MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

DDoS Attacks and the Cyber Threatscape

Rohit Kumar Sharma

August 01, 2023

Summary

DDoS attacks are posing a formidable challenge than ever before, due to technological advancements and other facilitating factors. When combined with other form of cyberattacks, the impact of disruption multiplies, leading to severe consequences for digital infrastructure.

Introduction

In June 2023, Microsoft identified increased traffic against some services that temporarily impacted availability to the company's flagship office suite, including the Outlook email, OneDrive file-sharing apps, and cloud computing platform. On investigating the brief interruption, Microsoft identified a distributed denial-of-service (DDoS) operation orchestrated by a threat actor that the company tracks as Storm-1359.[1] Despite the sophistication involved in the operation, Microsoft assured customers that there was no evidence of unauthorised access to customer data. The company concluded that the threat actor appears to be focused on disruption and publicity. Within hours of the outage, a group named 'Anonymous Sudan' took responsibility for the attack on its encrypted Telegram channel with a message ending with, "We hope you enjoyed it, Microsoft".[2]

DDoS Attacks and Enablers

DDoS attacks are a form of cyberattack that render websites, servers, and other services inaccessible to legitimate users by overwhelming them with more traffic than they can handle.[3] The perpetrators in such attacks attempt to exhaust network, server, or application resources to make them unavailable to legitimate users. In the event of a DDoS attack, a website or service is flooded with a barrage of HTTP requests and traffic, which originates from a coordinated network of bots known as a botnet.[4] There are several types of DDoS attacks that are carried out by using different attack vectors.

DDoS attacks have existed for decades; nevertheless, their prevalence has surged exponentially in terms of volume and intensity, owing to many factors. Threat actors are no longer limited to 'computer geeks' or 'script kiddies' but constitute sophisticated and organised groups with varying motivations. Advancement in technology has also been an enabler in amplifying such cyber incidents. The ubiquity of digital devices such as the Internet of Things (IoTs) has increased the threat landscape of DDoS attacks. The widespread adoption of digitalisation has expanded the attack surface, while the persistent problem of inadequate cybersecurity measures continues to persist.

[1] **"Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks"**, Microsoft, 16 June 2023.

[2] Stefanie Schappert, **"Microsoft Outlook Down After Reported Hack"**, *Cybernews,* 8 June 2023.

[3] Omer Yoachimik and Jorge Pacheco, **"DDoS Threat Report for 2023 Q1"**, Cloudfare, 11 April 2023.

[4] **"What is a DDoS attack?"**, Microsoft.

Another facilitating factor that has contributed to the rise in the frequency of such attacks is the ready availability of DDoS attack services, which is narrowing the gap between skilled and amateur hackers. Not that this is a new phenomenon of the underground market, as illustrated in 2016 report detailing the underground hackers market. The report noted that providing DDoS remains a popular service hackers offer on the underground market.[5] The report also pointed out that most of these hackers were willing to perform a free 5 to 10 minutes DDoS test for customers and even charged higher if the target website had anti-DDoS protection installed. The black market also provides rented botnet infrastructure to execute DDoS attacks.

Motivation

The motivation behind DDoS attacks varies with threat actors; hacktivists may use it for ideological reasons, cybercriminals for financial motives, and states for larger geopolitical reasons. According to an assessment, the DDoS threat landscape in the first half of 2022 was dominated by geopolitical events, with the financial sector being the most targeted segment.[6] The ideologically driven APTs such as pro-Russian 'KillNet' and pro-Ukrainian were not only targeting the opposing nation with DDoS attacks but also countries and organisations seen to be supporting those nations. The most notable event was when the Vatican City website was knocked offline by a DDoS attack, allegedly by a group sympathetic to Russia.[7] Another major geopolitics-driven attack was against the key Taiwanese websites by China-state-backed threat actors at the time of Nancy Pelosi's visit to Taiwan.[8]

Occasionally, DDoS attacks were carried out to extort ransom payments, colloquially known as Ransom DDoS (RDDoS) attacks. The RDDoS attack should not be mistaken for ransomware, which may be driven by similar motivations but employs different tactics, techniques, and procedures (TTPs). The operational method in ransomware requires 'denial of data' by a malicious script, whereas RDDoS involves denial of service, generally by a botnet.[9] Running a ransomware operation requires access to internal systems, which is not the case in ransom DDoS attacks. In RDDoS,

[5] "**Underground Hacker Market: Annual Report**", Dell, April 2016.

[6] "**The Imperva Global DDoS Threat Landscape Report 2023**", Imperva.

[7] Claudia Glover, "**Vatican Cyberattack: DDoS Strike Could Be Work of Russian Hacktivists**", *Tech Monitor,* 2 December 2022.

