Limit Login Attempts Reloaded

The State of Brute Force Attacks in WordPress: 2025

A Comprehensive Analysis by Limit Login Attempts Reloaded (LLAR)

Summary

Key findings from this report

Brute force attacks continue to pose a significant threat to WordPress websites worldwide. With over 40% of the internet powered by WordPress, the stakes are higher than ever to secure the ecosystem. This report explores the trends in brute force attacks from 2021–2024, shares LLAR's critical achievements, and outlines the future of WordPress security.

Brute force attacks from premium users per domain have increased 120% since Feb 2024, with emerging markets and Q4 seeing the highest activity likely due to increased internet adoption and cheaper resources.

LLAR now protects nearly 3 million websites globally, with premium users blocking 97% of attacks before reaching local databases - 20% YOY Improvement.

Attackers may be leveraging AI to bypass CAPTCHA, crack passwords, automate large-scale attacks, and use deepfake technology for social engineering.

LLAR’s future plans include AI-powered defenses, faster blocking times, enhanced reporting, and expanded services like backups to strengthen WordPress security.

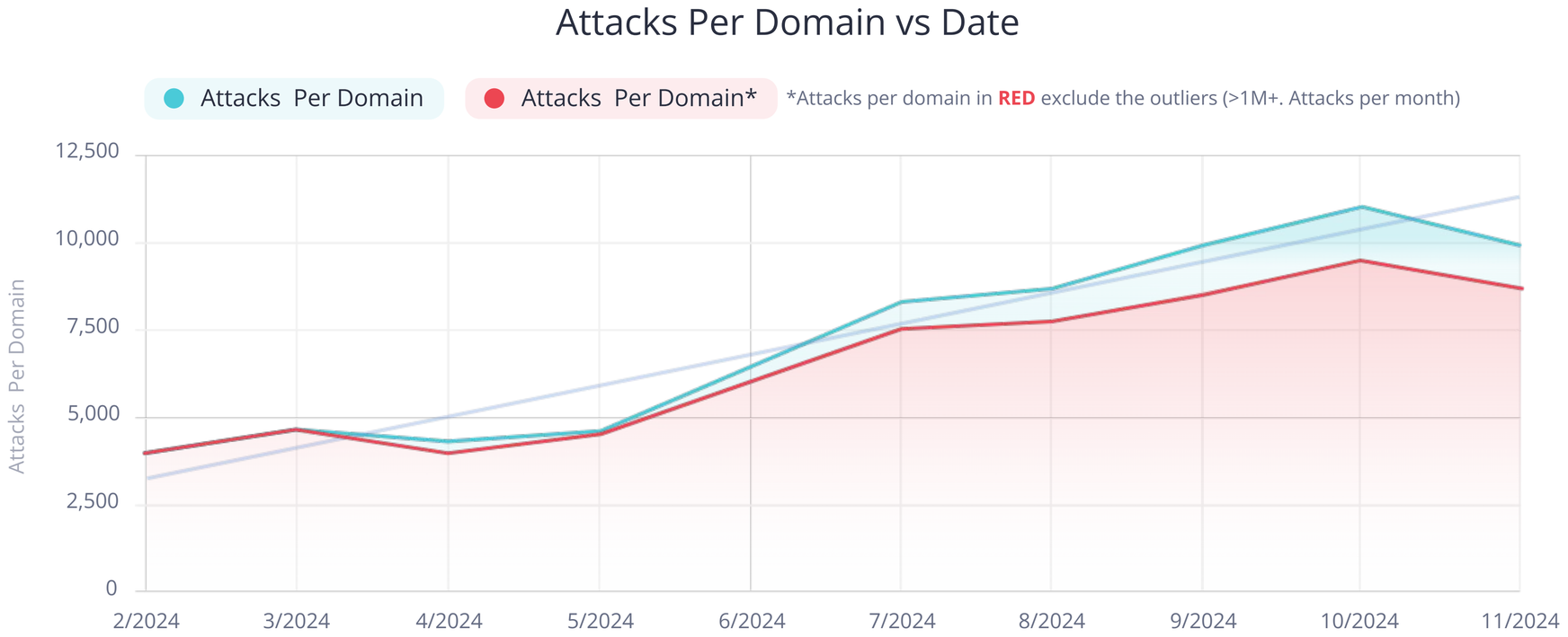
Trends in Brute Force Attacks

Attacks per domain (premium users): 2024

The data in this report is aggregated from premium and micro cloud users. IP data is not collected or accessible from non-cloud users of our plugin.

Attack Growth:

Attacks per domain **increased by over 120%** from February to December of 2024 indicating an increased threat level.



Top 10 days for attacks: 2021-2024

The data in this report is aggregated from premium and micro cloud users. IP data is not collected or accessible from non-cloud users of our plugin.

