



H1 2026

DNS THREAT INTELLIGENCE REPORT

DGA: The Overlooked Malware Indicator

A Malware-First Landscape, Signaled by DGA

WHAT H1 2026 DNS INTELLIGENCE REVEALED — AT A GLANCE

H1 2026 reveals a threat landscape defined by scale and a changing mix of activity. Malware nearly doubled and became the leading threat category. The surge was signaled in advance: DGA momentum strengthened in February, and newly observed domains accelerated alongside malicious activity through March and April, confirming infrastructure signals as strong early indicators.

Among DGA families, BaitHook and Phobia, tracked since 2025, persisted or returned, while TravelLog, DayDream and Unmasked surfaced as newly identified families, first observed in the wild during H1 2026. Phishing rotated sharply across sectors and brands, with Logistics & Couriers emerging as the half's biggest mover; delivery and courier lures now warrant particular caution.

KEY NUMBERS

TOTAL THREAT SIGNALS

+24%

Overall growth: from 11.2B to 13.9B hits

MALWARE

4th → **1st**
Place

×2.0

Nearly doubled to 3.9B hits, the new leading threat category

NEWLY OBSERVED DOMAINS

×2.0

Hits on domains first seen within a day (NOD_1d): 530,000,000 in H1 2026

PHISHING: LOGISTICS & COURIERS

7th → **3rd**
Place

×3.4

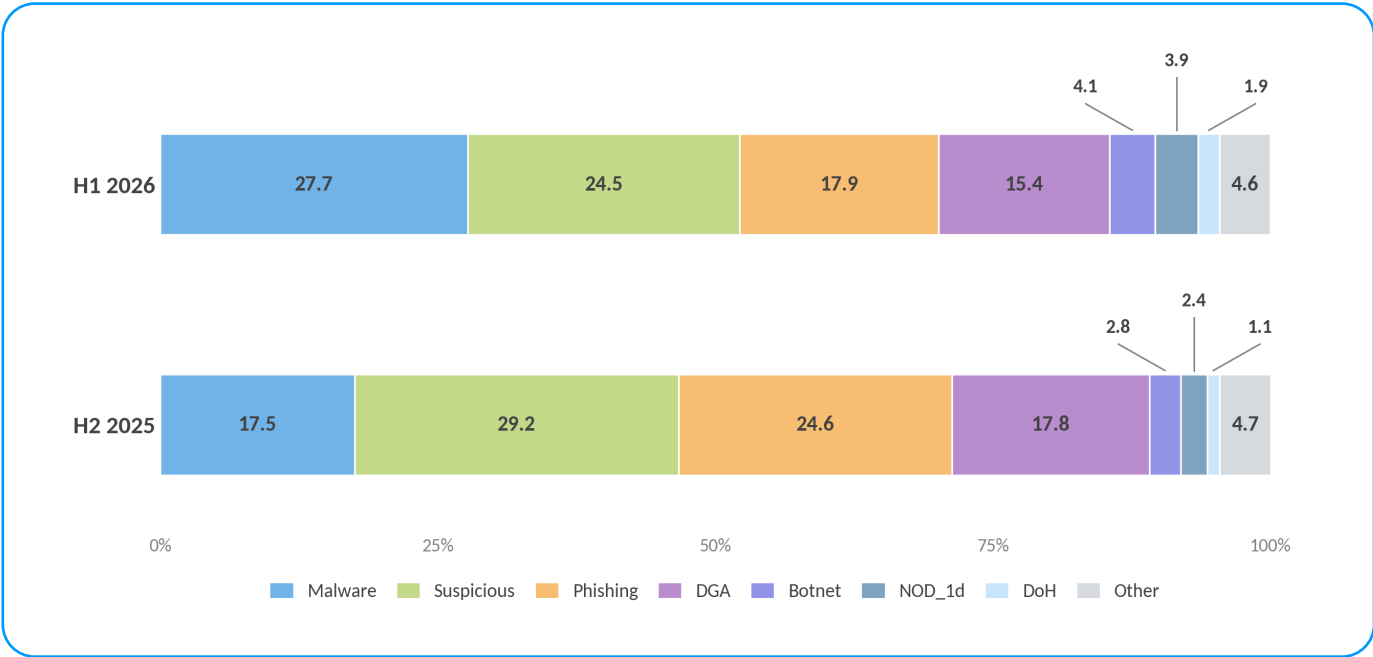
Logistics & Couriers share of detections: from 4.0% to 13.6%

ABOUT THE INTELLIGENCE Produced by EfficientIP's AI-driven DNS threat intelligence, analyzing linguistic, visual, behavioral and infrastructure signals together, based on 150B+ DNS transactions analyzed daily. Comparison period: H2 2025 vs H1 2026.

The Threat Hierarchy Has Been Reordered

From H2 2025 to H1 2026, total threat-signal volume increased 24%, from 11.18 billion to 13.85 billion hits. Malware nearly doubled to 3.84 billion hits, becoming the leading threat category. Domains first observed within the past day (NOD_1d) also nearly doubled to 0.53 billion hits. These domains can reveal emerging infrastructure before it develops an established reputation, giving defenders an earlier opportunity to investigate. DoH-related activity accounted for 0.26 billion hits as a new reporting category.

Share of total threat-signal volume (%): each bar represents 100%



Suspicious = potential threats that cannot yet be categorized · “Other” combines Abuse, Adware, Disinformation, Miner, Scam, Scanner, Spam and Tunneling.

The shift was already visible by H2 2025: Phishing represented 24.6% of threat-signal hits, compared with 30.4% in the full-year 2025 distribution, while Suspicious rose to 29.2% and became the largest category. In H1 2026, Malware moved into first place at 27.7%.

