EDISON
BRILLIANT KNOWLEDGE

DESTRUCTIVE BY DESIGN

EDISON EXPLAINS

DDoS attacks are surging worldwide, with incidents doubling since 2022, leaving businesses facing downtime, disruption and escalating threats to service availability.

BY NEIL SHAH

A distributed denial of service (DDoS) attack is a cyberattack designed to make a website, online service or network unavailable by flooding it with malicious traffic from multiple sources. Unlike a denial of service (DoS) attack from a single source, DDoS attacks use numerous devices (often harnessing tens to hundreds of thousands of attacking systems) to overwhelm targets with traffic volumes that the connecting infrastructure and systems cannot handle. When successful, these attacks prevent genuine users from accessing internet-based services, causing business disruption and potential financial losses.

How attacks play out

Attackers typically use exploitable systems – legitimate internet services that can be tricked into participating, or botnets (networks of infected computers, IoT devices and servers) to generate attack traffic. In the case of botnets, these 'zombie' devices are compromised without their owners' knowledge through malware infections. The attacker controls these devices remotely, instructing them to simultaneously send requests to a target or victim. The ensuing volume of traffic overwhelms the target's resources, or connection to the target, causing service degradation or complete failure.

Types of DDoS attacks

DDoS attacks can be categorised based on which open system interconnection (OSI) network layer they target.

Layer 3/4 (network/transport) attacks target network infrastructure by exhausting bandwidth or connection capabilities. For example:

- SYN floods exploit the transmission control protocol (TCP) handshake process. When computers connect, they use a 'handshake' where one sends a synchronize (SYN) request, the other acknowledges with synchronize-acknowledge (SYN-ACK) and the first completes with ACK. Attackers send many SYN requests without completing the handshake, leaving the server with partially open connections that exhaust its resources.

- UDP floods send large numbers of user datagram protocol (UDP) packets to random ports. Unlike TCP, UDP doesn't require handshakes, making it easier to spoof. This forces the target to process each packet, overwhelming its capacity.

- ICMP floods overwhelm targets with echo request (ping) packets. Internet control message protocol (ICMP) is normally used for

network diagnostics like the 'ping' tool, but attackers can exploit this legitimate service using it to send massive volumes of these requests or responses.

Layer 7 (application) attacks target web applications and are typically more sophisticated.

- HTTP/HTTPS floods send seemingly legitimate hypertext transfer protocol (HTTP) requests (the standard protocol for web browsing), which consume server resources. By targeting resource-intensive functions like searches or login processes, attackers can overwhelm servers with requests that appear genuine.

- Low and slow attacks (eg Slowloris) keep many connections open by sending partial HTTP requests at a deliberately slow rate. Named after the slow-moving sloth, these attacks keep connections open indefinitely with minimal bandwidth cost to the attacker, gradually occupying all available server connections.

- DNS query floods overwhelm domain name system (DNS) servers with numerous or hard-to-process requests. DNS translates human-readable domain names (like example.com) into IP addresses that computers use to locate services. By flooding these servers with malicious queries, attackers can disable this critical piece of internet infrastructure for targeted victims.

A growing threat

The scale and frequency of DDoS attacks have increased dramatically in recent years. According to industry data, attacks doubled between 2022 and 2024, with some estimates suggesting global attacks exceeded 100m in 2024 alone. This

growth is driven by:
— the proliferation of poorly secured IoT devices, making botnet creation easier;
— increasing geopolitical tensions, with state-sponsored attacks becoming common;
— the rise of 'DDoS-for-hire' services that commoditise attack capabilities; and
— more sophisticated attack techniques that can evade traditional defences.

Who is targeted?

