

## Quick look at another Alina fork: XBOT-POS

Archived: 2026-04-05 20:40:11 UTC

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](#)

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.

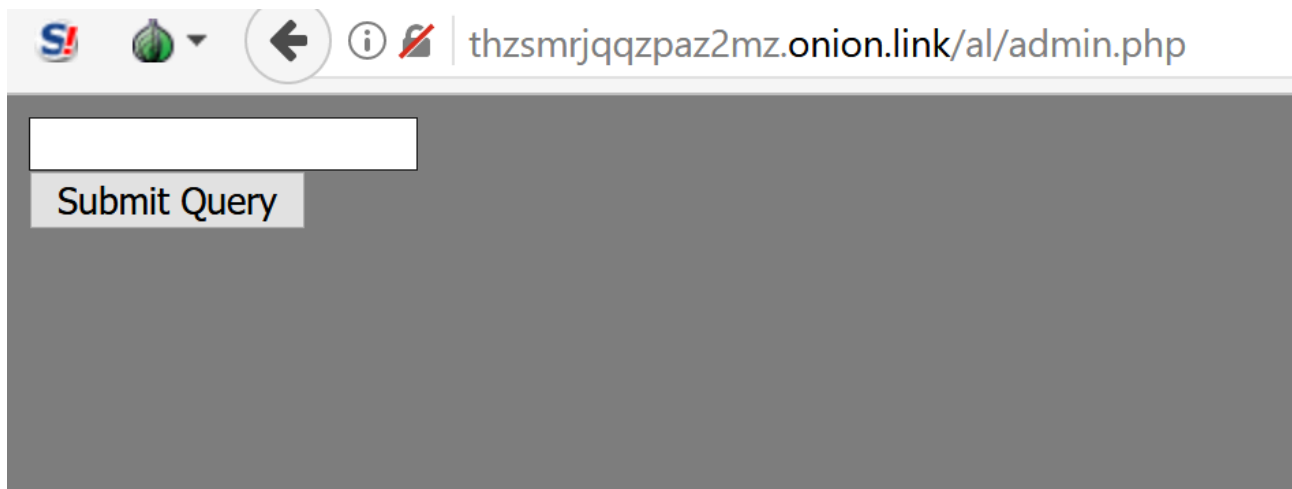
Let's have a look on this server.

As we know, we have an Alina ([Well known POS malware](#)) panel at

thzsmrjqzpz2mz.onion.link/al/loading.php .

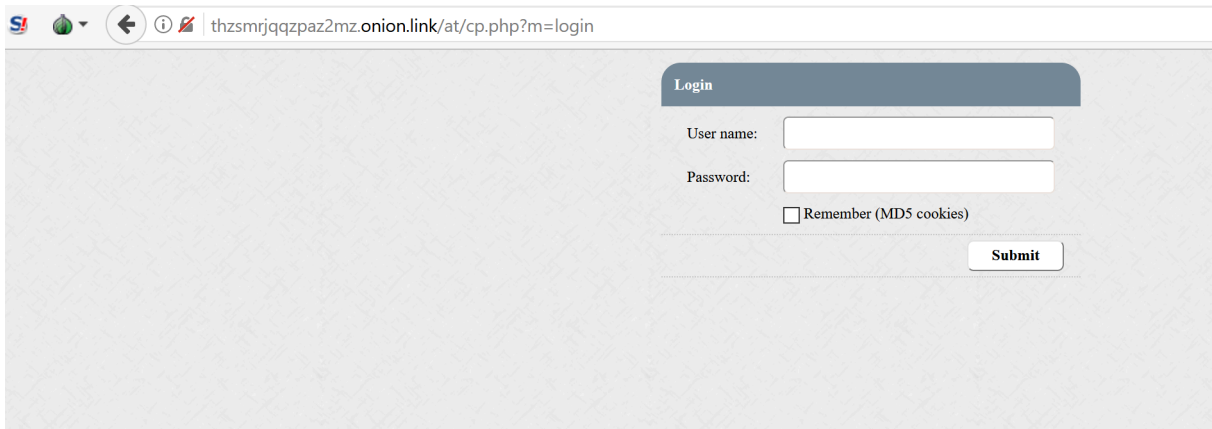
Samples: 26aa9709d0402157d9d36e4849b1f9bacecd8875169c7f26d7d40c5c0c3de298

(<http://thzsmrjqzpz2mz.onion.link/al/Spark.exe>)



In the same boring way, we can found:

- a Fareit/Pony panel at <https://thzsmrjqzpz2mz.onion.link/pn/admin.php> (I don't have sample)
- an [Atmos](#) at <https://thzsmrjqzpz2mz.onion.link/at/cp.php> :  
Sample e34720cc8ab3718413064f19af5cc704e95661e743293a19f218d3b675147525  
(<https://thzsmrjqzpz2mz.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://22klzn6kzjwlmt2.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://thzsmrjqzpz2mz.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](#)

