Pro-Russian Hacktivist Groups Target Ukraine Supporters

intel471.com/blog/pro-russian-hacktivist-groups-target-ukraine-supporters

As the war in Ukraine rages on, unseen but related battles occur daily across the globe. These confrontations stem from pro-Russian hacktivist groups targeting countries that support Ukraine, likely with support from the Kremlin. These hacktivists have been targeting a wide swath of industries and sectors, including aviation, energy, financial, government and public safety, technology, media and telecommunications sectors.

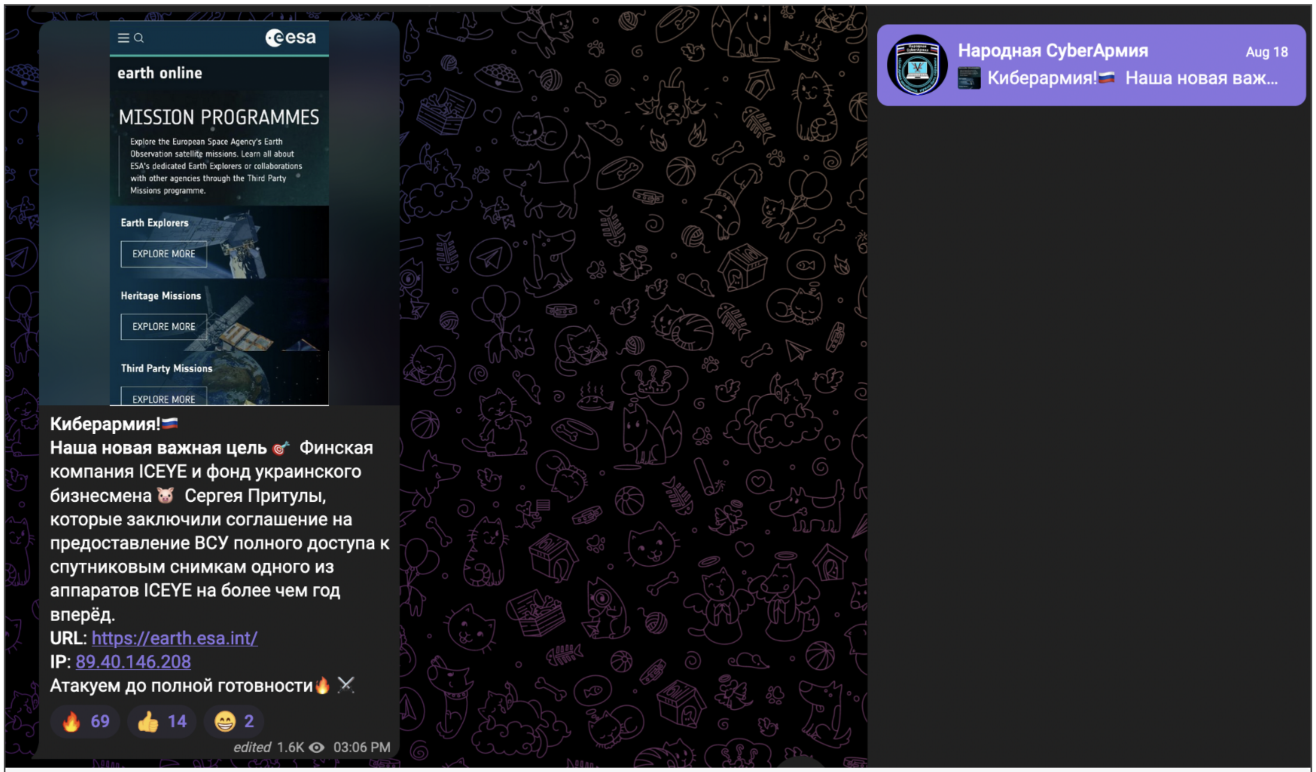
Hacktivism is the combination of hacking (unauthorized access to or control over computer network security systems for some illicit purpose) and political activism. Because of this, hacktivists have social and political agendas as opposed to hackers who commit cyber crimes for profit and often times infamy. It should be noted that many pro-Russian hacktivists are also likely to be hackers responsible for attacks across enterprises and governments.

Pro-Russian hacktivist activity

The pro-Russian hacktivist groups targeting governments and organizations that oppose Russia's stance on the war in Ukraine have been observed using several cyber tactics, including DDoS attacks, network intrusion and stealing personally identifiable information (PII).

In July and August 2022, numerous hacktivist groups accelerated their nefarious activities. The most impactful Ukrainian-specific incidents conducted by major pro-Russian hacktivist groups detected by Intel 471 were:

Народная Cyberармия (Eng. People's CyberArmy) aka **CyberArmyRussia**: The faction conducted multiple DDoS attacks against entities in Europe and Ukraine across many industries, targeting Ukrainian news outlets and local government websites. Their most significant targets were in August when group members attacked the website of Ukraine's nuclear power company, Energoatom. The cyberattack came as tensions flared over the Zaporizhzhia power plant in the south of Ukraine, occupied by Russian forces since March 2022. They also targeted the European Space Agency following news that Finnish company ICEYE agreed to provide the Ukrainian government access to the SAR satellite constellation to fight against Russian aggression.



MISSION PROGRAMMES

Explore the European Space Agency's Earth Observation satellite missions. Learn all about ESA's dedicated Earth Explorers or collaborations with other agencies through the Third Party Missions programme.

Киберармия!🇷🇺
Наша новая важная цель 🎯 Финская компания ICEYE и фонд украинского бизнесмена 🐷 Сергея Притулы, которые заключили соглашение на предоставление ВСУ полного доступа к спутниковым снимкам одного из аппаратов ICEYE на более чем год вперёд.
URL: https://earth.esa.int/
IP: 89.40.146.208
Атакуем до полной готовности🔥⚔️

🔥 69 👍 14 😁 2

edited 1.6K 03:06 PM

Народная CyberАрмия Aug 18
Киберармия!🇷🇺 Наша новая важ...

The image depicts a message posted on **CyberArmyRussia's** Telegram channel, where group members announced ICEYE as a new target.

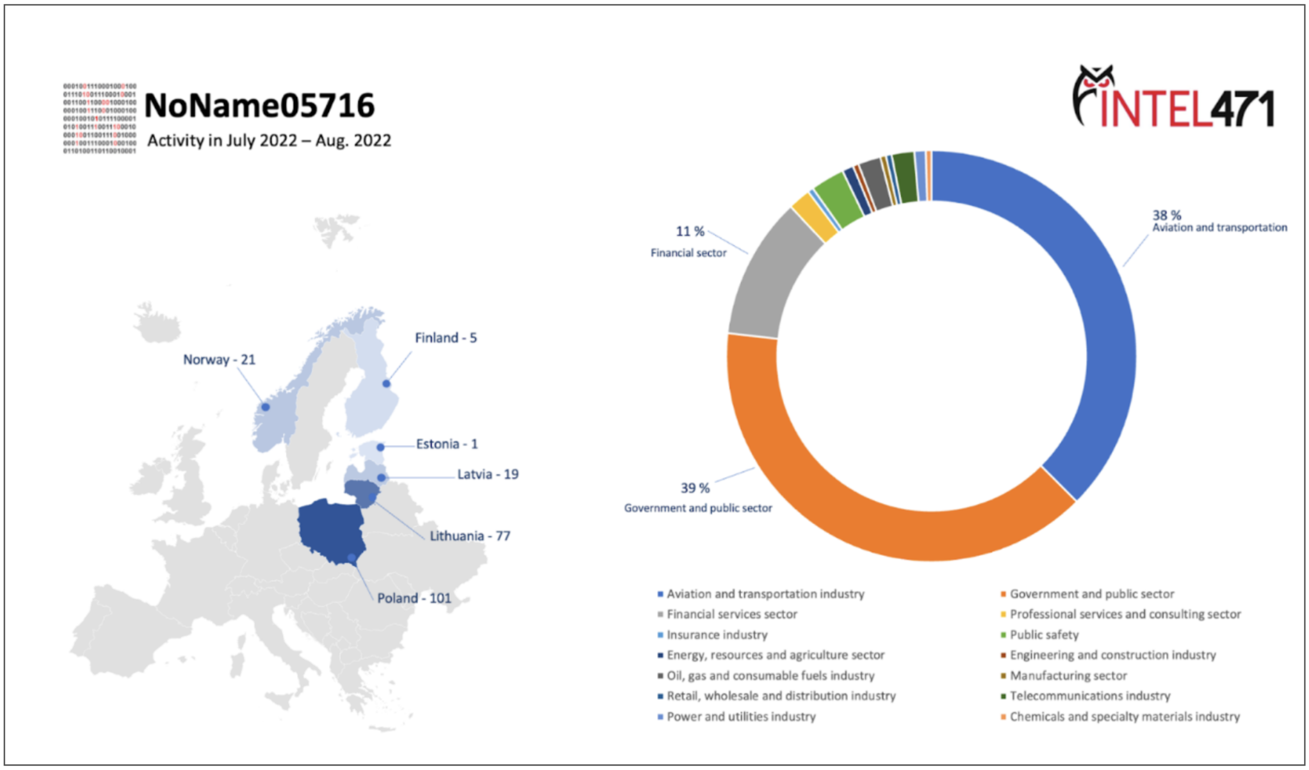
- **CyberArmyRussia** members continue to proclaim their opposition to the "West, European Union and Ukraine" and release pro-Russian propaganda articles and videos in addition to website breach announcements.

