

DDoS Attacks

An Overview of The Use of DDoS Attacks in Geopolitical Conflicts

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

April 2023

Introduction 3
Techniques and Modus Operandi 4
Services on the Darkweb 6
DDoS Attacks in Geopolitical Conflicts 8
Cooperation Between Hacktivists and Cybercriminals 9
    Anonymous Sudan 9
    KillNet 11
Financing DDoS Attacks 14
A Means of Diversion and Destabilization 16
Conclusion 17
About The Author 18
References 19

Introduction

Distributed Denial of Service (DDoS) attacks are undoubtedly one of the most popular in the threat landscape. They have been around for decades but have become much more important recently, especially against governments and public institutions. Hacktivists and cybercriminals mainly use this type of attack for different reasons but with the same result. A DDoS attack is generally defined as a malicious attempt to disrupt the regular traffic of a targeted server, service, or network by overwhelming it with a flood of Internet traffic.

DDoS attacks are usually effective when threat actors use multiple compromised computer systems as sources of attack traffic. The machines exploited are generally computers, servers, and other network resources such as CCTVs. If a DDoS attack does not impact the confidentiality or integrity of a system or that data, it affects availability by interfering with the legitimate use of that system. Techniques evolved over the past few years. Threat actors have found new methods to counter anti-DDoS systems and have developed more complex types of attacks. For example, carpet bombs, which are particularly popular among nation-state actors. In such attacks, multiple IP addresses on the target are bombarded simultaneously with less traffic per host. DDoS attack tools and botnets for rent are standard on many cybercriminal forums, particularly Russian ones.

DDoS attacks have increased dramatically in recent years, probably due to two factors. First, many cyber criminals turned to developing, selling, and using DDoS tools. Indeed, many cybercriminals use DDoS attacks as leverage to extort money from private companies or governments. There is a black market on forums or encrypted chat applications like Telegram on which many cybercriminals, especially Russian speakers, offer DDoS services and tools for sale or rental. Prices generally vary depending on the volume of the attack and the downtime. The second factor is the place DDoS attacks have taken in geopolitical events in the ongoing cyberwar between Russia and Ukraine. New groups with political, religious, or ideological motivations are using DDoS as a weapon. These groups seek to disrupt government infrastructures by trying to disable their websites and services.

Techniques and Modus Operandi

DDoS attacks constantly evolve as the nature of the technology used and the attackers' motivations change. Many threat actors launch DDoS attacks via botnets that cause tens of thousands of dollars in damage to victims. Suppose several protection systems have been developed by companies like Akamai and Cloudflare however, threat actors have adapted their techniques from simple flooding tools to massive attacks involving thousands of bots worldwide, allowing them to bypass these security systems. DDoS attacks can be divided into three main categories:

Volume-Based Attacks

The objective of the volume-based attack is to saturate the bandwidth of the attacked site. This attack category includes UDP floods, ICMP floods, and other spoofed packet floods. It is measured in (bps).

Protocol attacks

This type of attack uses the real resources of the server or those of intermediate communication equipment, such as firewalls and load balancers. It is measured in packets per second (Pps). Protocol attacks include SYN floods, fragmented packet attacks, Ping of Death, and Smurf DDoS.

Application Layer Attacks

The goal of these attacks is to crash the web server using requests that appear legitimate. This is measured in requests per second (fps). This includes weak and slow attacks, GET/POST floods, and attacks that target Apache, Windows, or OpenBSD server vulnerabilities.

A typical DDoS attack requires multiple components, including an attacker, master hosts, zombie hosts, and a targeted host. Using exploits in a remote system, a threat actor usually installs the attack program, which the primary host remotely controls (Figure 1).

