
corero
[NETWORK SECURITY]

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Network Resilience in the Real World

How regional conflict is shaping the threat of Distributed Denial of Service to our networks.



corero
[NETWORK SECURITY]

MDNOG

I'LL BE THERE



Join me at
MDNOG 1

October 8 - 9, 2026
Digital Park
Chişinău, Moldova

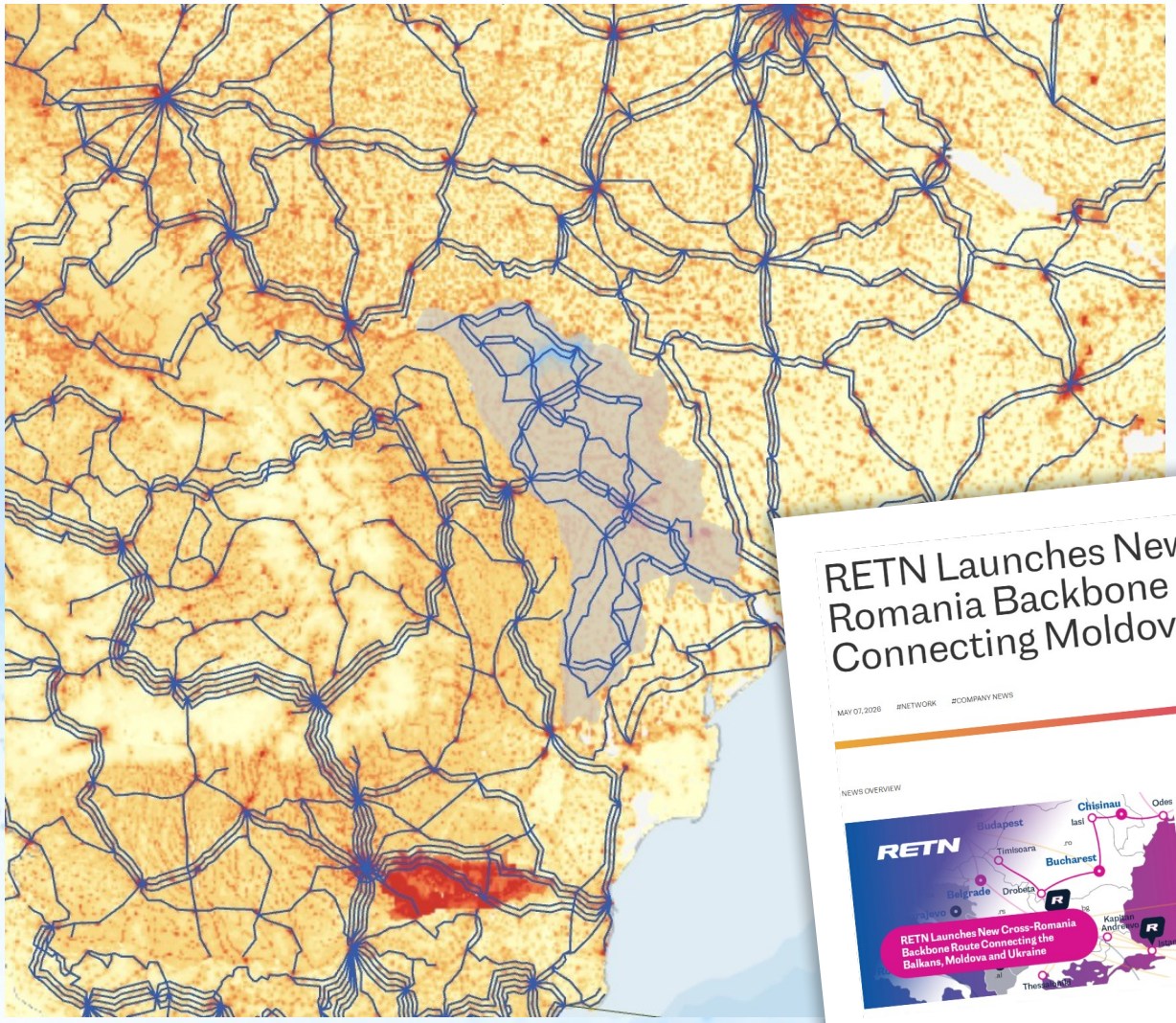
Peter Cutler
Senior International
Solution Engineer

Corero Confidentia

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Build out and physical route diversity in Moldova





RETN Launches New Cross-Romania Backbone Route Connecting Moldova and Ukraine

TALK TO US

MAY 07, 2026 #NETWORK #COMPANY NEWS

NEWS OVERVIEW

RETN Launches New Cross-Romania Backbone Route Connecting Moldova and Ukraine

Bucharest, London – May 7, 2026 – RETN, the leading independent global network service provider, announces the launch of a new end-to-end backbone route linking Drobeta, Bucharest, Iași and Chișinău. Delivered as a single continuous backbone path, the route provides a new physical connectivity option across Romania and into Moldova, creating an alternative to established regional IP transit corridors in Eastern Europe.

The route forms part of RETN's broader strategy to strengthen its optical network across Central and Eastern Europe. By connecting Romania and Moldova with RETN's existing Balkans' corridor linking Budapest, Timișoara and Sofia, the expansion creates a new geographical path across the region and delivers greater physical route diversity across its international backbone.

It also enables alternative routing to Ukraine via Moldova and into the Balkans via Bulgaria, providing additional options for regional and international traffic flows. This is particularly relevant for customers seeking physical route diversity across Eastern and South-Eastern Europe.

Moldova (ASC) enters trilateral Alliance for Cyber Resilience

20th February 2026

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Guvernul Republicii Moldova
Agenția pentru Securitate Cibernetică

Trei state – un singur vector strategic: Ucraina, România și Moldova Înființează Alianța Cibernetică pentru Reziliență Regională

Cooperare

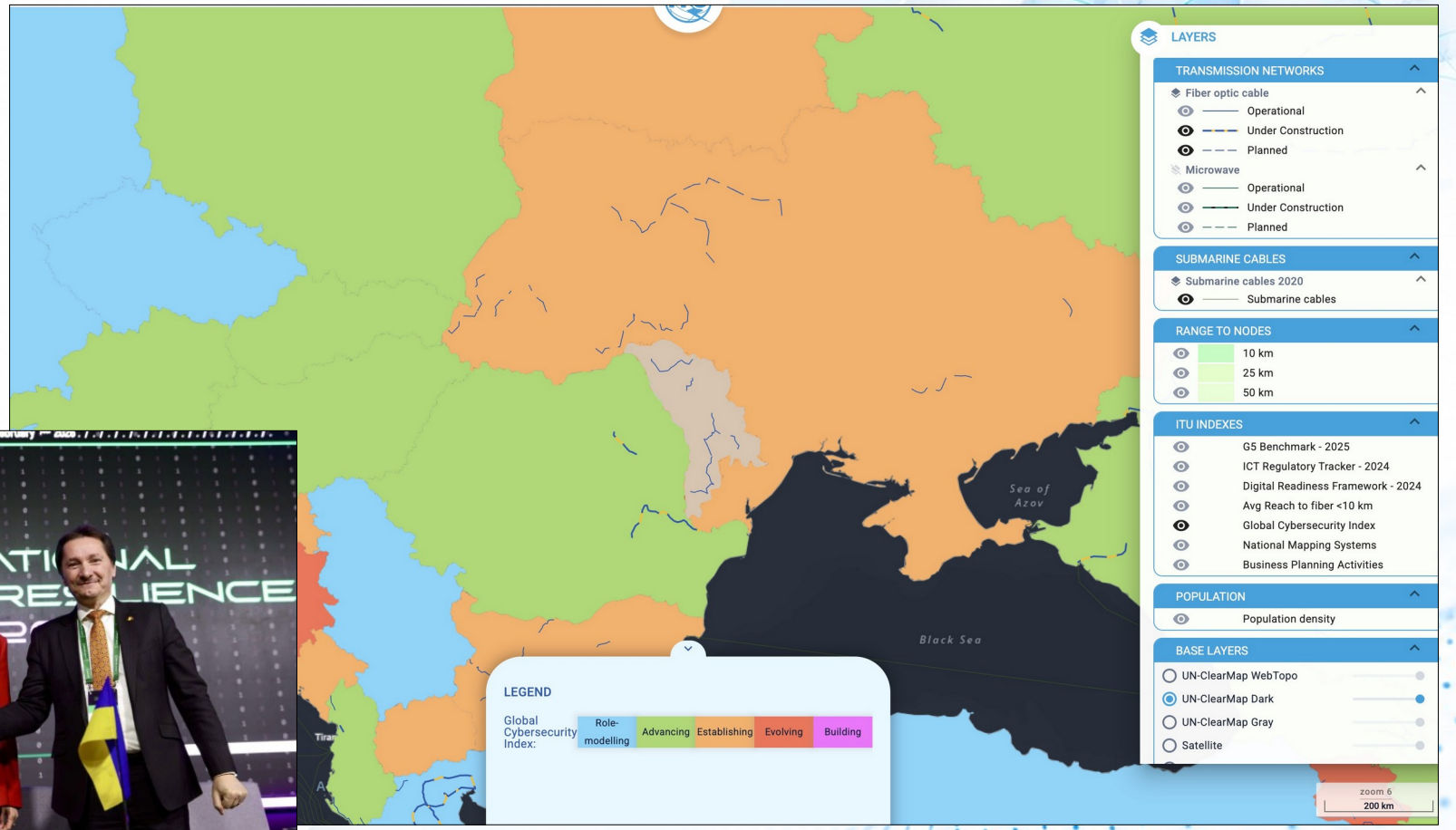
20 February 2026 Timp de citire: 6 minute

