KillNet’s Targeting of the Health and Public Health Sector (December 2022 – March 2023)

Executive Summary
Pro-Russia hacktivist group, KillNet, has actively targeted the United States health and public health (HPH) sector since December 2022. Their signature distributed denial-of-service (DDoS) attacks on critical infrastructure sectors typically only cause service outages lasting several hours or even days. However, the range of consequences from these attacks on the HPH sector can be significant, threatening routine to critical day-to-day operations. An examination of the group’s cyber offensive from December 2022 to March 2023 provides insight into how and why they target the healthcare industry, and recommendations for how HPH organizations can better protect themselves.

Overview
On January 28, 2023, KillNet and its affiliates conducted numerous coordinated DDoS attacks, targeting HPH organizations in the U.S. and several NATO countries, apparently, in retaliation for the allocation of tanks to and in support of Ukraine. Active since at least January 2022, KillNet is known for conducting DDoS campaigns against multiple critical infrastructure sectors in countries that support Ukraine in the war between Russia and Ukraine or appear to be “anti-Russia.” Although their primary type of cyber-attack method usually does not cause major damage, it can cause service outages to vulnerable systems lasting several hours or even days. Whereas many hacktivist groups abstain from targeting HPH organizations, the group has dispassionately targeted hospitals and medical organizations across the sector.

Impact to HPH Sector
In the late January 2023 attack, over 90 known orchestrated DDoS attacks took place on healthcare systems (covering multiple hospitals), lone hospitals, and medical centers. Of these, 55% were healthcare systems with at least one hospital and lone hospitals with Level I trauma centers, which provide the most comprehensive and highest level of trauma care to critically ill or injured patients. As they are normally large establishments with considerable patient data to enter and exploit, these types of HPH organizations are ideal targets for KillNet and its affiliates.

Figure 1: Graph of HPH Trauma and non-Trauma Organizations Allegedly Targeted by KillNet on January 28, 2023.

Figure 2: Map of 48 U.S. States Allegedly Targeted by KillNet on January 28, 2023.
Since the February 24, 2022 Russian invasion of Ukraine, KillNet continued its harassment of U.S. and NATO countries’ critical infrastructure. By December 2022, their targeting of the HPH sector was apparent, with announcements of their coordinated attacks across multiple countries posted on the Telegram channel of its founder and leader, KillMilk. A timeline of the posts exclusively targeting the sector from both KillMilk and KillNet can be found below. For purposes of this case study, only threats to and attacks on the HPH sector will be examined.

**December 2022**

**KillMilk**

United States Congress, you will regret your actions! I give my word and stake the fate of Killnet. Starting today, your citizens' money will begin to disappear. Today, your medical systems for tracking severe patients will be disabled. Your citizens will pay a huge price! I will sell all the data that I have about the credit cards of American citizens. The amount of my archive reaches 2.5 million ₽. I do not accept and will not accept apologies for insulting the DPR flag. Your destiny is darkness, your future is death.

We Are Killnet.

*Figure 3: KillMilk threatens U.S. Congress with extortion of health and personal data of Americans because of U.S. military aid to Ukraine. (December 8, 2022)*

**KillNet**

We are KillNet.

*Figure 4: KillNet targets U.S. DoD healthcare subsidiary, Humana Military. (December 16, 2022)*

**January 2023**

**KillMilk**

Всё очень просто - за поддержку нацистов Украины, мы сносим все сети медицинских учреждений этих стран:

- Сва
- Португалия
- Испания
- Германия
- Польша
- Финляндия
- Норвегия
- Нидерланды
- Великобритания

Эта информация не стоит ваших косых взглядов. Лучше вспомните Донбасс - расстрелы больниц, школ и детских садов. Эти твари каждую минуту жаждут смерти и стимулируют свою мечту с помощью тяжелого оружия.

Проснись земля - пока не поздно! У@БЁЙ ПЕРВЫЙ!

50.1K 06:23

*Figure 5: KillMilk announces targeting of U.S. and European HPH Sector in response to support for Ukraine. (January 27, 2023)*

**KillNet**

WE ARE KILLNET

14.04.2023

Сегодня, ваши деньги будут уходить. Сегодня, ваше здравоохранение будет уничтожено. Сегодня, мы уничтожим ваши сети.

