

Dark Web Profile: Killnet - Russian Hacktivist Group - SOCRadar® Cyber Intelligence Inc.

Published: 2022-12-16 · Archived: 2026-04-05 15:55:30 UTC

By *SOCRadar Research*

The ongoing conflict between Ukraine and Russia has attracted the attention of various cybercriminal groups and pushed them to get involved in this **cyber warfare**. According to CyberKnow's [research](#), over 190 threat actor groups actively play a role during Ukraine-Russia cyber warfare.

Some groups have aligned with one side of the conflict and are using their skills to support their chosen faction. KillNet is one of the groups that has played a significant role and is known for its **DDoS activities** in the interests of Russia.

Who is Killnet?

Killnet threat actor card

Killnet is a pro-Russian **hacktivist group** known for its DDoS campaigns against countries supporting Ukraine, especially NATO countries since the [Russia-Ukraine war](#) broke out last year. DDoS is the primary type of cyber-attack that can cause thousands of connection requests and packets to be sent to the target server or website per minute, slowing down or even stopping vulnerable systems.

While Killnet's **DDoS attacks** usually do not cause major damage, they can cause service outages lasting several hours or even days. It is known that **KillMilk**, its founder, left the group in July 2022, and its new leader is a hacker using the name **Blackside**. However, KillMilk is still related to the group and shares Killnet's announcements on his telegram channel, as seen below.

'OFFICIAL KILLNET CHANNEL' shared by Killnet in their Telegram group:

Killnet Telegram Post

How Did Killnet DDoS Service Become a Hacktivist Group?

Until the Russia-Ukraine war, Killnet was known as the name of a [DDoS attack tool](#) that only subscribers could rent and use. With the crisis in Russia and Ukraine, Killnet emerged as a **hacker group** and continued its attacks under the name "Killnet."

Afterward, the Killnet hacker group carried out many attacks to support Russia and fight for Russia's interests. They targeted countries that supported **Ukraine** in the war between Russia and Ukraine. For months, the Killnet group has attacked the countries that support Ukraine, and their political interests are against the Russian government.

They do not seem interested in **financial gain**; they aim to harm web services by disrupting them with mainly DDoS attacks.

Figure 2: KillMilk Telegram Link

Killnet Grows

The group has continued its operations for over a year and has become a serious **cyber threat**. With the encouragement from Killnet service users, which reached tens of thousands of subscribers, they formed subgroups under the name “**Cyber Special Forces of the Russian Federation.**”

The group also started another hacker group called **LEGION** in April 2022 and continued its DDoS attacks from there. Other groups were observed under the LEGION group, each carrying out different attacks. In July 2022, the group announced that LEGION had been disbanded and would be relaunched as **LEGION 2.0**. There are more than a thousand estimated group members with all these related groups.

Killnet mentioned in a post on their Telegram channel that their birth date is November 13, 2021.

However, they announced that they became a hacktivist group on February 23, 2022.

Killnet’s Relationship with Other Hacker Groups

A group formerly known as **XakNet** announced that it had merged with Killnet, targeting critical infrastructures. Another group, later known as **F**kNet**, also expressed its intention to work with Killnet, targeting the public and private sectors in countries that support Ukraine.

A former member of Killnet, now the leader of the **Zarya** group, also mentioned that other hacker groups act parallel with them and defend Russia’s interests in an interview. He named groups like **XakNet, Beregini, CyberArmy, Anonymous Russia, RaHDit, DPR Joker, NoName057, and Zsecnet.**

The Hacker also said that Anonymous Russia and the Zarya group were founded by hackers who left the Killnet group. Other hackers also joined Zarya from Killnet.

In the same interview, Zarya’s leader also explained the reasoning behind the creation of small groups by dividing Killnet. Smaller groups are easier to manage, and it is more difficult for the enemy to understand from whom to attack. He also revealed that Zarya was previously a part of the Killnet team but is now an independent entity.

SOCRadar Threat Actors Module provides detailed information on threat actors, IoCs, and exploited CVEs.

Killnet’s Targets and Operations

Killnet has attacked many **European and Western** countries, including Ukraine, since February 2022. The **US, the UK, Germany, Italy, Romania, Lithuania, Estonia, and Poland** are among these. Attacks on US airports, the **Eurovision contest** website, and more than a thousand websites in Lithuania were worth mentioning. There were also attacks on railways and government portals in the Czech Republic.

