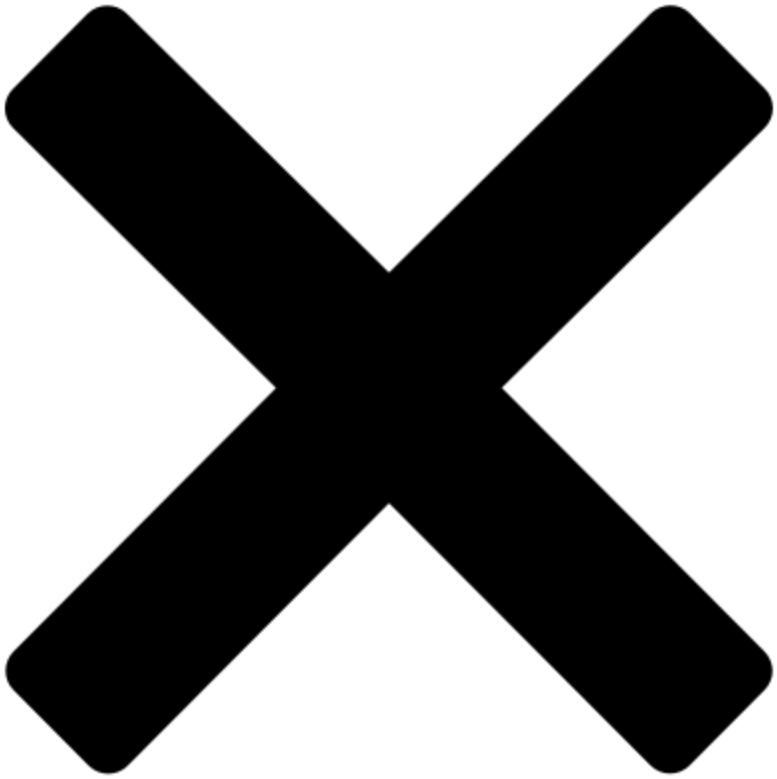
KillNet Showcases New Capabilities While Repeating Older Tactics

mandiant.com/resources/blog/killnet-new-capabilities-older-tactics



Key Judgments

- Mandiant Intelligence assesses with high confidence that operations for which the pro-Russia hacktivist collective KillNet has claimed responsibility consistently mirror Russian strategic objectives, although we have not yet uncovered direct evidence of the collective's collaboration with or direction from Russian security services.
- Mandiant assesses with moderate confidence that the collective's regular creation and absorption of new groups is at least partially an attempt to continue to garner attention from Western media and to enhance the influence component of its operations.

- KillNet's claimed operations have overwhelmingly focused on targets in the United States and Europe, even including operations from its claimed affiliates like Anonymous Sudan that purport to be focused on objectives unrelated to the Russian state.
- Anonymous Sudan's successful disruption of Microsoft services in June 2023 marked a significant increase in observed capabilities of the KillNet collective, which had previously struggled to impact claimed targets of previous operations. Paired with KillNet's reported compromise and leak of North Atlantic Treaty Organization (NATO) documents, this sudden increase in capability could indicate significant investment from more sophisticated actors, particularly when measured against KillNet's capabilities since the collective's inception in late 2021.

Background

In early 2022, Mandiant predicted that Russian cyber threat activity associated with the invasion of Ukraine would affect government and private sector targets in third-party countries, particularly neighboring countries, North Atlantic Treaty Organization (NATO) allies, and other nations voicing support for Ukraine. Russian government-linked actors have historically employed false hacktivist facades as a means of obscuring their role in targeting Western countries. Mandiant has previously identified instances of self-proclaimed hacktivist groups coordinating with such actors in the context of the war.

While we have not observed direct ties between KillNet and the Russian government, we cannot exclude the possibility of coordination, or more substantial ties, between some or all groups comprising the collective. We expect KillNet and its affiliates to continue conducting distributed denial-of-service (DDoS) and hack-and-leak operations intended to disrupt government and critical infrastructure functions in countries providing financial, economic, diplomatic or military support to Ukraine.

- Mandiant has tracked KillNet activity back to January 2022, despite a claim by the collective's alleged founder that it began operations in 2021. This claim could be an attempt to separate the group from Russian government interests and establish its legitimacy as a genuine hacktivist collective.
- The collective has claimed responsibility for DDoS attacks, data theft, and leaks against entities across multiple industries, including transportation, defense, government and military, financial services, global institutions, and telecommunications.

