Keymous+ Threat Actor Profile | NETSCOUT

Archived: 2026-04-05 17:51:29 UTC

- Arbor Networks - DDoS Experts

DDoS campaign with evolving partnerships

Executive Summary

Between February and September 2025, NETSCOUT's ATLAS telemetry confirmed 249 distributed denial-of-service (DDoS) attacks attributed to the threat actor Keymous+ targeting organizations across 15 countries and 21 industry sectors. Although the group's individual attacks peaked at 11.8Gbps, collaborative efforts with partners reached 44Gbps, demonstrating significantly enhanced disruptive capability.

Government agencies, hospitality and tourism, transportation and logistics, financial services, and telecommunications face the highest risk. Morocco, Saudi Arabia, Sudan, India, and France have experienced the most frequent attacks.

Keymous+ uses widely available DDoS-for-hire services and compromised devices, making its tactics accessible and repeatable. In April 2025, the group announced a partnership with threat actor DDoS54, with observed joint operations demonstrating a nearly 4x increase in attack bandwidth from 11.8Gbps to 44Gbps.
NETSCOUT continues monitoring this evolving threat and will provide updates as the situation develops.

Key Findings

- **Observed activity:** February through September 2025
- **Confirmed attacks:** 249 events, over 39 distinct active days
- **Target scope:** 60 organizations across 21 industries in 15 countries
- **Attack types:**
    - Reflection/amplification: chargen, CLDAP, DNS, memcached, NTP, NetBIOS, rpcbind, SNMP, L2TP, WS-DD
    - Direct floods: DNS query, UDP, TCP
- **Infrastructure:**
    - 42,000+ average unique source IPs per attack (ranging from tens of thousands to hundreds of thousands); distributed across Tor, public cloud, VPNs, access networks, and proxies
- **Peak observed bandwidth:** 11.8Gbps (individual); 44Gbps (collaborative)
- **Partnership noted:** Public collaboration with DDoS54 announced April 12, 2025

Observed DDoS Campaigns

Targeting Analysis

Top targeted industries:

- Government (administration and public sector)
- Hospitality and tourism
- Transportation and logistics
- Financial services (including banking and mortgage)
- Network and telecommunications

Most-targeted countries:

- Morocco
- Saudi Arabia
- Sudan
- India
- France

The campaign’s broad targeting across multiple sectors and geographies suggests opportunistic attacks rather than focused operations, potentially indicating DDoS-for-hire activity. However, the concentration on Middle Eastern and North African countries (Morocco, Saudi Arabia, Sudan) may also suggest regional geopolitical motivations.

Operational Timing Patterns

Analysis of Keymous+ attack timing reveals human-directed operations with strategic precision. The group concentrated more than 30 percent of attacks during a single hour (06:00 UTC), corresponding to 07:00-09:00 a.m. across Morocco, Saudi Arabia, and Sudan. This timing maximizes disruption when government agencies open, financial markets begin trading, transportation systems enter peak scheduling, and hotel systems process morning bookings. Security operations center (SOC) teams are still mobilizing while legitimate traffic surges, making attack isolation significantly more difficult.

The attack distribution shows clear operational discipline: sustained baseline activity (5 to 10 attacks) punctuated by coordinated surges (as many as 79 attacks). The complete absence of activity during specific hours could indicate various operational constraints, from resource limitations to infrastructure availability windows.

Key temporal indicators:

- **Primary strike window:** 06:00 UTC (79 attacks) targeting morning operational surge across critical sectors
- **Secondary peaks:** 01:00, 10:00, 12:00 UTC (22–32 attacks) maintaining pressure during business hours
  Operational gaps: Hours 4, 8, 9, 22, and 23 UTC show zero activity
- **Sector optimization:** Peak times align with maximum telecommunications strain as all targeted infrastructure simultaneously experiences demand spikes

Attack Infrastructure and Distribution

Keymous+ attacks utilized diverse infrastructure spanning Tor exit nodes, public cloud instances, compromised Internet of Things (IoT) devices, commercial VPN/proxy services, and directly infected hosts. The scale and variety of sources, ranging from tens of thousands to hundreds of thousands of unique IPs per attack, indicates the group leveraged multiple botnet infrastructures and DDoS-for-hire platforms during the campaign.