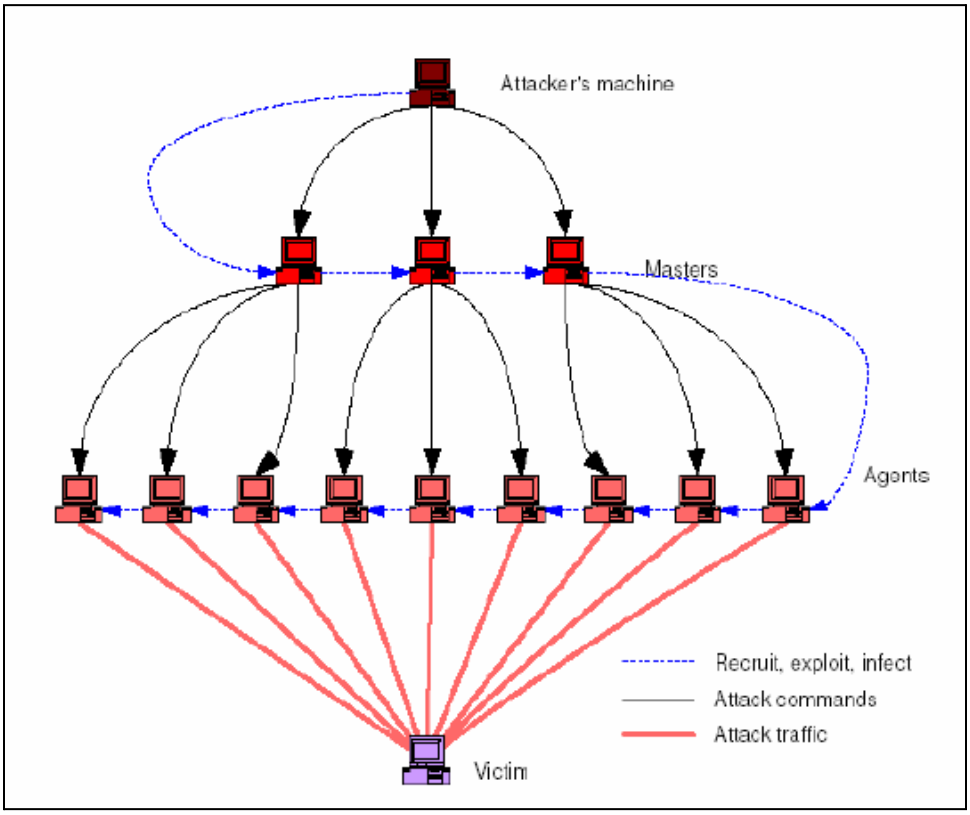


Figure 1 - DDoS Attack Structure

Before embarking on a DDoS attack, threat actors typically map their target's IT infrastructure and compile a list of server IP addresses to attack. They usually use web server scanning tools. Once the mapping has been performed, the threat actors have a global vision and can plan their attack strategy. For the past years, many botnets used to launch DDoS attacks are also composed of many IoT devices, these millions of poorly protected and, therefore, vulnerable connected objects. Indeed, many threat actors exploit known vulnerabilities in-home devices such as Wi-Fi routers, security cameras, and smart TVs. Threat actors use these sensitive devices to provide traffic flow to specific sites, disabling their servers. These attacks also pose a more severe threat to people whose devices are used in botnets. Many botnet victims don't even know their devices are being used this way, leaving them vulnerable to identity theft or physical harm. In addition, it also complicates the tracking of these attacks.

Services on the Darkweb

Many attacks use known attack vectors and DDoS services readily available for rent or sale on the Dark Web through cybercriminal forums and Telegram channels (Figures 2, 3, and 4). These illicit services usually offer a limited free demo DDoS attacks to potential customers, lowering the bar for would-be attackers to launch attacks at very little or no cost quickly. However, since these attack vectors are well known, they can be easily mitigated in most cases.

