August 1, 2024

New Advancements in DDoS-as-a-Service Tools Increase Security Risks

Key Attack Insights:

- AI-powered CAPTCHA-solving capabilities are emerging, potentially rendering traditional protections ineffective
- Hybrid architectures combining botnets and servers are becoming more prevalent, complicating attack source identification
- Attack power and efficiency have significantly increased with some tools claiming up to 600,000 requests per second (RPS)
- DDoS-as-a-service tools are expanding to international markets, particularly in Asia
- High-profile and diverse websites are increasingly targeted, demonstrating the evolving ambition of attackers

Radware's cyberthreat intelligence (CTI) team has observed significant advancements in DDoS-as-a-service tools throughout 2024. These developments pose increased risks to organizations across various sectors, necessitating a reevaluation of current DDoS mitigation strategies.

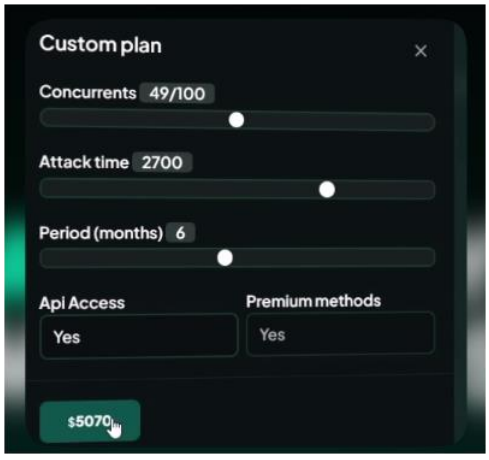

Figure 1: Screenshot of DDoS as a service tool (source: Telegram)

Figures 2-4: AI-generated advertisement for DDoS-as-a-Service tool (source: Telegram)

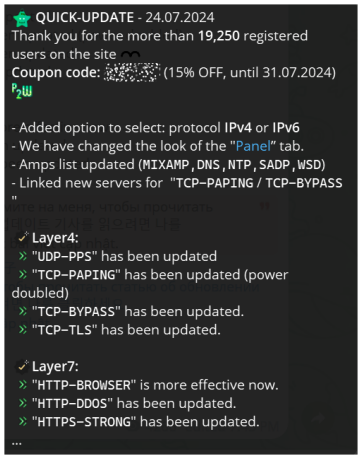

Figure 5 – Update showcasing advanced DDoS as a service capabilities (source: Telegram)

Our analysis reveals five key trends that characterize the latest generation of DDoS-as-a-service tools:

1. Enhanced CAPTCHA Bypass/Solving Capabilities

DDoS-as-a-service tools have demonstrated increasingly sophisticated CAPTCHA bypass and solving techniques with a notable shift towards AI-driven solutions. For instance, the Stresser Cat tool introduced HTTP-TESTAROSSA Browser, noting on Telegram that it had been "updated to bypass hCaptcha, reCaptcha [13 Mar 2024]" and later "enhanced to bypass DDoS-Guard protection and text captcha [18 May 2024]. " This tool reportedly uses Neural networks to solve various types of CAPTCHAS at different levels.

Similarly, the Stresser.SU Telegram channel reported improvements in its HTTPS-CUSTOM method, stating it is "now stable and highly powerful" as of May 7, 2024. The DDG Stresser tool also showed advancements, claiming its DDG-Browser "completely bypasses Cloudflare captcha."

2. Hybrid Architecture Adoption

There's a noticeable shift towards hybrid architectures combining both botnets and dedicated servers. For example, according to its Telegram channel, the DDG Stresser tool "started with just a botnet, then began incorporating server-based capabilities over time, transitioning to a hybrid architecture by late 2022 that leverages both a botnet and proxy servers." Similarly, QuickDown.Pro introduced a "Botnet addon and new plans related to the Botnet network" in September 2023.

3. Increased Attack Power and Efficiency

Throughout 2024, there have been consistent reports of increased attack power across multiple tools. Stresser Cat reported improvements in its HTTP-FUKU method, claiming on Telegram that it was "Enhanced to 350-600k rps and fine-tuned to bypass UAM and HTTP-DDOS [12 Jan 2024]". The DDG Stresser tool reported high request per second (RPS) rates for some methods, with its Strong-CF method claiming "250,000 requests/sec". QuickDown.Pro also boasted of high attack rates, with its DNS method "pushing around 40/50gbps" as of April 16, 2024.

