Hacktivists Call for Release of Telegram Founder with #FreeDurov DDoS Campaign

blog.checkpoint.com/security/hacktivists-call-for-release-of-telegram-founder-with-freedurov-ddos-campaign/

September 4, 2024

In recent weeks, a new hacktivist campaign has emerged to demand the release of Telegram CEO Pavel Durov, after his arrest by French authorities. In this report, Check Point Research explores the most prominent and dominant hacking groups involved in the campaign.

- On August 24, in response to the French authorities' arrest of Telegram CEO Pavel Durov, hacktivist groups started a hacking campaign called #FreeDurov or #OpDurov
- Among the first groups to react were pro-Russian People's Cyber Army of Russia and pro-Islamic RipperSec, with both groups posting on their channels on the day of the arrest to initiate the campaign
- In the following days, dozens of hacktivists groups joined the effort, collaborating to attack more than 50 targets in France, primarily with distributed denial of service (DDoS) attacks.

Participating Groups

Cyber Army of Russia Reborn (CARR)

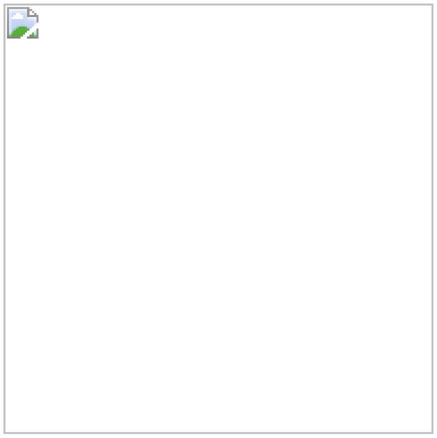
The CARR, Cyber Army of Russia Reborn AKA Russian Cyber Army Team, telegram channel was created in March 2022 shortly after the war between Russia and Ukraine began. The group primarily targets Ukraine and its allies with DDoS attacks. Previously, this group has performed significant attacks, such as compromising SCADA systems of water utilities in the United States, Poland, and France. Most recently, CARR was sanctioned by the US State Department for attacking US and Europe critical infrastructure. The group is affiliated to the Russia's military intelligence service and the Russian GRU-related Sandworm group.

As of September 3, 2024, CARR's main telegram channel has 62,181 members.

After announcing the operation #FreeDurov on August 24, AT 22:23 with a post on their channel, CARR began targeting French organizations with DDoS attacks.

The list of targets that were published on CARR's channel is following:

- santre.fr (August 25)
- aldo-carbonde.ademe.fr (August 25)
- sayne.fr (August 26)
- coe.int (August 26) (Together with CyberDragon group)
- cnrs.fr (August 27)



