OSINT Report: Killnet APT Group

KillNet is a pro-Russian hacktivist group that became highly active following Russia’s full-scale invasion of Ukraine in 2022. Prior to the war, the group operated as a DDoS-for-hire service, but later shifted its focus to politically motivated attacks against government institutions, private companies, and critical infrastructure in countries supporting Ukraine. KillNet’s primary activities remain distributed denial-of-service (DDoS) attacks, information and psychological operations, and intimidation campaigns, which are actively amplified through Telegram and other social media platforms.

The group presents itself as a “defender of Russia’s interests” and consistently employs pro-Russian rhetoric. A broad network of affiliated hacktivist groups has formed around KillNet, including Anonymous Sudan, Infinity Team, and other pro-Russian cyber communities.

KillNet has repeatedly claimed responsibility for attacks against government resources in NATO member states, healthcare institutions, defense companies, and the financial sector. Some of the group’s claims appear to be exaggerated or part of information manipulation efforts; however, it remains one of the most public and recognizable pro-Russian hacktivist brands. KillNet frequently collaborates with pro-Russian cybercriminal communities, increasing the risk of combined attacks involving DDoS, ransomware, and data leaks.

Despite the generally low to moderate technical sophistication of many of its operations, KillNet poses a significant threat due to its ability to rapidly mobilize large numbers of supporters to conduct mass campaigns and generate substantial information impact. The group’s primary targets remain government institutions, critical infrastructure, and organizations in countries supporting Ukraine in the war against Russia.

Support the organization’s activities: https://donate.shum-ng.org/

Ideology and Motivation

Since its emergence, KillNet has maintained a distinctly pro-Russian ideological position. Following Russia's full-scale invasion of Ukraine, the group's activities shifted toward supporting the Russian military campaign and targeting Ukraine and the countries that support it. This alignment facilitated closer cooperation between KillNet and other pro-Russian hacktivist groups, including the Belarusian group Infinity Hackers. The group consistently promotes anti-Western and anti-American rhetoric, portraying the United States as one of Russia's principal adversaries in cyberspace.

KillNet's primary motivation is ideological rather than financial. This is evidenced by the absence of ransom demands in many of its operations, as well as by the ideological justifications that the group's members themselves provide for their attacks. At the same time, the group regularly solicits donations to support its network of hacktivists.

Many publications discussing KillNet frequently state that: "Although a direct connection between KillNet and the Russian special services has not been officially confirmed, the group's activities often align with the geopolitical interests of the Russian Federation." However, based on an analysis of KillNet's activities, the following observations can be made regarding its possible cooperation with the FSB or other Russian state agencies:

1. The objectives pursued by KillNet closely align with those of the Kremlin. Although some reports describe individual KillNet members as holding xenophobic views, the group's target selection has consistently focused on countries supporting Ukraine or adopting positions unfavorable to Russia's foreign policy interests. This suggests that the operational planning of its campaigns has been driven by priorities extending beyond the personal ideological beliefs of individual members.
2. Lack of action by Russian law enforcement and favorable media coverage. Throughout its existence, KillNet has openly recruited participants, publicly claimed responsibility for cyberattacks, and maintained an active presence on social media platforms and messaging applications. Despite this, there is no publicly available information indicating systematic efforts by Russian law enforcement agencies to disrupt the group's activities. Instead, some of KillNet's operations and public statements have received positive or neutral coverage in Russian state-controlled media.
   Source: https://www.rbc.ru/rbcfreenews/6a27f7299a794768a9e67668
3. Potential use of the plausible deniability model. This approach involves the use of formally independent hacktivist or criminal groups to pursue state objectives while allowing the government to officially deny any connection to their activities. Cybersecurity researchers have repeatedly identified this practice as a characteristic element of Russia's cyber strategy, enabling the state to benefit politically from proxy actors while minimizing reputational and legal risks.

Support the organization's activities: https://donate.shum-ng.org/

3. The absence of sophisticated cyber espionage operations by KillNet is not sufficient grounds to dismiss its potential role in advancing Russian state interests. Unlike APT groups that focus on covert intelligence collection and long-term network access, KillNet has specialized in DDoS attacks and information and psychological operations. This may indicate not the absence of ties to the state, but rather a different functional role within the broader ecosystem of pro-Russian cyber operations.

