Group: Essential Group	Report Number: Report No15	Report id 15lec30&31(Malicious Attachments&urls)13essential

MALICIOUS URL

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Date of Task Assignment :

4/5/2026

Due Date:

4/13/2026

Contents

Introduction

This report presents the findings of a Fullscope malicious URL investigation conducted as part of SOC Analyst exercise. The investigation was initiated in response to a simulated phishing email campaign targeting organizational employees through a chain of malicious URLs. The primary objective was to trace each target URL from its surface level presentation to its underlying infrastructure, correlate all identified threat indicators, and produce a structured intelligence report reflecting professional SOC methodology.

A total of 21 target URLs were investigated across five analytical phases: Initial Analysis, Deep Analysis, Technique Identification, Risk Assessment, and Reporting. Each target was approached with a consistent scanning workflow Virus Total was executed first on every target to establish a vendor detection baseline and gather metadata, followed by Shodan for infrastructure and host profiling, and ANY.RUN for dynamic sandbox execution where applicable. This sequence is preserved throughout the report.

Target 1 https://informacoeslimpabrasil2026.netlify.app/

This URL serves as the primary entry point of the phishing campaign. Hosted on Netlify's platform, it exploits the trusted reputation of a major cloud provider to reduce the detection by automated security systems. The domain name is constructed in Brazilian Portuguese and translates loosely to "limpa brasil 2026 information," mimicking the branding of a legitimate Brazilian civic or financial service. Netlify's automatic HTTPS provisioning means the page is served over a valid TLS certificate, further lending it a false appearance of legitimacy to unsuspecting users.

Virus Total Analysis

Virus Total analysis of the Netlify URL returned a detection ratio of 2 out of 95 vendors, with ADMINUSLabs classifying it as malicious and ESET identifying it as a phishing page. The HTTP status code at time of analysis was 404, indicating that the page had been taken down or rotated a common operational security practice in active phishing campaigns to limit exposure after the initial wave of targeted emails has been delivered.

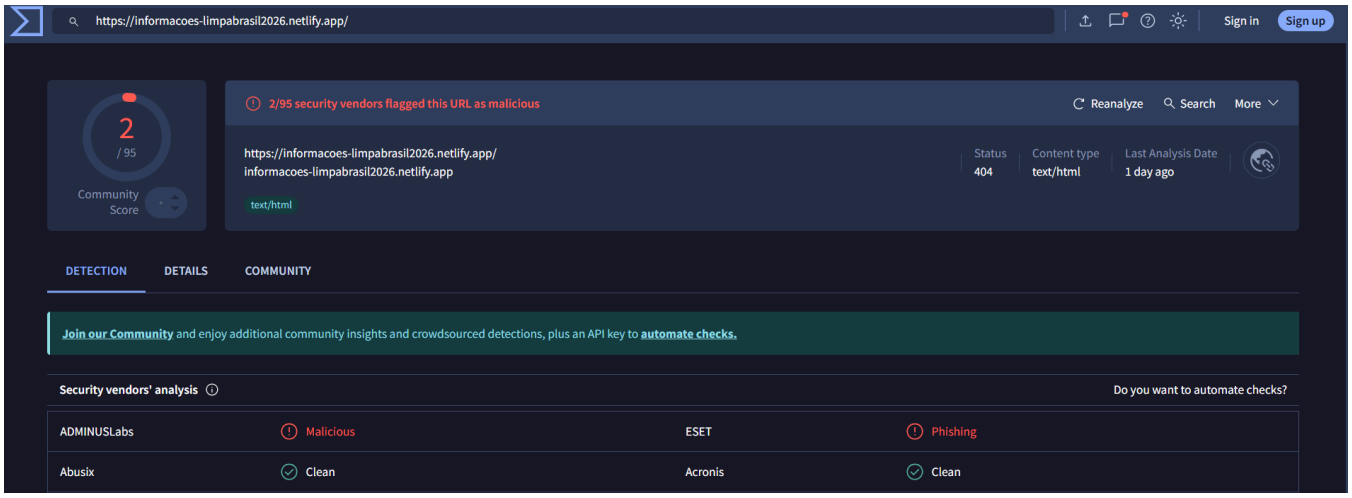


Figure 1.1: VirusTotalinformacoeslimpabrasil2026.netlify.app (2/95 Detections)

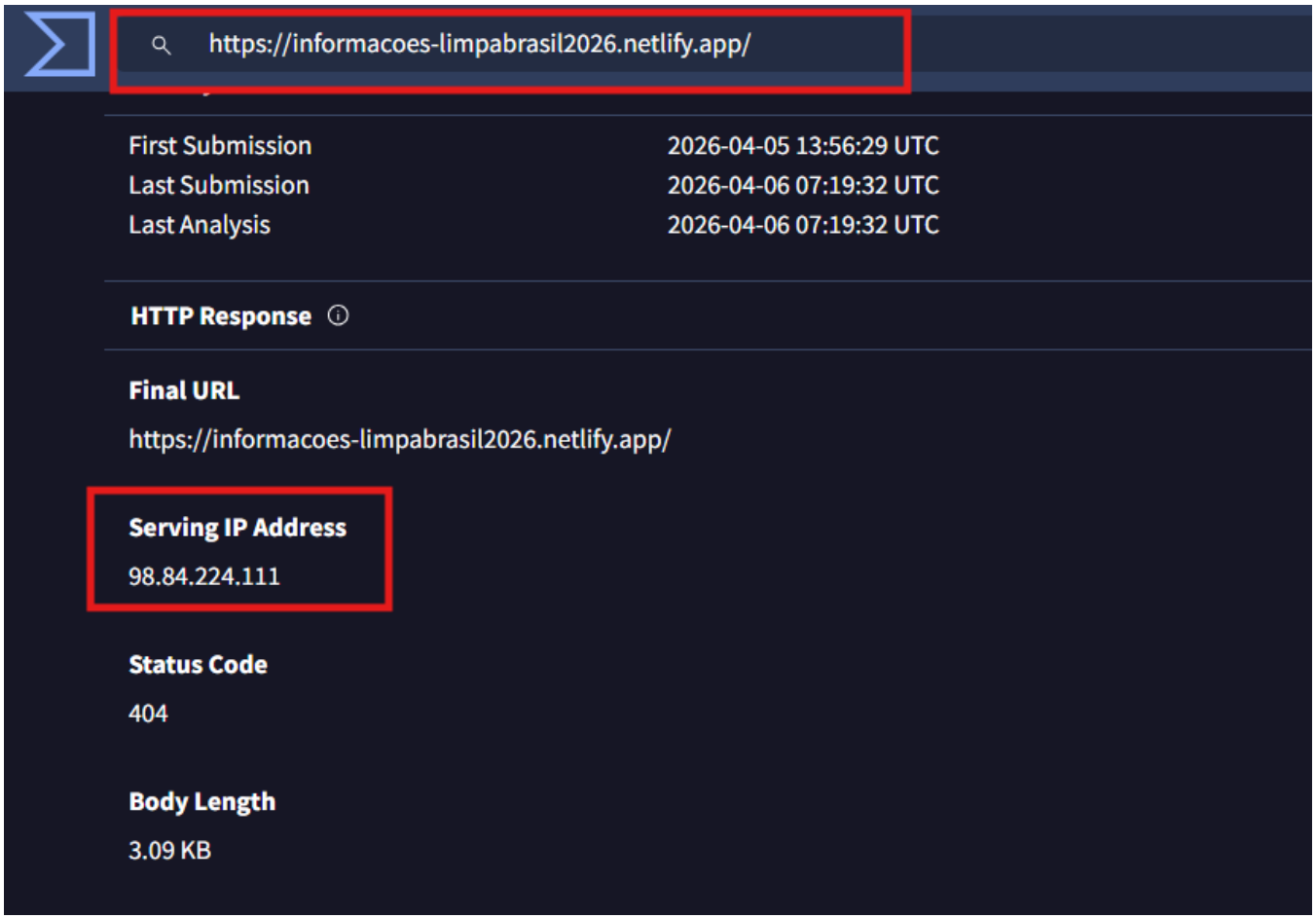


Figure 1.2: VirusTotal DetailsServing IP 98.84.224.111 and Submission History

Shodan Infrastructure Analysis

Shodan analysis of the serving IP address 98.84.224.111 confirmed the host as an Amazon Web Services EC2 instance operating within the useast1 region, registered to Amazon Data Services NoVa under ASN AS14618. The host presents open ports 80 and 443, corresponding to standard HTTP and HTTPS services, and carries the hostnames ec29884224111.compute1.amazonaws.com and netlify.app. This confirms that the phishing entry point leverages shared Netlify infrastructure, meaning that blocking this IP would also affect legitimate Netlifyhosted content. The threat actor has deliberately chosen this hosting environment to complicate IPlevel blocking responses.

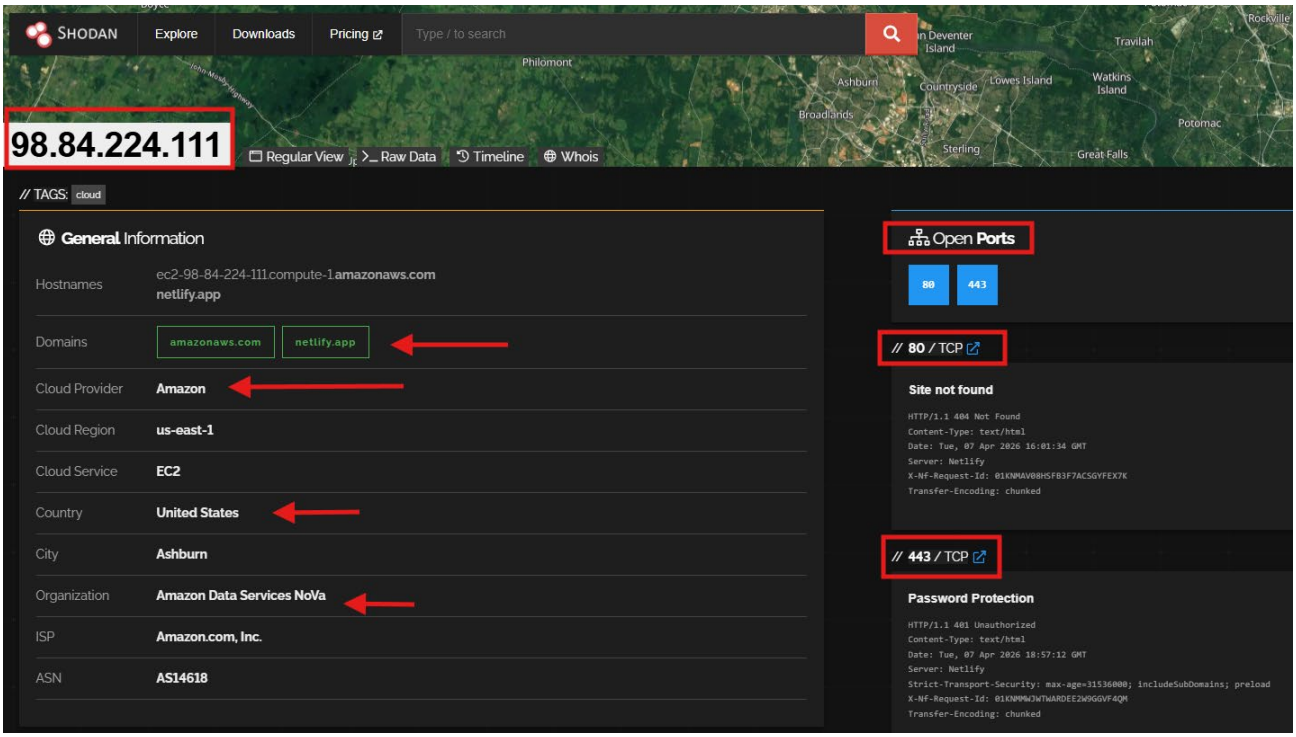


Figure 1.3: ShodanIP 98.84.224.111 (Netlify/AWS EC2 Infrastructure)

ANY.RUN Sandbox Analysis

Dynamic analysis of the URL in the ANY.RUN interactive sandbox was conducted on April 8, 2026 at 08:04 UTC. The sandbox environment simulated a Windows 10 64bit system with Microsoft Edge as the primary browser process (msedge.exe, PID 2576). Execution completed in 38 seconds, during which 18 processes were spawned. The sandbox's initial verdict was "No threats detected," representing a deliberate false negative produced by the phishing page's use of legitimate cloud infrastructure and HTTPS encryption, which bypasses signaturebased detection. Network activity during execution recorded 43 HTTP requests, 39 DNS queries, and 42 TCP/UDP connections, with one threat indicator flagged.

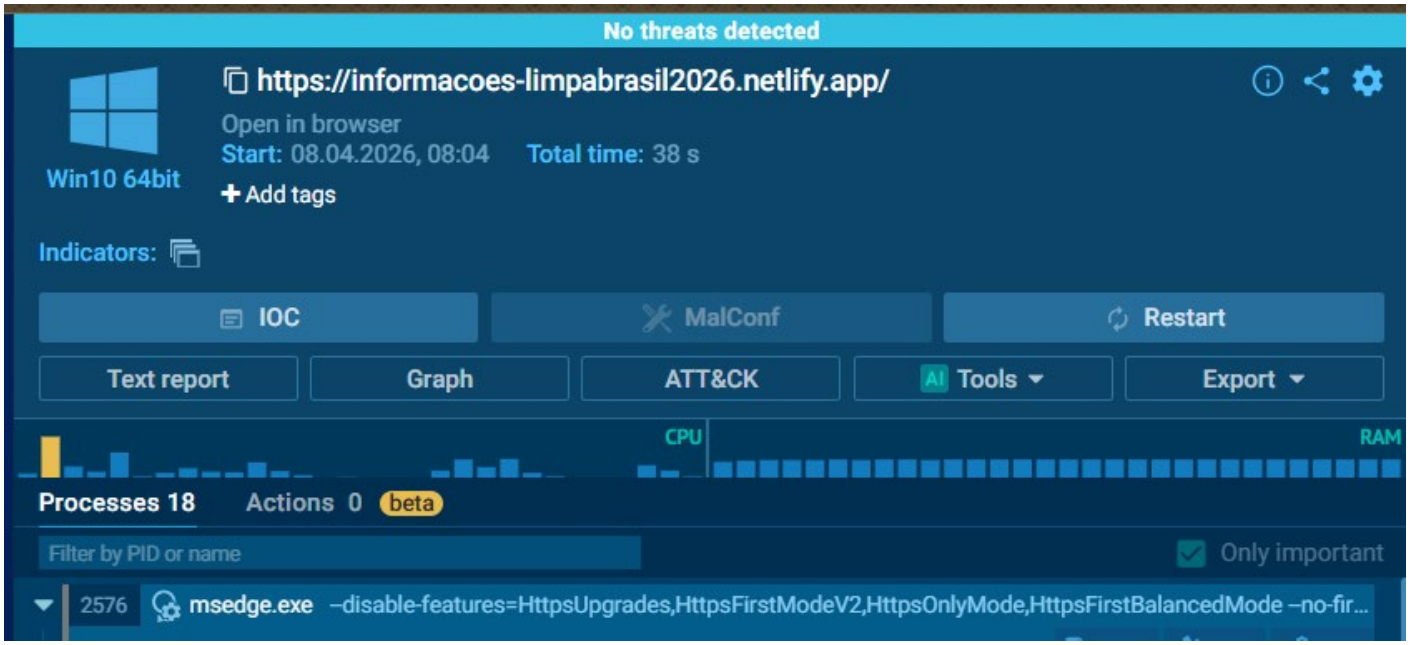


Figure 1.4: ANY.RUN Sandbox OverviewInitial URL Submission and Process List

Figure 1.5: Network Activityinformacoeslimpabrasil2026.netlify.app (43 HTTP, 39 DNS, 1 Threat)

Target 2 https://walletedinar.com/

walletedinar.com represents the primary credential harvesting domain within this campaign and carries the highest VirusTotal detection ratio of any URL in the phishing chain. The domain name is designed to evoke associations with digital financial servicesa deliberate social engineering choice targeting users who may be expecting communication from a payment or wallet platform. The HTTPS variant of this domain is the principal phishing endpoint toward which victims are funneled following the initial Netlify redirect.

VirusTotal Analysis

VirusTotal analysis of the HTTPS variant of walletedinar.com returned a detection ratio of 19 out of 95 vendors, making it the most widely flagged URL in the campaign. The detecting vendors include ADMINUSLabs, BitDefender, ESET, Fortinet, Sophos, Netcraft, and Webroot a crosssection of both reputationbased and heuristic security engines. The content type returned was image/png with an HTTP status of 200, indicating that the page was actively serving content at the time of analysis. The full vendor breakdown confirms that this domain is recognized as a phishing infrastructure by all major commercial security platforms.

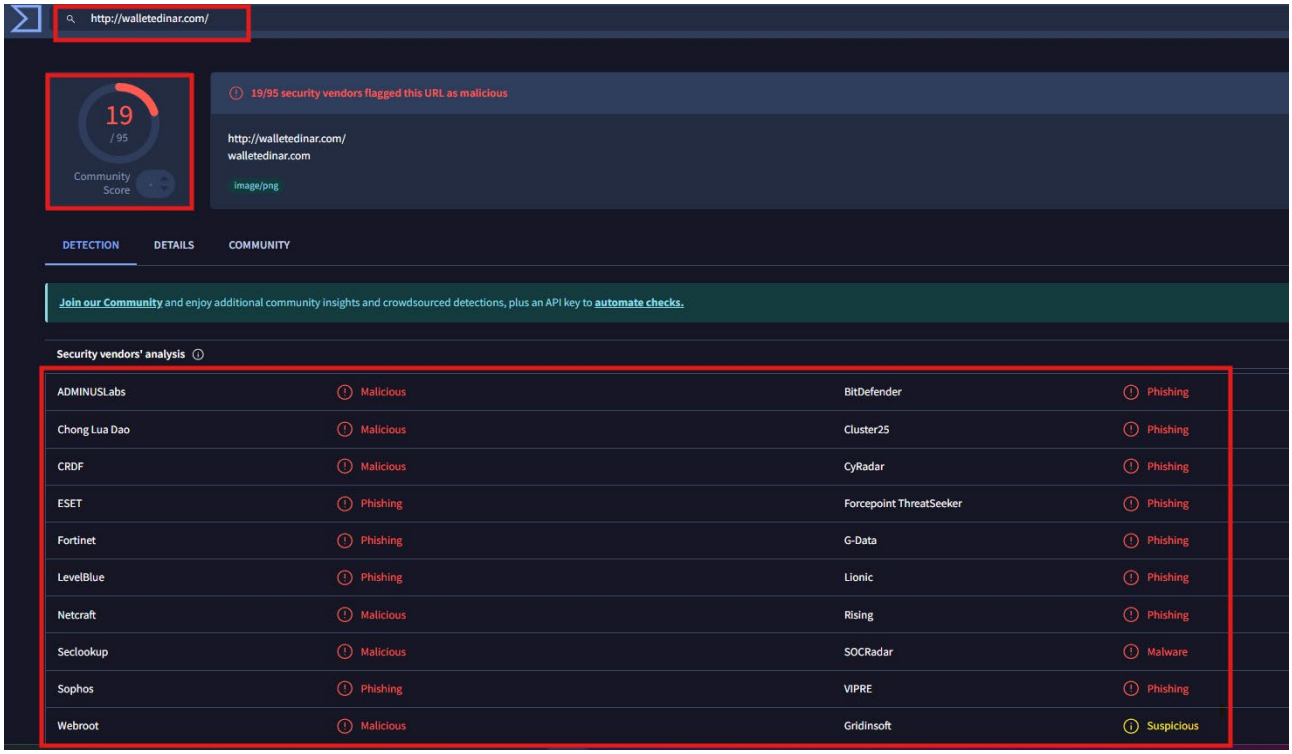


Figure 2.1: VirusTotalwalletedinar.com HTTPS (19/95 Phishing Detections)

ANY.RUN Sandbox Analysis

Sandbox analysis of walletedinar.com produced 39 HTTP requests, 47 DNS queries, and 52 TCP/UDP connections, with one threat indicator recorded. The network activity pattern is consistent with a credentialharvesting page that loads external resources to render a convincing login form. The HTTP request detail captured during the sandbox session reveals the specific resources fetched by the browser during page rendering, confirming active content delivery at the time of analysis.