*Figure 6: KillNet re-posts article on their targeting of HPH sector. (January 31, 2023)*
February 2023

Figure 7: KillMilk threatens specific U.S. medical organizations. Not pictured: other countries’ medical organizations also threatened include Finland, Germany, the Netherlands, Norway, Poland, Spain, and the United Kingdom. (January 28, 2023)

Figure 8: KillNet posts open invitation to its affiliates to join mass attack on United States and includes medical-related screenshot announcement of a "huge surprise" for American and European audiences. (February 1, 2023)
Figure 9: KillMilk announces DDoS attack on specific U.S. HPH sector organizations. (February 2, 2023)

Figure 10: KillNet announces more intended targets in disruption to HPH sector. (February 2, 2023)
March 2023

Few incidents in the HPH sector have been attributed to KillNet this month, with the exception of a DDoS attack on a laboratory, blood, and pharmaceutical sub-industry organization. While little to no content on their Telegram channel could be found that indicated a targeting of the sector, one information security publication unveiled a campaign that had gone previously unnoticed. On March 17, 2023, Microsoft Security published its observations that KillNet had been targeting healthcare applications using the Microsoft Azure infrastructure for over three months.

The findings illuminated new trends on KillNet and other hacktivist organizations’ characteristic DDoS campaigns in Azure from November 18, 2022 to February 17, 2023. Of those, Microsoft observed:

- An increase from 10-20 attacks in November to 40-60 attacks daily in February.
- The types of HPH organizations attacked included pharma and life sciences with 31% of all attacks, hospitals with 26%, healthcare insurance with 16%, and health services and care also with 16%.
- In contrast to overall DDoS attack trends for 2022, in which Transmission Control Protocol (TCP) was the most common attack vector, 53% of the attacks on healthcare were User Datagram.
Protocol (UDP) floods, and TCP accounted for 44%, reflecting a different mixture of attack patterns used by adversaries.

**Figure 12: Microsoft Security graph of DDoS attacks on healthcare applications in Azure. (March 17, 2023)**

**Figure 13: Microsoft Security graph of types of healthcare organizations targeted by DDoS attacks. (March 17, 2023)**

**Leadership and Key Individuals**

On January 24, 2022, the Telegram channel “We are KillNet” was created, offering a DDoS/Stressor tool on various URLs. Ostensibly, KillNet appears to have a semi-formal organization, founded by KillMilk, with...
over 90,000 followers on their Telegram channel. The group collaborates with and recruits affiliates with similar ideologies or goals that align with Russian interests. Demonstrating that the group is acutely aware of their online image, KillNet recently rebuked one online analysis of their organizational structure, or lack thereof. In a March 21, 2023 post, the group emphasized that they are decentralized, that KillNet is just an “idea” that unites the cyber patriots of Russia, and that they are not supported by the [Russian] state.

Ironically, this comes just one week after another KillMilk post detailing his creation of a new private military hacking company, Black Skills. The new group appears to be highly organized and structured with 24 “departments” in charge of various distinct functions such as intelligence, public relations, investments, accounting, and general staff. Adding more formality to the initiative, KillMilk even requires every applicant to list their skills whether they have served in the military or as public servants in a formal questionnaire. It remains unknown whether this is a rebranding of KillNet or an organizational initiative to better separate more skilled members from the rest of the community. Undeniably, however, is the fact that since the February 2022 Russian invasion of Ukraine, KillNet and its leader, KillMilk have garnered support from other hacktivist organizations, making them leaders in the cybercriminal underworld.

