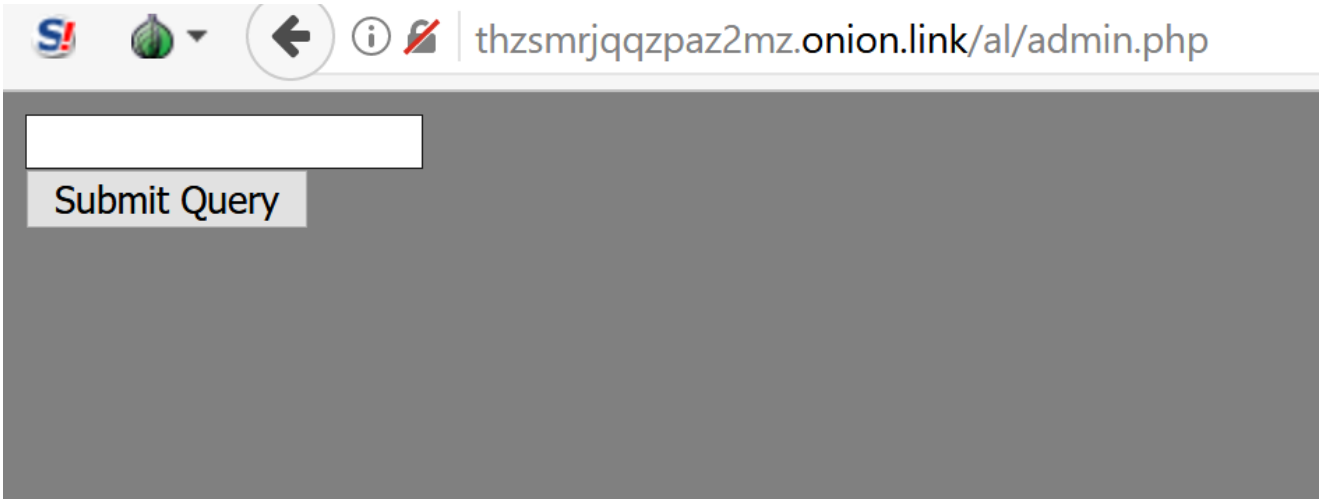
Quick look at another Alina fork: XBOT-POS

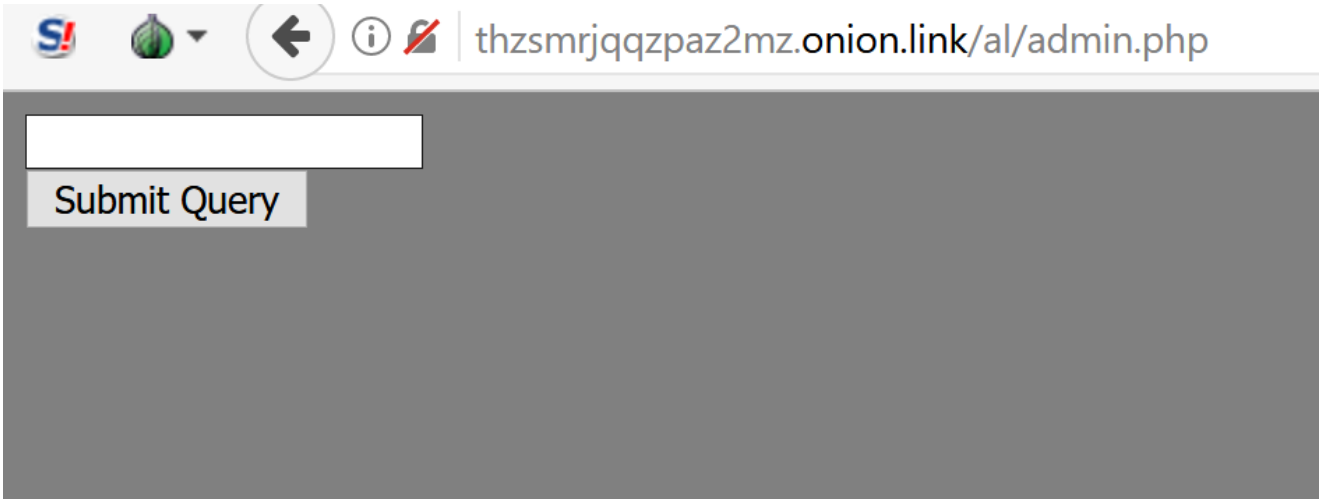
benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html