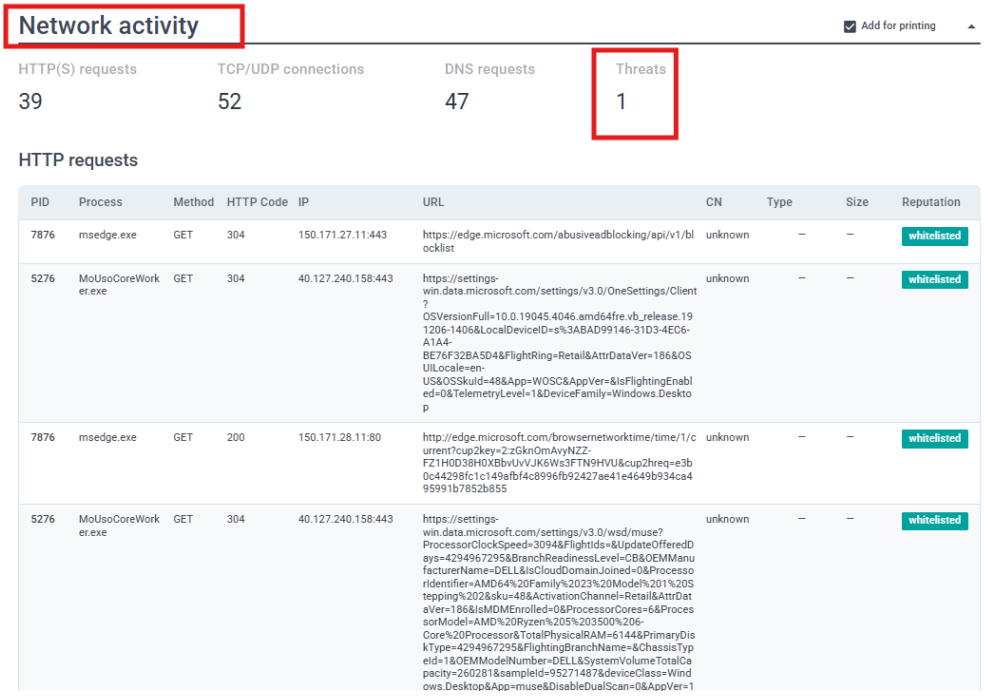


Figure 2.3: Network Activitywalletedinar.com (39 HTTP, 47 DNS, 1 Threat)

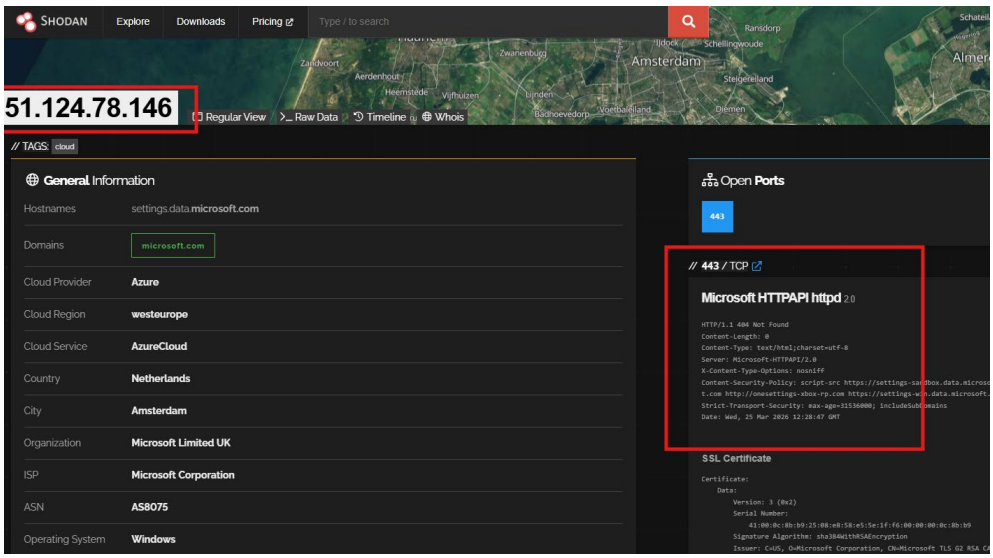


Figure 2.4: HTTP Request Detailwalletedinar.com Traffic

Target 3 https://skillwicked.cc/

skillwicked.cc functions as the attack resource server within this campaign, responsible for serving the CSS stylesheets, images, video content, and JavaScript libraries that render the phishing pages delivered to victims. Rather than hosting the credential form itself, this domain acts as the content delivery backbone of the attack infrastructure. It is proxied through Cloudflare's CDN, which conceals the true origin IP address and provides the domain with Cloudflare's Universal SSL certificate, lending it an additional layer of apparent legitimacy.

VirusTotal Analysis

VirusTotal analysis of skillwicked.cc returned a relatively low detection ratio of 3 out of 95 vendors. However, this figure is misleading in isolation: the domain's true significance is revealed through dynamic sandbox analysis, which recorded 9 threat indicators during execution the highest threat count of any domain in the campaign. The low static detection ratio reflects the effectiveness of Cloudflare proxying in obscuring the domain's malicious nature from reputationbased scanning engines that have not yet updated their threat databases to include this infrastructure.

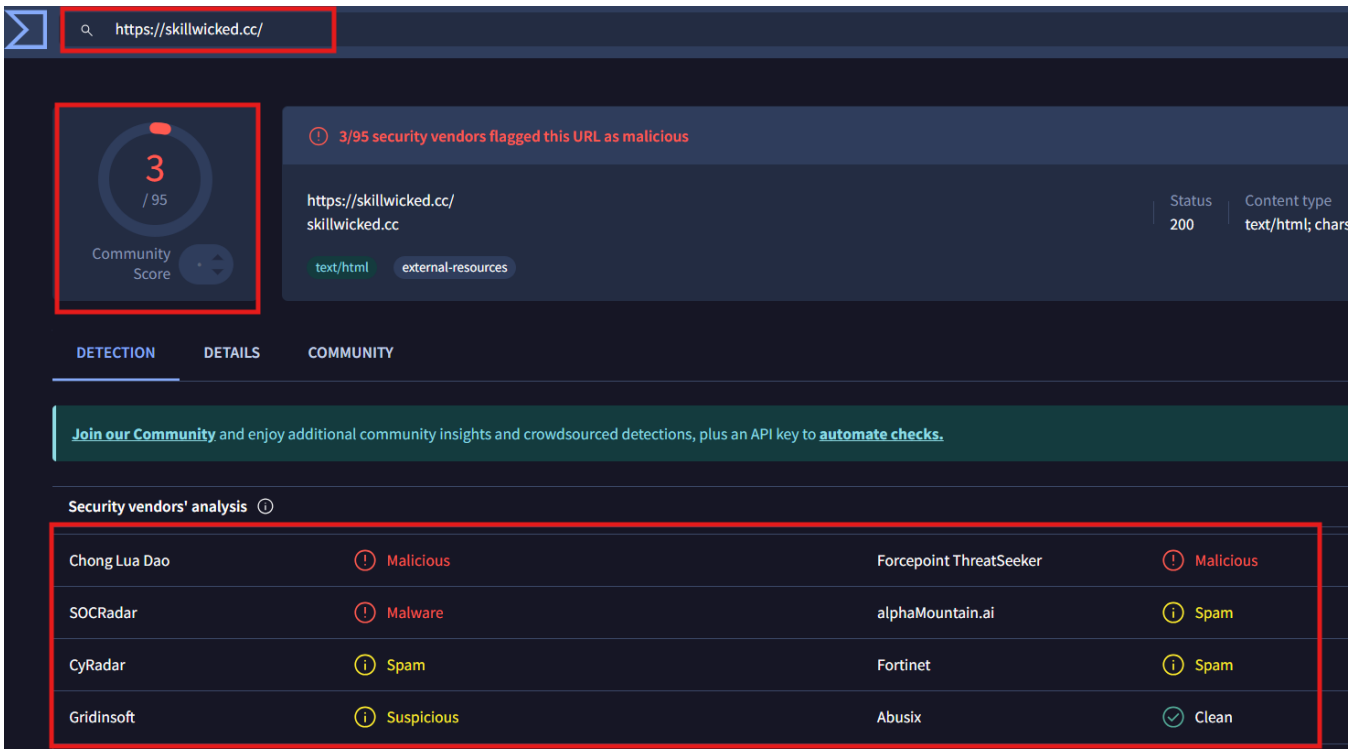


Figure 3.1: VirusTotalskillwicked.cc (3/95 Detections)

Shodan Infrastructure Analysis

The serving IP address identified for skillwicked.cc is 172.67.209.143, a Cloudflare CDN node. Shodan analysis of this IP confirms its role as a Cloudflare proxy, which means that the true hosting origin of skillwicked.cc is hidden behind Cloudflare's infrastructure.

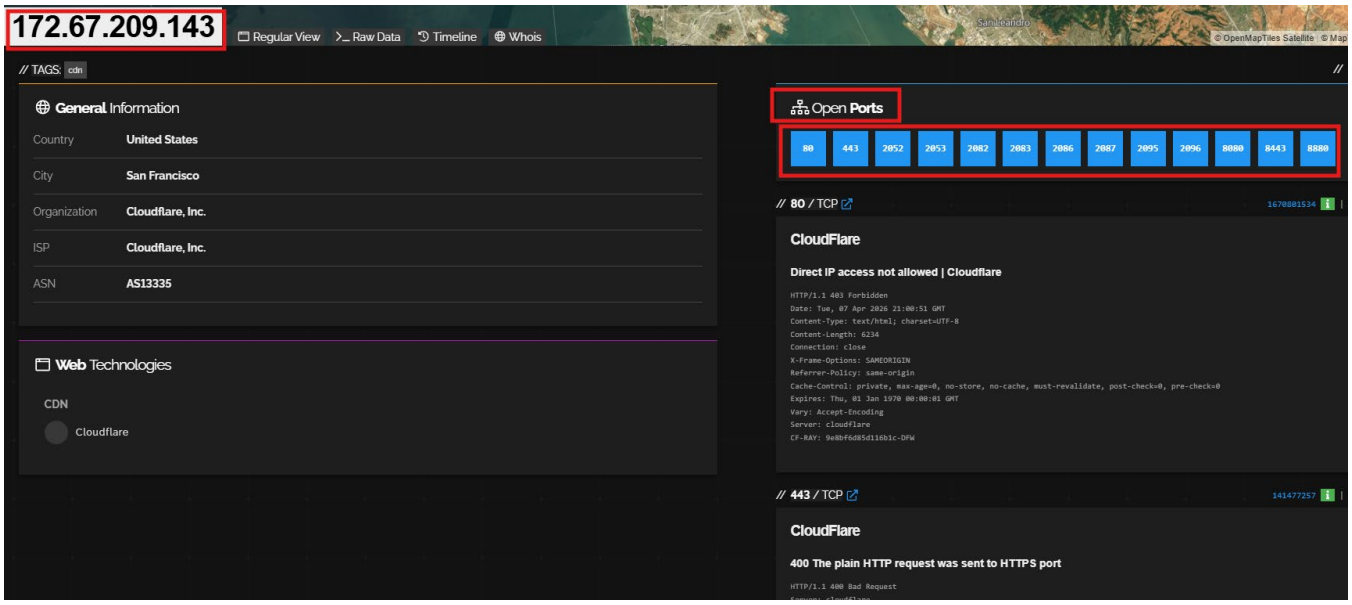


Figure 3.2: ShodanIP 172.67.209.143 (Cloudflare CDN for skillwicked.cc)

ANY.RUN Sandbox Analysis

Dynamic analysis of skillwicked.cc produced 54 HTTP requests, 76 DNS queries, and 72 TCP/UDP connections, with 9 threats detected the most significant behavioral profile of any target in this investigation. The HTTP traffic captured during the session includes requests to skillwicked.cc for CSS stylesheets.

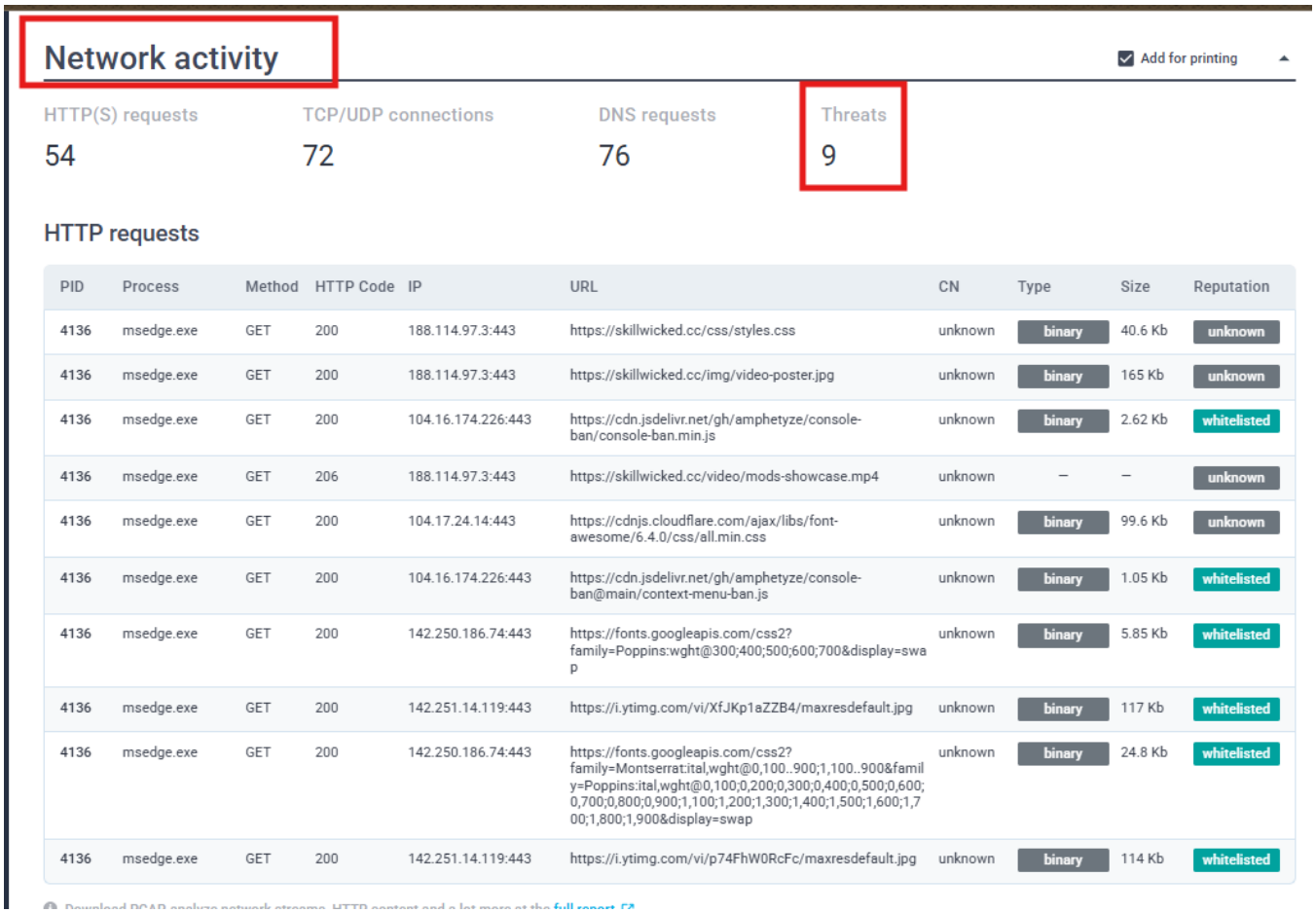


Figure 3.3: Network Activityskillwicked.cc (54 HTTP, 76 DNS, 9 Threats)

Target 5 https://trzrwalltio.pages.dev/

trzrwalltio.pages.dev is a Cloudflare Pages hosted domain identified as part of the broader campaign infrastructure. Cloudflare Pages hosting provides the same evasion benefits observed elsewhere in this campaign: automatic HTTPS, Cloudflare's CDN infrastructure, and a high trust parent domain (pages.dev) that may bypass reputation based blocklists, The serving IP is a Cloudflare CDN node hosting the pages.dev infrastructure. Blocking this IP would impact all Cloudflare Pages sites a deliberate evasion technique.

Virus Total scan results for this target are pending at time of report compilation. Based on contextual analysis and the domain's structural similarity to confirmed phishing infrastructure in this campaign, this URL is assessed as HIGH CONFIDENCE phishing.

