I. Introduction

KillNet is a cyber mercenary group that has emerged as a frontrunner among over a hundred similar groups stemming from proxy cyberwars. KillNet's primary strategies revolve around conducting low-level Distributed Denial of Service (DDoS) attacks against vital infrastructure, government services, airport websites, and media enterprises in NATO nations.

KillNet is also known for its robust and confrontational misinformation efforts targeted at its 90,000 Telegram followers. These campaigns involve openly taunting the victims of their DDoS attacks and issuing threats that suggest the attacks could result in loss of human life, contradicting their proclaimed anti-war stance.

KillNet directed its focus towards the Parliament's website, resulting in the site becoming temporarily unavailable. In response to an investigation initiated against KillNet due to its assault on the European Parliament, the group targeted Belgium's Cybersecurity Center.

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. KillNet has also claimed to have 280 members in the US, attributing an attack on Boeing to their US "colleagues".

KillNet's victimology is extensive and includes a variety of sectors and countries:

- **Geographical Focus**: The majority of KillNet's victims are in Europe, with over 180 documented attacks. North America has experienced fewer than 10 attacks
- **Targeted Industries**: Common targets include the financial industry, transportation, governmental institutions, and business services
- **Healthcare Sector**: KillNet has targeted the U.S. healthcare industry, causing concerns due to the potential impact on critical health services
- **Government Services**: Attacks on government websites have been reported in several countries, including Romania, Moldova, Latvia, and the United States
- **Transportation**: U.S. airports and other transportation systems have been targeted by DDoS attacks
- **Media Enterprises**: Media companies within NATO countries have also been affected

Over time, KillNet developed a semi-formal organizational structure with a significant presence on Telegram and began to expand its operations. The group started to build a global team of operators from the darknet, offering services such as misinformation, impact on network infrastructure, reputation killing, data exfiltration, and data leaks, along with DDoS attacks. They also developed their own tools and botnets after initially using open-source tools.

II. Primary Strategies of KillNet & Tactics, Techniques, and Procedures (TTPs)

KillNet's primary strategies revolve around DDoS attacks and brute-force dictionary attacks.

A. DDoS Attacks

KillNet primarily employs low-level DDoS attacks and has been known to use brute-force dictionary attacks. The group does not typically use sophisticated tools or strategies, and while their DDoS attacks can cause service outages, they usually do not result in major damage. KillNet conducts DDoS attacks on the OSI model's layer 4 (SYN flood attacks) and layer 7 (high volume POST/GET requests). These attacks aim to cause resource exhaustion by flooding a target service with malicious connection requests.

B. Brute-Force Dictionary Attacks

KillNet also employs brute-force dictionary attacks against various services. These attacks use predefined wordlists to hunt for exposed services that seek to exploit default or weak credentials. The group primarily targets services like FTP (port 21), HTTP (port 80), HTTPS (port 443), and SSH (port 22), with a particular focus on the root account. They also target Minecraft and TeamSpeak servers.

C. Targets of KillNet's DDoS Attacks

KillNet's DDoS attacks have primarily targeted critical infrastructure, government services, and media companies within NATO countries, including the U.S., Canada, Australia, Italy, and others. The group has also targeted organizations in the healthcare and public health sectors. Other targeted industries include the financial industry, transportation, and business services.

KillNet has also targeted or intends to target military entities, marine terminals and logistics facilities, other forms of transportation, and online trading systems. The group has been particularly active in targeting U.S. organizations, including state government websites and major airport domains.

In addition to these, KillNet has targeted international institutions such as NATO and 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.

It's important to note that while KillNet's DDoS attacks can cause service outages lasting several hours or even days, they usually do not cause major damage. However, they can disrupt essential services and pose a significant threat to organizations, especially those in critical sectors like healthcare.

D. Techniques, and procedures (TTPs)

KillNet's primary attack vector is DDoS, which involves flooding a target service with malicious connection requests, causing resource exhaustion. The group has also been known to engage in data exfiltration from targeted networks, including high-ranking officials' email inboxes and bank data.

In terms of tools, KillNet has used a variety of methods, including DDoS scripts and stressors, recruiting botnets, and utilizing spoofed attack sources. One In October 2023, KillNet began selling a new DDoS tool, which analysts fear will encourage more attacks. This tool is reportedly efficient and sophisticated, with precision-targeting capabilities and a user-friendly interface.

They utilize several known DDoS scripts, including "Aura-DDoS," "Blood," "DDoS Ripper," "Golden Eye," "Hasoki," and "MHDDoS". They also use a tool called "CC-Attack," a publicly available attack script that automates the use of open proxy servers and incorporates randomization techniques to evade signature-based detection. In addition, KillNet has been observed using slow POST DDoS attacks and other techniques such as ICMP flood, IP fragmentation, TCP SYN flood, TCP RST flood, TCP SYN/ACK, NTP flood, DNS amplification, and LDAP connectionless (CLAP) attacks.

E. Recruitements

KillNet's activities have not been limited to cyberattacks. The group has also engaged in recruitment, fundraising, and promoting their message through various channels, including social media to expand its support base, targeting individuals with diverse skill sets—including coders, network engineers, penetration testers, system administrators, and social engineers. Despite claims of the group's leader, KillMilk, stepping away from the group in mid-2022, he continues to be a central coordinator for the KillNet Collective.

In 2023, the group announced the launch of its Dark School, a cybercrime school that aims to train the next cohort and swell the ranks of the collective. KillNet recruits new members by actively seeking suitable candidates from supporters of their cause, leveraging various social media channels like Telegram and VK. They have a detailed form that potential recruits must fill out before they are considered for membership. KillNet operates with a military-like structure, with a clear top-down hierarchy and multiple smaller squads, which they call their "Legion," that act upon instructions given out in their Telegram channels.

