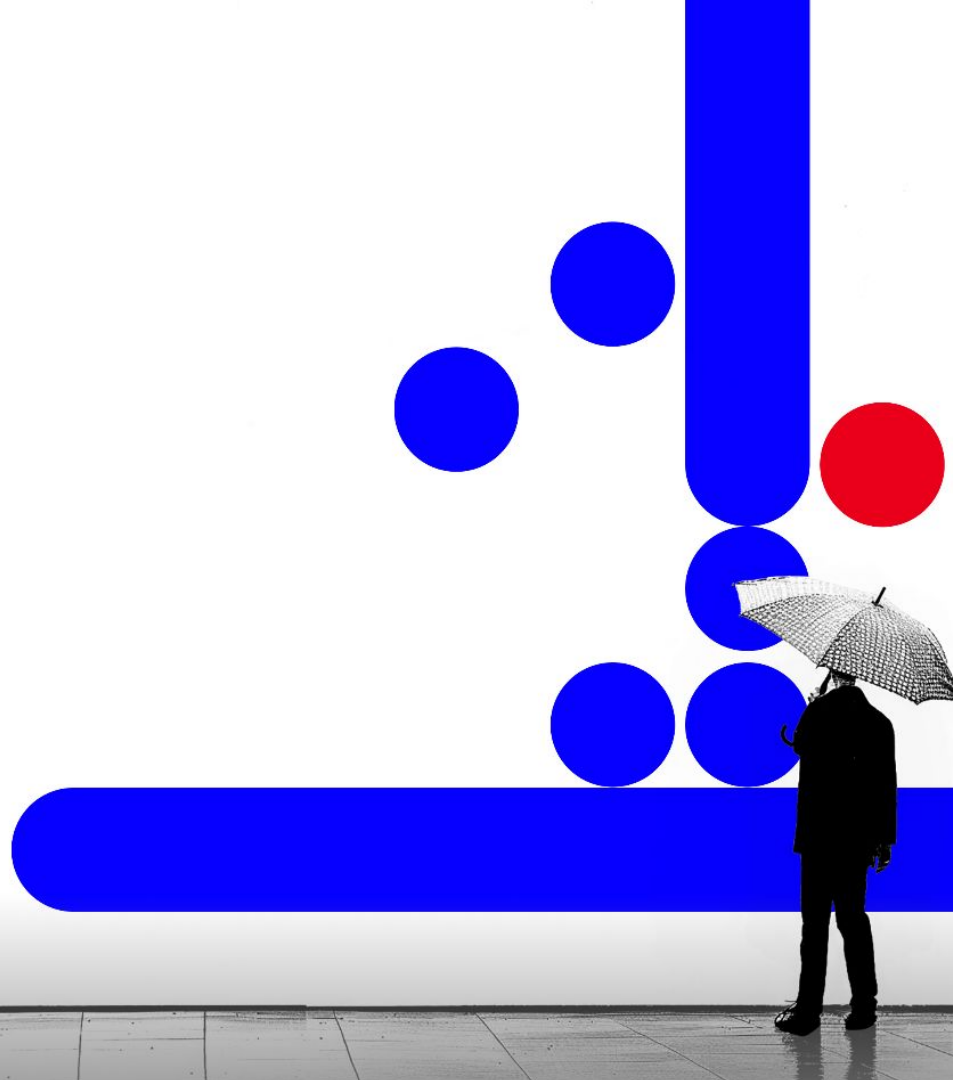
Recorded Future®

Unmasking TAG-124

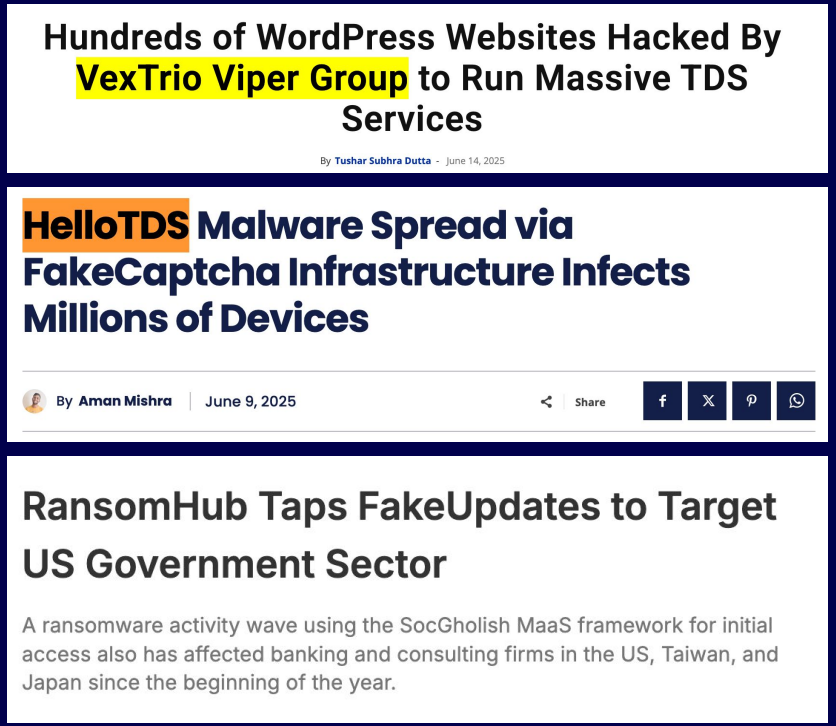
Julian-Ferdinand Vögele
Principal Threat Researcher
Virus Bulletin Berlin 2025



