MAZEBOLT

Summer of DDoS

June - August 2023 | DDoS Attacks

Summer of DDoS

June - August 2023 DDoS Attacks

In recent years, DDoS attacks have become the leading cyber threat to organizations and governments on a global scale. As networks become more complex, DDoS attacks continue to evolve and grow in frequency and sophistication. The dynamic nature of cloud environments, along with their associated workflows, has provided threat actors with opportunities to bypass DDoS protection measures, whether they are on-premises or cloud-based, thereby causing significant disruptions to an organization's operational continuity.

On average, 60% of businesses lose over $120,000 in downtime. Shockingly, 15% of affected organizations report losses exceeding $1 million USD, with some even suffering market capitalization losses of up to $3 billion. The Russia-Ukraine conflict has illustrated that attackers no longer require expensive and advanced weapon systems to wreak havoc. In addition, the DDoS vulnerability gap is huge; automated sequences and multi-vectored attacks have become more frequent and sophisticated as they're easy to implement.

But on the other hand, vulnerabilities in the DDoS protections deployed, which are caused by misconfigurations, remain the only reason DDoS attacks succeed - no matter how simple the attack is. The list of victims who have experienced detrimental downtime due to relatively simple DDoS attacks continues to grow.

Despite the tumultuous events that unfolded globally during the summer of 2023, ranging from natural disasters to political and social unrest, the reality defies expectations. Rather than relenting, some of the most destructive DDoS attacks of the year occurred during this period. Microsoft's online services fell victim to rudimentary DDoS attacks, while numerous countries, including Switzerland, Poland, the Czech Republic, Spain, the Netherlands, and France, experienced severe disruptions to their governmental services and banking systems.

Kenya, for instance, grappled with a five-day shutdown caused by Anonymous Sudan's relatively simple DDoS attacks. Even gaming companies experienced severe downtime while launching new products and updates, and critical infrastructure like oil conglomerates and nuclear facilities in countries from Japan to the UAE also bore the brunt of DDoS threat actors.

The summer of 2023 left no one immune to the DDoS threat, stemming primarily from two prominent threat actors: Anonymous Sudan and NoName057(16). Both groups are presumably state-sponsored by Russia, which continues to be a red flag for organizations, as financial institutions and governmental services that are brought down by state-sponsored DDoS attacks will not be able to sue for compensation, following the damages. In March of 2023, Lloyd's, the leading London-based insurance company, decided to exclude liability for losses arising from any state-sponsored cyberattack. As you will see in the following report, state-sponsored DDoS attacks can cause millions in damages that cannot be recouped - and this is before taking into account the reputational damage and losses.

