

2026

Threat Landscape Report

The Cybercrime Machine

infoblox

Table of contents

Executive Introduction: Industrialized Cybercrime, Overwhelmed Defenders 03

The Cybercrime Machine: By the Numbers 04

Observations from the Front Line 09

- The Cybercrime Machine 10
- Hidden Malicious Infrastructures 16
- Evolving Lures 21
- Attack Surface Evolution 27

Turning the Tables on Attackers with Preemptive Security 32

- Predictive Intelligence via Protective DNS 32
- Digital Risk Protection 33
- External Attack Surface Management 34

Appendix: Actors and Domain Metrics 36

Terminology Used 41

References 42



Industrialized Cybercrime, Overwhelmed Defenders



Cybercrime is no longer just growing; it is becoming more efficient, automated, and harder to stop. Driven by economics and fueled in part by frontier AI, it has reached an unprecedented scale. The line between financially motivated and state actors has blurred in a complex economy that allows criminals to evade disruption through segmentation and the adoption of commodity services.

The *Infoblox 2026 Threat Landscape Report* examines this reality through insights from trillions of DNS queries, underground criminal transactions, and extensive threat intelligence research. It reveals how attackers scale increasingly sophisticated lures and exploit emerging attack surfaces beyond the reach of traditional security tools.

Our mission remains unchanged: to help organizations stop attacks before they reach users, systems, and data. As cybercrime continues to industrialize, this preemptive approach is no longer just an added layer of defense—it is essential for reducing organizational risk and maximizing the effectiveness of security investments.

This report highlights the research conducted by Infoblox Threat Intel over the past 12 months across three key areas:

Key Threat Intelligence Metrics
Overview of our telemetry, threat actor activity, and strategic insights derived from Infoblox's visibility into the threat landscape.

Frontline Observations
Unique viewpoints on the threat landscape based on threat research from the past 12 months.

New Defense Opportunities
Insights into the effectiveness of Infoblox Threat Intel, along with practical recommendations to help organizations strengthen their defenses.



Dr. Renée Burton
Vice president of Infoblox Threat Intel

The Cybercrime Machine: By the Numbers

Between June 2025 and June 2026, Infoblox monitored the evolving cyber threat landscape through different lenses. Our continuously expanding visibility revealed new findings that highlight the rapid industrialization of cybercrime. Key figures below demonstrate how adversaries increasingly rely on automation, highly scalable infrastructure, and specialized criminal services to execute campaigns with unprecedented efficiency and reach.

- Infoblox's DNS visibility expanded by more than **24% year over year**. During the reporting period, Infoblox observed over **120 million newly registered domains**, of which more than **22% were weaponized or exhibited threat characteristics**.
- **Traffic distribution systems (TDS)** affected the largest share of customers (96%), reflecting their critical role in cybercriminal campaigns by routing victims through traffic brokers, profiling tools, and redirectors before delivering tailored lures.
- **65%** of Infoblox Threat Defense Cloud customers queried domains associated with **residential proxy networks**, highlighting the widespread use of infrastructures for rent that enables malicious activity to blend in with legitimate internet traffic.
- **88%** of threat-related domains were observed in a maximum of one environment, while **44%** were active for just a single day, illustrating both the scale of domain weaponization and the rapid infrastructure rotation.
- The **number of named threat actors increased 67%** year over year, while **unnamed threat clusters grew 97%**, reflecting both increased adversary activity and improved visibility into emerging campaigns.
- **5.3 billion+ unique leaked credentials** and **373,000 brand abuse incidents** were identified, highlighting the scale of digital risk exposure.

- **Enterprise use of AI took a substantial leap.** DNS queries to AI applications increased **158%**, reflecting rapid adoption of AI services while simultaneously expanding the enterprise attack surface.
- Domains generated by **DGA/RDGAs** continue to constitute the largest group of identified threat-related domains (21.5%), demonstrating continued adversarial investment in automating attack infrastructure.
- **Less widely used top-level domains (TLDs)** like .vip, .gdn or .pw can present a higher risk because they often provide threat actors with easier registration processes and are subject to less scrutiny.
- **Scam-related domains increased 62% year over year**, making them one of the fastest-growing threat categories. They enable brand impersonation, identity theft, account compromise, and financial fraud, putting both consumers and enterprises at risk.

Global DNS Visibility

19.1B
average DNS queries/day inspected/day

+24%
YoY growth in DNS queries

1.8B
threat events/day, May 2026

Global Domain Intelligence

120,301,660
new observed domains (distinct SLDs)

2,467,308
new malicious indicators

25,025,603
new suspicious indicators

Threat-Related Domains by Customer Reach

Persistence	1 customer	2–5 customers	6–20 customers	20+ customers
1 day	43.4%	0.6%	0.2%	0.1%
2–7 days	34.8%	2.1%	0.5%	0.3%
8–30 days	1.1%	1.7%	0.3%	0.1%
31–90 days	8.5%	2.7%	0.4%	0.2%
>90 days	0.4%	1.8%	0.5%	0.2%
Total	**88.3%**	**8.9%**	**1.9%**	**0.9%**

Global DNS Visibility

1,112
named actors, June 2026

+67%
YoY growth, named actors

402,216
unnamed clusters, June 2026

+97%
YoY growth, unnamed clusters

Domain Classification and Threat Categories

High-Level Domain Classification	% of Discovered Domains 2026	YoY Growth
Malicious Domains Domains that are confirmed to be involved in cybercriminal activity.	**9.0% +**	**40.0%**
Suspicious Domains Domains that show strong signs of potential malicious activity but have not yet been confirmed as malicious.	**91.0%**	**+5.8%**
↳ **Emergent Domains** Subgroup of suspicious domains that became active after being idle and exhibiting suspicious characteristics.	**30.5%**	**+100.7%**

Discovered Domain Categories and Year-over-Year Change

Threat Categories	% of Discovered Domains in 2026	YoY Growth 6/1/24-6/1/25 to 6/1/25-6/1/26
DGA/RDGA	21.5%	+65.3%
Scam	4.1% +	62.4%
Phishing	4.0% +	54.1%
Lookalikes	2.3% +	30.2%
TDS	1.8%	+28.7%
Parked/Decoy	<1% +	196%
Malvertising	<1%	-42.9%
Stealers/Malware	<1% +	191%
Residential Proxy	<1% +	847%
DNS C2	<1% +	90.1%
Suspicious–Low-Regret Domains	69%	

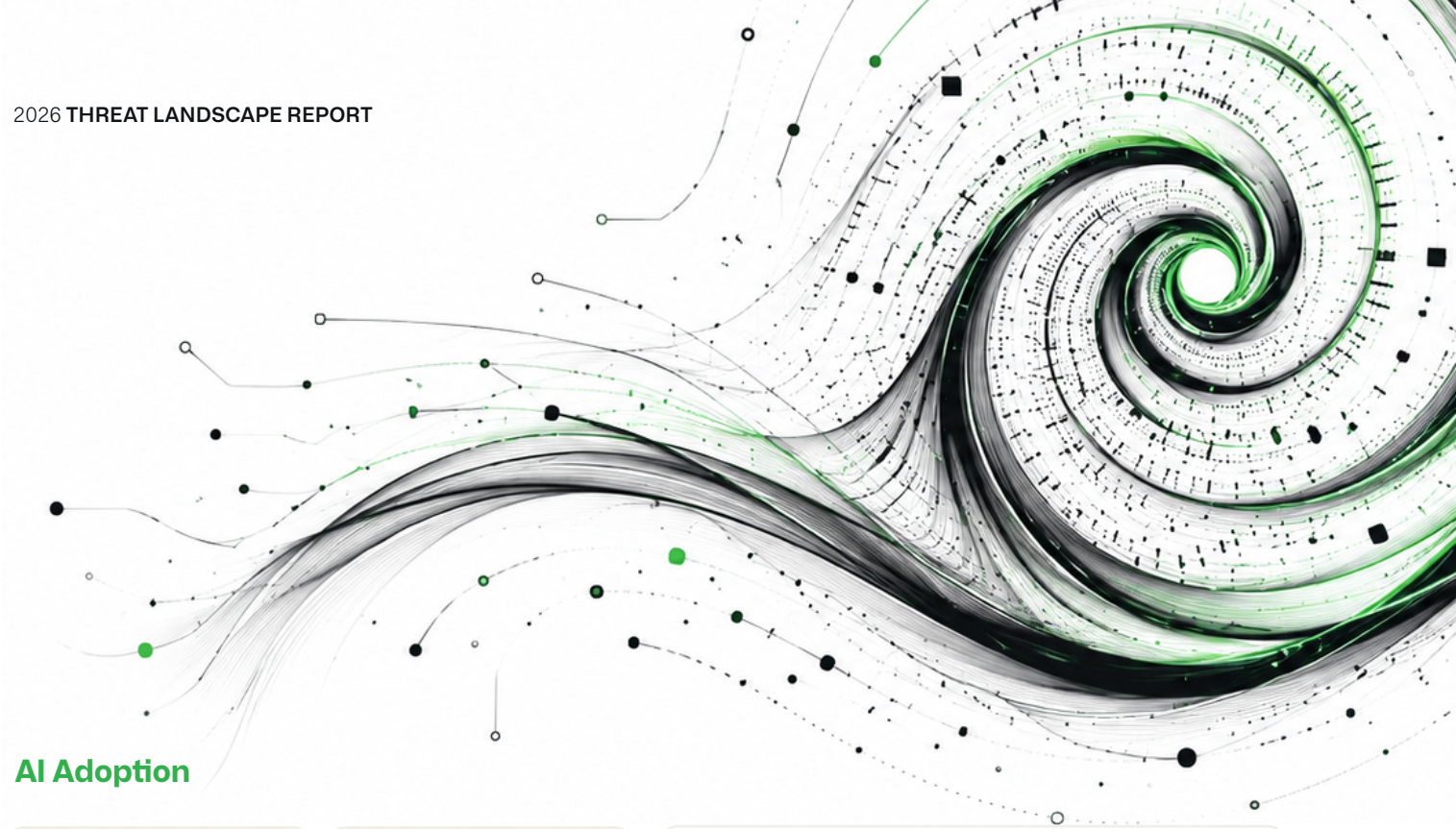
* **Suspicious – Low-Regret Domains:**
Domains with multiple suspicious characteristics that are yet to be confirmed malicious.
For more info, see https://www.infoblox.com/blog/security/getting-in-front-of-threats/

Domain Categories and Customer Prevalence

Threat Categories	Peak Customer Percentage
TDS	96%
Lookalikes	91%
Phishing	73%
Parked/Decoy 5	6%
Malvertising	46%

Threat Categories	Peak Customer Percentage
Scam	43%
RDGA/DGA	43%
Stealers/Malware	38%
Residential Proxy	32%
DNS C2	2.7%

Peak Customer Percentage:
Max daily customers for the single most-queried domain of that type between June 1, 2025–June 1, 2026



AI Adoption

112

AI applications discovered

+159%

AI DNS query growth

TOP 8 AI APPS BY QUERY VOLUME

Cursor · ChatGPT (OpenAI) · Microsoft Copilot
Claude (Anthropic) · ByteDance AI (Doubao/Coze)
Google AI · Codeium/Windsurf

TOP 10 AI SOLUTIONS BY PEAK CUSTOMERS

ChatGPT	98.2%
Microsoft Copilot	96.6%
Claude	93.3%
Google AI	91.3%
Grok AI	78.7%
ElevenLabs	70.6%
Hugging Face	70.4%
Replit	64.4%
Perplexity	62.9%
Sun AI	58.5%

Observations from the Front Line



Between July 2025 and June 2026, Infoblox Threat Intel researched threats across multiple areas, leading to four viewpoints:

View 1: **The Cybercrime Machine**

The criminal services, business models, and operational forces that drive the global cybercrime ecosystem.

View 2: **Hidden Malicious Infrastructures**

The covert networks and infrastructure that adversaries create, compromise, or exploit to enable attacks and evade detection.

View 3: **Evolving Lures**

How attackers are refining their lures, delivery methods, and campaigns to reach and deceive their intended targets.

View 4: **Attack Surface Evolution**

The continuous search for new opportunities within the enterprise where attackers can bypass defenses and maintain an advantage.