TDS Around Since Ever

In Many Shades of Existence

- Used to redirect victims' web traffic to malicious content based on specific factors
- Malicious and "benign" ones
- Around since many years, new ones popping up regularly
- Advantages: targeted, scalable, flexible, and evasive



Hundreds of WordPress Websites Hacked By VexTrio Viper Group to Run Massive TDS Services

By Tushar Subhra Dutta - June 14, 2025

HelloTDS Malware Spread via FakeCaptcha Infrastructure Infects Millions of Devices

By Aman Mishra | June 9, 2025 Share

RansomHub Taps FakeUpdates to Target US Government Sector

A ransomware activity wave using the SocGholish MaaS framework for initial access also has affected banking and consulting firms in the US, Taiwan, and Japan since the beginning of the year.

What Is TAG-124?

A Brief Background

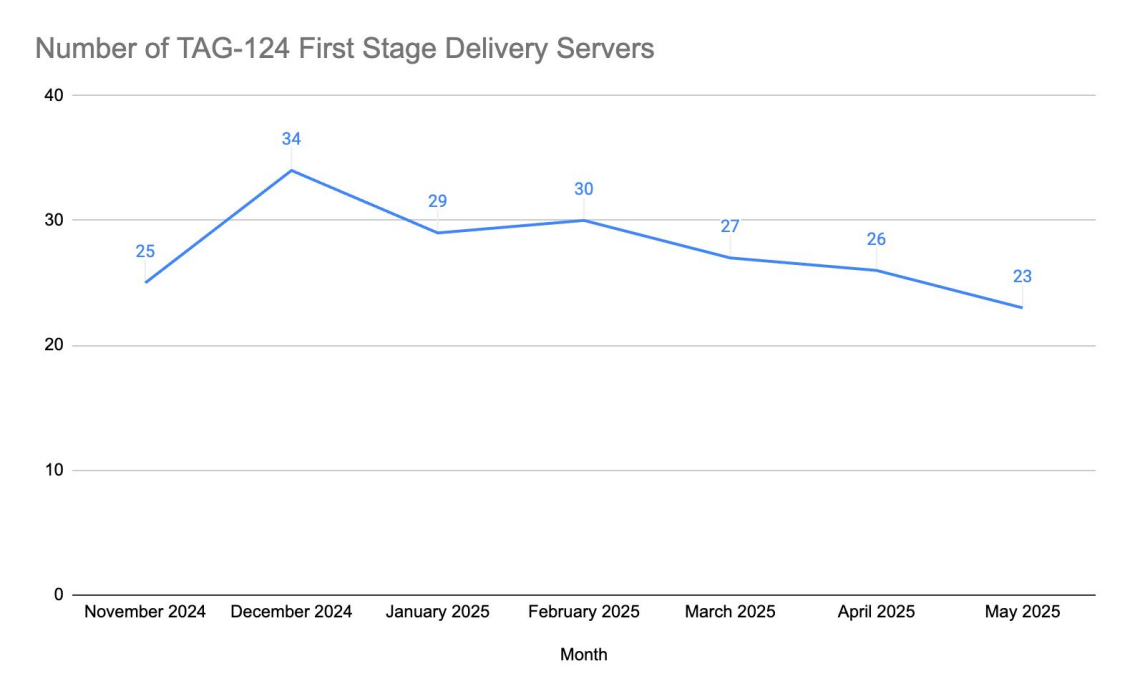
- Threat actor behind TDS, also known as LandUpdate808, KongTuke, or Chaya_002.
- First observed in early 2024 and has steadily expanded its user base since.
- Operates thousands of compromised WordPress sites along with actor-controlled infrastructure.
- Little is known about the individuals or group behind TAG-124 (so far anonymous).