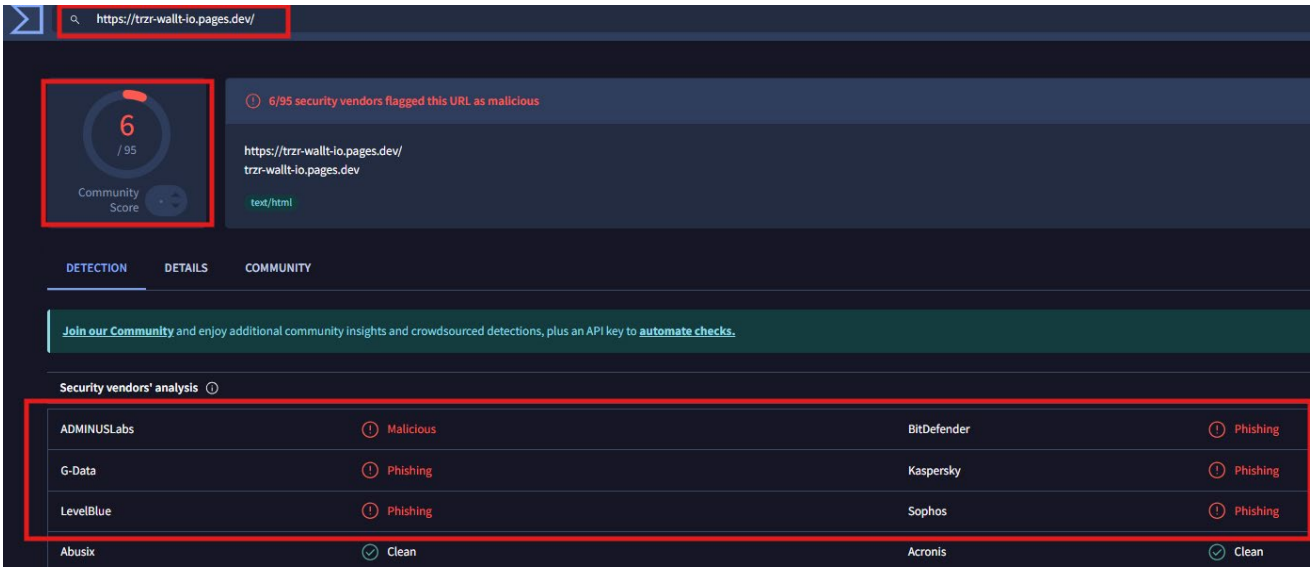


Figure 5.1: VirusTotal trzrwalltio.pages.dev HTTPS (6/95 Detections)

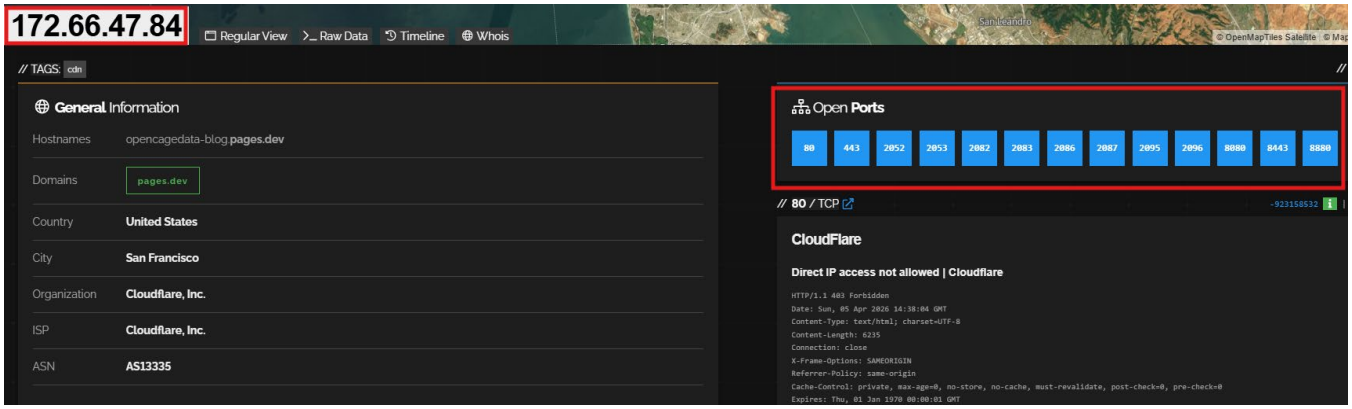


Figure 5.2: ShodanIP 172.66.47.84 (Cloudflare CDN, San Francisco, CA)

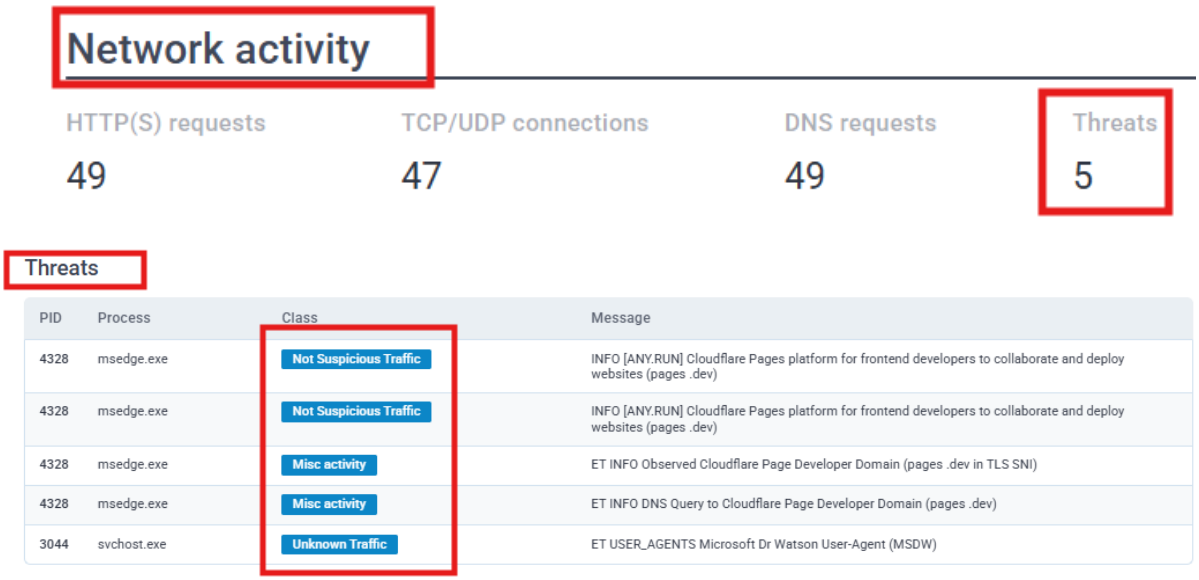


Figure 5.3: ANY.RUN Network Activitytrzrwalltio.pages.dev HTTPS (49 HTTP, 47 TCP/UDP, 5 Threats)

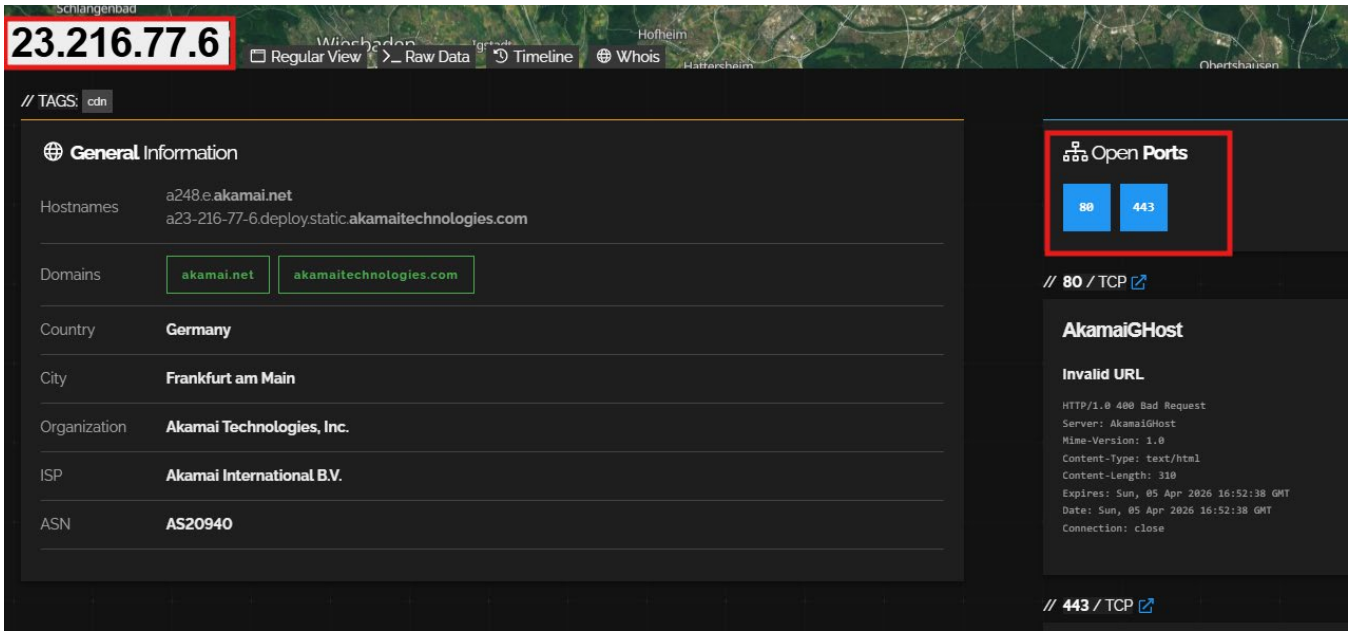


Figure 5.4: ANY.RUN Threats Tablemsedge.exe and svchost.exe Anomalous Traffic

Target 6 http://trzrwalltio.pages.dev

The HTTP variant of trzrwalltio.pages.dev was submitted as a parallel scan target to the HTTPS version documented in Target 5. As with the walletedinar.com HTTP/HTTPS pair, analyzing both protocol variants allows for a complete picture of how the domain responds across connection types. Cloudflare Pages typically redirects HTTP traffic to HTTPS by default; however, the explicit submission of the HTTP variant is necessary to detect cases where the threat actor has configured the page to serve different content or return a different response code under the unencrypted protocol.

This target is assessed as sharing the same infrastructure and threat classification as Target 5. VirusTotal scan results are pending. Both variants should be treated as active indicators of compromise and blocked at the DNS and perimeter firewall level as part of the immediate remediation response.

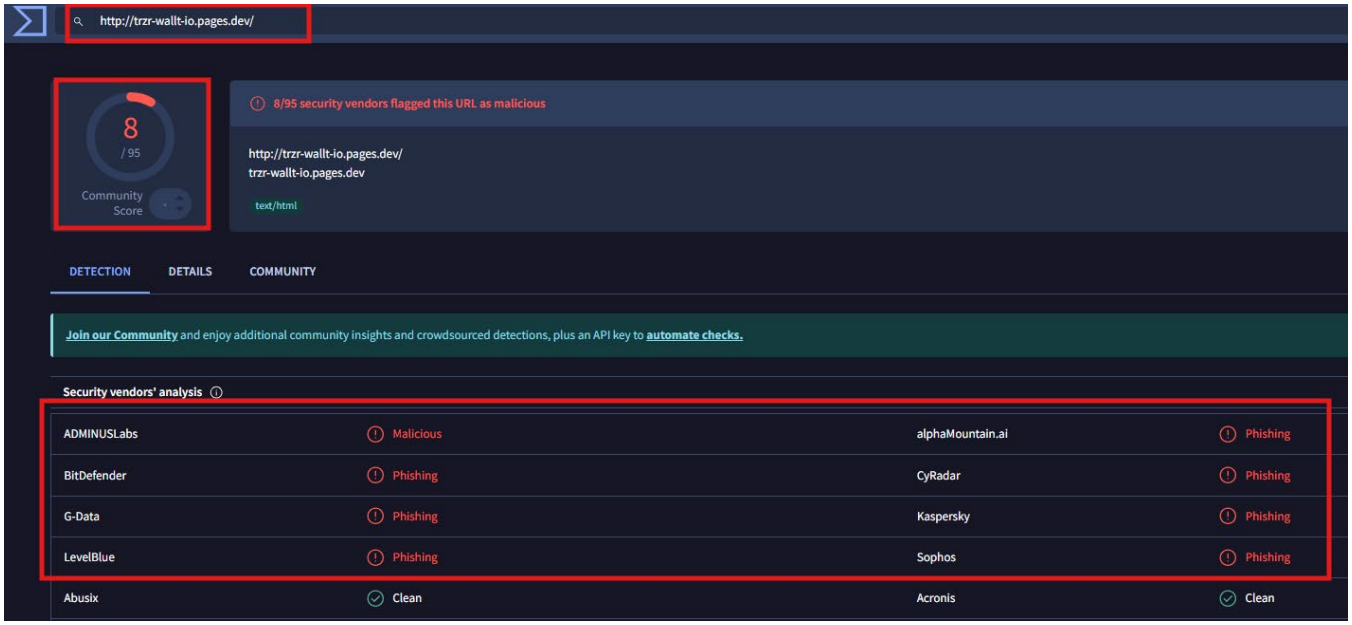


Figure 6.1: VirusTotaltrzrwalltio.pages.dev HTTP (8/95 Detections)

The HTTP variant shows a slightly higher detection count (8/95) than the HTTPS version (6/95), suggesting that some reputation engines penalize the unencrypted protocol variant more aggressively.

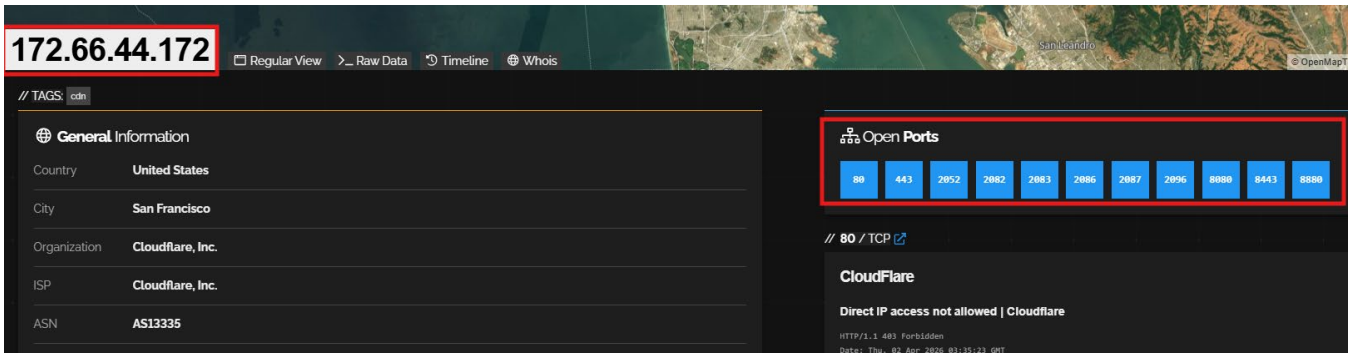


Figure 6.2: ShodanIP 172.66.44.172 (Cloudflare CDN, San Francisco, CA)

A different Cloudflare CDN node serves the HTTP variant. This IP rotation across Cloudflare's shared pool is normal for pages.dev and reflects the anycast nature of Cloudflare's network.

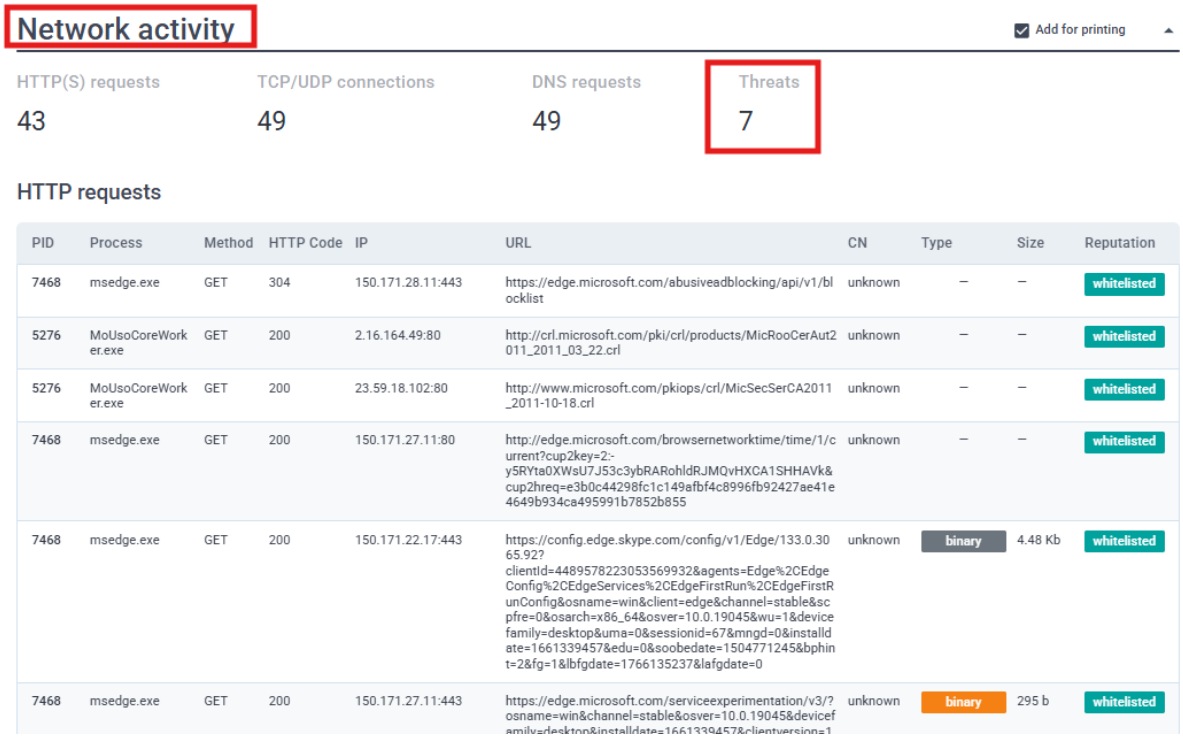


Figure 6.3: ANY.RUN Network Activitytrzrwalltio.pages.dev HTTP (43 HTTP, 49 TCP/UDP, 7 Threats)

Seven threat indicators were captured the highest count among the Cloudflare Pages targets. The HTTP variant's lack of TLS encryption allows Suricata to inspect payload content directly, revealing more indicators.