 **3.84B**

Malware hits: the new leader

 **0.53B**

NOD_1d hits: nearly doubled

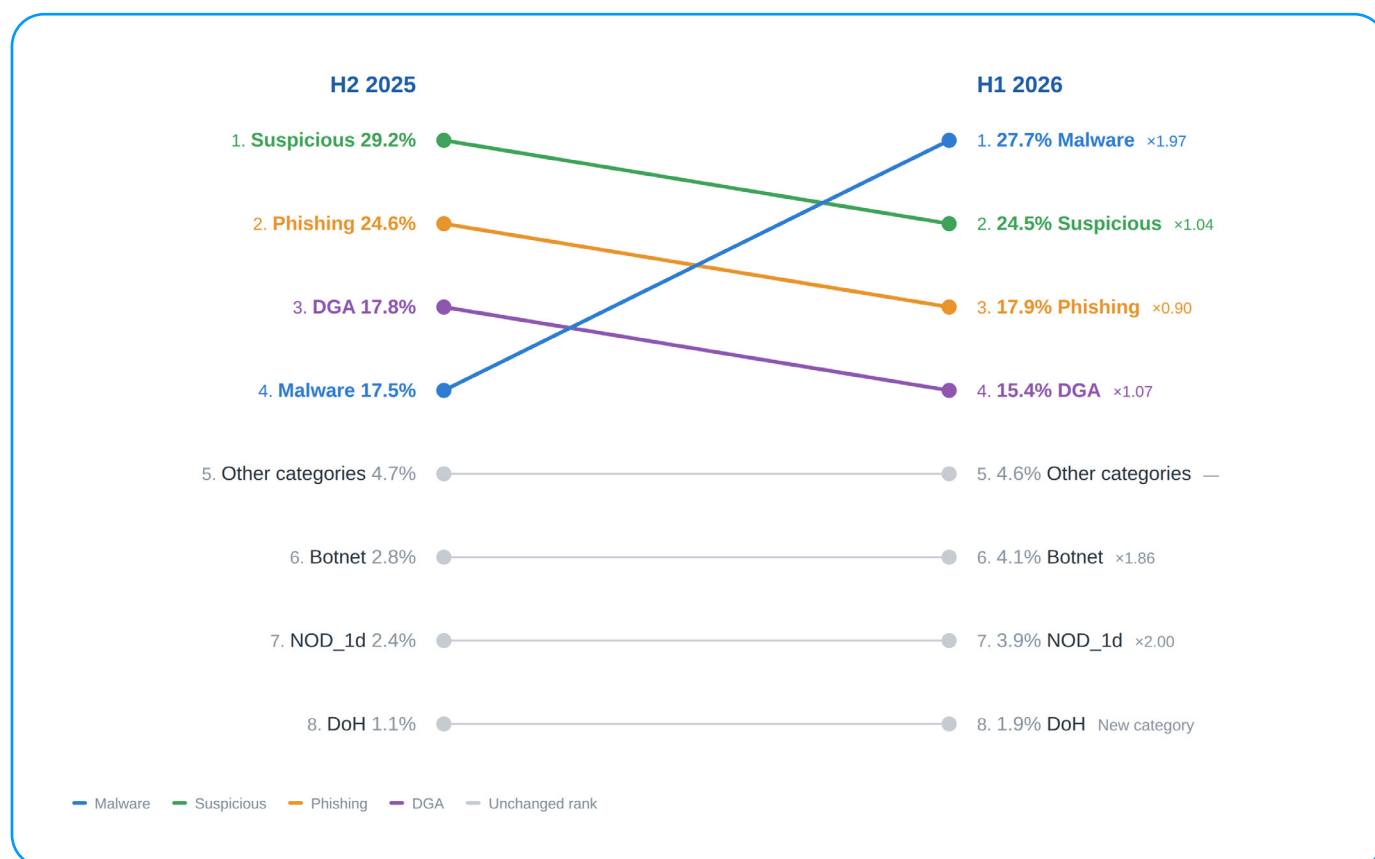
 **0.26B**

DoH-related activity:
new category

Threat Categories Are Moving at Different Speeds

Threat categories followed markedly different trajectories from H2 2025 to H1 2026. NOD_1d recorded the strongest comparable growth at $\times 2.00$, followed closely by Malware at $\times 1.97$ and Botnet at $\times 1.86$. DGA and Suspicious grew more modestly, while Phishing declined by 10%. DoH-related activity reached 0.26 billion hits but is presented without a growth comparison because it is a new reporting category.

CATEGORY RANKING: H2 2025 VS H1 2026 (SHARE OF THREAT SIGNALS, GROWTH MULTIPLE)



Outpacing overall growth

NOD_1d, Malware and Botnet grew substantially faster than the overall 23.9% increase in threat-signal volume.



Ranking reshuffled

Malware's growth changed the category ranking, moving it into first place in H1 2026.



Growing yet losing share

DGA and Suspicious increased in absolute volume but lost share because faster-growing categories expanded around them.



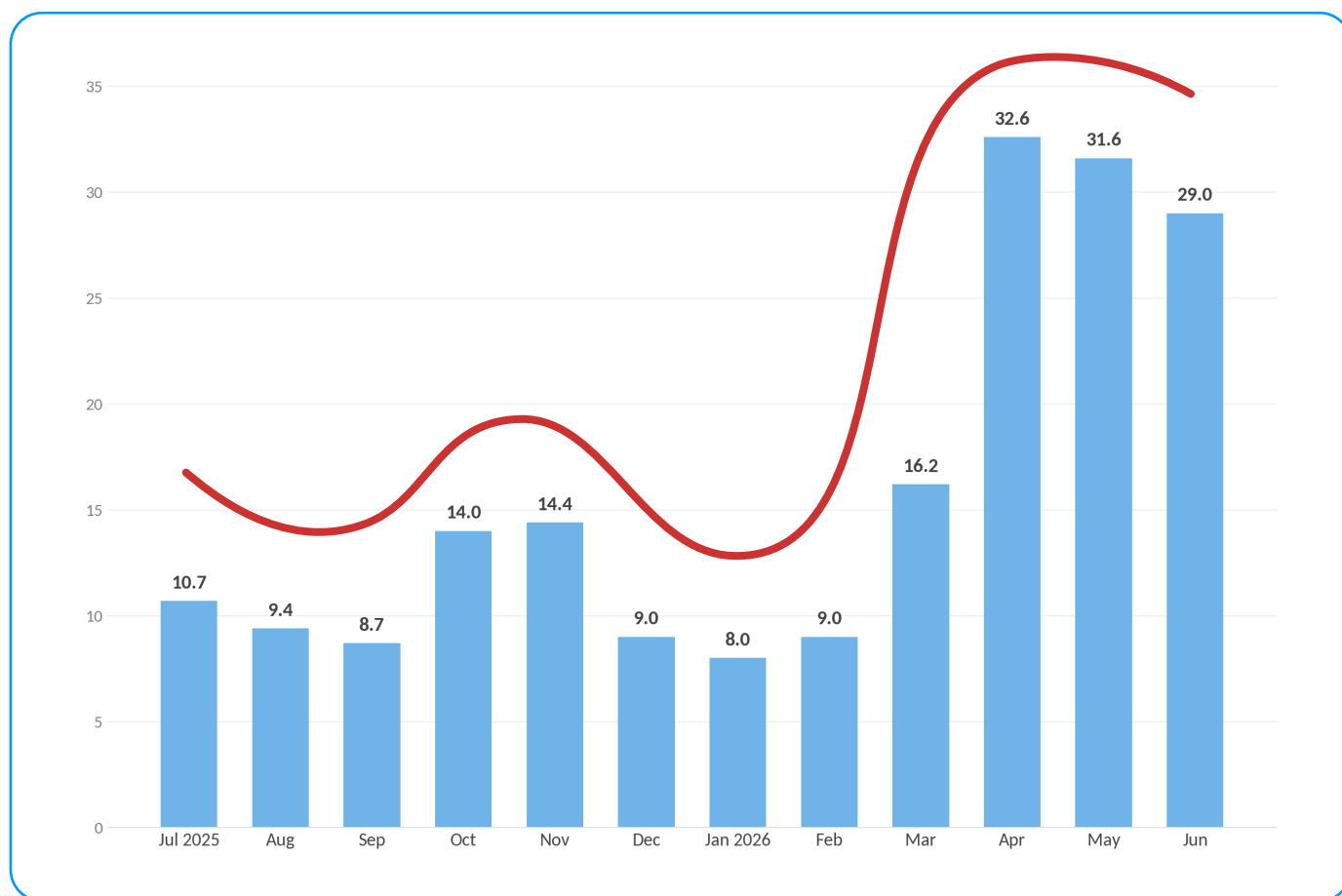
Phishing declined

Phishing remained significant at 2.48 billion hits despite declining in both volume and share.

Malware Is Escalating in Waves

Malware activity rose in distinct waves across H2 2025 and H1 2026. After reaching an H2 2025 high of 14.4 million hits per day in November, activity fell to 8.0 million in January before rising to 16.2 million in March and 32.6 million in April. It remained elevated at between 29 million and 32 million hits per day through June.

