K logix
Be confident.

JANUARY 2025 | THREAT INTEL NEWSLETTER

The DDoS Shortcut: How Threat Actors Are Simplifying Large-Scale Attacks

C-Suite level threat review by applicable business area addressing active threats.

K logix has tracked a rise in Distributed-Denial-of-Service (DDoS) attacks, a trend we expect to see continue in 2025. The increase can be attributed to the ease of access to DDoS tools and incentives for cybercriminals. Groups like NONAME057 (16) offer rewards to boost participation in DDoS attacks, while the threat actor Matrix allows attackers to easily purchase powerful DDoS tools, lowering the barrier for unskilled hackers. As these DDoS attacks become easier to execute, they pose an even greater threat for 2025, with organizations facing greater risk of downtimes and disruption to critical operations.

NONAME057(16):

NONAME057(16) is a pro-Russian cybercriminal group with strong geopolitical motivations, primarily targeting countries aligned with NATO. Known for their large-scale DDoS attacks, NONAME057(16) focuses on critical sectors like government, transportation, and finance. Since gaining prominence in 2022, the group has also been seen targeting election websites.

Matrix:

Matrix is a cyber threat actor known for launching financially motivated DDoS attacks by exploiting vulnerabilities and misconfigurations in Internet of Things (IoT) systems. Their operations started in late 2023 and primarily target countries such as China, Japan, and the United States due to their high IoT device usage. By compromising these devices, Matrix builds botnets that can carry out massive DDoS attacks.

NONAME057(16)

Threat Level: Medium

Attack:

NONAME057(16) has created a custom tool, Project DDoSia, to carry out DDoS attacks. This tool is voluntarily run by users to help NONAME057(16) operations. If the attack is successful, NONAME057(16) will reward the user with cryptocurrency. DDoSia operates across multiple platforms such as Windows, Linux, and macOS and does not require administrator privileges, making it easier for the participants to carry out attacks. What makes NONAME057(16) attacks particularly effective is the reconnaissance they conduct (MITRE TA0043). Before attacking, the group carefully identifies critical pages that are essential to the functionality of the organizations site. They then craft traffic that closely resembles legitimate user activity making it harder for security systems to detect malicious requests (MITRE T1562.001). By targeting key functions, they can cripple important website features, resulting in significant downtime and service disruption (MITRE T1489 and MITRE T1498). The participation from cyber criminals who are motivated by potential rewards enhances the scale and effectiveness of NONAME057(16) DDoS attacks.

Remediation:

- Implement DDoS defense solutions
- Deploy Web Application Firewalls
- Ensure rate limits are set to reduce the number of requests from a single IP address

Matrix

Threat Level: Medium

Attack:

Matrix runs a large DDoS campaign, supported by their Kraken Autobuy service, which allows cyber criminals to easily buy access to Matrix DDoS tools. Kraken Autobuy makes it simple for attackers of all skill levels to complete attacks, expanding the reach and impact of Matrix's operations. Matrix's DDoS attacks start with brute-force attempts and exploiting public facing applications to access vulnerable IoT devices (MITRE T1078 and MITRE T1190). Once inside, they deploy malware, such as Mirai, to control and turn devices into bots that can be used to flood other sites with traffic (MITRE T1610). They also use scripts to disable security measures, such as antivirus software, ensuring the malware on the bots remains undetected (MITRE T1070). Matrix manages their botnet through encrypted channels on apps like Telegram and Discord (MITRE T1102 and MITRE T1573). With Kraken Autobuy and their extensive network, Matrix's DDoS attacks are powerful and capable of causing major disruptions and downtime for their victims (MITRE T1489 and MITRE T1498).

Remediation:

- Ensure password best practices are followed for all accounts
- Maintain a comprehensive patching program to ensure all vulnerabilities are addressed
- Ensure no default credentials are used for IP cameras, DVR's, or routers

NONAME057(16):

- **Overview of NONAME057(16) capabilities**: https://www.netscout.com/blog/asert/noname057-16
- **NONAME057(16) Attack Toolkit**: https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/

Matrix:

- **Overview of Matrix's capabilities**: https://www.aquasec.com/blog/matrix-unleashes-a-new-widespread-ddos-campaign/#section-1
- **Matrix Botnet Campaign:** https://thehackernews.com/2024/11/matrix-botnet-exploits-iot-devices-in.html

How K logix Can Help

Technology Advisory

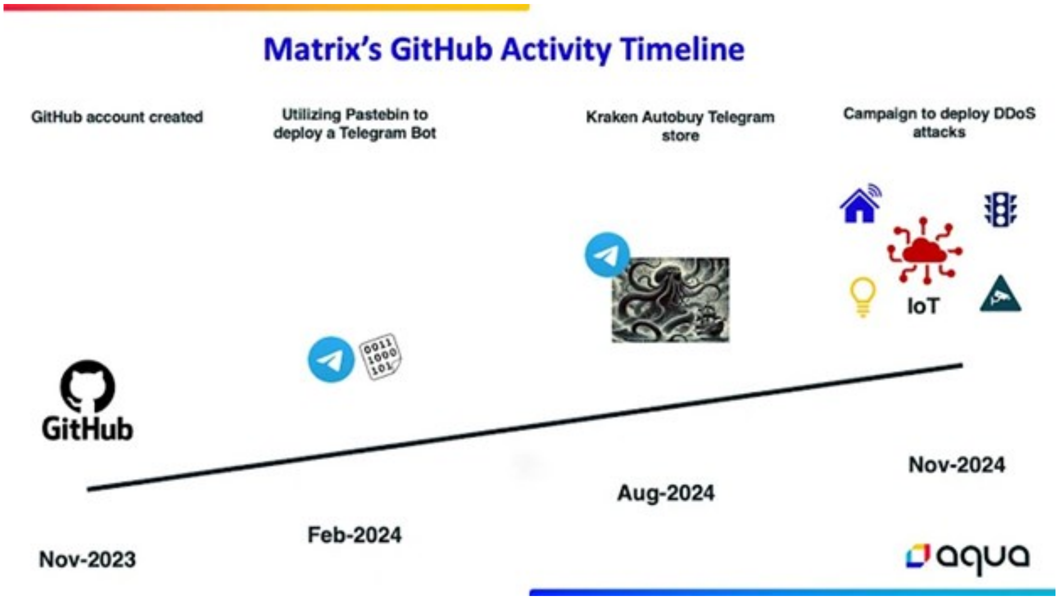
- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports


Matrix's GitHub Activity Timeline
GitHub account created
Utilizing Pastebin to deploy a Telegram Bot
Kraken Autobuy Telegram store
Campaign to deploy DDoS attacks
IoT
GitHub
Nov-2023
Feb-2024
Aug-2024
Nov-2024
aqua

Source: https://www.aquasec.com/blog/matrix-unleashes-a-new-widespread-ddos-campaign/

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.