



IT ARMY OF UKRAINE

<https://t.me/itarmyofukraine2022>

itarmyua@gmail.com

Behaviour in chatrooms, potential malicious scripts, policies and what to look out for.



Version	Author	Release date	Changes/comments
1.1	Hactic	21.03.2022	First release



Protect yourself

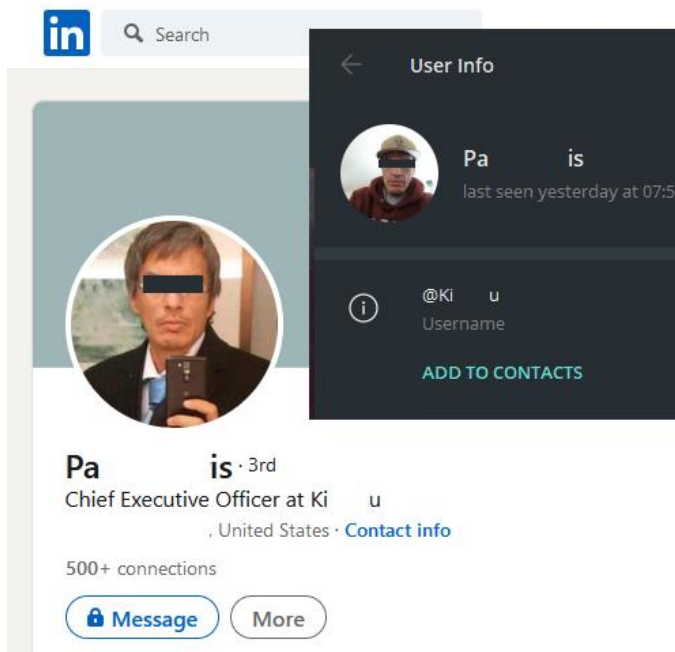
Chatting in channels and chat rooms is really nice. You get to meet a lot of people and you get to share a lot of information. It almost feels like home. And like at home, you tend to let your guard down if things get cozy and familiar. When you spend a lot of time in chat rooms you get to know all the key players and you think you know who is who.

But, like many things in life, looks can be deceiving. So please follow the rules below to stay safe. These rules do not just apply to the IT Army of Ukraine channels and chats, it's just good practice to do this in every single chat room, newsgroup or channel you will ever visit on this planet in your life from now on.

Please don't share your personal information with anyone regardless what you're working on or the topics you're discussing. Even in DM. Use your common sense when somebody ask you for personal information. Protect your anonymity as much as you can. Here are a few rules that sounds trivial but are so important:

- * Don't give out your personal address.
- * Don't give your real name or use your real name in your profile.
- * Don't tell the country you're from.
- * Don't give them your phone number or e-mail address.
- * Don't use your real picture in your profile.
- * Set a strong password with 2FA or MFA

Unfortunately, many people still join Telegram under their own account and name. You're so easy to find, not just by the opponent but also by law enforcement.



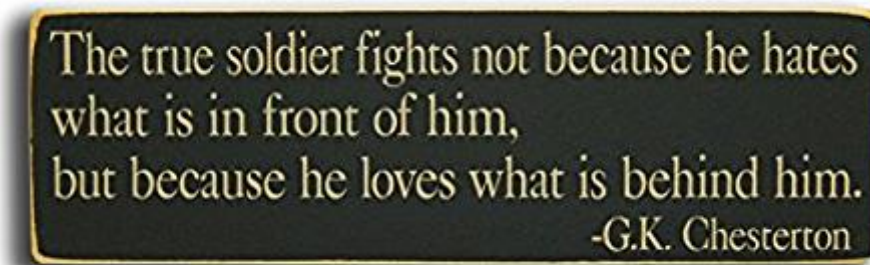


Policies

We have many discussion about what targets to go after in our chat rooms. Our targets are set by the Ukrainian government and we don't invent our own targets. All attacks and testing is done in close liaison with those who are responsible for the target list. We strongly discourage you to attack anything that may cause direct physical injury to civilians or put their lives at risk. Amongst them are, but not limited to:

- Nuclear power plants (we don't want a meltdown causing a global disaster)
- Hospitals
- Elderly homes
- Orphanages
- Schools (not being universities)
- Pharmacies

We are very well aware that the Russian don't play by these rules and that it may cause strong emotions and a need for revenge with some people and we don't blame them. However, if we would allow such thinking or condone these actions, where would that leave us? We would be just like them and we're much, much better than that.