[8] Kevin Collier, "**Taiwanese Websites Hit with DDoS Attacks as Pelosi Begins Visit**", *NBC News,* 2 August 2022.

[9] Omer Yoachimik and Jorge Pacheco, "**DDoS Threat Report for 2023 Q1**", no. 3.

threat actors leverage the threat of denial of service to conduct extortion, which may include sending a private message by email demanding ransom amount to prevent the organisation from being targeted by a DDoS attack.[10] According to a threat intelligence report, throughout the 2020–2021 global RDDoS campaigns, attacks ranged from few hours up to several weeks with attack rates of 200 Gbps and higher.[11]

The DDoS attack can also serve as a means of reconnaissance, allowing attackers to assess the target's vulnerabilities and gauge the strength of its defenses. Lately, these attacks have been incorporated into triple extortion ransomware strategies, where data is not only encrypted and exfiltrated, but in case the ransom fails, the attackers may initiate a DDoS attack on the targeted services to intensify their operation.[12]

The Case of Anonymous Sudan

Anonymous Sudan best exemplifies the re-emergence of DDoS as a form of weaponisation of cyberspace to achieve varying objectives. According to reports, Anonymous Sudan emerged on 18 January 2023 and swiftly initiated its operations aimed at Sweden within a week.[13] The group initiated cyber attacks against the Swedish government and companies in response to what it considered anti-Islamic actions in Sweden. Driven by 'religious' motivations, the group subsequently decided to focus its efforts on targeting Denmark and France.

Upon creating its Telegram channel, the Anonymous Sudan account initially engaged in minimal activity, primarily expressing its objective to target "enemies of Sudan".[14] The account also shared posts amplifying the activities of Russian hacktivists groups such as KillNet and Anonymous Russia.

Reportedly, on several occasions, the group has undertaken operations in tandem with other threat actors. For instance, in May 2023, Anonymous Sudan and an Iranian hacking collective known as Asa Musa (Persian for Moses Staff) made a failed bid to sabotage Israeli rocket alert applications during an episode of violence between Israel and Palestinian Islamic Jihad.[15] In another incident, Anonymous Sudan,

---

[10] **"The Definitive Guide to Ransom Denial of Service"**, Check Point.

[11] Ibid.

[12] Daniel Smith, **"Welcome to the New World of Triple Extortion Ransomware"**, *Security Magazine*, 18 May 2021.

[13] **"Anonymous Sudan: In-Depth Analysis Beyond Hacktivist Attacks"**, ThreatMon, 2 May 2023.

[14] Mattias Wahlen, **"Anonymous Sudan: Threat Intelligence Report"**, TRUESEC, 23 February 2023.

[15] Avi Davidi, **"Slapdash Attempt to Hack Rocket Sirens May Be Cause for Serious Alarm about Iran"**, *The Times of Israel,* 14 May 2023.

alongside KillNet (a pro-Russia hacker group) and REvil (notorious for ransomware attacks), unveiled their plans for attacks on the US and European Banking systems on their Telegram channels.[16] A few days later, the European Investment Bank confirmed a DDoS attack affecting its operations without attributing the incident to any threat actor. However, the group claimed responsibility for the cyber incident on its Telegram channel. To date, the group has targeted many countries, including Australia, Germany, Israel, India, and the US. These countries have experienced attacks across various sectors such as government institutions, educational establishments, financial institutions, airports, and healthcare facilities.

Motivation and Modus Operandi

Anonymous Sudan has gained notoriety for engaging in DDoS attacks and defacing websites during its nearly six months of existence. The group asserts that it operates from Sudan and is involved in cyber activism, commonly referred to as hacktivism. The group's claims and announcements provide significant insight into the 'social' and 'political' motivations driving their operations. Nevertheless, some assessments indicate a potential association between Anonymous Sudan and the pro-Russian hacktivist collective known as KillNet.[17] Others suggest that the group is likely a state-sponsored Russian actor pretending to be motivated by Islamist ideologies.

Based on its operational pattern and choice of target, the group initially appeared as a threat actor driven by religious motives. The group also asserted its affiliation with the larger Anonymous collective, which gained prominence in the early 2000s by instrumentalising digital activism to advocate for societal and political transformation. However, a detailed report on the group refuted this claim and indicated a potential connection between the group and the Russian hacker collective ecosystem. Other cyber threat intelligence firms have also reaffirmed the presence of a Russian connection in their assessments. Another sign of its close association with Russian threat actors, if not directly with the state, is the use of Russian language in its official Telegram channel alongside Arabic and Persian.