III. TARGETS, IMPACT AND CONSEQUENCES OF KILLNET ATTACKS

The impact of KillNet's attacks can range from temporary service outages to potential financial losses and damage to reputation. Governmental responses have included classifying KillNet as a terrorist organization and issuing alerts through cybersecurity agencies.

A. Healthcare industry

KillNet has targeted the United States health and public health (HPH) sector since December 2022. Their signature DDoS attacks on critical infrastructure sectors typically cause service outages lasting several hours or even days. These attacks have severe consequences for patient care as they can interrupt patient care, lead to patient data loss, and disrupt communication between healthcare providers. In January 2023, KillNet and its affiliates conducted numerous coordinated DDoS attacks on healthcare organizations in the US, which resulted in service outages and significant disruption to routine and critical day-to-day operations. In some cases, the group has also exfiltrated data from a number of hospitals.

In the healthcare sector, Killnet's attacks have caused service outages lasting several hours or even days. These attacks have primarily targeted healthcare systems with at least one hospital and lone hospitals with Level I trauma centers. The group has also targeted pharmaceutical and life sciences industries.

The role of law enforcement in addressing Killnet's attacks includes investigating the incidents, coordinating with international law enforcement groups, and taking actions to disrupt the group's activities. For instance, the FBI, in coordination with international law enforcement groups and Europol, has previously infiltrated the infrastructure of other cyber threat groups.

The Cybersecurity and Infrastructure Security Agency (CISA) also plays a crucial role in helping organizations respond to such attacks. CISA provides resources and guidance to help organizations protect against cyber threats, and it works with affected organizations to mitigate the impacts of attacks.

B. Energy and financial industry

In the energy sector, the attacks could disrupt industrial control systems that support US energy infrastructure. While the impact on the energy sector's ability to provide localized services has been minimal so far, the threat remains. If successful, these attacks could potentially disrupt energy supply, leading to power outages and affecting critical infrastructure.

In the financial sector, DDoS attacks have become a growing concern. These attacks can cause intermittent downtime, forcing security staff to repel the attacks and potentially disrupting financial transactions. Killnet has even threatened imminent attacks on the SWIFT banking system and other financial institutions. While the actual impact of these threats is uncertain, they could potentially disrupt global financial transactions if successful.

It's important to note that while Killnet uses DDoS as its main tool, this method is typically used more to draw attention than to do major damage. However, the group has been increasing its capabilities and has shown a willingness to target critical infrastructure. Therefore, while the actual damage caused by Killnet's attacks has been minimal so far, the potential for more significant disruption exists.

C. Aviation industry

These attacks have primarily targeted public-facing websites of airports, causing them to slow down or become completely inaccessible. The group has targeted more than 30 European airports and several major U.S. airports, including Hartsfield-Jackson Atlanta International Airport, Los Angeles International Airport, Chicago O'Hare International Airport, Orlando International Airport, Denver International Airport, Phoenix Sky Harbor International Airport, and others.

The impact of these attacks on the aviation industry has been primarily disruptive rather than destructive. The DDoS attacks have caused interruptions to airport websites, affecting customer interactions with airlines. However, the attacks have not impacted critical airport operations or disrupted flights. The European Air Traffic Control Agency Eurocontrol, for instance, confirmed that a DDoS attack by KillNet affected its website but did not disrupt flights or pose any threat to air traffic.

Despite the limited impact of these attacks, experts warn of the potential for more severe attacks in the future. The group has shown a willingness to target critical infrastructure and has called on other groups to launch similar attacks against U.S. civilian infrastructure, including marine terminals, logistics facilities, weather monitoring centers, and healthcare systems. Therefore, while the actual damage caused by KillNet's attacks on the aviation industry has been minimal so far, the potential for more significant disruption exists.

The airlines that have been affected by KillNet's attacks are not publicly known. However, the attacks have targeted the websites of several major U.S. airports, which could indirectly affect airlines operating at those airports by disrupting customer interactions with airlines. The airports that have been targeted include Hartsfield-Jackson Atlanta International Airport (ATL), Los Angeles International Airport (LAX), Chicago O'Hare International Airport (ORD), Orlando International Airport (MCO), Denver International Airport (DIA), and Phoenix Sky Harbor International Airport (PHX). While the DDoS attack have caused interruptions to airport websites, they have not impacted critical airport operations or disrupted flights.

The damage caused by KillNet's attacks on the aviation industry, including airlines, has been primarily disruptive rather than destructive. The group's Distributed Denial of Service (DDoS) attacks have targeted the websites of several major U.S. airports, causing them to slow down or become completely inaccessible. However, these attacks have not impacted critical airport operations or disrupted flights.

The impact on airlines operating at these airports would primarily be in the form of disrupted customer interactions. For instance, passengers may have experienced difficulties accessing flight information, booking or changing flights, or checking in online while the airport websites were down. However, the actual extent of this disruption is unknown.

D. Other industries

Besides the healthcare and energy sectors, KillNet has targeted a variety of other sectors and industries. These include:

- Government Services: KillNet has attacked government websites in several countries, including at least three states in the U.S. last year
- Transportation: U.S. airport websites have been victims of KillNet's DDoS attacks
- Media and News Outlets: Media companies have also been affected by KillNet's operations
- Dark Web Markets: KillNet has engaged in attacks against dark web markets
- Financial Sector: The group has threatened the financial sector, including the SWIFT banking system and other financial institutions
- Critical Infrastructure: KillNet has targeted critical airport websites, government services, and media companies within NATO countries, including the U.S., Canada, Australia, Italy, and Poland, as well as Ukrainian supporters in practically all Eastern European, Nordic, and Baltic countries