Countries affected by Killnet (Source: SOCRadar)

In April 2022, Killnet focused entirely on supporting Russian geopolitical interests worldwide. They claimed to have carried out more than **550 attacks** between late February and September. Only 45 of these attacks were directed against Ukraine, **less than 10%** of the total attacks.

You can find previous attacks of Killnet on SOCRadar's research [article](#) published on July 28, 2022.

Killnet's Recent Cyber Attacks

May 2022:

Killnet attacked Romanian government websites.

They attacked Italy and managed to block a few websites, while the attack on the **CSIRT** site was unsuccessful. Killnet hacked **Istituto Superiore di Sanità** and the **Automobile Club of Italy** websites in the same attack. The Italian Senate website was also hacked and closed for an hour. The attack was not as devastating as predicted.

June 2022:

The group targeted **Norwegian organizations** through various DDoS attacks. Also, the group took responsibility for the DDoS attack through the Lithuanian government and private institutions.

August 2022:

The group and its founder, called "**KillMilk**," claimed responsibility for a cyber-attack on the American defense contractor **Lockheed Martin** as a retaliation for the HIMARS systems supplied by the US to Ukraine.

September 2022:

Killnet announced that it had attacked **23 websites of 4 ministries** and agencies in Japan, including e-Gov, a portal site for administrative information administered by the Digital Agency, and eLTAX, a local tax website administered by the **Ministry of Internal Affairs and Communications**.

October 2022:

Several US airport websites were attacked.

Killnet posted a list of several government websites they would target in the coming days beneath an image of a nuclear explosion behind the Statue of Liberty.

Alleged targets are listed below:

- Alabama
- Alaska
- Connecticut
- Colorado
- Delaware
- Florida
- Hawaii

- Idaho
- Indiana
- Kansas
- Kentucky
- Mississippi

November 2022:

On the Killnet Telegram channel, the group shared a post that said, “We have gained strength and now we are able to reduce the traffic of drug addicts to sellers’ websites to zero! Not without your help, of course, comrades!”

Killnet threat actors hacked Russia’s largest dark web drug site. They published dealers’ and drug addicts’ data, storage locations, etc.

In a mail from a Latvian State Revenue Service employee, they announced they have VPN access to corporate government networks and downloaded **200 gigabytes** of documents.

Killnet hacker group declared that they attacked western governments’ and companies’ websites. They have posted a gateway to a **government portal** for authentication and access to various web resources in their Telegram group.

The **White House** announced that it has temporarily closed its official website and **Starlink API**. Experts stated it is a critical target because the Ukrainian army uses Starlink

Killnet posted an announcement on its Telegram channel, asking all hackers for help attacking and targeting Poland. They said several of the targets would be inoperable for four days. Following this announcement, Warsaw Airport, Gdansk Airport, and Rzeszow Airport became victims of cyberattacks.

December 2022:

In a post, the Killnet group mentioned a new project called Infinity. They plan to launch the project sometime this winter-spring, which is getting a lot of attention at this stage.

They have also published a post asking President Putin for nuclear strikes on the capitals of Ukraine’s allies on the Killnet telegram channel:

Another critical piece of intelligence about the Killnet group is that some members said they attacked the Bankers Automated Clearing Service (BACS), the London Stock Exchange, and the Prince of Wales official website. Killnet stated that the “royal official site” was not working. “Perhaps this is due to the supply of high-precision missiles to Ukraine,” the group said.

Killmilk, a senior member of the Killnet group, has threatened the **US Congress** with the sale of the health and personal data of the American people because of the Ukraine policy of the US Congress.

January 2023:

In late January 2023, KillNet shared that it was targeting Germany via the **Passion Botnet** with the hashtag #ГерманияRIP.

A day after the announcement, the group posted screenshots showing that they had denied access to several German websites, including the Cabinet of Germany (**Bundesregierung**) and the Federal Ministry of the Interior (**Bundesministerium des Innern und für Heimat**).

Killnet shared a list of other German websites they targeted on the same day, categorized by industry:

The **NetSide and SARD Telegram groups** also shared that they had hacked the admin panels of hundreds of websites to support Killnet and posted the credentials on Killnet's page:

It is noteworthy that NetSide and SARD make such posts at regular intervals.

At the end of the month, Killnet shared that they carried out a massive **Layer 7 DDoS attack** on several healthcare organizations all over the US. In addition, according to the [Daily Mail](#), hospitals in the Netherlands reportedly experienced a DDoS attack from Russian hacking groups.