4. Expansion to International Markets

There's a clear trend of these services expanding their reach to international markets, particularly in Asia. QuickDown.Pro, for instance, added translations in Chinese, Russian and Korean on May 10, 2024, followed by Vietnamese on July 5, 2024. Stresser.SU consistently provided translations in English and Chinese throughout its chat history. The DDG Stresser tool added Russian translations on February 6, 2023, and Chinese translations on December 22, 2023.

5. Targeting of High-Profile and Diverse Websites

In 2024, these tools demonstrated their capabilities by successfully attacking a wide range of high-profile targets. Stresser.SU reported successful attacks on major platforms like Instagram and Binance, claiming on Telegram to have taken "Instagram.com (World's largest social media platform offline with 500 concurrent attacks)" on March 21, 2024, and "Binance.com (World's largest cryptocurrency exchange offline with 1000 concurrent attacks)" on March 17, 2024.

Reasons for Concern

- AI-powered CAPTCHA bypass capabilities could render traditional bot detection methods ineffective, potentially leading to a surge in successful DDoS attacks.

- Hybrid architectures make it more challenging to identify and block malicious traffic sources, potentially overwhelming existing defense mechanisms.
- The significant increase in attack power and efficiency may outpace current DDoS mitigation capacities, leaving organizations vulnerable to more potent attacks.
- The expansion to international markets could lead to a more diverse and unpredictable threat landscape, complicating threat intelligence and response efforts.
- The targeting of high-profile websites demonstrates the growing ambition and capabilities of attackers, raising the stakes for organizations across various sectors.

Recommendations

- Implement advanced behavioral analysis tools to distinguish between human and bot traffic more accurately.
- Develop more sophisticated traffic analysis techniques that can detect attack patterns across diverse sources.
- Reassess and potentially upgrade DDoS mitigation infrastructure to handle higher volumes of attack traffic.
- Enhance threat intelligence capabilities to monitor a wider range of underground forums and markets, including those in different languages.
- Increase the frequency and depth of security audits and penetration testing, particularly for high-profile targets.
- Develop specialized DDoS mitigation strategies for different types of services within your organization.
- Implement 24/7 monitoring and rapid response capabilities to maintain a constant high-level security posture.
- Work closely with business continuity and public relations teams to develop comprehensive incident response and communication plans.

Resources List

- Stresser Cat Telegram channel
    1. March 13, 2024, HTTP-TESTAROSSA Browser updated to bypass hCaptcha and reCaptcha
    2. May 18, 2024, HTTP-TESTAROSSA Browser enhanced to bypass DDoS-Guard protection and text captcha
    3. January 12, 2024, HTTP-FUKU enhanced to 350-600k rps, bypassing UAM and HTTP-DDOS
    4. November 2, 2023, HTTP-REACT enhanced to 400k rps for unprotected targets with 120 slots
    5. October 9, 2023, Started providing translations in English and Chinese
- Stresser.SU Telegram channel
    1. May 7, 2024, HTTPS-CUSTOM method updated, reported as stable and highly powerful
    2. March 21, 2024, Claimed attack on Instagram.com, taking it offline with 500 concurrent attacks
    3. March 17, 2024, Claimed attack on Binance.com, taking it offline with 1000 concurrent attacks
    4. Continuous, Provided consistent translations in English and Chinese throughout its history
- DDG Stresser Telegram channel
    1. February 6, 2023, Added Russian translations to some posts
    2. December 22, 2023, Added Chinese translation for a service outage notification
    3. No specific date, Reported high RPS rates for methods like HTTP-BYPASS (35,000 requests/sec) and Strong-CF (250,000 requests/sec)
    4. Late 2022, Transitioned to a hybrid architecture leveraging both botnet and proxy servers
- QuickDown.Pro Telegram channel
    1. May 10, 2024, Added translations in Chinese, Russian, and Korean
    2. July 5, 2024, Added Vietnamese translation
    3. April 16, 2024, Claimed DNS method pushing around 40/50gbps
    4. March 28, 2024, Reported OVH-BYPASS pushing ~4.50/5.00/GBPS per connection
    5. September 13, 2023, Introduced 'Botnet' addon and new plans related to the Botnet network
    6. October 9, 2023, Reported attack on github[.]com

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.