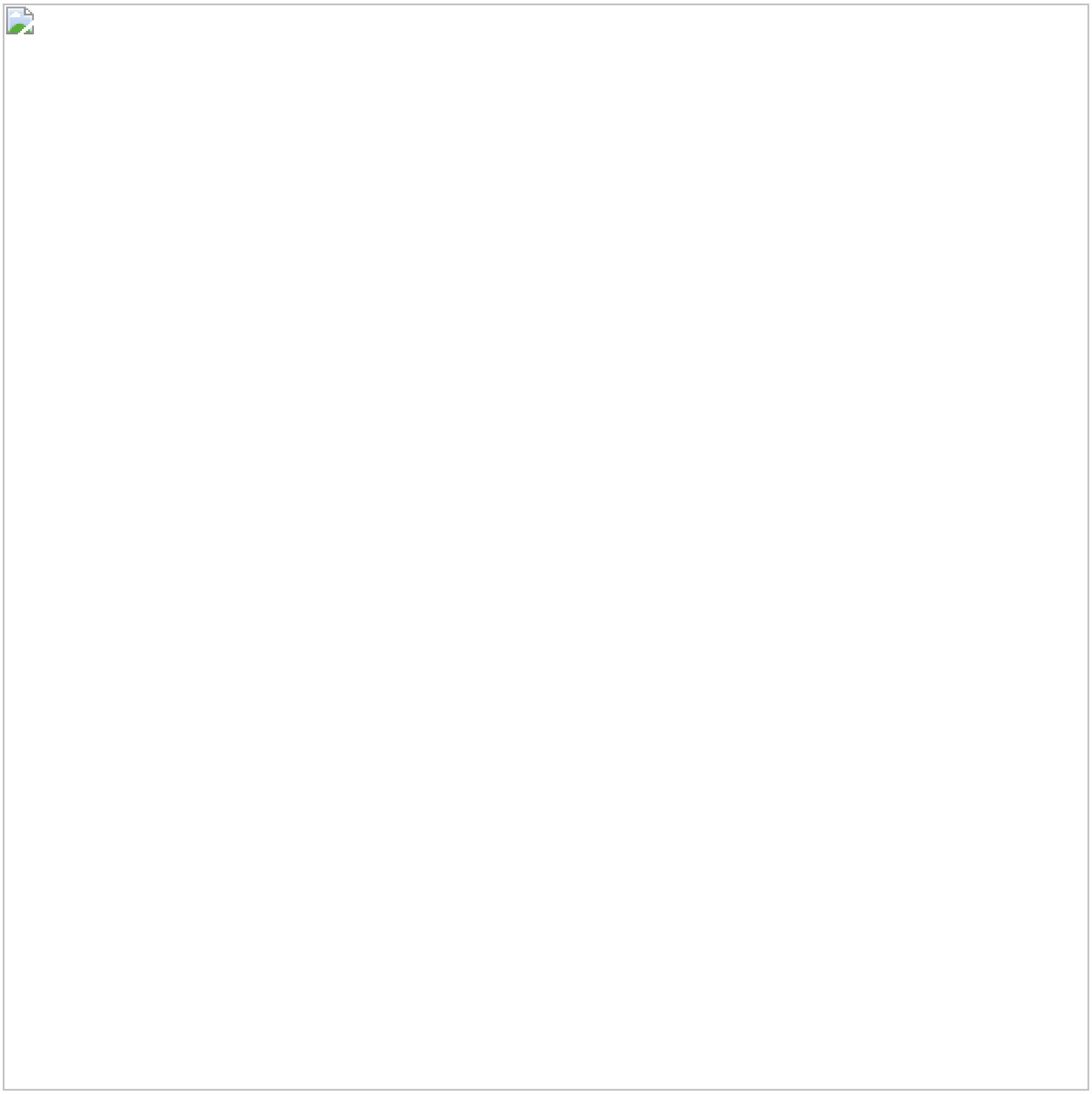
Notably, the posts disclosing the attacks were removed from CARR’s channel after September 2nd.

The reason for the post removal is unclear given the group has a reputation of being “loud” and often boasts about their attacks, especially when mainstream media reports on their activity.