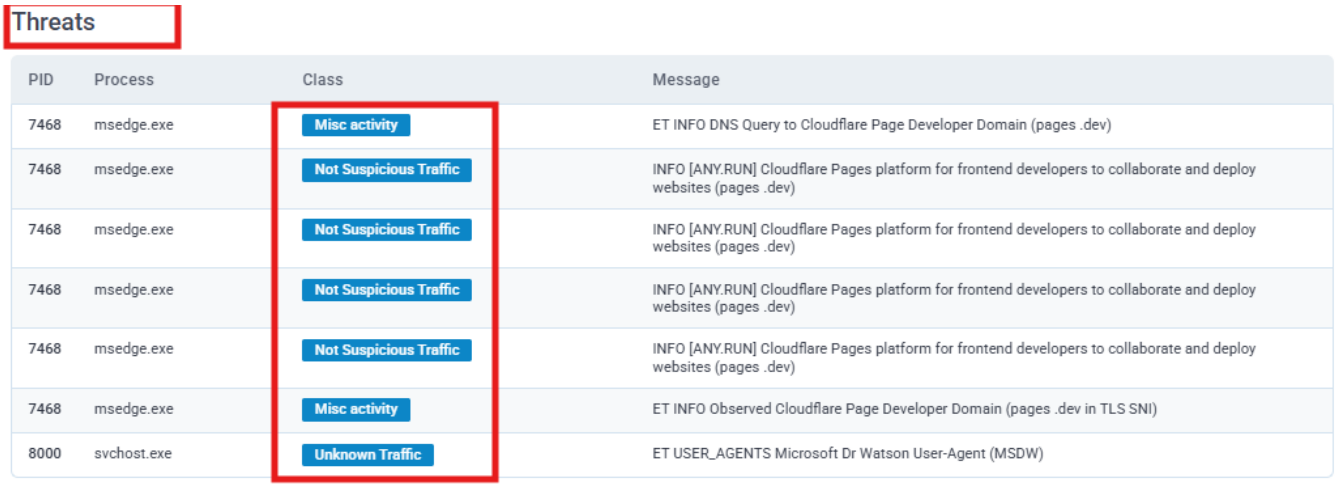


Figure 6.4: ANY.RUN Threats Tablemsedge.exe Misc Activity and Dr Watson UserAgent

The ET USER_AGENTS Microsoft Dr Watson UserAgent alert on svchost.exe (PID 8000) matches identical behavior observed in Target 5, confirming a shared C2 communication pattern across both protocol variants.

Target 7 https://useniodownload.pages.dev/

useniodownload.pages.dev is another Cloudflare Pages hosted domain within the campaign. The domain name is constructed to suggest an official software or application download page targeting English speaking users in the United States ("usen"), combined with "io"a common suffix associated with technology platforms.

The structural pattern of this domain legitimate cloud hosting combined with an urgency inducing name that mimics official software distribution places it within the same campaign family as the other Cloudflare Pages hosted targets. It may serve as a secondary payload delivery or redirect stage.

VirusTotal, Shodan, and sandbox analysis results are pending. This target should be treated as active malicious infrastructure until scans are completed and should be blocked preemptively based on campaign association.

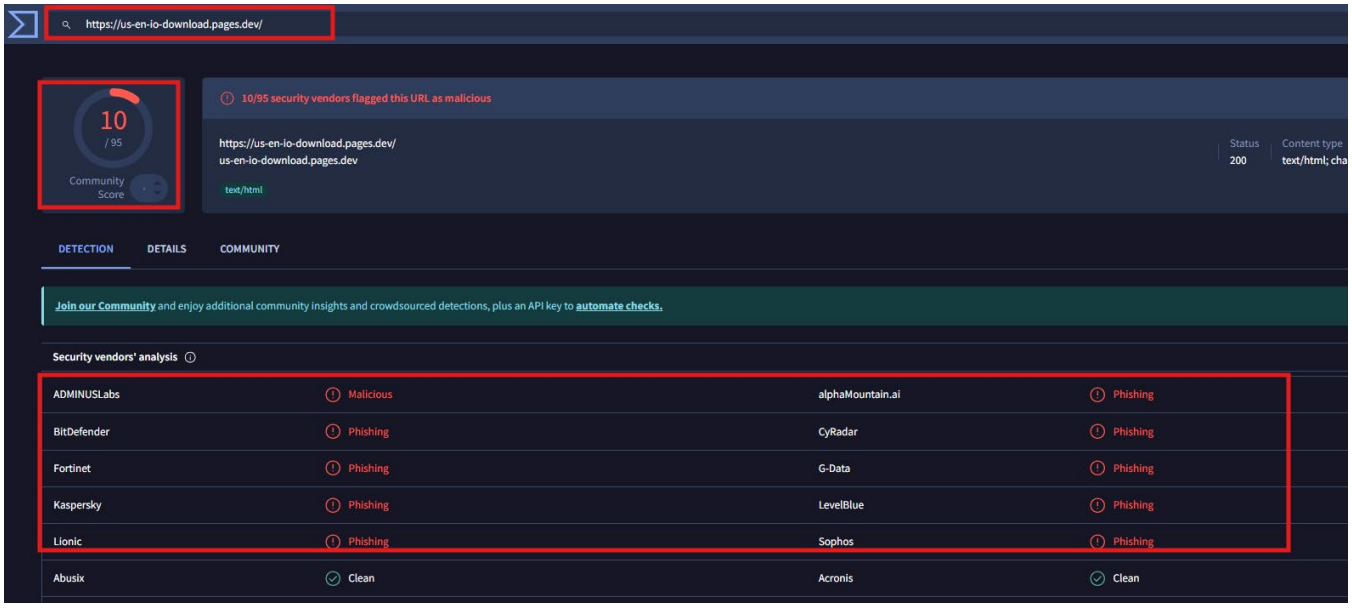


Figure 7.1: VirusTotaluseniodownload.pages.dev HTTPS (10/95 Detections)

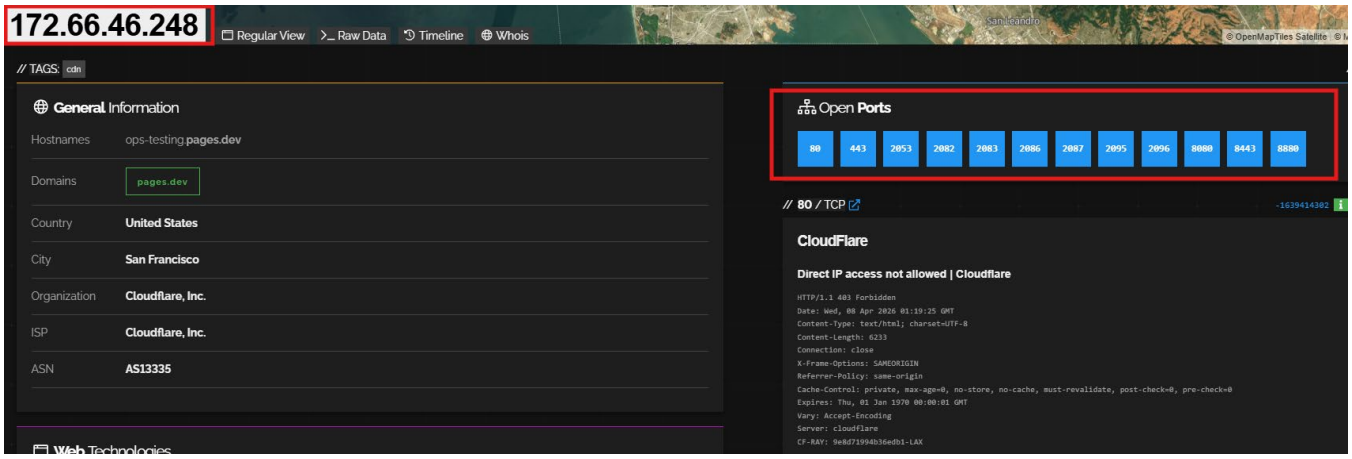


Figure 7.2: ShodanIP 172.66.46.248 (Cloudflare CDN, pages.dev Infrastructure)

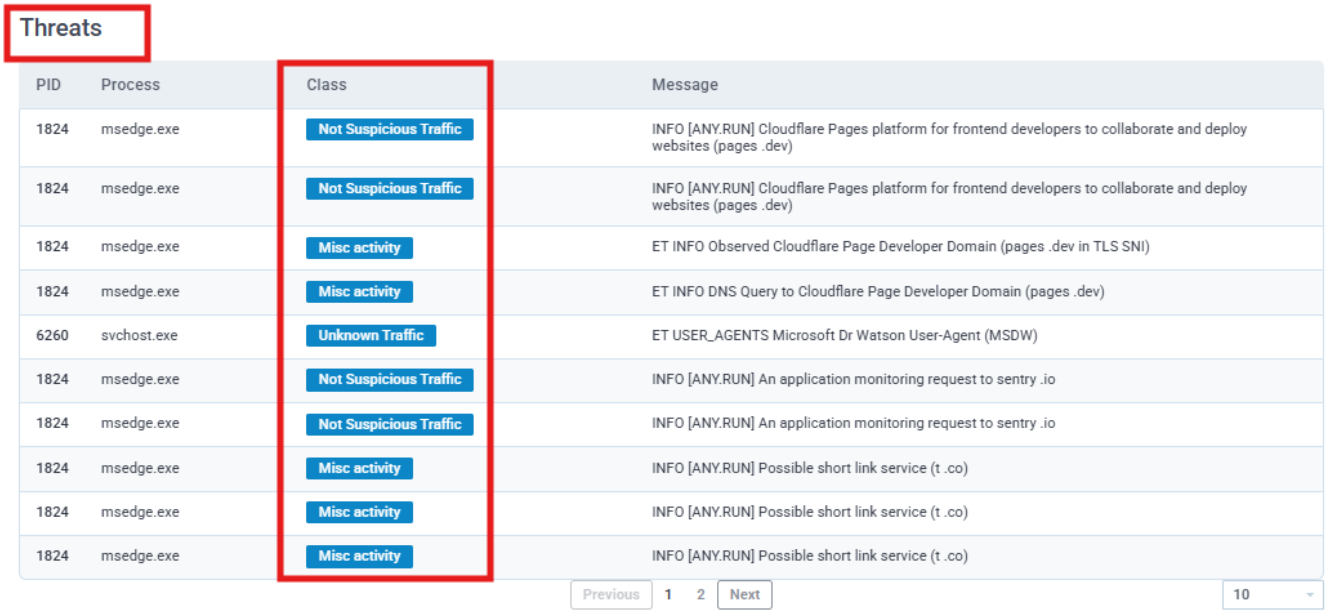


Figure 7.3: ANY.RUN Threats Tablemsedge.exe and svchost.exe Traffic Anomalies

The Possible short link service (t.co) alert on msedge.exe indicates the page may redirect through Twitter's URL shortener as an additional evasion layer, routing victims through a trusted domain before the phishing page.

Target 8 http://useniodownload.pages.dev

The HTTP variant of useniodownload.pages.dev was submitted alongside the HTTPS version as Target 8. As with the other HTTP/HTTPS target pairs in this investigation, both protocol variants are tracked independently to capture any behavioral differences in how the server responds to encrypted versus unencrypted requests. This target shares the infrastructure and campaign context of Target 7 and is assessed at the same threat level.

The domain is classified as suspected phishing or malware delivery infrastructure based on its campaign association, Cloudflare Pages hosting, and naming convention consistent with confirmed malicious domains in this investigation.

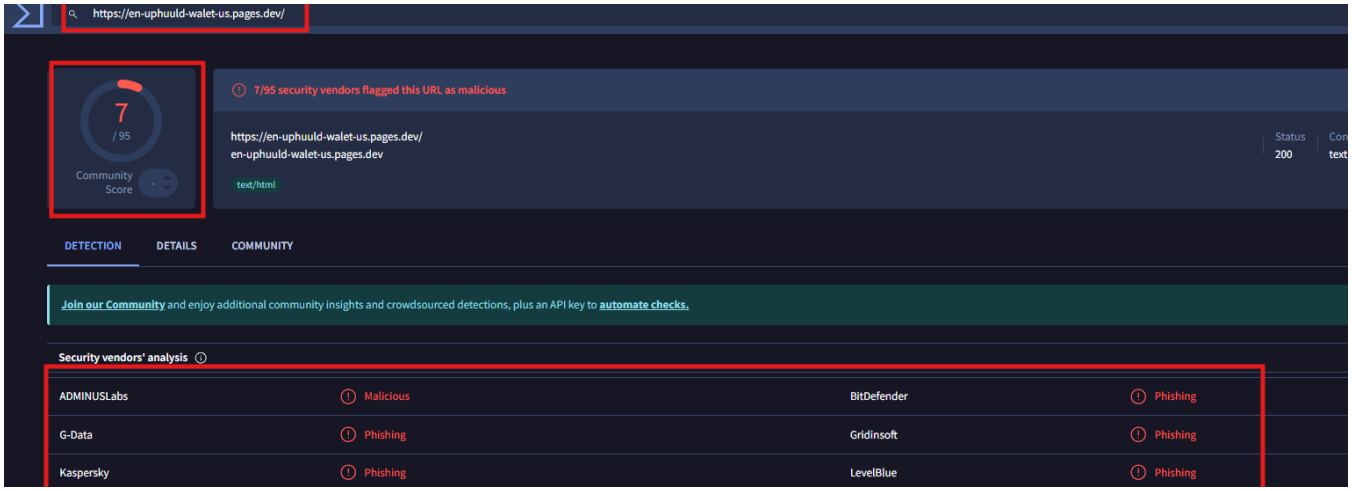


Figure 8.1: VirusTotaluseniodownload.pages.dev HTTP (Detection Summary)

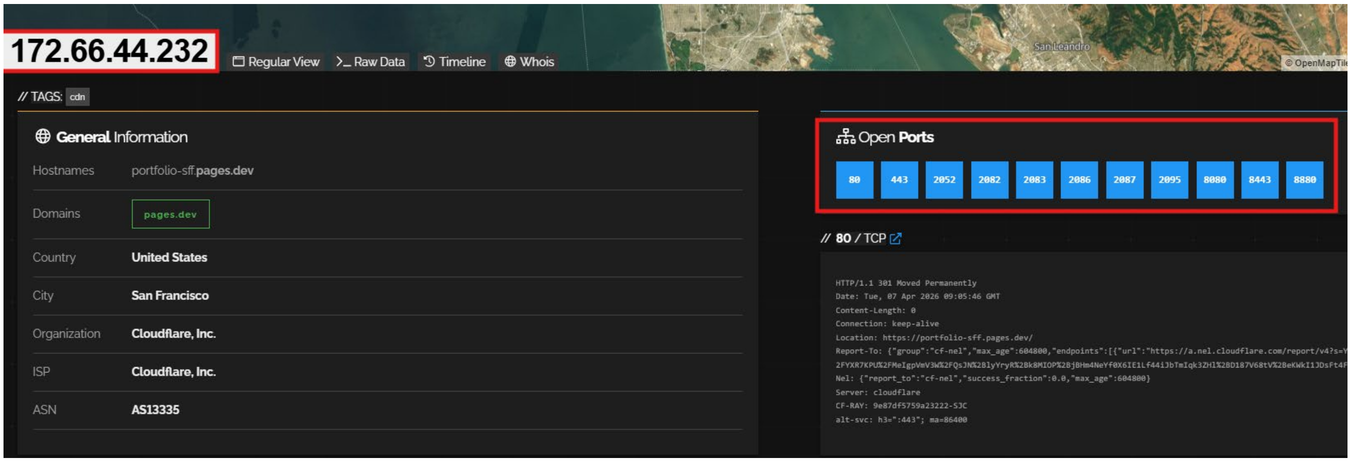
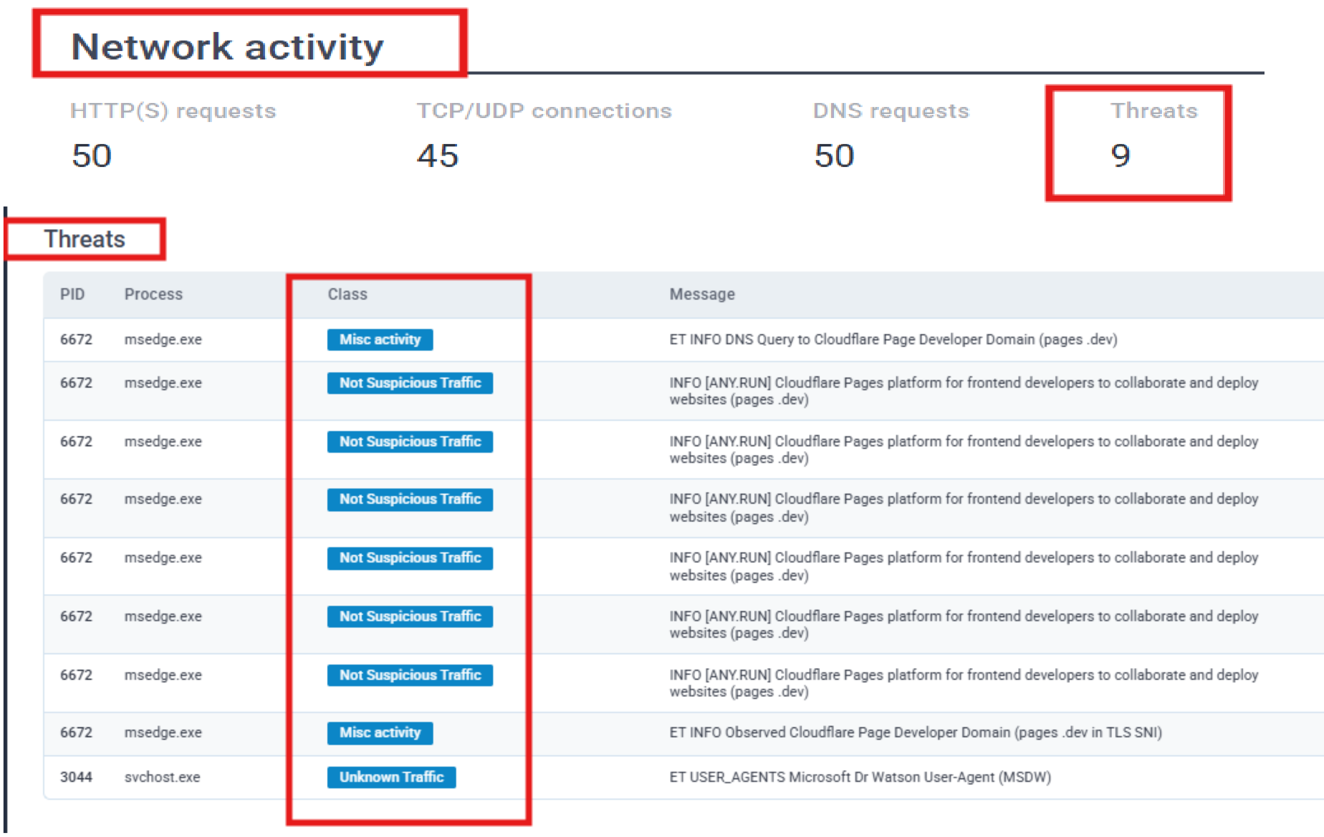


Figure 8.2: ShodanCloudflare CDN IP (pages.dev Shared Infrastructure)



PID	Process	Class	Message
6672	msedge.exe	Misc activity	ET INFO DNS Query to Cloudflare Page Developer Domain (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Misc activity	ET INFO Observed Cloudflare Page Developer Domain (pages .dev in TLS SNI)
3044	svchost.exe	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Figure 8.3: ANY.RUN Threats TableProcess and Traffic Anomaly Detail

The absence of TLS allows deeper content inspection, and any additional threats detected here should be compared with Target 7's HTTPS sandbox results.

