Detour Dog: DNS Malware Powers Strela Stealer Campaigns

By Infoblox Threat Intel

Published: 2025-09-30 · Archived: 2026-04-05 16:26:48 UTC

Tens of thousands of websites worldwide are infected with malware that utilizes the Domain Name System (DNS) to conditionally redirect visitors to malicious content. These DNS requests are made server-side, meaning from the website itself, and are not visible to the visitor. We have tracked the threat actor that operates this malware since **August 2023**. The malicious name server conditionally instructs the website to redirect the visitor based on their location and device type. While traditionally these redirects led to scams, the malware has evolved recently to execute remote content through the DNS-based command-and-control (C2) system. We are tracking the threat actor who controls this malware as Detour Dog.

Detour Dog played a major role in campaigns to spread Strela Stealer this summer. In June, we learnt from external researchers that Detour Dog-owned infrastructure was hosting a backdoor malware, **StarFish**, used to install the information stealer. The domains were seen in malicious email attachments that targeted Germany. Digging into our own spam collection, we discovered that websites compromised by Detour Dog also appeared to host the first stage of the information stealer. Of the confirmed StarFish staging hosts, at least 69 percent were under Detour Dog control; the true percentage is likely much higher.

To our surprise, another system we track via DNS, a MikroTik botnet advertised as REM Proxy, was part of the attack chain. Strela Stealer is operated by an actor known as Hive0145 and traditionally distributed through attachments in mass email. The spam seen in June and July was delivered by both REM Proxy and a different botnet, Tofsee. Detour Dog hosted the first stage of the attack in campaigns from both sources.

But Detour Dog did more than host the backdoor malware: they helped distribute the stealer via DNS TXT records. The actor-controlled name servers were modified to interpret specially formatted DNS queries from the compromised sites and to respond with remote code execution commands. Starting June 8, we saw responses from the servers that directed the infected site to fetch the output of PHP scripts from verified Strela Stealer C2 servers, and from these covert communications we perceive the likelihood of a malware distribution system, where DNS

acts as both a command channel and a delivery mechanism. A novel setup like this would allow an attacker to hide their identity behind compromised websites making their operations more resilient, meanwhile serving to mislead threat hunters because the malware isn't really where the analyzed attachments indicate the stage is hosted.

This marks the first time Detour Dog is known to deliver malware to home users.

For years, Detour Dog exclusively forwarded traffic to Los Pollos. In late-November 2024, that changed. The servers began redirecting visitors to Help TDS, which in turn routed traffic via Monetizer TDS. In those flows we observed malicious campaigns operated by third-party affiliates. While the advertising network utilized by Detour Dog changed, the outcome did not.

The website malware fundamentally advanced in spring 2025. The actor added a new capability to command infected websites to execute code from remote servers. Responses to TXT record queries are Base64-encoded and explicitly include the word "down" to trigger this new action. We believe this has created a novel networked malware distribution model using DNS in which the different stages are fetched from different hosts under the threat actor's control and are relayed back when the user interacts with the campaign lure, for example, the email attachment.

To our knowledge, this technique, shown in Figure 1, has not been reported. Through this method, the actor misdirects defenders and obfuscates the true location of the malware. With a large network of infected hosts, this might be considered a three card monte version of malware distribution.

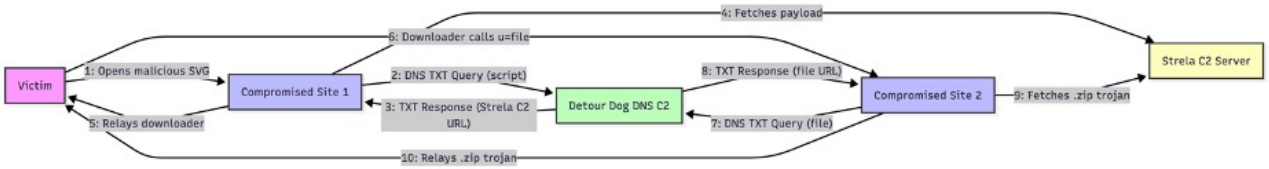

Figure 1. Diagram of theorized attack chain utilizing DNS TXT records for C2

Most of the time, when a user visits one of the sites, they see the original site. In some cases, they will be redirected to a scam via Help TDS. But in rare cases, the site will receive a remote file execution command. The fact that most of the time there is no apparent compromise of the site, and that it is difficult to reproduce malicious redirections, allows Detour Dog to persist. We have seen sites infected for over a year. When combined with the new remote execution feature, the ways in which the threat actor can deliver malicious content are complex. The attack chains currently known to utilize Detour Dog-controlled assets are shown in Figure 2.