4. Although Killmilk has attempted to dispel the perception that KillNet is a Russian proxy group, the group adheres to long-established norms observed within the Russian hacking community. KillNet requires its members to affirm that they will never operate within the Russian segment of the Internet or target Russian systems or initiatives. Ultimately, Killmilk keeps the group's activities within the boundaries of what the Russian government considers acceptable behavior, thereby avoiding any significant adverse response from the state.

Key Events

Date / Year	Event	Brief Description of the Attack
29.04.2022 – 01.05.2022	Attacks on Romanian government websites	KillNet conducted DDoS attacks against the websites of Romanian government institutions.
April 2022	Cyberattacks against Moldova following the events in Transnistria	A pro-Russian group associated with KillNet targeted Moldovan government websites and public institutions. The attacks originated from abroad and primarily involved DDoS techniques.
April 2022	Attacks on Czech government institutions	KillNet claimed responsibility for attacks against the websites of Czech government institutions. The primary method was DDoS attacks intended to overwhelm online services.
14.05.2022	Attack on Italian government resources	The websites of the Istituto Superiore di Sanità, the Automobile Club of Italy, and the Italian Senate were targeted. The attacks aimed to temporarily disrupt access through DDoS attacks.
29–30.05.2022	Large-scale cyberattack against Italy	KillNet announced a "destructive" attack against Italy. Multiple government websites were targeted, although most attacks were successfully mitigated by Italy's CSIRT.
May 2022	Attempted Attack on Eurovision 2022	A suspected DDoS attack targeted the Eurovision Song Contest website during Ukraine's performance. The attack was blocked by the Italian police. Following this, KillNet launched a DDoS attack against the Italian police website.

Support the organization's activities: https://donate.shum-ng.org/

Date / Year	Event	Brief Description of the Attack
June 2022	Cyberattacks against Lithuania	KillNet claimed responsibility for attacks against Lithuania’s network infrastructure in response to restrictions on transit to Kaliningrad. The campaign primarily involved DDoS attacks targeting government and network resources.
28.06.2022	Attacks on Norwegian organizations	Norwegian organizations experienced a series of DDoS attacks. According to the Norwegian authorities, no leakage of private data was detected.
2022	Largest cyberattack against Latvia’s public broadcaster	KillNet attacked Latvia’s state broadcaster. The attack was considered one of the largest in the country’s history but was successfully mitigated.
01.08.2022	Attack on Lockheed Martin (United States)	KillNet claimed responsibility for a cyberattack against defense contractor Lockheed Martin in response to the delivery of HIMARS systems to Ukraine. The group claimed to have targeted production systems and employee data.
10.10.2022	Attacks on U.S. airport websites	Several U.S. airport websites were targeted in DDoS attacks intended to temporarily disrupt online services.
6–7.09.2022	Attacks on Japanese government resources	KillNet claimed attacks against ministry websites, e-Gov, eLTAX, and the Mixi platform. The group also claimed attacks against Tokyo Metro and Osaka Metro. No evidence of data compromise was identified.
2022	Cyberattack threats against the Georgian government	KillNet and its leader, Killmilk, publicly threatened cyberattacks against the Georgian government over the country’s anti-Russian stance.
26.01.2023	Large-scale DDoS attacks against Germany	Germany’s Federal Office for Information Security (BSI) reported widespread DDoS attacks targeting airports, the financial sector, and government institutions. The attacks were linked to Germany’s decision to provide Leopard 2 tanks to Ukraine.
28.01.2023 - 23.04.2023	DDoS attacks targeting HPH organizations in the United States	More than 90 known DDoS attacks targeted healthcare systems, hospitals, and medical centers. Due to the large volume of patient data they manage, these organizations were considered attractive targets for KillNet and its affiliates. On 17 March 2023, Microsoft Security reported that KillNet had been using Microsoft Azure infrastructure to target healthcare applications for more than three months. The attacks were linked to military assistance provided to Ukraine, including the supply of tanks.

Conclusion: The documented attacks indicate that KillNet’s operations are largely reactive in nature. Rather than following an independent long-term strategic targeting agenda, the group primarily responds to political decisions made by states whose actions are perceived as conflicting with the interests of the Russian Federation.

Support the organization’s activities: https://donate.shum-ng.org/

Organizational Structure and Affiliations

On 4 January 2022, the Telegram channel “We are KillNet” was created to promote DDoS/Stressor-for-hire services targeting arbitrary websites. The group’s founder is widely believed to be the individual operating under the alias KillMilk. Following Russia’s full-scale invasion of Ukraine, KillNet evolved from a DDoS-for-hire service into one of the most prominent pro-Russian hacktivist communities. The group actively uses Telegram to coordinate its activities, disseminate propaganda, and recruit new supporters. Over time, a broad network of affiliated groups has emerged around KillNet, sharing common objectives and conducting coordinated cyber operations.

KillNet representatives have repeatedly emphasized that the organization does not have a rigid centralized structure. In official statements published i**n March 2023,** the group described itself as a decentralized community of so-called “Russian cyber patriots” and denied receiving any form of state support. At the same time, the activities of its leader, KillMilk, suggest efforts to formalize certain aspects of the group’s operations. In particular, **in March 2023,** he announced the creation of Black Skills PMHC (Private Military Hacking Company), an organizational structure reportedly consisting of more than twenty functional divisions responsible for intelligence, information operations, finance, investments, and other areas of activity.

In July 2022, KillMilk announced his departure from KillNet, stating that the decision was intended to protect the group’s members from potential risks. Despite his formal withdrawal, subsequent Telegram activity indicated that he continued to maintain close ties with KillNet. According to available reporting, leadership of the group was assumed by the hacker known as BlackSide, who has been linked to ransomware operations, phishing campaigns, and cryptocurrency theft.

Among KillNet’s most prominent partners and affiliated groups are Anonymous Russia, Infinity Hackers, National Hackers Russia, NETSIDE Group, Passion Botnet, and Phoenix. Analysis of the group’s information campaigns indicates that KillNet has exerted significant influence over the broader pro-Russian hacktivist ecosystem. Unlike professional cyber threat groups associated with Russian intelligence services, such as Fancy Bear and Sandworm, KillNet’s operations are generally more reactive and ideologically motivated. Its primary targets are government institutions, organizations, and companies that the group perceives as supporting Ukraine or adopting anti-Russian positions. This combination of extensive media visibility, a broad supporter network, and the ability to rapidly mobilize participants for large-scale campaigns has made KillNet one of the most influential pro-Russian hacktivist brands. (5)

Support the organization’s activities: https://donate.shum-ng.org/

In March 2023, KillNet leader N**ikolay Serafimov** announced the creation of an organization called Black Skills, describing it as a Private Military Hacking Company (PMHC). The term is an explicit reference to the concept of private military companies, which gained significant prominence in Russia following the extensive use of organizations such as the Wagner Group.

Unlike KillNet's previous model as a relatively decentralized hacktivist collective, the Black Skills initiative envisioned a more formalized organizational structure. According to statements made by the group's members, the new model would include dedicated functional divisions responsible for recruitment, financial administration, public relations, technical support, penetration testing, intelligence collection and analysis, information and psychological operations, and offensive cyber operations against designated targets. This approach reflected an effort to transition from a volunteer-based community to an organization with clearly defined responsibilities and an internal hierarchy.