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

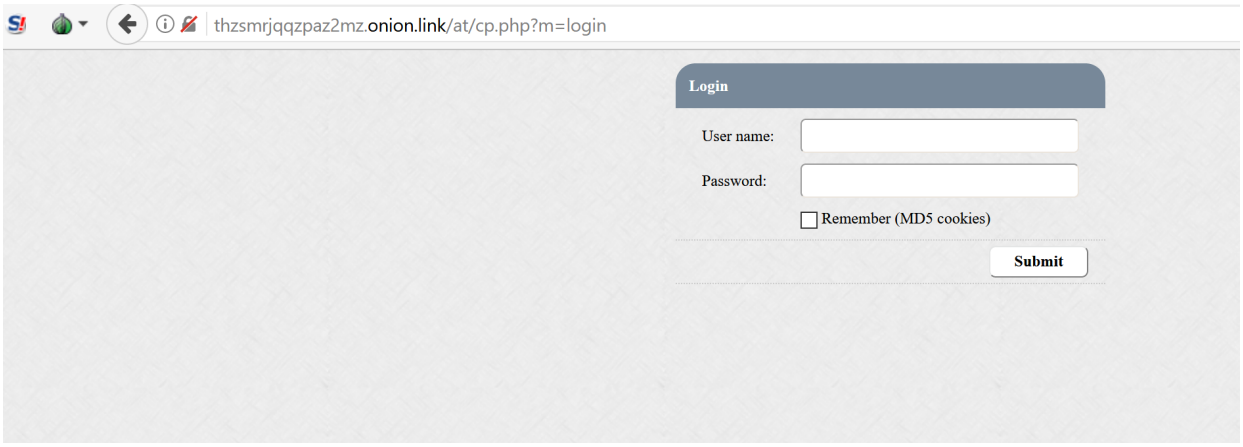
> Alina: https://t.co/ttyh5aEJDX
> C2:thzsmrjqqzpaz2mz[.]onion[.]link/al/loading[.]php,t[.]ht/al/loading[.]php,
>
> — ScumBots (@ScumBots) 15 août 2017

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 `thzsmrjqqzpaz2mz.onion.link/al/loading.php`. Samples: `26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298 (http://thzsmrjqqzpaz2mz.onion.link/al/Spark.exe)`



In the same boring way, we can found:

- a Fareit/Pony panel at `https://thzsmrjqqzpaz2mz.onion.link/pn/admin.php` (I don't have sample)
- an Atmos at `https://thzsmrjqqzpaz2mz.onion.link/at/cp.php` : Sample e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525 (https://thzsmrjqqzpaz2mz.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://22klzn6kzjlwlmt2.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://thzsmrjqqzpaz2mz.onion.link/ed2/` without success...

BLOCKCHAIN WALLET CHARTS STATS MARKETS API Search fo

Bitcoin Address Addresses are identifiers which you use to send bitcoins to a

Summary	
Address	1Dh6zY9U1V3XJELDh8hQdox3eR765XyR4H
Hash 160	8b372656bc83a0238ac5abbec5e3e22da68ae338
Tools	Related Tags - Unspent Outputs