June

Date of attack	Country	Vertical	Downtime	Companies affected	Estimated Damage	Press headlines	Threat Actor + Affiliation
June 1	India	Cybersecurity	72 hours ongoing downtime	CloudSEK	35K USD	Link	Unknown
June 4	India	Education	24 hours ongoing downtime	The Institute For Teacher Education, The Bengal College of Teacher Education, P.G. INSTITUTE OF MEDICAL SCIENCES, Gopsai Avinandan Sangha Primary Teachers' Training Institute, Institute of Science & Technology, COLLEGE FOR TEACHER EDUCATION, Anindita College for Teacher Education	NA	Link	Unknown Indonesian Hacking Group
June 5	USA	Communications	24 hours attack - 10 hours downtime	Microsoft Outlook, SharePoint Online, OneDrive for Business	4.2mil USD	Link	Anonymous Sudan
June 6	Netherlands	Ports	12 hours attack - 6 hours downtime	The websites of the port authorities in Rotterdam, Amsterdam, and Den Helder + Groningen Seaport website	NA	Link	NoName057(16) - State Sponsored by Russia
June 8	USA	Communications	8 hours attack - 4 hours downtime	Microsoft OneDrive	1.7mil USD	Link	Anonymous Sudan
June 8	India	Education	24 hours ongoing downtime	Bharatpedia - India's local Wikipedia	NA	Link	Unknown
June 8	Russia	Banks	72 hours attack - 24 hours downtime	Several Leading Banks & Credit Unions	NA	Link	"Cyber Anarchy Squad" - Pro-Ukrainian Hacktivists
June 9	USA	Communications	4 hours attack - 2 hours downtime	Microsoft Azure	7mil USD	Link	Anonymous Sudan
June 12	Switzerland	Gov, Military, Aviation	72 hours ongoing downtime	Swiss Parliament's website (parlament.ch), Swiss Federal Railways, Armed Forces of Switzerland, Bern regional airport, Geneva International Airport, St. Grenchen, Gallen-Altenrhein, and Samedan airports, airline companies Zimex Aviation and Heliswiss, Geneva tourism website	NA	Link	NoName057(16) - State Sponsored by Russia
June 13	Poland	Gov	72 hours ongoing downtime	Electronic Platform of Public Administration Services – ePUAP	NA	Link	Suspected - Anonymous
June 14	USA	Shipping	4 hours attack - 1.5 hours downtime	UPS	4mil USD	Link	Anonymous Sudan
June 19	Luxembourg	Bank	12 hours attack - 3 hours downtime	EIB - European Investment Bank	260K USD	Link	Anonymous Sudan & Killnet
June 20	New Zealand	Ports	8 hours attack - 6 hours downtime	North Sea Port website, the company that operates the ports of Vlissingen and Terneuzen in Zeeland, and the Gent port in Belgium	NA	Link	NoName057(16) - State Sponsored by Russia
June 23	Czech Republic	Gov	5 hours attack - 1 hour downtime	website of the Ministry of Foreign Affairs of the Czech Republic	NA	Link	NoName057(16) - State Sponsored by Russia
June 25	USA	Gaming	24 hours attack - 12 hours downtime	Blizzard's Battle.net - Diablo 4, world of Warcraft, and other titles	8mil USD	Link	Unknown
June 26	USA	Gaming	36 hours attack - 3 hours downtime	BattleBit	NA	Link	Unknown

July

Date of attack	Country	Vertical	Downtime	Companies affected	Estimated Damage	Press headlines	Threat Actor + Affiliation
July 3	Russia	Infrastructure	48 hours attack - 6 hours downtime	RZD, The Russian state-owned railway company	NA	Link	The Ukrainian hacktivist group IT Army
July 3	India	Infrastructure	12 hours ongoing downtime	Bangladesh Railway online ticket portal	NA	Link	Unknown
July 8	USA	Gaming	36 hours ongoing downtime	Sandbox Interactive	60K USD	Link	Unknown
July 8	Hungary	Infrastructure	10 hours attack - 6 hours downtime	Budapest Pride's official webpage	NA	Link	Unknown
July 8	USA	Social Media	1 hour attack and downtime	Tumblr	NA	Link	Anonymous Sudan
July 10	USA	Gaming	36 hours ongoing downtime	Sandbox Interactive	60K USD	Link	Unknown
July 11	USA	Media	48 hours ongoing downtime	Archive of Our Own (Ao3)	NA	Link	Anonymous Sudan
July 11	Lithuania	Government	24 hours ongoing downtime	Several websites in Lithuania, including the exhibition center LITEXPO	NA	Link	NoName057(16) - State Sponsored by Russia
July 12	Norway	Government	Unknown	12 Norway Government Ministries	NA	Link	Pro-Russian group
July 16	USA	Finance	30 seconds attack and downtime	PayPal	NA	Link	Anonymous Sudan
July 18	New Zealand	Government	2 hours ongoing downtime	New Zealand Parliament website	NA	Link	NoName057(16) - State Sponsored by Russia
July 23	Spain	Government	4 hours attack - 3 hours downtime	Ministry of the Interior + La Moncloa, INE, Renfe, the Casa Real Central Electoral Board	NA	Link	NoName057(16) - State Sponsored by Russia
July 26	USA	Gaming	8 hours ongoing downtime	Neopets	NA	Link	Unknown
July 27	Kenya	Government	1 week attack - ongoing for several days	Media websites including The Standard Group, and Kenya News Agency, 10 university websites, including the University of Nairobi, seven hospitals and Kenya's transport agency's website, KPLC token systems, M-Pesa to bank services, and government services offered on the e-citizen	NA	Link	Anonymous Sudan
July 29	Spain	Telecom	6 hours attack - 5 hours downtime	Telefónica and Orange	4.6mil USD	Link	NoName057(16) - State Sponsored by Russia
July 30	Israel	Infrastructure	24 hours attack - 4 hours downtime	BAZAN Group - oil refinery operator	NA	Link	Anonymous Sudan