Recorded Future, 2025

Malasada, 2024

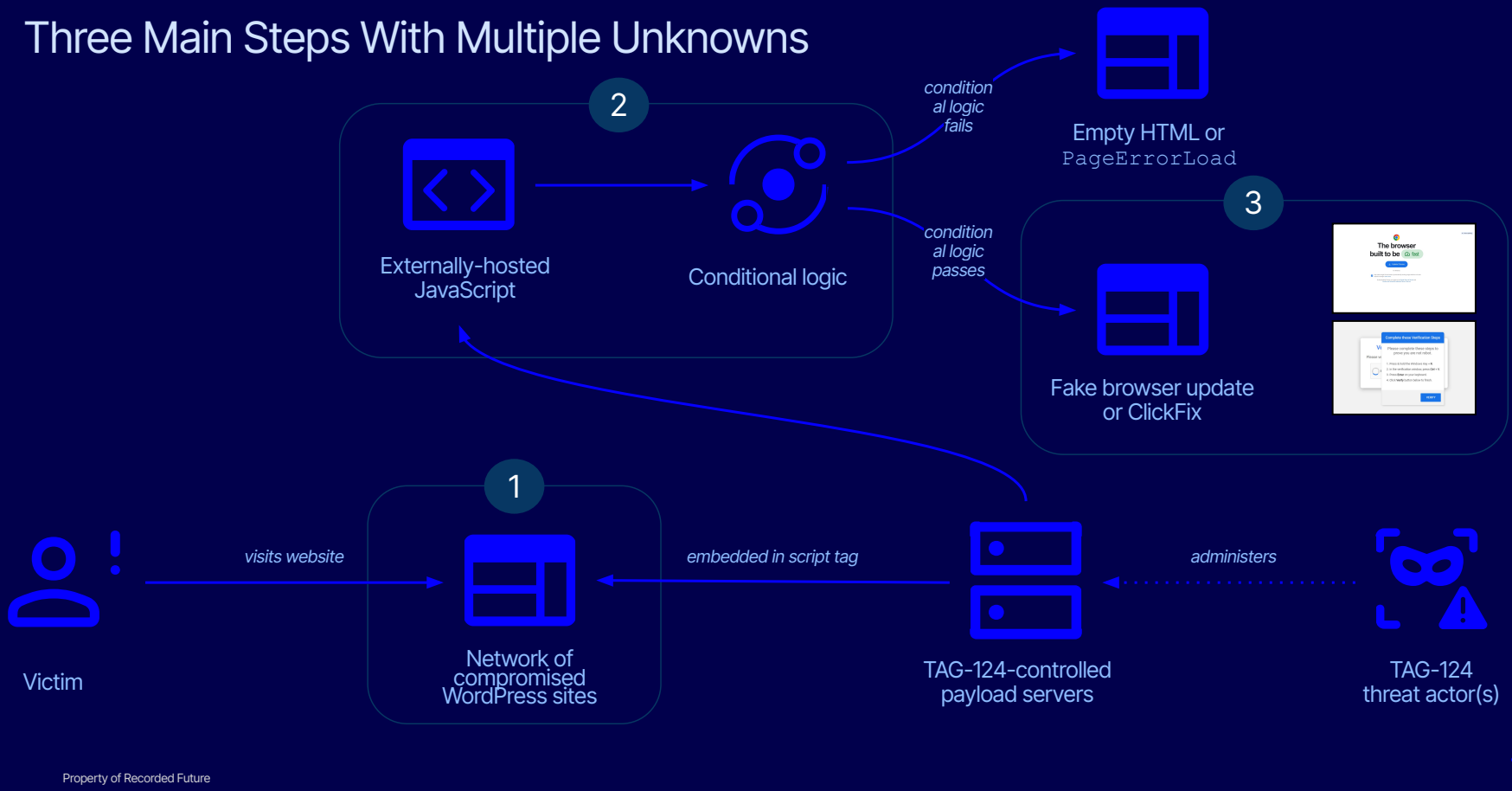
TAG-124's Activity Over Time

Activity Has Decreased, Possibly Due to Detection



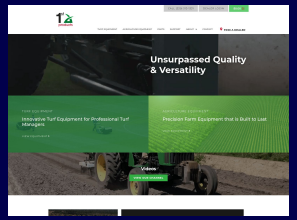
Overview of TAG-124 Infection Chain

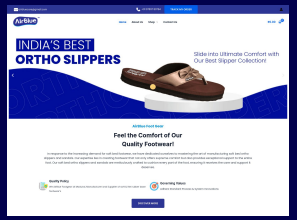
Three Main Steps With Multiple Unknowns

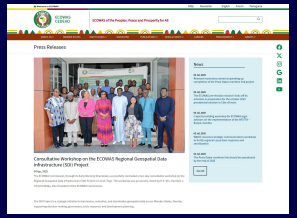


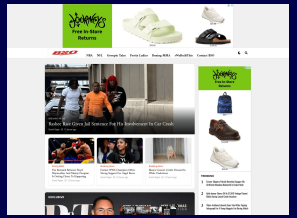
TAG-124's Infection Chain

Stage 1: Compromised WordPress Sites





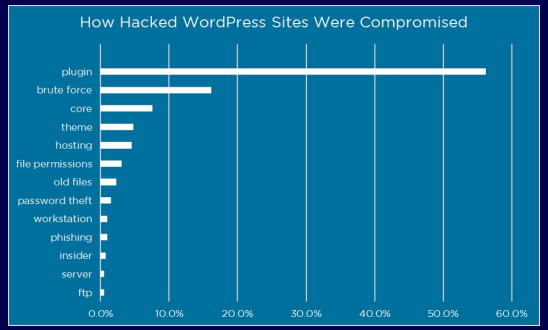




- 1000+ sites compromised.
- No specific sectoral or geographic targeting.
- Likely opportunistically compromised.
- Mostly WordPress 6.7.2, some on 6.7.1 and 6.6.2, suggesting generally up-to-date installations.