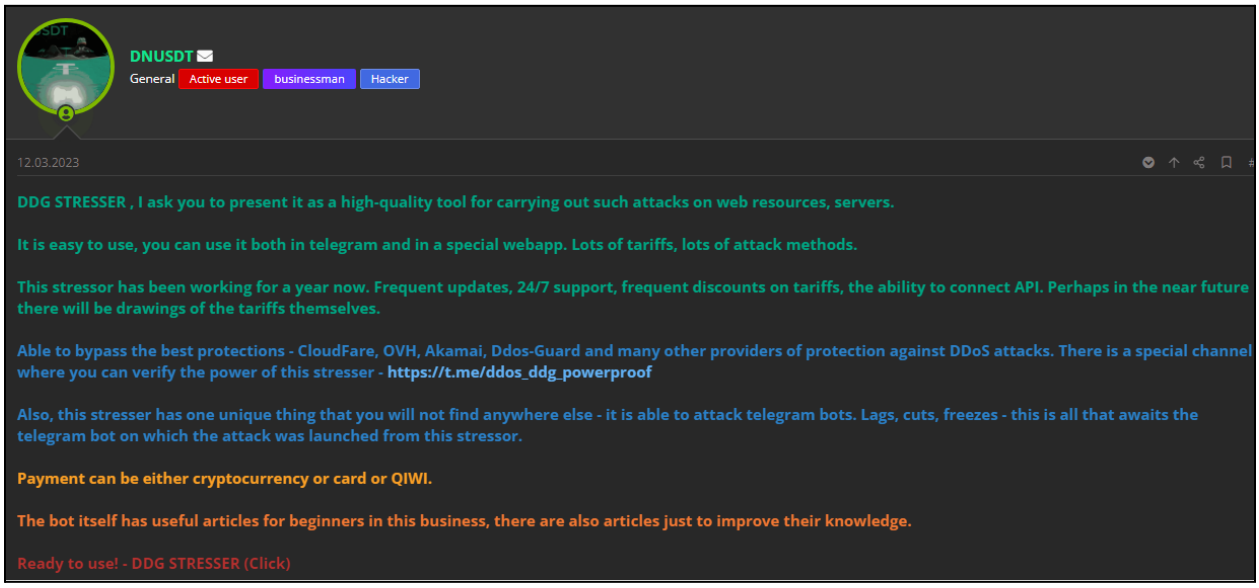


Figure 2 - DDoS stresser service for sale on a cybercrime forum

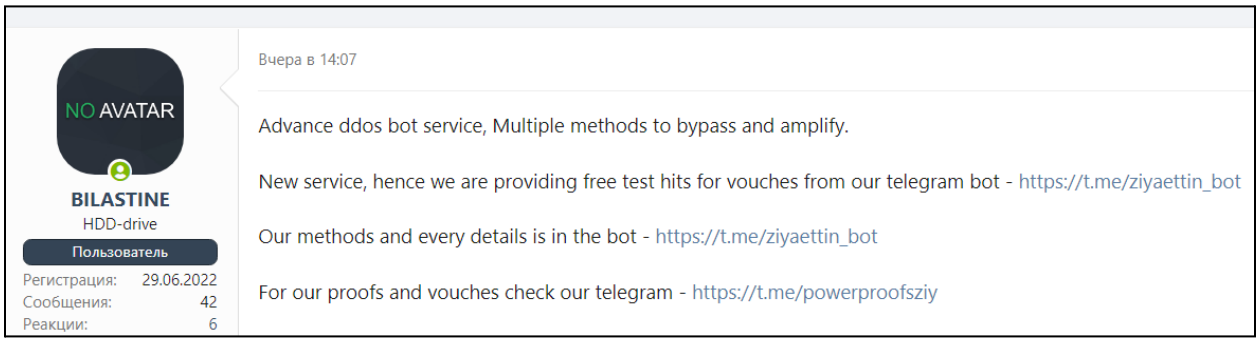


Figure 3 - DDoS bot service for sale with multiple methods to bypass security

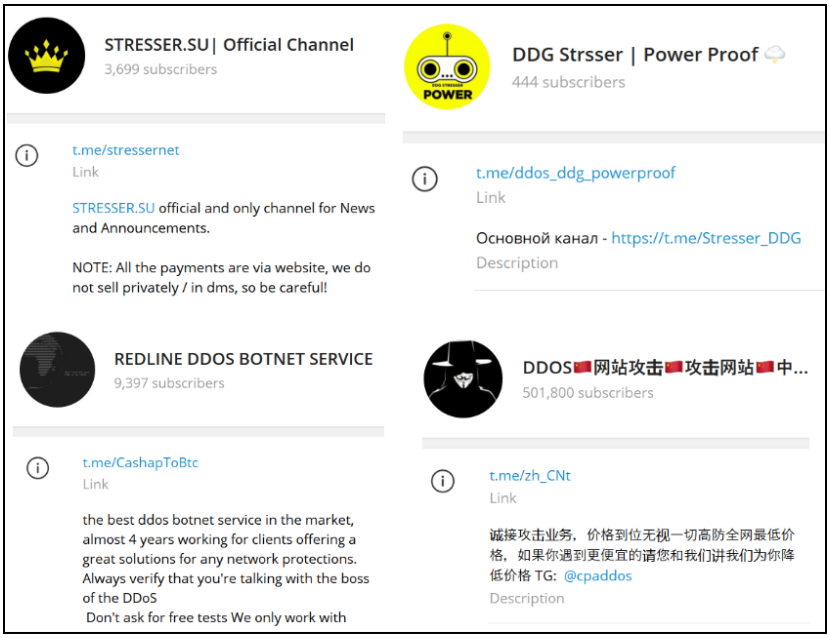


Figure 4 - Several DDoS services for sale on Telegram

DDoS attack prices vary depending on the attack volume and time. (Figure 5).

Product	Avg. Price USD (2021)	Avg. Price USD (2022)	YoY Difference
Unprotected website, 10-50k requests per second, 1 month	$1,000	$850	-$150
Unprotected website, 10-50k requests per second, 1 week	$500	$450	-$50
Europe, low-quality, slow speed, low success rate per 1, 000 requests	$320	$300	-$20
Unprotected website, 10-50k requests per second, 1 hour	$15	$10	-$5
Unprotected website, 10-50k requests per second, 24 hours	$50	$45	-$5
Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	$200	$200	$0

Figure 5 - DDoS attack index price in 2022

DDoS Attacks in Geopolitical Conflicts

DDoS attacks in geopolitical conflicts are not new. Indeed in 2007, Russia launched a series of massive DDoS attacks against Estonia's cyber infrastructures to destabilize the government. However, the intensity with which DDoS attack has developed in recent years is dazzling. According to the security company Netscout, 2022 will have been a record for DDoS attacks. This increase is partly due to the Russian-Ukrainian conflict.

If the conflict had started in March 2022, DDoS attacks against Ukraine would have escalated over time and stabilized. In addition, numerous attacks against countries declaring themselves allies of Ukraine have also been observed. The Russo-Ukrainian conflict also had an impact on the global Internet. Indeed, a number of countries that have taken a position in favor of Ukraine have been targeted by multiple DDoS attacks. According to the company Netscout in 2022, India experienced a significant increase in DDoS attacks following its abstentions during the votes of the Security Council and the General Assembly of the United Nations condemning Russian actions in Ukraine. Belize suffered its highest number of DDoS attacks the same day it made public statements supporting Ukraine. Finland has also seen a huge increase in DDoS attacks and those due to its application for NATO membership. Finally, Poland, Romania, Lithuania, and Norway have all been the target of DDoS attacks by threat actors linked to the Russian hacker group Killnet.