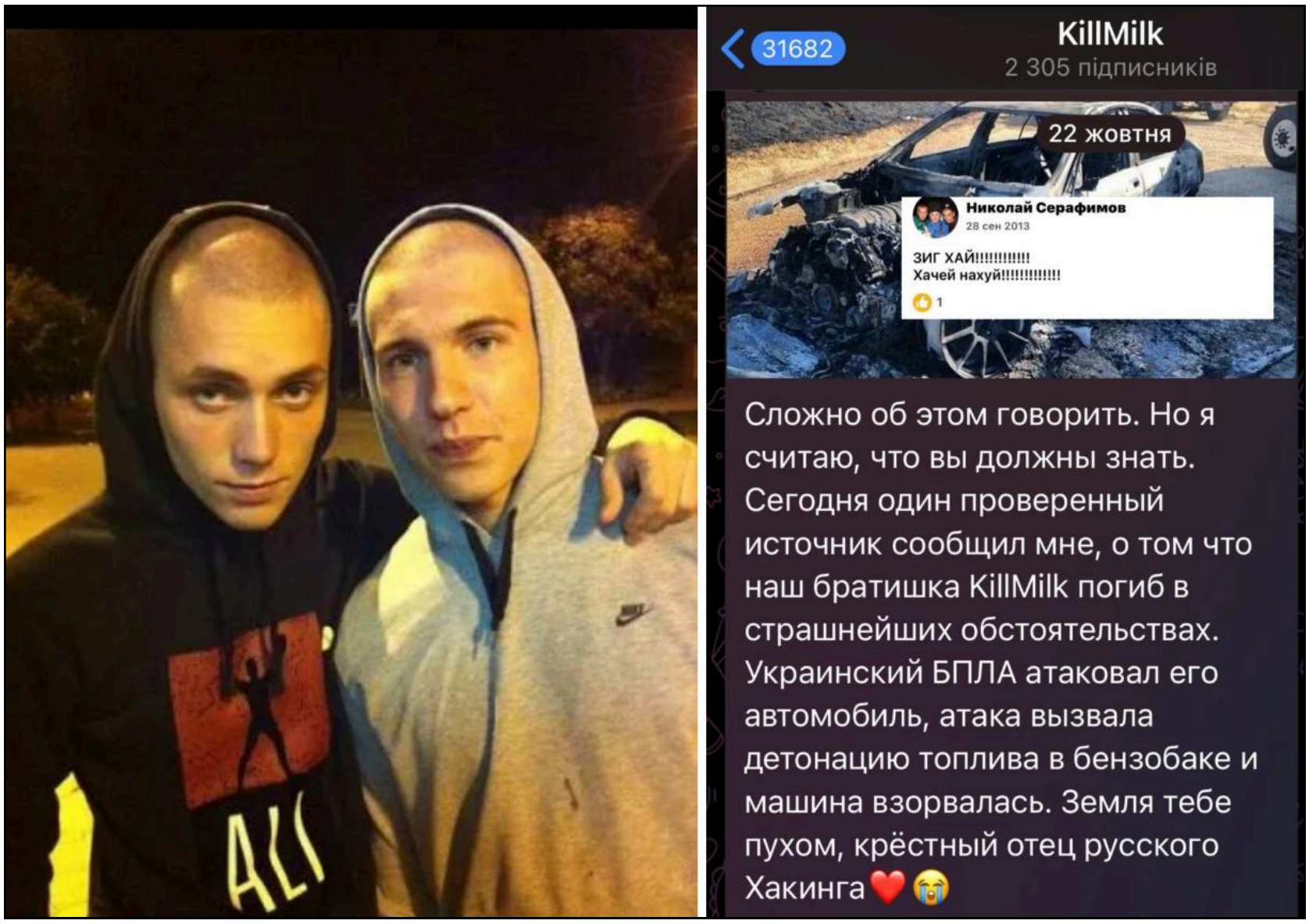
A further element of this formalization was the introduction of a structured recruitment process. Prospective members were required to complete application forms detailing their professional skills, work experience, military service, and government service. This differed significantly from KillNet's earlier practice of openly recruiting participants through Telegram channels and indicated an attempt to establish an internal vetting process and assign roles based on individual competencies.

The emergence of Black Skills may also be viewed as a response to the limited success of KillNet's previous attempts to expand its activities. In particular, the Infinity forum, launched in **late 2022** as a platform intended to facilitate cooperation between hacktivists and cybercriminals, failed to attract a sufficiently active user base. Likewise, the group's so-called "hacker school" initiative achieved little practical success. Against this backdrop, Black Skills represented an effort to move away from an informal network model toward a more structured organization with dedicated administrative, operational, and financial mechanisms.