Most source IPs appear to be spoofed, leveraging modern DDoS-for-hire platforms that offer simple dropdown menus to spoof Autonomous System Numbers (ASNs) and IP addresses from major service providers and cloud platforms. Whether Keymous+ directly managed these resources or obtained them through third-party services remains unconfirmed.

Observed source categories:

- Tor exit nodes
- Public cloud instances
- Compromised consumer and IoT devices
- Commercial VPN and proxy services
- Direct-path traffic from infected hosts

Tactics, Techniques, and Procedures

Keymous+ demonstrates operational flexibility via varied attack methods and durations.
Primary techniques observed:

- Reflection/amplification attacks exploiting chargen, CLDAP, DNS, memcached, NTP, NetBIOS, rpcbind, SNMP, L2TP, and WS-DD protocols
- Direct flooding via DNS queries, UDP, and TCP
- IP spoofing across major service providers and cloud platforms
- Coordinated multivector attacks combining different methods

Attack durations and packet rates vary significantly between incidents, suggesting the group adapts tactics based on target defenses and desired impact. The combination of readily available DDoS-for-hire tools with custom attack patterns indicates both opportunistic and targeted operations.

Partnership with DDoS54

On **April 12, 2025**, Keymous+ publicly announced a partnership with threat actor **DDoS54**. NETSCOUT observed elevated traffic volumes and increased vector complexity beginning immediately thereafter.

Notable Collaborative Operation (April 13–14)

- **Peak bandwidth:** 44Gbps
- **Packet rate:** 4.23mpps
- **Packet size:** ~1,312 bytes
- **Attack vectors:** CLDAP amplification, DNS amplification, UDP flooding (notably UDP/443)
- **Duration:** ~11 minutes
- **Distribution:** Wide deployment using reflectors and amplification infrastructure (CLDAP, DNS, SNMP, L2TP)

Associated Threat Actors

Beyond the confirmed DDoS54 partnership, open-source intelligence suggests potential connections between Keymous+ and the following threat actors:

- **NoName057(16)**
- **Dark Storm Team**
- **Anonymous Gaza**

These associations remain unverified by NETSCOUT telemetry. Only the DDoS54 collaboration has been confirmed via both public announcement and observed joint operations.

Conclusion

From February to September 2025, Keymous+ executed 249 DDoS attacks across 15 countries, targeting 21 industries with conventional yet effective methods. Its operational model, leveraging widely available DDoS tools, diverse infrastructure, and a partnership with DDoS54 that amplified attack bandwidth to 44Gbps, underscores a growing threat.

The group’s broad, opportunistic targeting suggests expanding operations, requiring organizations to prepare for sustained attacks at increasing scale. To stay ahead, explore NETSCOUT’s Arbor solutions for gaining visibility, blocking malicious traffic, and mitigating these evolving DDoS campaigns.

Mitigation Strategy: Arbor Solutions from NETSCOUT

To help organizations defend against campaigns such as those operated by Keymous+ and its collaborators, NETSCOUT offers the following layered solutions:

1. **Arbor Sightline**: Real-time visibility and anomaly detection using flow telemetry across service providers and enterprises
2. **Arbor Edge Defense (AED)**: Inline, always-on protection that blocks both inbound DDoS and outbound threat communications
3. **Arbor Threat Mitigation System (TMS)**: High-throughput scrubbing that removes malicious traffic before it hits business-critical services
4. **Arbor ATLAS Intelligence Feed (AIF)**: Live global threat intelligence tailored to Arbor solutions, updating blocklists and detection logic in near real time

Explore NETSCOUT's Arbor solutions for gaining visibility, blocking malicious traffic, and mitigating evolving DDoS campaigns.

Posted In

- Arbor Networks - DDoS Experts
- Attacks and DDoS Attacks
- DDoS Tools and Services
