Team Cymru Cybersecurity Blog | Threat Research and Intelligence

By Annika Martins

Archived: 2026-10-29 02:37:11 UTC

1. Home
2. Resources
3. Blog

Team Cymru Blog

Cybersecurity Research from the Front Lines

Threat research, infrastructure analysis, and operational guidance from the Team Cymru intelligence team, drawn from the global network visibility we maintain across the internet.

Who
: Team Cymru threat analysts and researchers, with a named byline on technical posts.

What
: Named threat actors, mapped command-and-control infrastructure, ransomware toolkit teardowns, and the pivots behind them.

How
: Sourced from Team Cymru's own internet-scale network telemetry, not third-party feeds or aggregated reporting.

Research Library

Find research by threat, problem, or role

Every article carries the same Team Cymru tags as the rest of the site. Stack filters to narrow fast, or tap a category on any card.

177 articles

Search articles

Sort articles

3 min read

October 22, 2026 · *Annika Martins*

From Serengeti to Serengeti III: What Three INTERPOL Operations Reveal

INTERPOL's Operation Serengeti has led to 3,677 arrests across three operations since 2024. What changed from Serengeti to III, and what it means for defenders.

3 min read

October 14, 2026 · *Will Thomas*

LegionRelay: Ukraine Targeted by Five Previously Unidentified C2 Servers

See how threat hunting in Team Cymru Scout surfaced five previously unreported LegionRelay C2 servers tied to a Russia-aligned campaign targeting Ukraine.

5 min read

September 22, 2026 · *Scott Fisher*

Relaying to the Frontier

Team Cymru uncovered self-hosted LLM gateways relaying pooled credentials to frontier models like Claude, enabling model distillation and abuse.

4 min read

September 15, 2026 · *Will Thomas*

From the Disk to the Flows: Ransomware Infrastructure Analysis

A year of incident response data reveals how Akira, DragonForce & Clop build ransomware infrastructure — and how defenders can hunt it.

3 min read

September 2, 2026 · *Team Cymru*

The Transaction Is the Last Step, Not the First

Waiting for the transaction to catch fraud? You're already too late. Learn how tracking attack patterns in threat intelligence stops actors early.

5 min read

August 12, 2026 · *Eli Woodward*

Cl0p Til you Drop - 6 Years, 10 Campaigns, 8 Zero-Days

Analyze Cl0p ransomware's history of targeting MFT systems. Discover their attack pattern in threat intelligence to improve cyber attack surface reduction.

5 min read

August 5, 2026 · *Stephen Campbell*

Behind the Panels: Validating ShinyHunters Cluster A Infrastructure Through Network Telemetry

Use network telemetry to validate cyber threat actors' phishing infrastructure. Track ShinyHunters clusters and defend against SaaS data exfiltration.

3 min read

July 27, 2026 · *Josh Picolet*

From C2 Detection to Possible Victim Identification

Discover how to transition from C2 detection to possible victim identification. Improve your cyber incident response by tracking attacker infrastructure to compromised systems.

2 min read

July 14, 2026 · *Abigail Lorion*

Modernizing Incident Response: 4 Steps to Bulletproof Your Windows Logging

Improve your cyber incident response steps with our guide to bulletproof Windows logging. Discover incident response tools and how AI streamlines DFIR.

Showing 9 of 177 articles

Stay in the loop

Stay current with Team Cymru insights

Get the latest research, articles, and threat intelligence resources, delivered straight to your inbox.

Engage with Team Cymru and the Threat Intelligence Community

Connect with the global defender community and stay current with Team Cymru research, events, and conversations.

Source: https://blog.team-cymru.com/2020/02/19/azorult-what-we-see-using-our-own-tools/