În marja evenimentului Kyiv International Cyber Resilience Forum, desfășurat în perioada 19–20 februarie, a fost semnat un Memorandum de Înțelegere trilateral între Centrul Național de Coordonare a Securității Cibernetice din Ucraina (NCSCC), Directoratul Național de Securitate Cibernetică din România (DNSC) și Agenția pentru Securitate Cibernetică a Republicii Moldova (ASC), prin care este instituită „Alianța Cibernetică pentru Reziliență Regională", un nou cadru strategic de cooperare destinat consolidării rezilienței cibernetice și intensificării coordonării regionale în f

Scopul alianței este de a facilita schimbului de informații, expertiză și b
tehnologiilor avansate și acordarea de asistență reciprocă în protejarea v
consolidarea mecanismelor de răspuns coordonat la incidente cibernetice

În cadrul evenimentului, reprezentanții celor trei state au subliniat imp
regional marcat de provocări complexe de securitate:
„Este important nu doar că avem același inamic și ne confruntăm cu acel
și avem înțelegerea comună că doar împreună putem consolida și cons
Ucraina va depune toate eforturile, cunoștințele și expertiza noastră pent
impact real. Îndemn națiunile partenere și prietenii noștri să ni se alătu





MDNOG | corero NETWORK SECURITY

MDNOG | corero NETWORK SECURITY

DETECT | DEFEND | AUTOMATE | STAY AHEAD

Threat Research Insights

EU-Team: Observations for Moldovan ISPs

A pivot from traditional reflectors to Botnet driven activity from embedded IoT devices

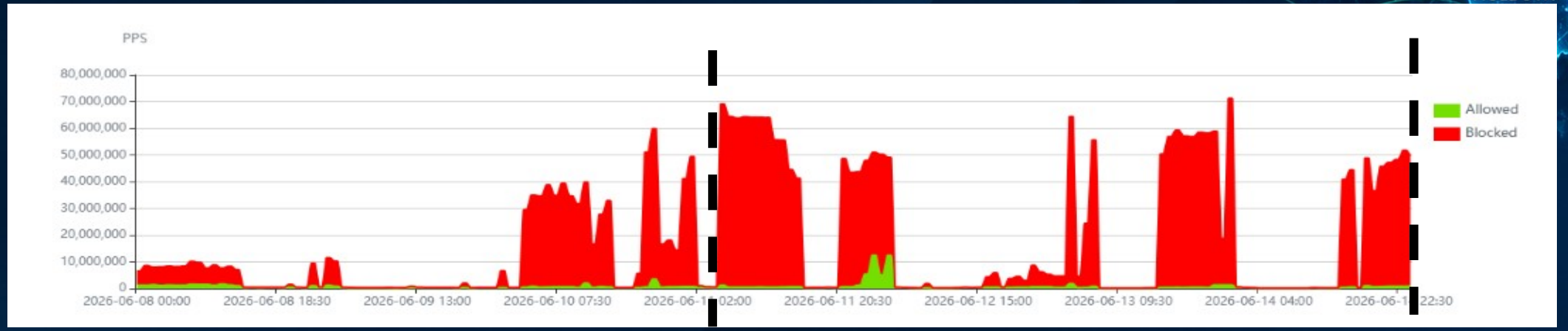


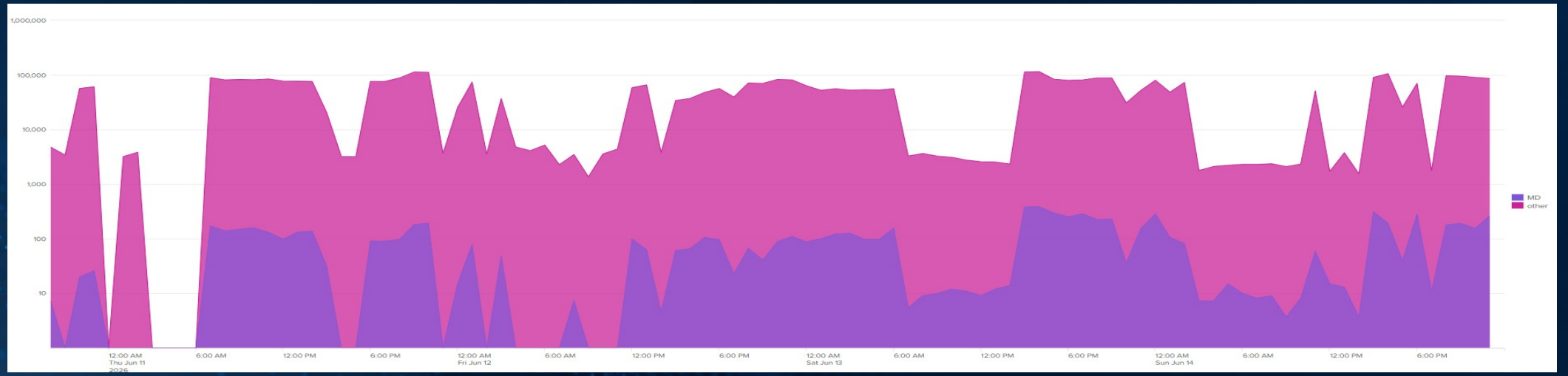
MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