August

Date of attack	Country	Vertical	Downtime	Companies affected	Estimated Damage	Press headlines	Threat Actor + Affiliation
August 8	France	Government, Finance	12 hours attack - 6 hours downtime	The national customs service, French financial regulator's website	NA	Link	NoName057(16) - State Sponsored by Russia
August 8	Netherlands	Government, Finance	12 hours attack - 6 hours downtime	Dutch public transport website, local bank SNS, the Groningen seaport, and the website of the municipality of Vlardingen	SNS Bank: est. 700K USD	Link	NoName057(16) - State Sponsored by Russia
August 12	UAE	Infrastructure	36 hours	International oil coorporation - the website of Levare International Ltd. (Levare)	NA	Link	Medusa ransomware group
August 12	Japan	Infrastructure	24 hours ongoing downtime	Several leading nuclear websites in Japan: the Japan Atomic Energy Agency, Japan Atom ic Power Corporation, and the Atomic Energy Society of Japan	NA	Link	Anonymous
August 22	South Africa	Media	1 hour	The Daily Maverick	NA	Link	Unknown attacker from India
August 28	Poland	Financial	36 hours ongoing downtime	The Warsaw Stock Exchange, the Polish government's website for public services, Bank Pekao, Raiffeisen Bank, Plus Bank, and Credit Agricole Bank	30mil USD	Link	NoName057(16) - State Sponsored by Russia
August 29	USA	Social Media	6 hours attack - 2 hours downtime	X (formerly Twitter) was offline in more than a dozen countries in an attempt to pressurise Elon Musk into launching his Starlink service in their country.	NA	Link	Anonymous Sudan
August 30	Czech Republic	Financial	48 hours ongoing downtime	Leading Banks: Česká spořitelna, ČSOB, Air Bank, Fio Banka and Komerční banka - Services restored on August 31st	8mil USD	Link	NoName057(16) - State Sponsored by Russia
August 30	France	Government, Infrastructure	12 hours attack - 9 hours downtime	La Poste - the postal service company in France	NA	Link	#OpFrance - Anonymous Sudan
August 30	Hungary	Media	13 hours attack - 8 hours downtime	Mex Rádió Network Kft. - Internet Radio	NA	Link	Probably HANO, A local threat actor
August 31	USA	Media	2 hours	Archive of Our Own (Ao3)	NA	Link	Anonymous Sudan

Summary:

What can you do to avoid damaging DDoS attacks?

DDoS protection misconfigurations lead to DDoS vulnerabilities, which lead to damaging DDoS attacks. DDoS protection will only automatically block attacks specifically configured per production environments deployed; all other attacks will cause damaging SLA's time-to-mitigation and emergency response time. Only through identifying vulnerabilities and prioritized remediation can organizations avoid damaging DDoS attacks, and ensure that all protection systems are up-to-date on all DDoS vulnerabilities, with full visibility into their automated DDoS protection.

MazeBolt RADAR™ is the only DDoS security solution that eliminates DDoS vulnerabilities, on every layer of DDoS security, and empowers stakeholders to adopt this transformative approach of automated DDoS security: Preventative, Proactive, automated Protection.

About MazeBolt

MazeBolt is pioneering a new standard in DDoS security. RADAR™ empowers organizations to leave behind unexpected damaging downtime and SLAs, transforming DDoS protection to be fully automated and reliable.

RADAR is an industry-first patented solution that identifies how attackers succeed in bypassing existing protection systems through vulnerabilities, through continuous non-disruptive DDoS attack simulations.

RADAR's autonomous risk detection enables cybersecurity teams to go light-years beyond traditional DDoS testing and identify and remediate vulnerabilities in every layer of DDoS protection.

Global enterprises, including financial services, insurance, gaming, and high-security government environments rely on MazeBolt to prevent damaging DDoS attacks.

MAZEBOLT

For more information visit www.mazebolt.com