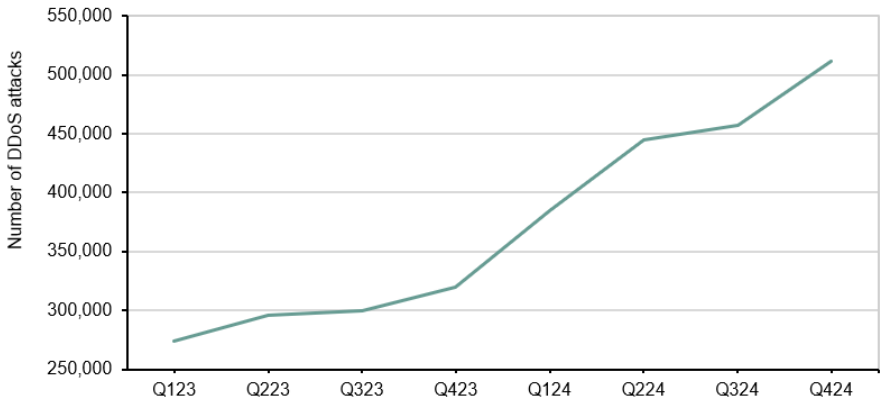
While any online service can be targeted, certain sectors face higher risks:
— IT and telecommunications (28% of attacks).
— Banking and finance (24%).
— Government and defence (15%).
— Energy and utilities (12%).
— Healthcare (7%).
Attacks are often motivated by financial extortion, political activism, competitive disruption or simply as diversionary tactics for more sophisticated breaches. Recent changes to the geopolitical landscape have resulted in a marked increase in state-sponsored attacks, which typically target critical IT infrastructure to maximise broader social and economic impact.

Mitigation approaches

Cloud DDoS protection typically uses so-called scrubbing services:
1. Traffic destined for the target or victim is detected as suspicious when it exceeds normal patterns.
2. It is redirected to dedicated scrubbing centres – specialised data centres designed to filter attack traffic.
3. Malicious traffic is identified and filtered out based on known attack signatures.
4. Clean, legitimate traffic is then forwarded to the original destination.

While effective, this approach has limitations:
— It can introduce latency (delays) for legitimate users during the redirection process.
— Detection and redirection takes time to implement, allowing initial service disruption before cloud protection is activated.
— It often requires manual intervention or coordination by security teams.
— Short, repeated or agile attacks can be difficult to mitigate effectively as they may end before mitigation begins.

Number of DDoS attacks worldwide from Q123-Q424



Source: Statista

Advanced strategies

Modern DDoS protection uses more sophisticated techniques:

■ Deep packet inspection (DPI): analyses the actual contents of data packets rather than just traffic patterns, enabling more accurate detection of malicious traffic. This allows security systems to examine the data being transmitted rather than just the volume or source.

■ Real-time monitoring: provides continuous traffic analysis without waiting for attack thresholds to be reached, allowing for earlier detection and response.

■ Hardware-agnostic solutions: software-based protection that can be implemented without changing existing network infrastructure, reducing implementation costs and complexity.

■ AI/ML detection: uses artificial intelligence and machine learning algorithms to help identify anomalous traffic patterns and predict likely attack vectors.

The most effective defences combine multiple approaches in a layered security strategy, with solutions that can adapt to evolving attack methods.

DDoS as a cybersecurity imperative

As organisations increasingly rely on online services, DDoS protection has become a critical component of cybersecurity strategy. The impact of successful attacks extends beyond immediate service disruption to include: loss of customer trust; financial losses from business interruption; regulatory complications; and damage to brand reputation.

With attack volumes increasing rapidly in recent years, for example up by more than 50% in 2024, organisations must ensure their DDoS mitigation capabilities evolve to match the growing threat landscape.

Neil Shah is executive director, content and strategy, Edison Group

General disclaimer and copyright

This report has been and prepared and issued by Edison. Edison Investment Research standard fees are £60,000 pa for the production and broad dissemination of a detailed note (Outlook) following by regular (typically quarterly) update notes. Fees are paid upfront in cash without recourse. Edison may seek additional fees for the provision of roadshows and related IR services for the client but does not get remunerated for any investment banking services. We never take payment in stock, options or warrants for any of our services.