Malware activity by month: average daily hits (millions)

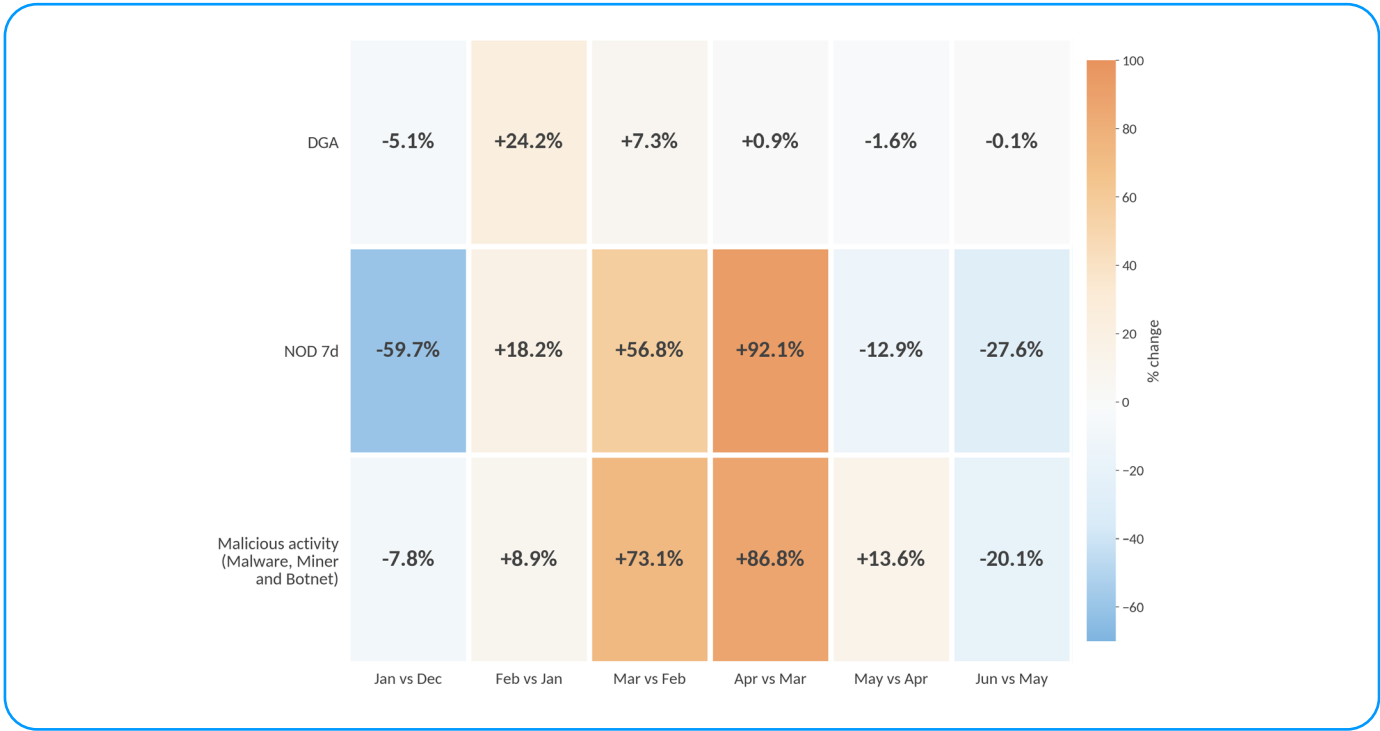


What this tells us: After declining across December and January, Malware activity began rising again in February and reached 16.2 million hits per day in March. The strongest increase occurred between March and April, when average daily activity doubled to 32.6 million hits. Malware remained above every H2 2025 monthly level from April through June, driving its rise to the leading threat category in H1 2026.

Infrastructure Activity Built Before the Malicious-Activity Surge

H1 2026 developed in a clear sequence: DGA momentum strengthened first, in February; malicious activity and domains newly observed during the preceding seven days (NOD 7d) then accelerated strongly through March and April. This progression shows how different DNS signals can illuminate different stages of threat activity.

Month-over-month change in average daily DNS hits January-June 2026



TWO SIGNALS, DIFFERENT QUESTIONS

DGA provides the earlier infrastructure view

Activity increased 24.2% in February, before the strongest rise in malicious activity, and then remained elevated as malicious activity accelerated sharply through March and April. This suggests infrastructure momentum was already building before the broader surge became visible.

NOD 7d provides a different view

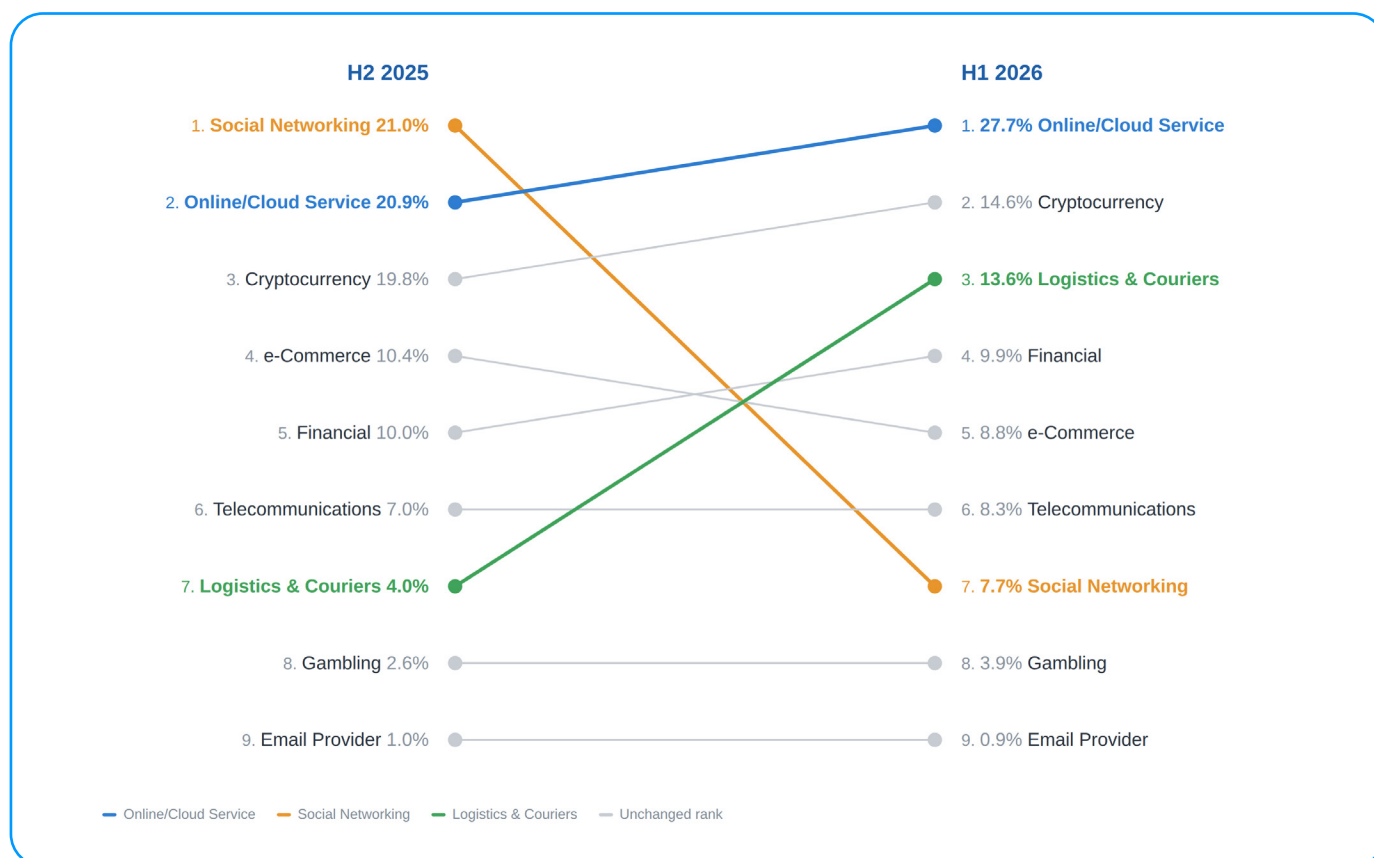
NOD 7d moved closely with malicious activity, rising 56.8% in March and 92.1% in April, while malicious activity increased 73.1% and 86.8% in the same months. Both signals then declined toward the end of the half.