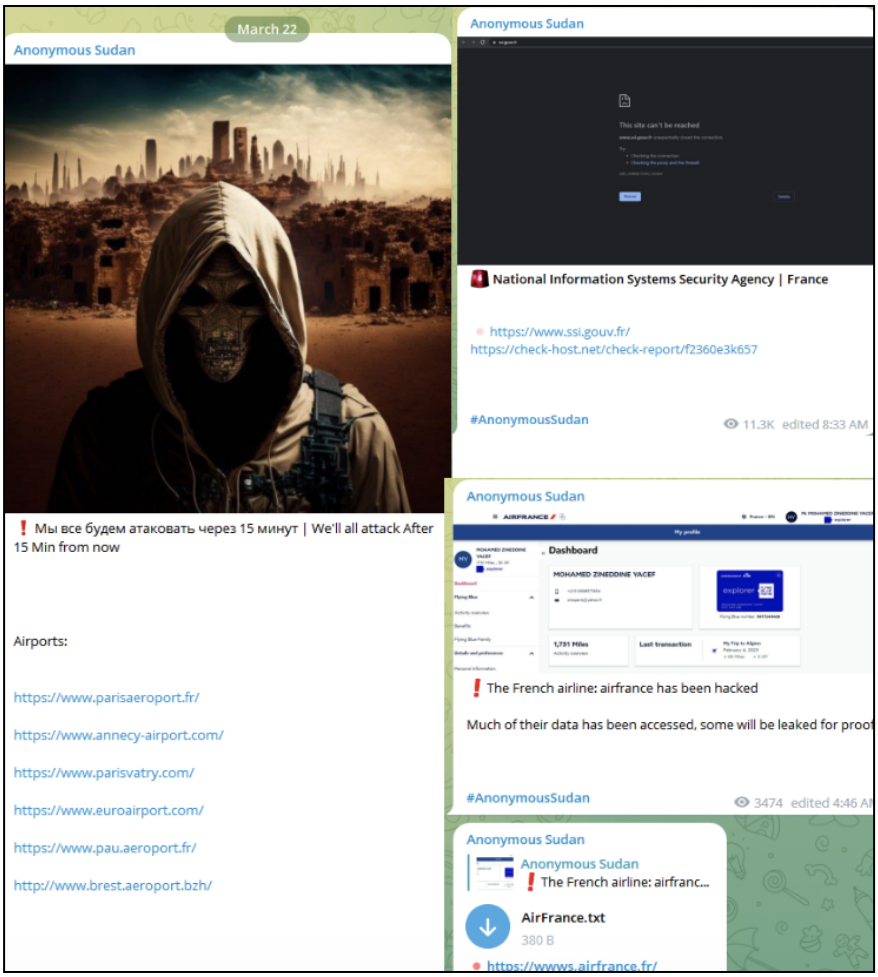
The Russo-Ukrainian conflict is not the only one to generate DDoS attacks. The political tensions between China and Taiwan also led to DDoS attack campaigns often coinciding with political events or decisions, notably Nancy Pelosi's historic visit to Taiwan. Moreover, the Israeli-Palestinian or Indo-Pakistani conflicts are strewn with multiple DDoS attacks against their Internet infrastructures. In the coming years, DDoS attacks will undoubtedly be increasingly used to strongly disrupt and destabilize governments in geopolitical conflicts. Despite a known and recurrent phenomenon in many conflicts, many countries are still poorly or insufficiently protected against mass DDoS attacks. In addition, they can also hide other more damageable and persistent attacks with the aim of data theft or destruction.

Cooperation Between Hacktivists and Cybercriminals

Recently, we observed rapprochement and collaboration between groups whose basic ideas differ but agree on specific points. The hacktivist group Anonymous Sudan has closely linked and collaborated with several pro-Russian hacking groups, including KillNet. Anonymous Sudan is a hacktivist group currently fighting against anyone they consider enemies of Islam. Meanwhile, the pro-Russian group KillNet is a nationalist group that fights for Russia and focuses on targeting any entity engaging against Russia or aiding Ukraine.

Anonymous Sudan

Anonymous Sudan is a hacktivist group that appears to have been active since at least January 2023. Anonymous Sudan was initially created to launch "cyberattacks against the enemies of Sudan, but the group later focused on target countries that desecrate Islamic symbols, primarily in the Nordic region and Central Europe. According to some cybersecurity researchers, the current operations by Anonymous Sudan are very different from those initially focused on the political situation in Sudan after the 2019 uprising. The hacktivist group is known for launching Distributed Denial of Service (DDoS) attacks, performing website defacements, and some data breaches. Moreover, the group is involved in several cyberattacks against Sudan, Denmark, Sweden, the United States, and, more recently, France. Recently, Anonymous Sudan decided to target several French government and hospital websites, claiming to have hacked the French national airline Air France (Figure 6). French justice has just opened an investigation in collaboration with the internal intelligence services on the various cyber-attacks. Anonymous Sudan is mainly active on the encrypted chat application Telegram where it runs a channel to expose its future targets and the results of its attacks. More recently, the group claimed to have targeted hospitals in India in response to what they claim India is doing to Muslims (Figure 7).



-

Figure 6 - Anonymous Sudan operation messages on Telegram



Figure 7 - Anonymous Sudan claiming on Telegram to target Indian hospitals

KillNet

KillNet is a pro-Russian hacker group active since January 2022. Before the Russian invasion of Ukraine, KillNet was known as a DDoS group for hire. However, today the group is best known for launching campaigns of DDoS attacks against various countries supporting Ukraine. The hacker group runs a Telegram channel that allows pro-Russian supporters to join in their cyberattacks against Western targets. Unlike some Russian APT groups, no concrete evidence shows links between KillNet and Russian government organizations. However, the group is considered a threat to critical state infrastructure.