At the same time, there is no independent evidence confirming that all of the announced organizational units ever became fully operational. Some of the proclaimed "departments" may have been largely symbolic, intended primarily to project the image of a professional cyber organization. This is understandable given that transforming an ordinary internet activist into a capable cyber operator is inherently difficult, as sophisticated cyber operations require extensive training, technical expertise, and practical experience—not merely motivation. Nevertheless, the attempt to organize KillNet according to a corporate or military-style model demonstrates the leadership's ambition to improve internal governance, monetize existing resources, and establish a sustainable organizational infrastructure to support the group's long-term operations. [6]

Support the organization's activities: https://donate.shum-ng.org/

Leader of KillNet



Nick — KillMilk
Full Name: Nikolay Nikolaevich Serafimov
DOB- 16.05.1993
Served his sentence in the Republic of Bashkortostan, Salavat (IK-2).
Convicted under Article 228.1, Part 5 and sentenced to 8 years of imprisonment.
Released on parole, later reportedly recruited by the FSB and sent to Krasnodar, allegedly for PTR (forced labor).

Primary Telegram account— t.me/sooosoosos
Source: https://telegra.ph/Lichnost-KillMilk-11-03

Conclusion:

Unlike traditional APT groups with clearly defined organizational structures and specialized operational units, KillNet operates as a decentralized hacktivist network. For an extended period, the group's founder, KillMilk, played the central role in shaping its strategic narratives and coordinating its activities. Around him, a core group of coordinators emerged, interacting with affiliated pro-Russian groups and a broader network of supporters on Telegram.

The absence of confirmed leaks of internal communications and the lack of reliable information regarding the group's membership make it impossible to accurately determine KillNet's size and organizational structure. Available evidence suggests that the group's primary strength lies not in centralized command and control, but in its ability to rapidly mobilize external supporters to conduct coordinated cyber and information operations.

Support the organization's activities: https://donate.shum-ng.org/

Tactics and Attack Techniques

Since the beginning of the Russia–Ukraine war, the group has successfully disrupted websites and interfered with the operations of organizations across multiple NATO countries. Although such attacks typically do not pose a direct threat to critical systems, they can cause significant operational disruptions and substantial financial losses due to service outages and lost revenue. Beyond their economic impact, KillNet's activities demonstrate an intent to disrupt communications and test potential targets for more advanced operations. Examples include the attack against an election-related website in the U.S. state of Kentucky and the group's claims of obtaining personal data belonging to Lockheed Martin employees, which could potentially be used for subsequent harassment or targeted operations. This reflects a gradual escalation in the group's cyber activities, with targets extending beyond direct participants in the conflict to include personnel from the defense industrial base and elements of civilian infrastructure. (4)

In addition, KillNet and similar hacktivist groups primarily employ DDoS attacks to attract public attention and generate media impact rather than to inflict long-term or large-scale damage. Most of the group's attacks last less than 12 hours, with commonly observed attack vectors including TCP SYN floods, TCP ACK floods, and malformed or anomalous network packets. To conduct these operations, the group is believed to rely on DDoS scripts, stresser services, botnets, and traffic source spoofing. The absence of ransom demands indicates that KillNet's objective is not financial gain.

Typical KillNet Operational Cycle

1. Target Selection: Typically triggered by a political event.
2. Reconnaissance: Passive and active reconnaissance.
3. Attack Preparation:
    a. Public announcement of the campaign.
    b. Mobilization of supporters.
    c. Preparation of attack infrastructure.
4. Execution of the DDoS Operation
5. Information Exploitation of the Results:
    a. Dissemination of narratives and media coverage.
    b. Recruitment of new participants by highlighting the perceived success of the operation.

To coordinate its attacks, KillNet relies on its Telegram channels, where it publicly identifies targets and provides supporters with instructions regarding the timing and execution of DDoS campaigns. The group's primary attack techniques include ICMP Flood, IP Fragmentation, TCP SYN Flood, TCP RST Flood, TCP SYN/ACK Flood, NTP Flood, DNS Amplification, and LDAP Connection-less (CLDAP) Amplification.

Over time, KillNet also expanded its arsenal by incorporating ransomware-wiper malware. In 2022, the group employed the Chaos 4.0 builder, which differs from traditional ransomware by overwriting large user files with random data instead of encrypting them, making recovery impossible. For this reason, the malware is classified as a wiper—malicious software designed to permanently destroy data.