DDoS Incident 8th-15th June. Targeting South American ASN

Viewpoint: Tier-1 operator observation



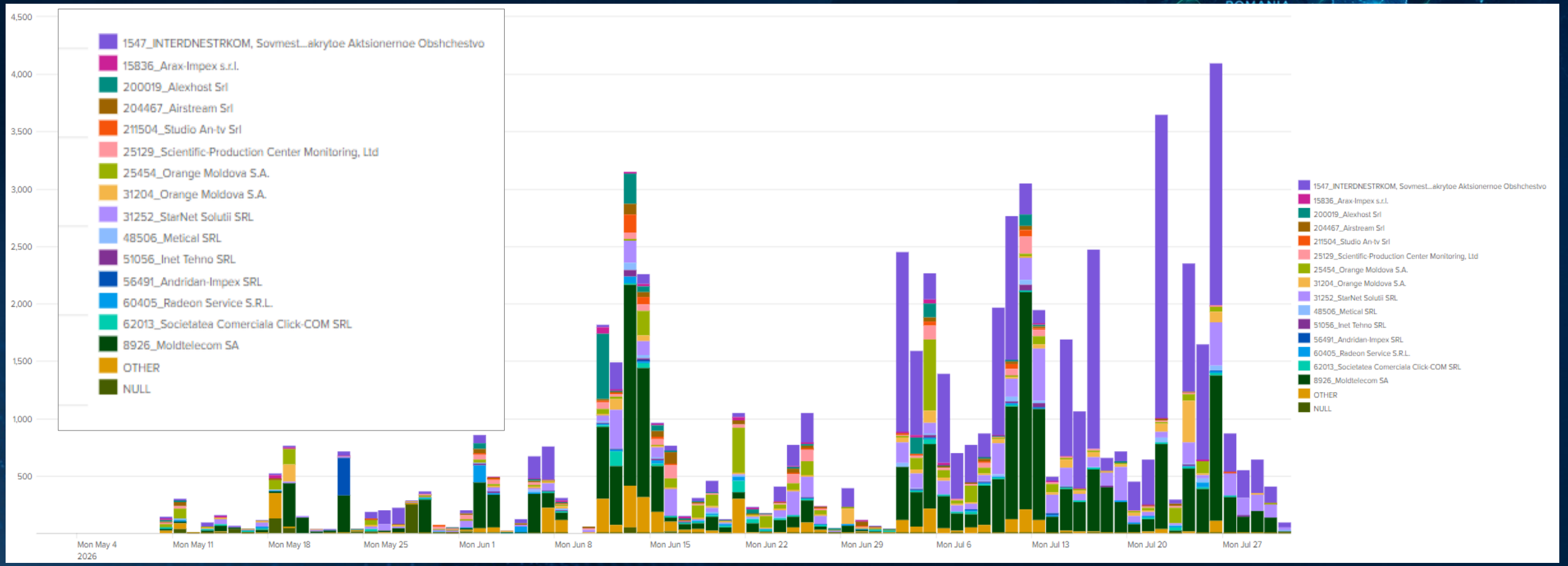


MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Relative DDoS participation by Autonomous System Source 3 months

Viewpoint: Tier-1 operator observation



MDNOG | corero NETWORK SECURITY

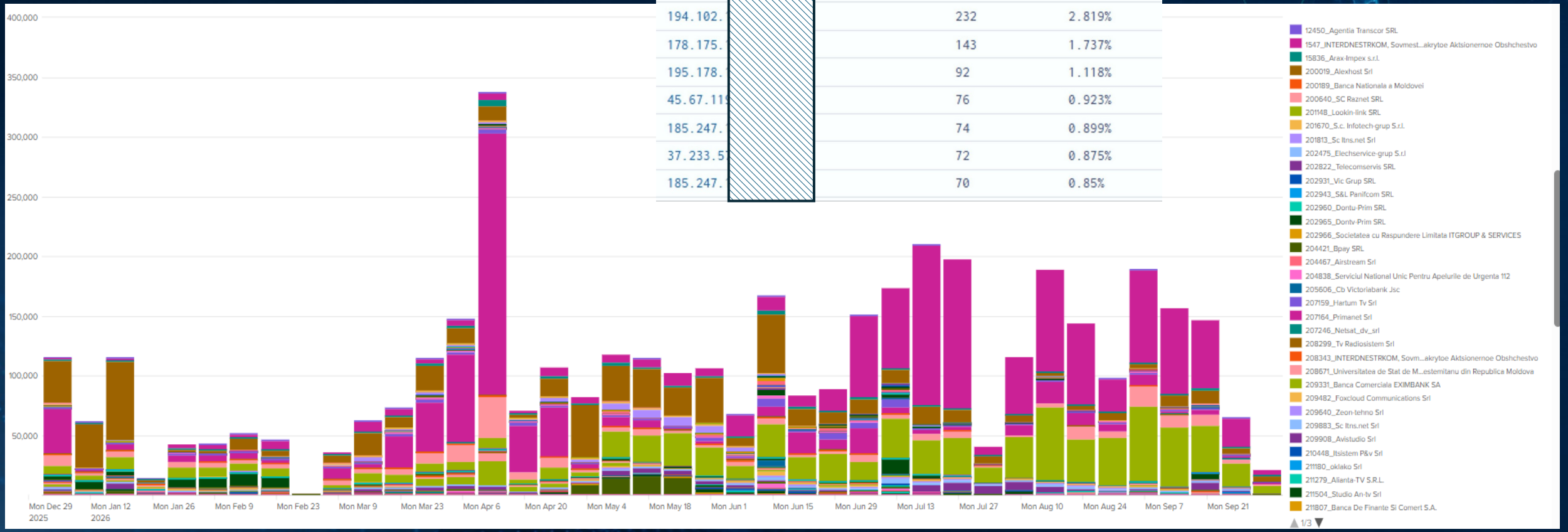
REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Relative DDoS participation by Autonomous System Source Year to Date

Viewpoint: Tier-1 operator observation



Top 10 Values	Count	%
93.116.3	343	4.167%
176.123.9	302	3.669%
217.156.1	263	3.195%
194.102.1	232	2.819%
178.175.1	143	1.737%
195.178.1	92	1.118%
45.67.119	76	0.923%
185.247.1	74	0.899%
37.233.51	72	0.875%
185.247.1	70	0.85%



93.116.

Regular View | Raw Data | Timeline | Whois

General Information

Hostnames	host-static-93-116-33-158.moldtelecom.md
Domains	moldtelecom.md
Country	Moldova, Republic of
City	Chisinau
Organization	JSC "Moldtelecom" S.A.
ISP	Moldtelecom SA
ASN	AS8926

Open Ports

83 554

// 83 / TCP

Hikvision IP Camera

<empty title>

```
HTTP/1.1 200 OK
Date: Tue, 29 Sep 2026 23:25:58 GMT
Server: webserver
X-Frame-Options: SAMEORIGIN
```

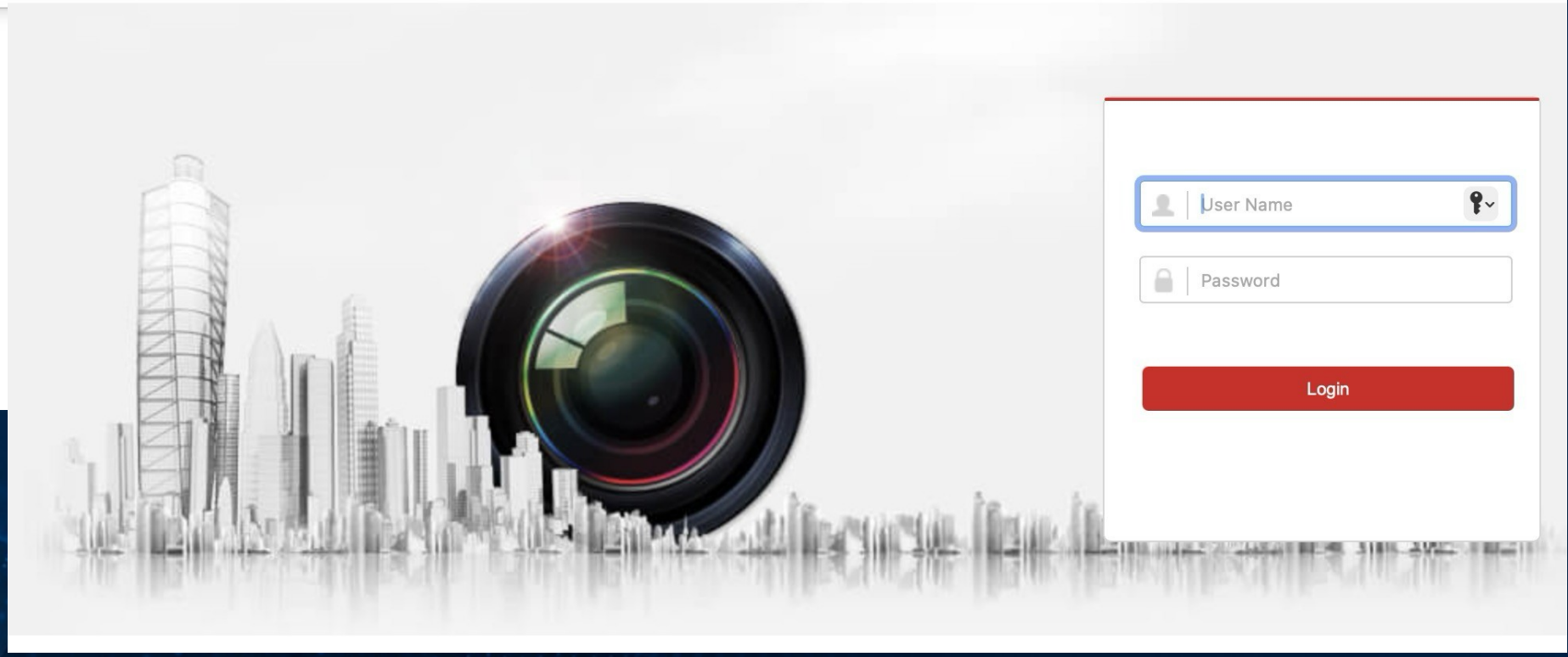
REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.