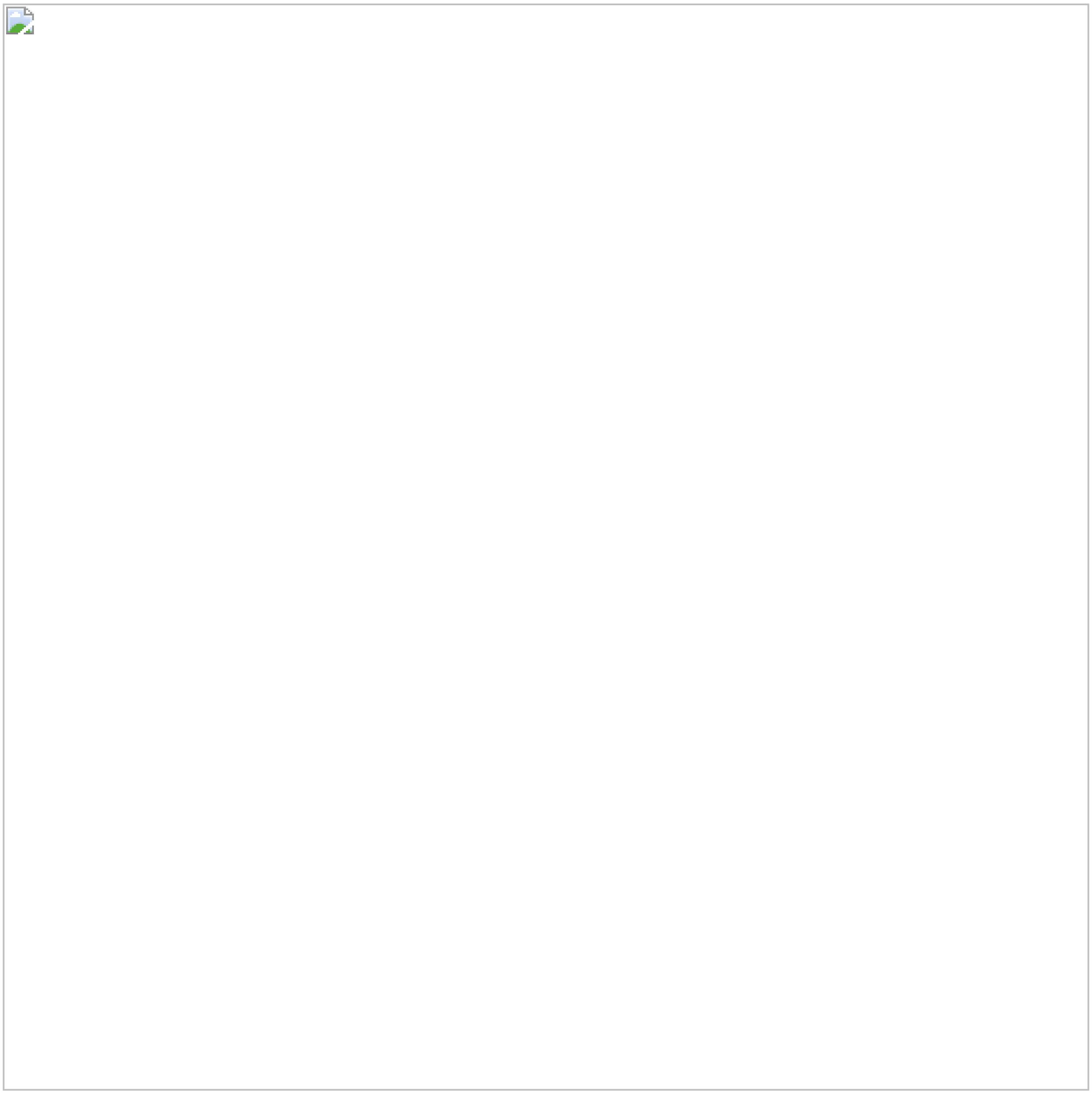
RipperSec

RipperSec is a pro-Islamic, likely Malaysian, hacktivist group that was created in June 2023. The Group’s previous targets included various organizations in Israel, governmental entities in the US, and Indian banking infrastructures. RipperSec claimed responsibility for attacking X (formerly Twitter) during the recent Donald Trump interview with Elon Musk. The group uses their own DDoS tool called MegaMedusa to launch attacks.