2021	Attacks	2022	Attacks	2023	Attacks	2024	Attacks
4-Jul-2021	766,655.00	4-Nov-2022	1,616,487.00	10-Feb-2023	1,360,594.00	1-Nov-2024	2,079,231.00
1-Jul-2021	735,689.00	1-Dec-2022	1,486,348.00	13-Mar-2023	1,336,437.00	1-Dec-2024	1,861,979.00
9-Apr-2021	669,395.00	5-Nov-2022	1,477,189.00	13-Mar-2023	1,336,437.00	6-Jun-2024	1,784,205.00
2-Sep-2021	660,350.00	26-Dec-2022	1,447,378.00	4-May-2023	1,321,960.00	1-Oct-2024	1,772,999.00
1-May-2021	646,356.00	2-Dec-2022	1,445,278.00	7-Feb-2023	1,255,254.00	2-Oct-2024	1,645,288.00
5-Jul-2021	643,614.00	3-Dec-2022	1,371,200.00	11-Feb-2023	1,244,771.00	2-Nov-2024	1,635,388.00
2-Aug-2021	632,232.00	4-Dec-2022	1,365,371.00	23-Jan-2023	1,243,454.00	1-Sep-2024	1,628,642.00
1-Aug-2021	631,153.00	3-Nov-2022	1,327,090.00	24-Jan-2023	1,228,909.00	2-Jun-2024	1,543,469.00
2-Jul-2021	628,726.00	6-Nov-2022	1,308,211.00	12-Feb-2023	1,203,832.00	1-Jul-2024	1,532,545.00
8-Apr-2021	619,551.00	8-Dec-2022	1,275,926.00	20-Jan-2023	1,167,146.00	1-Jun-2024	1,520,465.00

Top Days for Attacks:

The days with the most attacks more frequently occurred in the **2nd half of the year**, and **beginning of the month** opposed to the end.

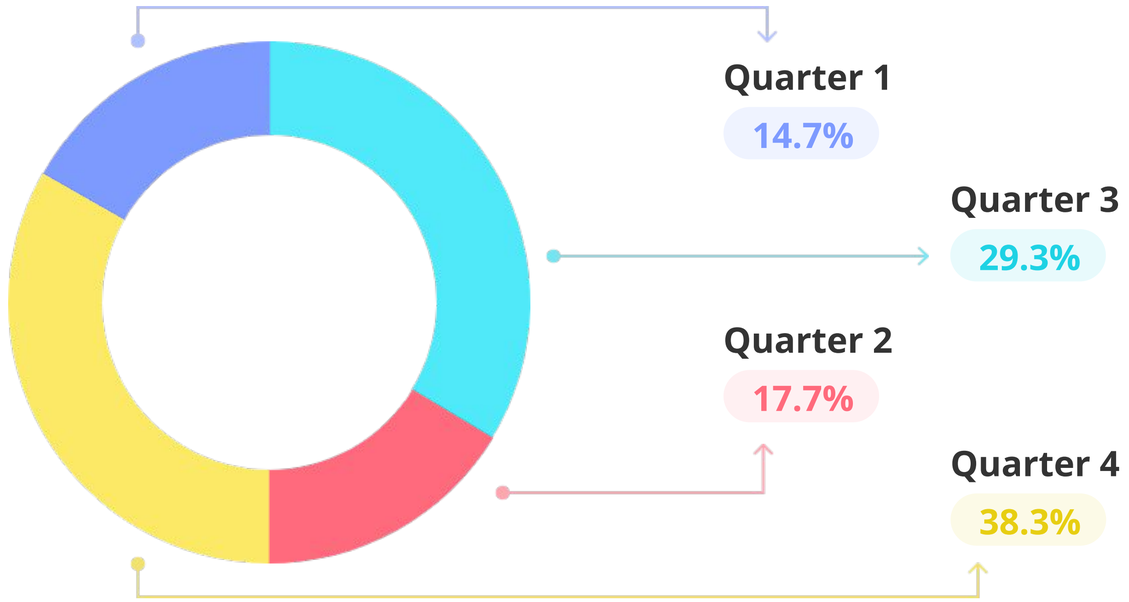
Quarters that receive most attacks: 2021-2024

The data in this report is aggregated from premium and micro cloud users. IP data is not collected or accessible from non-cloud users of our plugin.

Seasonal Trends:

Higher activity in Q4 aligns with e-commerce spikes and periods of reduced IT oversight (holidays).