TAG-124's Infection Chain

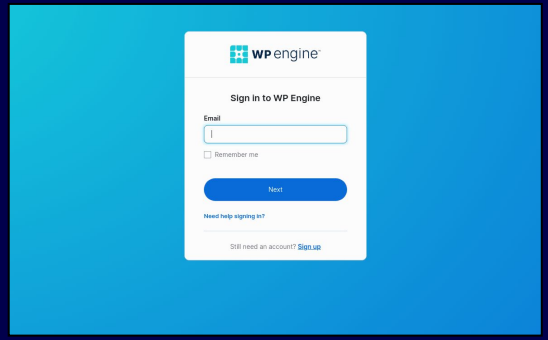
Stage 1: Compromised WordPress Sites



- WordPress plugin exploitation?
- Generally quite common vector.

```
3hti[.]com
academictutoringcenters[.]com
adpages[.]com
adsbicloud[.]com
advanceair[.]net
airbluefootgear[.]com
airinnovations[.]com
allaces[.]com[.]au
alumni[.]clemson[.]edu
ambir[.]com
americanreloading[.]com
antiagewellness[.]com
architectureandgovernance[.]com
astromachineworks[.]com
```

- Credentials from stealer logs?
- Numerous WordPress admin credentials observed for sale.



- Spear-phishing or SEO poisoning?
- Large number of WordPress-themed typosquatting domains linked to TAG-124 cluster.