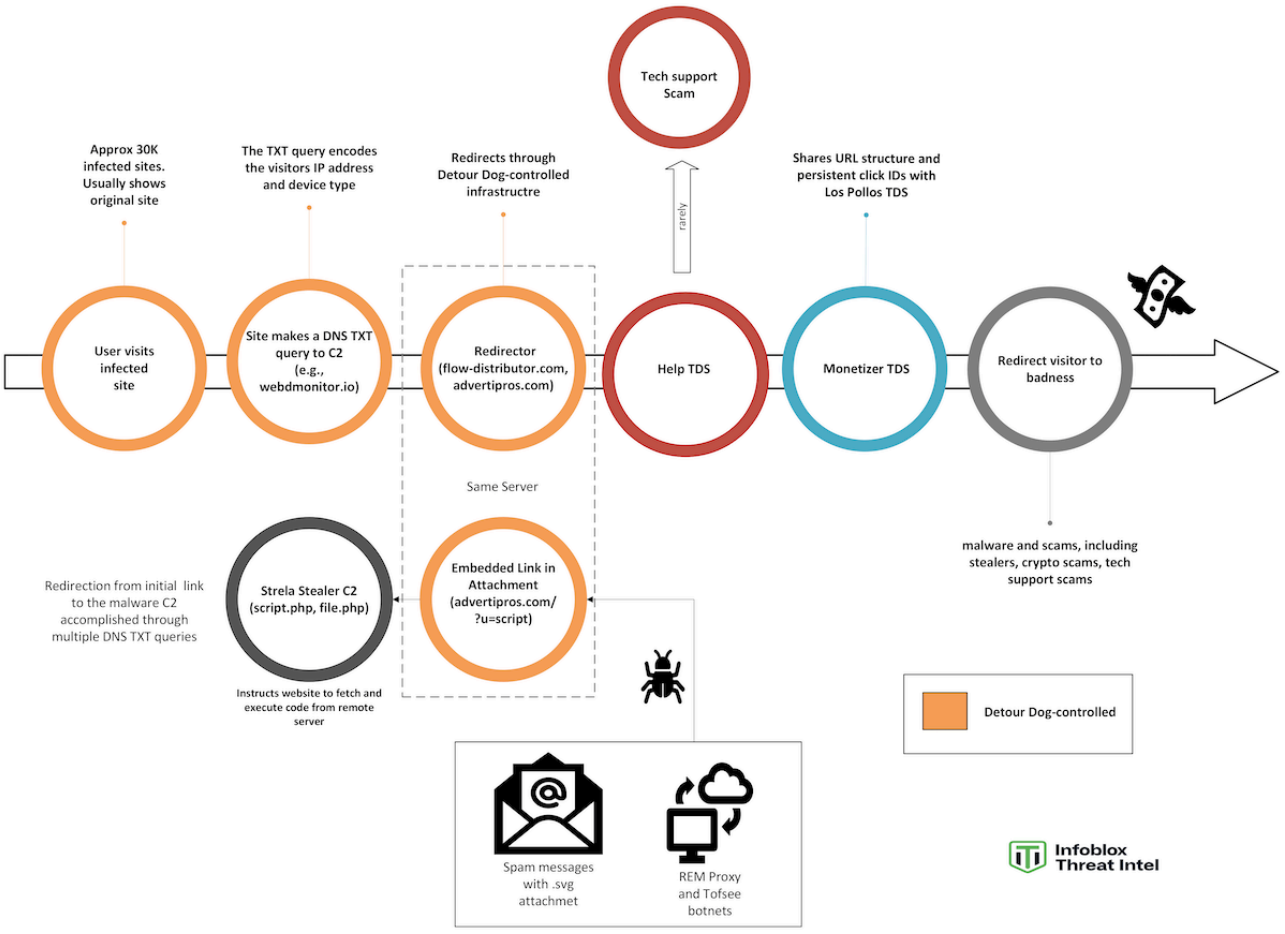

Figure 2. Multiple attack vectors utilize Detour Dog-controlled assets

Detour Dog operations appear to extend beyond the DNS C2 website malware. We unwound the history of Detour Dog back to February 2020, well before the website malware was discovered. Detour Dog handcrafts tracking identifiers that are carried across multiple traffic distribution systems (TDSs), which allowed us to connect seemingly independent activity over long periods of time.

We have attempted to disrupt Detour Dog through abuse reporting. In August 2025, after the registrar WebNIC refused to suspend the active DNS C2 server, webdmonitor[.]io, the Shadowserver Foundation sinkholed the domain. This gave us a fresh look at the infected websites, as well as the actor's ability to respond to the disruption. It took Detour Dog only a few hours to establish a new C2 and regain control of the infected sites.

