Multi-Layered TDS Infrastructure Linked to Major Cyber Threats

By Insikt Group®

Archived: 2026-04-05 13:24:22 UTC

NOTE: This report was updated on May 12, 2025, after it was discovered that TAG-124 is unrelated to 404TDS. All references to 404TDS as an alias belonging to TAG-124 have been removed.

Executive Summary

Insikt Group has identified multi-layered infrastructure linked to a traffic distribution system (TDS) tracked by Recorded Future as TAG-124, which overlaps with threat activity clusters known as LandUpdate808, KongTuke, and Chaya_002. TAG-124 comprises a network of compromised WordPress sites, actor-controlled payload servers, a central server, a suspected management server, an additional panel, and other components. The threat actors behind TAG-124 demonstrate high levels of activity, including regularly updating URLs embedded in the compromised WordPress sites, adding servers, refining TDS logic to evade detection, and adapting infection tactics, as demonstrated by their recent implementation of the ClickFix technique.

Insikt Group identified multiple threat actors using TAG-124 within their initial infection chains, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGholish, D3F@CK Loader, TA582, and others. Notably, the shared use of TAG-124 reinforces the connection between Rhysida and Interlock ransomware, which are already linked through similarities in tactics, tools, encryption behaviors, ransom note themes, code overlaps, and data exfiltration techniques. Insikt Group expects that TAG-124 will continue its operations within the increasingly sophisticated and specialized cybercriminal ecosystem, enhance its effectiveness, and attract additional users and partners.

Key Findings

- Insikt Group identified multi-layered infrastructure linked to a TDS tracked as TAG-124. This infrastructure includes a network of compromised WordPress sites, likely actor-controlled payload servers, a central server, a suspected management server, and an additional panel, among other components.
- The threat actor(s) associated with TAG-124 appear highly active, regularly updating URLs on compromised WordPress sites to evade detection, adding new servers to their infrastructure, and improving TDS-linked conditional logic and infection tactics.
- Multiple threat actors are assessed to incorporate TAG-124's service into their initial infection chains, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGholish, D3F@CK Loader, TA582, and others.
- While Rhysida and Interlock ransomware have been associated with each other due to similarities in tactics, tools, encryption behaviors, ransom note themes, overlaps in code, and data exfiltration techniques, the shared use of TAG-124 reinforces this connection.

Background

TAG-124, which overlaps with LandUpdate808, KongTuke, and Chaya_002, is a TDS used to distribute malware on behalf of various threat actors, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGholish, D3F@CK Loader, and TA582, among others (1, 2, 3). A TDS typically refers to a system used to analyze and redirect web traffic based on parameters like geolocation or device type, funneling only specific visitors to malicious destinations such as phishing sites, malware, or exploit kits, while evading detection and optimizing cybercriminal campaigns.

More specifically, TAG-124 operates by injecting malicious JavaScript code into compromised WordPress websites. When visitors access an infected website, they unknowingly load attacker-controlled resources designed to manipulate them into completing actions that result in the download and execution of malware. TAG-124 often deceives victims by presenting the malware as a required Google Chrome browser update.

In more recent variations, TAG-124 has been observed using the ClickFix technique. This approach displays a dialog instructing visitors to execute a command pre-copied to their clipboard. Once a visitor runs the command, it initiates a multi-stage process that downloads and executes the malware payload.

Threat Analysis

TAG-124

Insikt Group identified multi-layered infrastructure associated with the TDS TAG-124. This infrastructure comprises a network of compromised WordPress sites, likely actor-controlled payload servers, a central server whose exact purpose remains unclear at the time of analysis, a suspected management server, and an additional management panel. If visitors fulfill specific criteria, the compromised WordPress websites display fake Google Chrome update landing pages, which ultimately lead to malware infections as discussed in the Users of TAG-124 section of this report (see **Figure 1**).

Compromised WordPress Websites

TAG-124's infrastructure consists of an extensive network of WordPress websites (see **Appendix A**). These websites appear to lack a consistent theme regarding industry, topic, or geography, suggesting they were likely compromised opportunistically through exploits or by acquiring credentials, such as those obtained via infostealers.

First-Stage WordPress Websites in Initial Delivery

The compromised websites of the first stage in the initial delivery phase typically include a script tag with an async attribute at an arbitrary location in the document object model (DOM), enabling the loading of an external JavaScript file in parallel with the page to avoid rendering delays (see **Figure 2**).

The JavaScript filename has changed frequently over time, with earlier names following recognizable patterns (such as metrics.js) and more recent ones appearing to be randomly formatted (such as hpms1989.js). Example filenames include:

- 3561.js
- 365h.js
- e365r.js
- hpms1989.js
- metrics.js
- nazvanie.js
- web-analyzer.js
- web-metrics.js
- web.js
- wp-config.js
- wp.js

Notably, the threat actors appear to be regularly updating the URLs on the compromised websites. For instance, the website associated with *www[.]ecowas[.]int* has consistently changed the URL used to fetch the JavaScript file. This behavior indicates that the threat actors maintain ongoing access to these WordPress sites and frequently alter the URLs, including the domain and JavaScript filename, likely to evade detection.

Although many of the compromised WordPress websites appear to be associated with lesser-known organizations, Insikt Group identified notable cases, including a subdomain linked to the Polish Centre for Testing and Certification, *www[.]pcbc[.]gov[.]pl*, and the domain of the Economic Community of West African States (ECOWAS) (*www[.]ecowas[.]int*). Both have been compromised and used in TAG-124 campaigns.

Final Stage WordPress Websites in Initial Delivery

If visitors meet specific criteria, which could not be fully determined, the compromised WordPress domains typically present fake Google Chrome update landing pages. These pages prompt users to click a download button, triggering the download of the actual payload from designated endpoints on a secondary set of compromised WordPress websites, including but likely not limited to:

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

Fake Google Chrome Update Landing Pages

Insikt Group discovered two variants of fake Google Chrome update landing pages associated with TAG-124 (see **Figure 3**). According to URLScan submission data, Variant 1 has been active longer, with its earliest submission recorded on April 24, 2024.

Only victims meeting a specific set of still unknown conditions are directed to the fake Google Chrome update landing page, resulting in the observation of only a limited number of domains (see **Table 1**). These domains can be attributed to TAG-124 based on the URLs embedded in the DOM, public reporting, or other indicators. Notably, the threat actors consistently misspell the word “referer” as “refferer” in the query parameter, a typographical error observed in earlier reports.