Taken together, the two signals provide complementary context: DGA highlights infrastructure activity building earlier, while NOD 7d closely reflects the rise and decline of active malicious activity, giving a clearer view of how threats develop over time.

Phishing Focus Rotated Across Sectors and Brands

Phishing attention shifted noticeably in H1 2026. Online and cloud services regained the lead after being overtaken by Social Networking in H2 2025, while Logistics & Couriers emerged as a much stronger target area. At the same time, Social Networking fell back as Telegram-related activity declined. The pattern shows how quickly phishing priorities can change, with a small number of active campaigns reshaping the sector landscape.

SECTOR RANKINGS: H2 2025 VS H1 2026 (SHARE OF DETECTIONS)



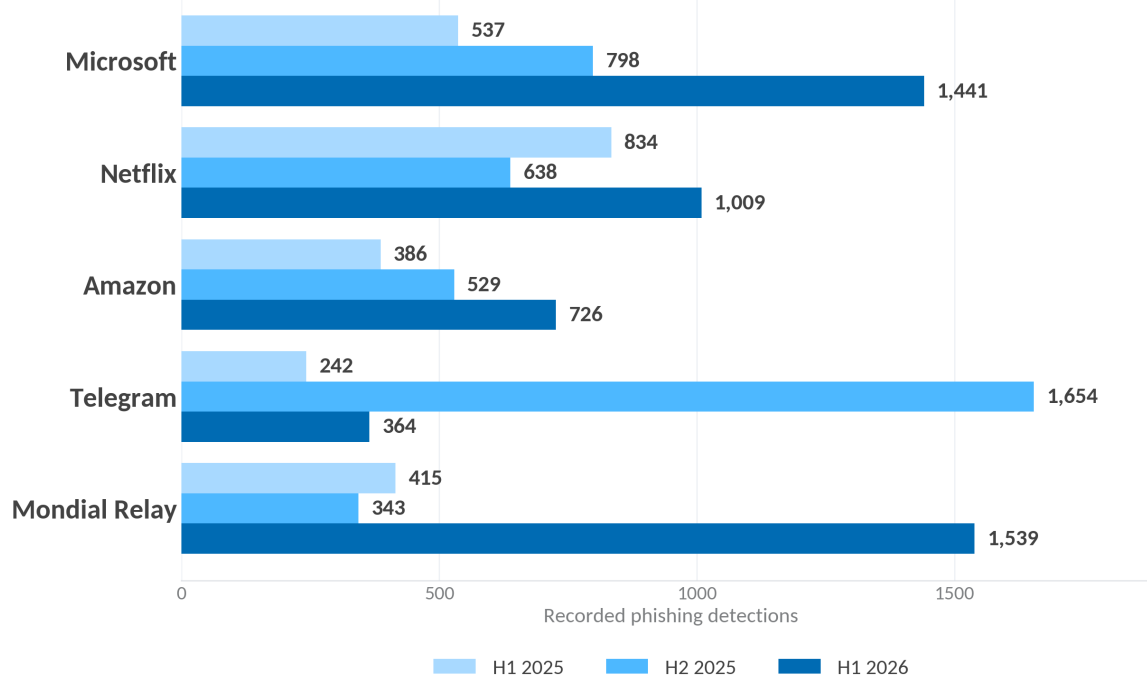
ONLINE AND CLOUD SERVICES RECLAIMED THE LEAD

Online and cloud services had led in H1 2025, then slipped behind Social Networking in H2. In H1 2026, they returned to first place with 27.7% of detections.

The biggest movement came from Logistics & Couriers, which rose from 4.0% to 13.6% between H2 2025 and H1 2026. Social Networking moved sharply in the opposite direction, falling from 21.1% to 7.7%. Cryptocurrency also declined, while Financial remained relatively stable.

Looking at sector trends together with brand-level activity helps distinguish persistent targeting from temporary spikes.

A Few Brands Drove Much of the Change



Telegram fell back

Activity fell sharply after its H2 2025 spike, helping explain the decline in Social Networking.



Mondial Relay surged in late June

A phishing campaign emerging in the final days of June drove much of the rise in Logistics & Couriers.



Microsoft, Netflix & Amazon climbed

All saw higher activity in H1 2026, reinforcing the continued prominence of online and cloud services as phishing targets.

DETECTION COVERAGE EXPANDED

New detection techniques introduced during H1 2026 broadened visibility into cryptocurrency landing pages, delivery and banking lures, and suspicious CAPTCHA entry points. This provides a wider view of phishing beyond known brand impersonation and helps reveal additional ways campaigns are designed and delivered.

What this means: phishing patterns can change quickly, and major shifts are often driven by a small number of active campaigns.

Known DGA Families Evolve as New Patterns Emerge

DGA activity does not follow a single pattern. H1 2026 revealed persistent infrastructure, sharp changes in observed activity, concentrated domain-registration bursts and continued queries to expired domains. Detecting these behaviors requires combining DNS activity with domain-generation patterns, registration data and infrastructure history. Five family stories from H1 2026 follow.

WHAT THIS MEANS



Established families persist or return

They can remain persistent, decline sharply or return after periods of lower visibility (BaitHook, Phobia).



New families move fast

They can move rapidly from initial observation to meaningful activity (TravelLog, Unmasked).



Generation runs ahead of registration

Generated domains may be observed before only a small subset is registered or activated (DayDream).



