Continue

# T33n leak 5-17 invite

**Sign-up link to malicious websites** The text appears to be a collection of sign-up links to various websites. These links are likely attempts to lure users into registering for suspicious or malicious purposes. Some details about these links are as follows: * There are four different sign-up URLs provided, each pointing to a different website. * Two of the websites (kisqf.in and paradise907.in) have similar names and structures, suggesting they may be related or part of a larger operation. * The other two websites (america25.site and vanced56.xyz) also have suspicious-sounding names. * All four URLs attempt to redirect users to the same IP address (23.36.76.226), which is likely a proxy server. **Security warnings** The text also includes some security-related data, indicating that these sign-up links may be malicious: * The "Quad9 DNS" analysis tool has identified the website vaer63kmp.cc as having "malicious" properties. * A GET request to the website's /invite/i=959 endpoint resulted in a 403 Forbidden error, suggesting that the site is blocking access or attempting to evade security measures. **HTTP requests** The text includes several HTTP requests made by a browser (Firefox) when trying to access these sign-up links. These requests include: * POST and GET requests to various IP addresses * Headers indicating attempts to bypass security features (e.g., Pragma: no-cache) * Accept-Language headers set to English, suggesting that the website is targeting English-speaking users. Overall, this text appears to be a collection of suspicious sign-up links, HTTP requests, and security-related data. It's likely intended for analysis or research purposes rather than general reading. **HTTP Response Headers** The HTTP response headers from the server `vaer63kmp.cc` include various security and caching directives. Some key headers are: * **Security**: The server requires a specific set of permissions for the client, including no access to accelerometer, camera, microphone, or payment features. * **Caching**: The response is cached for a short period (0 seconds) with a maximum age of 0, indicating that the content should not be stored by the browser or any intermediate caches. * **Origin**: The server enforces same-origin policies, meaning that resources can only be accessed from the same domain. * **Content**: The response contains compressed JavaScript code and HTML documents. **Server Information** The server is identified as `cloudflare` with a specific Ray ID (`895760251b0a56a2`) and CF-RAY header. This suggests that the server is using Cloudflare's content delivery network (CDN) to serve its resources. **Other Headers** There are several other headers present in the response, including: * **Cross-Origin-Embedder-Policy**: Requires a specific set of policies for embedding content from another origin. * **Permissions-Policy**: Specifies which permissions are allowed or denied by the client. * **Report-To**: Provides information about how to report security issues or errors. Overall, these headers suggest that the server is taking steps to secure its resources and enforce certain policies on clients. A request was made to vaer63kmp.cc from a Firefox browser (version 96.0) with Linux x86_64 architecture. The User-Agent string is Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0. The Accept header specifies that the client can accept various types of content, including image formats. The Referer header indicates that the request originated from a URL on vaer63kmp.cc. The server responded with an HTTP/1.1 200 OK status code, indicating that the request was successful. The Content-Type header specifies that the response is text/html with UTF-8 character encoding. The Transfer-Encoding and Connection headers indicate chunked transfer and keep-alive connections, respectively. The Cache-Control and Pragma headers specify that caching should be disabled. The Last-Modified header indicates that the resource has not been modified since June 17, 2024 at 22:54:43 GMT. The Report-To header provides information about Cloudflare's reporting system. The NEL (Node.js Extension) header specifies that the client should send reports to a specific endpoint. The Vary and Server headers indicate that the server supports Accept-Encoding and is running on Cloudflare. The CF-RAY and Content-Encoding headers provide additional information about the request. The request was flagged as malicious by Quad9 DNS, which indicates that it may be related to sinkholing or other types of malicious activity. **HTTP Response Header** The response from ` ` contains: * A challenge token (`CF-Challenge`) with a specific value * Details about the server, including its type (Cloudflare) and location (OSL) * Information about the client's browser and operating system **Client Request Header** The client's request to ` ` includes: * An HTTP method (`GET`) * A specific path within Cloudflare's challenges platform * Details about the client's browser and operating system **Server Response Header** The server responds with: * A success code (200 OK) * The content type of the response (text/html; charset=UTF-8) * Various security-related