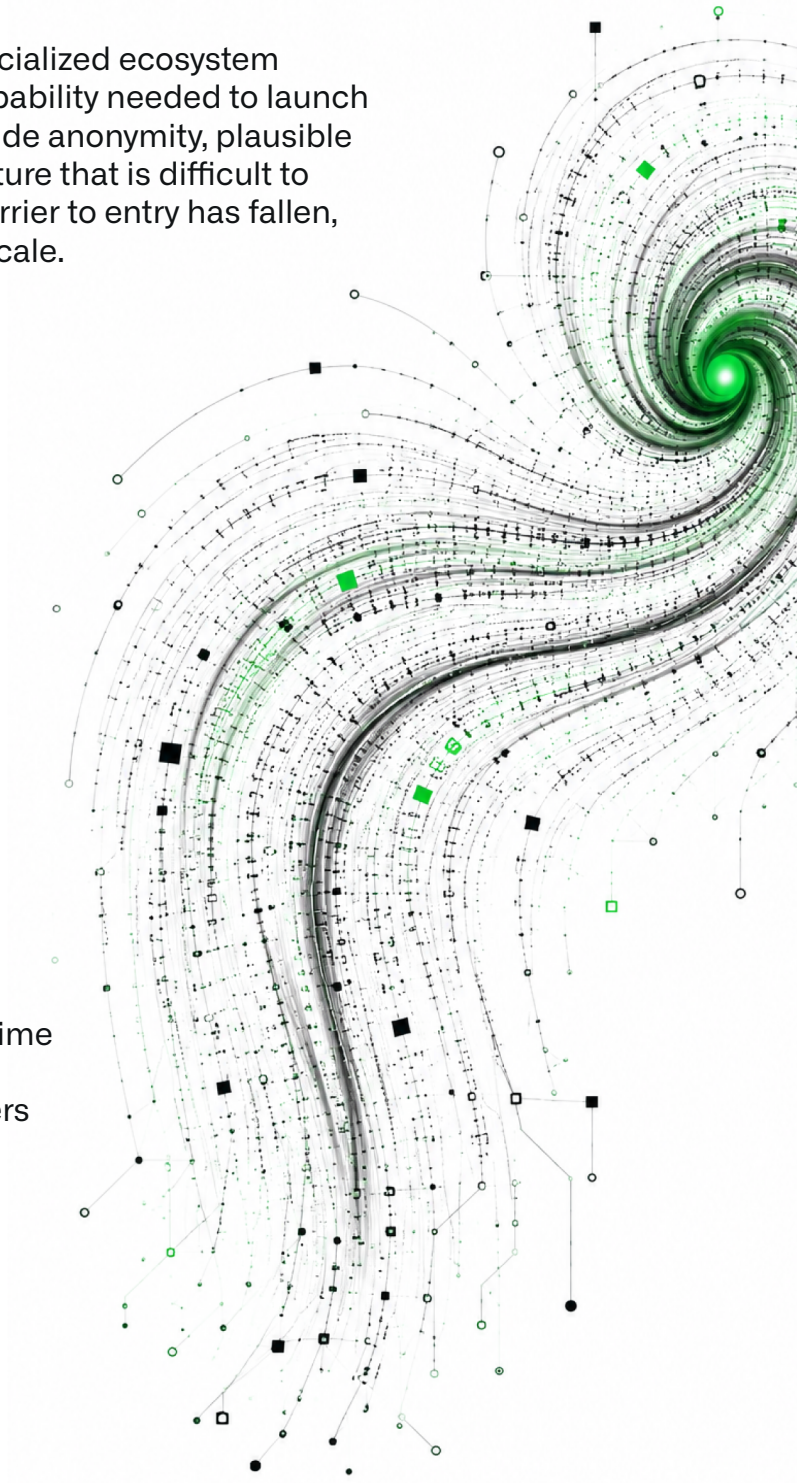
View 1:

The Cybercrime Machine

Cybercrime has evolved into a mature, commercialized ecosystem where criminals can buy or rent nearly every capability needed to launch sophisticated attacks. These services also provide anonymity, plausible deniability, and access to short-lived infrastructure that is difficult to detect, attribute, and disrupt. As a result, the barrier to entry has fallen, enabling even low-skilled actors to operate at scale.



In 2025, reported cybercrime losses in the United States reached **$20.9 billion—a 26% increase over 2024**, according to the FBI's Internet Crime Complaint Center



AI is accelerating this trend by automating reconnaissance, generating convincing lures, and increasing the speed and scale of attacks. As profits attract more participants, the cybercrime ecosystem continues to expand and specialize, allowing attackers to evolve faster than defenders while making traditional, investigation-driven defenses increasingly ineffective.



Figure 1.
Services used by cybercriminals

As cybercriminals target more consumers, enterprises are also increasingly at risk through brand impersonation and fraud. Additionally, once sufficient customer credentials and personally identifiable information (PII) have been leaked to the criminal ecosystem, attackers may reuse the data to extort the organization, create new lures and stage new attacks.

A particularly vulnerable group is executives and other VIPs, whose identities are often exploited in impersonation-based fraud, business email compromise (BEC), and social engineering schemes. Service providers and telecommunications companies are likewise part of the victim landscape, as threat actors frequently abuse their legitimate platforms and infrastructure to facilitate attacks.



Inside the Cybercrime Services:
Recent Research by Infoblox Threat Intel

By analyzing DNS activity at scale, Infoblox Threat Intel recently discovered several examples of services enabling large scale cybercrime services.

Penguin
One-Stop Shop for Pig-Butchering Operators

Penguin is a crime-as-a-service marketplace that provides the infrastructure and services needed to conduct pig-butchering and other online fraud schemes. Offerings include:

Telecom and Infrastructure:
Pre-registered SIM cards, 4G/5G routers, IMSI catchers, and disposable devices, giving scammers infrastructure for account creation, OTP reception, and victim contact while hiding true origins.

Fake Identities and Social Engineering:
Image packs from real social media profiles (“character sets”) and fraud kits with scripts and assets for creating convincing fake personas and scam narratives.

Fraud Management and Payments:
SCRM AI, a platform for managing large volumes of accounts and victim interactions, and BCD Pay, a payment platform linked to Bochuang Guarantee that supports scam payments and money-laundering activities.

DNS evidence shows that Penguin’s customers use shared backend services—including CRM platforms, fake investment websites, and mobile app download infrastructure—allowing multiple scam groups to use the same systems.

FaiKast
AI-Generated Assets to Lure Victims

FaiKast is a threat actor cluster that uses AI-generated fake news broadcasts and deepfake videos to lure victims into fraudulent investment platforms. The FaiKast campaign sits on top of a broader adtech platform (Keitaro) that leverages domain cloaking, conditional routing, registered domain generation algorithm (RDGA). The actor also customizes domains for a victim's country or language to make scams look more legitimate and improve their success rate.

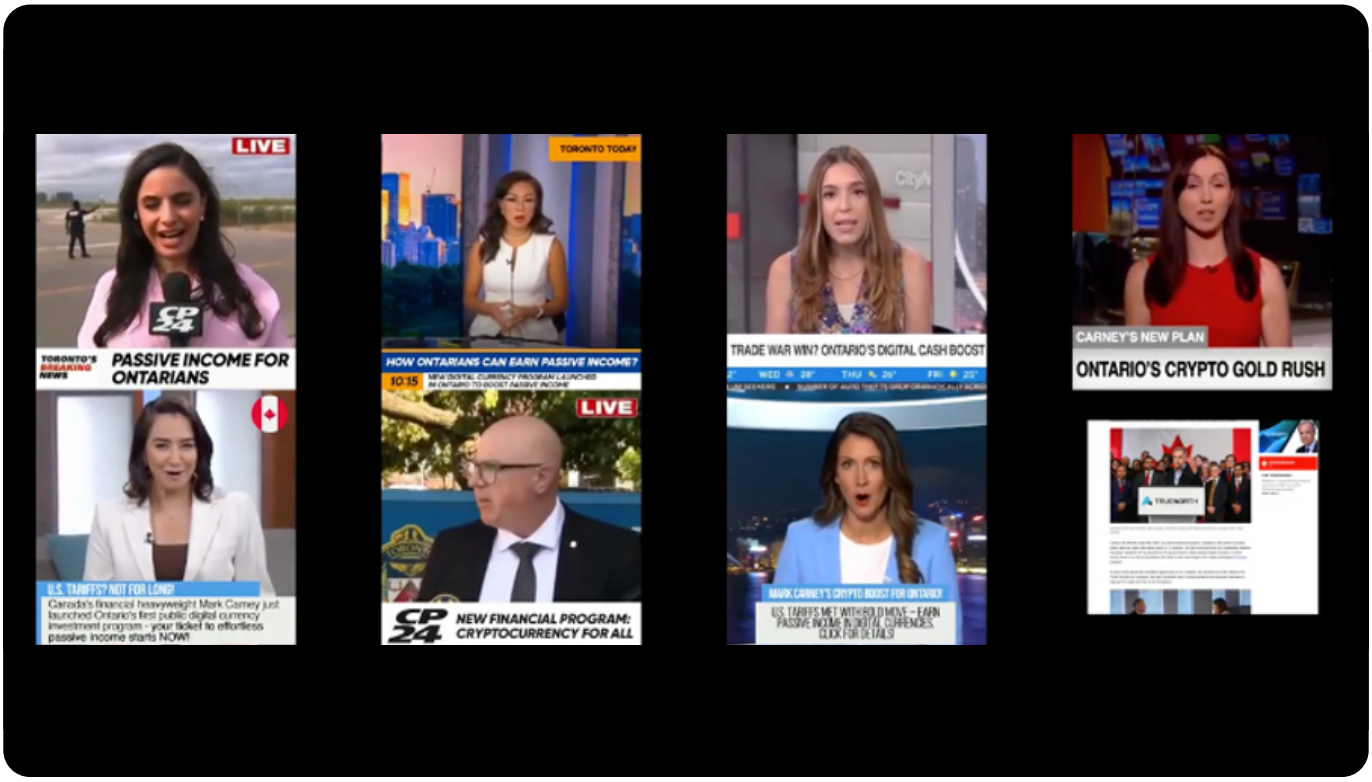


Figure 2. FaiKast news anchor deepfakes

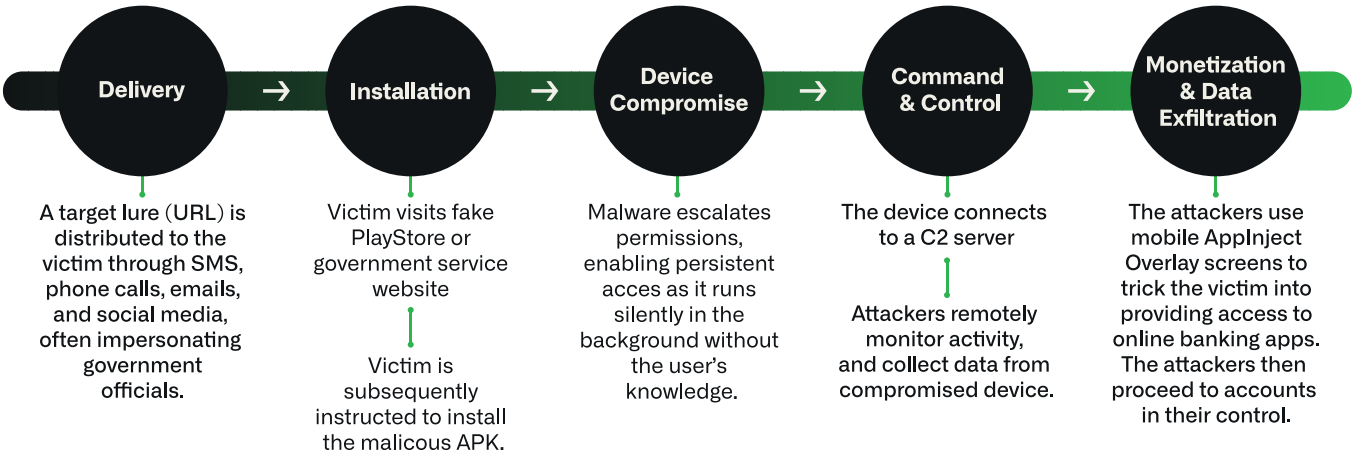
Credential and Data Theft at Scale

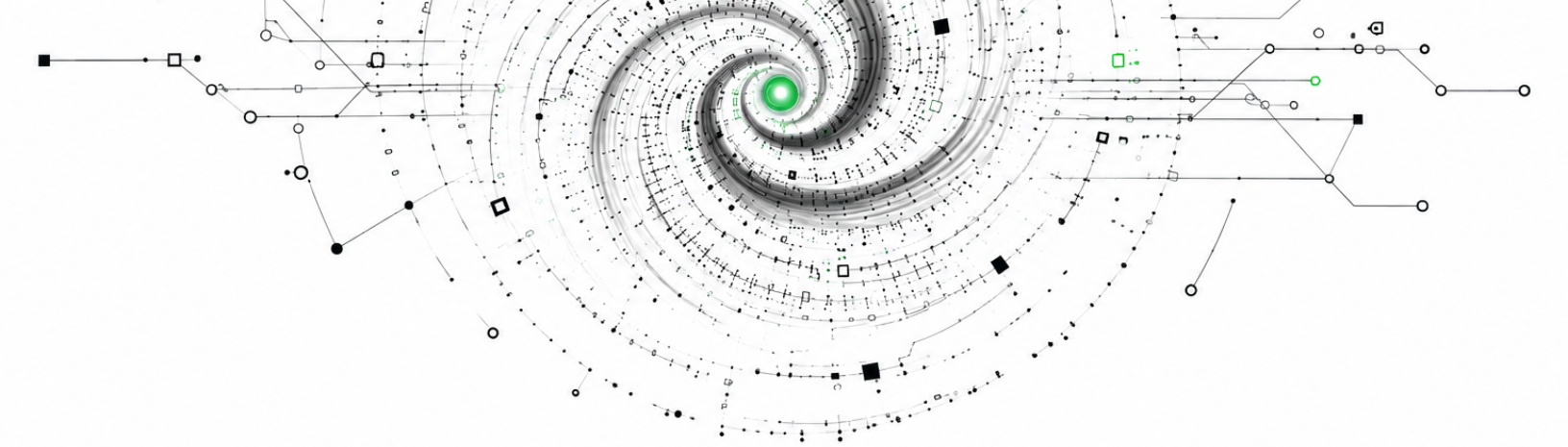
An Android banking trojan malware-as-a-service (MaaS) platform provides cybercriminals with the tools and infrastructure needed to steal banking credentials and personal data at scale. The malware captures banking credentials, SMS one-time passwords (OTPs), call content, biometrics, contacts, and other sensitive information, enabling account takeover, identity theft, and long-term fraud.