KillNet is the most active Russian hacking group from the Russian-Ukrainian proxy cyberwar. The technical level of KillNet cannot be compared to that of the APT groups. Still, it is sufficient to launch harmful attacks against the websites of airports, government departments, and media companies in NATO countries. KillNet attacks do not use particularly sophisticated strategies and do not demand a ransom like other groups. In most cases, KillNet attacks have only caused service boundary outages. Recently, the group posted a message in Russian on its Telegram channel indicating that Anonymous Sudan was now a member of KillNet, formalizing their cooperation (Figure 8).



Figure 8 - Announcement of Anonymous Sudan being a member of KillNet on Telegram

More recently, KillNet claimed responsibility for launching several DDoS attacks against NATO cyber infrastructure and breaching its security to steal internal data. The Russian group reportedly successfully paralyzed 40% of NATO's electronic infrastructure. The attacks were claimed on its Telegram channel, where KillNet listed its targets and leaked NATO email addresses and plaintext passwords it claimed to have stolen from the school. NATO, apparently the NATO School Oberammergau (NSO) (Figure 9).

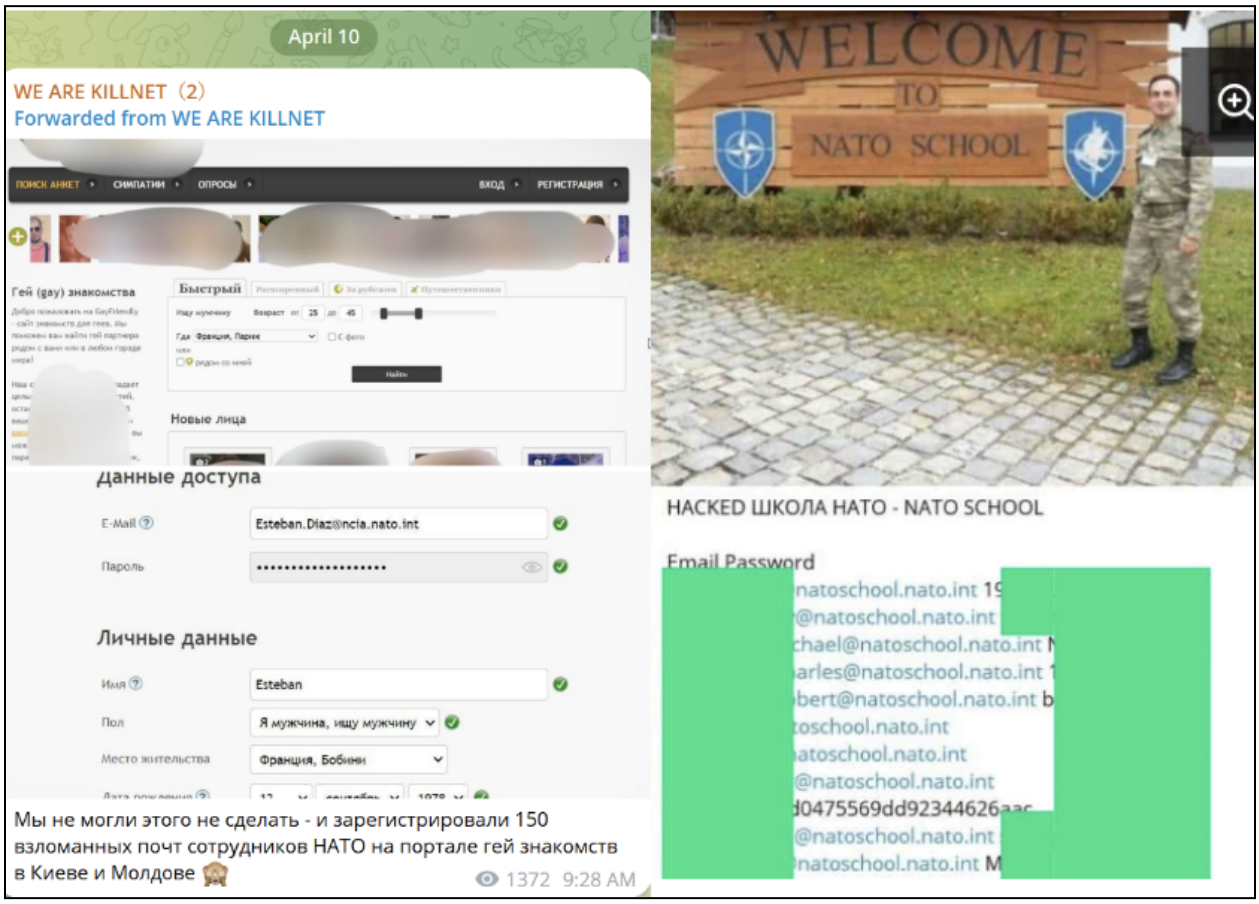


Figure 9 - On the left, KillNet logged alleged stolen NATO credentials on gay dating sites. On the right are stolen credentials (email and passwords)

If, at first glance, these two groups seem different in terms of ideology and objective, they are similar in specific points. Indeed, due to their shared goals regarding Sweden, Killnet recently announced the addition of Anonymous Sudan as an official member of its group targeting Western nations and countries opposed to Russia. For its part, Anonymous Sudan also continues to target countries that they consider hostile to Islam. As in the real world, alliances based on shared interests are common currency in cyberspace.

Financing DDoS Attacks

While many threat actors use botnets of infected machines worldwide to attack their targets, some hacker groups like KillNet launch fundraising campaigns to invest in infrastructure and increase their capabilities. The KillNet group recently posted a message on Telegram calling its supporters to donate to finance the purchase of servers to continue their DDoS operations, particularly against NATO and the United States (Figures 10, and 11). For several years, crowdfunding has become a significant source of income for hacker groups wishing to invest in infrastructure and the development of tools. The development of crypto monies has dramatically favored this type of financing because of the anonymity of donations and the difficulty of tracing transactions.