Which Quarter Receives The Most Brute Force Attacks (2021-2024)



Global attacks by country: 2021-2024

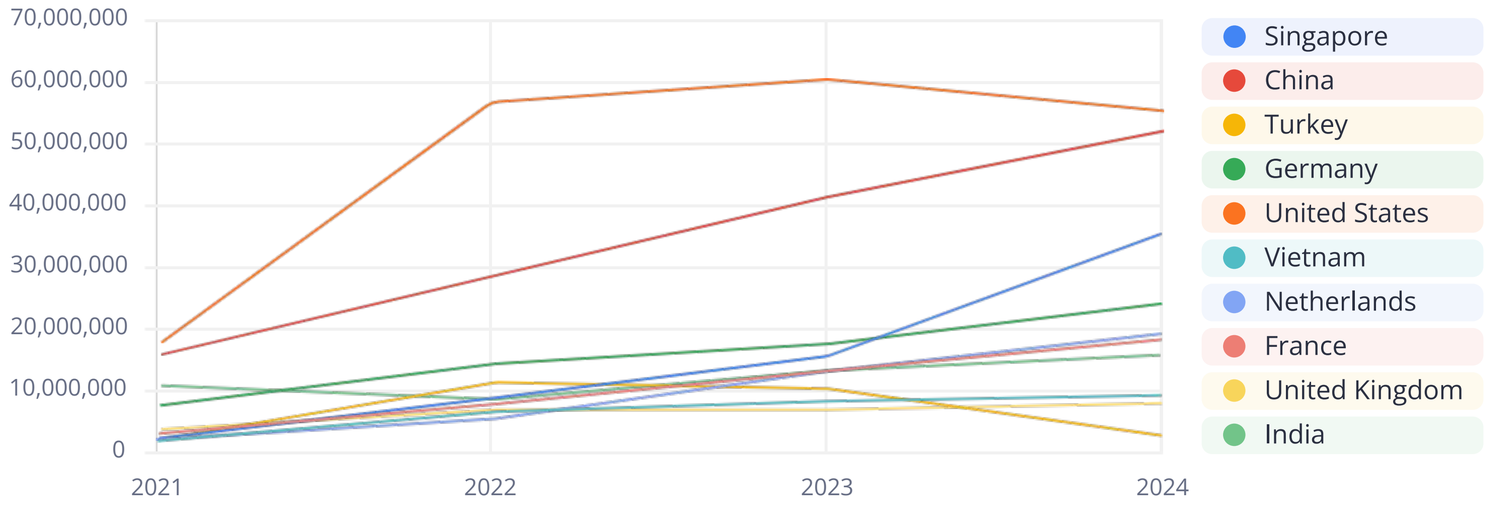
Attacks from United States IPs Decline:

For the first time in three years, the number of attacks originating from U.S.-based IPs has decreased. This shift suggests **less servers in the US are being used to launch attacks**, as well as hackers redirecting their efforts to emerging markets.

Global Distribution:

Emerging markets showed recent growth in attack volumes likely due to **increased internet adoption, cheaper resources, and lower cybersecurity awareness.**

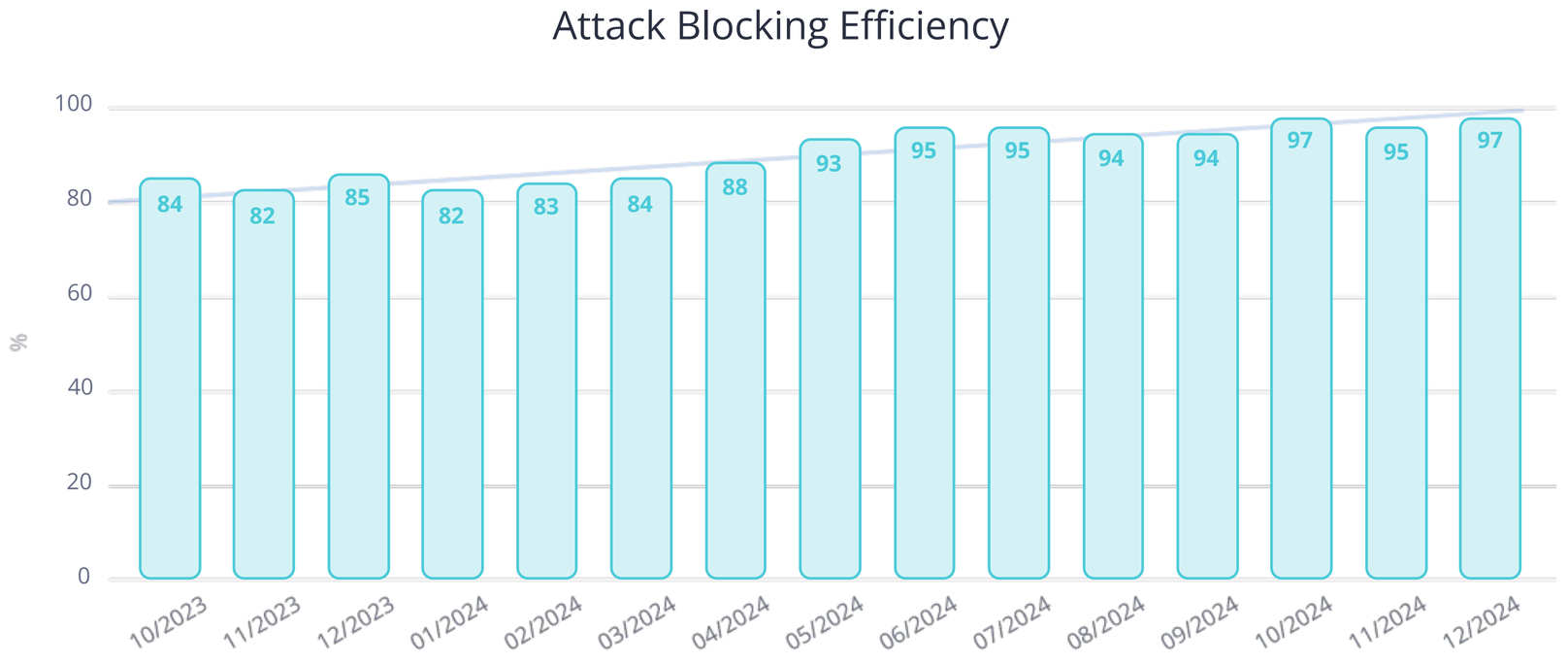
Global Attacks By Country (2021-2024)