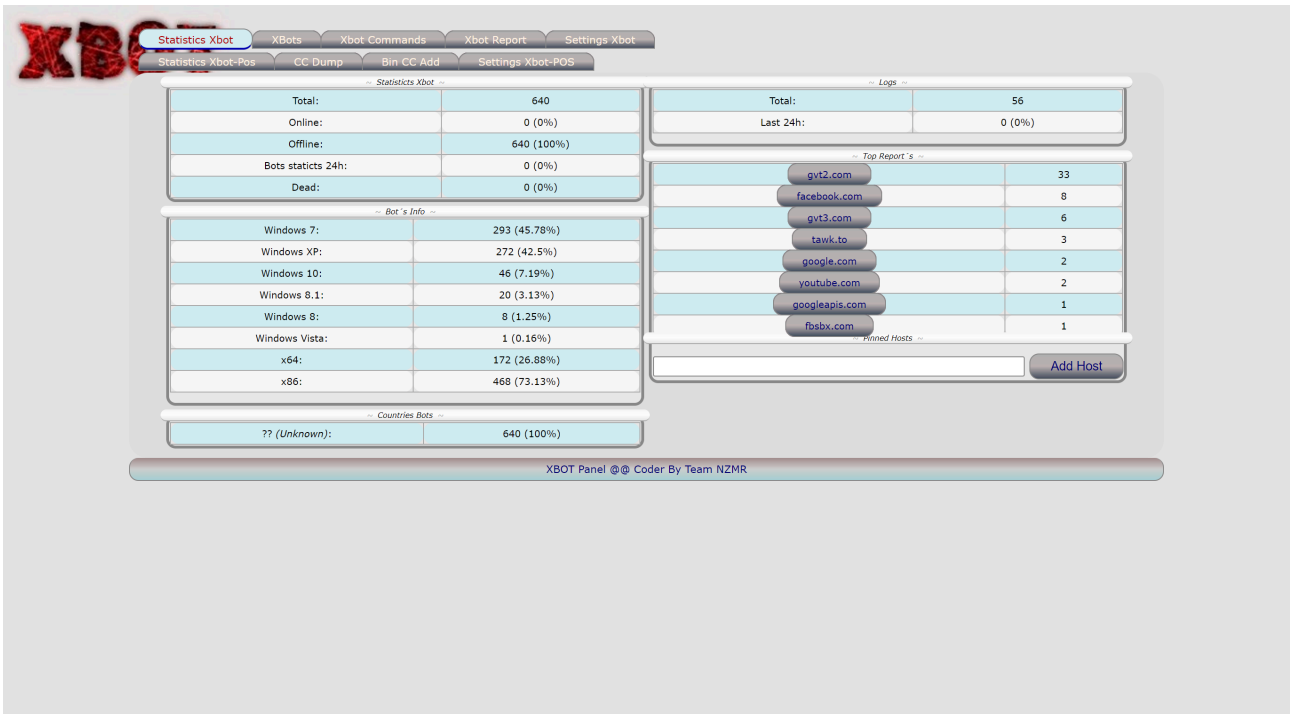
### Transactions (Oldest First)

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://thzsmrjqzpz2mz.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":

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:



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

XBOT Panel @@ Coder By Team NZMR

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"/>

Save  
name val  
Add  
**Dlex**  
http://... Currently executed by 0  
Set Delete

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 screenshot shows the XBOT Panel interface. At the top, there are navigation tabs: Statistics Xbot, XBots, Xbot Commands, Xbot Report, Settings Xbot, Statistics Xbot-Pos, CC Dump, Bin CC Add, and Settings Xbot-POS. Below these is a search section with fields for Country Codes, UHIDs, and IPs, and a Submit button. The main area displays a table of results with columns: UHID, IP, Country, OS, Computer, Username, Last Seen, and First Seen. Each row represents a bot and includes a Command button. The table contains 70 rows of data. At the bottom, there are navigation buttons: First, Previous, 1 / 13, Next, and Last. A footer note reads: XBOT Panel @ Coders By Team NZMR.

UHID	IP	Country	OS	Computer	Username	Last Seen	First Seen	Command
24833CB508C12778904926	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
899556C8818C3625698399	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-DEDA7CG5A	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
781CC7ACA5801019693163	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 SP3 x86	MERKEN	Merken	2 days ago (Offline)	4 days ago	Command
FE2AAD04BE681681895587	127.0.0.1	?? (Unknown)	Windows XP SP3 x86	TTTTTTTTTTTTTT	Ayman	2 days ago (Offline)	3 days ago	Command
67F12D6F44A8525370364	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
AB072ED8C14C3897250831	127.0.0.1	?? (Unknown)	Windows 7 x86	SERVIDOR-PC	SERVIDOR	2 days ago (Offline)	3 days ago	Command
8FA61331615D2702611826	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
A9FBE6FF198B2936050476	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
59686E91518D20379026	127.0.0.1	?? (Unknown)	Windows XP SP3 x86	FANNAN6	Fannan6	2 days ago (Offline)	3 days ago	Command
51292E5D91291301979414	127.0.0.1	?? (Unknown)	Windows XP SP3 x86	LIGHT-SP3	Administrator	2 days ago (Offline)	3 days ago	Command
2DF525D678A560445529	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	DDQ0411VOW	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	egllall	2 days ago (Offline)	3 days ago	Command
47FED7EACECE3120641781	127.0.0.1	?? (Unknown)	Windows 10 x64	HRISIP	Hrisi	2 days ago (Offline)	3 days ago	Command
A7E67E19B9052312027626	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	RADIO PONGAI FM	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
4010F6125F863799621165	127.0.0.1	?? (Unknown)	Windows XP SP3 x86	NOUR	Administrator	2 days ago (Offline)	4 days ago	Command
B6D063FC2750236809691	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
D6048BA02BD42963495975	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
3AB9019FEF5B1340093196	127.0.0.1	?? (Unknown)	Windows 7 SP1 x64	PARKOTO	PARK OTO	2 days ago (Offline)	3 days ago	Command
A2985E054144033060071	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://thzsmrjqzpz2mz.onion.link/al/Spark.exe> (Alina)  
<http://thzsmrjqzpz2mz.onion.link/payload.exe> (Neutrino)  
<http://thzsmrjqzpz2mz.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)

---

Source: <https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html>