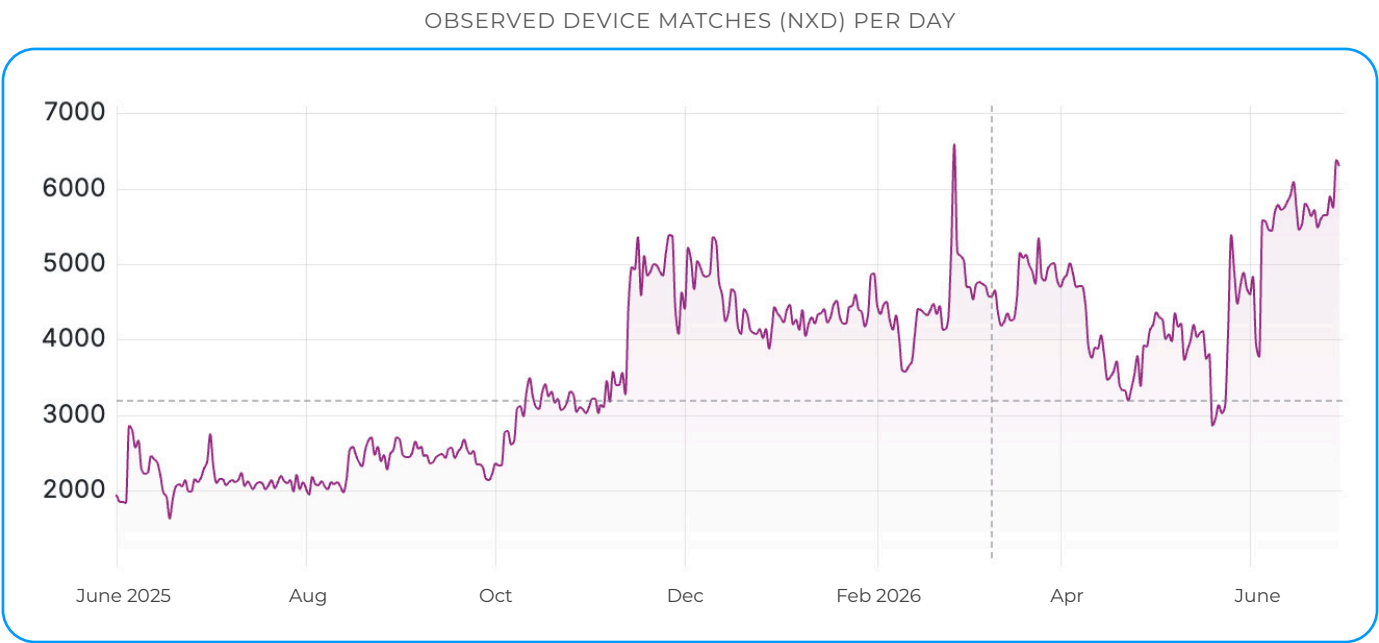
Registration arrives in short bursts

Registration activity can be concentrated into short, registrar-specific batches (TravelLog, DayDream).

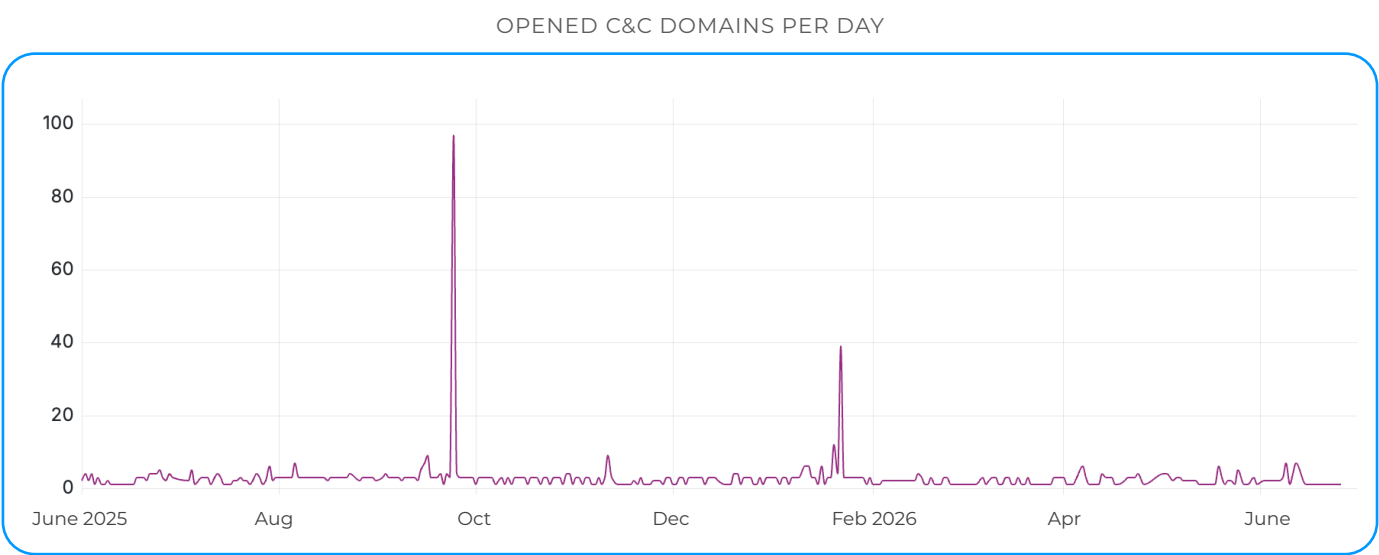
Device matches, opened C&C domains, WHOIS records and domain-generation patterns provide different views of DGA activity: analyze them together, without assuming that changes in one directly cause changes in another.

BaitHook: Persistent Activity and Infrastructure Reuse

BaitHook, introduced in the 2025 report, remained consistently active throughout H1 2026. It averaged approximately 4,500 observed device matches per day across the half-year, rising to approximately 5,500 per day in June.

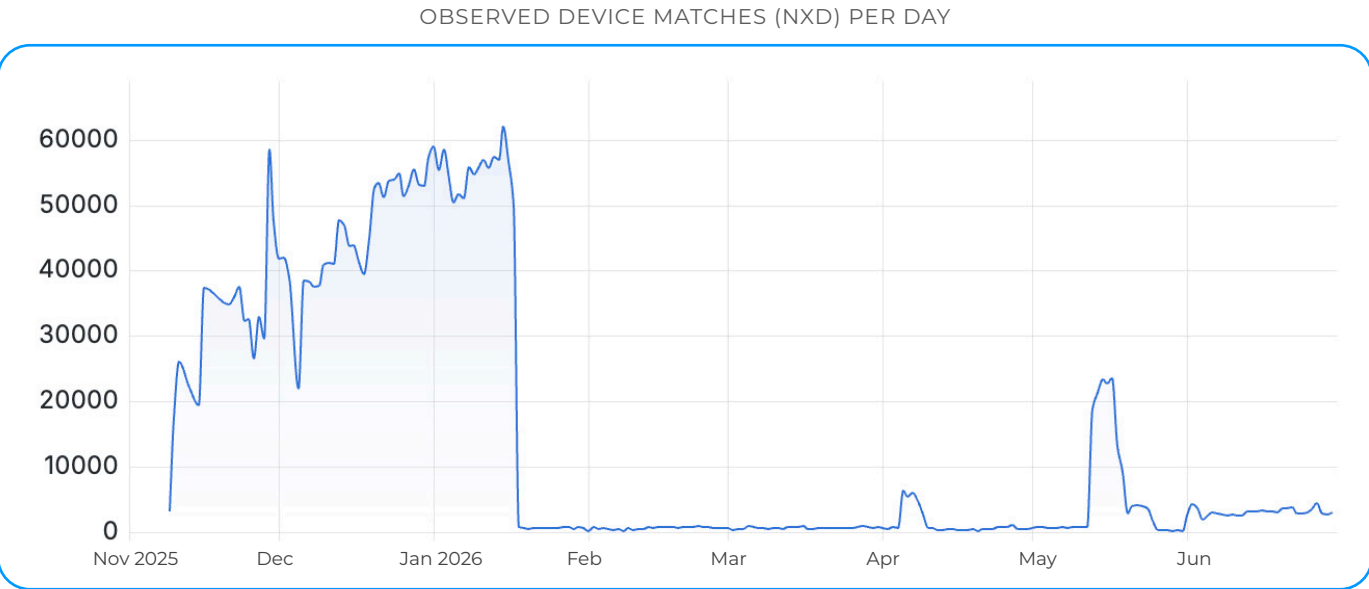


The opened C&C data recorded 335 BaitHook domains across 124 days during H1 2026. Activity generally appeared as small, recurring daily counts rather than a few dominant bursts. Research also found that many associated IP addresses had previously been observed, indicating continued infrastructure reuse.