A week later, Shadowserver sinkholed the second domain and provided us with over 39 million DNS TXT queries to analyze. Approximately 30,000 infected hosts, within 584 top-level domains (TLDs), were seen in a 48-hour window. The queries show a significant amount of bot traffic; at its peak, the sinkhole received 2 million TXT requests in an hour and included encoded IP addresses that didn't correspond to natural human traffic. While bot traffic is a known plague in affiliate advertising, the sheer volume was astonishing. We will dig into the details later in the section entitled **Sinkholing the C2 Domain**.

DNS queries hint that Detour Dog is still maturing remote file execution capabilities. Currently, evidence suggests that Detour Dog and Hive0145 are distinct actors. It's possible, based on history from the last four years, that

Detour Dog is providing a service to others, in which case Hive0145 may just be the first partner to receive malware distribution support via the network of infected hosts.

DNS TXT C2

Detour Dog-infected websites make queries to the DNS C2 using a subdomain that includes user information. The query format has changed slightly over the last few years but retains the same general structure:

<infected-host>.<visitor-ip>.<rand-num>.<type>.c2_domain

where the “type” is not always present. Initially, these queries were client-side, but **changed to server-side** in April 2024. With this change, the actor began encoding information about the client device type, for example, “ni” for iPhone. We have seen several values in the “type” field over the last few years.

Most of the time, Detour Dog instructs the infected site to display its original content, that is, “do nothing.” We analyzed over 4 million TXT records from the C2 server, which is the authoritative server for the C2 domain, recorded between August 6 and August 8. The responses were distributed as shown in Figure 3. Queries to the server include a very high volume of bot traffic; however, we haven’t observed a consistent pattern for which the server responds with a redirect. We suspect they limit redirections in part to avoid detection.

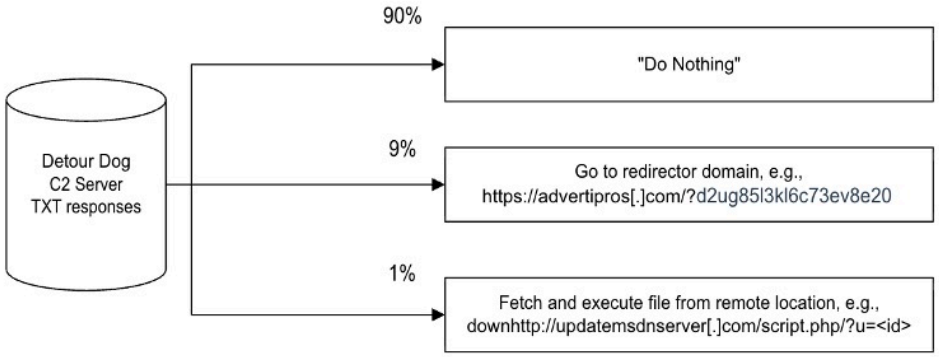

Figure 3. Detour Dog responses August 6-8 to queries from infected hosts

The TXT responses are Base64 encoded and currently have the form

https://<redirector_domain>/?<alphanumeric_string>

where the alphanumeric string changes in each response. This redirector has no filtering logic and has exclusively redirected to Help TDS URLs since November 20, 2024. Table 1 shows the redirector domains observed in 2025. These domains were traditionally hosted with Cloudflare, allowing them to hide their true IP address. However, after multiple disruptions, the actor began to openly run their servers, most recently in IP space belonging to Kazakhstan (93[.]152[.]230[.]52).

Redirector Domain	First Seen	Last Seen
infosystemsllc[.]com	August 1, 2024	April 1, 2025
ecomicrolab[.]com	December 8, 2024	June 10, 2025
flow-distributor[.]com	June 15, 2025	July 15, 2025
advertipros[.]com	June 10, 2025	Now

Table 1. Domains contained in TXT record responses since January 2025

On April 1, 2025, a new type of TXT record response was identified, with the answer of "ZG93bmh0dHBzOi8vdGhpbmtwYWR3b3JrLmNvbS9kb3du", which decodes to "downhttps://thinkpadwork.com/down", and the server continued to occasionally respond like this to requests until June 26, 2025. Unfortunately, we were unable to determine what this URL hosted. The domain thinkpadwork[.]com was registered January 23, 2025, and uses Cloudflare nameservers.

The "down" command instructs the infected site to request the specified URL with curl and pass the output of the request into the body of the response to the victim. In the case of a PHP endpoint, the PHP script is executed on the C2 server and the output is received by the compromised server and passed back to the victim.

Enter StarFish Backdoor and Strela Stealer

Strela Stealer is an information stealer first observed in late 2022. The operators, known as **Hive0145**, target European countries, primarily Germany, using broadly distributed email that includes a malicious file. This summer, malicious SVG attachments were used to download a reverse shell backdoor malware called StarFish. IBM X-Force and other researchers witnessed cases where StarFish then downloaded Strela Stealer.

To our surprise (and delight?), the latest **reporting** from IBM included a Detour Dog redirector domain, advertipros[.]com. **This sample**, submitted to VirusTotal of an SVG file found in spam using German language lures about outstanding invoices, makes the following call to download the stealer malware:

hxxps://advertipros[.]com//?u=script

This meant that Detour Dog domains were used to host malware, in addition to redirecting website visitors to scams. We set out to see if we could verify this with our own data. For months, we have tracked a spam **botnet of compromised MikroTik routers** via DNS, which we now know, based on **Black Lotus research**, to be REM Proxy. Using our own spam collection, we located multiple samples of Strela Stealer SVG distribution and discovered that they were all distributed by REM Proxy, confirming that Hive0145 is a customer of REM Proxy. Other external researchers reported spam delivered through the botnet, Tofsee.

Samples in our spam collection led victims to download malware from domains compromised by Detour Dog. As an example, this **SVG attachment** downloaded StarFish from ywcanevada[.]org. But, a **scan of the domain** in urlscan has the telltale signs of a Detour Dog infection: visiting the domain led to a redirection through flow-distributor[.]com and on to Help TDS.

At this point in our investigation, we knew that the threat actor was hosting malware connected to Strela Stealer from their own infrastructure and that the same files were hosted on infrastructure they had compromised. Then we discovered more connections between Detour Dog and Strela Stealer.

TXT Record Connections

When StarFish executes, it starts regular communication with the malware C2 server, exfiltrating data from the host until it is told to stop. According to IBM, it does this by connecting to a hardcoded C2 server with the "server.php" endpoint and passing a unique identifier for the compromised machine. The server responds with "OK" and an optional command. If the string "%SCRIPT%" is included in the response, it gets converted to the local path of the reverse shell. The infected device responds via POST commands to the server.

Detour Dog also included the StarFish C2 in TXT responses. On June 8, we saw the following response in decoded records:

downhttp://176[.]65[.]138[.]152/script.php?u=j6cwaj0h67

This IP address was found in a **public submission to ANY.RUN** on June 10, 2025, that included an obfuscated JavaScript file. The script attempted to call out to an https[:]//176[.]65[.]138[.]152/server.php endpoint. The IP address is also seen in a number of **JavaScript files submitted** to VirusTotal, which are categorized as remote access trojans.

The URLs contained within TXT responses are slightly different from those reported for the stealer; they contain a script.php endpoint and a "u" parameter. The DNS query that triggered this response incorporates new values for the "type," for example:

<infected-host>.<ip-address>.<rand>.nwuuj6cwaj0h67.webmonitor[.]io

The traditional two-letter values for the device type were replaced with a string that must be parsed by the name server to respond correctly. If the query includes a type value of the format <na|nw|nd>.uu.<value>, the server will interpret this and return an endpoint on the malware C2 server. If the query contains "nwuuscript", the response has no additional parameter:

downhttp:updatemsdnserver[.]com/script.php.

In addition to script.php, we have seen file.php returned in TXT records from June 11 to July 25, 2025 when the query includes "nauufile".

In the Strela Stealer attack chains we analyzed, "script" and "file" are parameters seen in requests sent to compromised sites, originally initiated by the StarFish downloader, in the first and second stages respectively. For example, in the REM Proxy emails within our spam collection this was the case. We consulted Golo Mühr, a researcher at IBM X-Force who tracks Hive0145 and Strela Stealer. Golo speculated that the files could potentially include the decoy and the Strela payload. He clarified that the C2 server is used for all other parts of the operation except staging StarFish.

These returns were a bit of a mystery, as we were unable to fetch the scripts ourselves, however IBM X-Force alerted us to a campaign they observed in July 2025, targeting Ukrainian government domains (gov[.]ua) that used

script.php and file.php endpoints. Unlike the operation by Hive0145 that leveraged Detour Dog infrastructure to obscure C2 locations, this campaign sent victim traffic directly to updatemssoft[.]com, which was hosted at the same IP address as updatemsdnserver[.]com. Although the updatemssoft[.]com domain was not seen in Detour Dog TXT responses, use of the file.php and script.php endpoints here were linked to StarFish/Strela staging.

Examples of the malware samples used in this campaign can be seen here: **https://www.virustotal.com/gui/domain/updatemssoft.com/relations**.

We do have a theory based on his input. The sequence of events as shown in Figure 1 could explain the behavior:

1. **Initial Trigger**
   The victim opens a malicious document (e.g., a fake invoice), which launches an SVG file that calls out to an infected domain using the u=script parameter.
2. **DNS TXT Query**
   The infected site sends a TXT record request to the Detour Dog C2 server via DNS. The query includes a type identifier like nwuuscript+{random string}, where the random string likely serves as a unique identifier.
3. **C2 URL Response**
   The name server responds with a TXT record containing a Strela C2 URL, prefixed with down.
   Example: downhttp://updatemsdnserver.com/script.php?u={random string}
4. **Payload Retrieval**
   The infected site strips the down prefix and uses curl to fetch the next-stage payload from the Strela C2 server. We suspect the output of this request to script.php is the **StarFish downloader**. Because the curl request occurs server-side, it is not visible to the visitor.
5. **Payload Delivery**
   The compromised site acts as a relay for the C2, passing the output from the C2 server to the client. One hint that server-side commands are occurring is shown in this example, where the URL redirects to itself repeatedly before displaying the StarFish downloader script.
   Example at: **https://urlscan.io/result/019782b4-1f1f-7718-a9a4-246596e0ecb1**
6. **Second Stage Callout**
   The downloader script initiates another callout to a different compromised domain, this time using the u=file parameter.
7. **Second DNS TXT Query**
   The second compromised site sends a similar DNS TXT query to the Detour Dog C2 server, now using nwuufile+{random string}.
8. **Second C2 URL Response**
   The Detour Dog name server responds with a new Strela C2 URL pointing to file.php, again prefixed with down.
9. **Second Payload Retrieval**
   The compromised site strips the prefix and initiates another curl request to the Strela C2 server, this time receiving a file in the response.
10. **Second Payload Delivery**
    The second compromised site relays the file to the client. The payload is a .zip archive containing a

wscript trojan, believed to be StarFish; see the VirusTotal report **here**.
Example at: **https://urlscan.io/result/0197f99f-45fd-75f4-be91-a5529e8c6168**

This theory would indicate that the attack cleverly leverages DNS as a covert channel to orchestrate a multi-step delivery process. URLs embedded in DNS TXT records are used to fetch staged payloads—first a downloader script, then a ZIP file—all relayed back to the victim via compromised infrastructure. Passive DNS logs include many TXT queries with the phrase “test” embedded into the type string, indicating that the threat actor is continuing to evolve and perfect the system.

We also saw these domains in similar TXT record responses:

- nupdate0625[.]com
- msdnupdate[.]com

The IP address used by updatemsdnserver[.]com, 95[.]164[.]123[.]57, also hosted:

- mssoftupdateserver[.]com
- domainzone123[.]com
- updatemssoft[.]com

Figure 4 shows the overlap between Detour Dog TXT responses and known Hive0145 infrastructure, with specific examples of known domains.

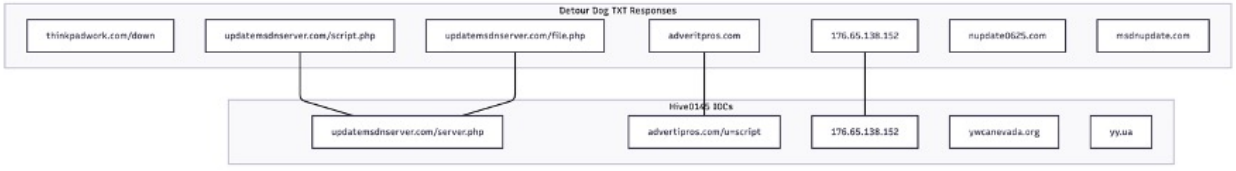

Figure 4. Diagram of overlap in Detour Dog and some Hive0145 (StarFish/Strela Stealer) C2 infrastructure

What’s Detour Dog All About?

We’ve been hunting this website malware using DNS for over two years. Bulletproof hosting and registrars, in combination with the cloaked nature of Detour Dog’s activity, has allowed infections to persist on sites for very long periods of time. When they moved from the scam delivery business to the information stealer business, we doubled our efforts to trace the threat actor’s history.

Earlier this year, we demonstrated that the DNS TXT C2 domains **broke into two distinct sets**. Each of these sets have distinct hosting and redirection patterns. Detour Dog refers to the actor who controls the larger set of domains, including those shown in Table 2 as well as those we have previously reported. We have not seen the smaller set since December 2024, and we are unable to definitively tie them to Detour Dog although they outwardly appear the same.

C2 Domain	First Seen	Last Seen
aeroarrows[.]io	August 1, 2025	August 6, 2025
airlogs[.]net	April 23, 2024	Current
cdn-routing[.]com	July 8, 2024	Current
webdmonitor[.]io	October 7, 2024	July 28, 2025

Table 2. C2 domains observed with remote file URLs in TXT records

We originally attributed Detour Dog to the Los Pollos affiliate identified in push monetization links by "CHiI7Gh3GUyTa8XGgNqDyQ". Specifically, this value was seen in URLs returned by Detour Dog for the "pl" parameter; we believe these are Taco Loco links. This affiliate id was **first seen in public sources** on August 20, 2023, consistent with **initial reporting** of the use of TXT records. The second, possibly unrelated, DNS C2 set contains a Los Pollos affiliate id, pe7k605, that dates to December 2019.

More recently, we extended our understanding of Detour Dog by locating attack chains that included both the known Detour Dog redirector domains and a **Los Pollos affiliate id**, bt1k60t. This affiliate id predates the use of DNS TXT records as a control mechanism and was only exposed for a few days while Detour Dog migrated from one TDS to another, but these few days allowed us to unwind several years of the threat actor's operations.

To explain how we unraveled the Detour Dog campaigns, we need to provide a little history of the change. On November 13, 2024, Qurium **disclosed** that Russian Dopplegänger disinformation campaigns leveraged Los Pollos to disguise their operations. Shortly after, Los Pollos announced to their affiliates that they were suspending their "push monetization" vertical. This vertical served fake CAPTCHAs that duped users into accepting browser notifications, creating a persistent mechanism to deliver scams to a device.

On November 17, Detour Dog routed site visitors to **Help TDS**, which then forwarded them to Los Pollos, where they received the fake CAPTCHA per usual. This change, visible in a **public scan**, provided critical clues to understanding the actor. In affiliate advertising platforms, there are unique identifiers for publishing affiliates (i.e., those who source traffic for the platform). Additionally, there are often parameters that can be set by the affiliate to track their own campaigns. Figure 5 shows the redirection chain from Detour Dog on that date. This series of redirects shows that following a visit to the infected site:

- The Detour Dog C2 redirected the user to infosystemsllc[.]com, which in turn redirected them to the Help TDS, as identified by the "help" path.
- The user entered the Help TDS with the affiliate id 32161731835980 and was redirected to a Los Pollos domain incomehub-your[.]on.
- Detour Dog configured the t (tracker) and cid (click id) parameters of their Los Pollos link to include cid:11005.
- The Los Pollos link also includes the affiliate id bt1k60t and the site is redirected to another domain, braraildye[.]live, hosted in Hetzner, which we believe is part of Taco Loco.
- The chain redirects through AS6898/AS5398, then through Amazon, before finally leading to a decoy page at Google.

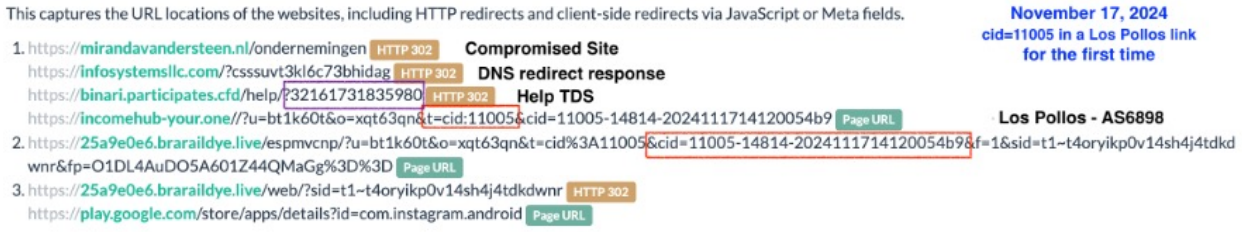

Figure 5. A Detour Dog redirect chain through Help TDS and Los Pollos, seen on November 17, 2024. This is the first time cid=11005 is observed in a Los Pollos smartlink. Credit **urlscan[.]io**.

The redirection chain in Figure 5 associates Detour Dog with the Help TDS affiliate id 32161731835980 and the Los Pollos affiliate id u=bt1k60t. This is also the first known time that the value “cid:11005” is used as a tracking parameter (t=) in a Los Pollos URL. Over the next few days, this behavior of redirecting through Help TDS to Los Pollos via these same affiliate ids continues.

On November 20, Detour Dog attack chains shifted to what they are today. Figure 6 shows a redirection chain from that date:

- Detour Dog redirects the infected site visitor to infosystemsllc[.]com, which immediately redirects to Help TDS.
- The Help TDS affiliate id is 32161731835980, and that causes a redirection to Monetizer TDS.
- The Monetizer URL contains “utm_campaign=cid:11005”, the exact value previously used by Los Pollos affiliate u=bt1k60t.
- The Monetizer URL contains a cid structured identically to that of the Los Pollos TDS.

