows XP SP4 x86 | MERKEN          | Merken            | 2 days ago (Offline) | 4 days ago | Command |
| FE2AADD4BE681681895587  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | TTTTTTTTTTTTTTT | Ayman             | 2 days ago (Offline) | 3 days ago | Command |
| 67F12D6F44AB525370364   | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | ITOP-PC         | itop              | 2 days ago (Offline) | 3 days ago | Command |
| 28BC041402A82768236643  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | KUCA            | pedja             | 2 days ago (Offline) | 3 days ago | Command |
| AB072ED814C3897250831   | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | SERVIDOR-PC     | SERVIDOR          | 2 days ago (Offline) | 3 days ago | Command |
| 8FA61331615D20702611826 | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | KWORLDPRINTER   | Owner             | 2 days ago (Offline) | 3 days ago | Command |
| 26044109BC752040409402  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | BAKLAJAN-PC     | Baklajan          | 2 days ago (Offline) | 3 days ago | Command |
| A9FBE6FF19BB2936050476  | 127.0.0.1 | ?? (Unknown) | Windows XP SP2 x86 | MISHO           | abo nassar        | 2 days ago (Offline) | 3 days ago | Command |
| C72A4B5026041622379703  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | UNBCO-222       | Matbakh           | 2 days ago (Offline) | 3 days ago | Command |
| C29E045DB7291301979414  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | ALMADINATELECOM | al madina telecom | 2 days ago (Offline) | 4 days ago | Command |
| 58686E9151BD20379026    | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | FANNAN-PC       | Fannan6           | 2 days ago (Offline) | 3 days ago | Command |
| 512925D91291301979414   | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | LIGHT-SP3       | Administrator     | 2 days ago (Offline) | 3 days ago | Command |
| 2DF525D67B5A650445529   | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | SERVIDORMANIA   | servidormania     | 2 days ago (Offline) | 3 days ago | Command |
| 22C1084764C34158135236  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | LENOVO-PC       | lenovo            | 2 days ago (Offline) | 3 days ago | Command |
| C83E083B47171806970752  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | FIX-PC          | fix               | 2 days ago (Offline) | 3 days ago | Command |
| FC1577847298340779059   | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | DQ0411VOW       | BNComputer        | 2 days ago (Offline) | 3 days ago | Command |
| 0500647B61572876534592  | 127.0.0.1 | ?? (Unknown) | Windows XP SP2 x86 | USER7           | Zovq              | 2 days ago (Offline) | 3 days ago | Command |
| DD80CCE999551497239002  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | BAKEER-PC       | bakeer            | 2 days ago (Offline) | 3 days ago | Command |
| 9677CFEB0947465854224   | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | USER-PC         | User              | 2 days ago (Offline) | 3 days ago | Command |
| 83265B7005242148772887  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | EGLALL-PC       | eglall            | 2 days ago (Offline) | 3 days ago | Command |
| 47FED7EACECE3120641781  | 127.0.0.1 | ?? (Unknown) | Windows 10 x64     | HRISIPC         | Hrisi             | 2 days ago (Offline) | 3 days ago | Command |
| A76E7E19B9052312027626  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | ADMIN-PC        | Admin             | 2 days ago (Offline) | 3 days ago | Command |
| A1005EE591713576850798  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | JIMMI32H-PC     | Jimmi32h          | 2 days ago (Offline) | 3 days ago | Command |
| EFEC516A3C4E981579381   | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | ORIENT          | Administrator     | 2 days ago (Offline) | 3 days ago | Command |
| 1CECD00953752040409402  | 127.0.0.1 | ?? (Unknown) | Windows XP SP2 x86 | SICOWIN         | mohamed           | 2 days ago (Offline) | 3 days ago | Command |
| DDAB784F688B4293944220  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | RADIOPONGAIFM   | RADIO PONGAI FM   | 2 days ago (Offline) | 3 days ago | Command |
| 7C78721400A82768236643  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | VENTAS3-PC      | ventas3           | 2 days ago (Offline) | 3 days ago | Command |
| 9140DFE78F632545466276  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | THEBROTHERS-PC  | The Brothers      | 2 days ago (Offline) | 3 days ago | Command |
| EA52608EAC523740105281  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | NAMCAN-PC       | NamCan            | 2 days ago (Offline) | 3 days ago | Command |
| 500603015AAD1904665954  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | USER-PC         | User              | 2 days ago (Offline) | 3 days ago | Command |
| 4010F6125FB63799621165  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | NOUR            | Administrator     | 2 days ago (Offline) | 4 days ago | Command |
| 86D063FC27502360809691  | 127.0.0.1 | ?? (Unknown) | Windows XP SP2 x86 | ESSAM           | Essam             | 2 days ago (Offline) | 3 days ago | Command |
| 6038A958A7CC1758188687  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | SONY-PC         | sony              | 2 days ago (Offline) | 3 days ago | Command |
| D6048BA028D42963495975  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x86  | MEDION-PC       | evenx             | 2 days ago (Offline) | 3 days ago | Command |
| 24CCBCF930E51768856970  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | SEATEL-PC       | SEATEL            | 2 days ago (Offline) | 4 days ago | Command |
| 0232D6D41F681681895587  | 127.0.0.1 | ?? (Unknown) | Windows 7 x86      | PDV-PC          | pdv               | 2 days ago (Offline) | 3 days ago | Command |
| 850CBAC7C3432002295620  | 127.0.0.1 | ?? (Unknown) | Windows 10 x64     | DESKTOP-TPP91TT | Furkan            | 2 days ago (Offline) | 3 days ago | Command |
| 3AB9019FEF581340093196  | 127.0.0.1 | ?? (Unknown) | Windows 7 SP1 x64  | PARKOTO         | PARK OTO          | 2 days ago (Offline) | 3 days ago | Command |
| A298E5E054144033060071  | 127.0.0.1 | ?? (Unknown) | Windows XP SP3 x86 | DC204           | xlshen            | 2 days ago (Offline) | 4 days ago | Command |

I've uploaded the whole list of bots on [this album](#). Ping me if you're on the list :D I'm really curious to see the binary part And finally the database structure reminds again Alina: By this way we will find soon more Alina forks than Zeus forks \o/ So, NOPE! it's not a super new next gen POS malware, it's just another Alina Fork :D but this webinjects part looks curious :) and the team seems very active. But come one, 3k\$ for open sourced malware haha...

Thanks for your time, thanks to Xylitol and happy hunting :) IOCs:

- <http://thzsmrjqqzpaz2mz.onion.link/a1/Spark.exe> (Alina)
- <http://thzsmrjqqzpaz2mz.onion.link/payload.exe> (Neutrino)
- <http://thzsmrjqqzpaz2mz.onion.link/at/files/us.exe> (Atmos)



<http://22klzn6kzjwlmt2.onion.link/al/Spark.exe> (Alina)  
<http://22klzn6kzjwlmt2.onion.link/al/payload.exe> (Neutrino)  
<http://22klzn6kzjwlmt2.onion.link/al/files/us.exe> (Atmos)  
<http://netco1000.ddns.net> <http://netco400.ddns.net/Dia> (Gorynch)  
<http://netco400.ddns.net/at/>(Atmos)  
[e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525](http://e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525) (atmos)  
[26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298](http://26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298) (Alina)  
[8a62f61c4d11d83550ab4baceb9b18d980a4c590723f549f97661a32c1731aff](http://8a62f61c4d11d83550ab4baceb9b18d980a4c590723f549f97661a32c1731aff) (neutrino)