The MaaS operator rents or sells malware, command-and-control (C2) panels, Android packaging tools, and supporting infrastructure to multiple scam groups, turning credential theft into an on-demand service.

The platform's C2 infrastructure relies primarily on .top domains (39 of 42 active C2 domains), with a smaller number using .xyz, .vip, and .pro. These domains are consistently registered through Domain International Services and Namemart, and use DomainNameDNS name servers.

Attacks begin by luring victims to fake websites that impersonate trusted banks or government services. From there, a customizable malware kit delivers one of several Android banking trojan variants, allowing operators to tailor campaigns to different targets.





In this attack chain, adversaries are no longer stealing just credentials—they are stealing entire digital identities. By capturing SMS OTPs, device fingerprints, contacts, and facial biometrics through fake know-your-customer (KYC) processes, they can bypass identity verification and enable long-term account compromise and fraud.

Harvest and Concealment: Vault Viper's iGaming Ecosystem

Vault Viper operates a white-label online gambling platform that helps criminals launder money and move illicit funds across borders while disguising them as legitimate gambling transactions. The operation relies on a massive, constantly changing infrastructure with tens of thousands of domains and more than 1,000 nameservers supporting gambling sites, malware infrastructure, and proxy services.

DCloud Uni-App Infrastructure stack

DCloud Uni-App is a legitimate cross-platform development framework that has become a key enabler of industrialized online fraud. Threat actors use shared templates and reusable code to rapidly launch scam campaigns, significantly reducing the time and cost of creating new operations.

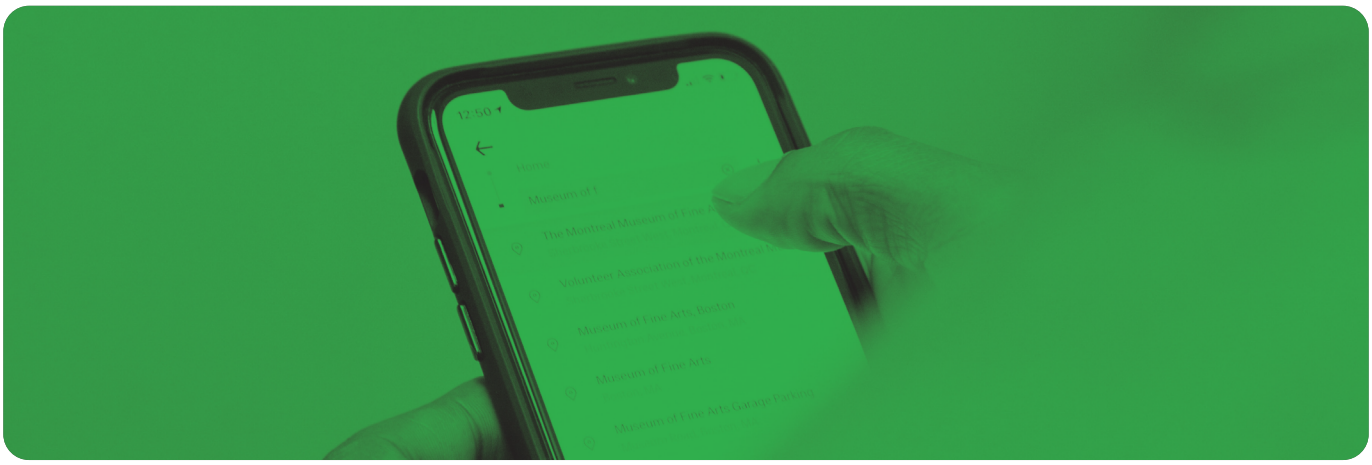
These campaigns include fake cryptocurrency exchanges, pig-butchering schemes, phishing sites, wallet drainers, gambling portals, and fraudulent investment platforms. Victims are typically lured through WhatsApp, Telegram, social media, and other messaging platforms before being directed to convincing websites designed to steal money or credentials.

Since January 2024, Infoblox has identified more than 18,000 DCloud-based scam domains accessed by approximately 985 enterprise customers. Although these campaigns primarily target consumers, they routinely expose enterprise networks as employees encounter scam links during personal browsing on corporate or personal devices.

View 2:

Hidden Malicious Infrastructures

Attackers increasingly rely on legitimate-looking and hidden infrastructures to evade detection. Using DNS intelligence, Infoblox Threat Intel exposes the hidden internet infrastructure that powers modern cybercrime—a key differentiator of our research. Over the past 12 months, our team has published research uncovering previously unseen attacker infrastructure and revealing how cybercriminals operate. Here are a few highlights:



Abused Adtech

Adtech platforms were designed to optimize digital advertising by routing traffic and directing users to relevant content. Threat actors now exploit the same capabilities to profile visitors based on their device, location, and behavior, delivering scams or malware only to intended targets while showing harmless content to everyone else.

Using TDSs and cloaking, attackers hide malicious activity behind trusted advertising domains and redirect chains, making detection difficult. On June 18, the FBI warned that TDSs are increasingly being usedto facilitate ransomware and financial fraud.

In March 2026, Infoblox Threat Intel and Confiant revealed how threat actors abuse Keitaro Tracker, a legitimate advertising platform, to scale scam and malware campaigns. Keitaro enables attackers to selectively target victims based on factors such as location, device, or referral source, while hiding malicious content from security researchers and automated scanners.

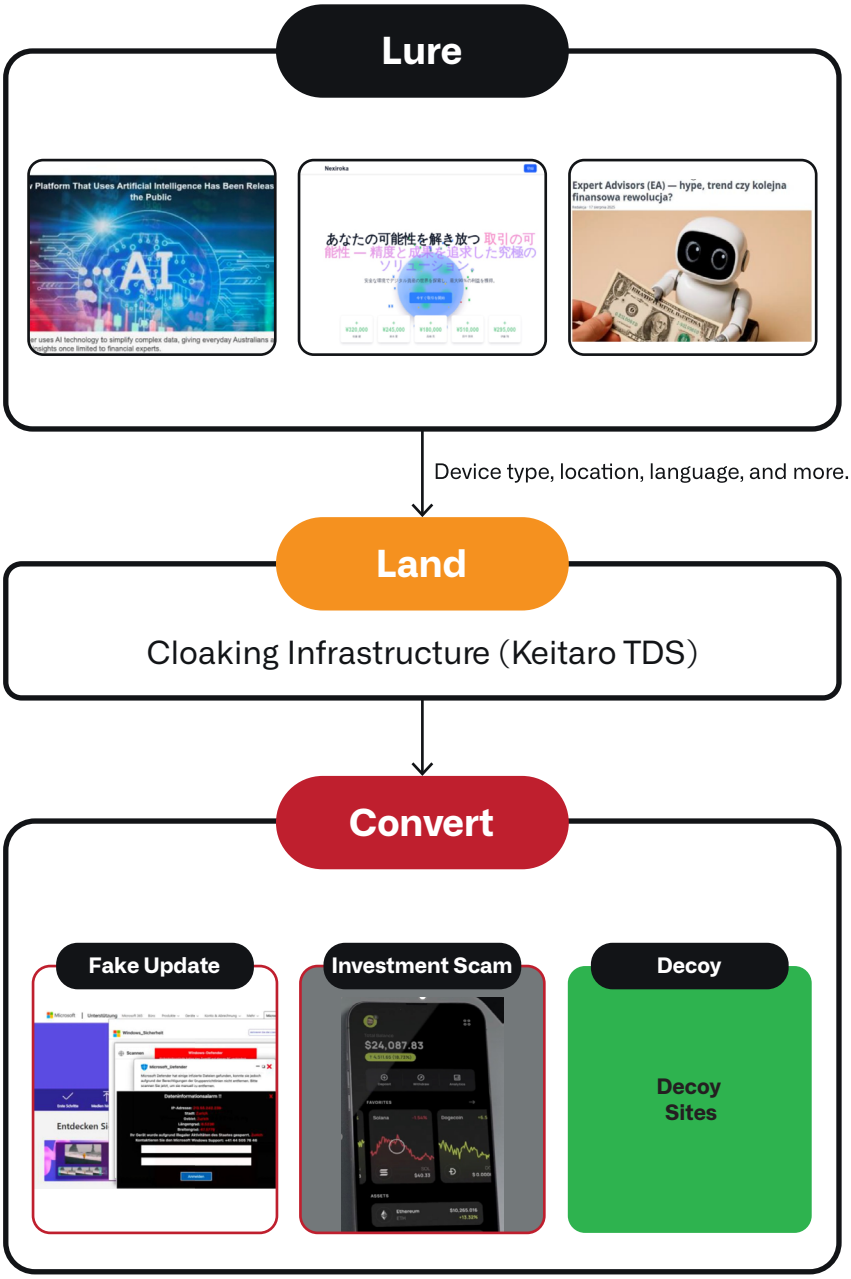


Figure 3. Keitaro Tracker abused to deliver lures.

Actors Advantages

Track Campaigns
Monitor where traffic comes from (ads, affiliates, social media)

Cloaking
Collect device type, location, language, and more

Send visitor to different landing pages based on rules

Manage and Optimize Funnels
Advance lures for effectiveness

Automate and increase intensity of attacks

The scale of the abuse is both significant and persistent. During a four-month study beginning in October 2025, researchers identified approximately 15,500 domains linked to malicious Keitaro deployments. More than 9,000 of these domains were registered specifically for use in the campaigns.

These domains were used across multiple delivery channels, including online advertising, spam email campaigns, compromised websites, and other traffic sources, highlighting the broad reach and adaptability of the operation.

Bulletproof Hosting

Bulletproof hosting providers offer a highly resilient environment where malicious infrastructure can operate with minimal risk of takedown or disruption. By focusing on anonymity, ignoring abuse reports, and enabling rapid infrastructure migration, these networks help cybercriminals sustain phishing, fraud, malware, and other illicit operations at scale.

In February 2026, Infoblox Threat Intel exposed a long-running campaign that compromised internet routers and hijacked DNS settings, redirecting victims through attacker-controlled infrastructure hosted by Aeza International, an OFAC-sanctioned bulletproof hosting provider. By controlling DNS, the attackers effectively gained a "steering wheel" for every internet connection originating from the compromised network.

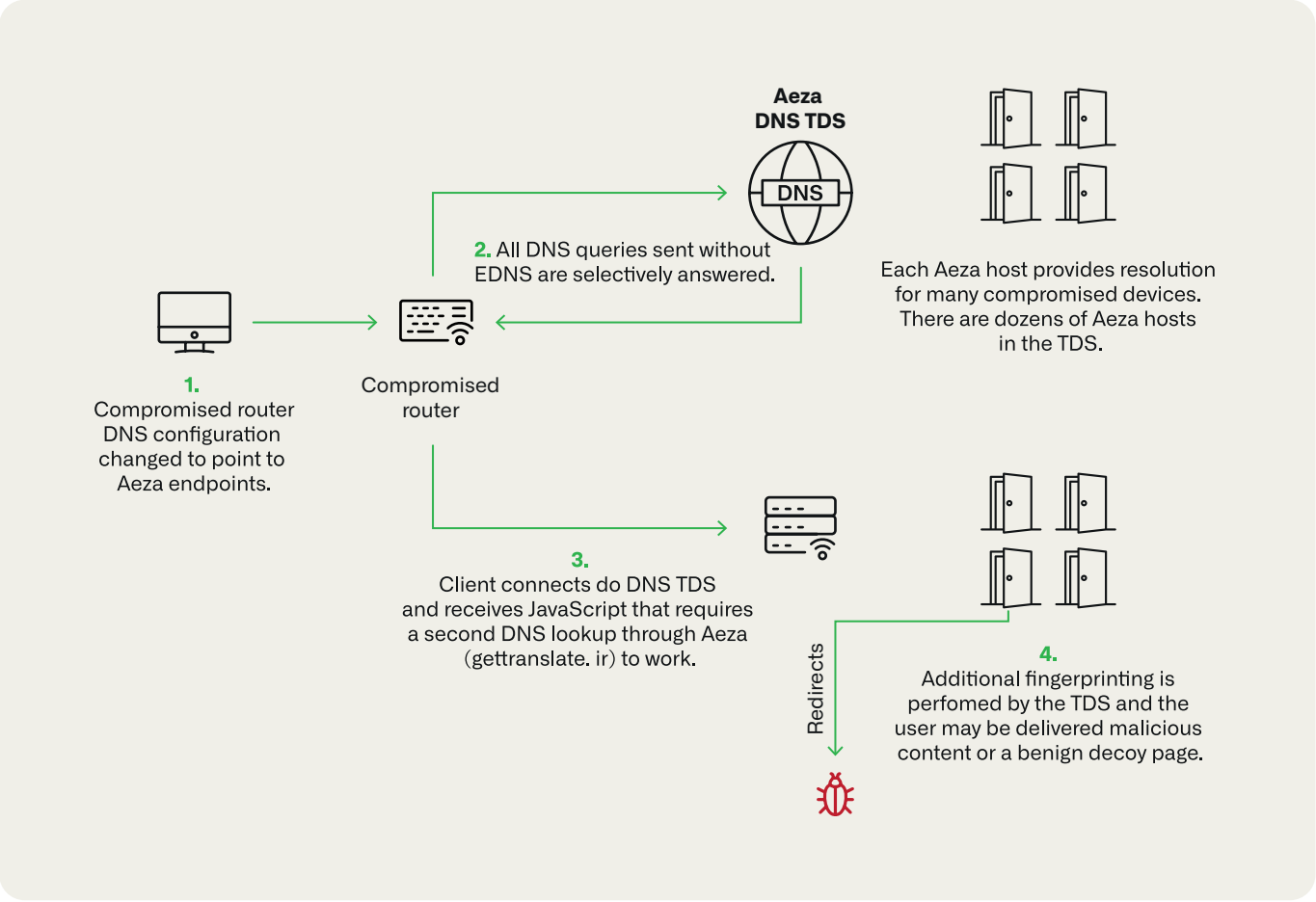


Figure 4. Two-part TDS hosted in Aeza International

Abuse of Trusted Internet Infrastructure

Actors abuse trusted infrastructure like CDNs, registrars, reverse DNS infrastructure, and hosting providers because trust raises success rates, cuts costs, hides activity, improves resilience, and sometimes gives them privileged access to users or networks that would otherwise be hard to reach.

Abuse of .arpa Research

The .arpa TLD was originally created during the transition from manually maintained host tables to the DNS. Although its original purpose is no longer needed, .arpa was retained and repurposed as a critical part of internet infrastructure. Today, it is primarily used for technical networking functions such as reverse DNS lookups, which map IP addresses back to domain names.

Despite its infrastructure-focused role, threat actors have found ways to abuse the .arpa namespace. By obtaining IPv6 address space and control of associated reverse-DNS zones, attackers created DNS records that made spam-email links appear more legitimate. When victims clicked links they were redirected through distribution systems to short-lived phishing pages, scams, or other malicious content. By hiding behind trusted .arpa infrastruture, attackers were able to exploit the limited scrutiny often applied to the .arpa namespace.

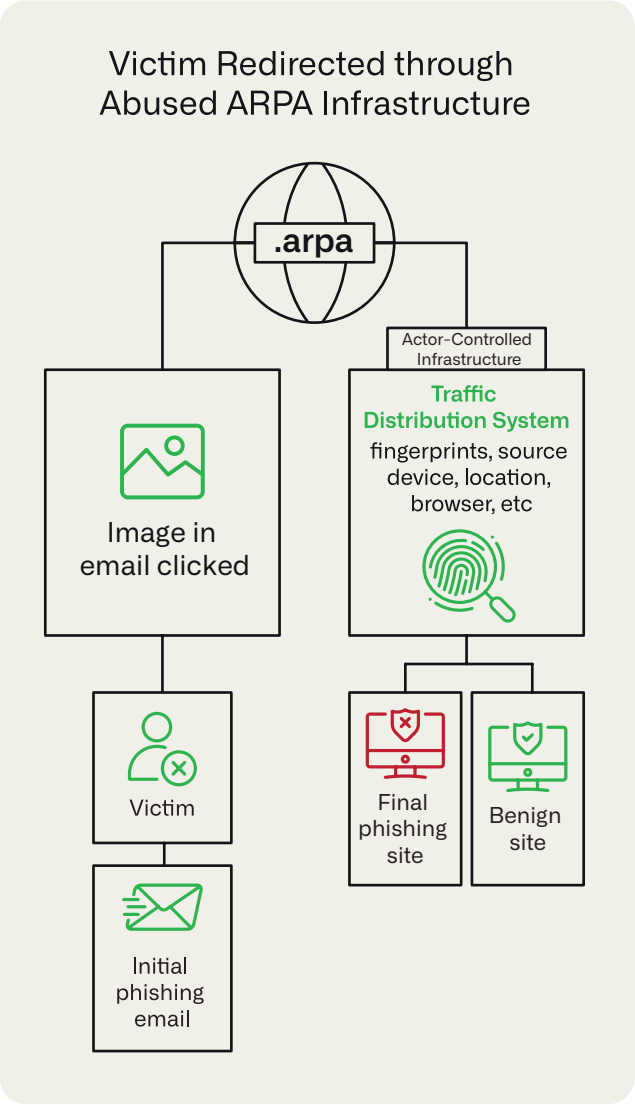


Figure 5. Abuse of .arpa redirecting victims to actor-controlled infrastructure

International Revenue Share Fraud Operation Abuses Telco Providers

In 2026, Infoblox Threat Intel uncovered a fake CAPTCHA scam linked to International Revenue Share Fraud (IRSF). The scam tricks mobile users into sending expensive international text messages by presenting fake "prove you're human" verification pages. While victims believe they are completing a simple CAPTCHA, their actions silently trigger SMS messages to premium-rate international numbers. In one observed case, a single interaction generated around 60 text messages, costing the victim approximately $30. Figure 6 shows a partial sequence recorded on our research device in February 2025, and video of a full "user experience" is here.

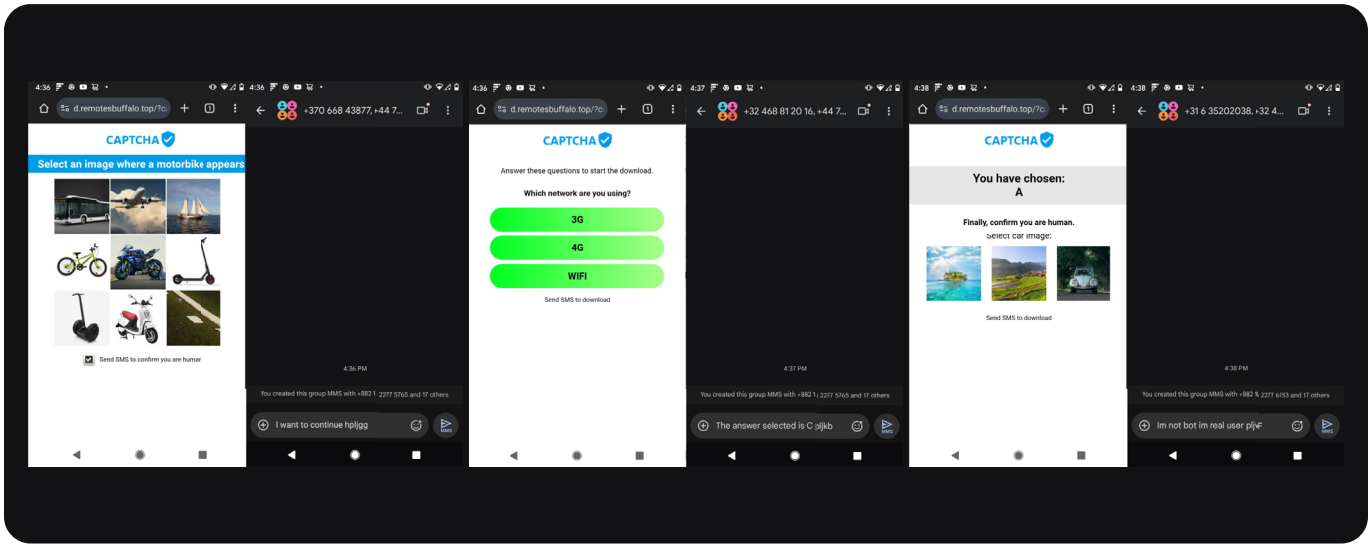


Figure 6. When a user encounters this IRSF actor, they will be taken through a series of fake CAPTCHAs, each requiring an SMS message to prove they are human. The images demonstrate a partial sequence of this experience.

The operation uses traffic-filtering technology to identify and target mobile users, while redirecting others to gambling sites, adult-content scams, or push-notification schemes. Behind the scam is a network of fake CAPTCHA pages, premium-rate numbers, and TDSs spanning at least 17 countries. The campaign highlights how cybercriminals combine simple social engineering with automated infrastructure to generate revenue at scale.

View 3:

Evolving Lures

Attackers use AI to make phishing or scams more targeted, convincing, and scalable. AI-generated content allows them to quickly create personalized lures that improve success rates while making campaigns harder to detect. Over the past 12 months, Infoblox Threat Intel uncovered several ways cybercriminals evolved their luring techniques. Here are a few examples:

Perfecting the Lure

Brand impersonation remains one of the most effective phishing techniques, but attackers are changing their approach. Rather than relying on lookalike domains that include a company's name, they are creating highly convincing phishing pages that closely resemble legitimate websites. This shift is reflected in a 12-month analysis of individual customer phishing incidents, which found that 71% of discovered phishing URLs did not include the impersonated brand name in their domains. Instead of using deceptive domains, attackers focus on realistic branding, logos, and user experiences that make fraudulent sites appear trustworthy.



71% of customer phishing incidents involved URLs with no brand mentioned in the domain, relying instead on convincing website design to deceive users.

In June 2026, Infoblox took part in an international takedown of SocGholish (TA569). The group makes its lures more convincing by showing fake browser-update prompts directly on the legitimate websites that victims are trying to visit. Because the prompt appears inside a trusted site, it looks far more believable than a separate download page.

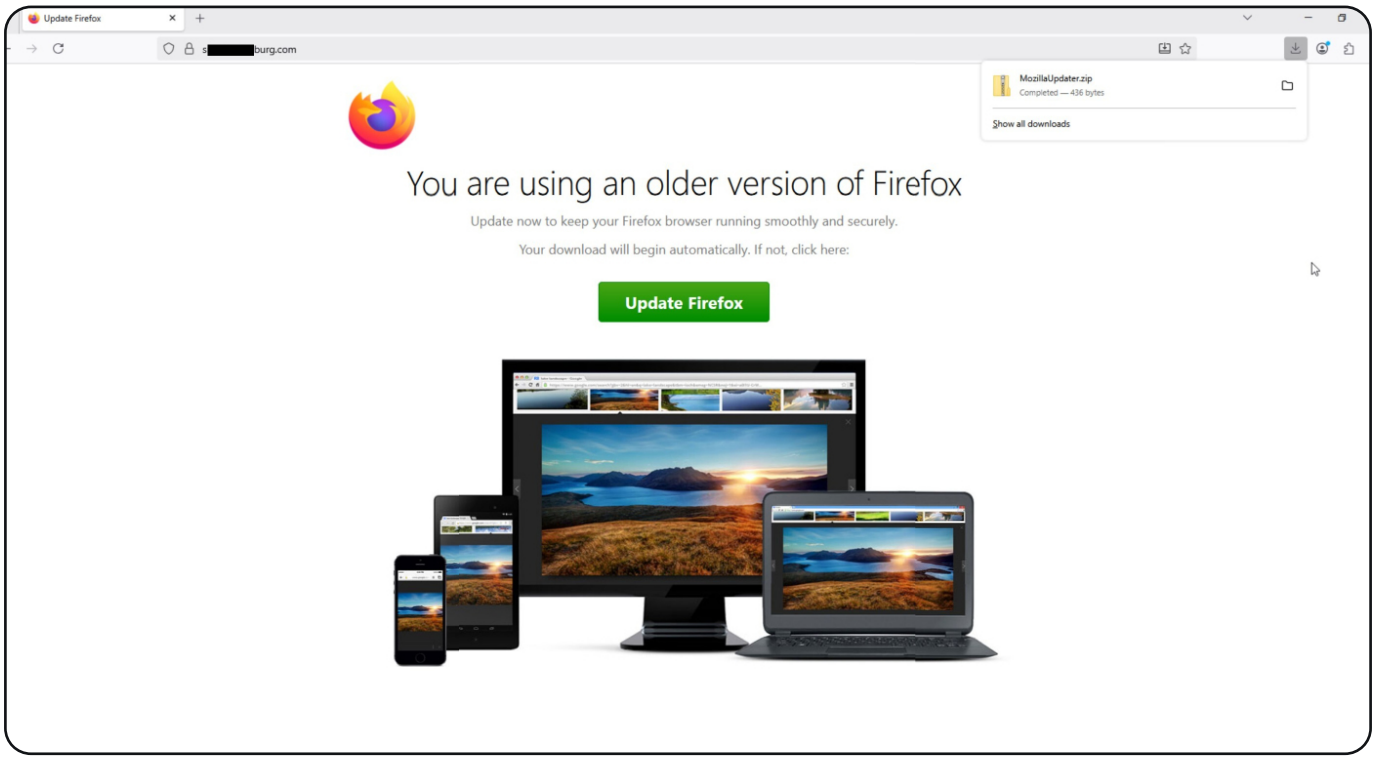


Figure 7. SocGholish Fakeupdate template triggered in Firefox on June 11, 2026

SocGholish also uses device fingerprinting and domain shadowing to evade detection. In domain shadowing, attackers who gain access to a real domain's DNS or registrar account quietly create malicious subdomains under that legitimate domain. This lets them hide behind a trusted parent domain for long periods, making phishing links look authentic and takedowns much harder.

Selective Targeting

Attackers are moving away from broad “spray-and-pray” campaigns and focusing on carefully selected victims. By delivering malicious content only to specific targets, they leave fewer traces behind, making campaigns harder for security teams, email providers, and researchers to detect.

One example is Detour Dog, a threat actor investigated by Infoblox Threat Intel in 2025. Detour Dog evaluates visitors to compromised websites and redirects only selected victims to malware such as Strela Stealer. Everyone else sees the legitimate website, helping the operation remain hidden. Combined with DNS-based C2, bulletproof hosting, and abuse-tolerant registrars, this approach creates resilient infrastructure that is difficult to identify and disrupt.

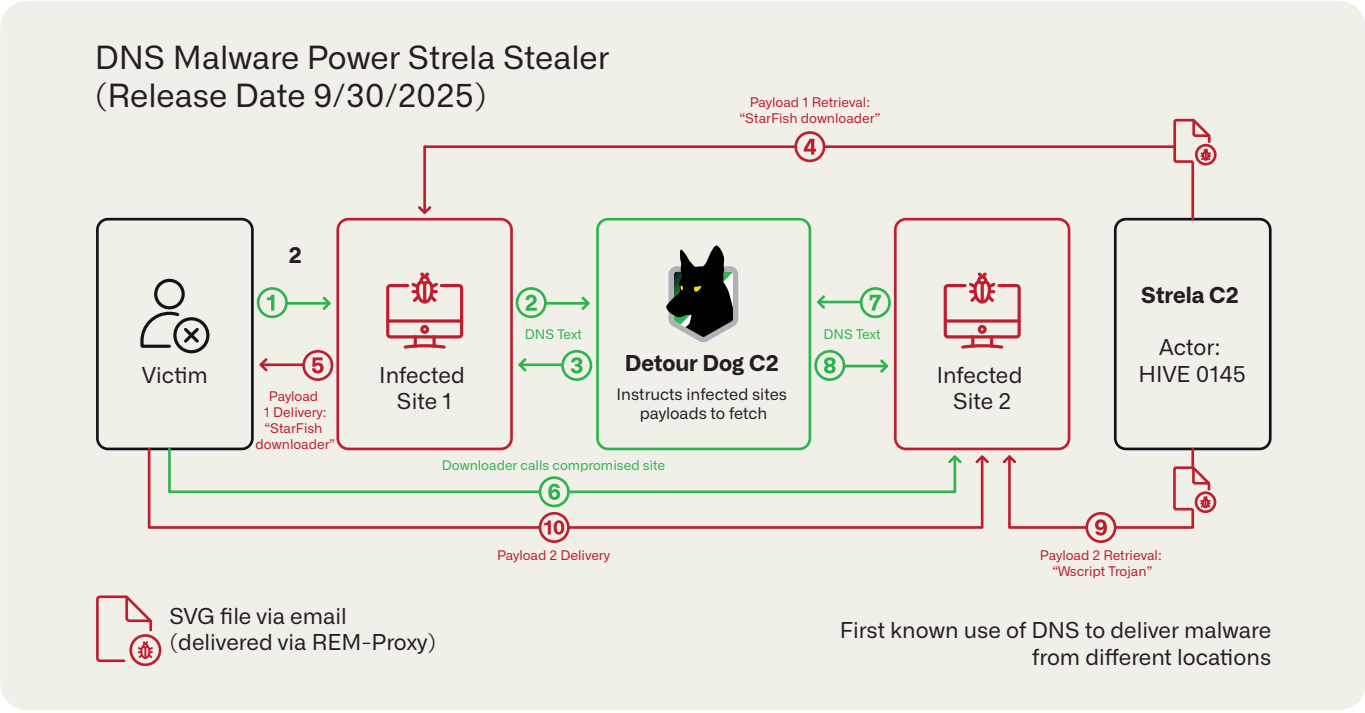


Figure 8. DNS usage to redirect victims

1. Initial Trigger: The victim opens a malicious document and calls an infected domain.
2. DNS TXT Query: Site 1 sends a DNS TXT request to the Detour Dog C2 server.
3. C2 Response: The Detour Dog name server returns a TXT record with instructions to fetch Payload 1.
4. Payload Retrieval: The site uses curl to retrieve the payload part 1.
5. Payload Delivery: The compromised site relays the payload to the victim.
6. Second-Stage Callout: The payload downloaded in part 1 contacts another compromised domain.
7. Second DNS TXT Query: The second site also sends a TXT request to the Detour Dog C2.
8. Second C2 Response: The name server returns another Strela C2 URL.
9. Second Payload Retrieval: The site fetches the next payload from the Strela C2 server.
10. Second Payload Delivery: The payload is delivered as a ZIP archive containing a Wscript trojan believed to be StarFish.

Important: 95% of visits to Infected Site 1 serves benign content. Only visitors who match the ideal target profile are routed into the victim funnel.

Personalized via Mobile Devices

As people increasingly use the same mobile devices for both work and personal activities, smartphones have become a prime target for cybercriminals. Attackers are taking advantage of this behavior by creating highly personalized lures that appear relevant and trustworthy to individual victims.

Recent examples include stolen iPhone smishing campaigns, where attackers send SMS or WhatsApp messages to the contact number displayed on a lost device's lock screen. Victims are directed to convincing Apple lookalike pages customized with personal details such as their name, email address, device information, and location, prompting them to enter their Apple ID credentials.

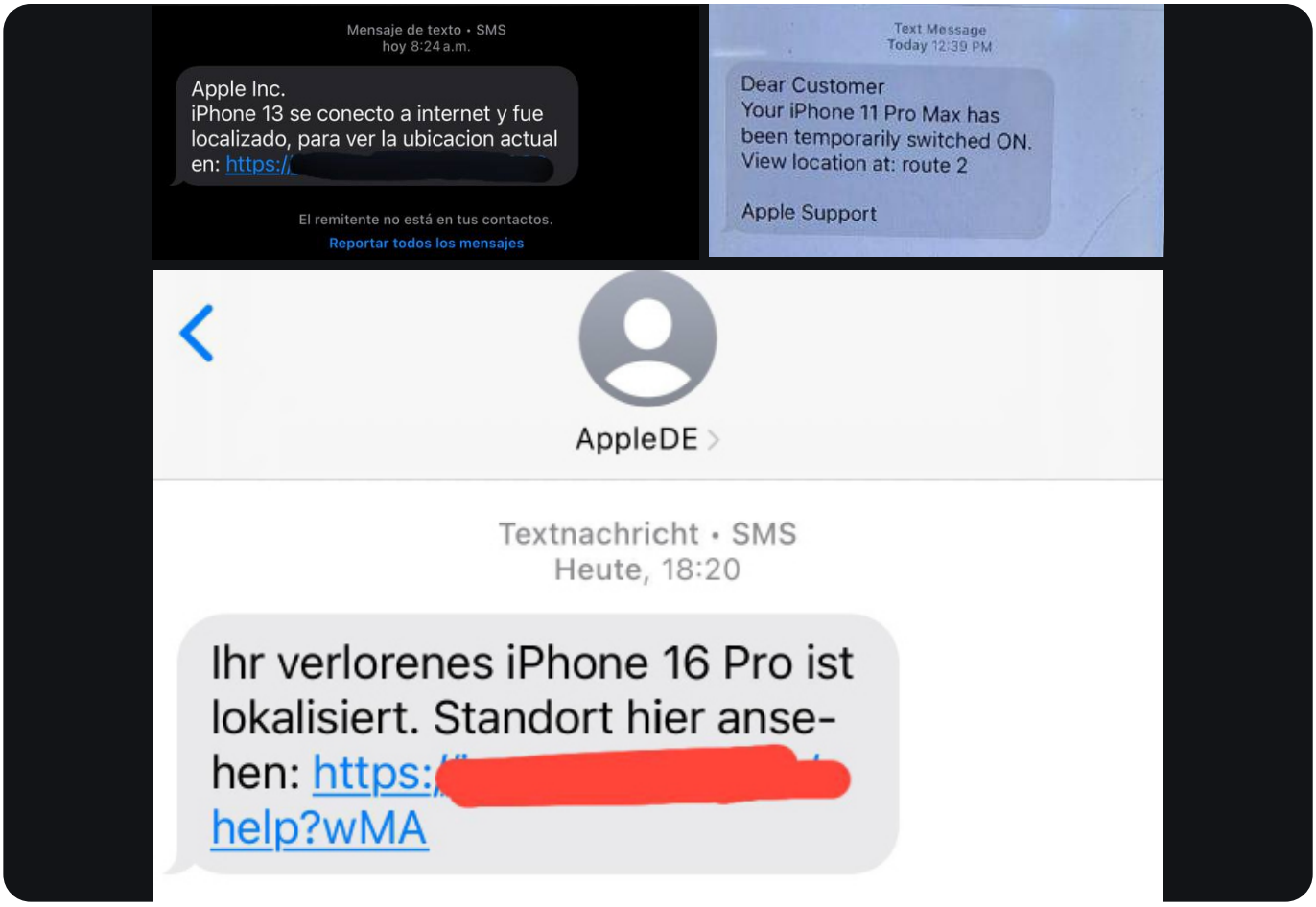


Figure 9. Example smishing text

Another example is Android banking MaaS operations. Victims are exposed to familiar user experiences, such as voice calls, SMS messages, or QR codes, that lead to mobile pages impersonating trusted organizations, including banks, tax agencies, utilities, airlines, and e-commerce brands. These pages then persuade users to install malicious Android applications and grant extensive permissions, giving attackers control over the device.

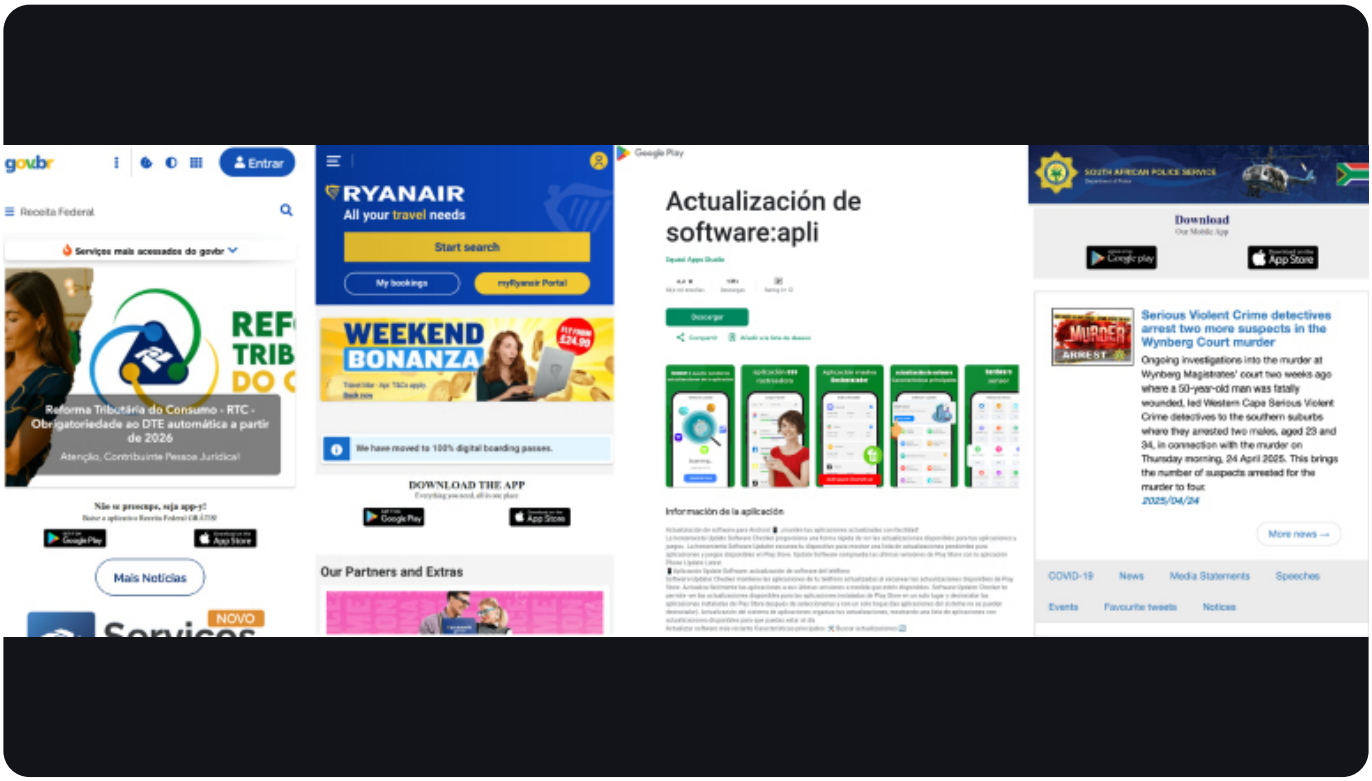


Figure 10. Screenshots of samples of targeted lure pages distributing the malware, impersonating entities including the Brazilian Federal Revenue Service, Ryanair, Openbank, and South African Police Service

Short-Lived Campaigns

While phishing infrastructure is often large and resilient, the phishing pages themselves are increasingly short-lived. Attackers frequently rotate domains, hosting providers, and URLs, allowing campaigns to remain active while evading blocklists and traditional detection methods.

A good example is a phishing campaign uncovered by Infoblox Threat Intel in December 2025 that targeted student single sign-on (SSO) portals at more than 18 U.S. universities. Using the Evilginx adversary-in-the-middle framework, attackers created convincing phishing pages designed to steal credentials and bypass multi-factor authentication.

Each phishing URL closely resembled a legitimate SSO portal but included a unique random path and typically expired within 24 hours. This short lifespan reduced the detection window, made investigation more difficult, and helped attackers stay ahead of security controls. By analyzing DNS patterns associated with the campaign, Infoblox identified nearly 70 malicious domains and exposed the hidden infrastructure supporting the attacks.

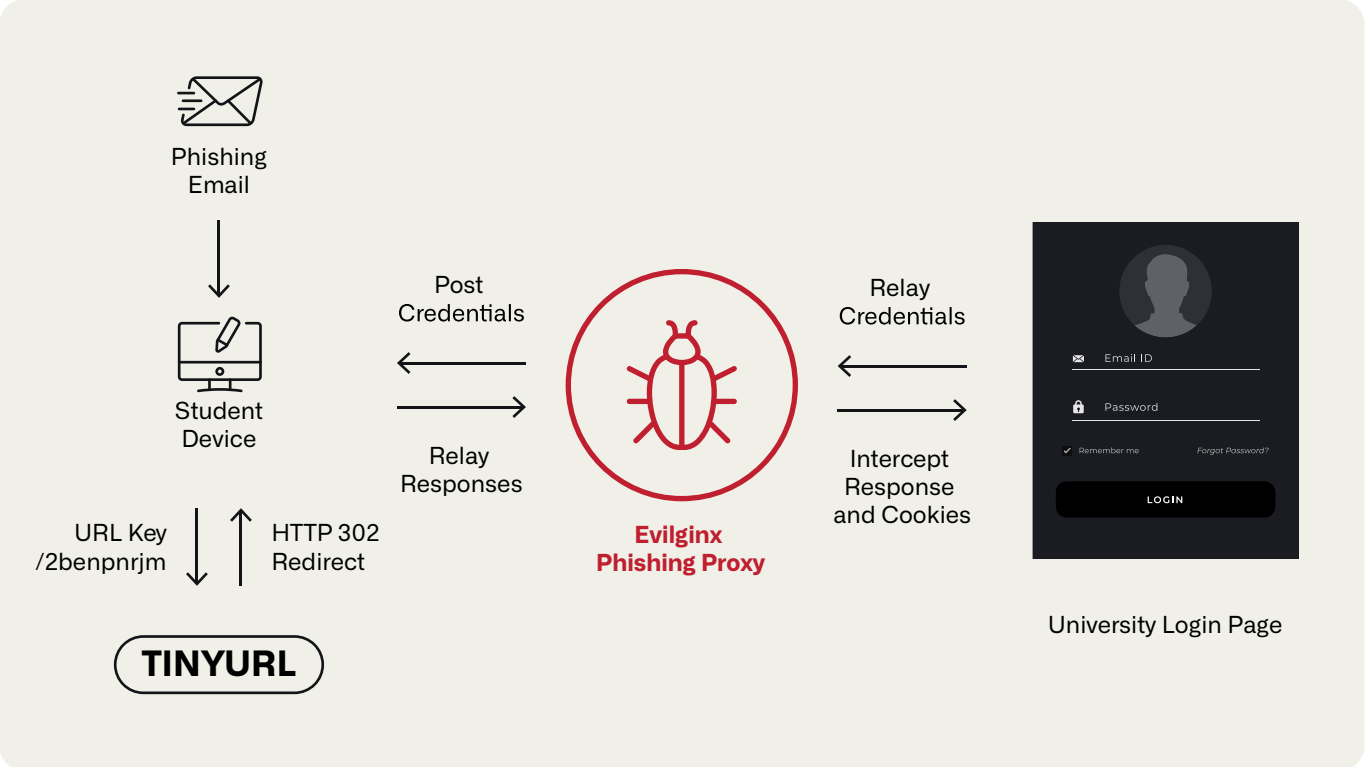


Figure 11. Usage of Evilginx to target University of San Diego students

View 4:

Attack Surface Evolution

As security controls improve, attackers look for areas where visibility is limited and ownership is unclear. New technologies and attack surfaces often create security gaps that can be exploited before organizations establish effective monitoring and protection.

Security teams must then determine who owns the risk, collect the necessary data, build detections, update policies, and train staff. This delay creates a window of opportunity that attackers consistently exploit.

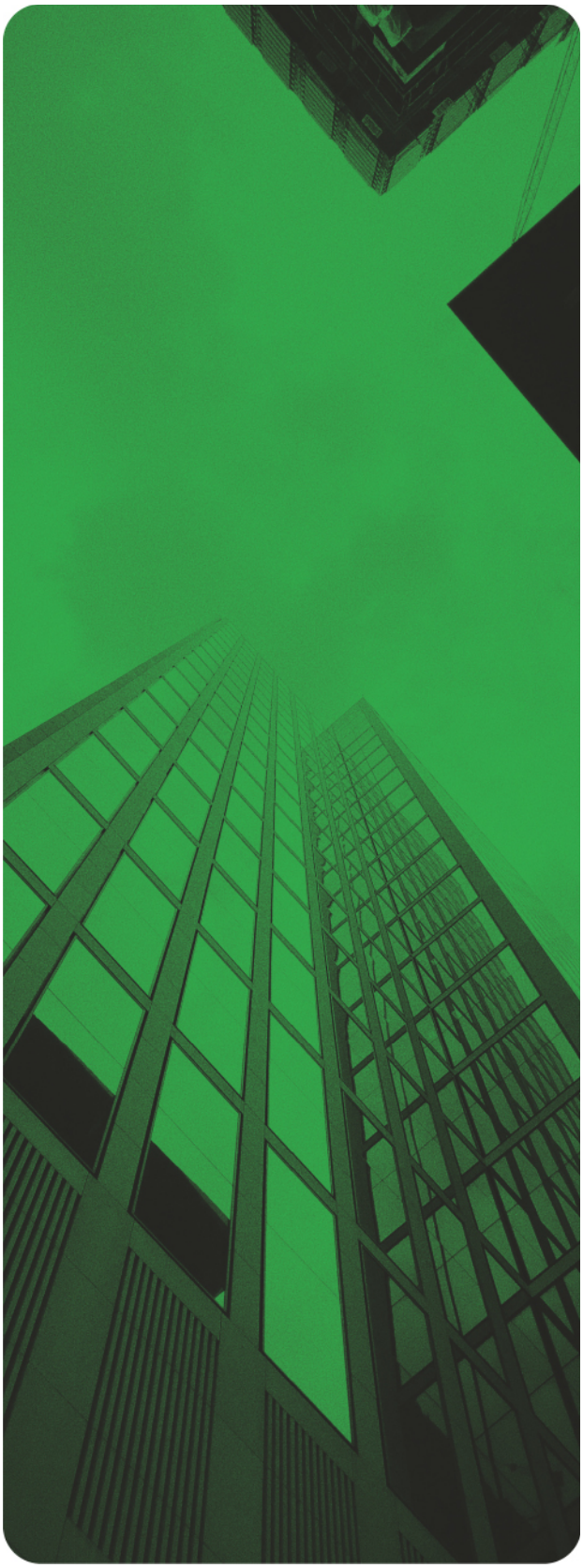
Residential Proxy Services: Hiding Malicious Activity in Plain Sight

Residential proxy services route internet traffic through everyday devices such as phones, laptops, and smart TVs. This makes malicious activity appear to originate from legitimate residential IP addresses, making it harder to detect, block, and attribute.

In June 2026, Infoblox Threat Intel published research showing the widespread use of residential proxy services:

→ **65%** of Infoblox Threat Defense™ Cloud customers queried domains associated with residential proxy services in 2026.

→ **DNS queries to residential proxy domains increased 25%**, growing from nearly 400 billion in January 2025 to more than 500 billion by April 2026.



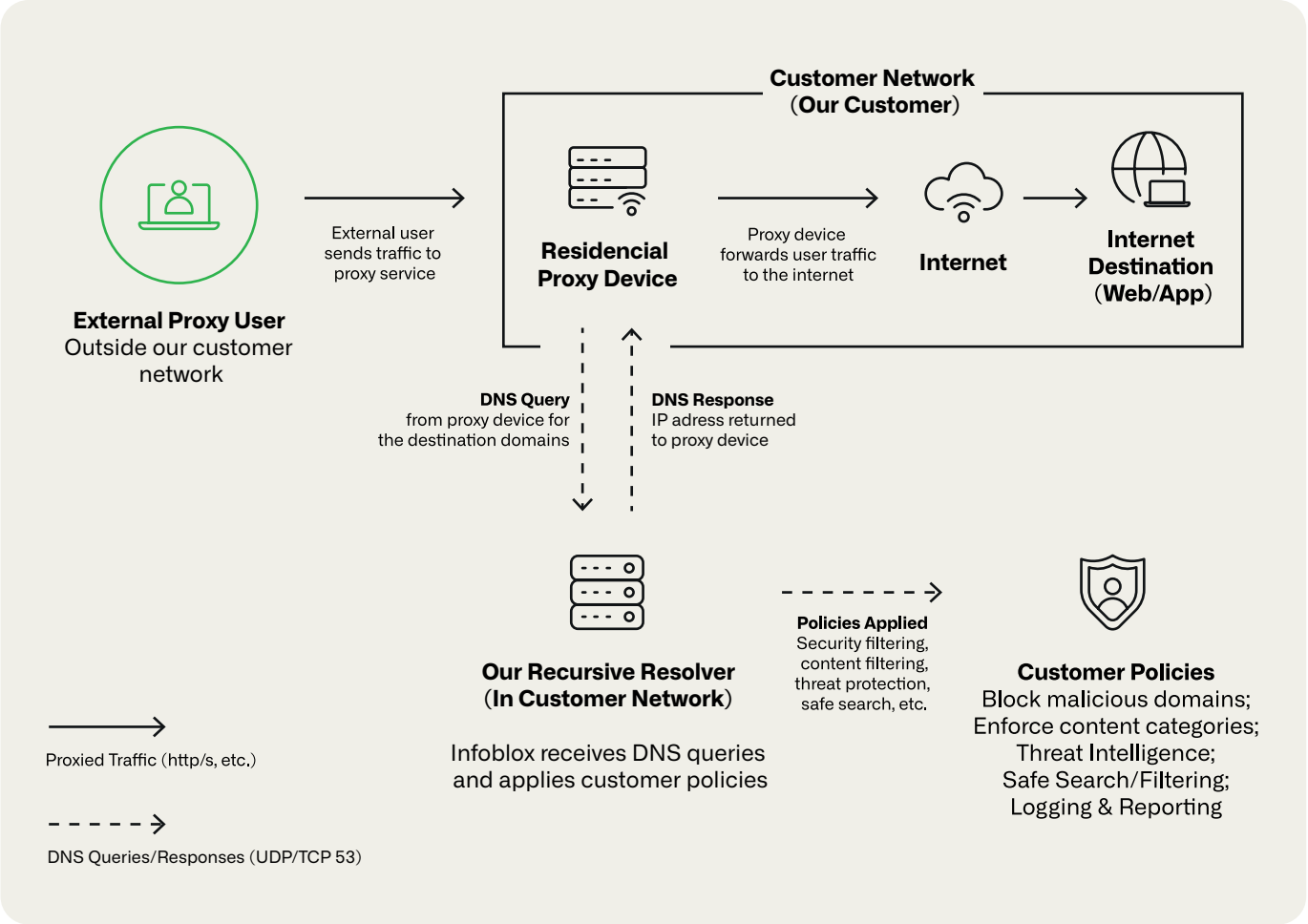


Figure 12. Infoblox visibility into residential proxies

Using DNS telemetry, Infoblox identified residential proxy services such as **Bright Data, Hola VPN, Honeygain, and Grass** operating within enterprise networks. Although these services are often marketed for privacy or passive income, they can also be used to hide attacker activity, evade detection, complicate attribution, and abuse enterprise resources.