Figure 6. A Detour Dog redirect chain through Help TDS and Monetizer, seen on November 20, 2024. The Monetizer cid value is constructed identically to the Los Pollos value seen on November 17th. Credit urlscan[.]io

These scans imply that Detour Dog had the Los Pollos affiliate id bt1k60t. We discovered that Detour Dog operations began well before DNS TXT records were used for a C2. The earliest known activity occurred on February 27, 2020, and the last time that affiliate id was observed was December 11, 2024. But using ids across affiliate programs and unusual tracker values, we uncovered more of the threat actor’s activity.

During the entire time that Detour Dog was an affiliate of Los Pollos, they were also an affiliate of Help TDS. Detour Dog uses a unique cid value for each Help TDS affiliate id. For example, cid:10 was used exclusively with Help TDS affiliate 51577283903. Combining the known Los Pollos and Taco Loco affiliate ids with the Help TDS values, we created a composite view of Detour Dog campaigns between February 2020 and September 18 of this year, shown in Figure 7.

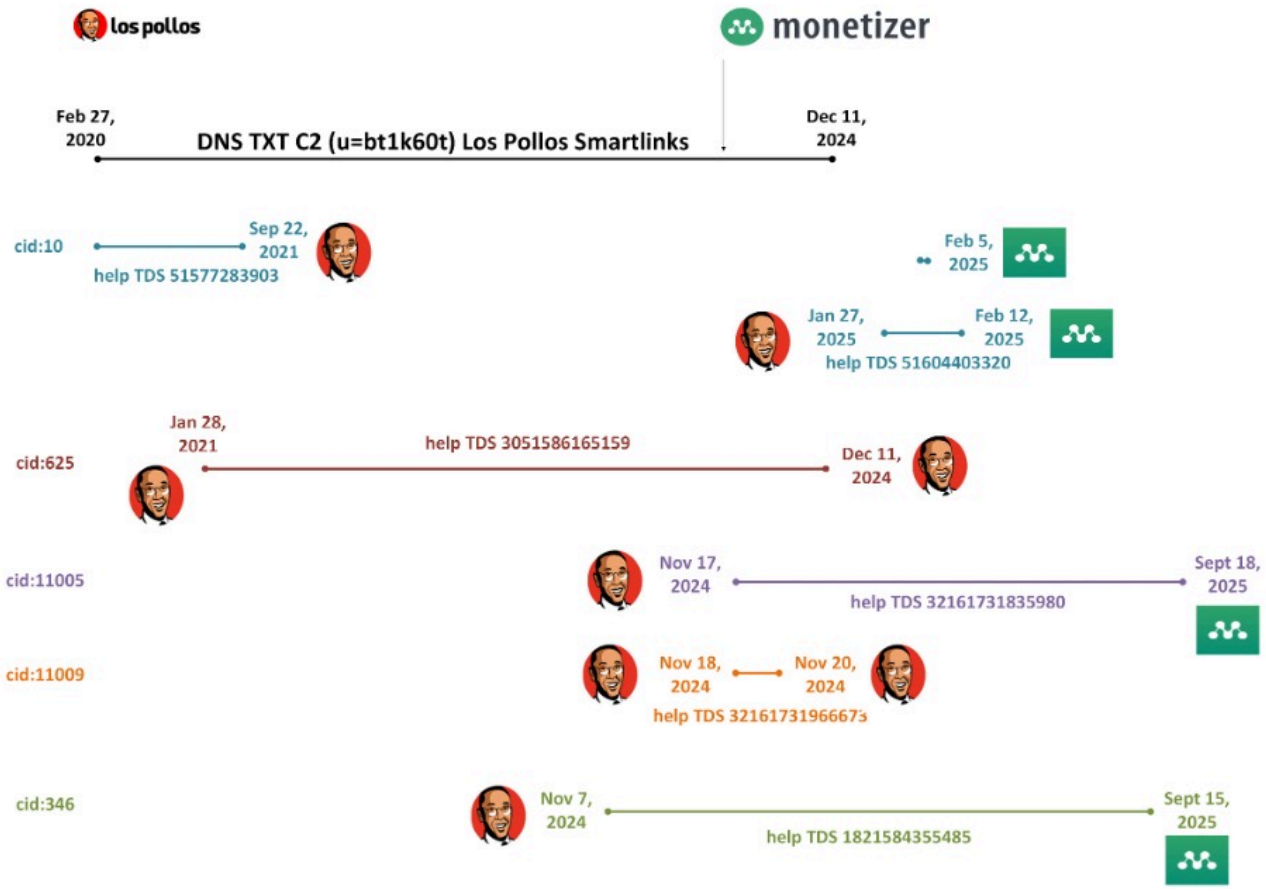

Figure 7. Timeline of Detour Dog flows observed via Los Pollos, Help TDS, and Monetizer, as tracked through affiliate ids and custom cid values. Details as of September 18, 2025. The logos shown are logos of the affiliate networks used by the actor. This timeline is created through analysis of data from urlscan[.]io and Infoblox Threat Intel independent open-source research.