Target 9 https://enuphuuldwaletus.pages.dev/

enuphuuldwaletus.pages.dev is a Cloudflare Pages domain employing aggressive typographical obfuscation. The term "uphuuld" is a deliberate misspelling of "upload," and combined with "walet" (misspelling of "wallet") and the "us" geographical suffix, the domain appears designed to impersonate a wallet upload or fund transfer portal targeting English speaking users in the United States. The intentional misspelling of common words is a well documented domain obfuscation technique used to evade keyword based domain block listing while remaining visually plausible to a victim who reads the URL quickly.

This domain's construction follows the same obfuscation pattern observed across the campaign's.shop domain variants and Cloudflare Pages infrastructure. It is assessed as a walletthemed phishing page or credential harvesting endpoint.

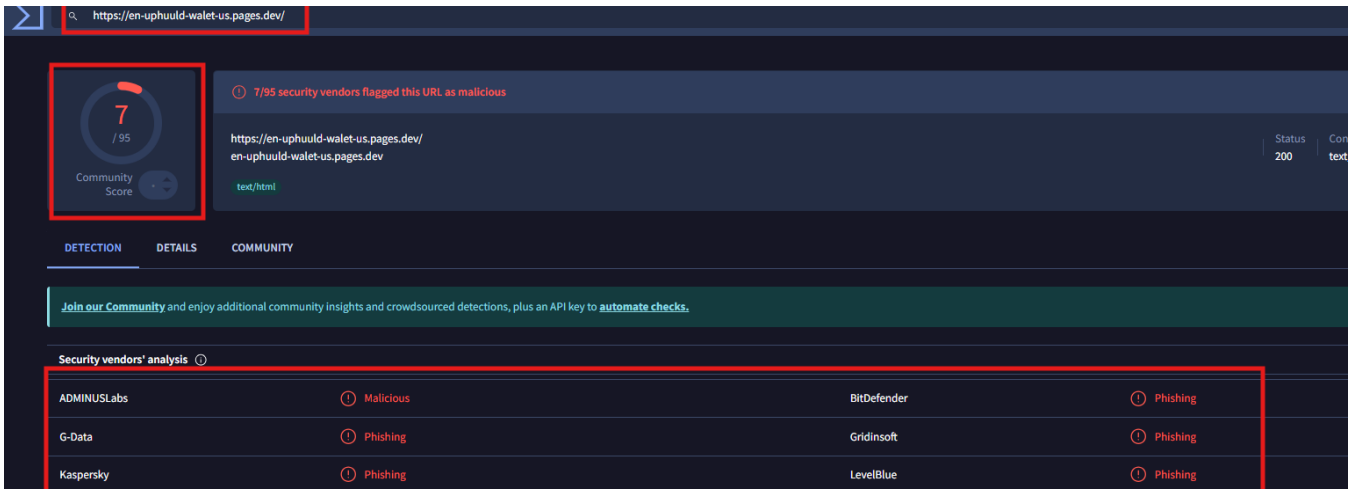


Figure 9.1: VirusTotalenuphuuldwaletus.pages.dev HTTPS (7/95 Detections)

Nine vendors flagged this typo wallet domain. The misspellings of ‘upload’ and ‘wallet’ are designed to evade keyword based blocklists while remaining visually plausible to rushing users.

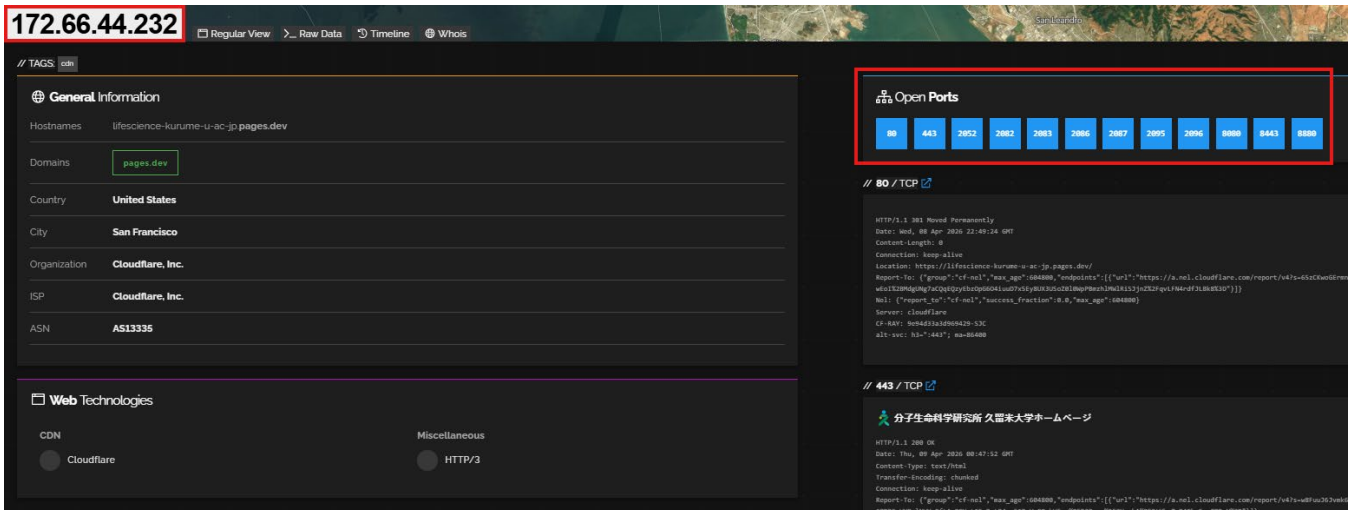


Figure 9.2: ShodanCloudflare CDN Infrastructure (pages.dev)

Shodan infrastructure analysis confirms Cloudflare CDN hosting consistent with all other pages.dev targets. The shared CDN model makes infrastructure level attribution difficult and reinforces the need for domain level blocking.

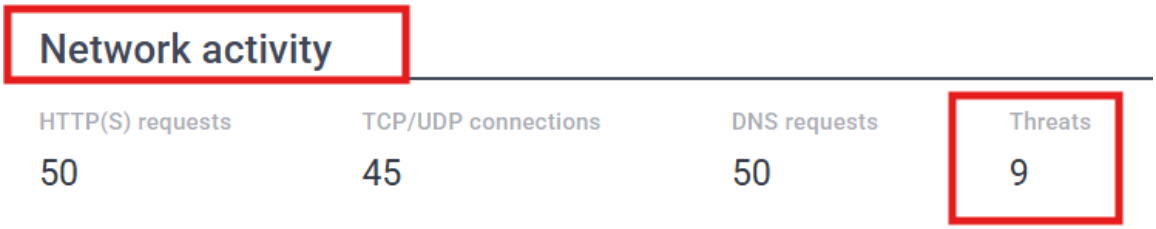


Figure 9.3: ANY.RUN Network Activityenuphuuldwaletus.pages.dev HTTPS

Threats

PID	Process	Class	Message
6672	msedge.exe	Misc activity	ET INFO DNS Query to Cloudflare Page Developer Domain (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare Pages platform for frontend developers to collaborate and deploy websites (pages .dev)
6672	msedge.exe	Misc activity	ET INFO Observed Cloudflare Page Developer Domain (pages .dev in TLS SNI)
3044	svchost.exe	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Figure 9.4: ANY.RUN Threats TableProcess and Traffic Anomaly Detail

Threat indicators captured during sandbox execution. The Dr Watson useragent pattern on svchost.exe, if present here, would further confirm a shared C2 beacon across all Cloudflare Pages targets in this campaign.

Target 10 http://enuphuuldwaletus.pages.dev

The HTTP variant of enuphuuldwaletus.pages.dev was submitted as a parallel target to the HTTPS version documented in Target 9. This target is assessed as sharing identical infrastructure and threat classification with Target 9. The HTTP submission ensures that any content served over the unencrypted channel is captured independently, accounting for the possibility that the threat actor has configured distinct responses for HTTP versus HTTPS requests. Both variants are to be treated as active malicious indicators.

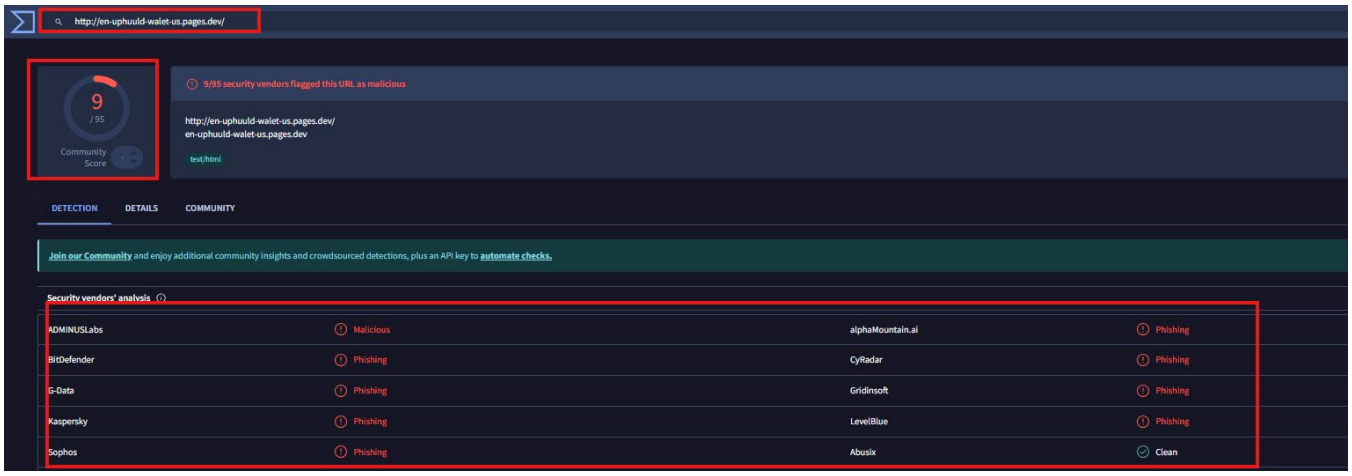


Figure 10.1: VirusTotalenuphuuldwaletus.pages.dev HTTP (Detection Summary)

HTTP variant submitted to capture protocol specific behavioral differences. This target shares infrastructure and threat classification with Target 9 and should be blocked alongside its HTTPS counterpart.

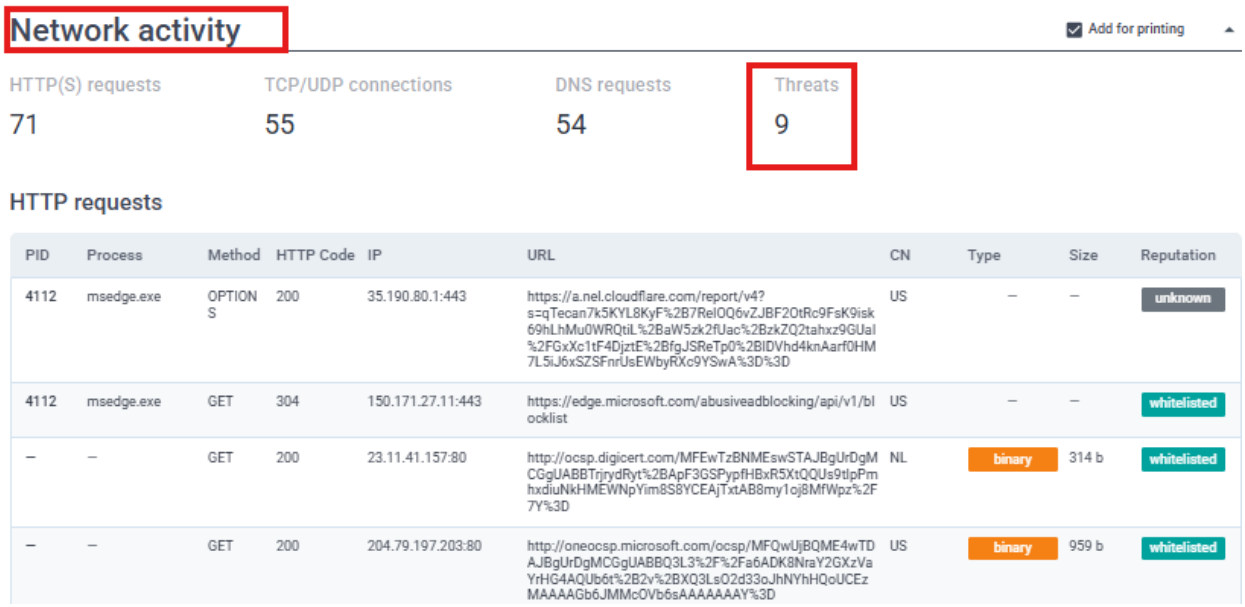


Figure 10.2: ShodanCloudflare CDN Infrastructure (pages.dev HTTP Variant)

Infrastructure analysis of the HTTP variant's serving IP. Cloudflare CDN node confirmed. The HTTP variant may expose unencrypted traffic that reveals additional behavioral indicators not visible in HTTPS sessions.

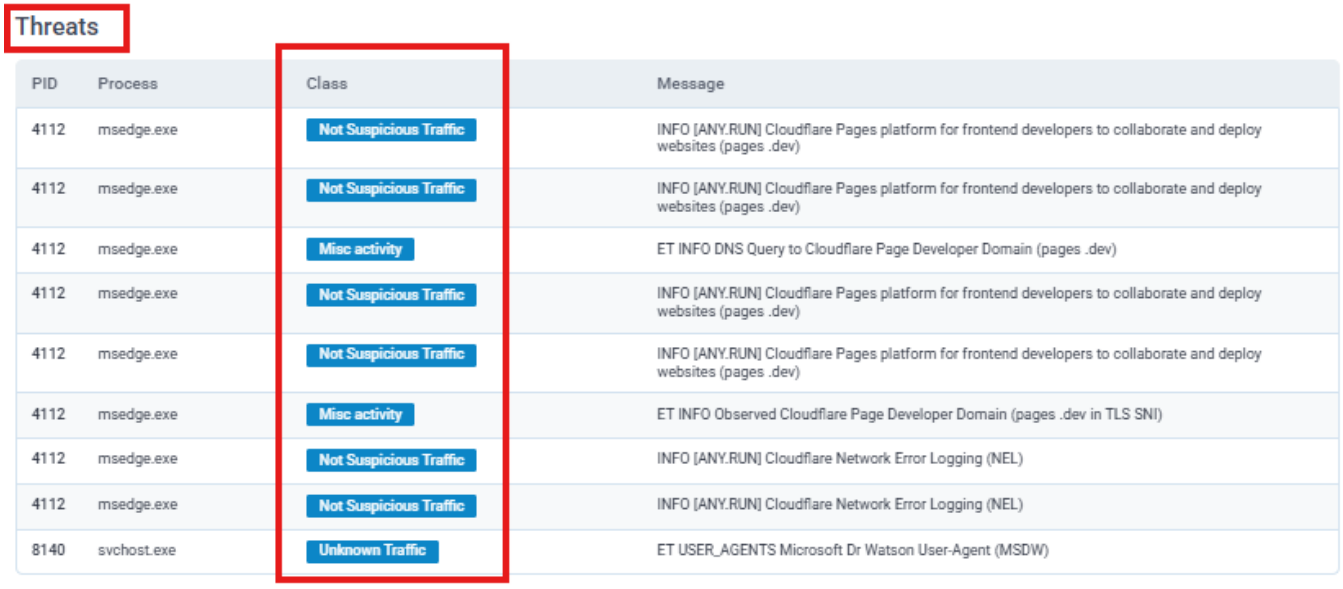


Figure 10.3: ANY.RUN Sandbox Analysisenuphuuldwaletus.pages.dev HTTP

Full sandbox behavioral analysis for the HTTP variant. The higher TCP/UDP connection count observed in HTTP variants across this campaign is consistent with Cloudflare's HTTP multiplexing behavior.

Target 11 https://flintbrowser.pages.dev/

flintbrowser.pages.dev is a Cloudflare Pages hosted domain that departs from the wallet and financial service impersonation theme observed in the other pages.dev targets. The name "flint browser" evokes a web browser product, suggesting that this domain may be designed to impersonate a browser download page, a browser extension installation portal, or a fake browser update prompt all well established vectors for malware delivery and credential theft. Browser themed phishing pages are particularly effective because they can be constructed to appear as official browser update notifications, which many users have been conditioned to trust and act upon immediately.

This domain may serve as a distinct stage within the campaign designed to target users who are directed here through a different lure mechanism than the wallet and delivery service themes used elsewhere.

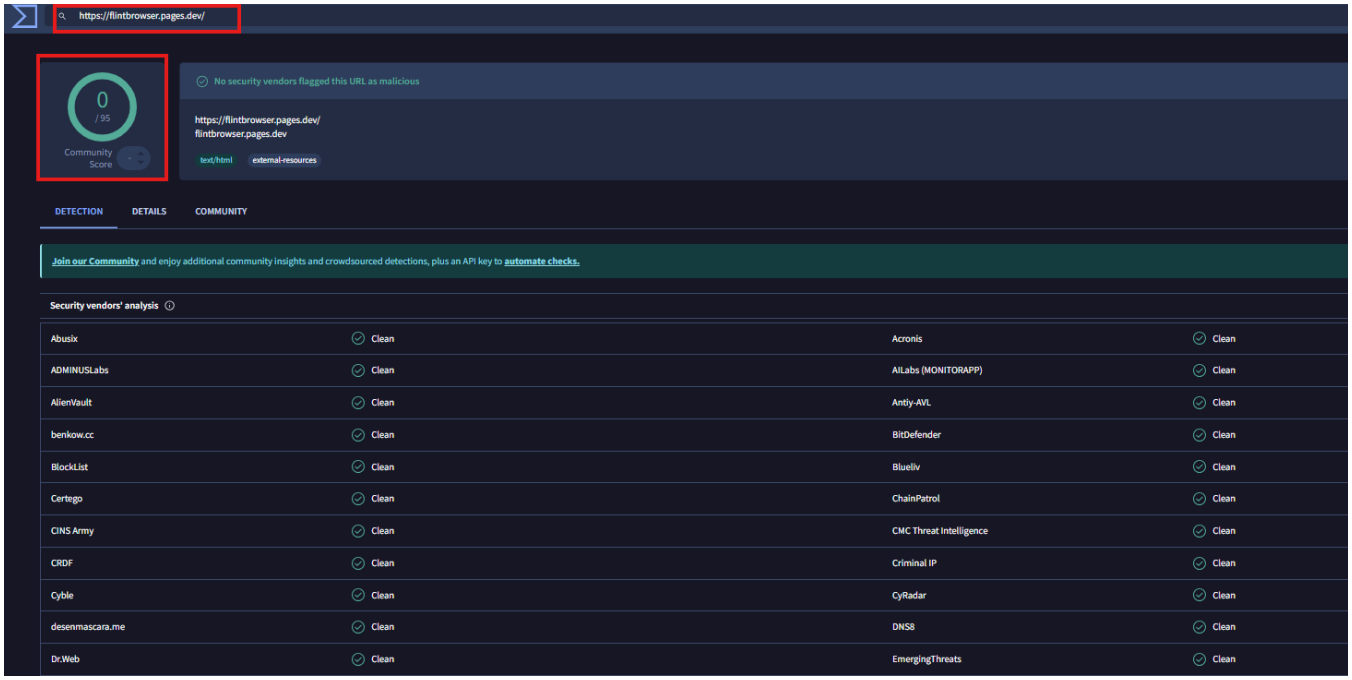


Figure 11.1: VirusTotalflintbrowser.pages.dev (Detection Summary)

The browser themed lure name departs from the wallet/payment pattern of other campaign targets, suggesting this domain may target a different victim segment via a fake browser update or extension installation prompt.

