DDoS Threat Assessment by Industry

Recommendations from the DRS Board

(August 25, 2025 / Version No. 1.0)

1. Introduction

Distributed Denial-of-Service (DDoS) attacks pose a significant threat to companies across various industries. The DDoS Resilience Score (DRS) provides a standardized assessment of resilience against such attacks. This document offers an initial evaluation of the DDoS threat level for different industries based on the DRS Score. The assessment follows a high-level overview, considering typical attack patterns and preferred targets of attacker groups.

Short Explanation of the DRS

The DRS Score is a metric designed to assess the resilience of an entity against DDoS attacks based on historical data, known vulnerabilities, and mitigation capabilities. It provides a comparative measure within and across industries to facilitate risk-based decision-making.

Reasons for This Document

This document aims to provide organizations with a preliminary understanding of their DDoS risk exposure based on industry trends. While it does not replace an in-depth security audit, it helps in recognizing potential threats and prioritizing mitigation efforts.

Legal Disclaimer

The DRS provide general recommendations based on years of experience. Each entity must conduct its own due diligence and gather individual threat intelligence. Documents always lag reality and may not reflect the full spectrum of attack techniques or zero-day vulnerabilities.

2. Methodology

The DRS Board monitors current developments in the DDoS scene and provides assessments for various threat actors and industries regarding the expected DRS level. Manufacturer reports, DFIR activities, and observations of ongoing activities are regularly incorporated into updates of the DRS standard. It follows a data-driven approach of measuring DRS for the industries by DRS board members and will be updated on a yearly basis. The following criteria are considered:

- **Attack Likelihood**: How frequently are companies in this industry targeted by DDoS attacks?
- **Attack Strength**: What is the typical intensity of attacks?
- **Impact**: What operational and financial damages can arise from an attack?
- **Resilience (DRS Score)**: An estimate of the industry's average resilience against DDoS attacks.

3. Exclusions

DRS 7 Level

This document does not consider DRS 7 threat actors, as these attackers have virtually unlimited resources, making effective defence difficult with reasonable countermeasures. State-sponsored entities or highly advanced threat actors operating at this level can overwhelm even the most robust defences. Companies facing such threats require specialized, case-specific security strategies beyond the scope of this assessment.

Tactics, Techniques, Attack Patterns (TTPs)

The tactics, techniques, and attack patterns used by adversaries are defined within the DRS standard and are therefore not the focus of this threat level assessment. This document solely provides an industry-level evaluation based on historical attack trends and known attacker groups. Organizations seeking a deeper technical analysis should refer to the full DRS framework for specific attack methodologies.

4. DDoS Threat Levels by Industry

The following table serves as the primary deliverable of this document, summarizing the DDoS threat levels across industries, common attacker motivations and techniques. (Industry sorted top down by Threat level)

Industry	Threat Level	Common Attacking Groups	Common Techniques
Banking, Financial Services, Insurance	6.0	Hacktivism, Ransom, DDoS Specialist	Layer 3,4,7 IoT, Browserbots
Energy	6.0	Hacktivism, DDoS Specialist, State Sponsored	Layer 3,4,7 IoT, Browserbots
Government	6.0	Hacktivism, State Sponsored	Layer 3,4,7 IoT, Browserbots
Internet and Telecommunications	6.0	Hacktivism, Ransom, DDoS Specialist	Layer 3,4,7 IoT, Browserbots
Gaming and Gambling	6.0	Ransom, DDoS Specialist	Layer 3,4,7 IoT, Browserbots
Computer Software, SaaS	5.5	Ransom, DDoS Specialist	Layer 3,4,7 IoT, Browserbots
Transportation and Logistics	5.0	Hacktivism, Ransom	Layer 3,4,7 IoT, Browserbots
Cryptocurrency	5.0	Ransom	Layer 3,4,7 IoT, Browserbots
Healthcare Providers	5.0	Booter Service	Layer 3,4 IoT
Manufacturing, Automotive	5.0	Hacktivism, Ransom	Layer 3,4,7 IoT, Browserbots
Retail, E-Commerce	4.5	Ransom, DDoS Specialist	Layer 3,4,7 IoT, Browserbots
Utilities	4.5	-	-
Marketing and Advertising	4.0	Booter Service	Layer 3,4 IoT
Education	4.0	Booter Service	Layer 3,4 IoT

5. Attacking Groups and Severity

To better understand the risk levels associated with each industry, the following table provides an overview of common attacking groups, their motivations, and the likelihood of their attacks.