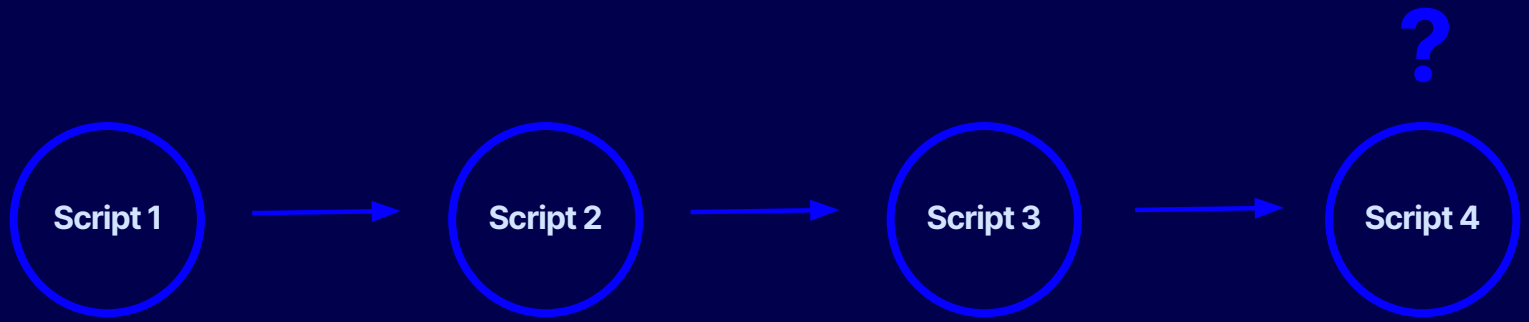
A Little Thought Experiment

Not Even That Unlikely

1. **Traffic is highly skewed:** ~1% of sites capture ~90% of visits, and these large sites are generally secure and rarely WordPress.
2. **Risk lies in the long tail:** Small/medium sites make up 10% of traffic, with ~44% using WordPress.
3. **Vulnerabilities concentrated:** 20–30% of WordPress sites run vulnerable versions (plugins, themes, or core).
4. **Per-pageview probability:** ~0.9%–1.3% chance that any given pageview hits a vulnerable WP site.

TAG-124's Infection Chain

Stage 2: Conditional Logic



Sets `isCompleted` cookie for 4 days if missing to prevent repeated actions (e.g., by bots)

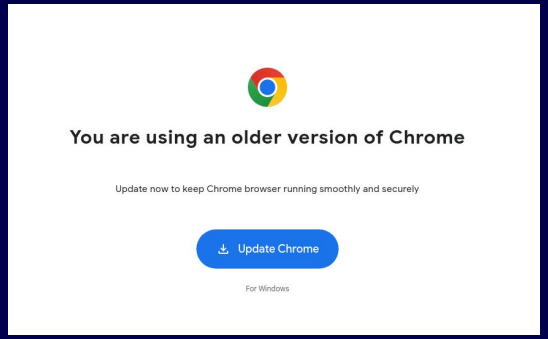
Collects system info (e.g., OS, IP, location), encodes it, and queries Cloudflare for trace data.

Sends data to C2 endpoint with rotating .php filename.

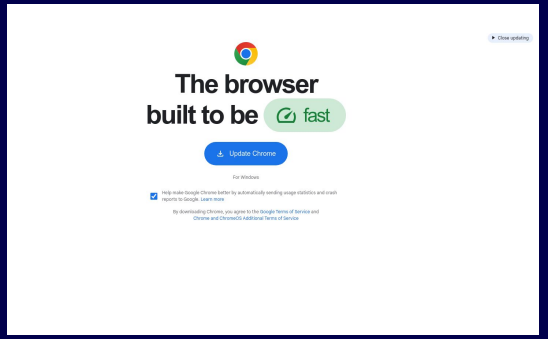
If C2 response ≥35 bytes, injects next-stage payload; else reloads page.

TAG-124's Infection Chain

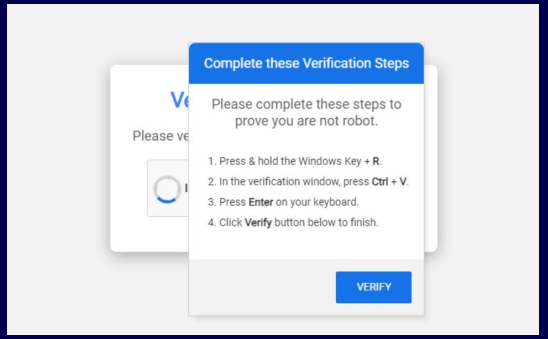
Stage 3: Fake Browser Updates or ClickFix Using JavaScript



Fake browser update variant 1
first seen in April 2024



Fake browser update variant 2
first seen in second half of 2024



ClickFix first seen in
beginning of 2025 (most recently also
FileFix)