KillMilk, left the group on July 27, 2022, seemingly, to recruit a new group, but both continue to share the others’ posts on Telegram, indicating some level of support still exists. KillMilk’s next day post, “What I would do for my country now would be dangerous enough for my team. So I made the decision to withdraw from KillNet for their own safety.” signals a possible departure due to threat from law enforcement. A similar trend can be seen across other pro-Russian hacktivist groups like Evil Corp and Conti, which splintered into smaller groups and rebranded to evade law enforcement. A Mandiant report also reinforced this trend of loosely connected Russia-linked ransomware groups splintering into smaller cells to obscure their identities and evade crackdowns. Though not much is known about the threat actor, the group’s new leader is a hacker using the name Blackside, and specializes in ransomware, phishing, and crypto theft.
Nomenclature and Associations
A post of KillNet’s January 24, 2023 DDoS campaign against Germany highlighted many of their current affiliates, among them, Infinity Hackers, ANONYMOUS RUSSIA, KillNet Collective, NETSIDE GROUP, National Hackers Russia, KILLMIR, Passion Botnet, and PHOENIX. This campaign, while not against the HPH sector, revealed that KillNet has a huge influence over over pro-Russian groups. However, in a March 12, 2023 posting on his Telegram channel, former KillNet leader, KillMilk, stated that he had to “shrink [their] ranks from useless mobs and traitors” in preparation for the new Black Skills organization. On March 26, 2023, KillMilk subsequently announced that KillNet had undergone a reform of personnel. It is still unknown how KillNet’s proposed reorganization will pan out, but owing to their successful attack record and the current admiration they have online and across several Russian media outlets, it is likely they will continue to grow in size and support.

Unlike the skilled hackers working for Russia’s security services’ groups like Fancy Bear and Sandworm, KillNet is radically different. Behaving in a more reactionary manner, the group of hactivists oftentimes appear to work in an emotional way, seeking revenge and retaliation against anything perceived as anti-Russia or pro-Ukraine, given the current conflict between the two powers. While KillNet has been criticized on some forums for perceiving to be seeking cooperation from Russian security services, any ties to official Russian government organizations such as the Federal Security Service (FSB) or the Foreign Intelligence Service (SVR) remain unconfirmed.

Motivations
KillNet is hardly subtle in its political agenda. Since the group’s inception, they have always exhibited a pro-Russia or pro-Slavic state stance. This has garnered the support and coalescence of Russian and other Slavic hacktivist groups like the Belarusian Infinity Hackers. The promotion of a pro-Slavic sentiment, however, began to waver with the Russian invasion of Ukraine this past year, creating a new anti-Ukraine theme and strengthening their pro-Russian military theme. This, in turn, spurned a political antagonism.
toward any country or group that displayed or provided support to Ukraine during the conflict. While not exclusively their main target, the United States has historically been the “Main Enemy” to Russia during the Cold War. This anti-American posture breeds over into modern times, and especially in the cyberspace.

Interestingly, amongst the repository of boastful threats and attacks that KillNet and KillMilk both post on their separate Telegram channels, are numerous photo postings of cats or kittens that seemingly have no added strategic value, other than the fact that they like them. One such posting on January 23, 2023 even doxxes a Russian national and his parents for allegedly killing a cat. KillNet’s doxxing of a Russian national provides validation that they are more aligned with statecraft-level Russian support, but will make exceptions for low-level incidents that provoke offense.

In their assessment, SOCRadar reports that KillNet does not seem to be interested in financial gain. This is supported by donation links on and a review of their Telegram channel, where several posts ask for donations to support their network of hacktivists. However, like nearly all hacktivist groups, they aim to disrupt and harm organizations and critical infrastructure to procure a ransom.

Common Tactics, Techniques, and Procedures (TTPs)

In their March 2023 analysis, Microsoft Security highlighted that while KillNet uses DDoS as its main tool, they noted that that kind of attack method is a relatively easy, low-cost, and anonymous method of disrupting online services and websites. More so, KillNet and other similar hacktivist groups utilize them to draw attention than to do any major damage. Typically lasting less than 12 hours, attack vectors included TCP SYN, TCP ACK, and packet anomalies. KillNet and its affiliates likely launch attacks using DDoS scripts and stressors, recruiting botnets, and utilizing spoofed attack sources.
Like Russian security services, KillNet adopts similar active measure techniques in the form of propaganda, misinformation, and disinformation. In one Russian media interview on October 9, 2022, KillMilk continued his anti-American claims, stating in a media interview that his group had evidence that the United States created [the] COVID-19 [virus].

On their Telegram channels, both KillMilk and KillNet show that they are adroit in graphic design and have a penchant for using novel or “millenial” ways of announcing boastful threats or attacks, to include memes, gifs, emojis, and short edited videos. Demonstrating their hostility to the U.S. HPH sector, on February 4, 2023, five days after the release of HC3’s most recent Analyst Note on KillNet, former leader, KillMilk, posted a meme that seemingly threatened the U.S. Department of Health and Human Services (HHS). Whether signaling a future warning to HHS writ large or coincidentally in response to the Analyst Note, it has already been shown that the hacktivist group remains aware of open source articles or publications about their group (namely, from Medium user, CyberKnow, and online publicaton, SOCRadar).