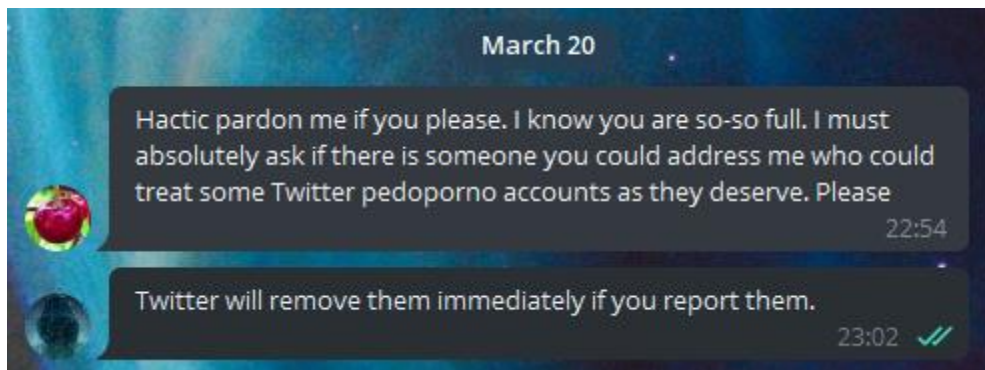
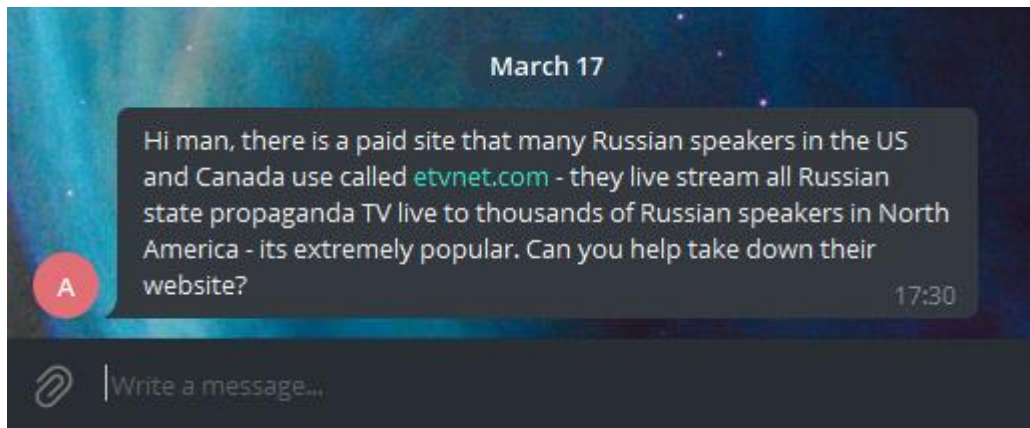


It is not allowed to post links from other channels, Telegram or any other media platform in the IT Army of Ukraine channels. We don't want splinter cells as this diminishes the striking force of the army. We should all stick together and attack the same targets at the same time. That is when we're most effective which we have proven time and time again.



Administrators

We have administrators that are extremely busy with the target lists, the pen testers, the DDoS'ers, communications, news, media, defensive actions, special projects, documentation, checking and writing scripts and programs and loads of other stuff. They do not have the time to teach you in person how to hack nor to help and assist you with personal projects that you've kicked off in your shed. Every minute that you spend in an administrators DM asking a question that could have easily be found by a simple DuckDuckGo search on the internet is time the administrator could've spend on something else. They're also not DJ's, they don't take requests.



That doesn't mean you can't ask questions. On the contrary. If you have a question, or you are just curious about something, you can ask in the chat and there are many very friendly and knowledgeable people that will answer your question and will help you find the answer you're looking for.



You can always talk to an administrator if you really need to, if you have important information, such as trolls or spies or other information that needs to be dealt with or processed immediately. They will take all the time in the world to listen to you and try to sort things out.