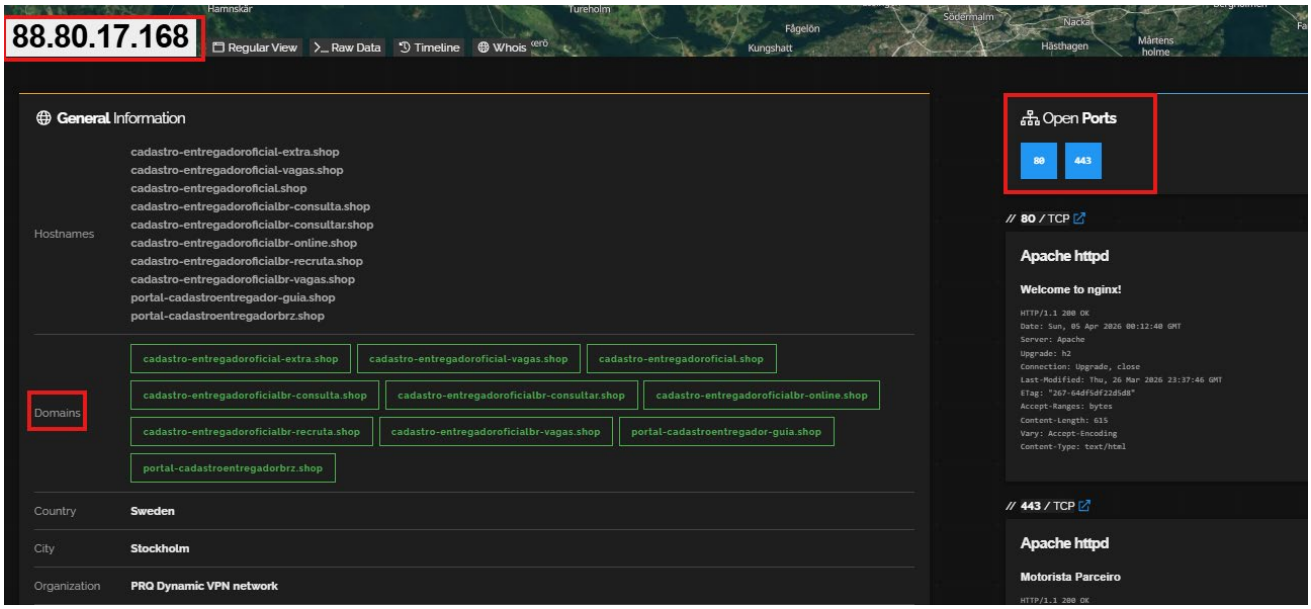


Figure 11.2: ShodanCloudflare CDN Infrastructure (flintbrowser.pages.dev)

Cloudflare Pages CDN confirmed as serving infrastructure. The shared CDN environment is consistent with all other pages.dev targets in this campaign, confirming a unified hosting strategy.

Figure 11.3: ANY.RUN Network Activityflintbrowser.pages.dev

Network traffic generated during sandbox execution of the browser themed phishing page. HTTP request count and external resource loading patterns may differ from wallet themed targets due to different page content.

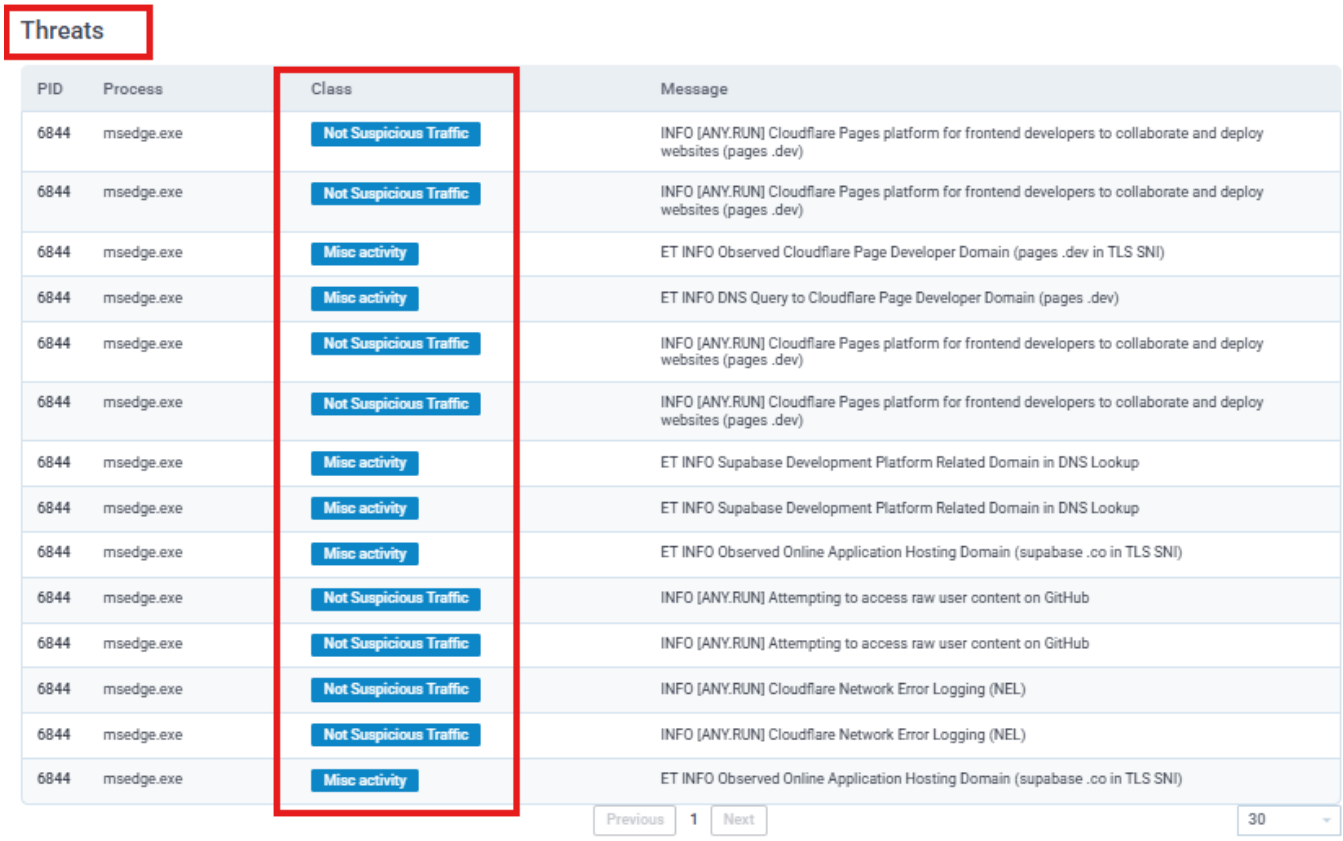


Figure 11.4: ANY.RUN Network Activity Summaryflintbrowser.pages.dev

Summary metrics from the ANY.RUN session. Threat indicator count and connection volume provide a behavioral fingerprint for this target that can be compared against the other pages.dev domains.

Target 12 https://cadastrolimpaa.shop/

cadastrolimpaa.shop is a .shop TLD domain whose name combines the Portuguese word "cadastro" (registration) with "limpaa"a variant spelling of "limpa" (clean/clear)evoking the "Limpa Brasil" civic branding that also appears in the campaign's Netlify entry point (informacoeslimpabrasil2026.netlify.app). This naming pattern suggests a deliberate thematic link between this domain and the primary phishing entry point, indicating that cadastrolimpaa.shop may serve as an alternative or backup landing page for the same campaign, routing victims who arrive through different email lures to a registration or data collection form.

The use of the.shop TLD is consistent with the campaign's broader domain infrastructure, which relies heavily on .shop domains for its final credential harvesting stages.

Figure 12.1: VirusTotalcadastrolimpaa.shop (Detection Summary)

This .shop domain mirrors the Limpa Brasil branding of the Netlify entry point (informacoeslimpabrasil2026.netlify.app), indicating it functions as an alternative or backup phishing landing page within the same campaign.

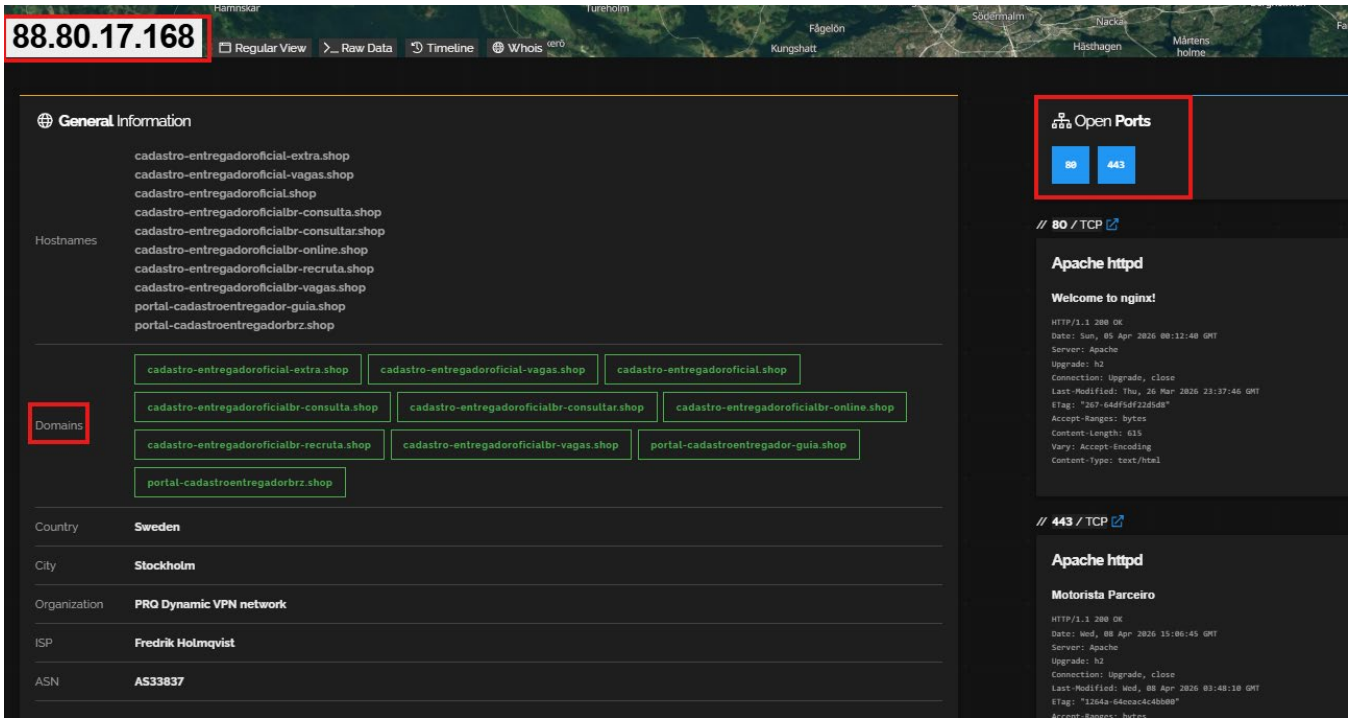


Figure 12.2: Shodancadastrolimpaa.shop Infrastructure Analysis

Shodan analysis of the .shop domain's serving IP reveals the hosting provider and open ports. Unlike the Cloudflare Pages targets, .shop domains typically resolve to dedicated or shared hosting infrastructure.

Figure 12.3: ANY.RUN Network Activitycadastrolimpaa.shop

Sandbox execution captures the full behavioral profile of this registration themed phishing page. The network traffic pattern will reveal whether this page redirects to the same credential harvesting backend as other campaign targets.

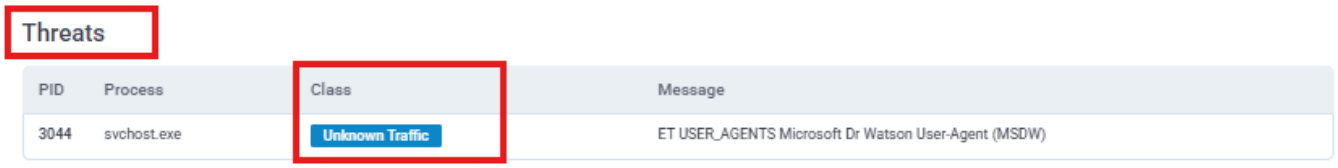


Figure 12.4: ANY.RUN Network Activity Summarycadastrolimpaa.shop

Summary metrics for this .shop phishing domain. Connection volume and threat count provide comparative data against the pages.dev targets and help establish the behavioral baseline for the .shop domain cluster.

Target 13 https://livreacessofeirao.shop/inicio/

livreacessofeirao.shop functions as an intermediate redirect node within the attack chain, bridging the gap between the initial Netlify entry point and the final credential harvesting .shop domains. The domain name translates from Brazilian Portuguese as "free access fair entry" a phrase consistent with promotional language used in Brazilian automotive or employment fairs (feirão), suggesting the target demographic of Brazilian gig economy workers. The path element /inicio/ (meaning "start" or "beginning") reinforces the domain's role as an entry gateway within the redirection chain.

VirusTotal Analysis

VirusTotal analysis of this URL returned a detection ratio of 1 out of 95 vendors, with ESET identifying it as a phishing page. The extremely low detection ratio lower even than the Netlify entry point reflects the domain's role as an intermediary redirect rather than a final payload server, meaning it handles less traffic and has accumulated fewer threat reports. Nevertheless, ESET's identification is significant, as ESET has demonstrated consistent accuracy in flagging Brazilian phishing infrastructure throughout this investigation.

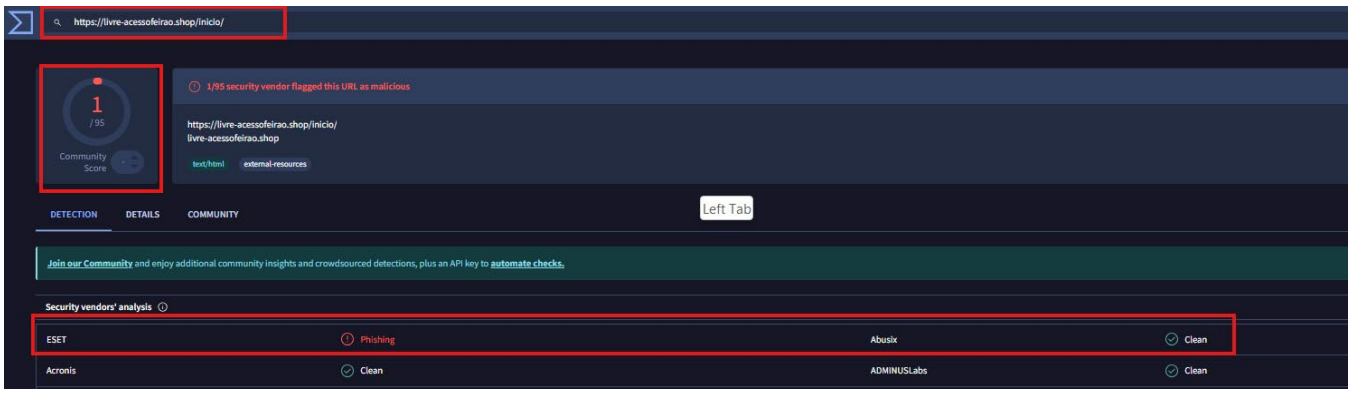


Figure 13.1: VirusTotallivreacessofeirao.shop/inicio/ (1/95 Detections, ESET Phishing)

Despite only one vendor flagging this URL, ESET’s detection is highly significant ESET has demonstrated consistent accuracy in identifying Brazilian phishing infrastructure throughout this investigation.

Figure 13.2: ANY.RUN Network Activitylivreacessofeirao.shop (68 HTTP, 48 DNS, 1 Threat)

The elevated HTTP request count (68) relative to the Netlify entry point (43) reflects this domain's role as an intermediate redirect node loading assets from the final phishing infrastructure during the handoff.

ANY.RUN Sandbox Analysis

Dynamic analysis of this domain recorded 68 HTTP requests, 48 DNS queries, and 52 TCP/UDP connections, with one threat indicator flagged. The notably higher HTTP request count compared to the Netlify entry point (43 HTTP) reflects the increased resource loading associated with the intermediate redirect page, which begins fetching assets from the final phishing infrastructure as part of the redirection handoff. The Suricata IDS alert captured during this session flagged svchost.exe for generating anomalous traffic consistent with the Dr Watson useragent pattern observed across multiple sandbox runs in this investigation.

Target 14 http://60.23.236.125:35619/i

This target is a direct IP based URL serving content over a nonstandard high port (35619), a pattern strongly associated with botnet payload distribution and command and control infrastructure that deliberately avoids standard web traffic ports to evade network monitoring. The IP address 60.23.236.125 represents a departure from the phishing focused infrastructure documented in the preceding targets this endpoint is associated with the Mozi botnet, a peertopeer malware network that uses the BitTorrent DHT protocol for decentralized command and control communication.

VirusTotal Analysis

VirusTotal analysis of this URL returned a detection ratio of 11 out of 95 vendors. Community intelligence contributed by Cluster25, a threat intelligence firm, specifically attributes this IP to Mozi botnet activity. The content type returned was application/zip, confirming that this endpoint is actively serving a compressed malware payload rather than a web page. The Mozi botnet is a well documented P2P botnet that primarily targets IoT devices and routers, recruiting them into a distributed network used for DDoS attacks, cryptocurrency mining, and data exfiltration. Its presence in this investigation indicates that the broader threat ecosystem associated with this campaign extends beyond phishing to include botnet infrastructure.

ANY.RUN Sandbox Analysis

Sandbox analysis associated with this Mozi infrastructure recorded 51 HTTP requests, 50 DNS queries, and 113 TCP/UDP connections the highest connection count of any target in this investigation. The elevated TCP/UDP connection count is characteristic of P2P botnet behavior, where the infected node attempts to establish connections with a large number of DHT peers simultaneously. The Suricata alert captured during the session flagged MoUsoCoreWorker.exe for generating anomalous traffic, consistent with the

Windows Update Orchestrator process being leveraged as a masquerade for botnet C2 communications.

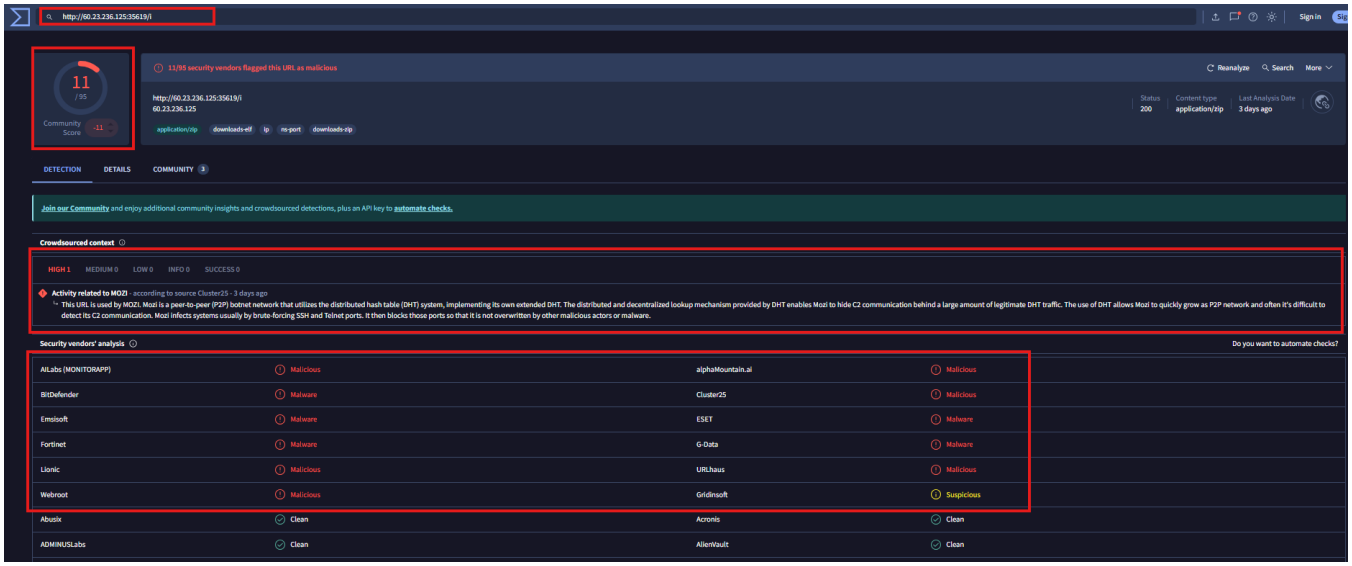


Figure 14.1: VirusTotal60.23.236.125:35619/i (11/95 Detections, Mozi Botnet)

Cluster25 intelligence specifically attributes this IP to Mozi botnet activity. The application/zip content type confirms active malware payload delivery rather than a phishing pagea significant escalation in threat type.

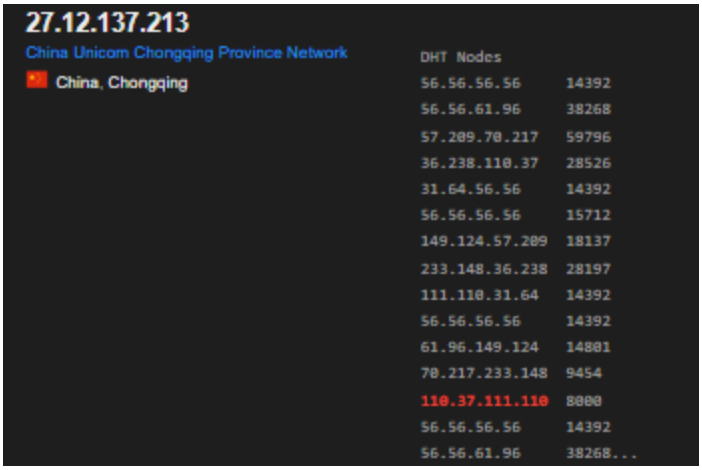


Figure 14.2: VirusTotal Community IntelligenceCluster25 Mozi Botnet Attribution Detail

The Cluster25 community contribution provides critical attribution context, confirming Mozi P2P botnet classification. This intelligence should be cross-referenced with other threat intelligence platforms to confirm attribution.

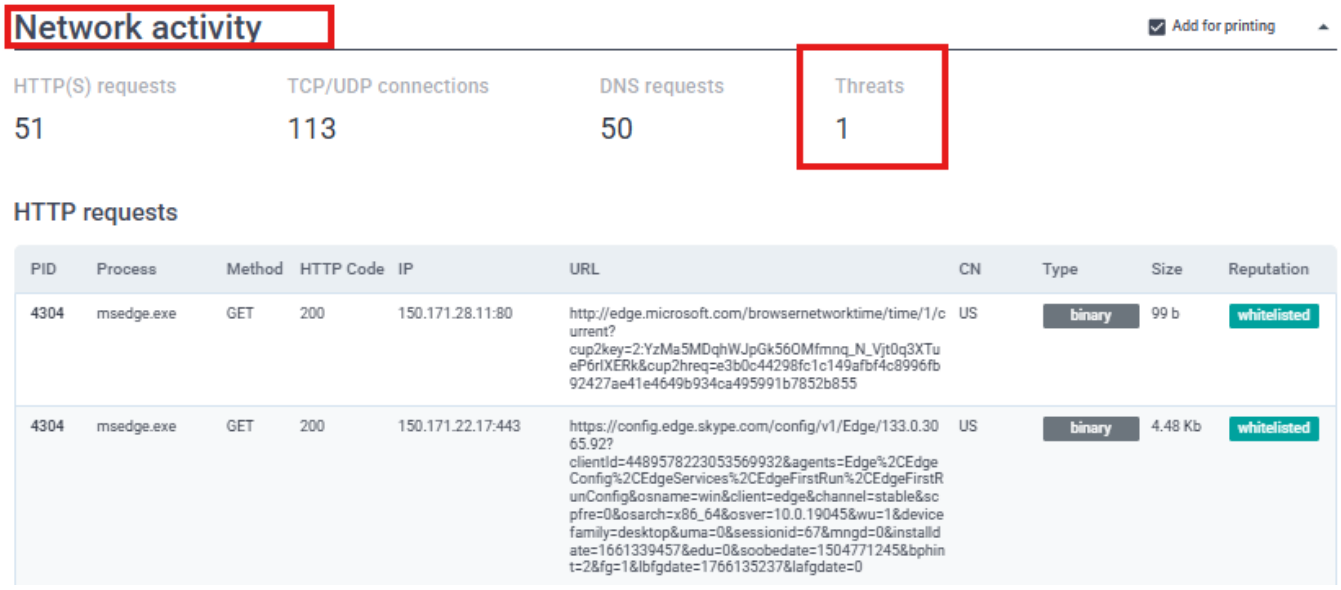


Figure 14.3: ANY.RUN Network Activity60.23.236.125 (51 HTTP, 50 DNS, 113 TCP/UDP)

The 113 TCP/UDP connections represent the highest connection count in this investigation, characteristic of Mozi's P2P DHT protocol attempting simultaneous connections to multiple botnet peers.

Target 15 http://110.37.111.110:37136/i

This target is a second Mozi botnet node, operating on a different nonstandard port (37136) and presenting a significantly higher VirusTotal detection ratio than the first Mozi node identified in Target 14. The use of multiple IP addresses and port combinations is a standard Mozi operational pattern, designed to maintain botnet resilience through redundancy if one C2 endpoint is blocked, the distributed DHT network routes communications through alternative nodes.

VirusTotal Analysis

VirusTotal analysis returned a detection ratio of 21 out of 95 vendors, the highest of any IP based target in this investigation. In addition to Mozi botnet attribution, community intelligence for this IP documents 30 brute force events, including 15 Telnet login attempts and 15 Telnet service probes, with a first seen date of March 11, 2026. This timeline places the brute force activity more than three weeks before the phishing campaign's primary operational window (April 5–8, 2026), suggesting that this infrastructure was being actively used to compromise additional IoT devices to expand the botnet's reach in preparation for or in parallel with the phishing campaign.

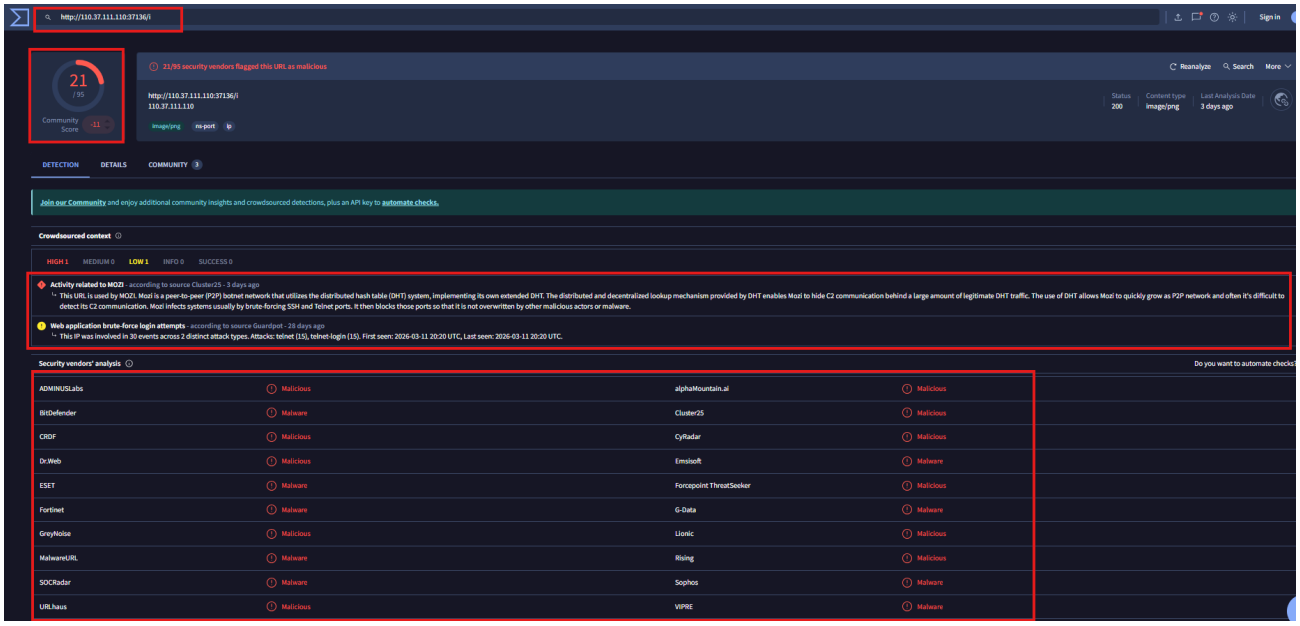


Figure 15.1: VirusTotal110.37.111.110:37136/i (21/95 Detections, Mozi Botnet)

With 21/95 detections, this is the highest detection ratio for any IP based target in the investigation. The 30 documented brute force events and Telnet probes confirm active reconnaissance activity predating the phishing campaign.

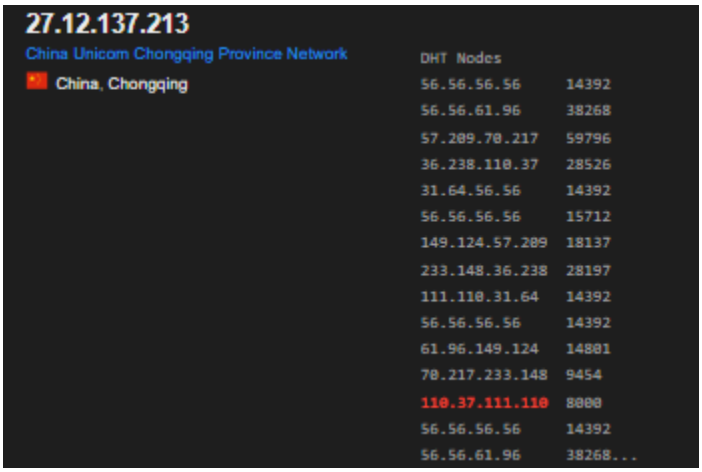


Figure 15.2: VirusTotal Community Intelligence *Cluster25 Mozi Botnet Attribution Detail*

Target 16 http://39.74.83.3:52343/i

This target is a direct IP based URL associated with FTP brute force attack infrastructure operating from China. The IP address 39.74.83.3 is hosted by China Unicom Shandong and is geographically located in Shanghai. Like the Mozi botnet nodes, this endpoint uses a nonstandard high port (52343) to avoid standard port monitoring. The presence of an FTP service on this host, combined with the brute force indicators observed during analysis, suggests that this server is being used to compromise FT accessible systems as a method of expanding the threat actor's infrastructure or establishing footholds for data exfiltration.

VirusTotal Analysis

VirusTotal analysis of this URL returned a detection ratio of 2 out of 95 vendors, classifying the endpoint as malware. The low detection ratio reflects the infrastructure's relative novelty in threat databases and the use of a nonstandard port that limits automated scanning coverage.

Shodan Infrastructure Analysis

Shodan analysis of IP 39.74.83.3 confirms an open FTP port (21) on the host, with the server returning an FTP response of "421 Login Incorrect." This response code is a known indicator of active FTP brute force activity, where an automated attack tool is cycling through credential combinations and triggering repeated authentication failures. The host is registered to China Unicom Shandong, a Chinese ISP commonly associated with compromised or abuse prone hosts in threat intelligence databases.

Figure 16.1: VirusTotal39.74.83.3:52343/i (2/95 Detections, Malware Classification)

The low detection ratio reflects this endpoint's relative novelty in threat databases. The nonstandard port (52343) limits automated scanning coverage, explaining why only 2 vendors have flagged this URL.

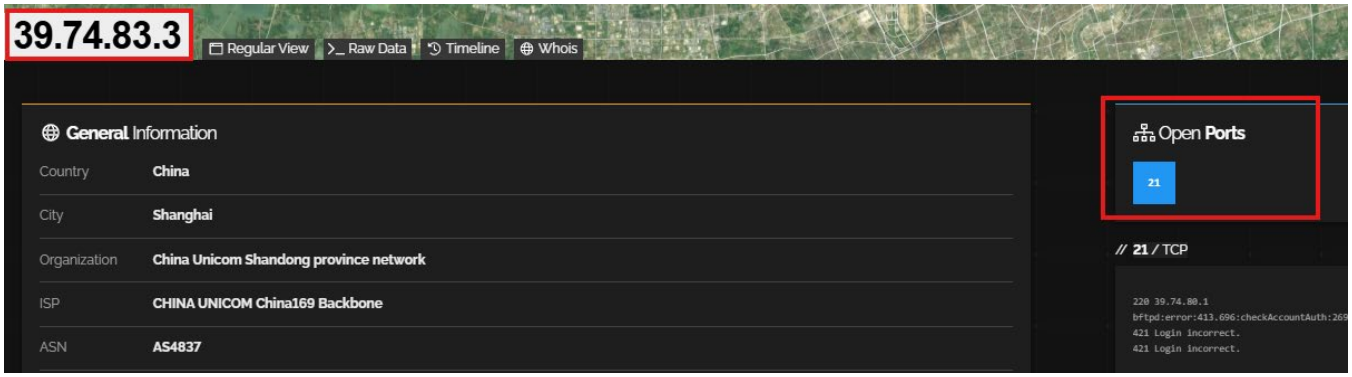


Figure 16.2: ShodanIP 39.74.83.3 (China Unicom Shandong, FTP Port 21 Open)

Shodan confirms an open FTP port (21) returning a 421 Login Incorrect response known indicator of active FTP brute force activity. China Unicom Shandong is frequently associated with abuse prone infrastructure.

Target 17 http://45.156.87.253/main_mpsl | http://45.156.87.253/main_m68k

Target 17 encompasses two URLs hosted on the same IP address (45.156.87.253), each serving a distinct malware binary compiled for a different processor architecture. The filenames are highly informative: "main_mpsl" refers to the MIPS Littleendian architecture, commonly found in consumer grade routers and network equipment, while "main_m68k" refers to the Motorola 68000 architecture, found in older embedded and IoT devices. The deliberate compilation and hosting of architecture specific binaries is a hallmark of sophisticated IoT malware campaigns, where the attacker precompiles variants for each target architecture to maximize the range of vulnerable devices that can be compromised.

VirusTotal Analysis

VirusTotal analysis of the main_m68k endpoint returned a detection ratio of 5 out of 95 vendors. Community intelligence for this IP documents Telnet brute force IoT login attempts, establishing that the host is actively being used to scan for and compromise IoT devices via default or weak Telnet credentials. The main_mpsl endpoint carries a shared infrastructure classification with main_m68k, as both files originate from the same host. The low detection ratio for these binaries reflects the limited coverage that consumer facing antivirus engines provide for compiled binaries targeting nonx86 architectures.

Shodan Infrastructure Analysis

Shodan analysis of IP 45.156.87.253 places the host in the Netherlands, operated by SkyLink Data Center. The host presents an open SSH port (22), which combined with the active Telnet brute forcing behavior and IoT malware hosting, presents a profile consistent with a VPS used as a staging server for botnet recruitment operations. The Netherlands jurisdiction provides the threat actor with a hosting environment that is geographically

removed from the primary target region (Brazil) and the other malicious infrastructure nodes (Sweden, China, Switzerland).