If threats such as KillNet are not detected and contained in a timely manner, the only practical means of recovering affected information may be existing backups. Any data that has not been included in backup copies at the time of the attack may be permanently lost. (4)

Support the organization's activities: https://donate.shum-ng.org/

MITRE ATT&CK

- **T1498 – Network Denial of Service**

Confidence: High

This is the technique most strongly associated with KillNet. The group has employed TCP SYN Flood, TCP ACK Flood, ICMP Flood, DNS Amplification, and CLDAP Amplification attacks.

In its March 2023 analysis, Microsoft Security identified DDoS attacks as KillNet's primary operational capability. This attack type remains a relatively simple, inexpensive, and anonymous method of disrupting websites and online services.

- **T1595 – Active Scanning**

Confidence: High

Before launching DDoS campaigns, the group must identify target IP addresses, web resources, DNS infrastructure, and other externally accessible assets.

- **T1583 – Acquire Infrastructure**

Confidence: High

Virtually all large-scale KillNet DDoS campaigns have required the use of third-party infrastructure, including VPS instances, botnets, and leased servers. This was particularly characteristic of the group's early stage, when it operated as a DDoS-for-hire service.

- **T1589 – Gather Victim Identity Information**

Confidence: Medium

In the Lockheed Martin case, KillNet claimed to have obtained employees' personal information. Such targeting typically involves collecting email addresses, profiling employees through publicly available sources, and leveraging open databases.

- **T1584 – Compromise Infrastructure**

Confidence: Medium

Part of KillNet's botnet infrastructure may have consisted of previously compromised systems. The use of compromised infrastructure is common in DDoS operations of this scale.

- **T1499 – Endpoint Denial of Service**

Confidence: Medium

In several incidents, the group attempted to overwhelm specific services and web applications. However, the majority of confirmed cases are more accurately classified as Network Denial of Service (T1498).

- **T1485 – Data Destruction**

Confidence: Low-Medium

Following reports that KillNet employed Chaos 4.0 and ransomware-wiper malware, it is reasonable to assess that the group may have used data destruction techniques. However, this has not been a core component of KillNet's operational tradecraft.

Source: https://www.acronis.com/en/tru/posts/killnet-ransomware-a-wiper-from-the-chaos-family/?utm

Support the organization's activities: https://donate.shum-ng.org/

Information Operations

KillNet uses DDoS attacks not primarily as a means of destroying infrastructure, but as a mechanism for supporting information and psychological operations. In many cases, the actual impact of the attacks was limited or short-lived; however, extensive media coverage and the group's activity on Telegram enabled it to create the impression of far more significant operational success. This suggests that the information effect is one of KillNet's primary objectives, alongside the technical disruption of targeted systems.

Similar to Russian intelligence services, KillNet actively employs information influence techniques, including propaganda, disinformation, and the dissemination of false or misleading narratives. For example, in an interview with RT, the group's leader, KillMilk, claimed to possess evidence that the United States had created the COVID-19 virus.

Source: https://russian.rt.com/world/article/1059107-killnet-hakery-ssha-razoblachenie

Through their Telegram channels, KillNet and KillMilk make extensive use of modern visual communication formats, including memes, GIFs, emojis, and short videos to disseminate threats, propaganda, and announcements of their cyber operations. These activities also indicate that the group closely monitors publications by cybersecurity researchers and other open-source reporting related to its activities.

Summary

The primary characteristics and tactics of KillNet include:

- Targeting NATO member states and countries whose political positions conflict with the interests of Russia.
- Predominant use of DDoS attacks as its primary operational tool.
- A strong focus on government websites and public sector institutions.
- Publicly announcing attack campaigns and intended targets through Telegram channels prior to execution.
- Cooperation with other pro-Russian hacktivist and cybercriminal groups.
- Information and Psychological Operations

Support the organization's activities: https://donate.shum-ng.org/

Significance and Threat Assessment

Although most of KillNet's attacks have not resulted in long-term operational consequences, the group's activities illustrate the growing role of unofficial pro-Russian hacktivist communities alongside state-linked cyber groups such as Fancy Bear and Sandworm. These groups are becoming increasingly organized and capable of conducting attacks against any targets they perceive as hostile to Russia. A similar trend can be observed on both sides of the Russia–Ukraine conflict, reflecting the globalization of cyber conflict. Participation is no longer limited by geography, as volunteers from virtually any country with Internet access can contribute to cyber operations. The absence of geographic constraints and the difficulty of identifying participants significantly complicate the work of cybersecurity professionals and government authorities.