As of March 30, 2023, a simple Google search for “KillNet” in English reveals that HC3’s previous Analyst Note on the group is the top third result. KillNet, KillMilk, and their affiliates’ proficiency in English on their Telegram channel demonstrate that their members have some degree of open source situational awareness. This was reinforced when they acknowledged postings of SOCRadar’s analysis of the threat group on December 17, 2022 and Medium user, CyberKnow’s, analysis of the group on March 21, 2023.

In their analysis, SOCRadar defined several of their prominent characteristics and TTPs of the group:

- 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 websites of governments or public institutions. 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.
They are associated with other hacker groups that have common goals or act in Russian interests.

Defense and Mitigations
There is no single action that can protect an organization from cyber threat groups, such as KillNet. Nevertheless, healthcare organizations need to take proactive measures to mitigate against a wide variety of attacks like DDoS. This Analyst Note presents a sample of mitigations, countermeasures, indicators of compromise, and other courses of action from various cybersecurity organizations and governmental publications as a guide to better prepare themselves against threats.

CISA Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

Health-ISAC – Distributed Denial of Service (DDoS) Attacks
https://h-isac.org/distributed-denial-of-service-ddos-attacks/

Microsoft Security

Palo Alto Network – Unit 42

SOCRadar
https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

MITRE ATT&CK
SOCRadar lists two reconnaissance techniques for KillNet from MITRE ATT&CK’s map: Active Scanning and Gather Victim Identity Information.

![MITRE Map](image-url)

Figure 20: MITRE Map of KillNet. (SOCRadar)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction. This technique can easily
be mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Adversaries may also gather information about the victim’s identity that can be used during targeting. Information about identities may include a variety of details, including personal data as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via phishing for information. Information about users could also be enumerated via other active means such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. Information about victims may also be exposed to adversaries via online or other accessible data sets. This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Identity Management

One of the easiest ways for hacktivists to get information about you is through your online presence. Anyone can research you with just a few clicks of the mouse and a quick Internet search. It is important to know what is publicly available about yourself, and then decide what to do about unwanted information. One such way is through Identity Management (IdM), a program that could be utilized by HPH sector employees to proactively protect themselves against KillNet’s and other hacktivists’ Gather Victim Identity Information reconnaissance technique.

IdM consists of the discovery, analysis, and management of an individual or organization’s identity elements, characteristics, and/or other attributes in public and non-public records, social media, and other unstructured data sources. IdM programs seek to improve an organization’s ability to mitigate current threats to its mission, capabilities, and personnel from adversarial and/or criminal entities seeking to exploit identity data, as well as identify emerging threats to organizational assets.

![Figure 21: Sample IdM mitigation recommendation pages from DoD Social Media Smartcard booklet.](image-url)
One sample toolset is the Department of Defense’s (DoD) Social Media Smartcard booklet. This comprehensive and regularly updated publication covers how to effectively manage one’s Social Networking Services (i.e., Facebook, dating apps, message-to-message apps, etc.), Digital Ecosystems (i.e., Amazon, Coinbase, YouTube, etc.), Devices (i.e., Android, iOS, gaming systems, etc.), and General Best Practices of recommendations and tips of online use for both adults and children. A link to the full booklet can be found [here](#).

**Relevant HHS Reports**

- **HC3: Alert - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure** (May 9, 2022)
- **HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure** (March 1, 2022)
- **HC3: Analyst Note – Healthcare Sector DDoS Guide** (February 13, 2023)
- **HC3: Analyst Note – Pro-Russian Hacktivist Group ‘KillNet’ Threat to HPH Sector** (January 30, 2023)
- **HC3: Analyst Note – Pro-Russian Hacktivist Group ‘KillNet’ Threat to HPH Sector** (December 22, 2022)
- **HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector** (March 1, 2022)

**References**


HC3 Analyst Note
April 5, 2023     TLP:CLEAR     Report: 202304051200


Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback