The Era of Staged Attacks

How 2025 DNS Threat Intelligence Shapes 2026

Table of Contents

The 2026 DNS Threat Intelligence Report confirms that *DNS provides early visibility* into attack preparation, staging, and activation across *phishing*, *malware*, and *DGA activity*.

Executive Summary

In 2025, cybercrime became faster, quieter, and far more industrialized. Attackers increasingly operate at machine speed, staging campaigns in advance and activating them briefly to evade traditional, reactive defenses.

Based on the findings detailed in this report, modern threats no longer rely on single, visible attack launches. Instead, adversaries pre-position large volumes of domain infrastructure, keep it dormant for extended periods, and activate only a small subset at carefully chosen moments. This operational model appears consistently across phishing, malware, and DGA-based activity.

DNS analysis exposes this hidden preparation phase. Patterns such as large-scale domain generation, delayed activation, infrastructure reuse, and burst-driven command-and-control behavior repeatedly emerge before attacks fully materialize. These early signals enable defenders to intervene upstream in the attack lifecycle, before customers, employees, or revenue are affected.

As 2025 has shown, DNS has become a leading indicator of staged attacks and a critical source of threat intelligence. These patterns are already shaping what defenders should expect in 2026, as adversaries continue to rely on automation, short-lived infrastructure, and rapid activation cycles. Anticipation and proactive defense will be as important as response, meaning that organizations that leverage DNS threat intelligence effectively will gain a clear strategic advantage in the year ahead.

Key Insights

CRIMINALS BUILD MASSIVE ARSENALS IN ADVANCE

One operation (BaitHook) prepared ***580,000 web addresses***, allowing attacks to be launched instantly.

ATTACKERS' INFRASTRUCTURES ARE HIGHLY CENTRALIZED AND AUTOMATED

Just 69 systems controlled ***150,000 fake sites***, enabling small groups to run global campaigns.

ATTACKERS TIME THEIR STRIKES TO REVENUE CYCLES

Amazon-style scams rose ***228% in December***, hitting consumers when spending peaks.

THREATS SCALE AT UNPRECEDENTED SPEED

A single outbreak grew ***60x in infection volume*** within months.

PHISHING IS STILL A TOP BUSINESS RISK

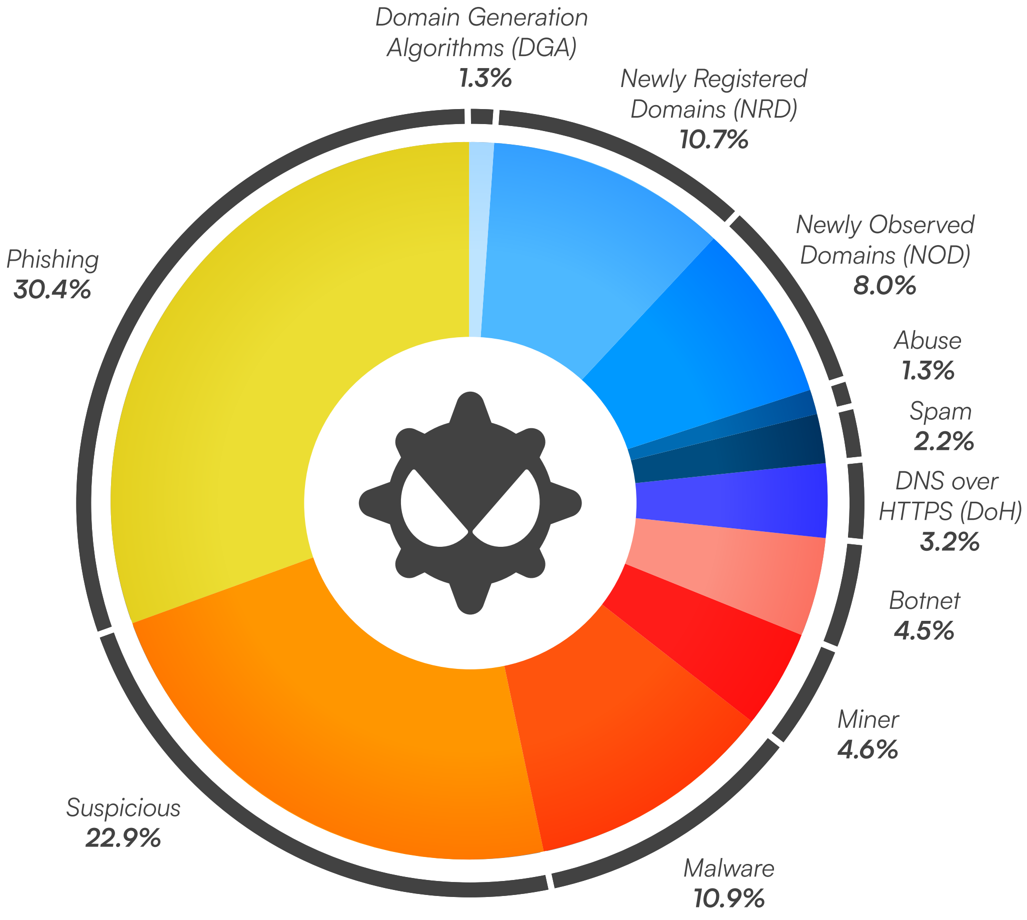
30% of all malicious domains were used for phishing.

CRYPTOCURRENCY SCAMS GREW STEADILY

Fraud targeting digital currencies ***more than doubled*** during the year.

DNS Threats in 2025: A Bird's-Eye View

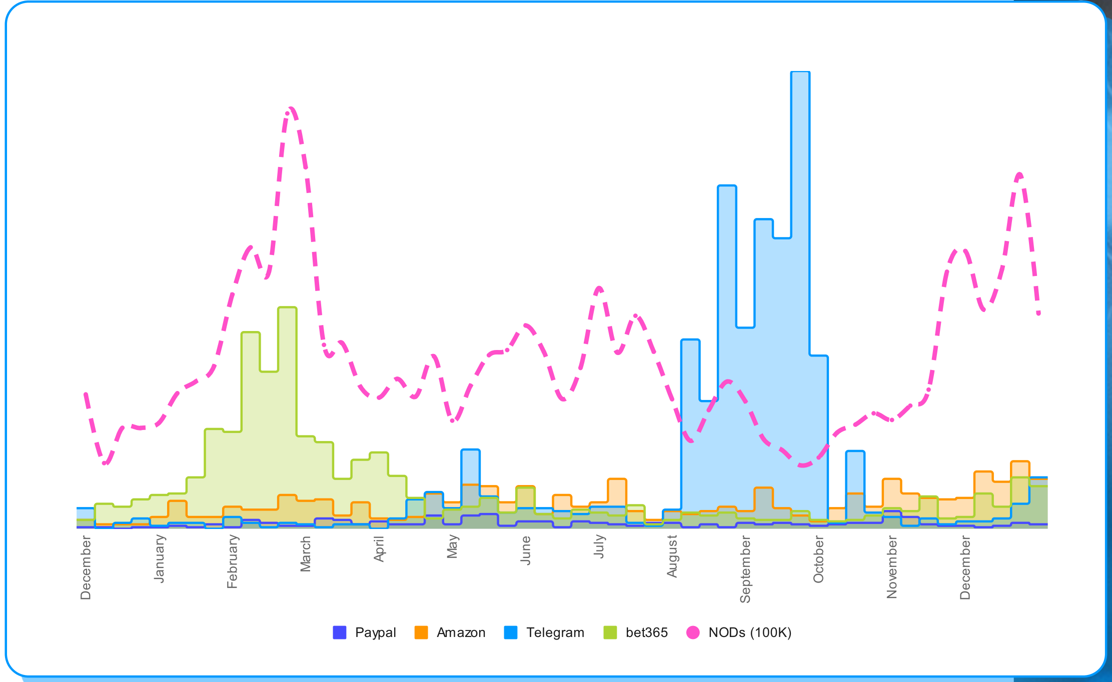
At the yearly level, analysis of DNS traffic matched against threat intelligence shows a stable and highly imbalanced distribution across categories. **Phishing** was ranked first with a **30% share** followed by **suspicious domains (23%)**, indicating potential threats that are not yet confirmed. **Malware** accounts for **11%** of detections, representing domains used to host or distribute malicious software. **Newly Registered Domains (NRDs) (11%)** and **Newly Observed Domains (NODs) (8%)** also represent a significant share of detections, particularly during the early stages of phishing campaigns. As for **DGA**s, despite their lower overall share, they remain consistently present throughout the year, reflecting persistence and controlled activation.



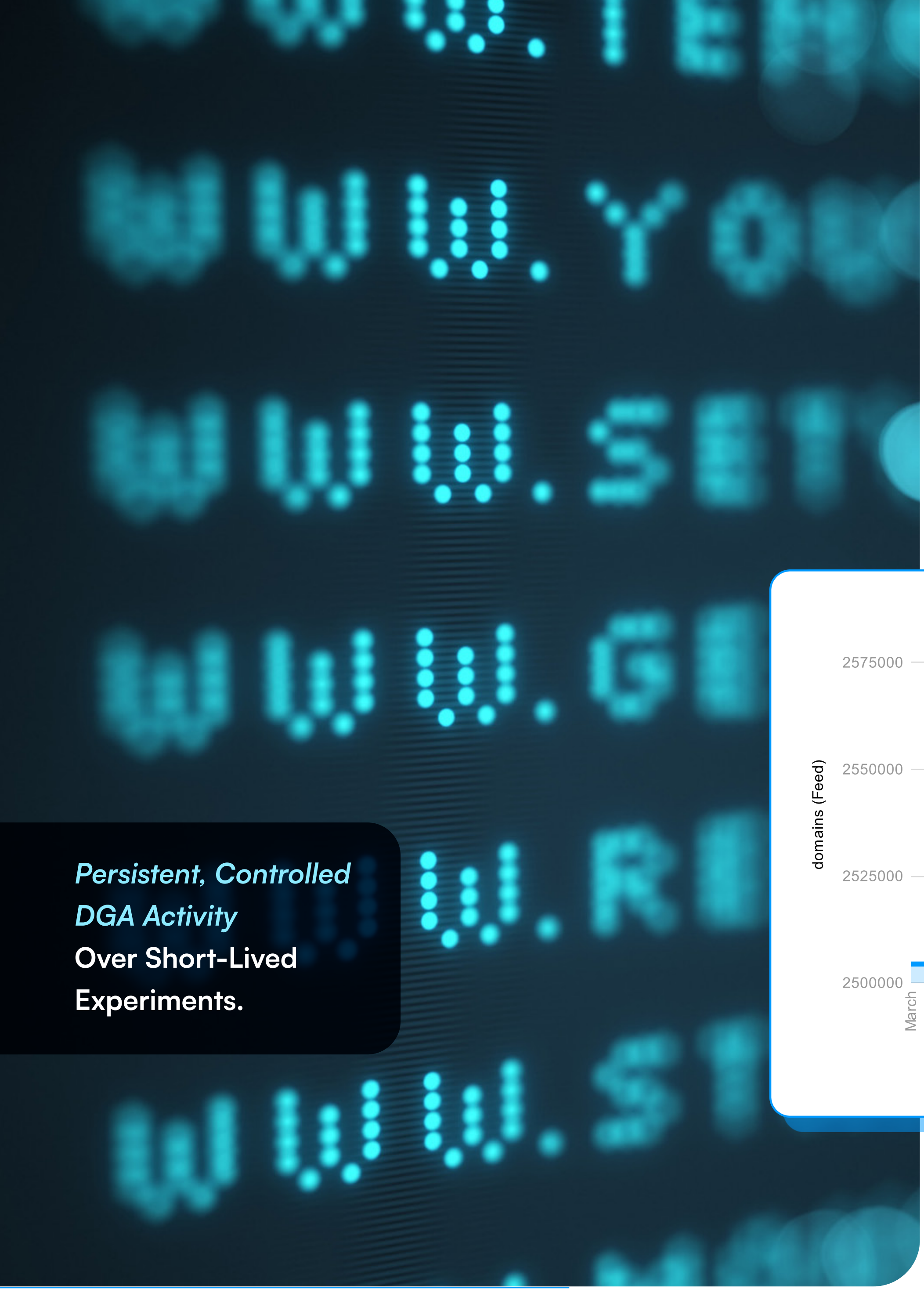
DNS Matched Traffic Categories

Monthly aggregation shows that spikes in suspicious domains and newly registered domains frequently precede phishing campaign peaks by one or more months. This confirms that much of the malicious activity visible in DNS reflects infrastructure preparation rather than immediate exploitation.

This bird's-eye view summarizes how different DNS threat categories contribute to the overall landscape and sets the foundation for the deeper analysis that follows. The next sections examine how these threats evolve over time and how DNS reveals their full attack lifecycles.



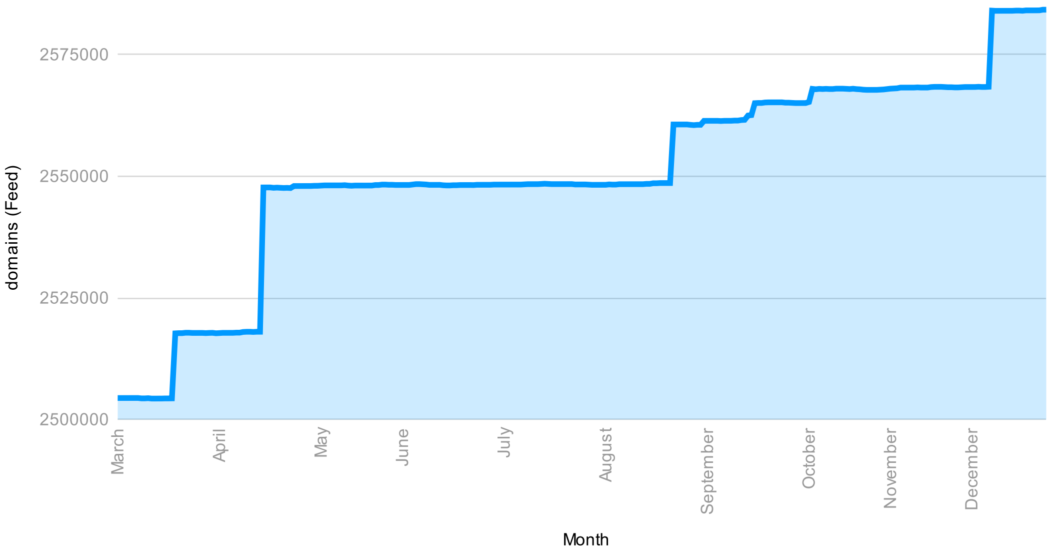
Newly Observed Domains Followed By Phishing Campaigns



Persistent, Controlled DGA Activity Over Short-Lived Experiments.

DGA Threat Landscape in 2025

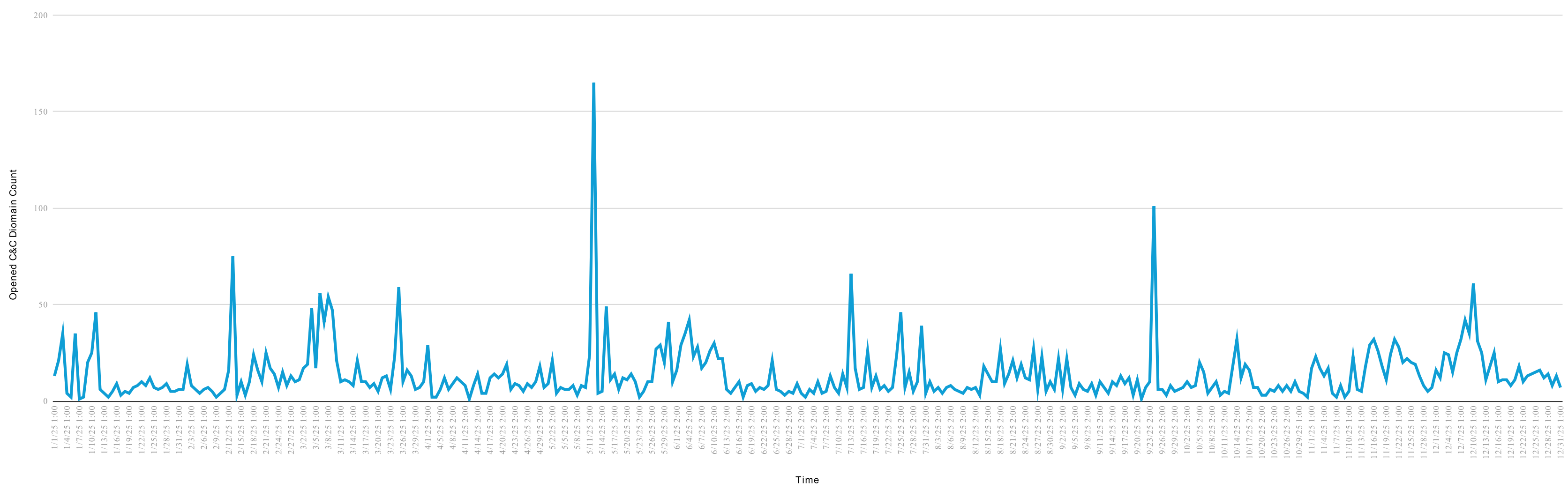
Across 2025, DGA-related DNS activity shows persistent presence and controlled growth rather than short-lived experimentation. DGA traffic remains visible every month, with infected device populations increasing steadily across extended periods before stabilizing at elevated levels, particularly in the second half of the year.



Domains Associated With DGA Activity Over Time

A well-established characteristic of DGA-based malware is the imbalance between the large number of domains generated by algorithms and the very small subset that ever become operational. Analysis of EfficientIP's DNS threat intelligence data from 2025 reflects this expected behavior consistently across all DGA families. High volumes of algorithmically generated domain queries are visible every month, while only a limited number of domains are ultimately registered and successfully resolved. As a result, NXDOMAIN responses dominate DGA-related DNS traffic throughout the year.

When DGA infrastructure does become active, command-and-control domains appear in short, punctual bursts, with brief activation windows rather than sustained use. As shown in the graph below, this activity manifests as sharp, isolated spikes of domain activity. This pattern indicates deliberate, tightly controlled activation, where only a small number of domains are opened momentarily for coordination before being quickly rotated or abandoned.



DGAs That Opened Command-and-Control (C&C)

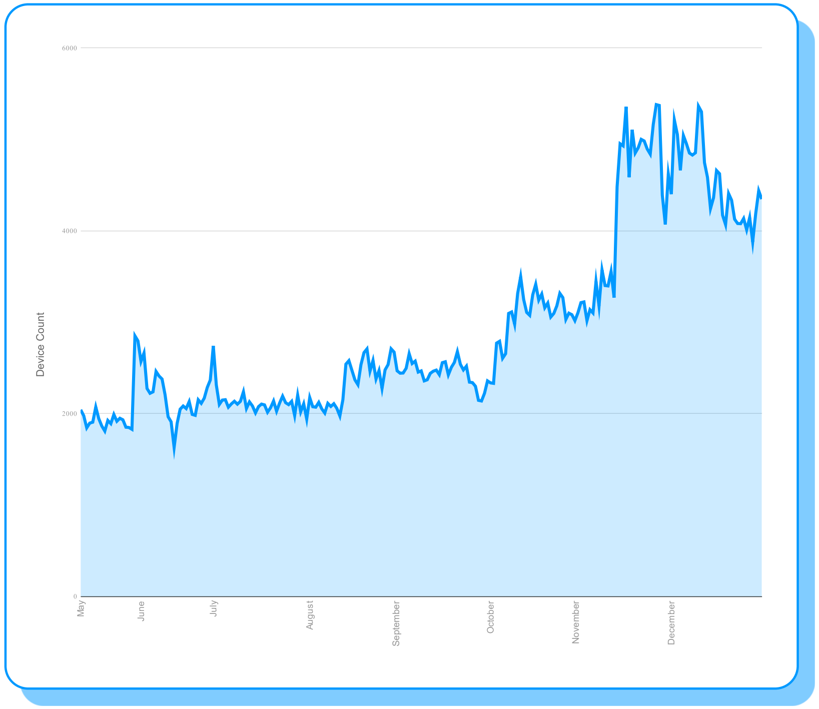
BaitHook

BaitHook (EIP-443) is a DGA-based malware family identified by EfficientIP. It was first observed in EfficientIP's DNS telemetry in October 2024, generating large volumes of algorithmic domain names following a structured pattern of five letters and eleven hexadecimal characters across ".com," ".net", and ".top" top level domains (TLDs), from which a small subset is later registered and used for command-and-control.

BaitHook produced
~580,000
potential C&C domains

BaitHook exemplifies industrial-scale DGA operations. Analysis of EfficientIP's DNS data shows sharp increases in previously unseen non-existent domains (NXDOMAINs) during the specific months, including more than 70,000 new requested domains in late July and over 12,000 in September. Despite these volumes, only three to four domains per day were registered on average. Many domains remained in NXDOMAIN state for weeks before activation. Once activated, domains consistently resolve to previously observed IP addresses, confirming backend infrastructure reuse.

Across the year, the BaitHook activity produced a pool of approximately 580,000 potential command-and-control domains, which could be registered and used as C&C by this malware at any time.



Daily Devices Generating DNS Queries to EIP-443 (BaitHook) Domains

Orchard

Orchard DGA is a bitcoin-seeded DGA malware family originally discovered in 2022. New domains related to this DGA were identified by EfficientIP through DNS telemetry analysis in mid-2025. It generates large volumes of short hexadecimal domain names across a narrow set of TLDs. Its domain activity remained highly consistent over time, allowing large-scale detection based on DNS behavior rather than static malware signatures.

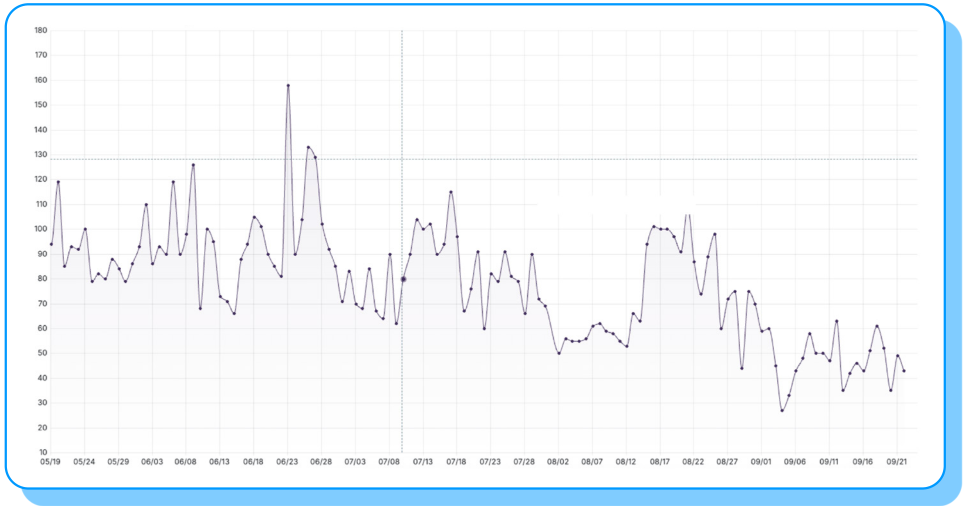
DGA detection increasingly depends on ***DNS behavior analysis***

The Orchard malware demonstrates how DGA detection increasingly depends on DNS behavior rather than code signatures. Using a Bitcoin Genesis Block—seeded algorithm, Orchard generated millions of domains with six-character hexadecimal labels across a narrow TLD set. Although many domains did not match known malware code, their DNS behavior remained consistent over time, making DNS analysis the only reliable detection layer at scale.

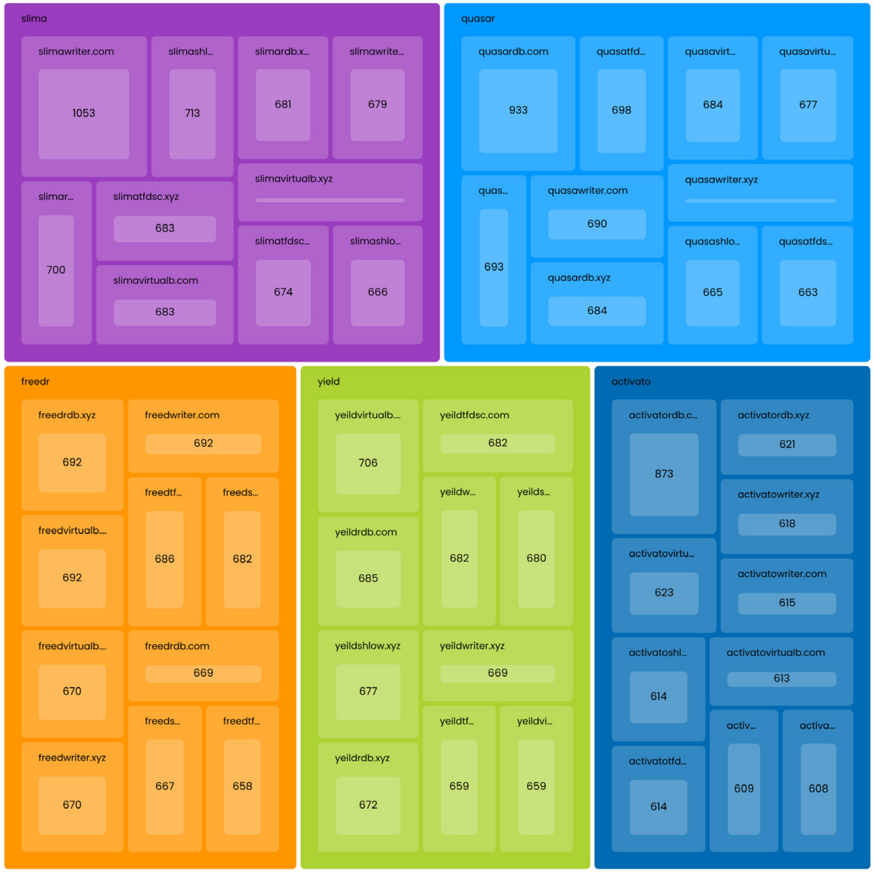
EconoMimics: Dormant DGA-Driven Infostealer

EconoMimics is a DGA-based infostealer campaign [discovered by EfficientIP]() in DNS telemetry, characterized by long periods of dormant domain activity followed by tightly coordinated activation. Large numbers of algorithmically generated domains were queried weeks before any payload delivery, making DNS behavior the primary signal of compromise.

As shown below, infected client activity fluctuates over time, reflecting ongoing infections rather than a single short-lived outbreak, while domain-level behavior reveals delayed activation patterns.



Clients Infected by EconoMimics Throughout 2025



EconoMimics Top Level Domains Cluster

DGA-generated domains were queried extensively but remained dormant for weeks. A cluster of domains was registered in late September, yet DNS resolution activity did not begin until late October.

The visualization below highlights the structured naming patterns across multiple related domain families and TLDs, illustrating large-scale algorithmic domain generation prior to activation.

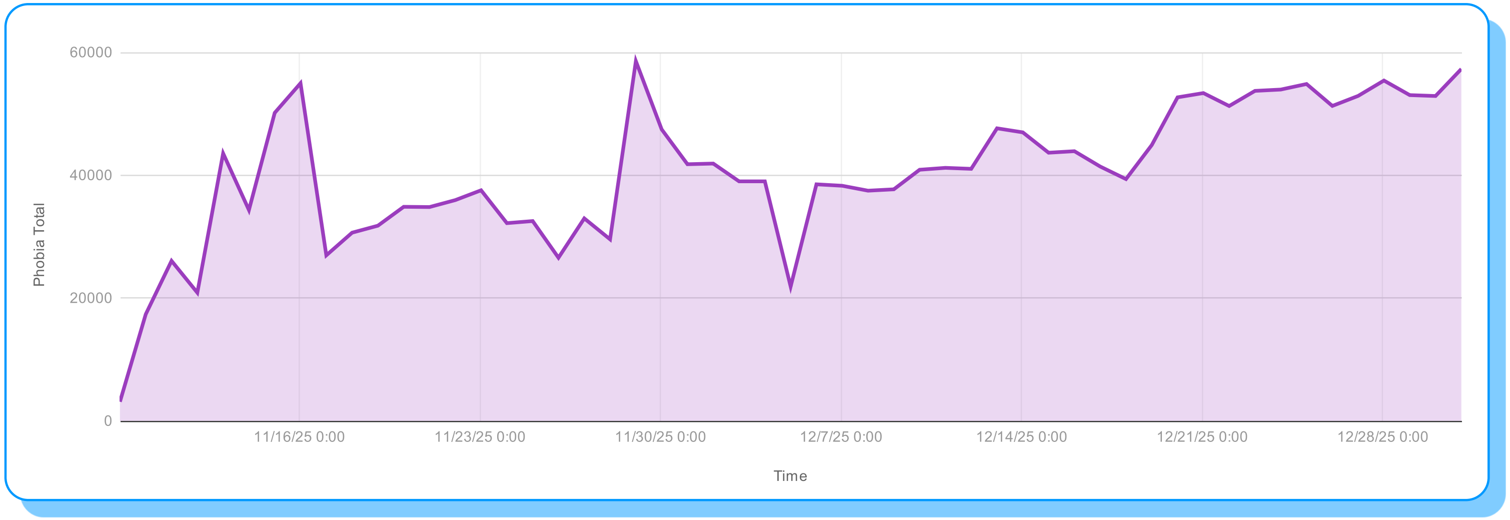
When activated, the infrastructure relied heavily on DNS TXT record queries to deliver Base64-encoded PowerShell fragments that acted as an initial stager before transitioning to encrypted HTTPS communication. Payloads were executed entirely in memory, evading file-based detection. DNS exposed the campaign through DGA-like domain generation, delayed activation, unusual query types, and coordinated resolution behavior across hosts. This case illustrates how DGA infrastructures are increasingly used as dormant delivery mechanisms, not only as active command-and-control channels.

EfficientIP identified ***dormant DGA infrastructure*** later used for infostealer activation

Phobia

Phobia is a DGA-based malware family first observed in EfficientIP's DNS telemetry in early November, when infected devices across multiple telecom networks began querying large volumes of algorithmically generated .cn domains. Initial activity involved roughly 1,000 infected devices per day and a rotating, time-dependent domain pattern that produced hundreds of new domain candidates daily. The malware is marked by rapid scaling and frequent changes in its domain-generation logic, and within a few months it expanded from a limited infection base to tens of thousands of active devices while repeatedly modifying the structure of its generated domain names.

This growth is clearly visible in DNS traffic, with infected device counts rising from approximately 1,000 per day to more than 60,000 per day during peak months and daily NXDOMAIN volumes reaching 16,000. Over time, domain formats evolved from numeric to alphabetic and later alphanumeric structures. Registration activity was highly concentrated, with more than 15,600 domains registered through a small number of registrars, while over 150,000 FQDNs ultimately resolved to just 69 IP addresses, revealing an extremely centralized backend infrastructure.



Devices Generating DNS Queries to Phobia Domains

Phishing never takes a break - **30%** of threat domains

Phishing Activity in 2025

In 2025, phishing accounts for approximately 30% of all domains associated with cyber threats, a proportion that remains stable across the year. This stability establishes phishing as a structural and persistent component of the threat landscape.

Phishing activity observed through DNS threat intelligence follows a sustained, long-term pattern with periodic campaign-driven peaks. Notable peaks align with identifiable campaigns, including a Q3 Telegram impersonation and e-commerce targeting during the shopping season.

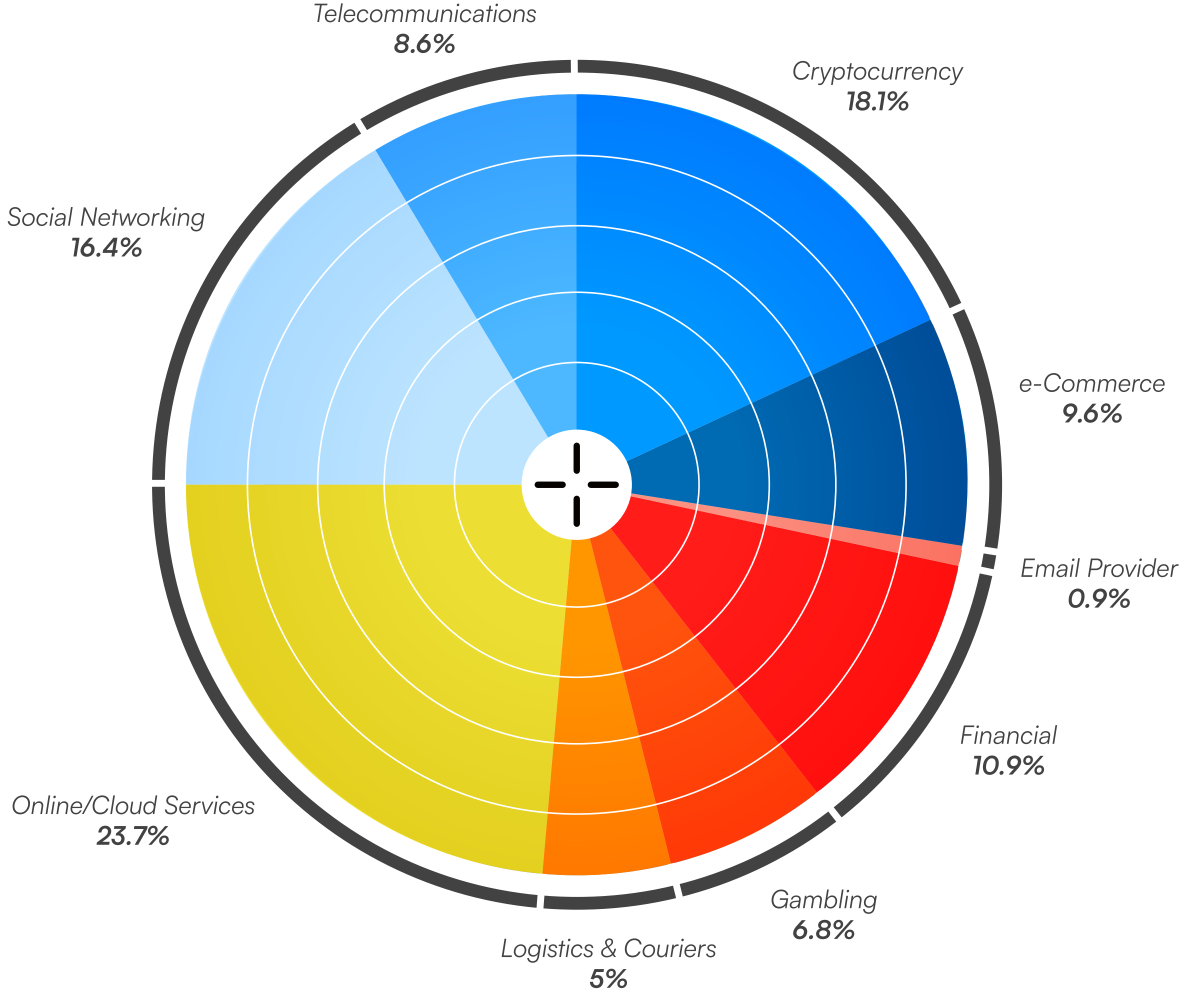
DNS analytics show that phishing activity frequently overlaps with newly observed domain activity, as detailed in the Newly Observed Domains (NODs) chapter. When active, phishing domains can generate elevated DNS query volumes for varying durations depending on campaign scale and target, reflecting sustained use rather than single-use activity. This behavior reflects an operational model favoring rapid activation and flexible use of infrastructure.

Taken together, these observations show that phishing activity in 2025 combines continuous operational presence with opportunity-driven campaigns, maintaining a persistent baseline while activating short-lived operations in response to specific contexts and targets.

Targeted Phishing Sectors

Phishing campaigns in 2025 primarily target a concentrated set of sectors that together account for the majority of phishing-related domains observed during the year. These sectors correspond to services that are widely used, trusted, and often business or life-critical, making them attractive targets and difficult to block without disrupting legitimate activity.

Core digital sectors
dominate phishing targets



2025 Targeted Phishing Sectors

Online and cloud services represent the largest share of phishing activity, accounting for ***23%*** of phishing domains in 2025. These include platforms used for authentication, collaboration, messaging, and account management. Their central role in daily workflows results in sustained targeting throughout the year, with limited variation between quarters.

Cryptocurrency platforms account for roughly ***18%*** of phishing activity and show the strongest growth trend over the course of the year. Their relative share increases steadily from quarter to quarter, with end-of-year activity **more than double** that observed at the beginning of the year. This reflects a growing and sustained attacker focus on cryptocurrency services rather than isolated campaign-driven spikes.

Social networking and messaging platforms represent ***16%*** of phishing activity and exhibit a pronounced ***peak in Q3***. While present throughout the year, phishing targeting these services intensified during the third quarter, aligning with the expansion of large-scale messaging impersonation campaigns, most notably Telegram. Activity declines somewhat in Q4 but remains above early-year levels.

Financial services account for ***11%*** of phishing activity and maintain a steady presence throughout the year. Phishing domains impersonating banks and payment platforms appear continuously rather than in isolated bursts, indicating long-term targeting rather than event-driven exploitation.

E-commerce represents ***9%*** of phishing activity overall. Activity remains relatively stable from Q1 through Q3 and then ***approximately doubles in Q4***, aligning with the shopping season. This increase reflects opportunistic exploitation of heightened consumer activity during Black Friday and end-of-year holidays.

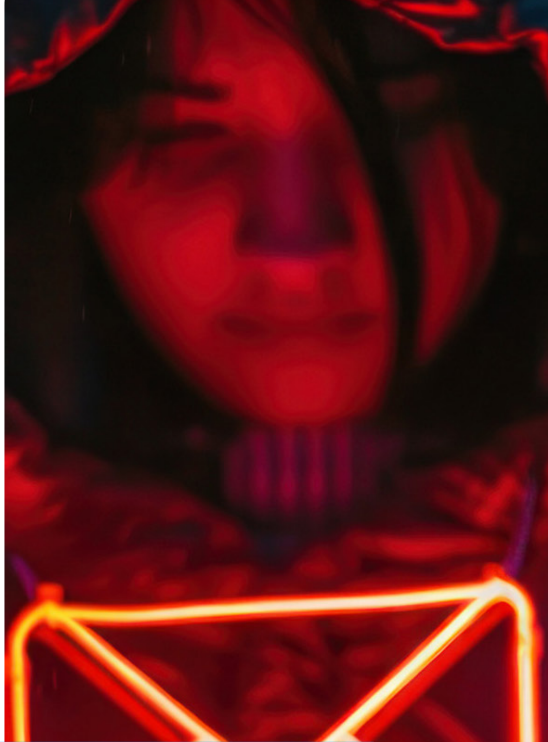
Gambling-related phishing starts the year at a high level, accounting for approximately ***18%*** of phishing activity in Q1. This elevated share aligns with ***periods of increased sports and betting*** activity early in the year. As the year progresses, gambling-related phishing declines steadily relative to other sectors, representing a much smaller share by the second half of the year. This shift suggests that attacker focus moves away from event-driven betting platforms toward targets offering broader or more sustained monetization opportunities.

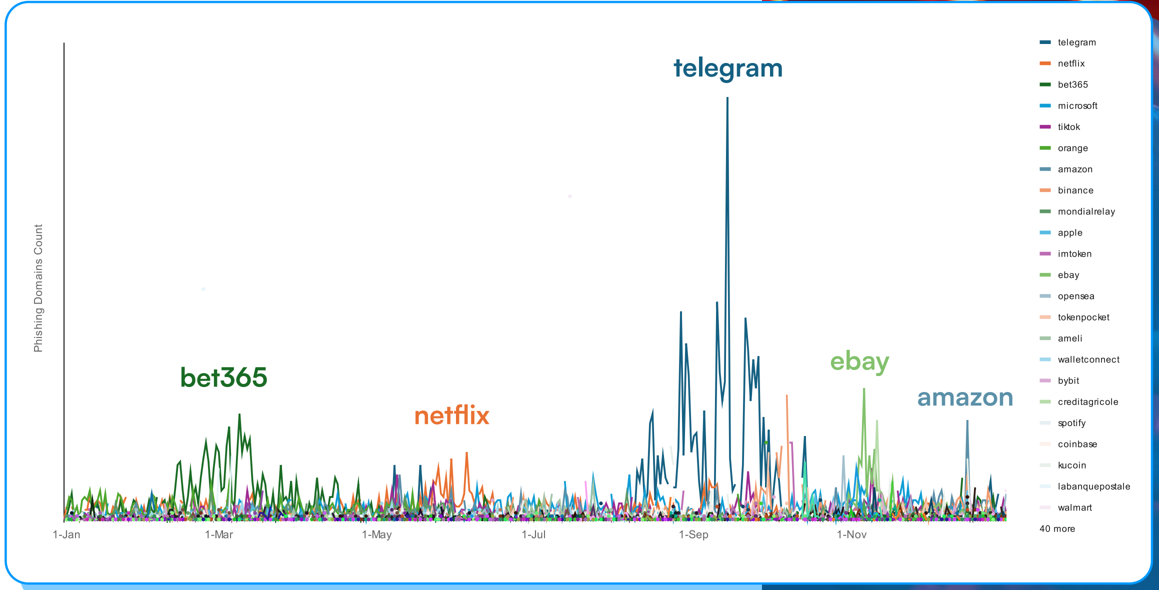
Overall, *targeted phishing sectors in 2025* reflect a combination of long-term operational focus on core digital services and adaptive shifts driven by seasonal behavior and major real-world events.

Phishing Targets and Dynamics

DNS threat intelligence data from 2025 shows that phishing activity is shaped by a stable set of commonly impersonated platforms, rather than constant churn in targets. Throughout the year, the same widely used services reappear consistently in phishing activity, forming a persistent baseline. Within this stable landscape, punctual, campaign-driven deviations temporarily elevate specific targets, creating visible shifts in activity that stand out clearly in DNS analytics. As reflected by the spike visible on the graph, these deviations align with identifiable campaigns or contextual opportunities such as bet365 early in the year, Telegram from Q3 onward, and e-commerce platforms including Amazon and eBay toward year-end.

As represented in the graph below, analysis of phishing detections per target over time reveals distinct operational profiles. Some targets experience short-lived surges followed by rapid decline, while others exhibit sustained growth and long-term persistence. These differences are not random; they reflect deliberate attacker choices around timing, monetization potential, and infrastructure investment.





Detected Phishing Domains per Target per Day (2025)

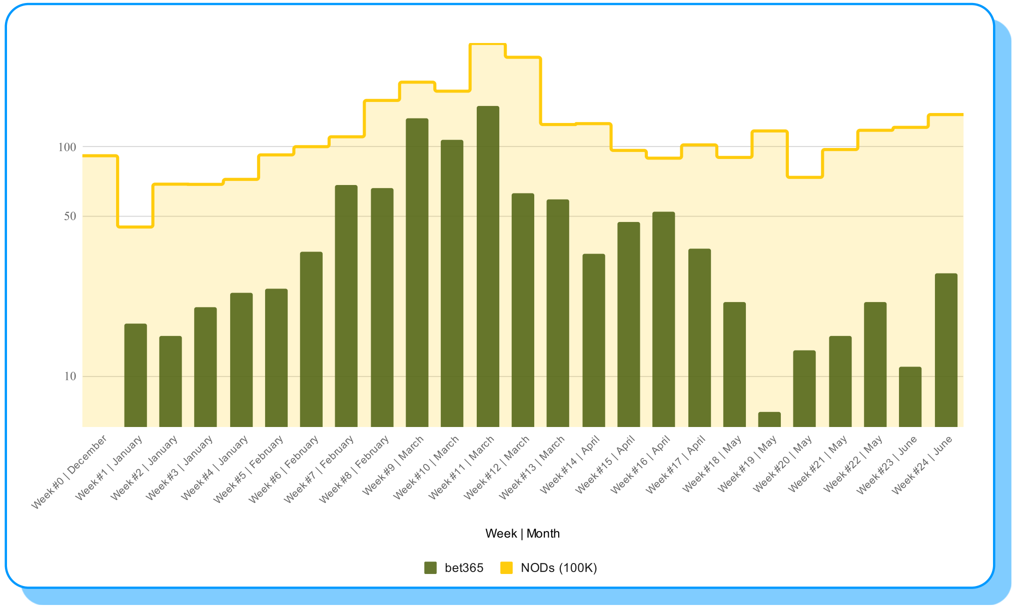
bet365 Phishing Campaign

Phishing activity impersonating bet365 peaks in Q1, with DNS analytics showing repeated spikes in detected bet365-related phishing domains during this period. Activity begins to slow in Q2 and reaches a relatively low, stable baseline in the second half of the year.

The bet365 campaign is characterized by short-lived bursts of activity, where phishing domains are introduced and activated rapidly, generate elevated DNS query volumes for brief periods, and are then abandoned. After the early-year campaign window closes, bet365-related phishing does not return to comparable levels later in 2025, indicating a time-bound campaign likely aligned with betting-related opportunity windows, such as major Q1 sporting events including the Super Bowl, the UEFA Champions League knockout stages, and other high-visibility competitions that typically drive increased online betting activity.

***Newly Observed Domains* Precede Bet365 Campaign Activity**

Consistent with this campaign-driven behavior, increases in newly observed domains (NODs) during Q1 align closely with spikes in bet365-related phishing activity, suggesting advance domain registration in support of the campaign. As bet365 activity declines, NOD levels stabilize, reinforcing the link between domain preparation and active phishing phases, as reflected in the graph below.



NOD Growth vs. Bet365 Phishing Campaign Spikes

Telegram Phishing Campaign

Telegram-related phishing domains appeared at low levels during the first half of 2025, then increased sharply beginning in Q3, with multiple distinct spikes observed through Q3 and into early Q4.

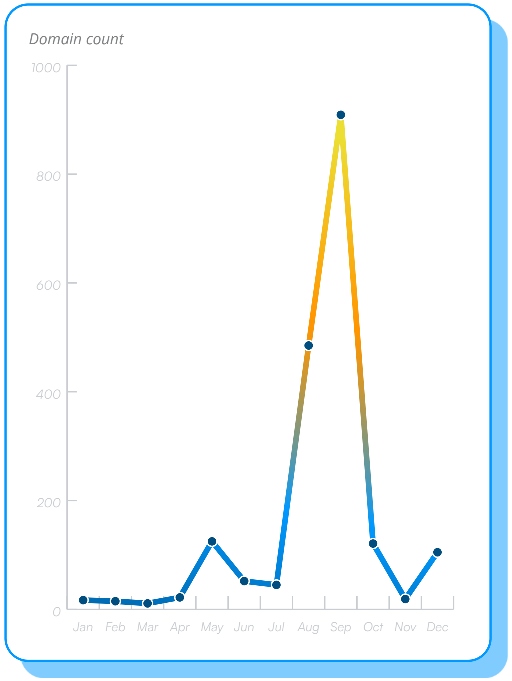
DNS analytics indicate rapid domain introduction, short operational lifetimes, and abrupt post-peak declines.

Telegram phishing activity is distinguished by extensive infrastructure preparation. Telegram-themed domains share a consistent naming pattern of the form te[i,l]e[a-z]{6}.tld, such as teietgbmko[.]blue and teieuijnbv[.]fit. This uniform structure indicates automated domain generation rather than manual registration.

Across the campaign, Telegram phishing infrastructure spans 47 distinct top-level domains, including .blue, .fit, .club, .work, .top, .wiki, and others. The breadth of TLD usage suggests a deliberate evasion strategy designed to dilute reputation signals and bypass domain-based filtering mechanisms.

A notable characteristic of this campaign is that many Telegram-themed domains remain dormant for a long period. This behavior indicates pre-positioned phishing infrastructure, with domains staged in advance for later activation.

When activity does occur, it manifests as short, repeated bursts rather than sustained use. Taken together, the standardized domain structure, wide TLD distribution, and delayed activation patterns point to a coordinated, centrally managed phishing operation, with infrastructure staged ahead of campaign execution.



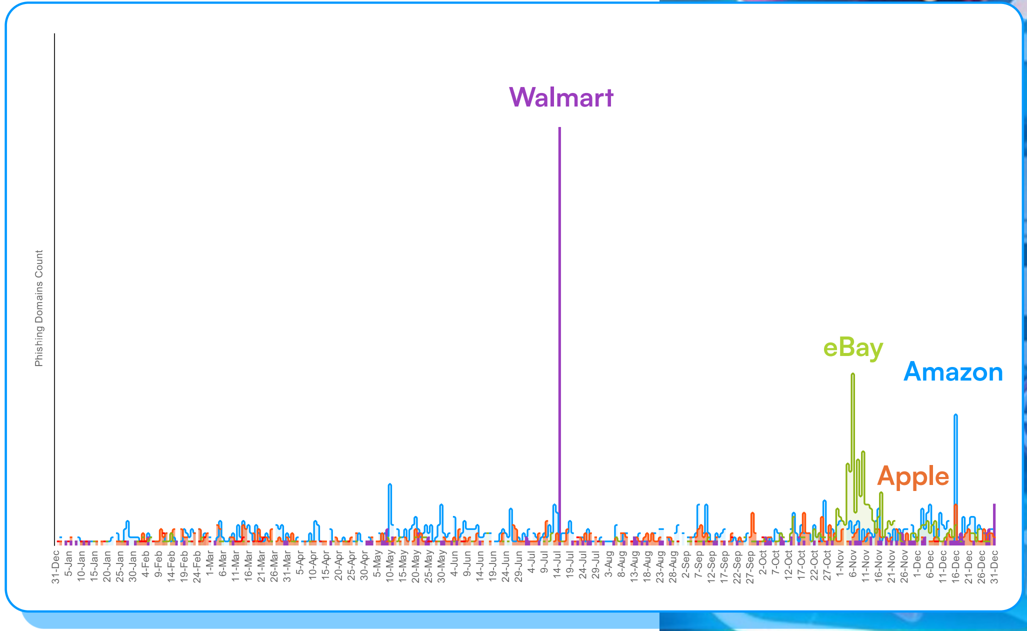
Domains Linked to Telegram Phishing Campaigns (2025)

Shopping Season Phishing Activity

DNS threat intelligence shows that phishing activity targeting e-commerce platforms follows clearly identifiable retail cycles throughout 2025, culminating in a pronounced and sustained peak toward the end of the year, with additional increases observed around other major shopping periods. Elevated activity is visible during January sales and mid-year summer sales in July, but the most significant concentration of activity occurs during November and December.

The strongest increase occurs in Q4, where phishing domains impersonating major online retailers rise sharply during **Black Friday and Cyber Monday** and continue to rise, reaching a peak during the Christmas shopping period. Target-level analysis shows that **Amazon-targeted phishing** activity in December is approximately 228% higher than the average monthly number of phishing domains observed from January to December, marking the most pronounced e-commerce phishing peak of the year. **Apple-themed and eBay-themed phishing** follows a similar pattern, with activity increasing during all major sales periods and reaching its highest sustained levels in the weeks leading up to Christmas.

DNS analytics show that e-commerce phishing campaigns during these periods are characterized by rapid activation and relatively short operational lifetimes. Domains typically appear and become active within narrow time windows, reflecting campaigns designed to exploit heightened consumer engagement and time-sensitive purchasing behavior.



Detected e-Commerce Phishing Domains Per Day

Newly Observed and Newly Registered Domains (NODs / NRDs)

Newly registered and newly observed domain activity remains consistently elevated throughout 2025, forming a continuous infrastructure supply layer that supports multiple threat types. DNS threat intelligence shows that this activity persists across all months rather than appearing only in isolated bursts, providing attackers with a steady pool of domains that can be activated opportunistically or in response to specific campaigns.

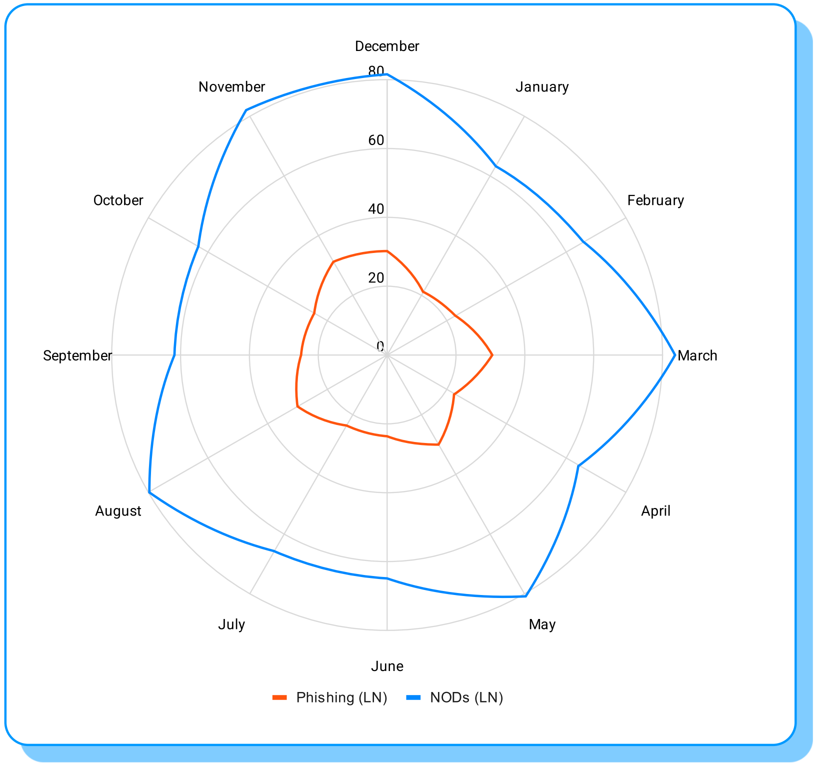
Analysis of newly observed domains shows a close temporal relationship with phishing activity during the year. Periods of increased NOD volumes frequently coincide with, or slightly precede, increases in detected phishing domains. This alignment is particularly visible during campaign-driven phases such as the Telegram impersonation activity in Q3 and the intensified e-commerce phishing observed toward the end of the year. The pattern indicates rapid introduction and activation of domains shortly after they first appear in DNS traffic, rather than long staging periods.

The graph below visually reinforces the trends described above using normalized values, allowing direct comparison of phishing activity and newly observed domain (NOD) volumes across months. On this normalized scale, peaks in NOD activity align closely with periods of intensified phishing, indicating that domain emergence and phishing operations rise and fall together. This alignment highlights the close temporal relationship between domain appearance and active phishing campaigns.

Attackers Are Always Ready: Maintaining a High-Volume, Low-Cost Domain Supply with Built-In Evasion

At the registry level, analysis of newly registered domains reveals pronounced peaks concentrated in a small number of top-level domains that are repeatedly favored by attackers. Throughout 2025, significant registration spikes are observed under TLDs such as .xyz, .top, and .bond. These TLDs are typically inexpensive, enabling low-cost bulk registration, and often impose restrictive WHOIS access or procedural limits that reduce visibility into registrant data. Some also support cryptocurrency payments, further complicating attribution.

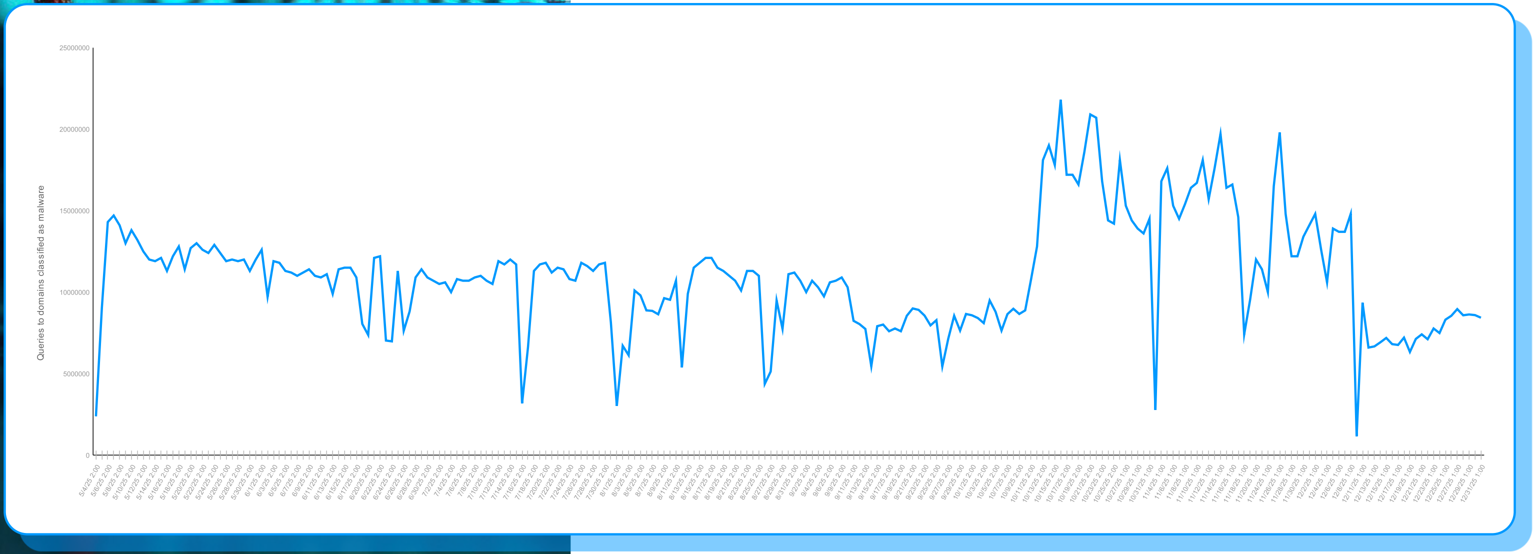
Taken together, NOD and NRD behavior in 2025 illustrates how attackers rely on continuously refreshed, low-cost domain infrastructure rather than static assets. DNS threat intelligence exposes this supply layer early, revealing how domain introduction and activation closely align with downstream phishing activity.



NODs And Phishing Correlation

Malware DNS Activity in 2025

Malware-related DNS activity observed in 2025 remains present throughout the year but shows a clear and pronounced concentration at the end of the year, with a distinct escalation occurring in Q4. For most of the year, malware DNS volumes fluctuate within a relatively stable range, marked by intermittent dips and short-lived increases rather than sustained growth.



Malware Matches In Global DNS Traffic (2025)

Q4 Marks Sustained *Malware Escalation*

This pattern changes sharply at the start of Q4. DNS analytics show a sudden step-up in malware-related query volumes, followed by an extended period of elevated activity that persists across multiple weeks. Unlike earlier fluctuations, the Q4 increase is not limited to a single spike but forms a sustained high-activity phase, indicating prolonged operational use rather than isolated campaign execution.

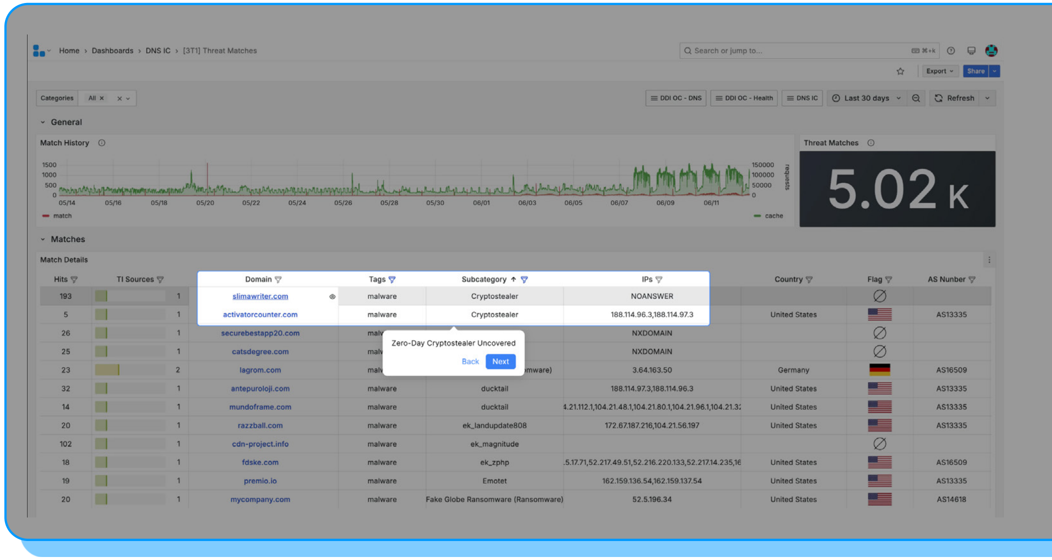
Following this elevated period, a sharp drop is observed, suggesting the deliberate teardown or suspension of infrastructure after an intensive end-of-year operational phase rather than organic decay of activity.

Resolution behavior observed in 2025 shows recurring backend consolidation, where rotating sets of malware-related domains repeatedly resolve to a limited number of IP addresses over extended periods. DNS analytics also reveal uneven distribution of query volumes across infected hosts. Across multiple malware families, a minority of devices generates a disproportionately large share of DNS activity during malware operations, indicating that communication patterns are not uniformly distributed across all infected endpoints. These concentration effects are most clearly observable at the DNS layer, where infrastructure reuse and host-level activity differences can be correlated over time.

DNS Zero-Day Infostealer

One of the most significant malware findings of 2025 was the discovery of a zero-day infostealer entirely through DNS behavior. The campaign was first identified through anomalous DNS TXT record lookups to domains that lacked associated A or AAAA records and exhibited automated naming patterns. This campaign was first documented in the EfficientIP blog "Zero-Day Malware First Detected by DNS Threat Intelligence".

DNS TXT responses delivered small Base64-encoded PowerShell fragments used as an initial stager. These fragments assembled and executed payloads in memory before transitioning to encrypted HTTPS communication for further instructions. Because execution was fileless, the malware initially evaded traditional endpoint detection, yet DNS exposed its presence through query types, volumes, and sequencing.



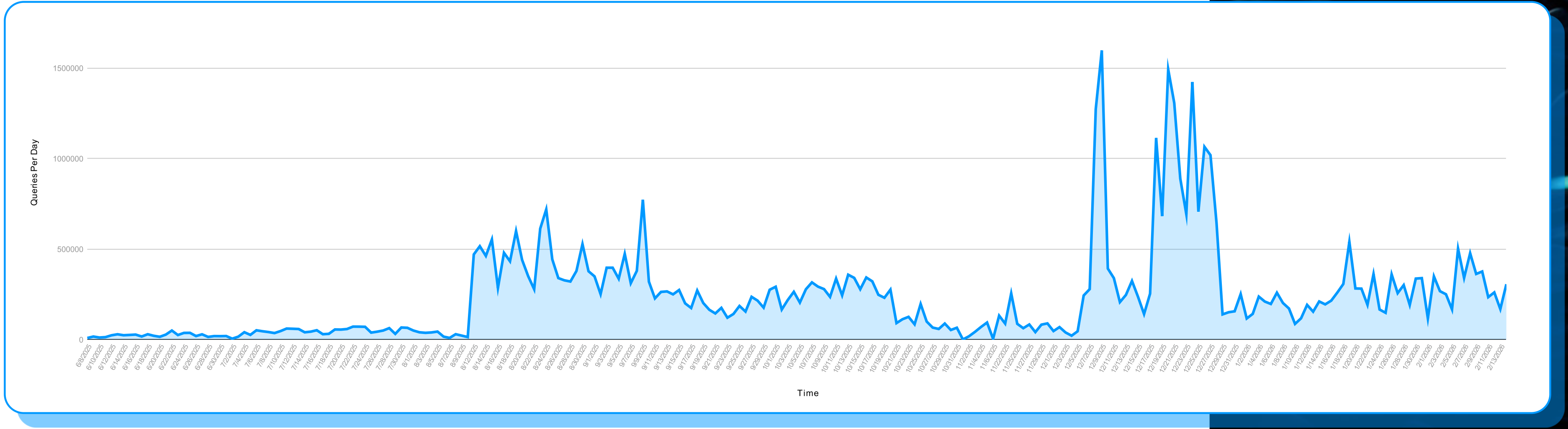
Zero-Day Cryptostealer Uncovered

Hits	TI Sources	Domain	Tags	Subcategory ↑	IPs	Country	Flag	AS Nunber
193	1	slimawriter.com	malware	Cryptostealer	NOANSWER		∅	
5	1	activatorcounter.com	malware	Cryptostealer	188.114.96.3,188.114.97.3	United States	🇺🇸	AS13335
26	1	securebestapp20.com	malv		NXDOMAIN		∅	
25	1	catsdegree.com	malv		NXDOMAIN		∅	
23	2	lagrom.com	malv	mware)	3.64.163.50	Germany	🇩🇪	AS16509
32	1	antepuroloji.com	malware	ducktail	188.114.97.3,188.114.96.3	United States	🇺🇸	AS13335
14	1	mundoframe.com	malware	ducktail	4.21.112.1,104.21.48.1,104.21.80.1,104.21.96.1,104.21.3	United States	🇺🇸	AS13335
20	1	razzball.com	malware	ek_landupdate808	172.67.187.216,104.21.56.197	United States	🇺🇸	AS13335
102	1	cdn-project.info	malware	ek_magnitude			∅	
18	1	fdske.com	malware	ek_zphp	.5.17.71,52.217.49.51,52.216.220.133,52.217.14.235,16	United States	🇺🇸	AS16509
19	1	premio.io	malware	Emotet	162.159.136.54,162.159.137.54	United States	🇺🇸	AS13335
20	1	mycompany.com	malware	Fake Globe Ransomware (Ransomware)	52.5.196.34	United States	🇺🇸	AS14618

Infostealer Detection

ViperSoftX Variants

ViperSoftX is an infostealer malware family that targets sensitive user data, including credentials and browser-stored information. EfficientIP's DNS Threat Intelligence detected new ViperSoftX infostealer variants linked to the previously exposed CryptoStealer campaign. These variants demonstrate how malware infrastructure evolves over time while retaining consistent DNS characteristics. DNS analytics show mid-year and late-year operational peaks, with infrastructure rotating through new domains while maintaining similar resolution and query patterns. These campaigns reinforce the role of DNS as the earliest and most reliable indicator of stealthy malware activity. Additional technical details were published in the EfficientIP blog "DNS Intelligence Detects ViperSoftX Infostealer Variant".



ViperSoftX Activity 2025

AI-driven DNS threat intelligence analyzes ***150B DNS queries and 500K new domains daily*** to reveal infrastructure-level insights

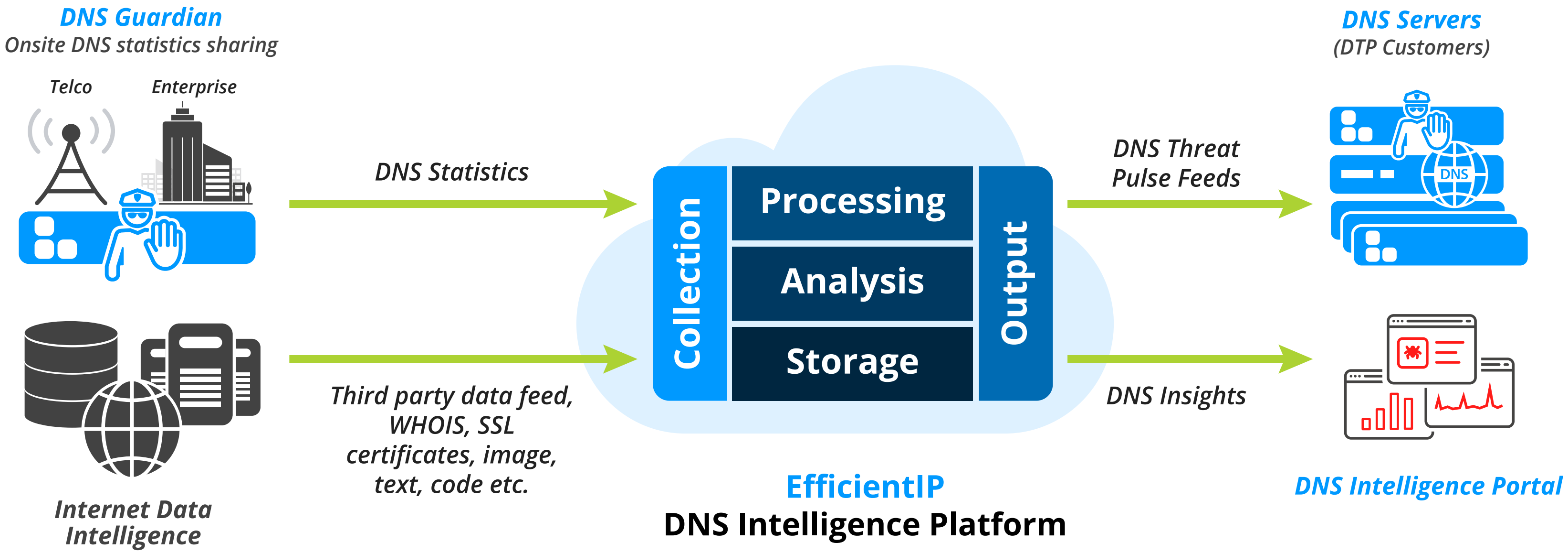
AI-Driven DNS Threat Intelligence Behind These Findings

The insights presented throughout this report are produced by EfficientIP's AI-driven DNS threat intelligence platform, a core component of the 360° DNS Security solution. It is built on a global collection of DNS traffic, which is processed and analyzed to generate DNS analytics and actionable insights at cloud scale and in real time.

Throughout 2025, more than 150 billion DNS transactions per day and over 500,000 newly observed domains per day were processed, allowing the platform to reconstruct how malicious infrastructure is generated, activated, rotated, and abandoned across phishing, DGA, malware, and domain abuse campaigns.

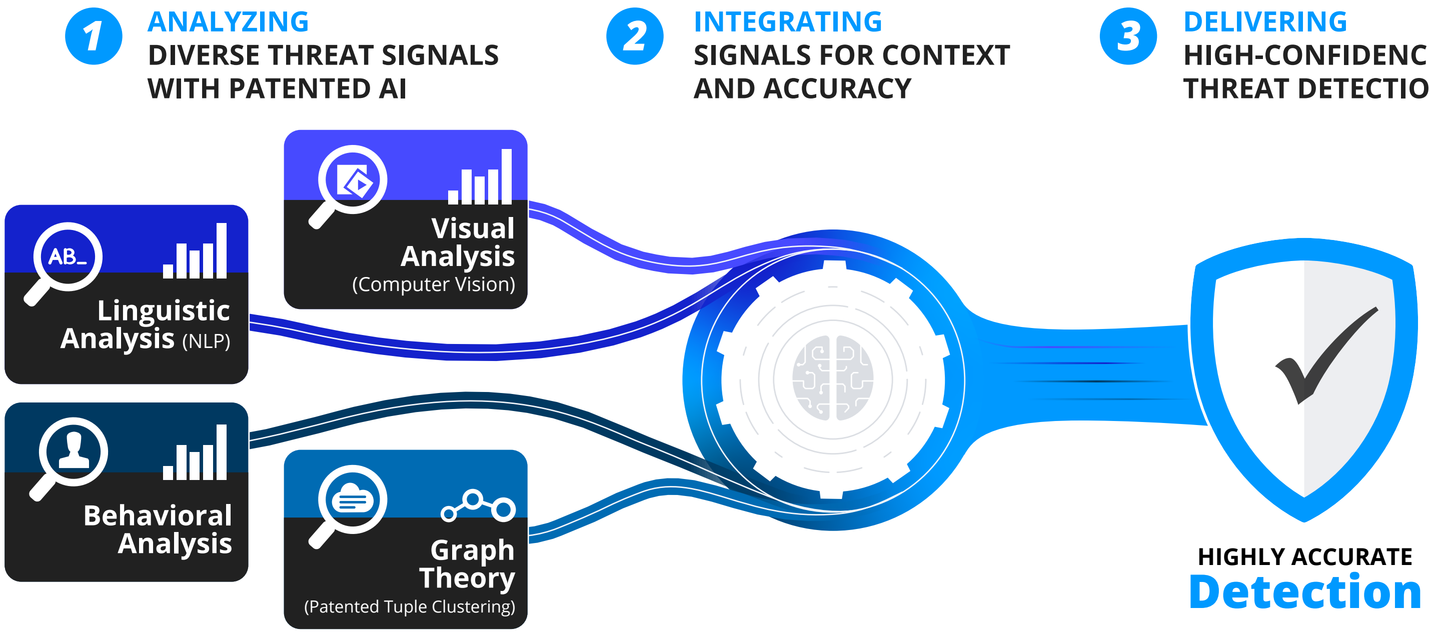
DNS Threat Intelligence Platform

This analysis is powered by a hybrid architecture combining real-time DNS inspection at the network edge with large-scale cloud intelligence. Local systems inspect live DNS transactions to detect anomalies such as unusual query rates, record types, latency, fragmentation, and malformed requests. In parallel, aggregated behavioral indicators and metadata are transmitted to the cloud, where EfficientIP's patented AI/ML technology applies deep behavioral, linguistic, and infrastructure analysis across the global dataset. These two layers continuously reinforce one another, enabling immediate response while maintaining long-term intelligence and historical context.