During a recent interview conducted via Telegram, a 'representative' of Anonymous Sudan shared some intriguing insights with the interviewers. Due to the group's tendency to seek publicity and make sensational claims, however, caution must be

[16] "**KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems**", Trustwave, 15 June 2023.

[17] "**Unmasking Anonymous Sudan: Timeline of DDoS Attacks, Affiliations, and Motivations**", Flashpoint, 20 June 2023.

exercised before fully believing their assertions. On being inquired about TTPs, it was revealed that the group tailor the plan of action depending on the target, which may vary from Layer 4 attack to Layer 7 attack based on requirements.[18] Refuting the allegations of being part of Russian cyber military campaign, Anonymous Sudan asserted that the accusations were unfounded. Interestingly, the interview was abruptly ended when questioned about the group's self-proclaimed role as the defender of Islam while also demonstrating inaction against China's persecution of one million Uyghurs .

Lately, the group seems to have shifted from presenting themselves as politically-motivated hacktivists to using extortion tactics for financial gains.[19] According to reports, the group demanded US$ 3 million from Scandinavian Airlines (SAS) to halt DDoS attacks against the airline's website. The underlining reason behind the shift is uncertain, but the group appears to be well-funded. Rather than employing networks of infected or compromised computers to launch attacks cheaply, the group opted for a different approach. For targeting infrastructure in Denmark, the group rented 61 servers located in Germany from IBM Corporation's SoftLayer division to carry out their operations.[20] By doing so, they effectively concealed their activities behind multiple layers of anonymity. Even in the recent Microsoft outage, it was observed that the attacks likely relied on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure.[21] Also, it is highly improbable for a grassroots hacktivist collective to utilise paid proxy services for carrying out their attacks, revealing subtle indications of the state's involvement in guiding their operations.[22]

Attacks in India

After drawing attention to its 'religiously' motivated attacks in the Western world, the group shifted its focus towards targeting Indian infrastructure. The attacks specifically targeted airports, hospitals, and other critical infrastructure.According

---

[18] **"Exclusive Interview: Anonymous Sudan, Cyber Warriors or Russian Puppets?"**, Intel Cocktail, 25 July 2023.

[19] Daryna Antoniuk, **"Hacker Group Anonymous Sudan demands $3 million from Scandinavian Airlines"**, *The Record*, 31 May 2023.

[20] Jordan Robertson and Niclas Rolander, **"Posing as Islamists, Russian Hackers Take Aim at Sweden"**, *Bloomberg,* 14 May 2023.

[21] **"Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks"**, Microsoft, 16 June 2023.

[22] Simon Hendery, **"Hacktivist Group Anonymous Sudan a 'bear in wolf's clothing"**, *SC Magazine,* 19 June 2023.

to a report, India ranked second in terms of being the most targeted country by religious hacktivist groups, after Israel.[23] In April 2023, a well-coordinated DDoS attack was launched against major airports and healthcare institutions in India.[24] Anonymous Sudan, which claimed responsibility for the incident, used a combination of Layer 3–4 and Layer-7 DDoS attacks that lasted nearly nine hours.[25]

According to the Indian Computer Emergency Response Team's (CERT-In) Annual Report of 2021, the agency handled 1,402,809 incidents, including website defacements and DDoS attacks.[26] Also, the Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) under CERT-In is instrumental in tracking botnet/malware infections and notifying end users in collaboration with internet service providers and organisations. The Cyber Swachhta Kendra initiative is crucial as botnets, through sheer volume, have been responsible for some of the most large-scale DDoS attacks.

While the consequences of DDoS attacks may appear insignificant, they should not be underestimated. These attacks can potentially incur significant costs to an organisation regarding time, finances, and reputation. Furthermore, they can lead to the loss or deterioration of essential services, including critical sectors such as healthcare. A threat actor might also employ a DDoS attack as a means to redirect focus from more sinister activities, such as the insertion of malware or the unauthorised extraction of data.

As the government continues to spread awareness about such threats, organisations, especially those managing critical infrastructure, must take initiatives to prevent and mitigate DDoS attacks. Such organisations must develop a DDoS response plan and promote a culture of cyber hygiene among their workforce. In short, DDoS is no longer a low intensity/low impact threat but a danger with actual loss and cost.

---

[23] Paulina Okunyte, **"Hacktivists Target Israel the Most, Analysis Shows"**, *Cybernews*, 26 April 2023.

[24] **"DDoS Attacks Strike Indian Airports. Here's How the Threat was Mitigated"**, *The Economic Times,* 13 April 2023.

[25] **"Six Major Indian Airports and Healthcare Institutions Under DDoS Attack"**, *CIONews,* 14 April 2023.

[26] **"CERT-In Annual Report (2021)"**, Ministry of Electronics and Information Technology, Government of India.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses