

Five hacker groups that attack Ukraine the most



22.04.2022 16:58

The Computer Emergency Response Team of Ukraine (CERT-UA) has recorded 802 cyber attacks in Q1 2022. A year ago, 362 cyberattacks were recorded in the same period.

Five groups that have waged the largest number of cyber attacks on Ukraine's critical IT infrastructure include hackers, whose activities are associated with the aggressor country or Belarus as its accomplice in the war against our homeland:

1. UAC-0010 aka Armageddon (GammaLoad, GammaDrop, HarvesterX): APT (advanced persistent threat), a group backed by the Russian FSB.
2. UAC-0041 (AgentTesla, XLoader): Russian hacktivists.
3. UAC-0056 (Pandora hVNC, RemoteUtilities, GrimPlant, GraphSteel): Russian hacktivists and cyber spies.
4. UAC-0051 aka UNC1151: APT, a group allegedly linked to special services of the Republic of Belarus.

5. UAC-0028 aka APT28: APT, a group allegedly linked to GRU (Main Intelligence Directorate) of the Russian Federation.

UAC-0041 and UAC-0056, associated by the international community with Russian hackers, are the ones being unusually active. They exploit the current military issues. Most likely, the Russian intelligence service shares data with these groups.

| [All news >](#)