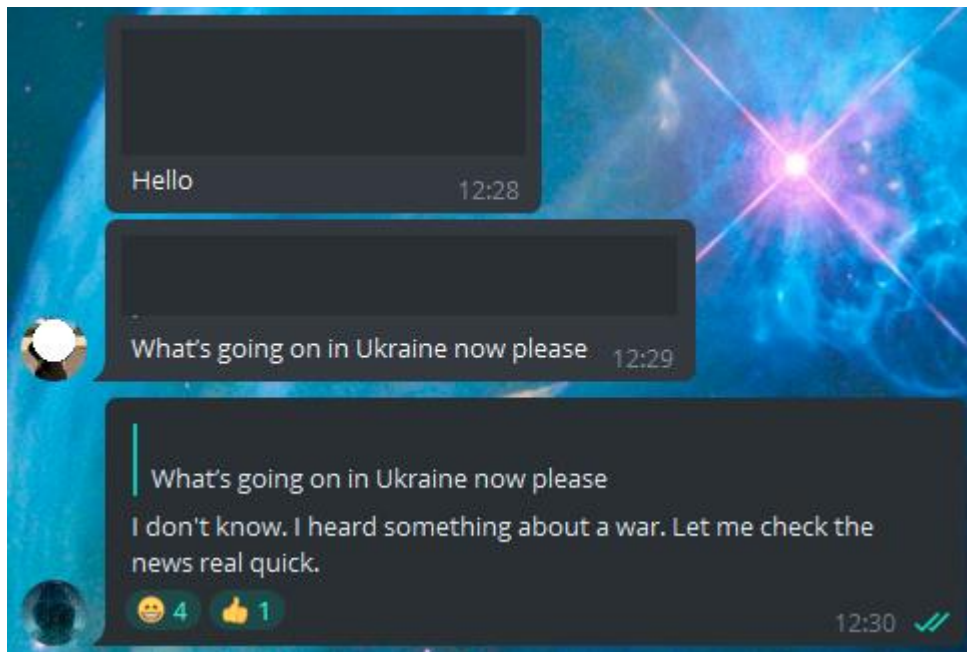
Please be aware that due to the workload their response time is not very quick.

Trolls and other undesirables

We know for sure that trolls and Russian spies have infiltrated the channels and chats. Although we have a highly moderated group with administrators that are doing an excellent job weeding out any trolls, spies and fake messages they can find, there is always the possibility that one slips past. Our enemy has launched a new malware campaign which takes advantage of all the good guys wanting to help the IT Army of Ukraine cyber warfare against him.

How do you recognize a troll?

Internet trolls are in it for the chaos. The main purpose of trolling is to stir up trouble and get a chain reaction of negative comments from other people. Chances are, trolls don't really even believe what they're saying – they just want to cause a little mayhem and disrupt the normal flow of operations. This can mean anything from luring people into silly, meaningless discussions (can someone please clarify if my computer runs faster on methane generated energy?) to posting purposely offensive, controversial or ignorant opinions. Please report this kind of behavior immediately to an administrator.



Trolls are kicked and banned from the channel immediately.



How do you recognize a spy?

Now this is a bit more challenging. Unlike trolls, spies are trained to gather information by being friendly to you, mislead you and trick you into revealing sensitive information. Questions like:

“Can you please tell me how the targets are selected and could you please walk me through the process?” are asked to admins on a daily base. It’s not a normal question.

If you believe that someone is asking you something inappropriate relative to the tasks at hand, you may be dealing with a pro-Russian sympathizer and this should trigger your internal alarm system. It’s not appropriate if someone asks you *“which country are you from and in which city do you live in?”*

There are more trolls and spies emerging as we grow bigger and we need to weed them out. Don't just report or block anyone who is generally interested in you, just use your common sense and be careful. Don't become paranoid though, always try to be friendly with people.

Again, when in doubt ask your administrator.

Scripts and programs

As you have probably have noticed, there are a lot of people offering self-made scripts and/or services in order to try and help those who don't have a proper IT education or background.

Although many of the developers mean well and truly try to help people along, there are trolls in the groups that try to diminish the IT Army's effectiveness by spreading scripts and programs that essentially do nothing or even may seriously harm your computer. We have even discovered scripts that de-anonymize you and expose your true digital identity to the outside world.