Residential proxies are difficult to detect because they are often embedded in mobile apps and software development kits (SDKs). Organizations may be unaware that employee devices have become proxy endpoints, while the resulting network traffic appears to be legitimate application activity.

Browser Push Notifications

Browser push notifications have become another overlooked attack surface. In 2026, Infoblox analyzed a large malicious notification network that tricked users into clicking “Allow” through fake CAPTCHAs, cookie banners, and verification prompts.

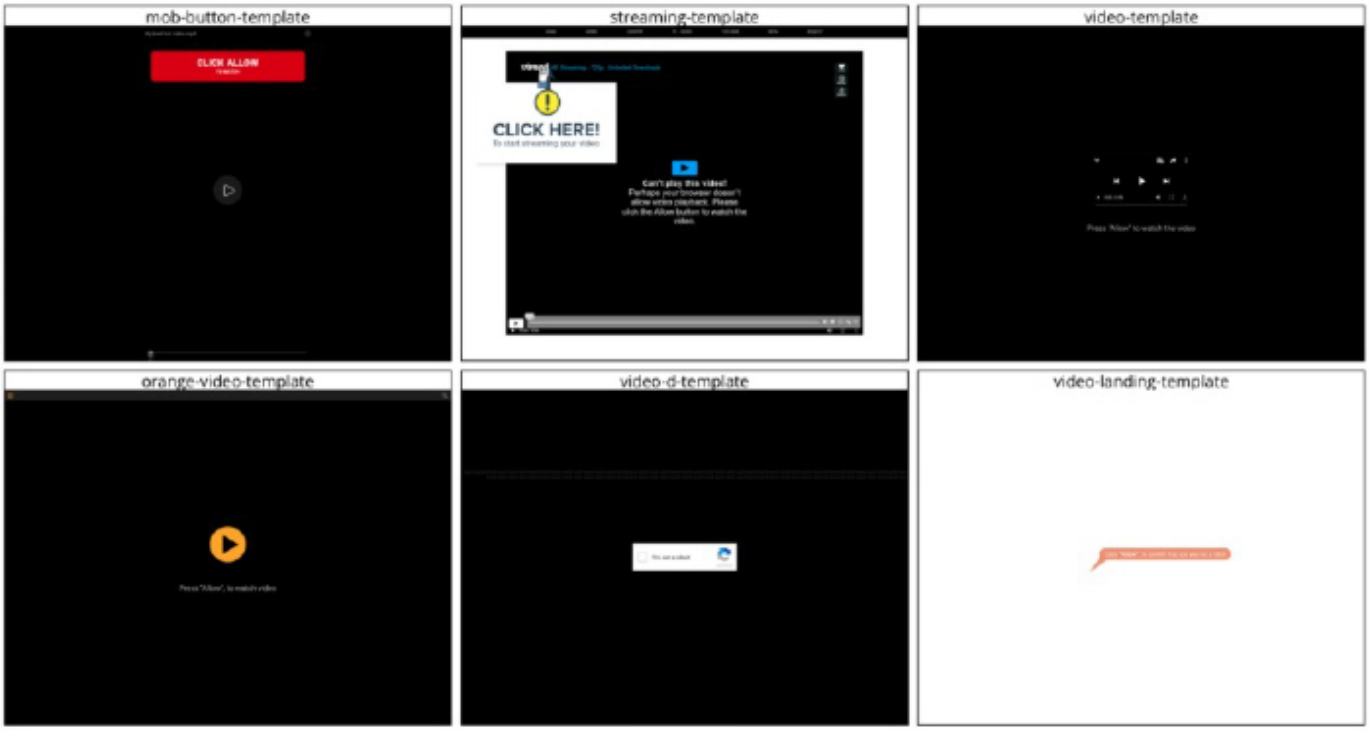


Figure 13. Example landing pages of a few “safe for work” templates

Once permission was granted, attackers gained a persistent communication channel to the victim’s device. Victims received more than 140 malicious notifications per day, including fake antivirus alerts, government impersonation, and messages promoting investment scams and gambling sites.

Unlike traditional phishing, attackers can continue delivering scams long after the victim leaves the original website, creating a long-term channel that bypasses many traditional security controls.

DNS as Attack Surface

As organizations create and retire cloud infrastructure, their DNS records must be updated accordingly. However, administrators sometimes leave behind CNAME records that point to cloud services or hostnames that no longer exist. Attackers can claim these abandoned cloud resources—for example, by recreating an Azure Web App or GitHub Pages site with the same hostname—and gain control of a trusted subdomain.

During the Infoblox External Attack Surface Management (EASM) early access program, researchers found that **one-third of identified dangling CNAMEs were easy or trivial to take over**, allowing attackers to exploit the trust associated with legitimate domains for phishing, malware delivery, or other malicious activity.

DNS as Attack Surface

The rapid adoption of AI has created a new attack surface. Many organizations lack clear governance and visibility into how AI tools are used, creating opportunities for attackers to abuse trusted platforms.

One example involved a publicly shared ChatGPT conversation that appeared to be a legitimate guide for freeing disk space on macOS. Hidden within the instructions were commands that directed users to download malware from an attacker-controlled website.

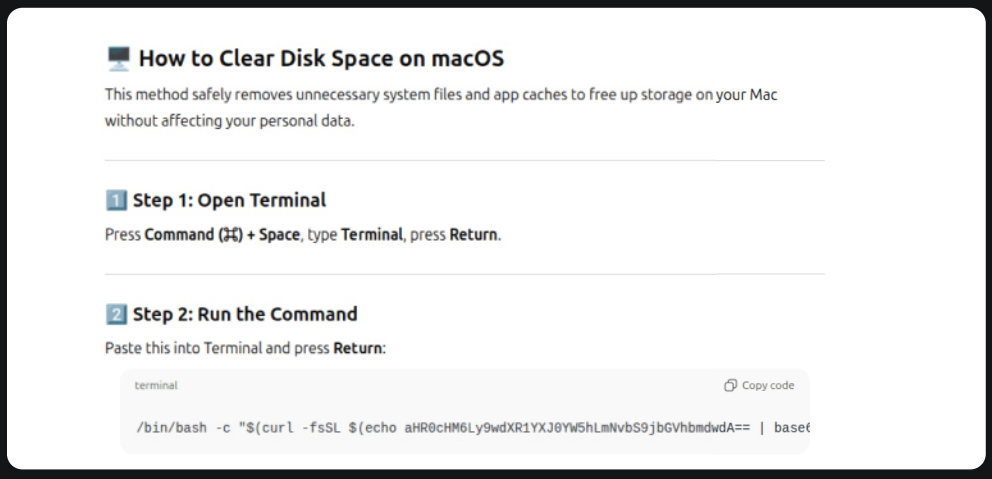


Figure 14. ChatGPT abuse

The technique is highly effective because it leverages trusted platforms and professional-looking content to exploit users' confidence in AI-generated information, while avoiding many of the traditional indicators that security tools and users rely on to identify phishing.

Supply Chain Attacks

Threat actors are increasingly targeting software supply chains to reach large numbers of victims through trusted software, libraries, and development tools.

A notable example was FunNull, a China-linked criminal group that compromised the widely used Polyfill.io service. After gaining control of the platform, the group launched a supply chain attack that impacted more than **110,000 websites**, demonstrating how trusted internet infrastructure can be weaponized at scale.

Another actor tracked by Infoblox Threat Intel is TeamPCP, which compromised several widely used open-source and security tools in 2026, including Trivy, KICS, LiteLLM, and the Telnyx Python SDK. By targeting software trusted by developers and security teams, the group gained opportunities to steal credentials and spread malicious code throughout downstream environments.

These incidents highlight a growing trend: attackers increasingly target trusted platforms, software, and services to reach victims indirectly, bypass traditional defenses, and scale their operations.



Turning the Tables on Attackers with Preemptive Security

Attackers are using AI, automation, and cybercrime services to launch campaigns at unprecedented speed and scale. Traditional patient-one security approaches—investigating individual attacks after they occur to form new defenses—can no longer keep pace.

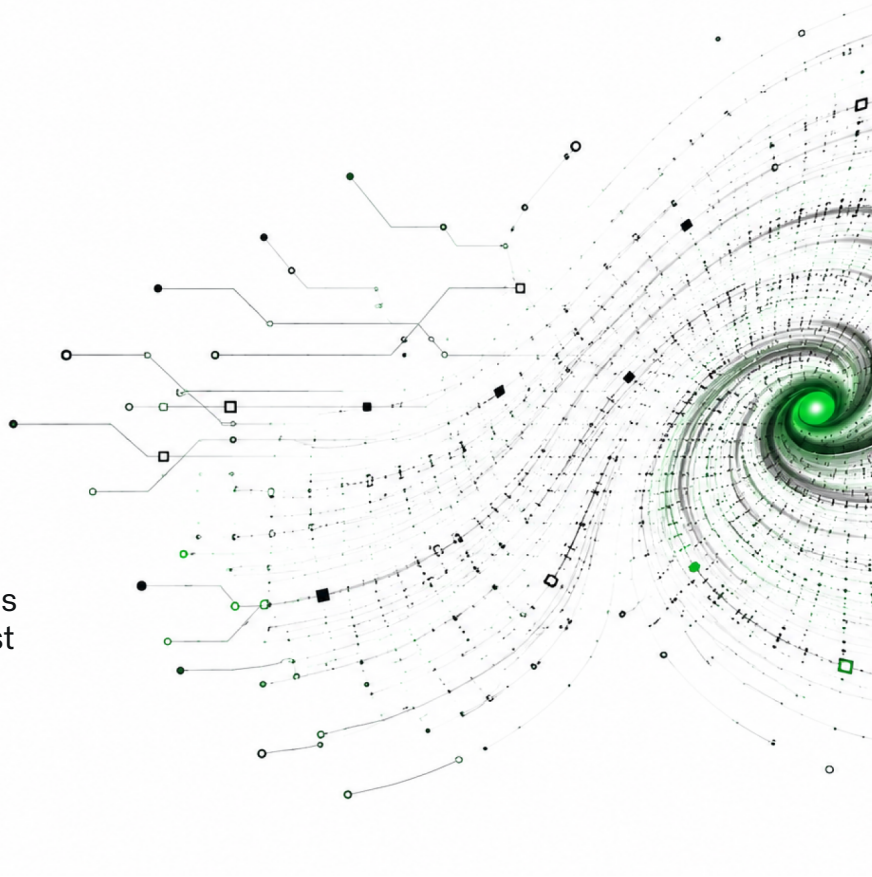
A more effective strategy is preemptive security: identifying and blocking malicious infrastructure before it can be used against your organization. This approach is built on four key pillars.

Pillar 1: Predictive Intelligence via Protective DNS

Every action on the internet—visiting a website, sending an email, or using an AI tool—starts with a DNS lookup. Because of this, DNS provides a rich, reliable source of network and security intelligence.

Cybercriminals also depend on DNS. They use domains and DNS infrastructure to deliver phishing attacks, malware, scams, and ransomware.

By analyzing DNS activity, organizations can identify malicious infrastructure before attacks occur. They can then automatically block connections to malicious and suspicious domains that have little or no legitimate business purpose. This low-regret and proactive approach protects users from phishing, malware, ransomware, and other threats while minimizing disruption to legitimate business activity.