Attacking Group	Explanation	Severity
Booter Service	Unpleasant customers using attack-for-hire services	Often and expectable
Ransom	Extortionists demanding payment to stop attacks	Often and expectable
Hacktivism	Political or ideological groups like NoName, Killnet, ect.	Often and expectable
DDoS Specialist	Competitors or contract offenders executing attacks	Often and expectable
Sportsman	Individuals attacking for fun, prospects, or as lone wolves	Seldom and less likely
State Sponsored	Nation-state actors conducting strategic cyber operations with high impact	Seldom and less likely

6. Conclusion and Recommendations

The threat landscape indicates that the financial sector, telecommunications, government and energy industries are at the highest risk of DDoS attacks. These industries should invest heavily in protective measures such as traffic filtering, scalable network infrastructures, and emergency response plans.

Industries with a medium threat level, such as healthcare and manufacturing, should enhance their resilience, especially through early detection and mitigation mechanisms.

Even industries with a lower risk should remain aware of potential threats and implement basic protection measures to safeguard against evolving attack patterns.

This assessment serves as an initial guideline. A detailed evaluation should be conducted through specialized audits and stress tests to obtain a more accurate understanding of the DDoS resilience of an entity..

7. Appendix - Industries in Detail

Based on the experience of the DRS Board members as well as DDoS Threat Intelligence Reports from companies like NETSCOUT, Imperva, Cloudflare, and Radware, the following industries are among the most affected by DDoS attacks. These sectors are particularly vulnerable due to their heavy reliance on online services, APIs, cloud infrastructure, and latency-sensitive applications.

In the DDoS context: ‘Tactics’ describe attackers’ objectives (e.g., service disruption or extortion), ‘Techniques’ are the methods used (e.g., volumetric floods, application-layer attacks), and ‘Procedures’ detail how attackers implement these techniques (e.g., leveraging IoT botnets or browser-based bots).

Top Industries Most Affected by DDoS Attacks:

Banking, Financial Services, Insurance

- **Tactics:** Disruption of critical financial services, extortion attempts
- **Techniques:** Layer 3/4 volumetric floods, Layer 7 HTTP(S) floods
- **Procedures:** Use of large botnets, browser emulation tools, coordinated multi-vector attacks

Computer Software, SaaS, and Internet Services

- **Tactics:** Service degradation to impact customer trust, ransom-driven attacks
- **Techniques:** API floods, reflection/amplification, Layer 3/4 attacks
- **Procedures:** Exploiting misconfigured services, hiring DDoS-as-a-Service platforms, leveraging cloud resource exhaustion

Energy, Utilities, and Manufacturing

- **Tactics:** Disruption of operational technology and critical services, politically motivated outages
- **Techniques:** Layer 3/4 volumetric attacks, targeted Layer 7 attacks
- **Procedures:** Use of IoT botnets, timing attacks to high-demand periods, occasional hacktivist coordination

Government and Public Sector

- **Tactics:** Visibility-driven disruptions, hacktivism, state-level pressure
- **Techniques:** Layer 3/4 volumetric floods, Layer 7 web service floods
- **Procedures:** Coordinated campaigns, rented botnets, exploiting public events as timing triggers

Healthcare Providers and Education

- **Tactics:** Temporary disruption of online portals, nuisance-level extortion

- **Techniques:** Layer 3/4 floods, limited application-layer attacks
- **Procedures:** Use of low-cost booter services, smaller botnets

Gaming, Gambling, Retail, and E-Commerce

- **Tactics:** Extortion through downtime threats, unfair competitive advantage
- **Techniques:** Layer 7 floods targeting login/APIs, Layer 3/4 volumetric attacks
- **Procedures:** Browser-based bots, botnets timed to product launches or tournaments

Transportation, Logistics, Marketing, and Advertising

- **Tactics:** Short-term disruption during campaigns, nuisance extortion
- **Techniques:** Layer 3/4 floods, small-scale Layer 7 attacks
- **Procedures:** Short rented botnet campaigns, occasional booter service use

This overview helps responsible stakeholders quickly assess which DDoS approaches are most relevant to their industry and adapt their defenses accordingly.

8. References

DRS Website: https://www.ddosresiliencyscore.org

DRS Standard: https://www.ddosresiliencyscore.org/wp-content/uploads/2024/11/DDoS-Resiliency-Score-Standard-2.1.0-1.pdf