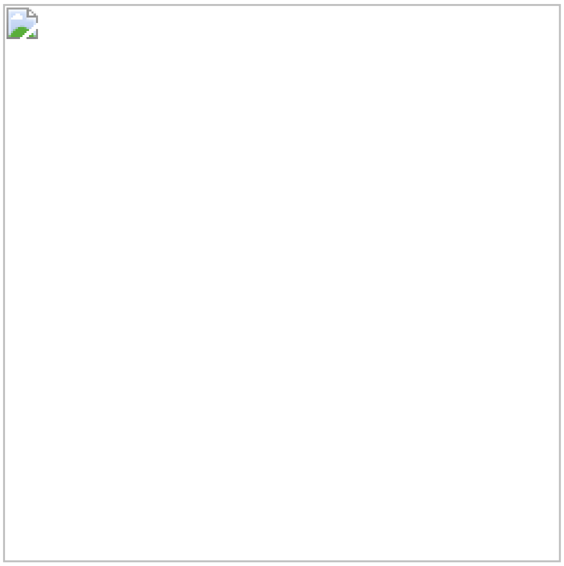
The group is believed to originate from Malaysia, although they claim that their founder has passed away and are now led by a Singaporean leader. As of September 3, 2024, their Telegram channel has 3,083 members.



On August 23rd, RipperSec published a post in their Telegram channel that they are shutting down their operations.



However, on the day of Durov’s arrest they revealed their intent to target France.



The list of targets that were published on the RipperSec channel:

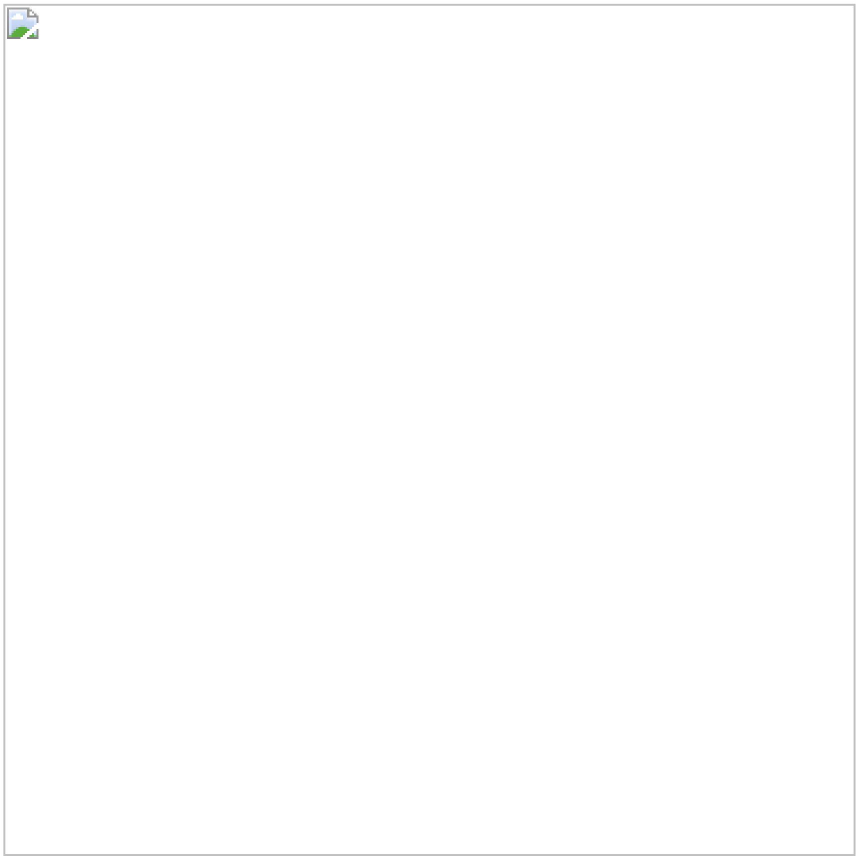
- pricebank.fr (August 25)
- confederationpaysanne.fr (August 25)
- amandes.gouv.fr (August 26)
- boursedeoaris.fr (August 26)
- lafrenchtech.gouv.fr (August 26)
- bonjourdefrance.com (August 26) (together with CGPLLNET group)
- univ-lehavre.fr (August 26) (together with CGPLLNET group)
- univ-ag.fr (August 26) (together with CGPLLNET group)
- utt.fr (August 26) (together with CGPLLNET group)
- cned.fr (August 26) (together with CGPLLNET group)
- auf.org (August 26) (together with CGPLLNET group)
- univ-montp3.fr (August 26) (together with CGPLLNET group)
- mediasat-tv.fr (August 27)
- campusfrance.org (August 27)
- asbv.fr (August 27)
- radiofrance.fr (August 27)
- francetelevisions.fr (August 27)
- oddo-bhf.com (August 27)
- dinard.aerport.fr (August 28)
- bpifrance.fr (August 28)
- police-nationale.interieur.gouv.fr (August 28)
- big.bpifrance.fr (August 28)
- dexia.com (August 28)
- degiro.fr (August 31)
- ieseg.fr (September 2)
- ants.gouv.fr (September 2)
- pricebank.fr (September 2)