HIKVISION®

English



User Name

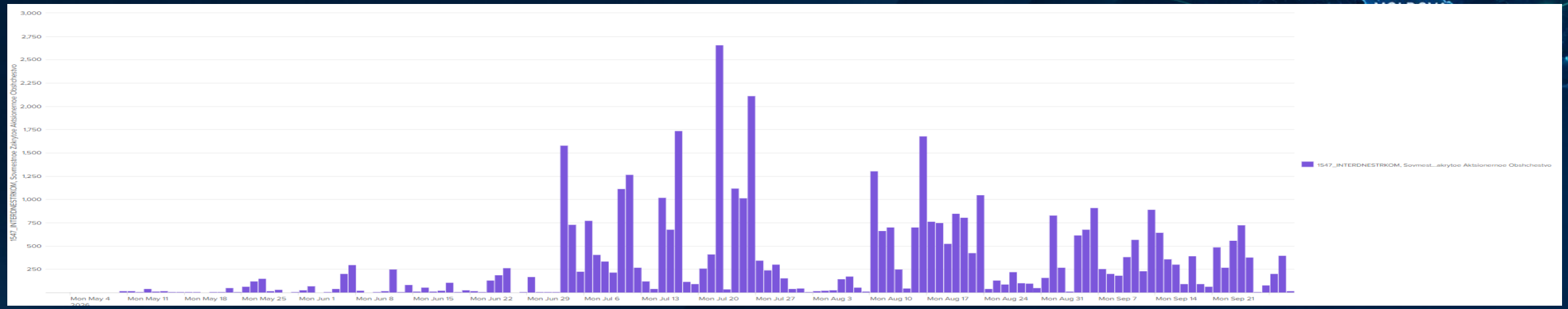
Password

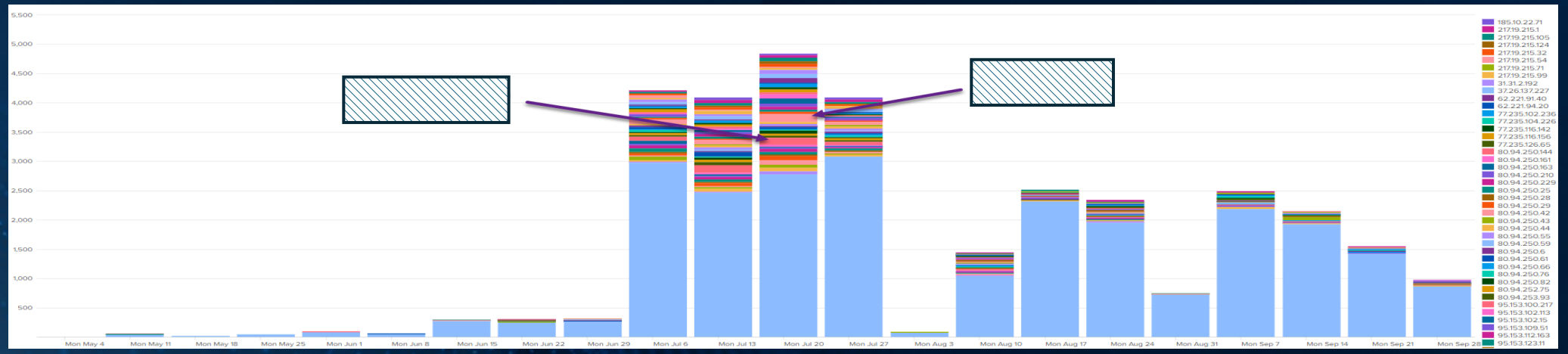
Login

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Top ASN Trending Botnet Activity

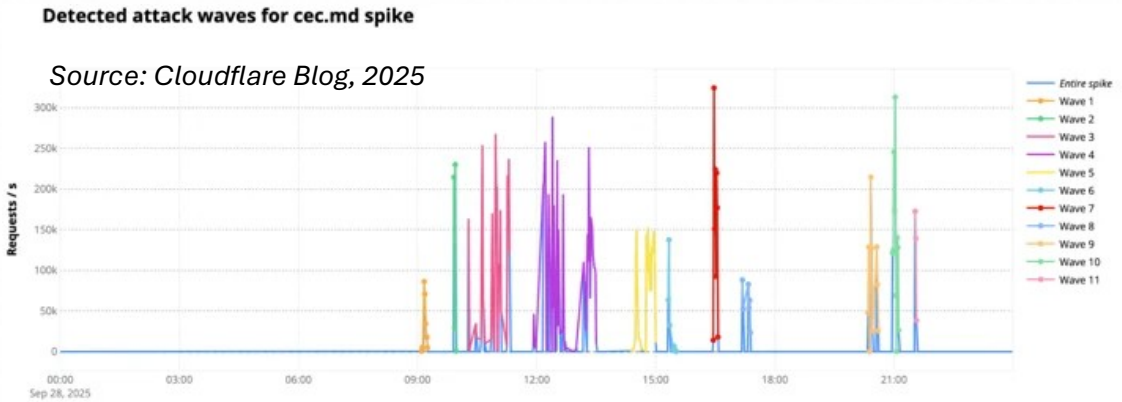




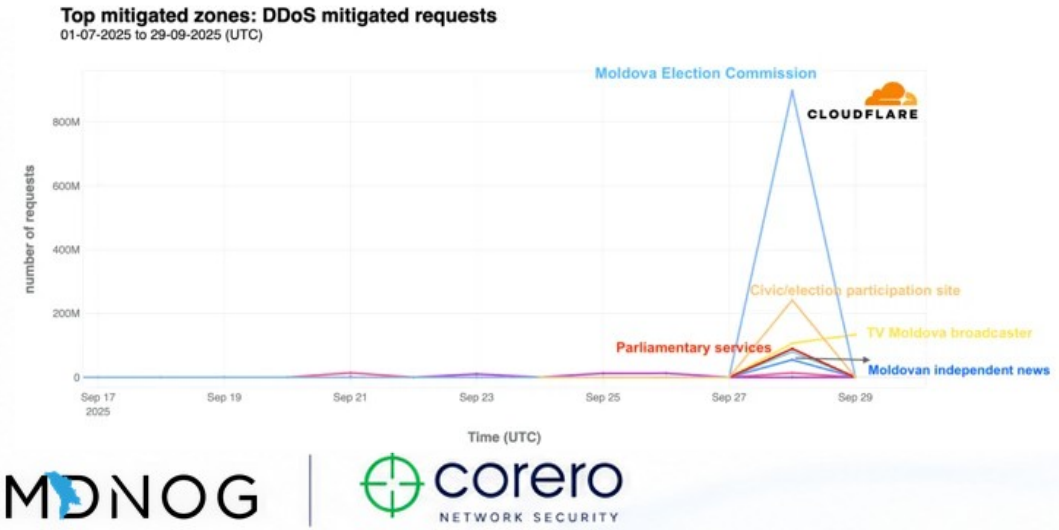
A Resilient Network Success Story? 2025

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

"...over 898 million malicious requests directed at the CEC over the twelve-hour period."



Source: Cloudflare Blog, 2025





Source: STISC, IT and Cyber Security Service



- "*designed to imitate legitimate traffic and bypass protection systems*"
- STISC blocked (TLD) host.md, restricting approximately 4000 websites
- Collateral damage
- **How do we preserve critical services while keeping the impact on unrelated services as small as possible?**

MDNOG | corero NETWORK SECURITY

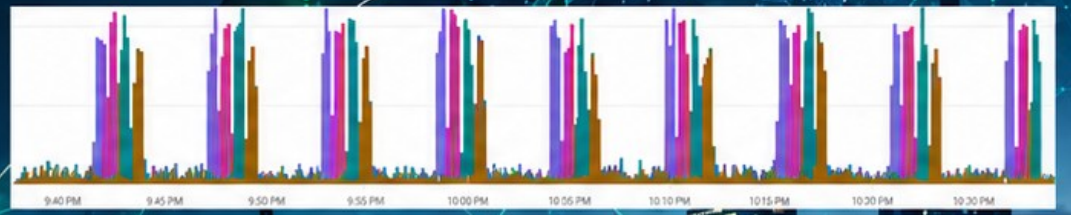
MDNOG | corero NETWORK SECURITY

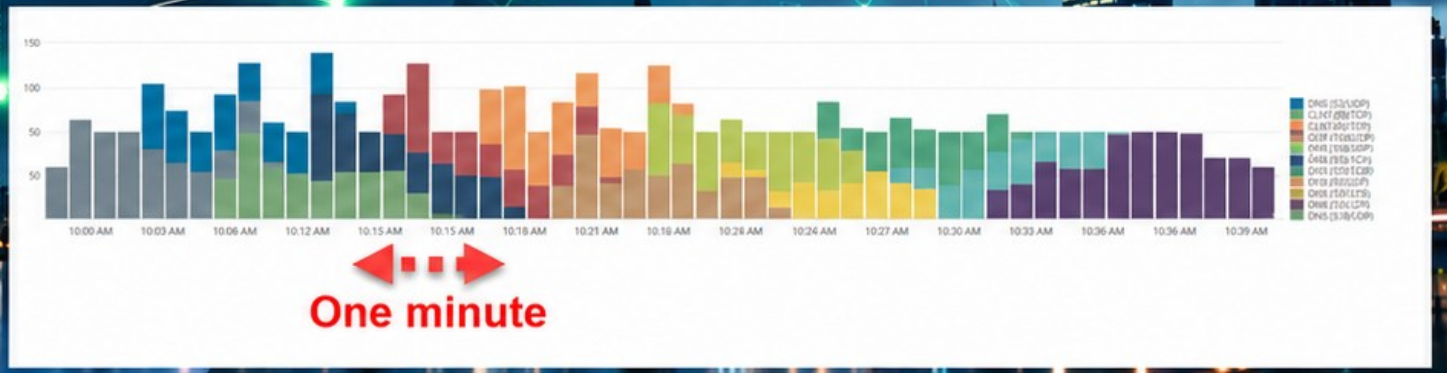
REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Botnets have changed the Economics of DDoS

What actually makes a 500,000 - device botnet difficult to defend against?







TOGETHER FOR A MORE
SECURE TOMORROW

Why MERIS and Masjesu Are So Difficult to Mitigate

MODERN BOTNETS. MASSIVE SCALE. EVASIVE TECHNIQUES.. CONSTANT EVOLUTION.

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

MERIS

LARGE-SCALE DDoS BOTNET

1. Built from compromised MikroTik RouterOS devices / professional networking equipment.
2. Delivers extreme requests-per-second, overwhelming CPU and memory, not just bandwidth.
3. Hard to mitigate because defenders cannot rely on third parties to patch devices and change passwords.

Masjesu

DDoS-FOR-HIRE BOTNET

1. Independently developed DDoS-for-hire botnet promoted on Telegram.
2. Supports attacks up to **300 Gbps or 200 million PPS.**
3. Multi-vector across L3/L4/L7 with methods including UDP, TCP SYN, TCP ACK/ACK-PSH, HTTP, ICMP, GRE, RDP, OSPF and others.
4. Randomizes payloads / ports / lengths, can spoof IPs in TCP SYN, and HTTP flood can mimic browser-like traffic.

Why they are difficult to mitigate

SCALE. DIVERSITY. EVASION.

Scale
Very high RPS/PPS/Gbps.

Multi-vector behaviour
Attacks switch methods rapidly.

Randomization and spoofing
Weakens static signatures.

Legitimate-looking traffic
Some activity resembles normal application behaviour.

Speed
Human-in-the-loop mitigation is often too slow.

Effective defence requires **deep visibility**, **real-time detection** and **automated enforcement.**

Amplification vs Botnet DDoS

DIFFERENT METHODS. DIFFERENT STRENGTHS. DIFFERENT CHALLENGES.

MDNOG | corero [NETWORK SECURITY]

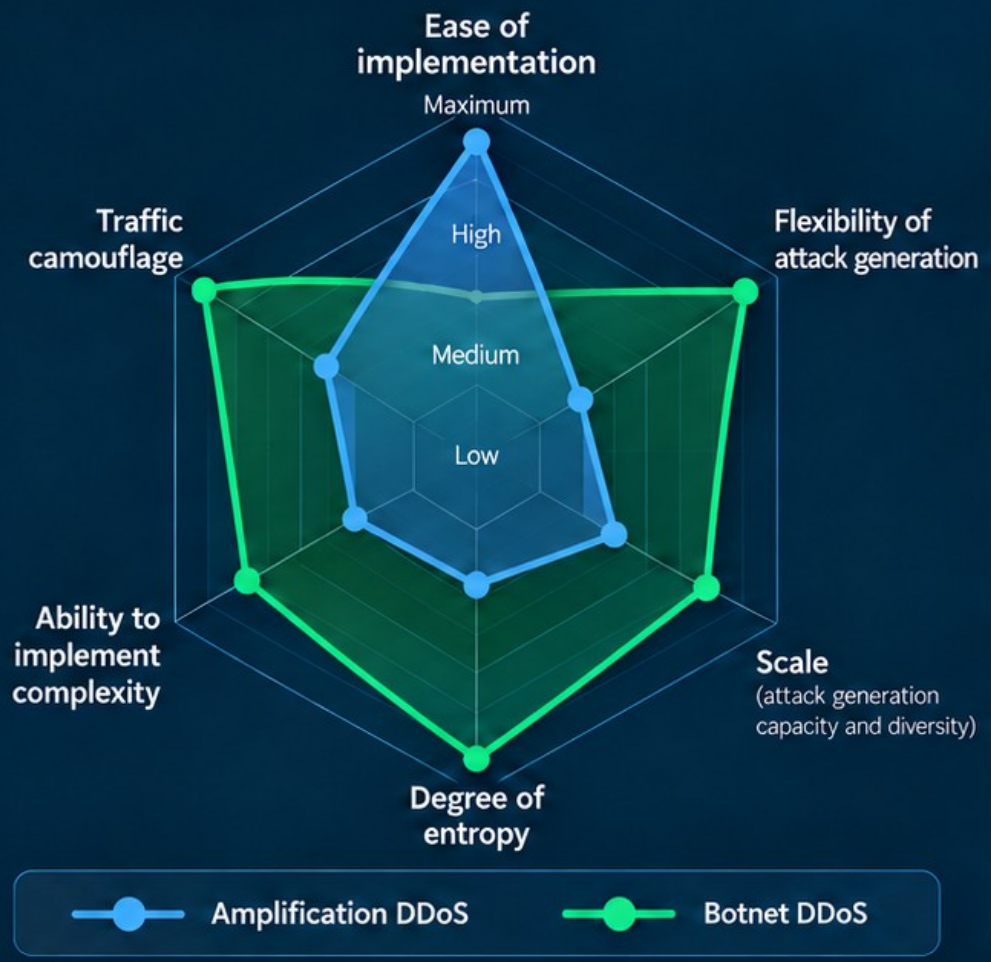
REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Amplification DDoS