Integrated Multi-Signal Threat Detection

Multiple AI models operate together as a unified detection pipeline. **Patented Tuple Clustering** identifies DGA-driven malware by grouping clients and domains based on DNS request behavior rather than domain strings, allowing detection even when domains never resolve. **Natural language processing models** analyze domain names and webpage content to detect brand impersonation, typosquatting, and phishing intent, while **computer vision models** inspect page screenshots to identify fraudulent login pages, logos, and deceptive layouts. **Behavioral analytics** profile both client and domain activity over time, detecting anomalies such as burst patterns, tunneling, and dormant infrastructure activation. Statistical and heuristic models complement these techniques by identifying short-lived or low-signal threats that may not trigger deep learning models on their own.



1 ANALYZING DIVERSE THREAT SIGNALS WITH PATENTED AI

2 INTEGRATING SIGNALS FOR CONTEXT AND ACCURACY

3 DELIVERING HIGH-CONFIDENCE THREAT DETECTION

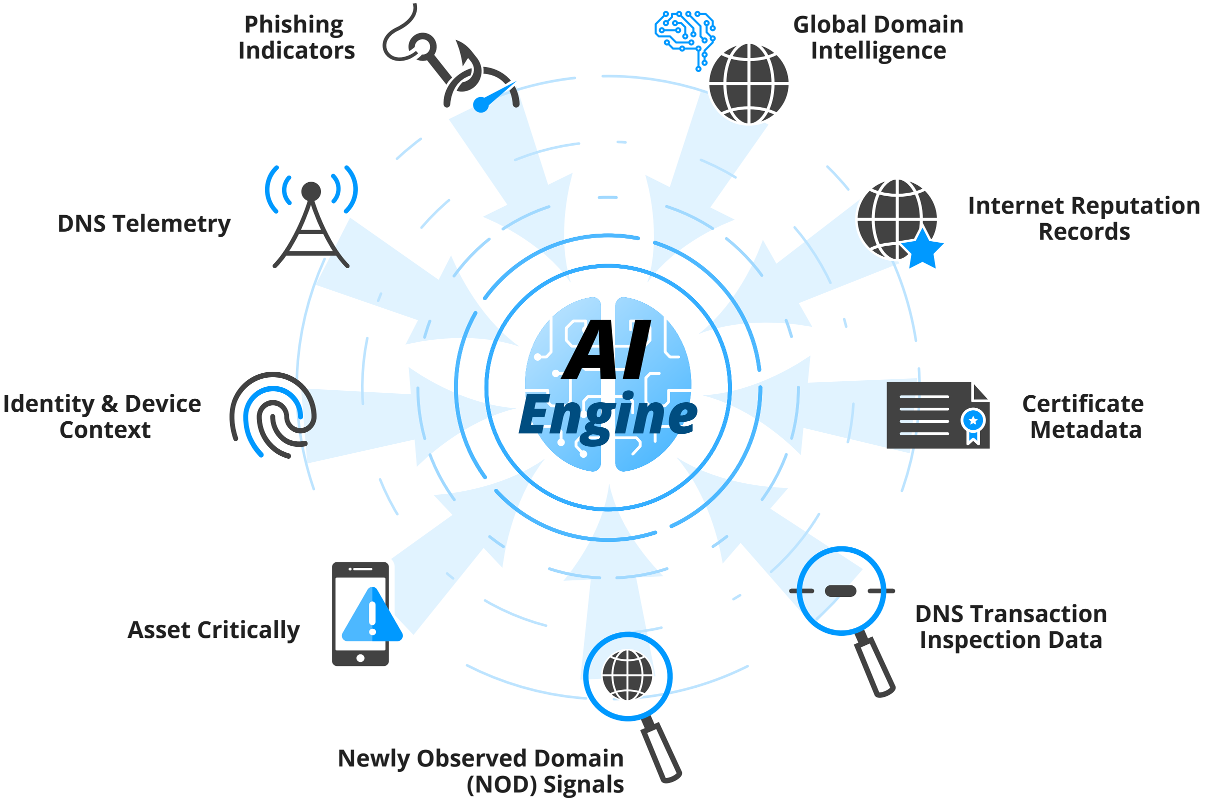
AB_
Visual Analysis (Computer Vision)
Linguistic Analysis (NLP)
Behavioral Analysis
Graph Theory (Patented Tuple Clustering)
HIGHLY ACCURATE
Detection

Integrated Multi-Signal Threat Detection

Multi-Source Threat Intelligence

All of these signals are enriched with contextual data including domain age, hosting and ASN information, certificate metadata, device identity, and Newly Observed Domain intelligence. Approximately five hundred thousand new domains are analyzed daily, with most never appearing in any other threat intelligence source, allowing early identification of emerging phishing, DGA, and malware infrastructure.

The findings presented in this report across phishing, DGA, malware, and domain abuse are the result of this correlation across large datasets and extended time periods. By combining real-time DNS inspection with historical analysis and iterative model refinement, DNS threat intelligence provides the foundation for the campaign-level and infrastructure-level insights documented in this report, offering a durable and data-driven view of the modern threat landscape.

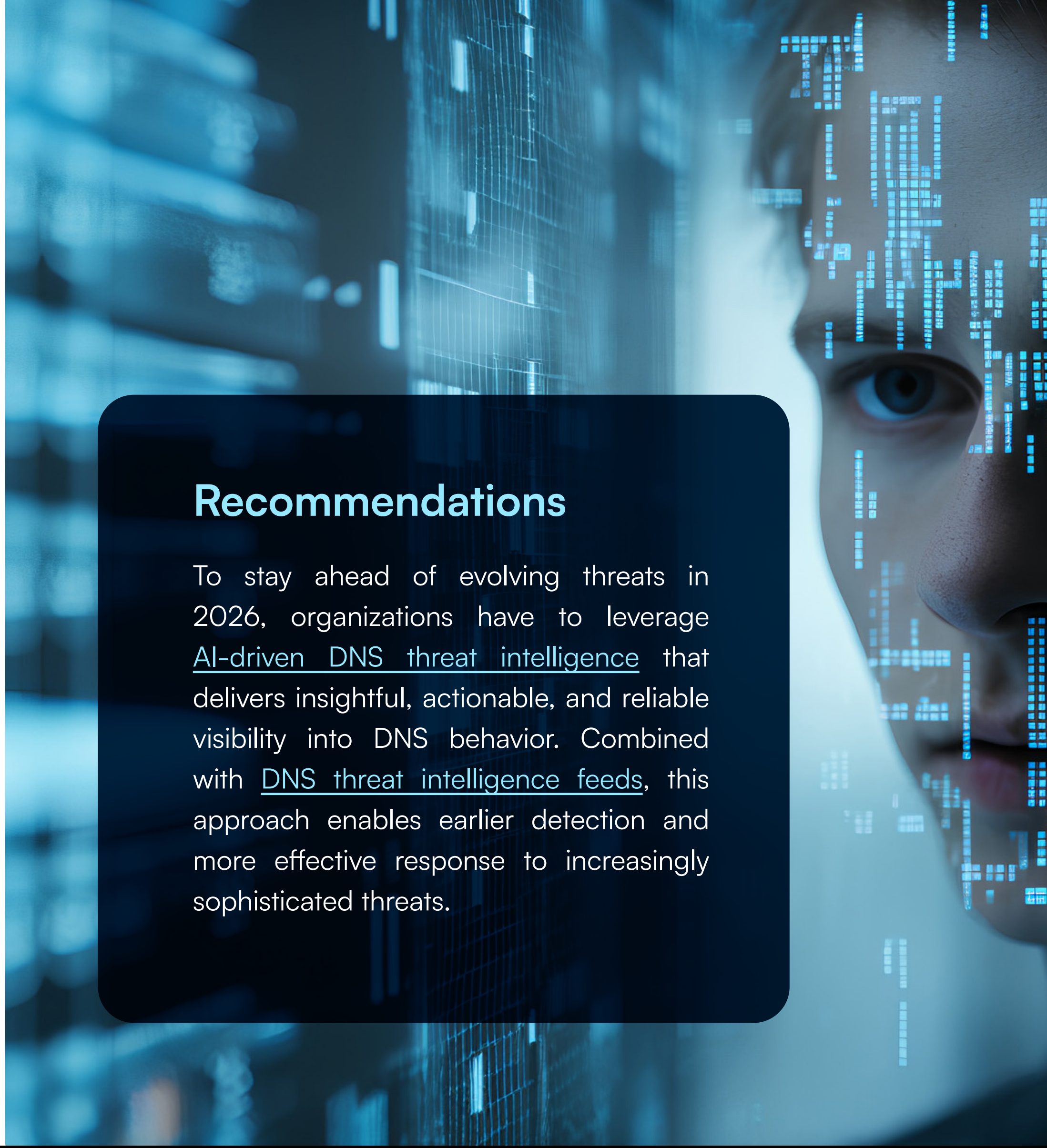

Phishing Indicators
Global Domain Intelligence
DNS Telemetry
Internet Reputation Records
AI Engine
Identity & Device Context
Certificate Metadata
Asset Critically
DNS Transaction Inspection Data
Newly Observed Domain (NOD) Signals

Multi-Source Threat Intelligence

Looking Forward into 2026

The DNS threat intelligence patterns documented throughout 2025 provide a clear indication of how the threat landscape is likely to evolve in 2026. The widespread use of automation, short-lived infrastructure, dormant domains, and burst-driven activation observed across phishing, malware, and DGA activity shows that attackers are already operating at machine speed. These behaviors are increasingly shaped by AI-enabled tooling that allows adversaries to generate, rotate, and activate infrastructure with minimal human intervention.

The findings from 2025 demonstrate that many campaigns expose detectable signals at the DNS layer well before full activation. Domain generation, registration clustering, delayed activation, and brief command-and-control windows consistently appear as early indicators across threat types. As attackers continue to compress operational timelines, the ability to detect and interpret these signals becomes essential for moving from reactive detection toward preemptive cybersecurity.



Recommendations

To stay ahead of evolving threats in 2026, organizations have to leverage AI-driven DNS threat intelligence that delivers insightful, actionable, and reliable visibility into DNS behavior. Combined with DNS threat intelligence feeds, this approach enables earlier detection and more effective response to increasingly sophisticated threats.

To learn more about the EfficientIP DNS Intelligence Center visit:
https://efficientip.com/products/dns-intelligence-center/

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 serves as a first line of defense, enabling teams to protect, detect, and respond to threats. Powered by advanced and AI-patented technologies, its DNS Threat Intelligence platform transforms billions of DNS queries into actionable insights, helping teams detect threats earlier and respond faster.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752