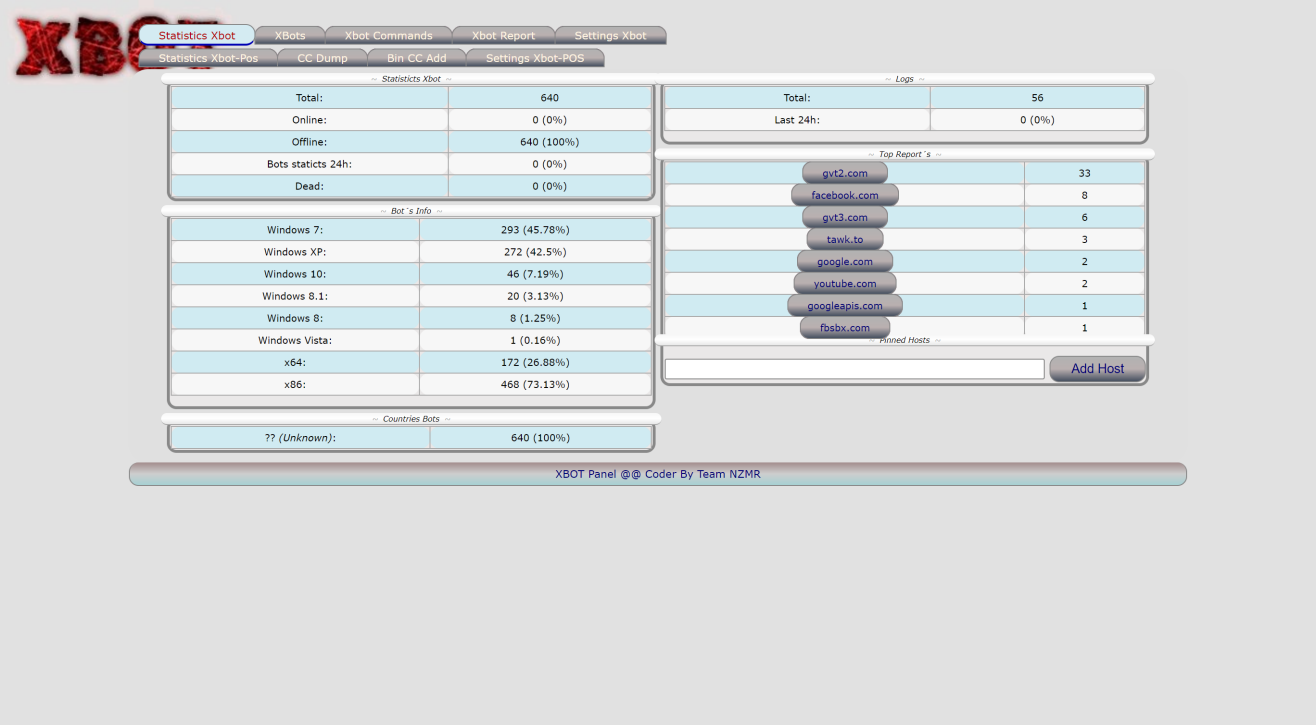
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

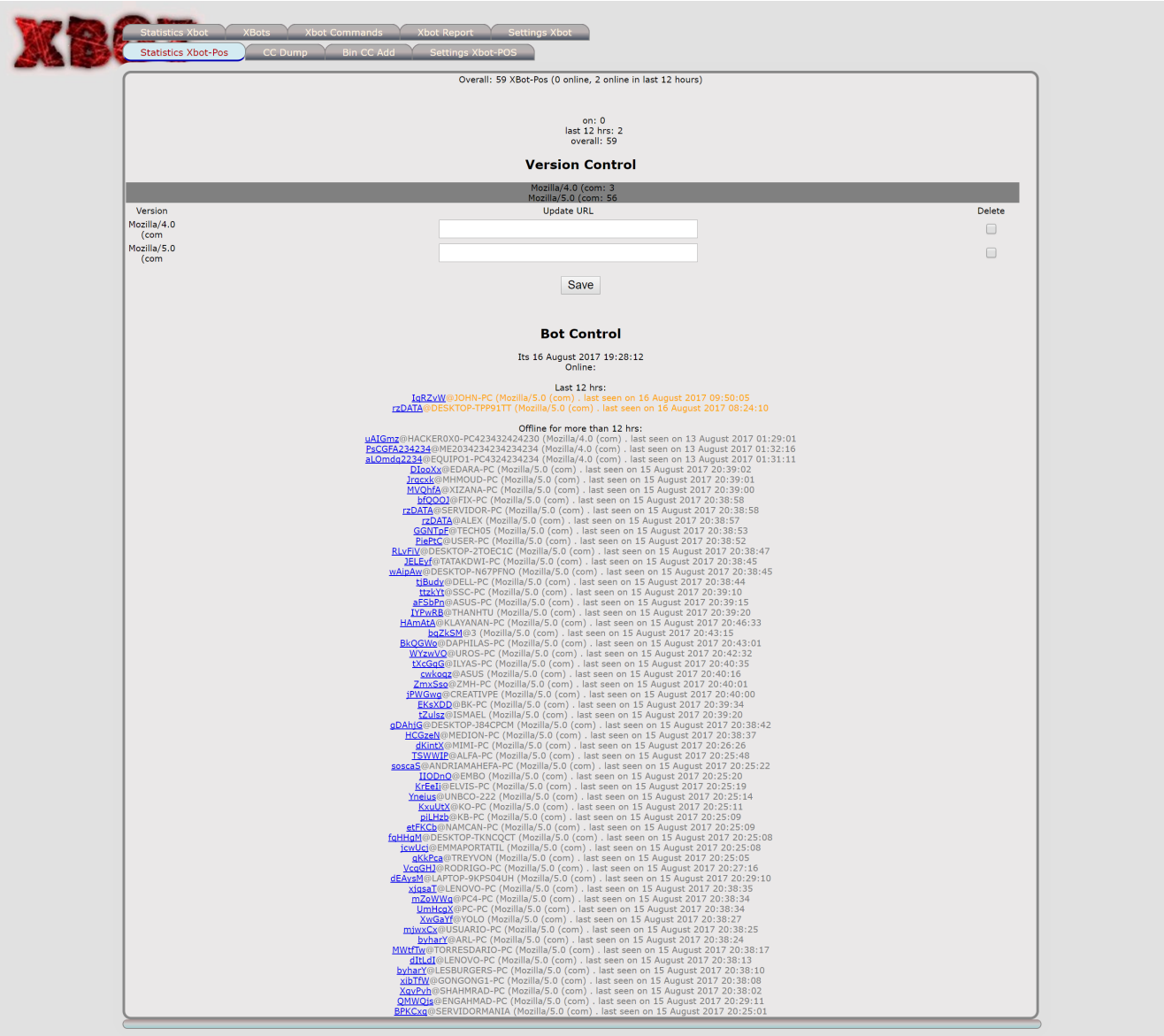
No transactions found for this address, it has probably not been used on the network yet.