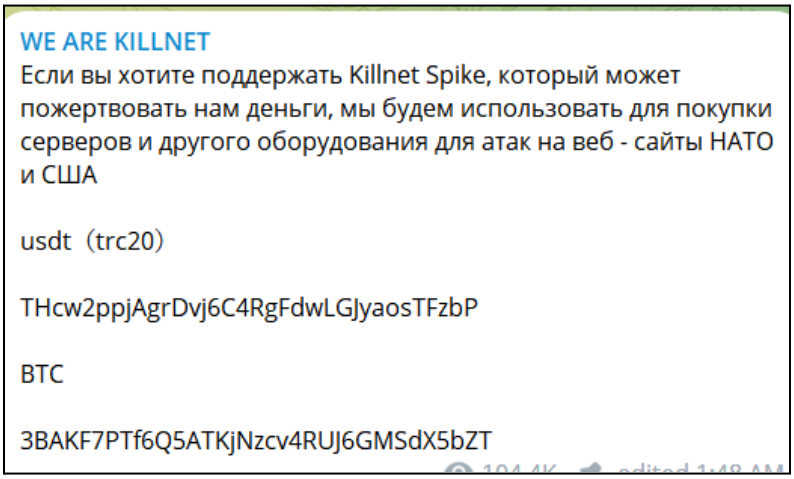


Figure 10 - KillNet message for donation on Telegram

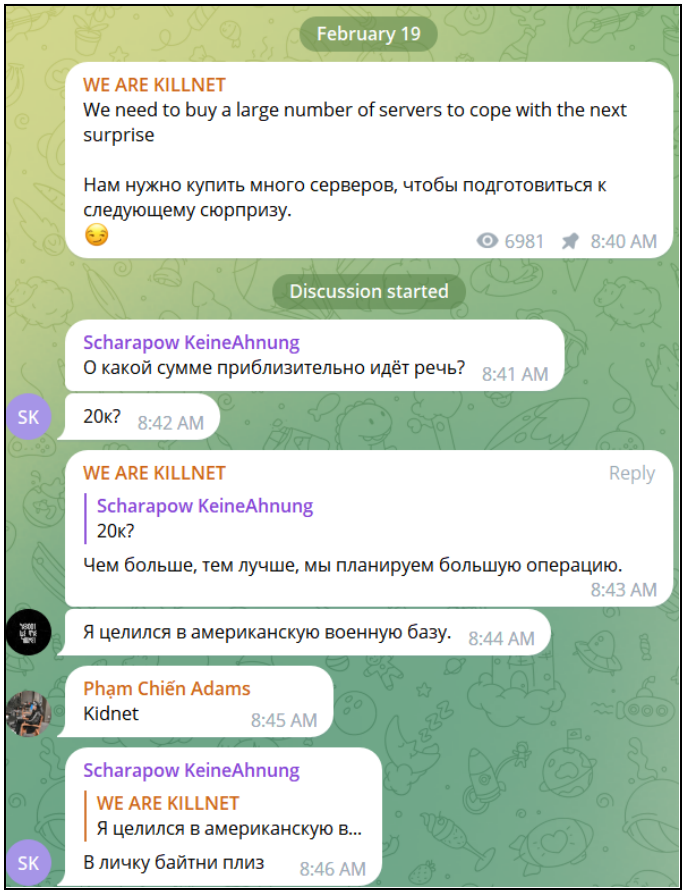


Figure 11 - Telegram messages regarding the enhancement of servers for future DDoS attacks against NATO and the US

A Means of Diversion and Destabilization

While a DDoS attack is a powerful way for cybercriminals and hacktivists to disrupt and temporarily affect state infrastructures, compared to other threats, such as ransomware attacks, they appear far less damaging. The vast majority of persistent cyberattacks against critical country infrastructure are not DDoS attacks but rather consist of network penetration through social engineering exploiting vulnerabilities and using sophisticated and encrypted malware. Nevertheless, DDoS attacks remain very disruptive for governments because the prolonged interruption of public services can have significant consequences, especially if they are recurrent. Although DDoS attacks may be considered more of a significant disruption than a real persistent threat, they can be used as a diversion during a cyberattack. A threat actor can use a DDoS attack to divert attention and insert malware or exfiltrate sensitive data in parallel. This is why authorities in charge of protecting government infrastructures must remain attentive to all types of malicious events and not only focus on defending against a DDoS attack to the point of ignoring other potential threats.

While DDoS attacks can be used as a means of diversion, they are, above all, a means for nationalist hacktivists and hacker groups to partially destabilize governments. DDoS attacks can seriously disrupt the intended targets' Internet operations, but they can also have a significant collateral impact on Internet traffic. While DDoS attacks may not seem as damaging as persistent attacks from APT groups or ransomware, they still strongly impact infrastructure. This impact depends in part on the ability of organizations to protect against DDoS attacks. Contrary to what one might think, many government IT infrastructures are still vulnerable to DDoS attacks due to poor risk assessment.

Conclusion

While DDoS attacks are not new, they have intensified considerably in recent years with the proliferation of conflicts worldwide and the development of cyber infrastructures. DDoS attacks are a powerful means of disruption and destabilization for the threat actors who launch them. However, they are not as persistant as other cyber threats but can be a great way to divert attention while launching other, more persistent attacks. If the so-called state or state-affiliated DDoS attacks were brought to light in 2007 with the attacks against Estonia, the Russo-Ukrainian conflict has undoubtedly accelerated their rise in power and demonstrated their effectiveness. DDoS attacks have a bright future and will surely be used even more in many international conflicts. Additionally, threat actors will find new and more sophisticated techniques to bypass protections to protect government IT infrastructures.

About The Author

I am a cyber intelligence expert who has worked in various environments over the past ten years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, and analysis, and the lead of Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep & Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.



References

1. The History and Evolution of DDoS Attacks, Embedded Computing, 2020. https://embeddedcomputing.com/technology/security/network-security/the-history-and-evolution-of-ddos-attacks

2. Geopolitical Unrest Drives DDoS Activity, NETSCOUT, 2022. https://www.netscout.com/blog/geopolitical-unrest-drives-ddos-activity

3. War and Geopolitical Conflict: The New Battleground for DDoS Attacks, Dark Reading, 2022. https://www.darkreading.com/attacks-breaches/war-and-geopolitical-conflict-the-new-battleground-for-ddos-attacks

4. Killnet: Russian Hacktivists DDoS US Airports, Government Websites, Anthony Eich on October 18, 2022 https://westoahu.hawaii.edu/cyber/uncategorized/killnet-russian-hacktivists-ddos-us-airports-government-websites/

5. Anonymous Sudan: Religious Hacktivists or Russian Front Group?, Trustwave, 2023. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/.