TAG-124: ClickFix

ClickFix Usage of TAG-124 Aligns with Industry Trend

Infosecurity Magazine, 2025

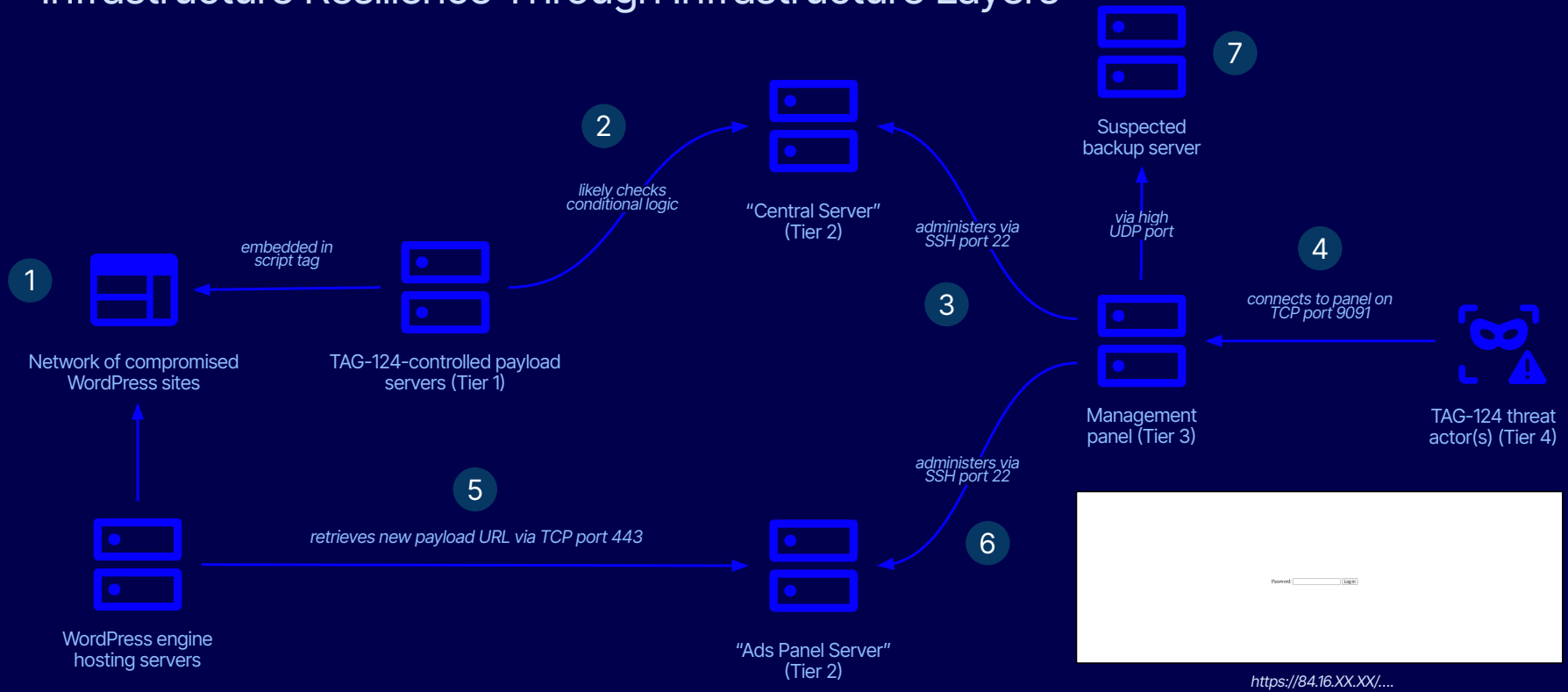
Proofpoint, 2025

- Advantages:
  - More evasive
  - User-convincing
  - More versatile

- State-sponsored actors use it too

TAG-124's Multi-Tiered Infrastructure

Infrastructure Resilience Through Infrastructure Layers



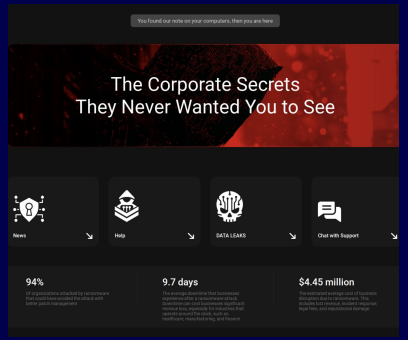
Users (or Customers) of TAG-124

Actual Relationship Between Users and TAG-124 Often Not Entirely Clear

Who Is Interlock?

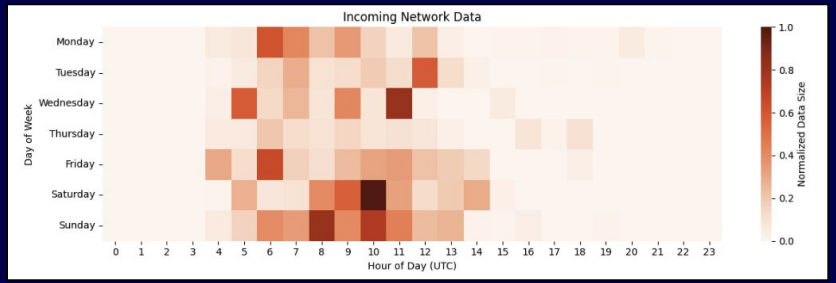
Increasingly Active, Likely Non-Affiliate Actor

- Active since at least September 2024, focused on legal, health, and critical infrastructure.
- Believed to have ties to the Rhysida and likely Russia-based.
- Does not operate as an affiliate model.

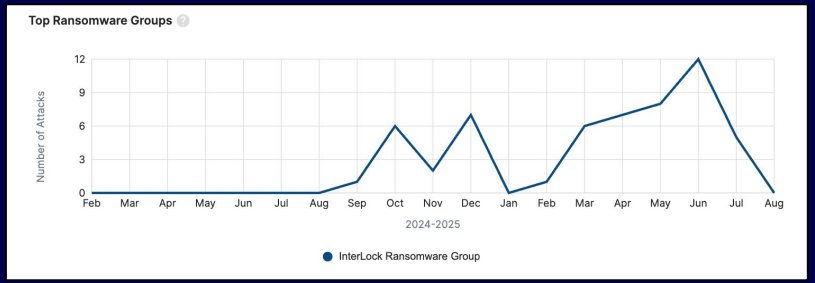


Interlock, 2025

CISA, 2025



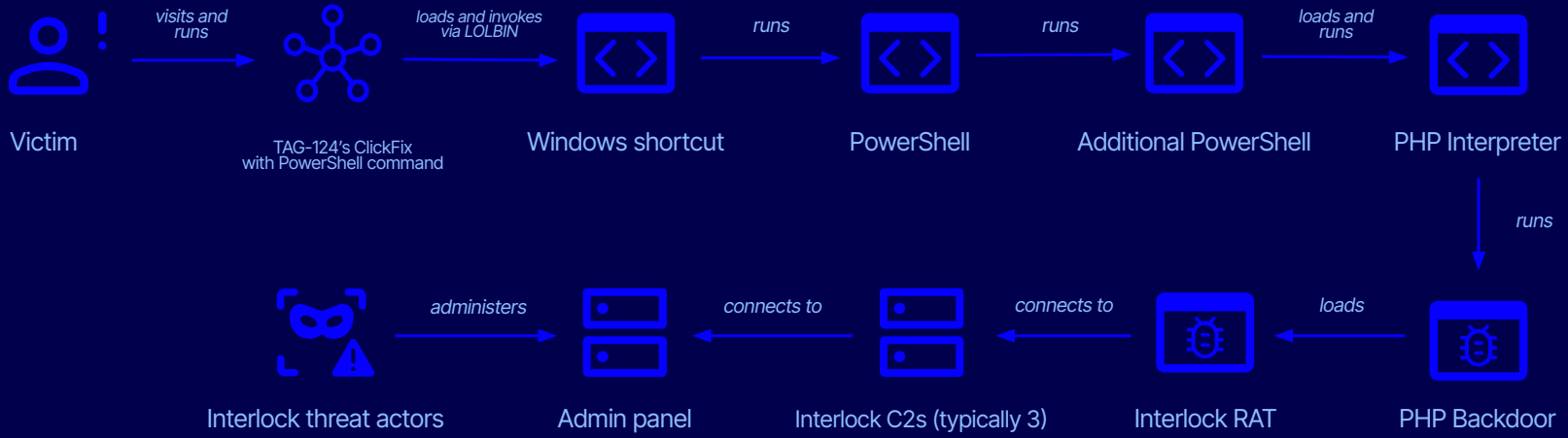
Recorded Future, 2025



Recorded Future, 2025

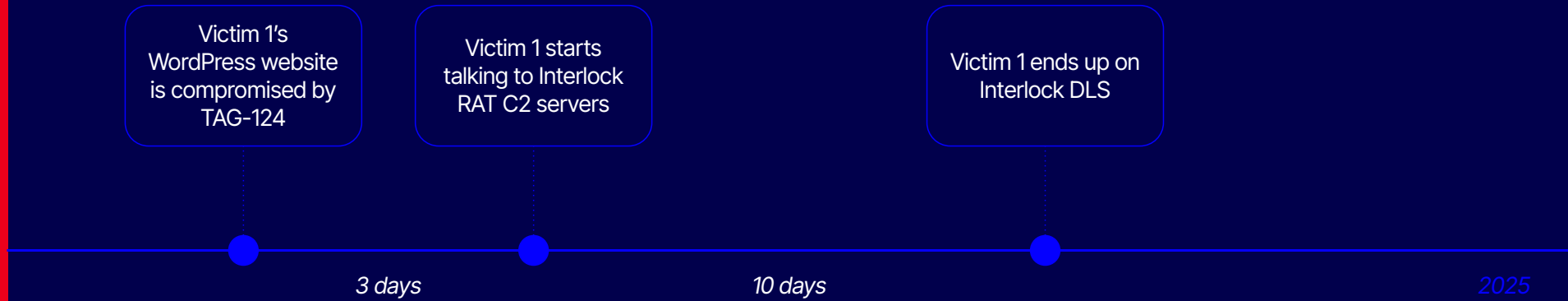
How Has Interlock Been Using TAG-124?