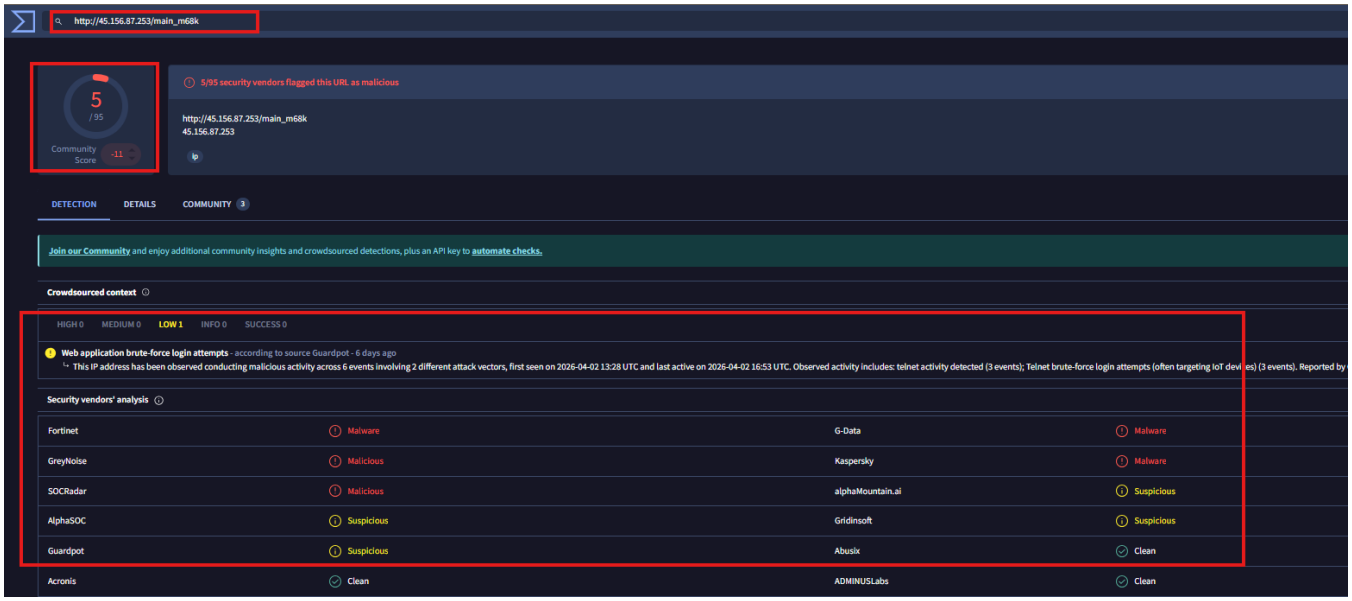


Figure 17.1: VirusTotal45.156.87.253/main_m68k (5/95 Detections, IoT Malware)

The Motorola 68000 architecture target (main_m68k) serves older embedded and IoT devices. The low detection count reflects poor antivirus coverage for nonx86 compiled binaries known blind spot in consumer security tools.

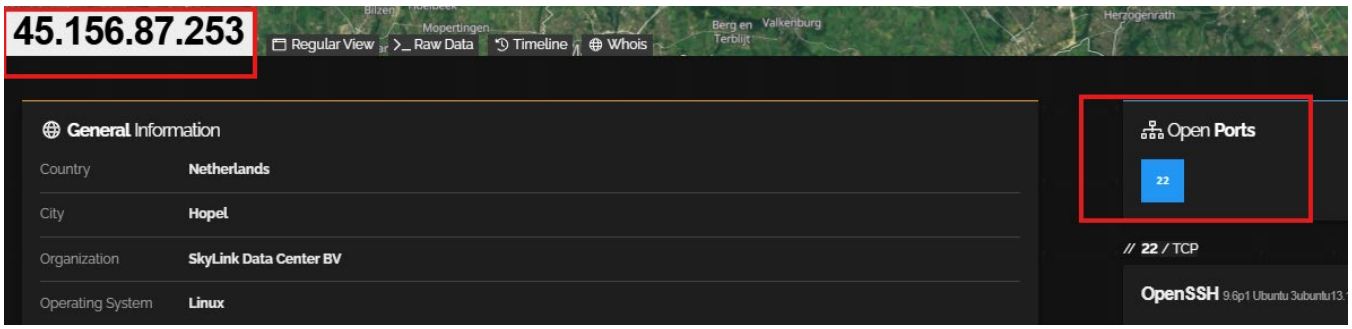


Figure 17.2: ShodanIP 45.156.87.253 (SkyLink Data Center, Netherlands, SSH Port 22)

The Netherlands VPS location provides geographical distance from the Brazilian target region. The open SSH port combined with active Telnet brute forcing establishes this as a multipurpose botnet staging server.

Target 18 http://185.208.159.132/harm7

This target is the first of four malware endpoints hosted on IP 185.208.159.132, a server located in Bern, Switzerland, operated by Global Data System IT Corporation. The filename "harm7" refers to a binary compiled for the ARMv7 architecture the processor architecture found in the majority of modern smartphones, single board computers (such as Raspberry Pi), network equipment, and a wide range of IoT devices. ARMv7 is one of the most prevalent embedded architectures globally, making a binary targeting this architecture capable of infecting an exceptionally broad range of devices.

VirusTotal Analysis

VirusTotal analysis of the harm7 endpoint returned a detection ratio of 13 out of 95 vendors. The detections classify the binary as malware consistent with IoT botnet recruitment payloads. The 185.208.159.132 host carries a self signed SSL certificate and presents an unusual combination of open ports22 (SSH), 135, 445 (SMB), 3389 (RDP), and 5985 (WinRM)on what Shodan identifies as a Linux system. The presence of Windows specific service ports (SMB, RDP, WinRM) on a Linux host with a self signed certificate is a strong indicator of either a compromised system, a dual boot configuration, or a deliberately misconfigured server used to evade detection while serving as a multipurpose C2 and malware distribution node.

Figure 18.1: VirusTotal185.208.159.132/harm7 (13/95 Detections, ARMv7 IoT Binary)

ARMv7 is the most prevalent embedded processor architecture globally, making this binary capable of infecting the widest range of devices including routers, IP cameras, and singleboard computers.

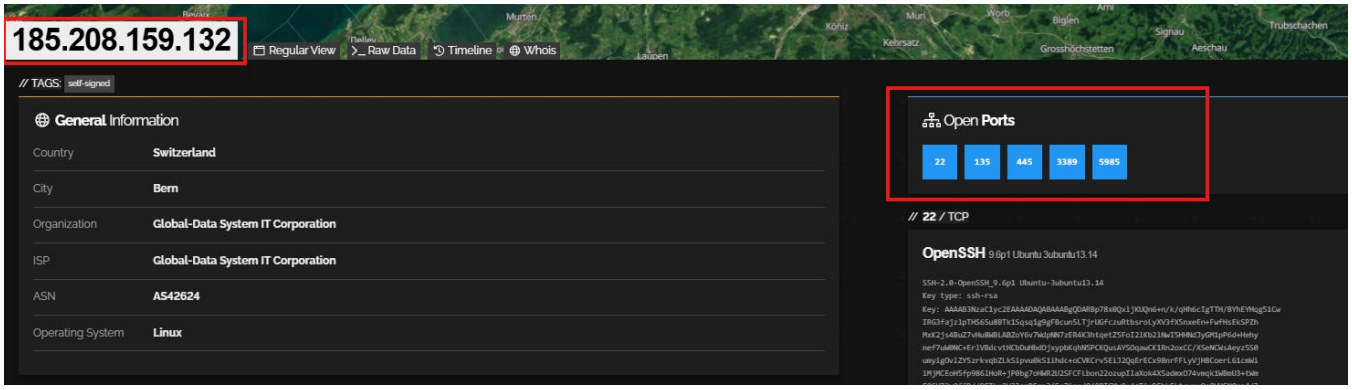


Figure 18.2: ShodanIP 185.208.159.132 (Bern, Switzerland5 Open Ports)

Windows specific service ports (SMB 445, RDP 3389, WinRM 5985) on a Linux system with a self signed certificate is a strong indicator of a compromised system or deliberately misconfigured multipurpose C2 server.

Target 19 http://185.208.159.132/arm6

The arm6 endpoint on 185.208.159.132 serves a malware binary compiled for the ARMv6 architecture. ARMv6 is an older ARM instruction set variant found in first generation Raspberry Pi devices, older smartphones, and certain embedded network equipment. Its inclusion alongside the ARMv7 binary on the same server confirms that the threat actor is systematically targeting a wide range of ARM based devices, prioritizing broad coverage over architecture specific optimization. The parallel hosting of arm6 and harm7 on the same server with matched detection ratios confirms a deliberate multiarchitecture payload strategy.

VirusTotal Analysis

VirusTotal analysis of the arm6 endpoint returned a detection ratio of 13 out of 95 vendors, identical to the harm7 endpoint. The matched detection ratios across both ARM variants confirm that the binaries are recognized as part of the same malware family by the detecting vendors. Both endpoints share the same hosting infrastructure on 185.208.159.132, and their analysis should be considered in conjunction with the Shodan infrastructure findings documented under Target 20.

Figure 19.1: VirusTotal185.208.159.132/arm6 (13/95 Detections, ARMv6 Binary)

The matched detection ratio with harm7 (13/95) confirms both ARM variants are recognized as the same malware family. Parallel hosting of ARMv6 and ARMv7 binaries confirms a systematic multiarchitecture targeting strategy.

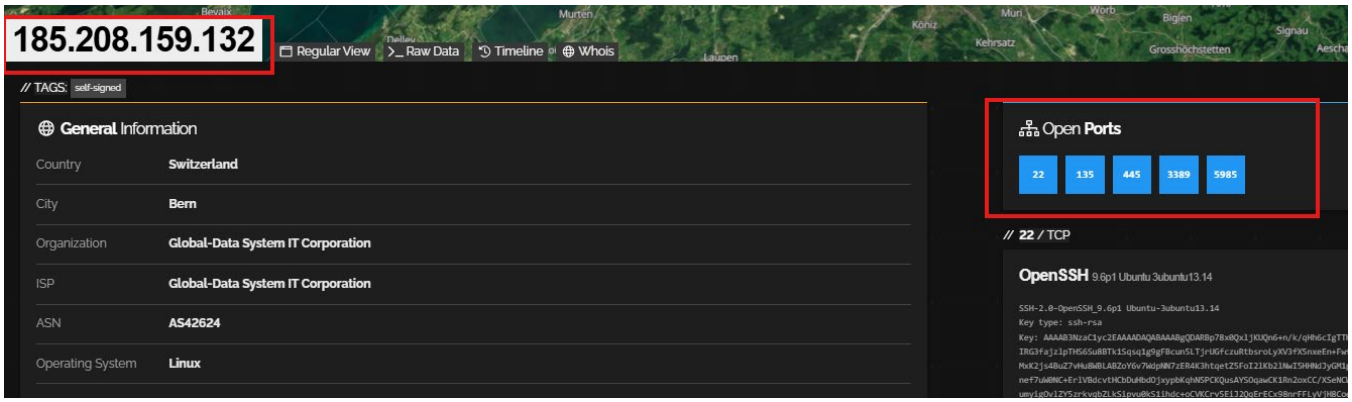


Figure 19.2: ShodanIP 185.208.159.132 SSH Key and Port Configuration Detail

The selfsigned SSL certificate observed alongside open Windowsspecific ports (RDP, SMB) on a nominally Linux host eliminates any possibility of legitimate enterprise use and confirms a dedicated malicious infrastructure node.

Target 20 http://185.208.159.132/hmips

The hmips endpoint represents the third malware binary hosted on 185.208.159.132, compiled for the MIPS architecture. "hmips" likely stands for "hard float MIPS"a MIPS variant with hardware floating-point support though it may also refer to big-endian MIPS (MIPSBE), which is the architecture used in many enterprise grade routers, cable modems, and network attached storage devices. The targeting of MIPS alongside ARM architectures confirms that this server is functioning as a comprehensive botnet recruitment payload server, hosting binaries capable of infecting virtually the full spectrum of IoT and embedded device types encountered on consumer and enterprise networks.

VirusTotal Analysis

VirusTotal scan results for the hmips endpoint are pending at time of report compilation. Based on the consistent 13/95 detection ratios observed across the harm7 and arm6 endpoints on the same server, the hmips binary is assessed as high confidence malware sharing the same threat family classification. The Shodan infrastructure analysis documented below applies to all endpoints hosted on 185.208.159.132.

Figure 20.1: VirusTotal http://185.208.159.132/hmips

Shodan Infrastructure Analysis

Shodan analysis of IP 185.208.159.132 reveals a host in Bern, Switzerland operated by Global Data System IT Corporation. The server presents five open ports: 22 (SSH), 135 (Microsoft RPC endpoint mapper), 445 (SMB), 3389 (RDP), and 5985 (WinRM/HTTP). The combination of Windows specific service ports on a system identified as running Linux, together with a selfsigned SSL certificate and the active hosting of multiple malware binaries, presents an extremely high risk profile. The Microsoft HTTPAPI banner observed on the WinRM port further supports the assessment that this is either a compromised Windows system, a system running both Linux and Windows workloads, or a deliberately configured C2 server designed to present Windowlike services as a deception layer. The self signed certificate eliminates the possibility that this is a legitimate enterprise server, as legitimate servers in this category would invariably use commercially issued certificates.

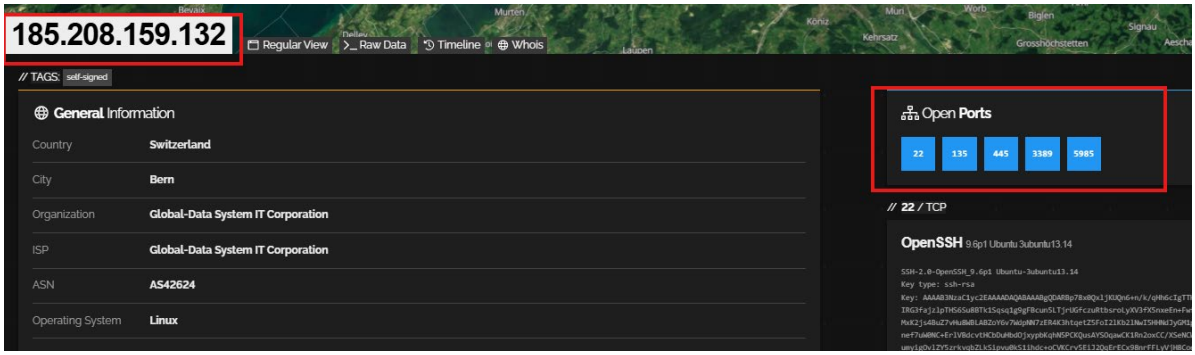


Figure 20.2: ShodanIP 185.208.159.132 SSH Key and Port Configuration Detail

Target 21 http://185.208.159.132/arm7

The arm7 endpoint is the fourth malware binary hosted on 185.208.159.132. Unlike the "harm7" endpoint which likely refers to "hard float ARMv7," the "arm7" designation without the "h" prefix suggests a soft float ARMv7 binary variant compiled without hardware floating-point support, broadening compatibility to older or stripped down ARMv7 devices that do not expose hardware FPU instructions. The deliberate provision of both hard float and soft float ARMv7 variants on the same server represents a level of operational sophistication that ensures maximum device coverage across the ARMv7 ecosystem, including legacy embedded systems that may not support the full ARMv7 EABI with hardware floating-point.

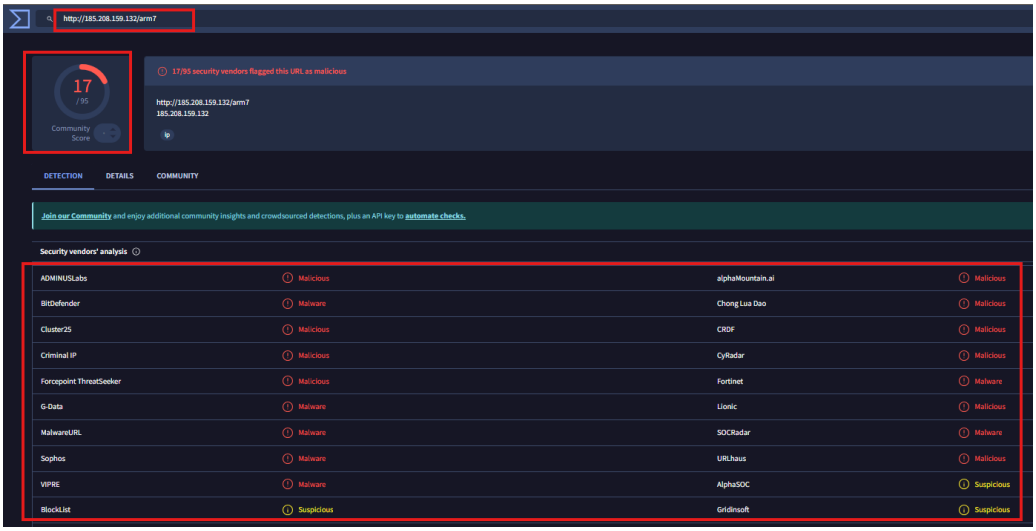


Figure 21.1: VirusTotal http://185.208.159.132/arm7

VirusTotal Analysis

VirusTotal scan results for the arm7 endpoint are pending at time of report compilation. Based on the established pattern of the 185.208.159.132 server where both the harm7 and arm6 binaries returned identical 13/95 detection ratios the arm7 binary is assessed as high confidence malware of the same family. The infrastructure analysis documented under Target 20 applies fully to this endpoint. All four binary endpoints on 185.208.159.132 (harm7, arm6, hmips, arm7) should be treated as active malware distribution points and their serving IP blocked at the perimeter firewall, with the additional recommendation to monitor network traffic for outbound connections to port 22, 445, 3389, and 5985 on this host.

Conclusion

This investigation originated from a single low-confidence phishing URL hosted on Netlify, initially detected by only 2 out of 95 VirusTotal engines. However, through structured threat analysis and correlation, it evolved into the identification of a **large-scale, multi-layered threat campaign** spanning **21 distinct indicators**, geographically distributed across multiple countries, and encompassing **three primary threat vectors**: credential harvesting, IoT botnet propagation, and infrastructure brute-force activity.

The attacker heavily relies on **trusted cloud services (Netlify, Cloudflare)** to host phishing pages. This allows the campaign to **bypass traditional security tools**, since these platforms are usually considered safe. The phishing infrastructure also uses **.shop domains and domain shadowing**, making it easy to replace blocked domains and stay active.

In parallel, the campaign includes a **malware operation targeting IoT devices**, using **Mozi botnet techniques** with decentralized (DHT-based) command-and-control. Malware is prepared for multiple device types (ARM, MIPS), showing intent to infect a wide range of systems.

A key finding is that **signature-based detection failed at the early stage**. Most malicious URLs had **very low or zero detection rates**, meaning users could be exposed before security tools react.