- justice.gouv.fr (September 2)
- sse.efopro.afpa.fr (September 2)

EvilWeb

EvilWeb is a pro-Russian hacktivist group that was created in March 2024. As part of the support of the Russian narrative, the group targeted various American and European entities. EvilWeb operates in a hack-and-leak method, in parallel to leveraging traditional DDoS attacks. EvilWeb made claims to have allegedly obtained data from various high profile American organizations. As of September 3, 2024, the EvilWeb Telegram channel has 1,146 members.

EvilWeb announced their participation in #FreeDurov operation on August 25, 2024, and began executing DDoS and hacking attacks.



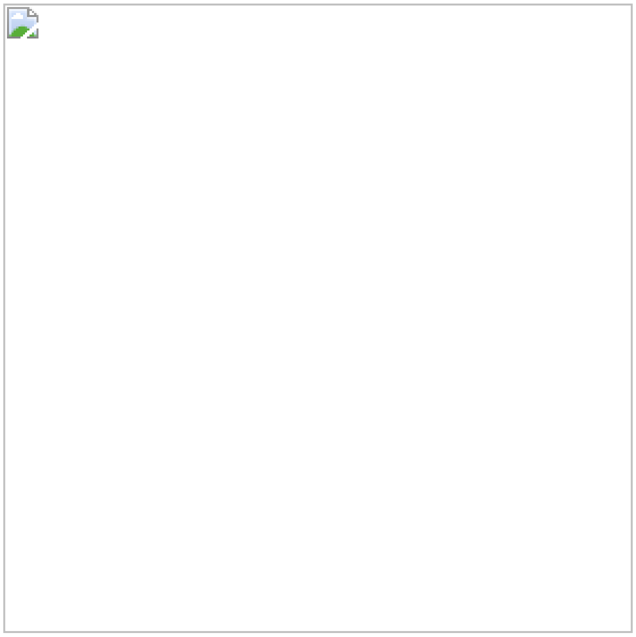
The following is the list of targets published by EvilWeb:

- service-public.fr (August 25)
- fr (August 25) (leaked DB)
- gouv.fr (August 25) (leaked part of DB)
- aeroport.fr (August 26)
- barseille-airport.com (August 26)
- fr (August 26) (leaked DB)
- gouv.fr (August 26)

CyberDragon

CyberDragon is a pro-Russian hacktivist group created in September 2023. The group sporadically targets various Ukrainian organizations and NATO entities in support of Russia. Before engaging in #FreeDurov, CyberDragon carried out a campaign called #OP404 in coordination with other pro-Russian hacktivists groups to target Ukrainian hosting providers.

On August 26th, CyberDragon announced their participation in #FreeDurov. They posted in their Telegram channel stating that European governments want to control Telegram. The group also indicated that the attack was carried out together with the CARR group.