Between June 2025 and May 2026, Infoblox identified approximately **90% of threat-related domains** before any customer network interaction, with an average lead time of **68 days** before the first observed connection and **false positive rate of 0.0002%.**

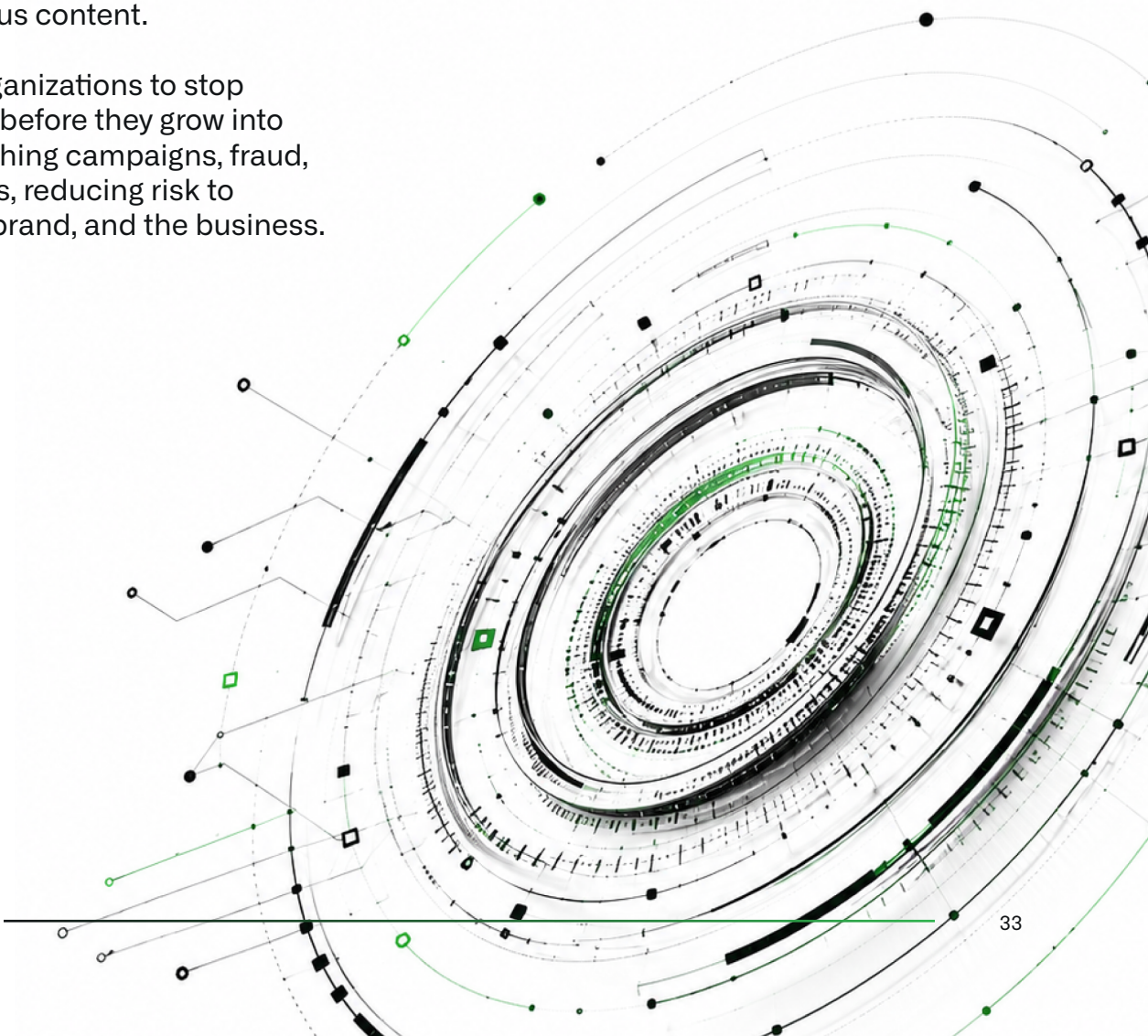
Pillar 2:
Digital Risk Protection

Digital Risk Protection Services (DRPS) identify and stop threats outside the traditional network perimeter, including phishing sites, brand impersonation, compromised credentials, and stolen payment card data.

By correlating attacker infrastructure, Digital Risk Protection Services uncovers related domains, websites, social media accounts, mobile apps, and leaked credentials, giving security teams early visibility into coordinated campaigns. Automated takedowns work with registrars, hosting providers, social media platforms, app stores, and advertising networks to quickly remove malicious content.

This enables organizations to stop external threats before they grow into large-scale phishing campaigns, fraud, or data breaches, reducing risk to customers, the brand, and the business.

Over the past 12 months, Infoblox initiated **more than 280,000 takedowns**, primarily targeting phishing sites, fake social media accounts, and brand abuse. **86% of takedowns were fully automated**, with a **median detection time of less than four minutes** and a **median removal time of just over nine hours** after confirmation.



Pillar 3: External Attack Surface Management

External Attack Surface Management (EASM) helps organizations discover, monitor, and reduce risks across internet-facing assets before attackers can exploit them.

As AI accelerates vulnerability discovery, security teams must prioritize the exposures that matter most. External Attack Surface Management continuously discovers exposed assets, identifies misconfigurations, and highlights the highest-risk vulnerabilities for remediation.

It is particularly effective at identifying DNS-related risks such as dangling CNAMEs, lame delegations, and other domain misconfigurations that can lead to subdomain hijacking or service abuse. It also uncovers unknown or unmanaged internet-facing assets, helping organizations reduce their overall attack surface.

Pillar 4: Asset and Application Inventory

Organizations cannot secure what they cannot see. Cloud resources, software-as-a-service (SaaS) applications, AI services, and internet-facing assets are constantly being created, changed, and retired, leaving many organizations with incomplete or outdated inventories. As AI adoption accelerates, the challenge extends beyond infrastructure to understanding which AI applications, services, and agents are being used—and whether they are approved.

By combining DNS telemetry with network and cloud visibility, organizations can identify managed and unmanaged assets, discover shadow IT and AI applications, and maintain an up-to-date inventory without relying solely on manual processes or traditional scanning.

A complete and trusted view of assets and application usage improves security, strengthens compliance, and provides the reliable data foundation needed for automation and AI. It enables organizations to reduce blind spots, identify unmanaged risks, govern AI adoption, and make better operational and security decisions with confidence.

To learn more about Infoblox Threat Intel and preemptive security:

VISIT INFOBLOX THREAT INTEL

To find out if your DNS defenses can hold up:

GET FREE ASSESSMENT



Appendix:

Actors and Domain Metrics



Key threat Actors by Active Domains

Vigorish Viper	SLDs: **656,311**

A sophisticated threat actor that operates the technology behind numerous online gambling brands. Although the brands appear unrelated, they share infrastructure linked to Chinese organized crime, money laundering, and human trafficking in Southeast Asia. The group provides the software, DNS infrastructure, hosting, payment systems, and mobile apps that power these operations.

Funnull	SLDs: **585,008**

A criminal group based in China and operating across Southeast Asia. It hosts illegal gambling and adult websites, was responsible for the **polyfill**[.]**io** compromise, and has been linked to domain hijacking and malware hosting. In May 2025, the U.S. Treasury sanctioned Funnull for its role in pig-butchering scams.

Tianbo Gambling Domains	SLDs: **261,887**

A large network of gambling, streaming, and adult websites targeting users in China and Southeast Asia. The infrastructure also shows additional suspicious activity and remains under investigation by Infoblox Threat Intel.

Toll Shipping Smishing	SLDs: **172,040**

A phishing operation that impersonates trusted brands such as **E-ZPass, USPS, DHL, Royal Mail, and Estafeta.** The campaign targets victims in the United States, United Kingdom, Mexico, and other countries through SMS phishing (smishing).

CC Panda	SLDs: **111,601**

A Chinese threat actor operating an illicit adult streaming platform across more than 40,000 rapidly rotating domains. Active since February 2025, the operation uses bulk domain generation and bulletproof hosting to evade takedowns.

1Win Lookalike RDGA	SLDs: **109,109**

A cluster of RDGA-generated domains across multiple TLDs that imitate the **1Win** online gambling platform. These domains use unique website content and are frequently reported to URLScan as suspected phishing or malware sites.

Undisclosed TDS	SLDs: **98712**

Malicious TDS network that uses custom cloaking, dictionary domain generation algorithm (DDGA), and lookalike domains to deliver threats such as malware, adware, and scams.

Fake Finance TDS	SLDs: **92191**

Actor running a TDS routing users to fake loan assistance, class action lawsuit, and spoofed VPN pages. These RDGA domains are likely distributed via phishing emails or texts.

Undisclosed TDS	SLDs: **71390**

Malvertising TDS network that not only abuses push notifications, pop-ups, and redirects within a browser, but continues to serve ads even after the user navigates away from the initial page.

Telegram Support Scam	SLDs: **61786**

Actor uses RDGA domains in scams to trick victims into granting access to their Telegram accounts. The actor also creates multiple domains with the same label, but on several different TLDs.

Prolific Puma	SLDs: **61786**

Actor that provides a link shortening service used for criminal activities, including phishing and malware distribution.

RDGA Dating Apps	SLDs: **55781**

Actor registers DGA domains using the TLD .top that lead to an installation of a dating and pornography app in Chinese.

Reckless Rabbit	SLDs: **39262**

Actor that specializes in financial investment scams advertised on Facebook.

BetasusGambling	SLDs: **35921**

Actor that operates geo-restricted illegal gambling sites.

Venal Viper	SLDs: **35802**

Actor that operates a malicious TDS that has been observed acting as an affiliate of other known malicious TDSs.

15 Top-Level Domains by Risk Score

TLD	Monthly Min Risk Score	Monthly Max Risk Score	Popular
vip	7	8	✓
gdn	7	8	
pw	7	8	✓
cn	6	9	✓
gen.in	5	8	
net.ng	6	8	
hl.cn	6	8	
top	6	8	✓

TLD	Min risk score	Max risk score	Popular
bid	6	8	
pink	5	8	
bar	5	8	
black	7	7	
loan	7	8	
pizza	7	8	
pro	7	8	✓

Reputation risk score measures the likelihood that an Internet entity (such as a TLD) is associated with malicious activity, based on observed behavior and threat intelligence. When a TLD is popular, it simply means it is widely used and frequently observed in DNS traffic. For more details, read https://insights.infoblox.com/resources-research-report/infoblox-research-report-reliable-reputation.

Threat Type Breakdowns

SCAM TYPES

Scam Type	New Domains
Generic	1,119,808
Other	54,740
Investment/ Financial	44,222
Crypto	40,786
Fake Storefront	12,349
Tech Support	10,265
Pig Butchering	6,665
Pharmaceutical	5,340
Telegram Support	1,907

INFOSTEALER FAMILIES

Family	New Domains
MetaStealer	30,001
Lumma Stealer	3,427
Dropper/Loader	3,423
Generic Infostealer	2,550
Generic Stealer	751
Shub Stealer	292
Atomic Stealer	130
PureLogs Stealer	92
macOS Infostealers	73
Aurotun Stealer	71

RESIDENTIAL PROXIES

Service	Max Daily Cust. %
Hola VPN	34%
Bright Data	21%
Wave Browser	21%
Grass	19%
Infatica	18%
Unknown Proxy	17%
Oxylabs Proxy	15%
Honeygain	14%
Geonode Proxy	11%
NetNut	11%
IPIDEA Proxy	10%

Data Leakage and Phishing Incidents

June June 1, 2025 – June 1, 2026

LEAKED DATA

Type	Count
Total credentials	161 billion
Unique credentials	5.3 billion
Credit card data	395 million

PHISHING INCIDENTS BY INDUSTRY VERTICAL

Vertical	Incidents	%
Finance & Insurance	26,911	41.5
Technology	12,642	19.5
Retail & E-commerce	12,502	19.3
Transport & Logistics	2,670	4.1
Public Sector & NGOs	2,380	3.7
Food & Beverage	2,220	3.4
Healthcare	1,557	2.4
Telco	959	1.5
Power & Chemistry	858	1.3
Travel & Tourism	850	1.3
Other	1,251	1.9
Total	**64,800**	**100**

Terminology Used



Adtech: Short for advertising technology, refers to the software, tools, and platforms used by brands, agencies, publishers, and platforms to plan, execute, manage, and analyze digital advertising campaigns. It is the backbone of the online advertising ecosystem.

APK: Android Package Kit—standard file format used by Android to distribute and install mobile apps

C2: command and control

CDN: A content delivery network is a network of geographically distributed servers that work together to deliver digital content (like websites, videos, images, and scripts) quickly, reliably, and securely to users based on their location.

CNAME: Canonical Name record is a type of DNS (Domain Name System) record that maps one domain name (an alias) to another domain name (the canonical name). It's used to point one domain or subdomain to another domain, instead of pointing directly to an IP address.

DDGA: dictionary domain generation algorithm

DDI: DNS, DHCP, and IP address management (IPAM)—three critical network services that work togetherto provide automated and centralized management of IP address spaces and name resolution across enterprise networks.

DGA: domain generation algorithm

DNS: Domain Name System

DNS queries: A DNS query (Domain Name System query) is a request made by a device (usually a computer or mobile phone) to translate a human-readable domain name (www[.]google[.]com) into a machine-readable IP address (like 142.250.190.68) so it can connect to the correct server on the internet.

KYC: know your customer—The identity verification process used by financial institutions, banks, and fintech platforms to verify the identity of their customers.

RDGA: registered domain generation algorithm

TDS: traffic distribution system



References

(1) The FBI's 2025 Internet Crime Report shows cyber-enabled crimes defrauded Americans of nearly $21 billion, with cryptocurrency and artificial intelligence-related complaints among the costliest. https://www.fbi.gov/file-repository/2025_ic3report.pdf/view

(2) https://insights.infoblox.com/resources-research-report/infoblox-research-report-reliable-reputation

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2026 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20260730