- KillNet's targeting has consistently aligned with established and emerging Russian geopolitical priorities, which suggests that at least part of the influence component of this hacktivist activity is intended to directly promote Russia's interests within perceived adversary nations vis-a-vis the invasion of Ukraine. The collective's activity also supports domestic Russian promotion of support for the war. As Russian government rhetoric has focused on various nations, we observed the group claim attacks targeting those same nations shortly thereafter.

    Since the beginning of 2023, the majority of observed KillNet targeting has focused on the U.S., Europe, and international institutions such as NATO. We have previously observed targeting in countries including Germany, Denmark, Sweden, France, Poland, Slovakia, Ukraine, Israel, the United Arab Emirates (UAE), and other NATO ally and partner countries such as Japan.

KillNet Appears to Increase Capabilities

Throughout its existence, KillNet's activities have primarily centered around DDoS attacks that generate only shallow impacts lasting short periods of time. However, the self-proclaimed hacktivist group Anonymous Sudan appears to have increased KillNet's capabilities and the group has become the collective's most prolific affiliate in 2023, conducting a majority of claimed DDoS attacks. Significantly, Anonymous Sudan has caused significant disruptions at a level not observed by KillNet affiliates previously.

> In June 2023, Anonymous Sudan claimed an operation targeting Microsoft services. Later in the month, Microsoft officially confirmed that numerous outages of its products were a direct result of DDoS attacks conducted by Anonymous Sudan.

Additionally, while KillNet has targeted NATO countries and organizations since early to mid-2022, it declared a focused operation against NATO in early 2023 and created a Telegram channel in April 2023 dedicated to this operation. It began referring to this operation as "FuckNATO" and using the hashtag #fuckNato. Subsequently, KillNet claimed to have compromised NATO's training site, Joint Advanced Distributed Learning, and published dozens of purportedly leaked images on its channels. While we cannot validate these claims, there are indications that some of these documents are legitimate, which would demonstrate another significant increase in capability for the group.

> In early 2023, KillMilk, the claimed founder of KillNet, attempted to ransom the purportedly stolen documents to NATO for 3 bitcoin, possibly in part to increase attention surrounding the activity. While no substantive posts have been made to the FuckNATO channel since late April 2023, Mandiant anticipates that KillNet and its affiliates will continue to target NATO for the continued future, with the potential for developments in the war in Ukraine to reinvigorate targeting.

In mid-June 2023, KillNet announced that the collective and actors claiming to be from the Russian ransomware group REvil were collaborating in a joint operation targeting Western financial systems. Days later, KillNet claimed to target the European Investment Bank (EIB). Beyond the disruptive intent implied by these groups' claimed plans, this activity appears at least partially intended to maximize the media coverage of the groups and their anti-Ukraine messaging by prioritizing high-profile targets in a strategic sector.

> EIB sites were down for at least a day and EIB confirmed the attack in a tweet in which it stated it was facing a cyber attack that had affected the availability of two of its main pages. Similar to the attack on Microsoft, the successful disruption of a high-profile organization like the EIB indicates a significant increase in KillNet's DDoS capabilities compared to previous claimed operations with little noticeable impact.

DDoS Trends and Statistics Jan. 1, 2023 – June 20, 2023

Mandiant reviewed the Telegram channels of KillNet and its affiliates and captured counts of claimed attacks that included checkhost links to corroborate actor statements. Although we cannot verify that the service disruptions occurred directly as a result of KillNet operations, the data below illustrates claims that overlap temporally with verified service disruptions. This blog focuses on the most prolific affiliates of KillNet, and as a result several groups mentioned in the statistics are not discussed elsewhere in this report.

- Between Jan. 1 – June 20, 2023, Mandiant identified more than 500 distinct victims that the KillNet collective has allegedly targeted with DDoS attacks.
- Consistent with KillNet activity in 2022, the majority of claimed attacks in 2023 targeted entities in the U.S. and Europe. Anonymous Sudan appeared to be a core driver of claimed attacks targeting countries further afield, and it is primarily responsible for the recent surge of Israeli targeting; however, nearly half of claimed Anonymous Sudan attacks still focused on U.S. or European organizations.
- Anonymous Sudan accounted for 63% of total identified DDoS attacks claimed by the KillNet collective in 2023. The group only emerged in January 2023, making the proportion of KillNet operations they comprise additionally notable.
- The top most targeted organizations included those from technology and social media, NATO, and the transportation sector. This generally aligns with historic targeting since KillNet's inception.
- We observed limited instances of Russia-affiliated domains being targeted. These infrequent instances appeared to primarily involve fringe domains and stand apart from the collective's core threat activity. We note separately that we have previously observed limited other instances of KillNet claiming Russian targets, such as high-profile Russian individuals opposed to the war.