But I've write this quick blog post for the last panel, Let me introduce you XBOT panel \o/: `https://thzsmrjqqzpaz2mz.onion.link/panel/` (click to enlarge)

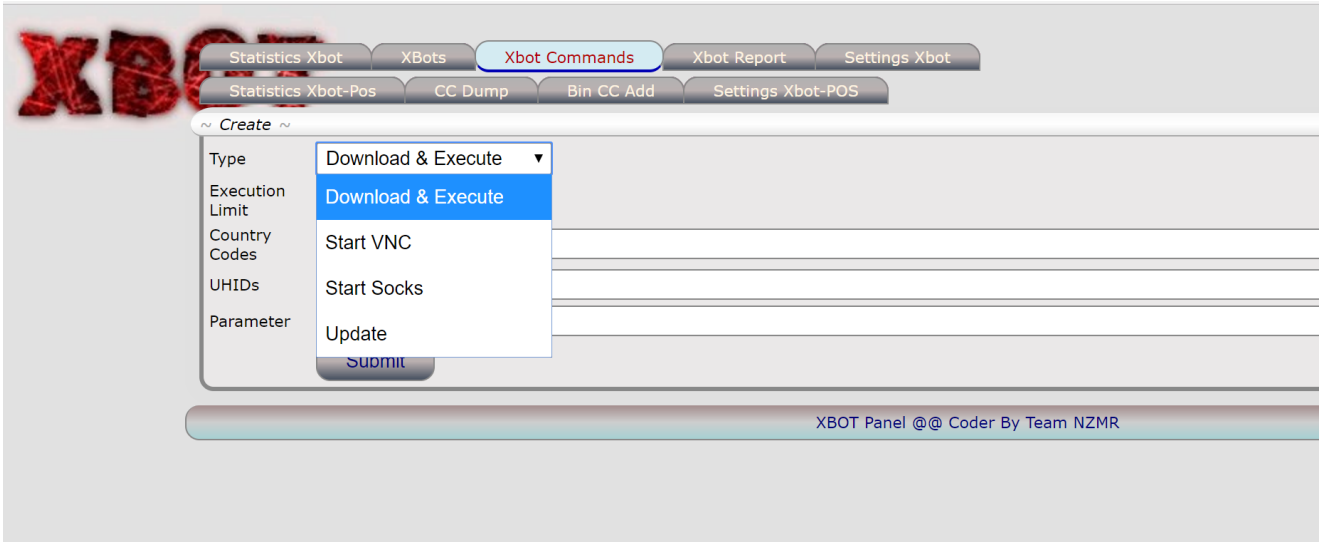


The bot ad: `Selling xbot ,new bank trojan -- Modules -- Webinject -- Formgrabber -- Socket4/5 -- Hidden VNC New bot bank xbot is available for rent (800$/monthly) -- server on tornetwork/clearnet Customized programming service and web developer/c/c++/Python/NET/others Team Coder/NZMR xbot costs 3k $ 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`