headers, such as `content-security-policy` and `permissions-policy` Overall, this text appears to be an exchange between a client (likely a browser) and a server (Cloudflare) involving authentication and security checks. The given text appears to be a cached response from an OCSP (Online Certificate Status Protocol) checker. It seems to be a DNS query response for the domain r10.o.lencr.org, which is maintained by Akamai International B.V. Here's a breakdown of the response: * The request was made using the HTTP/1.1 protocol and had a content length of 85 bytes. * The server responded with a status code of 200 OK, indicating that the request was successful. * The response contains an ETag (Entity Tag) value of "18FFB58DA62F40B37A43B0BAACEEFE8BC3EF83CCDF9EE19FF874CCB0D802C9F2" and a Last-Modified date of Sat, 15 Jun 2024 17:32:00 UTC. * The response also includes several Cache-Control directives that specify the cache behavior for this resource. This response is likely used to verify the status of an SSL/TLS certificate issued by Akamai International B.V. **HTTP Request/Response Summary** * The request was made to challenges.cloudflare.com, which sent a response to the client. * The response was an image (PNG) with a size of 61 bytes. * The server responded with a HTTP/3 status code of 200 OK. **Server Response Headers** * `Expires`: The date when the content will expire (June 18, 2024, 05:33:56 GMT). * `Date`: The current date and time (June 18, 2024, 01:06:15 GMT). * `Connection`: The server connection was kept alive. * `Content-Type`: The response type is image/png. * `Content-Length`: The size of the response body (61 bytes). **Client Request Headers** * `Host`: The requested host was challenges.cloudflare.com. * `User-Agent`: The client user agent was Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0. * `Accept`: The client accepted image types avif, webp, and any other type (*/*). * `Referer`: The request came from the URL . **Additional Information** * A POST request was made to vaer63kmp.cc with a suspicious URL and content. * The response from vaer63kmp.cc contained an HTML page with a set-cookie header. A report from Cloudflare (a content delivery network) includes information about an HTTP request and response. The request is for a URL at vaer63kmp.cc, specifically for an invitation to something. The request comes from a user agent identified as Mozilla/5.0 Firefox 96 on Linux. The request is made using the POST method and contains some encoded data. The server responds with an HTTP 200 OK status code, indicating that the request was successful. The response includes a text/html document, which is compressed using gzip. The report also notes that the request appears to be malicious, as determined by Quad9 DNS and Sinkholed. Additionally, there are two more requests included in the report: one for a CSS file (chunk-vendors.c57533e1.css) and another GET request for the same URL as before. Both of these requests are also deemed malicious. Throughout the report, you'll see various headers and values, including those related to Cloudflare's services (such as CF-RAY and Content-Encoding). The report concludes by indicating that the requests were successful and that the responses included HTML and CSS content. **HTTP Request and Response Details** The request was made to `vaer63kmp.cc` for two CSS and JavaScript files. The requests were made from a Firefox browser on Linux, with an IP address in Norway. **Cache Information** The first file requested had a cache status of "HIT" (cache hit), which means the file was already cached by Cloudflare's cache system. The cache age was 279 seconds, and the maximum age allowed by the server is 604800 seconds. The second file also had a cache status of "REVALIDATED", which means that the cache has been revalidated by Cloudflare to ensure it's still up-to-date. **Cloudflare Information** Both requests were served through Cloudflare, with the following information: * The response was cached by Cloudflare * The server is using Cloudflare for security and performance * The report-to endpoint is a Cloudflare-specific feature that allows reporting of security issues **Security Warnings** Quad9 DNS has flagged `vaer63kmp.cc` as malicious, indicating potential security risks. **HTTP Request Headers** The request headers included information about the browser type, language, and encoding preferences. A web request was made to vaer63kmp.cc using the Mozilla Firefox browser. The request was to retrieve a JavaScript file named "chunk-vendors.ea790e22.js" and was accompanied by various headers, including ones that specified the use of cloudflare (CF-RAY) and Quad9 DNS (AnalyzerVerdictAlert). The request was successful and returned a 200 OK response with a Content-Type of text/javascript. The request also included some suspicious activity, flagged by Quad9 DNS as malicious. This may indicate that the website or server is compromised or hosting malicious content. Additionally, there were two other requests made to vaer63kmp.cc: 1. A GET request to retrieve an invitation link, which was also successful and returned a 200 OK response. 