Analysis uncovered other affiliate ids associated with Detour Dog, but their patterns remained consistent over the last five and a half years. It is unknown whether Detour Dog is a service provider or simultaneously operating campaigns of their own. While there is a one-to-one match between their help TDS affiliate id and cid values, Los Pollos and Taco Loco affiliate ids are used across multiple cid values.

Detour Dog uses bulletproof providers, but we collaborated with the Shadowserver Foundation to disrupt their DNS C2 not just once, but twice in August 2025.

Sinkholing the C2 Domain

We reported the Detour Dog domain, webdmonitor[.]io, to the registrar, WebNIC, on June 24, 2025. In a series of 16 email exchanges, we explained to the registrar how the website malware operated and the importance within the threat landscape. After WebNIC responded “We have notified the respective parties to investigate and take the necessary action” on June 26, we expected the domain to be suspended. It was not. We continued to pressure the registrar to act. We also reached out to .io registry and did not receive a response. On July 22, despite our demonstration of how to trigger a response from the malicious name server, WebNIC responded:

“While we acknowledge that the registrar is not responsible for the content hosted on a third-party site, registrars are responsible for responding to well-documented complaints involving domain name abuse. In this context, we also rely on respective parties and supporting evidence to investigate and take appropriate action. That said, based on our current assessment, the domain in question has remained inactive and has not shown any recent hosting or web activity for a considerable period.”

During our four-week exchange, WebNIC acknowledged abuse but then accepted their customer’s word that no malicious activity took place. They repeatedly responded with irrelevant answers, such as providing IPv4 (A) record responses instead of TXT responses. They did not place the domain on a client hold to suspend it at any point. In our view, WebNIC’s responses were inadequate to address the reported abuse. **ICANN independently sent WebNIC a notification** on July 29, 2025, for breach of registrar accreditation agreement.

On July 30, Shadowserver Foundation sinkholed the domain. Within hours, Detour Dog had replaced the C2 domain with aeroarrows[.]io, again registered with WebNIC. On August 6, Shadowserver sinkholed the new C2 and provided us with over 39 million queries received over approximately 48 hours to analyze.

Despite the brief collection window, this dataset surfaced compelling insights into the campaign’s global footprint. We observed approximately 30,000 unique domains spanning 584 distinct TLDs, all generating properly crafted DNS TXT queries to aeroarrows[.]io via web traffic originating worldwide. Within this set, just under 1% were queries with the new longer “type” associated to download commands.

We reviewed both the IP address distribution of the encoded “visitor” and that of the infected sites. The sheer volume of queries in such a short time indicated bot traffic. Within the IP addresses included in the queries, 89 countries were represented. The United States, Germany, and Taiwan stood out by unique IP volume, with the United States alone accounting for 37% of all the IP addresses identified visiting the compromised sites. But, the data was heavily skewed as well: two IP addresses accounted for nearly 3 million queries alone. The reason for this is a mystery.

Using the infected hostnames, we also looked at the hosting services and countries. Consider the infected site yy[.]ua, which we used as an example in Step 5 of our theorized attack chain earlier in this paper. There were nearly 2,500 queries for this domain in the collection. For several years, this site has shown content for a law office in Moscow, but starting in June 2025, it was observed many times in urlscan submissions. In one case, it has the telltale Detour Dog redirection signature, but in many others the submission URL contains **u=script** or u=file.

Surprisingly, the percentage of download-style queries for yy[.]ua is much higher than average: a whopping 30% of the queries for the domain. Of these, the vast majority contained “nwuutest” and we are unsure what the “test” may indicate. But over a hundred queries were for the script or file endpoints. Traditionally, the IP address encoded in the query was that of the website visitor, but the sinkhole data not only demonstrates large volumes of automated traffic but presents a mystery in how the queries related to the new type are created. The encoded IPs included addresses that are unlikely to be connected to human users, such as ones belonging to the U.S. Department of Defense. For example, 29[.]87[.]121[.]154, 215[.]226[.]38[.]106, and 33[.]35[.]245[.]179 were all seen in queries; the likelihood of these being a source of human traffic is very low.

How was this enormous volume of queries generated? Why does it contain IP addresses that don’t relate to human users? These are mysteries that might be resolved with direct access to the malware on the sites.

Find our released threat indicators for Detour Dog, Stela Stealer, and other threats on our GitHub **here**.

Note: Entities, brands, and intermediaries are mentioned in this report because telemetry or public records link them to the observed redirection chains. Mention alone does not imply knowledge of or participation in unlawful activity.