Accuracy of content: All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report and have not sought for this information to be independently verified. Opinions contained in this report represent those of the research department of Edison at the time of publication. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

Exclusion of Liability: To the fullest extent allowed by law, Edison shall not be liable for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses incurred or suffered by you arising out or in connection with the access to, use of or reliance on any information contained on this note.

No personalised advice: The information that we provide should not be construed in any manner whatsoever as, personalised advice. Also, the information provided by us should not be construed by any subscriber or prospective subscriber as Edison's solicitation to effect, or attempt to effect, any transaction in a security. The securities described in the report may not be eligible for sale in all jurisdictions or to certain categories of investors.

Investment in securities mentioned: Edison has a restrictive policy relating to personal dealing and conflicts of interest. Edison Group does not conduct any investment business and, accordingly, does not itself hold any positions in the securities mentioned in this report. However, the respective directors, officers, employees and contractors of Edison may have a position in any or related securities mentioned in this report, subject to Edison's policies on personal dealing and conflicts of interest.

Australia

Edison Investment Research Pty Ltd (Edison AU) is the Australian subsidiary of Edison. Edison AU is a Corporate Authorised Representative (1252501) of Crown Wealth Group Pty Ltd who holds an Australian Financial Services Licence (Number: 494274). This research is issued in Australia by Edison AU and any access to it, is intended only for "wholesale clients" within the meaning of the Corporations Act 2001 of Australia. Any advice given by Edison AU is general advice only and does not take into account your personal circumstances, needs or objectives. You should, before acting on this advice, consider the appropriateness of the advice, having regard to your objectives, financial situation and needs. If our advice relates to the acquisition, or possible acquisition, of a particular financial product you should read any relevant Product Disclosure Statement or like instrument.

New Zealand

The research in this document is intended for New Zealand resident professional financial advisers or brokers (for use in their roles as financial advisers or brokers) and habitual investors who are "wholesale clients" for the purpose of the Financial Advisers Act 2008 (FAA) (as described in sections 5(c) (1)(a), (b) and (c) of the FAA). This is not a solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned or in the topic of this document. For the purpose of the FAA, the content of this report is of a general nature, is intended as a source of general information only and is not intended to constitute a recommendation or opinion in relation to acquiring or disposing (including refraining from acquiring or disposing) of securities. The distribution of this document is not a "personalised service" and, to the extent that it contains any financial advice, is intended only as a "class service" provided by Edison within the meaning of the FAA (i.e. without taking into account the particular financial situation or goals of any person). As such, it should not be relied upon in making an investment decision.

United Kingdom

This document is prepared and provided by Edison for information purposes only and should not be construed as an offer or solicitation for investment in any securities mentioned or in the topic of this document. A marketing communication under FCA Rules, this document has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research.

This Communication is being distributed in the United Kingdom and is directed only at (i) persons having professional experience in matters relating to investments, i.e. investment professionals within the meaning of Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended (the "FPO") (ii) high net-worth companies, unincorporated associations or other bodies within the meaning of Article 49 of the FPO and (iii) persons to whom it is otherwise lawful to distribute it. The investment or investment activity to which this document relates is available only to such persons. It is not intended that this document be distributed or passed on, directly or indirectly, to any other class of persons and in any event and under no circumstances should persons of any other description rely on or act upon the contents of this document.

This Communication is being supplied to you solely for your information and may not be reproduced by, further distributed to or published in whole or in part by, any other person.

United States

Edison relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Investment Advisers Act of 1940 and corresponding state securities laws. This report is a bona fide publication of general and regular circulation offering impersonal investment-related advice, not tailored to a specific investment portfolio or the needs of current and/or prospective subscribers. As such, Edison does not offer or provide personal advice and the research provided is for informational purposes only. No mention of a particular security in this report constitutes a recommendation to buy, sell or hold that or any security, or that any particular security, portfolio of securities, transaction or investment strategy is suitable for any specific person.

London | New York | Frankfurt
20 Red Lion Street
London, WC1R 4PS
United Kingdom