Attack blocking efficiency: 2023-2024

Blocking Efficiency Improves 20% YOY:

Thanks to an expanded network of domains and improved tools, **LLAR now blocks over 97% of attacks for premium and micro cloud users.**



Emerging Threats

Credential Stuffing

Attacks may exploit previously leaked credentials from data breaches.

AI in Brute Force

Attackers are leveraging AI tools to bypass CAPTCHA.

Deepfake Technology

Attackers using AI to create deepfake audio and video, impersonating trusted individuals to deceive targets into revealing sensitive information.

LLAR’s Achievements

2024 Milestones

Efficiency Gains

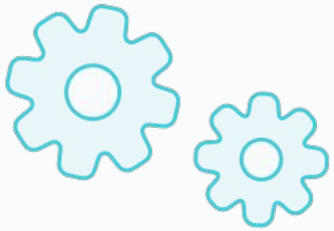
Avg blocking efficiency improved +20% since 2021, with LLAR now blocking 97% of attacks before reaching local databases.

Expanding Reach

LLAR now protects nearly 3 million websites, with 50,000 receiving advanced cloud protection.

Innovation

Major updates in 2024 included successful login logs, micro cloud, and several improvements within the plugin functionality.



Industry Challenges

Evolving Attack Vectors

Outdated Plugins

Large-scale botnets target vulnerabilities in outdated plugins and themes.

Weak Passwords

Despite awareness campaigns, weak passwords remain a major vulnerability.

Lack of Awareness

Many WordPress users adopt a reactive approach to security, often believing their websites are too small to be targeted by attacks.

Security Gaps in WordPress

- Many users fail to update plugins regularly, exposing them to known exploits.
- Poor hosting environments exacerbate vulnerabilities.

The Road Ahead: LLAR’s Vision for 2025

Future Developments

AI-Powered Defense
LLAR is working to integrate advanced AI tools that proactively predict and block attacks before they occur.

Faster Response Times
Efforts are underway to further reduce average attack blocking times by an additional 15%, ensuring quicker protection for users.

Form Protection
Leveraging cloud technology, LLAR will now safeguard a broader range of forms, including user registrations and blog comments.

Enhanced Reporting
New and improved dashboards will provide website owners with deeper insights into attack patterns and security trends.

Agency Tools
Advanced features will be introduced to help agencies manage multiple domains efficiently while enhancing security across their portfolios.

Expanded Services
LLAR plans to offer additional services, such as backups, to protect user data in the event of exploits or successful attacks.

Recommendations for Website Owners

Recommendations for Website Owners

1 **Upgrade to LLAR Premium**

Unlock advanced cloud protection with features like country blocking, form safeguarding, performance optimization, successful login tracking, a robust login firewall, and much more!

2 **Use Strong Passwords**

Replace weak passwords with randomly generated ones stored in a password manager.

3 **Monitor Logs**

Use tools like LLAR to stay informed about login attempts.

4 **Adopt Two-Factor Authentication (2FA)**

A simple yet powerful defense mechanism.

5 **Regularly Update Software**

Keep WordPress, plugins, and themes up to date.

Limit Login Attempts Reloaded

Thank You!

By Limit Login Attempts Reloaded