2. A POST request to send some data (JSON format) to the same URL, which was also successful and returned a 200 OK response. Throughout the requests, various headers were included, such as Accept-Encoding, Content-Type, and Connection, which indicate that the browser is capable of handling compressed data and using keep-alive connections. This is an HTTP request and response log that shows a series of requests made to various servers. The first request is for a video file (`ver.mp4`) from the Discord CDN server, but it returns a 404 "Not Found" error. The request headers indicate that the request was made using Mozilla Firefox on Linux, with a user agent string indicating a version 96 browser. The Accept-Language header is set to English (US) and the DNT header is set to 1, indicating that the request does not track the user's online activities. The response headers show that the request was received by Cloudflare, which served the request from its cache. The `cf-cache-status` header indicates that the request was a hit in the cache, and the `cache-control` header specifies that the cache should be kept for one year. The log also includes requests made to other servers, including vaer63kmp.cc, which appears to be a sinkholed domain (i.e., a domain that has been taken over by malicious actors). The request headers indicate that this request was also made using Mozilla Firefox on Linux. The server responds with a 200 OK status code for requests made to two URLs: challenges.cloudflare.com/turnstile/v0/g/6aac8896f227/api.js?onload=OZxW4&render=explicit and img/icons/favicon.svg. The response includes metadata about the request, such as the user agent, accept language, and content encoding. The server also responds with a 200 OK status code for requests made to two URLs: vaer63kmp.cc/invite/i=959 and vaer63kmp.cc/img/icons/favicon.svg. The response includes metadata about the request, such as the user agent, accept language, and content encoding. The server also includes several Cloudflare-specific headers, including NEL (Named Edge Cache), which provides information about cache hits and misses, and CF-RAY (Cloudflare Ray ID), which identifies the edge server responsible for serving the response. The URL `172.67.207.62:80` (vaer63kmp.cc) sent an HTTP request to itself, requesting the Apple touch icon image with a size of 152x152 pixels. The request was made by a browser running on an x86_64 Linux system, version 96.0. The request included several headers: * User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0 * Accept: image/avif,image/webp,*/* * Accept-Language: en-US,en;q=0.5 * Accept-Encoding: gzip, deflate The server responded with a 200 OK status code and an image of size 4046 bytes. A subsequent request was made to `ocsp.sectigochina.com` to verify the SSL certificate. This request included: * User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0 * Accept: */* * Accept-Language: en-US,en;q=0.5 * Accept-Encoding: gzip, deflate The response included an image of size 472 bytes and a digital signature (Etag). Finally, two requests were made to `b.yzcdn.cn` for images: * `vant/icon-demo-1126.png`: This request was made by a browser running on an x86_64 Linux system, version 96.0. + User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0 + Accept: image/avif,image/webp,*/* + Accept-Language: en-US,en;q=0.5 + Accept-Encoding: gzip, deflate, br * `icon-demo-1126.png`: This request was made by a browser running on an x86_64 Linux system, version 96.0. + User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0 + Accept: */* + Accept-Language: en-US,en;q=0.5 Note that the requests to `b.yzcdn.cn` were not successful, and the responses included error messages. The response headers for these requests included: * Content-Type: application/ocsp-request * Content-Type: application/ocsp-response * X-CCACDN-Proxy-ID: mcdpinlb3 * X-Frame-Options: SAMEORIGIN The response from the CDN (Content Delivery Network) for the specified URL is as follows: * Status code: 200 OK * Last modified date: June 18, 2024, 01:06:24 GMT * Content type: Image PNG with a size of 8886 bytes * Server information: OpenResty * Cache control: Public, max age of 2592000 seconds (approximately 28.5 days) * ETag: "Fo6Li9S6PmtshVfZSnJgYf3WJJL9" * Content disposition: Inline file with filename="icon-demo-1126.png" and UTF-8 encoding * Content transfer encoding: Binary However, when attempting to retrieve the same URL again after a short delay, the response is different: * Status code: 404 Not Found * Last modified date: June 18, 2024, 01:06:23 GMT * Content type: Application XML with UTF-8 charset and a size of 229 bytes * Server information: CF-RAY (Cloudflare Ray ID) * Cache control: Public, max age of 31536000 seconds (approximately 1 year) The response also includes various headers, such as Accept-Ranges, Access-Control-Allow-Origin, X-Log, and more. I encountered a suspicious website (vaer63kmp.cc) while performing DNS analysis, which triggered an alert from Quad9. The site is classified as malicious and has been sinkholed. A GET request was made to the socket.io endpoint with various headers indicating a potential WebSocket connection. However, I couldn't establish a secure connection due to JavaScript being disabled in my browser.