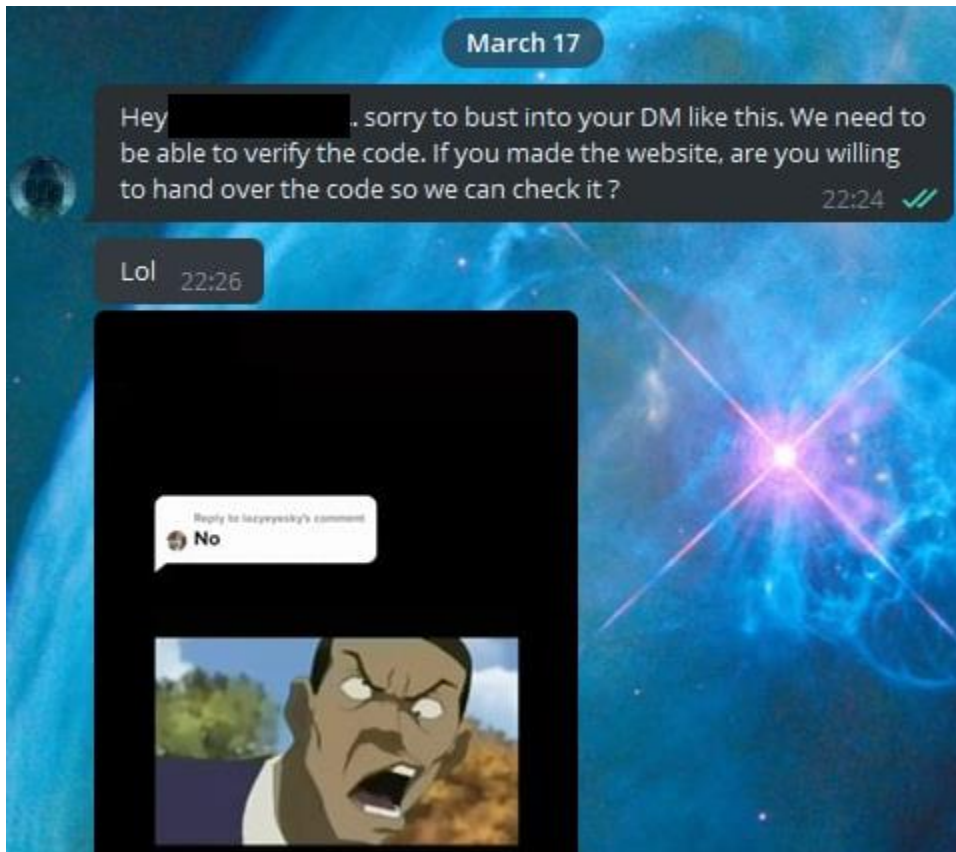
The power of the IT Army of Ukraine lies in attacking targets at the same time by as many people as possible for as long as possible. The target lists are known and pinned to the channels. They are carefully selected by our central team to maximize impact and distributed by several sister channels. As an individual it's difficult to identify and select meaningful targets. Just picking a random site that ends with *.ru* is simply not enough. That is why centralized target lists exist. Please stick to them.

The IT Army of Ukraine distributes scripts that are effective and work safely. These scripts are reviewed on a daily base and if needed, replaced. Using unsupported scripts is entirely at your own risk. Always test unknown scripts in a VM to avoid major disappointment. (Read: all your sensitive data being wiped). We are working extremely hard behind the scenes to create a safe environment for all of you. New versions of the beginner's manual are distributed regularly with newly added scripts that passed our scrutiny.



Please DO NOT just install a tool or script that is presented to you via links. Although most of the programmers in here are very talented and skilled and produce excellent and well written scripts that help the war effort, we simply cannot take the risk that a malicious script makes it into our systems and your computer.

- Be extremely careful with executing scripts or programs you don't know or never heard of.
- ALWAYS use a virtual machine (VM, or VirtualBox on Kali) to test a new script. No exceptions. Seriously.
- If it's a closed source program, always scan it for viruses before you execute it in a VM.
- Always report if you smell something fishy. We are all fighting for the same cause.
- Occam's razor. If it looks like a troll, smells like a troll, talks like a troll... It usually IS a troll. Report him/her to a chat administrator and they will figure it out.
- Last but not least... When in doubt, always contact an administrator.





Cyber security is a serious business and you cannot let your guard down, ever. You need to adhere to the rules above or this may not be the right field for you and there are other ways of helping the war effort. If you follow the rules you will stay alive to fight another day together with all the great guys and gals from the awesome IT Army of Ukraine!

We're so proud of all of you for what we've achieved already. We all play our tiny role in this huge machine and every single cog is important. Without YOU, we'd be lost and doomed. Keep up the amazing work that every single one of you is doing!!