Figure 1: DDoS attacks by date and actor

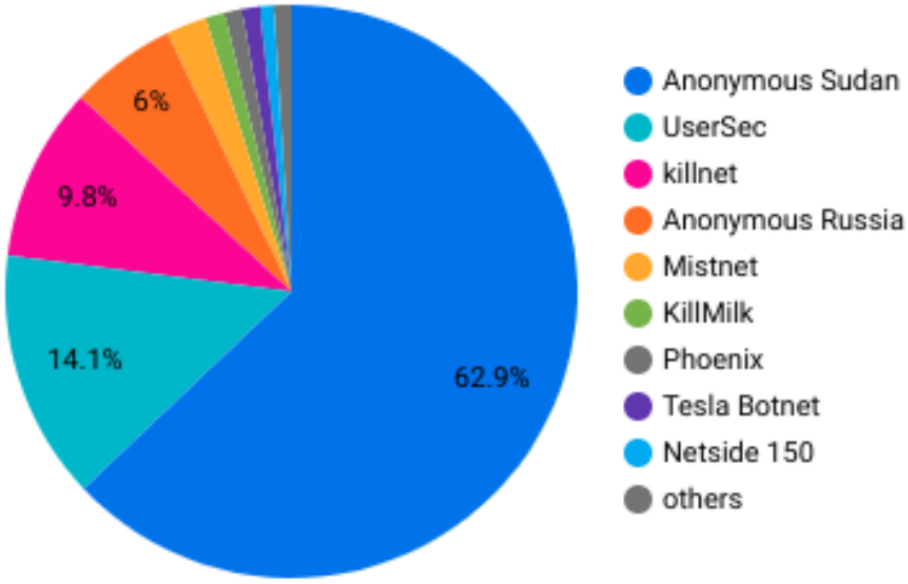


Figure 2: KillNet-associated groups claiming DDoS attacks

Figure 3: Countries targeted by DDoS attacks claimed by KillNet, January – June 2023

Claimed Cyber Crime Collaboration

Since early 2022, KillNet has claimed on multiple occasions to be partnering or coordinating with several criminal elements, including multiple occasions in which it claimed to be working with the widely known ransomware group REvil. However, besides actor claims, we have observed no independent information that the groups have collaborated. We have not observed indications that the group claiming to be REvil that took part in the attack on the EIB was connected to the widely known ransomware group. Notably, the Telegram channel in which actors claiming to be from REvil claimed links with KillNet had been created only days before the operation began on June 15, 2023. KillNet previously claimed various links to REvil and Conti, which we were unable to verify, including:

- On April 16, 2022, KillNet dedicated its attack on a U.S. energy company to REvil.
- On April 21, 2022, KillNet also stated that "REVIL is back in the ranks."
- On June 16, 2022, KillNet called on both Conti and REvil "to an unforgettable joint safari in the United States, Italy, and Poland."
- On June 25, 2022, KillNet messaging suggested that Conti was ready to fight, that Lithuania was its new testing ground for DDoS attacks, and that its "Zarya" hackers were preparing for cyber operations.

Composition of the KillNet Collective

Killnet's structure, leadership, and capabilities have undergone several observable shifts over the course of the last 18 months, progressing toward a model that includes new, higher profile affiliate groups intended to garner attention for their individual brands in addition to the broader KillNet brand (Table 1). Multiple new groups have joined the collective as others have overtly separated or appeared to become inactive or disbanded. Notably, through this process the collective has appeared to pivot from the seemingly hierarchical structure of squads it established in the early months of the Russian invasion of Ukraine.

> KillNet has also repeatedly promoted messaging related to changes or expansions in the collective's operations, ranging from KillNet reforming to become a "private military hacker company" to purported partnerships with cyber crime groups. However, these claims often appear to outpace documentable shifts in the collective's operations.

Table 1: KillNet-associated Telegram channels of interest

Affiliate Name	**Telegram Channel Creation Date**	**Still Active**	**Still Affiliated with KillNet**
Tesla Botnet	April 17, 2023	Yes	Yes
BlackSkills	March 12, 2023	No	Dormant
KillNet LATAM	Feb. 2, 2023	Yes	Yes
Anonymous Sudan	Jan. 18, 2023	Yes	Yes
UserSec	Jan. 8, 2023	Merged	Yes
Titan Stealer	Oct. 20, 2022	Yes	Yes
KillMilk	Aug. 7, 2022	Yes	Yes
Anonymous Russia	July 10, 2022 (original channel); April 15, 2023 (new channel)	Yes	Yes
Devils Sec	June 2, 2022	Yes	Yes
Zarya	March 18, 2022	Yes	No