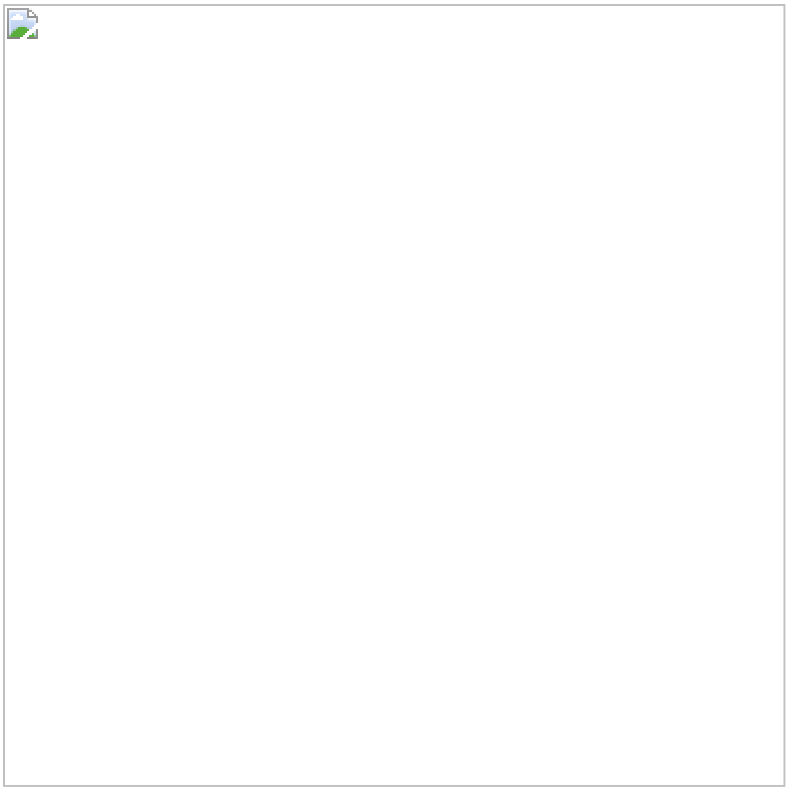
The list of targets that were published on the CyberDragon channel:

- coe.int (August 26)
- int (August 26)
- gouv.fr (August 26)
- corsica-ferries.fr (August 26)
- greffe-tc-paris.fr (August 26)

UserSec

UserSec is a pro-Russian hacktivist group that has been in operation since at least 2022. The current Telegram channel of the group contains 8,124 members as of September 3, 2024, and mostly targets NATO member states.

On August 25, 2024, the group published a post supporting the operation #FreeDurov and announced that they will target French entities in collaboration with CARR.



The list of targets that were published on UserSec channel:

- fr (August 25)
- tribunal-administratif.fr (August 25)
- com (August 27)

STUCX Team

Stucx team is a Malaysian hacktivist group that has been operating since at least March 2023. Before October 7th, the group targeted Indian entities with DDoS attacks. After the Israel-Hamas war began on October 7th, the Stucx team began targeting Israeli organizations. Recently, the group targeted Argentina in a massive defacement and DDoS campaign.

On August 26th, the group published a post supporting #FreeDurov and began targeting France.

The list of targets that were published on Stucx team channel includes:

- reseau-chaleur-chalons.fr (August 26)
- master-transports-tte.fr (August 26)
- fr (August 27)

Conclusion

The arrest of Telegram founder Pavel Durov resonated with many hacktivists groups, mainly pro-Russian and pro- Islamic groups. The sentiment of the groups towards Durov varies. Many groups simply stated their support of Durov without engaging in any public activity, while other groups stated that their concern is the operational safety of Telegram, and that NATO wants to coerce Durov into compliance. A few Russian groups have proclaimed that Durov is “one of ours” and engaged in cyberwarfare due to patriotic reasons. In addition, Telegram is currently one of the main facilitators of the hacktivist’s activity, so those groups will be the first one to suffer from possible privacy setback in Telegram.

With Durov’s release from police custody, it seems that the campaign #FreeDurov is in a dormant stage until the next action by the French authorities.