Although KillNet's leadership has experience operating DDoS services and botnets, the majority of the group's operations have relied on publicly available DDoS scripts and IP stressers—tools designed to generate large volumes of Internet traffic. Cybersecurity experts caution against underestimating politically motivated cyber actors, as they are not driven primarily by financial gain and may be willing to employ increasingly destructive malware in the future.

The group's principal strength lies not in conducting sophisticated cyber operations, but in its ability to rapidly mobilize large numbers of participants to execute mass DDoS campaigns and generate a significant information and psychological impact. A key element of KillNet's operations is the extensive promotion of its own activities, allowing the group to amplify public attention regardless of the attacks' actual technical effectiveness. A notable example is the attack against U.S. airport websites, which KillNet portrayed as a major blow to the United States, despite the attack causing no significant damage and lasting less than 20 minutes. In several cases, the group's public messaging has contributed to an exaggerated perception of its capabilities, leading some incidents to be incorrectly attributed to KillNet or to receive disproportionate media attention relative to their actual technical impact.

Despite the considerable media attention surrounding KillNet, most of its operations have not resulted in prolonged disruption of critical infrastructure or significant technical consequences. In my assessment, KillNet's primary strength lies not in the sophistication or destructive nature of its cyberattacks, but in its ability to use cyber operations as a vehicle for information and psychological influence.

Accordingly, DDoS attacks primarily serve as a means of attracting public attention, mobilizing supporters, and reinforcing pro-Russian narratives within the information environment. The greatest threat posed by KillNet is therefore not the technical impact of its attacks, but its ability to generate information resonance, disseminate propaganda, and create an inflated perception of its capabilities among target audiences.

Support the organization's activities: https://donate.shum-ng.org/

Recommendations for Mitigating DDoS Attacks

Completely eliminating the risk of DDoS attacks is not possible; however, organizations can significantly improve their resilience against such incidents. The UK National Cyber Security Centre (NCSC) recommends focusing on five key areas:

1. Understanding critical services and leveraging provider-side protection.
2. Scaling infrastructure and resources.
3. Developing an incident response plan.
4. Conducting regular testing.
5. Continuously monitoring infrastructure.

To strengthen their defensive posture, organizations should:

- Implement Web Application Firewall (WAF) solutions to filter malicious traffic and protect web applications from application-layer attacks.
- Deploy dedicated DDoS mitigation services and coordinate with Internet service providers (ISPs) and cloud service providers capable of filtering malicious traffic at the network level.
- Adopt a Multi-CDN architecture to distribute traffic across multiple content delivery networks, reducing the risk of service disruption caused by the failure or saturation of a single provider.
- Ensure the scalability of critical services by leveraging cloud technologies, load balancing, and automatic horizontal scaling mechanisms.
- Implement network traffic monitoring, centralized logging, and anomaly detection systems to rapidly identify indicators of DDoS activity.
- Utilize rate limiting, geographic traffic filtering (geo-blocking where appropriate), and network segmentation to reduce the impact of attacks.
- Develop and maintain a comprehensive DDoS incident response plan defining roles and responsibilities, communication channels, and response procedures in the event of an attack.
- Conduct regular cybersecurity training, tabletop exercises, and technical testing to validate both personnel readiness and the effectiveness of defensive controls.

Additionally, organizations should minimize the amount of publicly available information about their personnel, infrastructure, and operations. Reducing publicly exposed information decreases the likelihood that hacktivist groups, cybercriminals, or other threat actors will exploit it to support information and psychological operations, disinformation campaigns, or targeted cyberattacks.

Support the organization’s activities: https://donate.shum-ng.org/

Sources

1. https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf
2. https://www.ncsc.gov.uk/guidance/preparing-denial-service-dos-attacks
3. https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ddos.html
4. https://westoahu.hawaii.edu/cyber/uncategorized/killnet-russian-hacktivists-ddos-us-airports-government-websites/
5. https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf
6. https://flashpoint.io/blog/killnet-killmilk-private-military-hacking-company/
7. https://www.lawfaremedia.org/article/what-impact-if-any-does-killnet-have

Support the organization’s activities: https://donate.shum-ng.org/