February 2023:

February started with a stunning announcement and a call to action; Killnet posted an announcement message urging anyone interested in attacking the United States to contact the administrator of the **Infinity hacker group**:

SecurityScorecard has shared a list of public IP addresses known to belong to Killnet so that cybersecurity personnel can block them:

Anonymous posted a news article from [gazeta.ru](#) on its Telegram channel about an interview with KillMilk, the leader of KillNet. According to [KillMilk's interview](#), the Ukrainian hacking group Phoenix teamed up with the Russian group KillNet to take revenge for the arrest of their accomplices by the **SBU (Security Service of Ukraine)**:

Killnet in 2023

Since the end of January, Killnet has been actively targeting healthcare organizations. In their telegram post, they shared that the corporate entrances and websites of various hospitals were down and that this attack was a joint operation.

Some of those mentioned in KillNet's Telegram post are hacker groups, and some are known as [DDoS-as-a-Service](#) providers.

Killnet was recently observed operating with the Passion Botnet, a group that offers DDoS-as-a-Service. The origin of Passion is unknown, but they have become more active lately, especially at the beginning of 2023. They have a history of targeting individuals and organizations against Russia's invasion of Ukraine, using techniques like defacement and denial of service.

Also, other groups affiliated with Killnet offer DDoS as a Service model, such as AKL Client, Infinity Stresser, and MistNet.

Killnet’s cooperation with multiple DDos-as-a-Service providers may indicate that it will be more active in future events.

Prominent Characteristics & TTPs

By observing Killnet’s attacks and behavior to date, some inferences could be made about whether they are applied repetitively or consistently.

- Due to its motivation and determination to defend Russia, the group chose its targets among NATO-linked countries. It is also a potential threat to countries whose political interests contradict Russia.
- They prefer DDoS attacks against their targets. Victims can recover their systems from attacks, which usually take 1-3 days, with appropriate measures in a matter of hours.
- They target governments’ or public institutions’ websites. This way, they think that they signal to the victims that the victims chose the “wrong side.”
- They announce their attacks and targets on Telegram channels.
- Killnet is also associated with other hacker groups that have common goals with them or act in Russian interests. They have been collaborating with XakNet and F**kNet, and the additional threat actors aforementioned.

MITRE Map

Reconnaissance	Resource Development	Credential Access	Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1110: Brute Force	T1498: Network Denial of Service
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure		T1489: Service Stop

Primary Killnet Tactics

Brute-force dictionary attacks against:

- SSH (port 22) primarily targets the root account
- Minecraft and TeamSpeak servers

DDoS attacks on the OSI model:

- layer 4 (SYN flood attacks)
- layer 7 (high volume POST/GET requests) to cause resource exhaustion and system failure.

In various Telegram groups, they collaborate with the members who are instructed to use IP stresser-for-hire tools such as Crypto Stresser, DDG Stresser, Instant-Stresser, and Stresser.ai. Moreover, several scripts are used during their attacks. Some of them are CC-attack, MDDoS, Low Orbit Ion Cannon (LOIC), KARMA, and Dummy.

How to Prevent a Killnet Attack

Firstly, we need to pay attention to two main defense tactics. One is enforcing strong password policies that can withstand basic brute-force credential attacks, and the second is to have a proper strategy for fighting off DDoS attacks.

The other defensive tactics are listed below:

- Purchase DDoS mitigation services from an Internet Service Provider (ISP), Content Delivery Network (CDN), or Web-Application Firewall (WAF) provider.
- Deploy multi-factor authentication (MFA) mechanism for all remote accesses
- Use blocklisting known Killnet-related IoC, such as IP addresses used by Killnet attacks.
- Enable the DMZ (Demilitarized Zone) for internet-facing entities.
- Employ DDoS protection via web bot detection techniques.
- Reduce attack surfaces and make it easier with ASM (Attack Surface Management) platforms.
- Get the CTI (cyber threat intelligence) feeds that monitor dark web information to identify and predict potential threats and provide actionable intelligence data for your organization.
- Configure web servers and APIs with security modules to optimize performance during a web traffic spike.
- Perform stress tests on all critical services for their ability to handle resource exhaustion attacks
- Create and practice IRP (Incident Response Plan) for the worst case, which resulted in temporary downtime.

Learn What Hackers Talk About Your Company With SOCRadar

The fact that [Telegram](#) is a legit messaging app used by millions gave hackers a chance to conceal themselves and follow their malicious agenda. More and more threat actors use Telegram for communication and announcements, and it has become the main hub for [threat actors](#).

Source: <https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/>