From ClickFix to PowerShell to Custom Tooling



Special Connection Interlock and TAG-124?

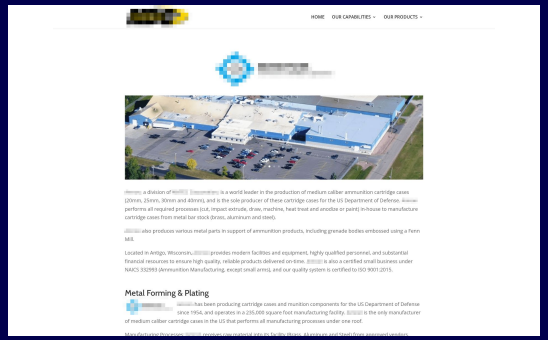
Similar Victim Overlaps In Close Time Frames Happened At Least 3 Times



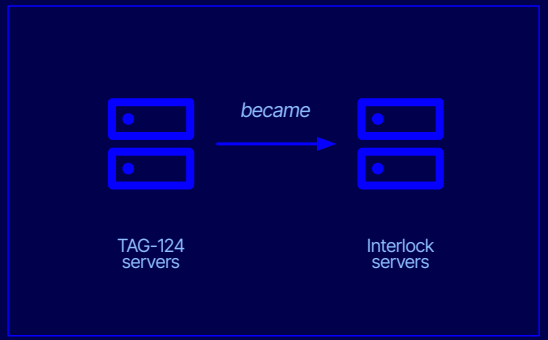
Coincidence?

Overlap Observed in Both Victims and Infrastructure

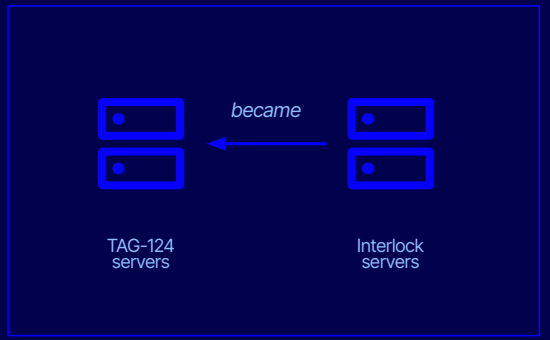
Infrastructure Movement Between TAG-124 and InterLock



Multiple shared victims in close time frames



Interlock servers became TAG-124 servers and talked to TAG-124's Tier 2



TAG-124 became Interlock servers and talked to Interlock's Tier 2

So What?

Possible Explanations

So Far Only Speculations

1. Coincidence?
2. Same group, different business model?
3. Close collaboration?
4. Shared services such as IABs and/or infrastructure providers?
5. Staff overlap?

So What?

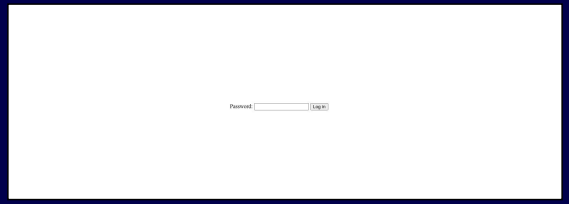
Some additional thoughts

Many Open Questions

- Where does TAG-124 advertise its TDS?
- How effective is it?
- Who is behind it?
- And: is there any special connection with Interlock?

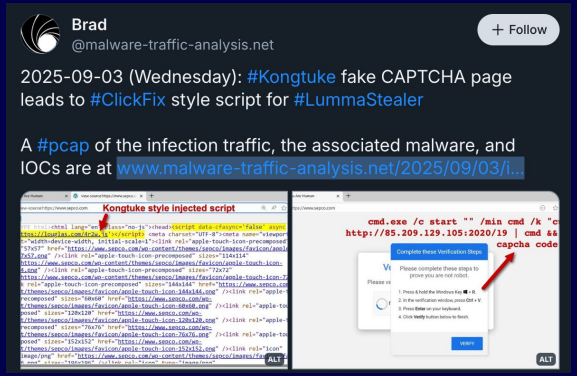
Analytical Difficulties

- Likely closed circles
- Highly anonymous (e.g., compromised, crypto, RU)
- Little footprint in general



What To Expect?

- Continued adaptation
- Possible change in infra
- New customers (!)



Thank you

Julian-Ferdinand Vögele
julian.vogele@recordedfuture.com
@julianferdinand.bsky.social