We Are KillNet (main channel)	Jan. 23, 2022 (original); Feb. 26, 2022 (new channel)	Yes	Yes
Phoenix	Jan. 5, 2022	Yes	Unknown
SkyNet Botnet/Godzilla-Botnet	Jan. 9, 2023/Dec. 28, 2021	Yes	Unknown

KillMilk: Self-Proclaimed Founder of KillNet

KillMilk continues to be a central coordinator for the KillNet Collective, despite claims of leaving the group in mid-2022. We cannot independently confirm KillMilk's claims of having previous affiliation with the hacktivist group Universal Dark Service. Although KillMilk claims the activity was by their own group, the previous operations of Universal Dark Service targeted the Russian government and were critical of its actions. This is in stark contrast to the avowed support by KillNet and KillMilk of the Russian government in its invasion of Ukraine and against the West. One possibility is that such claims were made disingenuously as an attempt to establish KillNet's credibility and/or as a means to distance the group from the Russian government.

Zarya Splinters from KillNet

Zarya's Telegram channel was created in March 2022, although the group's alleged leader claimed that elements of Zarya existed well before this, and were previously known by various names including "0x000000" and "Quarantine" (Russian: Карантин). Almost immediately after its channel's creation, the group began posting files from compromised Ukrainian organizations. Zarya was the most active "squad" within KillNet until it announced a rebrand in October 2022 in which ended cooperation with KillNet.

In April 2023, media reports suggested that the U.S. government determined that Zarya breached a Canadian oil pipeline. Furthermore, these reports indicated that Zarya was cooperating with or being handled by officers of Russia's Federal Security Service (FSB). Currently, Mandiant can neither validate claims related to Zarya's hacking capabilities, nor those related to the group's potential links to the FSB. Russia has historically used self-proclaimed hacktivist groups as a means to obfuscate its role in operations against Western nations and it is plausible that Zarya or various pro-Russia hacktivists that have risen to prominence since Russia's invasion of Ukraine may either be cooperating or coordinating with, or a front for, the Russian security intelligence services.

– How is Zarya different from KillNet?

> **"Back in KillNet, we were the only division dedicated exclusively to target hacking. We didn't do DDoS. In fact, this is the only thing in which we differed from others then and differ in this from many now.**

Figure 4: Quote from interview with Zarya's alleged leader (machine translated from Russian)

Anonymous Sudan

Mandiant first observed the self-proclaimed hacktivist group calling itself "Anonymous Sudan" in January 2023 and the group soon after declared allegiance to KillNet. Initially, the group claimed DDoS attacks against entities located in Western countries, seemingly prioritizing Sweden, the Netherlands, and Denmark. Anonymous Sudan has targeted organizations associated with infrastructure and key services, including in government and private sectors. The attacks that Anonymous Sudan has claimed in support of KillNet, both before and after it officially joined the collective, have broadened the geographic scope of its targeting to include entities elsewhere in Europe and the U.S.; it has since continued to expand the scope of its targeting further afield to include countries such as Israel and Ethiopia.

- The group's initial post on the Anonymous Sudan Telegram channel stated, "We will attack any country with cyber attacks against those who oppose Sudan," and continued messaging from the group has asserted that it is comprised of Sudanese individuals and has explicitly denied that the group is comprised of Russians or that it has links to Russia beyond support for KillNet's cause.
    - Messaging that Anonymous Sudan has promoted surrounding attacks it has claimed to take under its own initiative has cited motivations related to the defense of Islam and/or the interests of Sudan.
- The name "Anonymous Sudan" is likely an attempted appropriation of the brand of the well-known hacktivist collective "Anonymous," similar to another KillNet affiliate, "Anonymous Russia."

Outlook

KillNet has remained relatively consistent in its targeting of Ukraine's supporters and prioritization of DDoS attacks since Russia invaded in February 2022, and despite new capabilities, the collective has hardly altered its targeting patterns. While Mandiant cannot confirm collaboration or cooperation with Russian security services, KillNet's targeting of victims consistently reflects the interests of the Russian state. The collective's apparent significant growth in capabilities, demonstrated by Microsoft's confirmation that Anonymous

Sudan was responsible for the outages they experienced, potentially indicates a significant increase in outside investment in the collective, further suggesting a potential tie to the Russian state. We anticipate that KillNet and its affiliates will continue DDoS attacks and become more brazen in their targeting of organizations.

Mandiant's Mitigation and Hardening Recommendations for DDoS Attacks

Organizations that may be targeted by KillNet or any self-proclaimed hacktivist fronts should look to harden their networks to protect against DDoS attacks: Distributed Denial of Service (DDoS) Protection Recommendations.