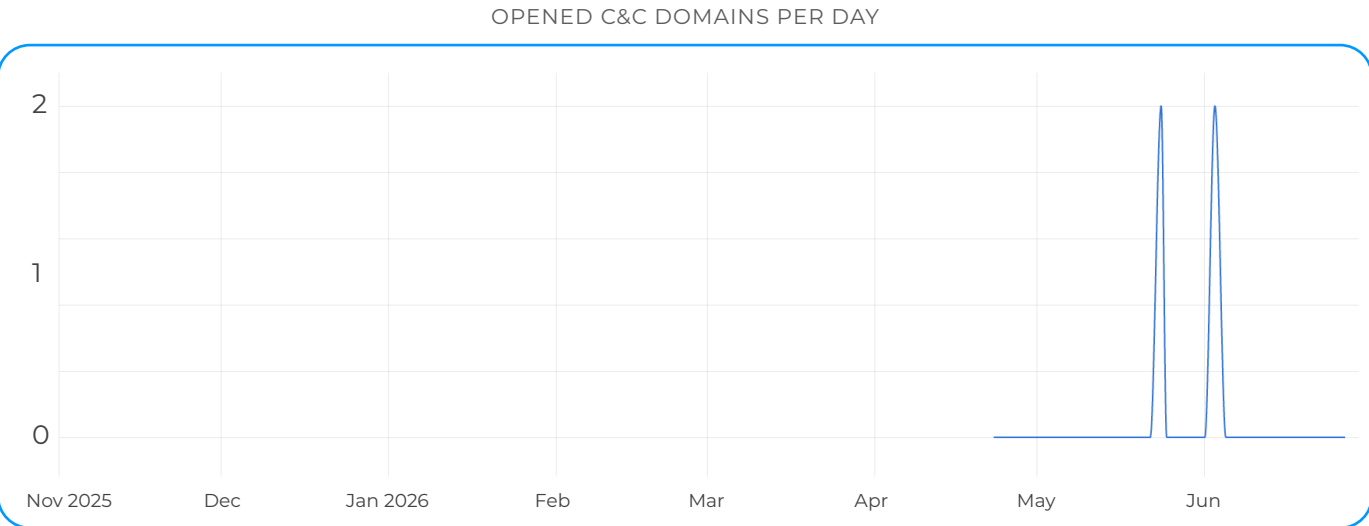


Phobia: Surge, Decline and Return

Phobia's late-2025 expansion, first discussed in the 2025 report, continued into January 2026. Observed device matches reached approximately 62,000 on January 15 before falling to approximately 600–700 per day from January 18.

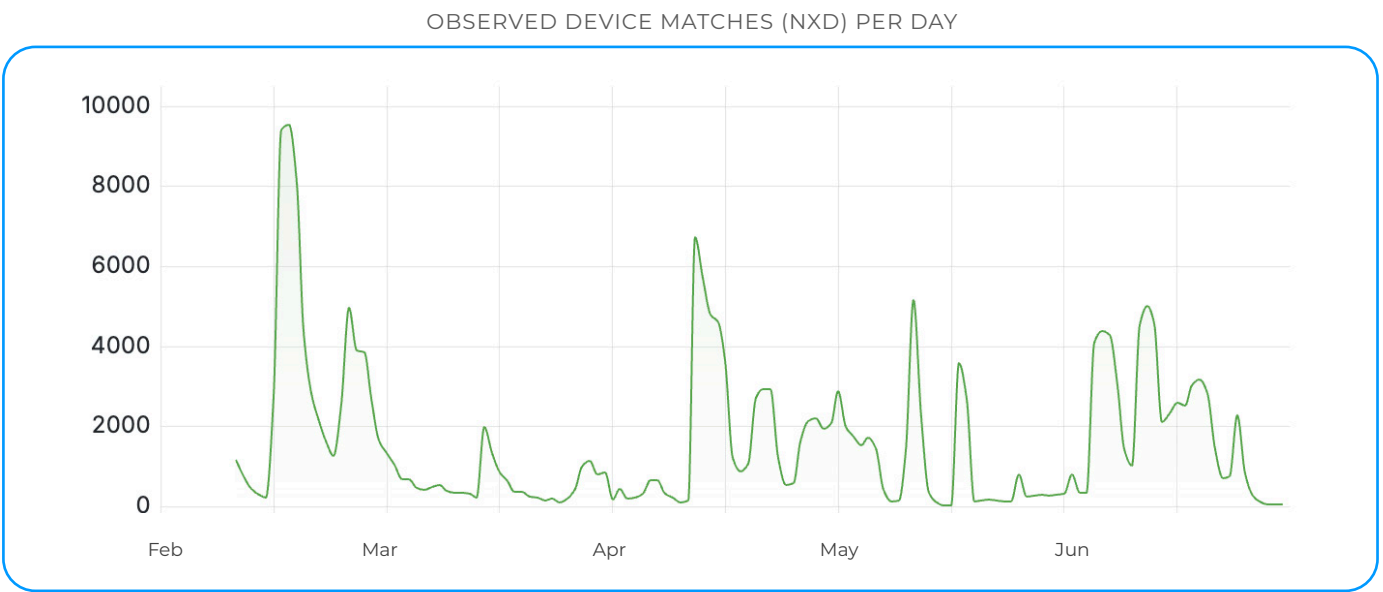


The family did not disappear. Activity returned at lower levels in April, reaching approximately 6,000 observed matches, and rose again to approximately 25,000 during May. This pattern shows that a sharp decline in daily observations does not necessarily mark the end of a DGA family's activity.

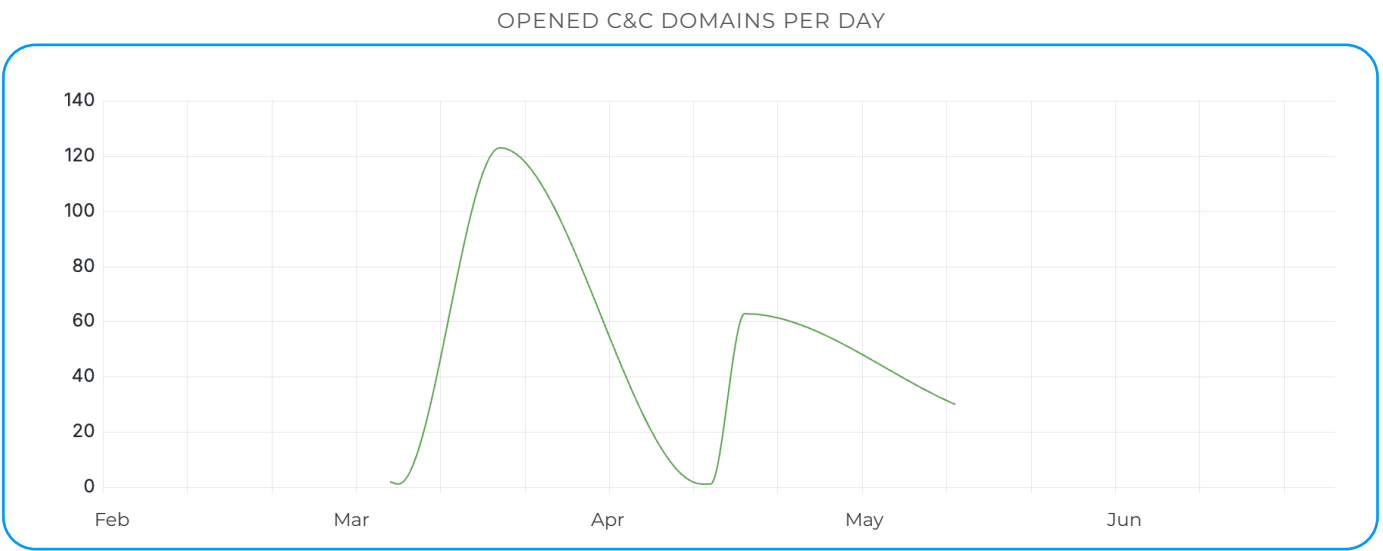


TravelLog: Registration in Concentrated Batches

TravelLog was first identified through approximately 1,500 suspicious domains in late January and February 2026 and was added to the threat intelligence platform on February 17. Its 15-character alphanumeric .xyz domains recur in monthly clusters of approximately 500, suggesting a monthly rotating generation pattern. The graph shows observed device matches rising sharply in February and peaking at 9,527 on February 18, followed by recurring, smaller waves of activity through June.