Reflection-based attack traffic

Attackers send spoofed requests to third-party servers (e.g. DNS, NTP, SSDP). The servers respond to the victim, amplifying the traffic volume by a significant factor.

- Uses legitimate protocols and open services
- Amplifies traffic volume using third-party infrastructure
- Relatively easy to implement using readily available tools and services



Botnet DDoS

Direct, malware-generated attack traffic

Compromised devices (servers, cloud instances, endpoints, IoT, etc.) run custom malware and receive instructions from a command and control infrastructure to generate attack traffic directly towards the target.

- Uses compromised compute across the internet
- Highly flexible – can generate many attack types and behaviours
- Capable of very large, complex and diverse attacks with high evasion potential

Ease of implementation
Amplification: High
Botnet: Medium

Flexibility of attack generation
Amplification: Low
Botnet: High

Scale
(attack generation capacity and diversity)
Amplification: Medium
Botnet: High

Degree of entropy
Amplification: Low
Botnet: Maximum

Ability to implement complexity
Amplification: Low
Botnet: Maximum

Traffic camouflage
Amplification: Low
Botnet: Maximum

Illustrative comparison of attacker capability based on common characteristics. Not a measured benchmark.

UNDERSTAND THREATS. BUILD STRONGER NETWORKS.

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Anatomy of an Attack, Real Investigation

Following the evidence from attack activity to operational insight.



TOGETHER FOR A MORE
SECURE TOMORROW

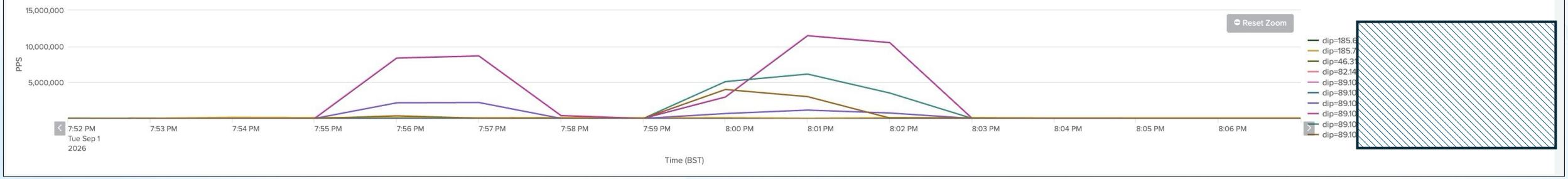
MDNOG | corero NETWORK SECURITY

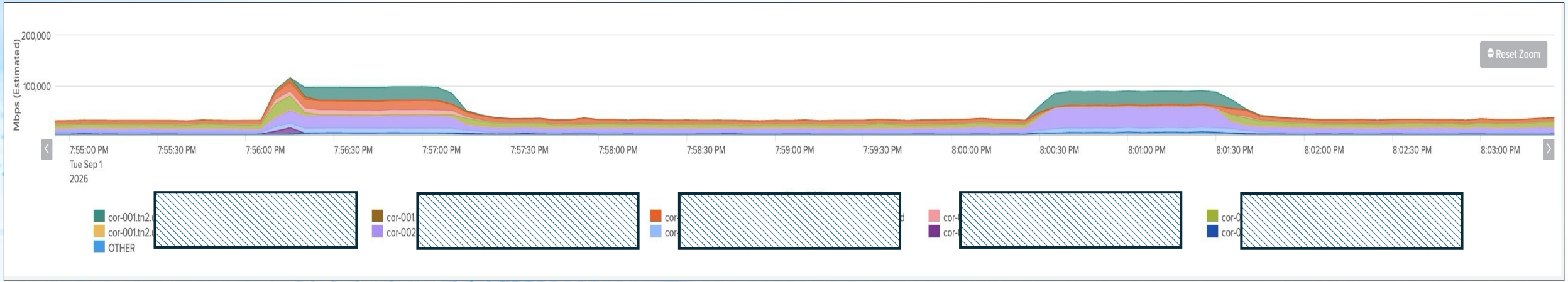
REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.

Aggregation: Total Reported Value

Number of Signatures: 10

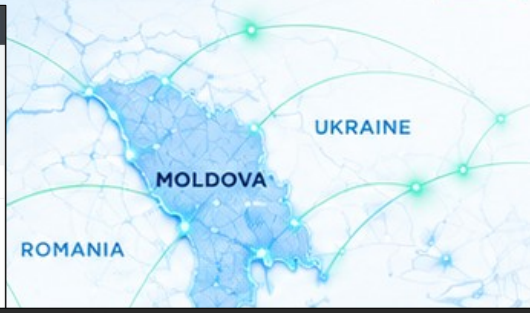
Smart-Rule Signatures by Max PPS > 0. Click on a signature to see detailed info.





MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.



Overview | Analytics | Search | Alerts | Dashboards | Reports | System | Help | support | corero

New Search

Save As | Close

```
index=* type=event dir=inbound rule="cns-002083"
```

Time range: during Tue, Sep 1, 2026

✓ 1,155 events (9/1/26 12:00:00.000 AM to 9/2/26 12:00:00.000 AM) No Event Sampling | Job | Smart Mode

Events (1,155) | Patterns | Statistics | Visualization

Timeline format | − Zoom Out | + Zoom to Selection | × Deselect | 1 hour per column

Format | Show: 20 Per Page | View: List | Prev 1 2 3 4 5 6 7 8 … Next

Hide Fields | All Fields

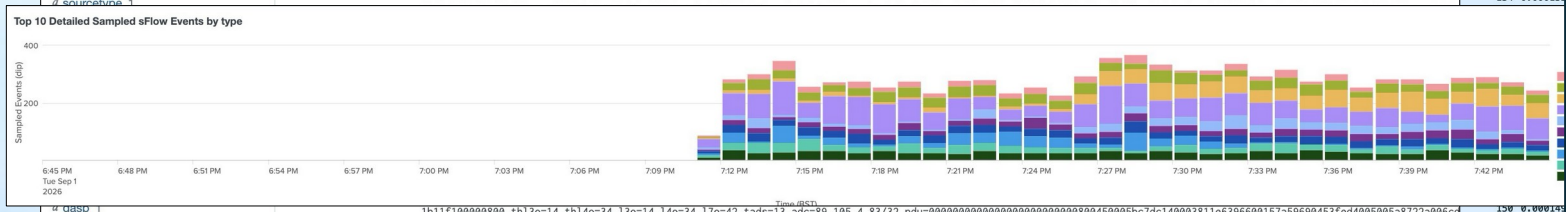
Time	Event
9/1/26 8:02:34.239 PM	Sep 1 20:02:34 127.0.0.1 2026-09-01T20:02:34.23957714+01:00 172.27.16.10 cat=security,type=event,v=1,dpm=detection,cl=detection,device=ntd-ngd-001,mm=0,profile=default,aip=5.4.83,dprt=80,ttl=48,dir=inbound,mp=xe-1/1,act=trigger,dm=detect,px=1,pxt=0,pxqd=2,lb=0,rule=cns-002083,pr=64600,br=696,time=1788290314464,ist=gre,isa=172.27.10.22,flen=269, ac1b11f100000800,thl3o=14,thl4o=34,l3o=14,l4o=34,l7o=42,tads=13,adc=89.105.4.83/32,pdu=0000000000000000000000000800450005894173400030 11b30abf7133b9596904534c5d00500575b8ec1f7 a98929b09b9d559b6d2414e9bc238b4268c257b067921fd1e190551ef0174a2d1b8183944f284255d1c73384167edf4b6525a8be981e6ef6d74b8c3811a994d75ff76ba0b320e71022995eb8a3d3870c6685caf7107bd2