- **FRwL Team**, aka **From Russia with Love**, **Z Team**: Group members published the personal data of people who support Ukraine or oppose the actions of Russia. They also allegedly publish classified Ukrainian and U.S. documents as hacktivist resources.
- **KillNet:** Gang members attacked the RuTor forum (a predominantly Russian-speaking underground forum), which they claim is sponsored by the Ukrainian government. **NBP Hackers** joined the effort to disable the RuTor forum and called for other hackers to participate. **KillNet** also claims the Security Service of Ukraine (SBU) paid them one million rubles (about $16,000 US) to stop an attack against the RuTor forum.

On August 17, 2022, **KillNet** claimed responsibility for extensive cyberattacks in Estonia shortly after government officials decided to remove Soviet-era monuments near the border with Russia. **KillNet** also allegedly blocked access to over 200 private and Estonian state institutions, including banks, government organizations, payment systems and public services.

> **NBP Hackers**: This group released personal information of Ukraine's government officials and high-profile personas perceived as enemies of Russia. They also encourage the hacking community to join their efforts in disabling the RuTor forum, adding to the efforts of the **KillNet** gang.

NoName057(16): This hacktivist group, the most active of the groups on this list, conducted multiple DDoS attacks against entities in Norway, prompted by the decision of Norwegian authorities to block Russian cargo to the Svalbard archipelago. In addition, members attacked numerous companies from the financial and government sectors in Lithuania, apparently due to the country's ban on transporting goods and cargo to the Kaliningrad region of Russia. The gang also conducted massive attacks on the Polish government and transportation sectors, including airports in Kraków, Warsaw and Wrocław, the gas pipeline EuRoPol, the logistics company PKP Cargo and defense weapon and military equipment provider Polski Holding Obronny. Last but by no means least, group members attacked various Finnish, Latvian and Polish government agencies all considered to be sympathetic to the Ukrainian effort. The graph below shows a breakdown of the impacted entities by country.



Due to the very nature of state-sponsored cyber attacks, there is limited conclusive evidence that the Kremlin is directing or supporting the aforementioned hacktivism. Although the link likely exists and state-sponsored hacking is nothing new, the Kremlin will be sure to distance itself from any malign activity so as not to risk breaching NATOs Collective Defence treaty, Article 5. In any case, companies, enterprises and governments should limit their attack surface, ensure that software patching is conducted routinely and invest in increased threat detection capabilities in the face of Russian cyber aggression.