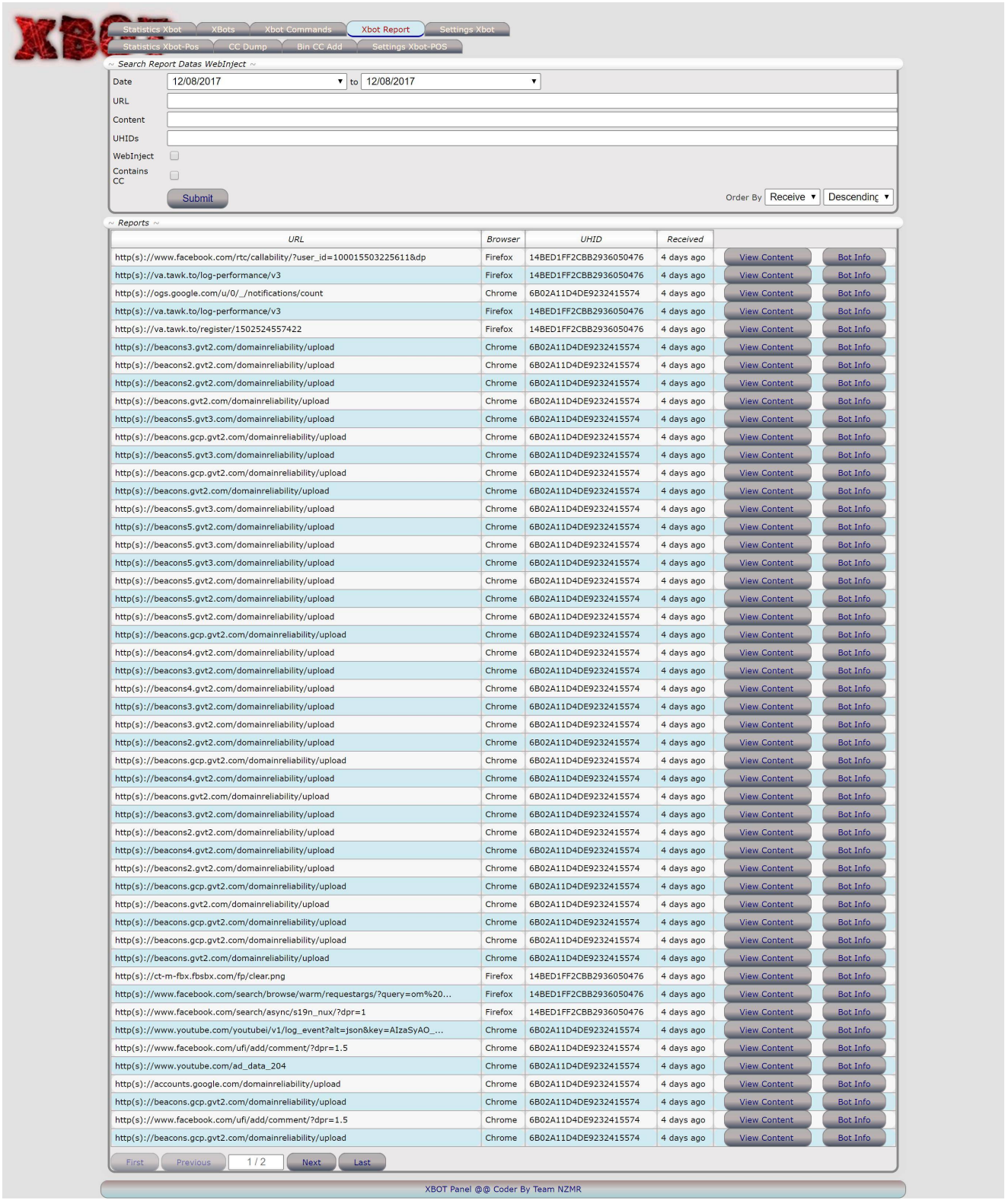
`$ (you choose,with or without support) [+] - Update bot for new version 400 $ [+] Rent xbot Panel access (Clearnet/Tornetwork) Bin (exe) Socket.exe/hvnc.exe Priçe 800 $ monthly (First 6 customers, others 1k $) Support monthly 100 $ (btc)` I don't have any sample yet but if you have one, i'm REALLY interrested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



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:

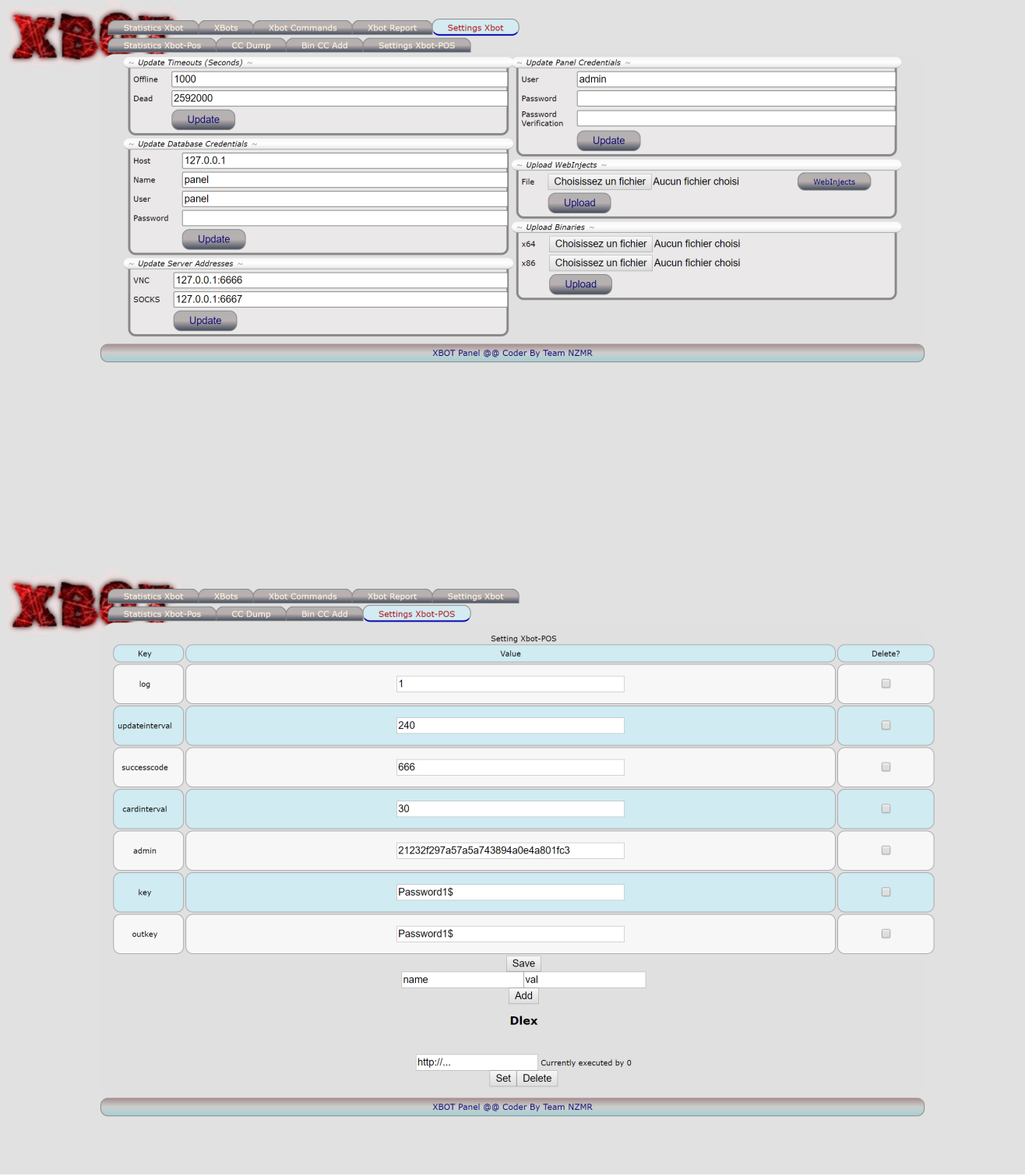


where "view content" leads to these kinds of data:

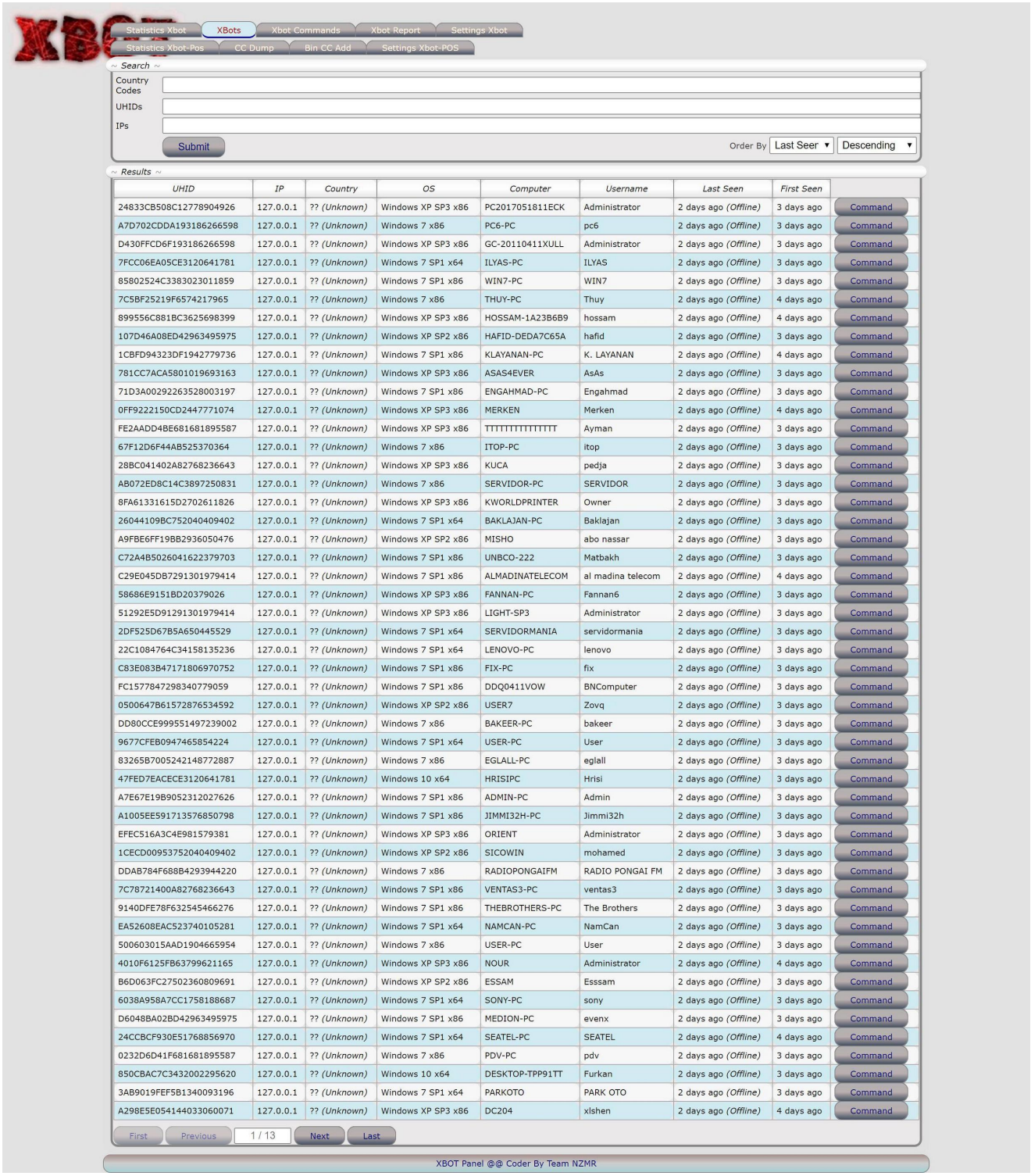
```
POST /domainreliability/upload HTTP/1.1
Host: beacons.gvt2.com
Connection: keep-alive
Content-Length: 1067
Content-Type: application/json; charset=utf-8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36
Accept-Encoding: gzip, deflate,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



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).



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/al/Spark.exe (Alina)
http://thzsmrjqqzpaz2mz.onion.link/payload.exe (Neutrino)
http://thzsmrjqqzpaz2mz.onion.link/at/files/us.exe (Atmos)
```

```
http://22klzn6kzjlwlmt2.onion.link/al/Spark.exe (Alina)
http://22klzn6kzjlwlmt2.onion.link/al/payload.exe (Neutrino
http://22klzn6kzjlwlmt2.onion.link/al/files/us.exe (Atmos)
http://netco1000.ddns.net http://netco400.ddns.net/Dia (Gorynch)
http://netco400.ddns.net/at/(Atmos)
e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525 (atmos)
26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298 (Alina)
8a62f61c4d11d83550ab4baceb9b18d980a4c590723f549f97661a32c1731aff (neutrino)
```