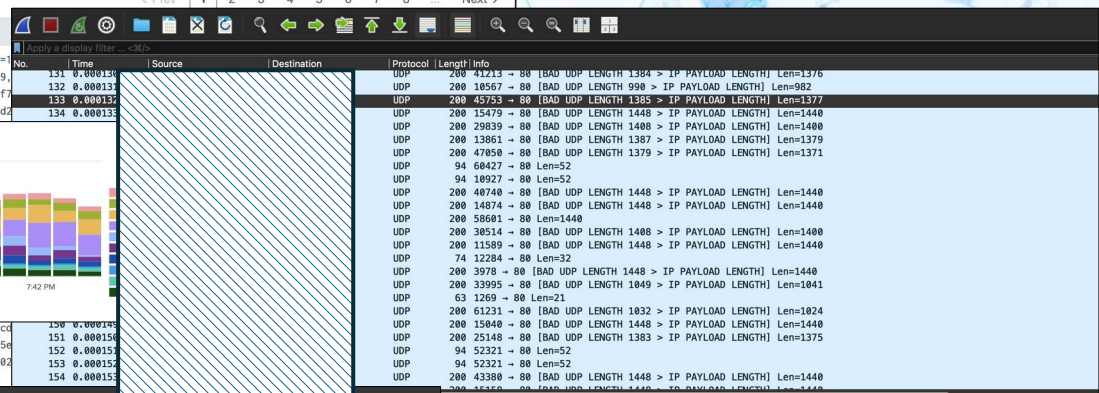
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

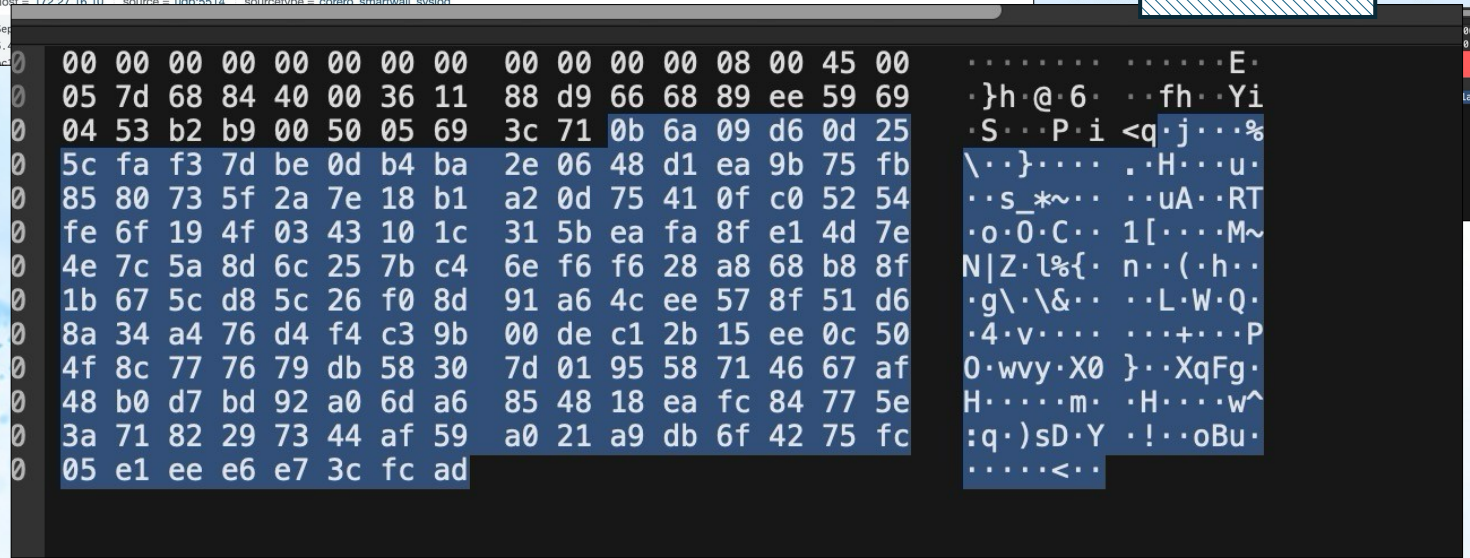
INTERESTING FIELDS
- # dasp 1
- # date_hour 2
- # date_mday 1
- # date_minute 6
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1

9/1/26 8:02:34.239 PM	1b11f100000800,thl3o=14,thl4o=34,l3o=14,l4o=34,l7o=42,tads=13,adc=89.105.4.83/32,pdu=0000000000000000000000000800450005bc7dc140003811e6396600157a59690453fed4005005a8722a006cd 74044805e69bec44a5643bf012b3676f963f03ec5dafaeb002453f1ae71a3b3b1d8d632b2a01debbcceb75bda7ff54e5e42978c889c56d48ea4e491a8006a2f194167734 67dc9e228ac4dab08e8f4d76fd20252e89e1e5e 9.105.4.83,scl=0, ddasn=59395,service-level=None,asset-name=None,sci=KE,dci=GB,sasn=36926,asset=None,sasp=102 host = 172.27.16.10 source = udp:5514 sourcetype = corero_smartwall_syslog
9/1/26 8:02:34.239 PM	Sep

Top 10 Detailed Sampled sFlow Events by type







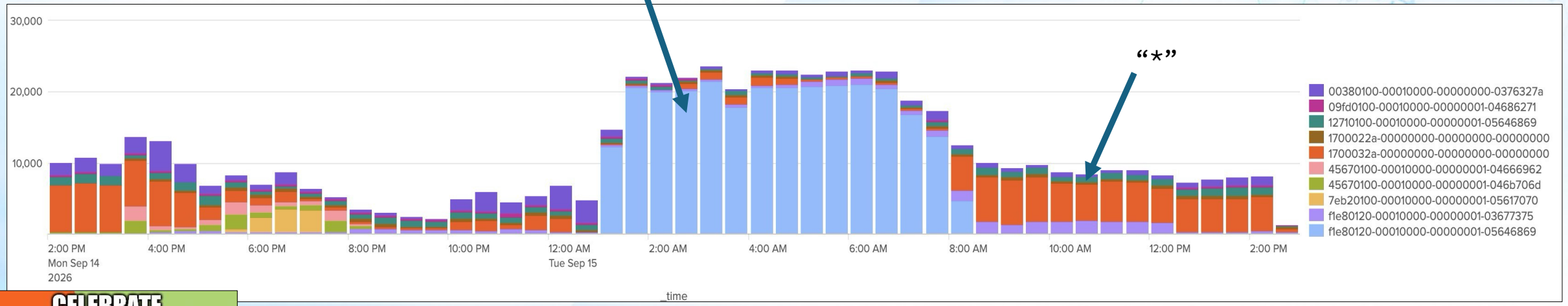
MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.



“ñè dhi”

“*”

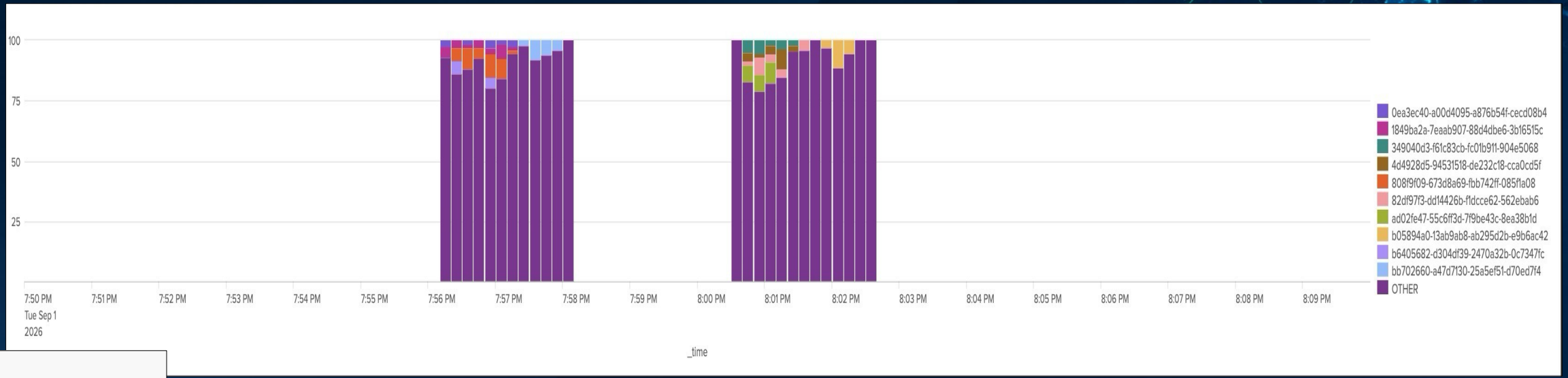


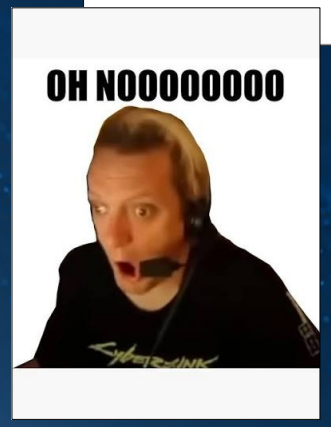


MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.







MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.



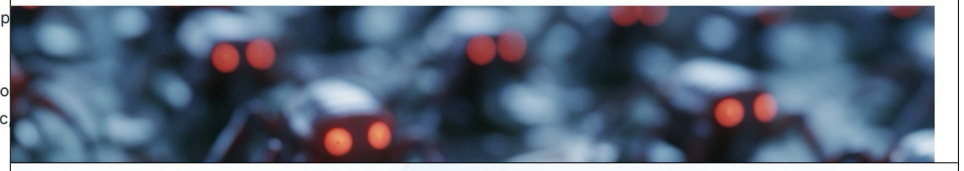
corero [NETWORK SECURITY]

Error fetching data.

PRODUCTS SOLUTIONS SERVICES RESOURCES PARTNERS INVESTORS ABOUT SUPPORT

Masjesu Botnet Reveals a Shift in DDoS Attack Strategy

April 15, 2025 | Huy Nguyen



UDP Flood Method

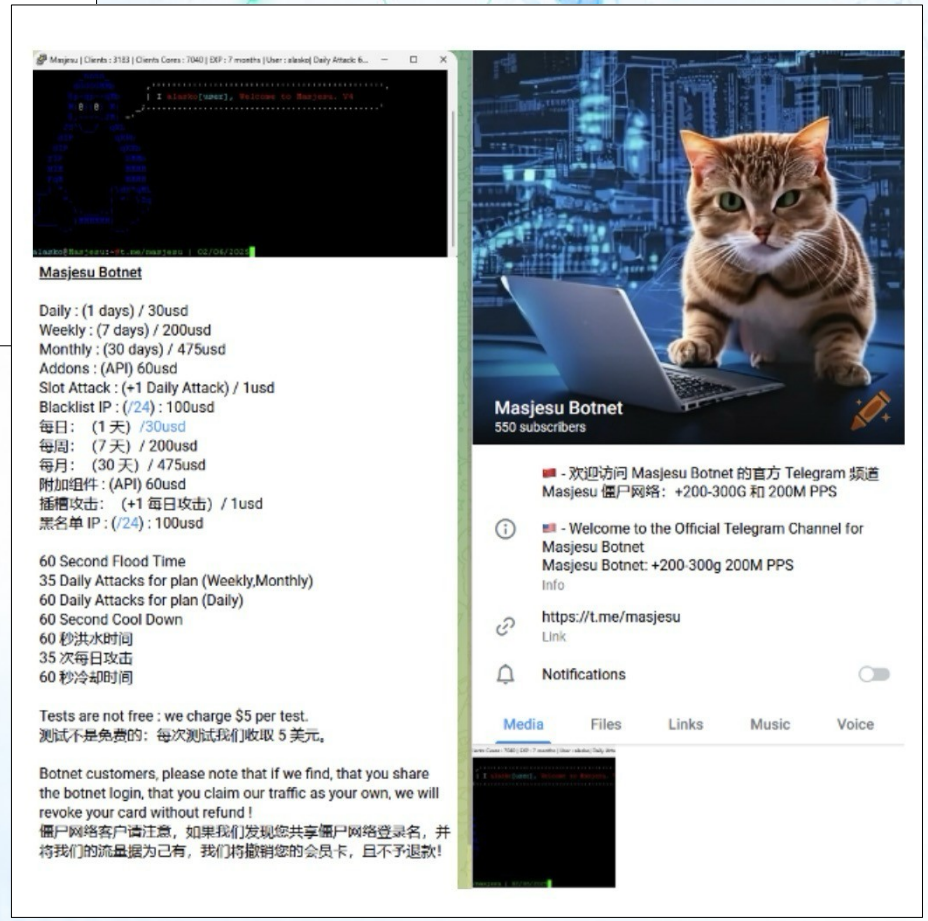
In this flood attack method, the random number generator is initialized using srand(timestamp. The rand() function is then utilized to generate randomized values for p lengths.

At address 0x0804a9ea, the function calls rand() to determine the size of 64 paylo randomly generated bytes. This approach introduces variability in the attack traffic using signature-based defenses.



How to Win:

- Trending Data sets clear.
- Visibility is not the same as cleaning accuracy.
- Reverse Engineering / Threat Research essential to identify botnet code base used.



Masjesu Botnet

Daily : (1 days) / 30usd
Weekly : (7 days) / 200usd
Monthly : (30 days) / 475usd
Addons : (API) 60usd
Slot Attack : (+1 Daily Attack) / 1usd
Blacklist IP : (/24) : 100usd
每日： （1 天） /30usd
每周： （7 天） / 200usd
每月： （30 天） / 475usd
附加组件 : (API) 60usd
插槽攻击： （+1 每日攻击） / 1usd
黑名单 IP : (/24) : 100usd

60 Second Flood Time
35 Daily Attacks for plan (Weekly,Monthly)
60 Daily Attacks for plan (Daily)
60 Second Cool Down
60 秒洪水时间
35 次每日攻击
60 秒冷却时间

Tests are not free : we charge $5 per test.
测试不是免费的：每次测试我们收取 5 美元。

Botnet customers, please note that if we find, that you share the botnet login, that you claim our traffic as your own, we will revoke your card without refund !
僵尸网络客户请注意，如果我们发现您共享僵尸网络登录名，并将我们的流量据为己有，我们将撤销您的会员卡，且不予退款！

MDNOG | corero NETWORK SECURITY

REAL THREATS.
REAL NETWORKS.
REAL OUTCOMES.



Thankyou!