Registration activity appeared in smaller, concentrated batches: three matching domains on March 7–8, 123 through Aceville on March 20, 63 split between Nicenic and NameCheap on April 18, and 30 through Gname on May 14.

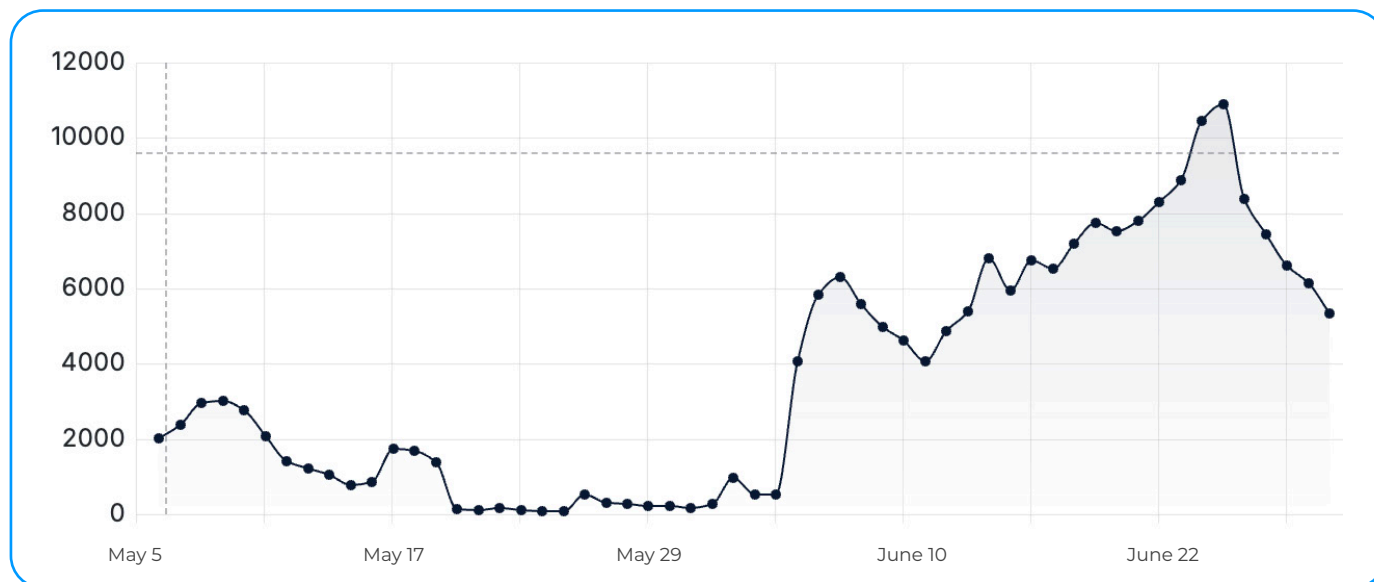


Together, the findings show how domains can be identified through their generation pattern, observed in DNS activity and later registered in smaller batches as potential C&C infrastructure.

DayDream: Broad Generation, Selective Registration

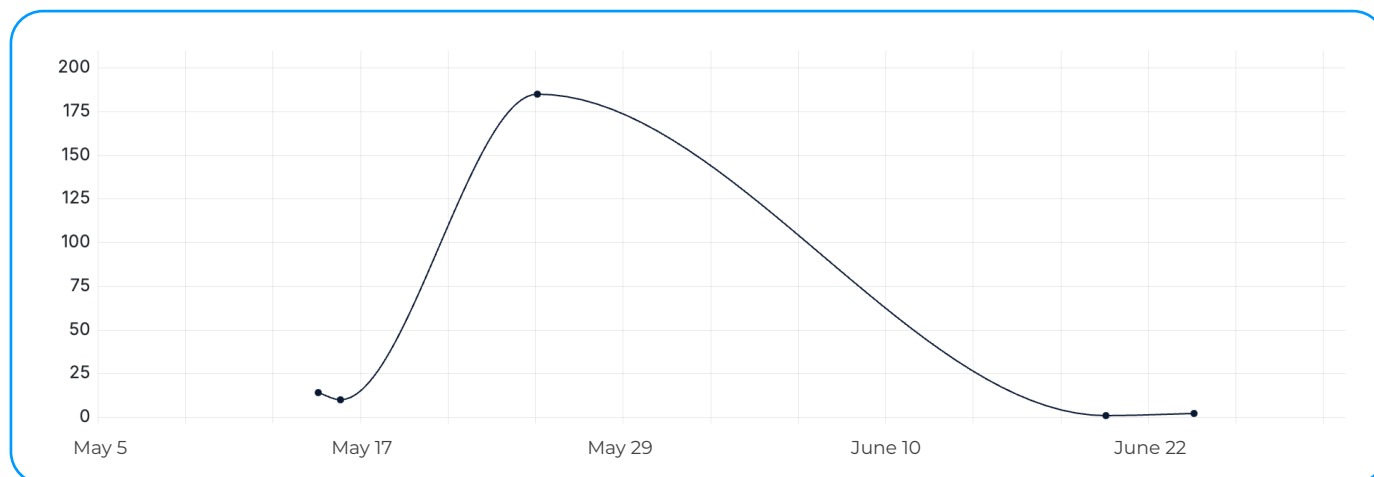
DayDream was first observed near the end of April 2026. Its generated domains appeared across 14 top-level domains and used alphanumeric labels of varying lengths, sometimes containing a dash. Approximately 500 generated domains were requested per day.

OBSERVED DEVICE MATCHES (NXD) PER DAY



Registration activity was much more concentrated than the generated-domain volume: 24 domains were registered through NameCheap on May 15, followed by 185 through Tucows on May 24 and one through Gname on June 20.

OPENED C&C DOMAINS PER DAY



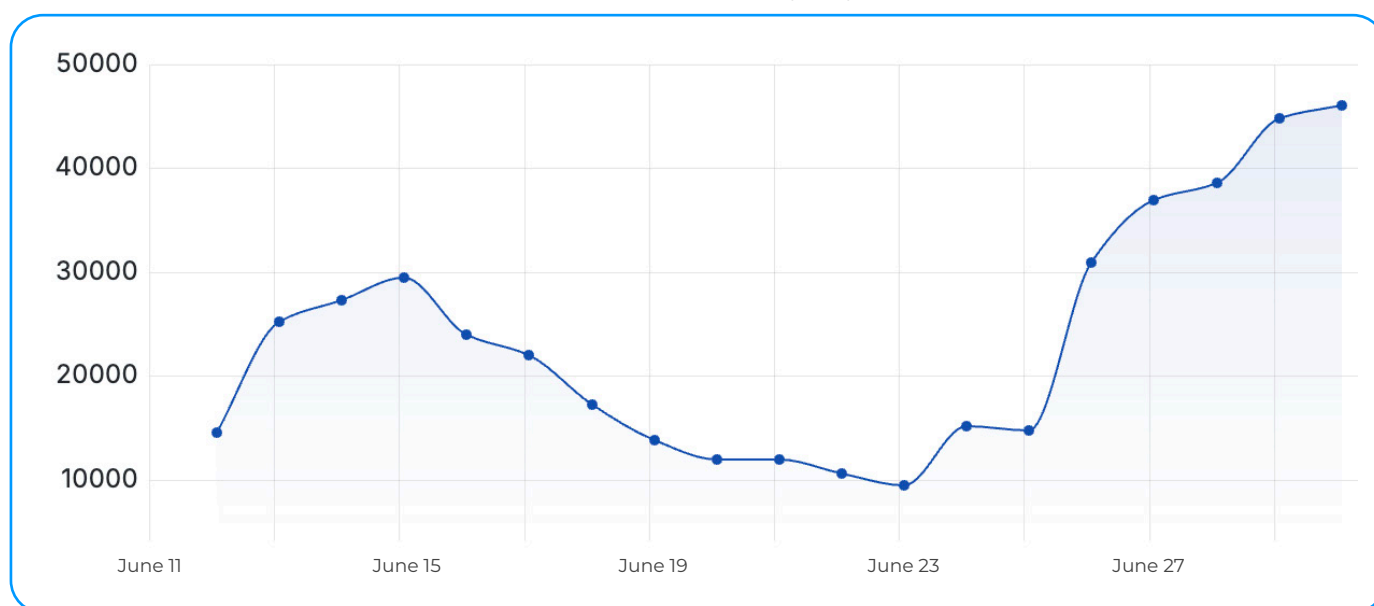
The findings show that broad domain generation does not necessarily lead to continuous registration: most observed activity was concentrated in a single batch.

Unmasked: Expired Domains, Continued Queries

Unmasked used domains composed of two short alphabetic strings separated by a dash across the .site, .online and .store top-level domains. WHOIS data confirmed that the associated domains had been registered during May and June 2025 and had expired by June 2026.

The opened C&C dataset recorded no new Unmasked openings during H1 2026. Separately, observed device matches rose rapidly after the family first appeared in the dataset on June 12, reaching 46,041 on June 30 and moving Unmasked into first place among the monitored DGA families by the end of the month.

OBSERVED DEVICE MATCHES (NXD) PER DAY



This combination shows that DNS queries can continue reaching previously used DGA domains after their registrations have expired.

AI-Driven DNS Threat Intelligence Behind These Findings

The insights in this report are produced by EfficientIP's AI-driven DNS Threat Intelligence platform, a core component of the 360° DNS Security solution. By analyzing DNS activity together with domain characteristics, visual signals and infrastructure relationships, the platform helps identify suspicious activity that would be difficult to understand from any single signal alone.

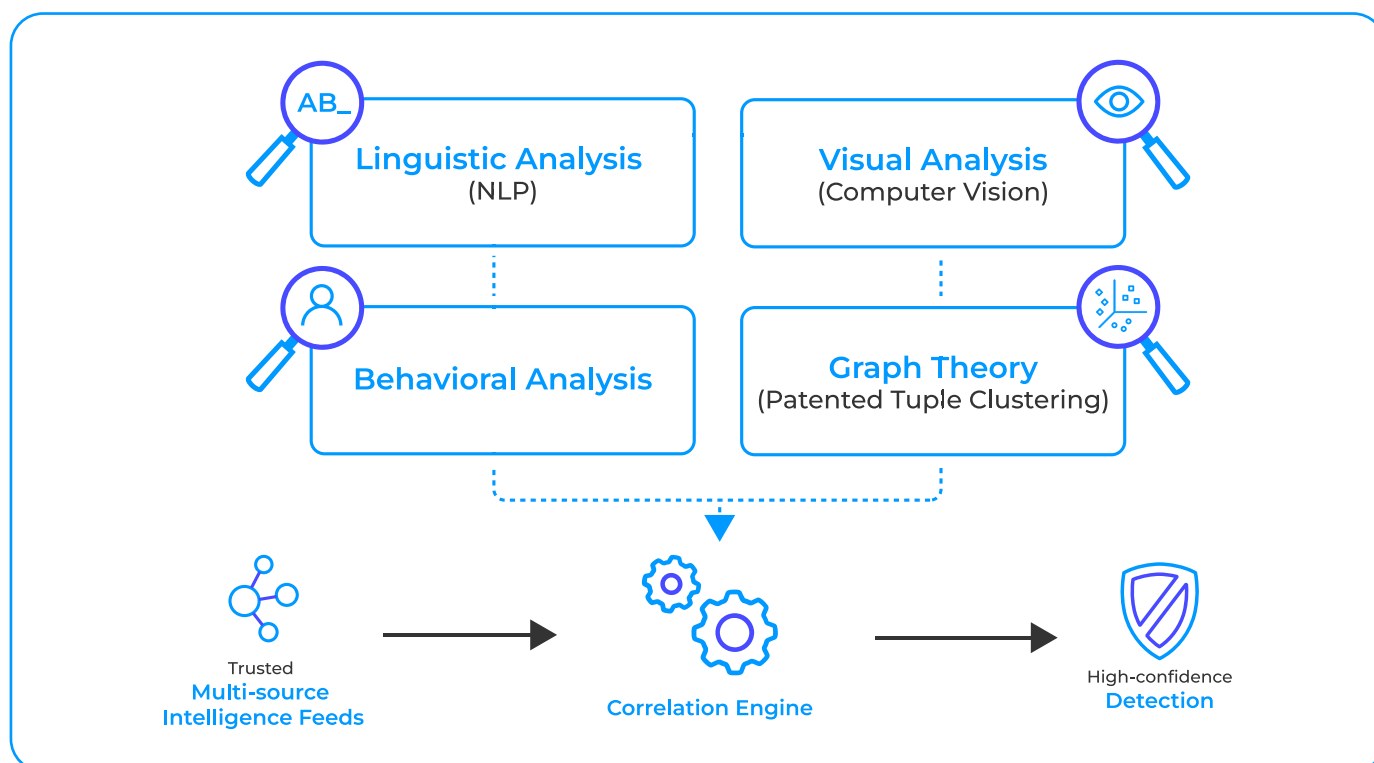
 **150B+**
DNS transactions
per day

 **500K+**
Newly observed
domains per day

 **2.6M**
Predictable
DGA domains

 **187**
DGA families
tracked

MULTIPLE SIGNALS, ONE VIEW



Linguistic analysis

Analyzes domain names for patterns tied to brand impersonation, typosquatting and other suspicious naming behavior.

Behavioral analysis

Examines DNS activity over time to identify unusual patterns, bursts and changes in infrastructure behavior.

Visual AI

Analyzes how websites look to identify phishing pages and brand impersonation, complementing domain and reputation-based detection.

DGA & infrastructure analysis

Uses generation patterns, DNS activity and infrastructure relationships to track DGA families, including domains that do not resolve.

No single DNS signal tells the whole story.

Malware activity, newly observed domains, DGA behavior, phishing campaigns and infrastructure changes each provide a different view. Combining these signals helps defenders understand what is happening, how activity is changing, and which infrastructure deserves closer investigation.



EfficientIP is a global leader in network automation and security, specializing in DNS, DHCP, and IP Address Management (DDI), with over 20 years of expertise. Its 360° DNS Security transforms DNS into a strategic security control point and source of intelligence, enabling organizations to protect against threats, detect them earlier, and respond faster.

Powered by advanced, AI-patented technologies, its DNS Threat Intelligence platform transforms billions of DNS queries into actionable insights, helping security teams identify malicious and emerging activity earlier and reduce risk.

Copyright © 2026 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS. All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.