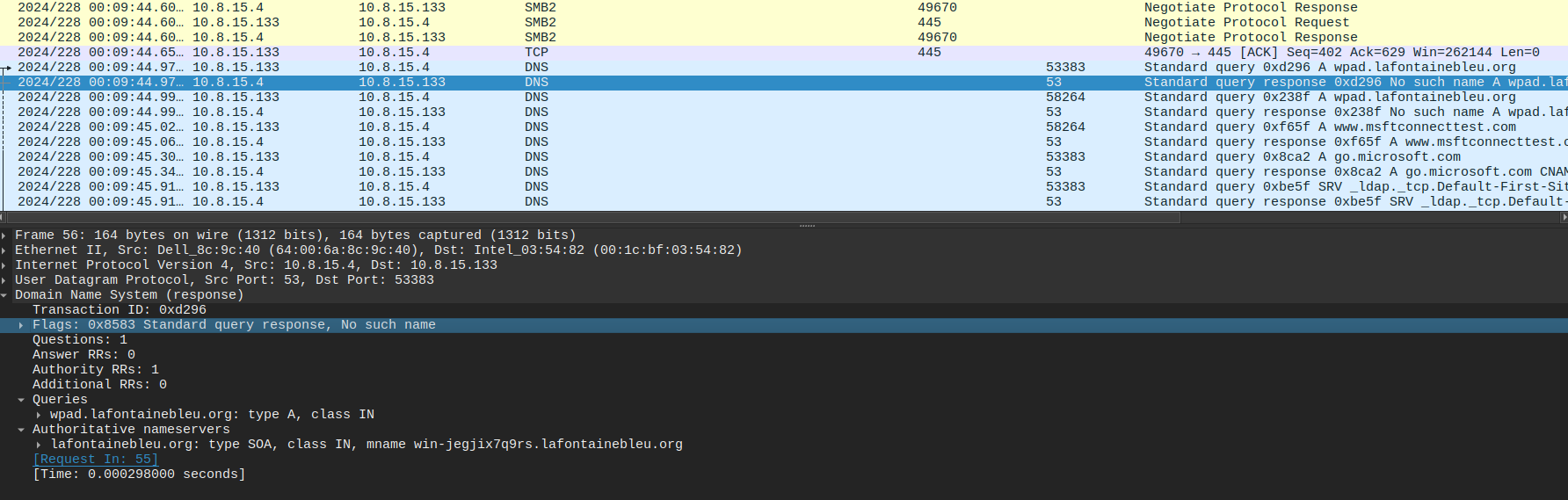
# INCIDENCE REPORT ON WARM COOKIE 2024-08-15 TRAFFIC ANALYSIS EXERCISE ON MALWARE TRAFFIC ANALYSIS. NET

**Executive summary**:

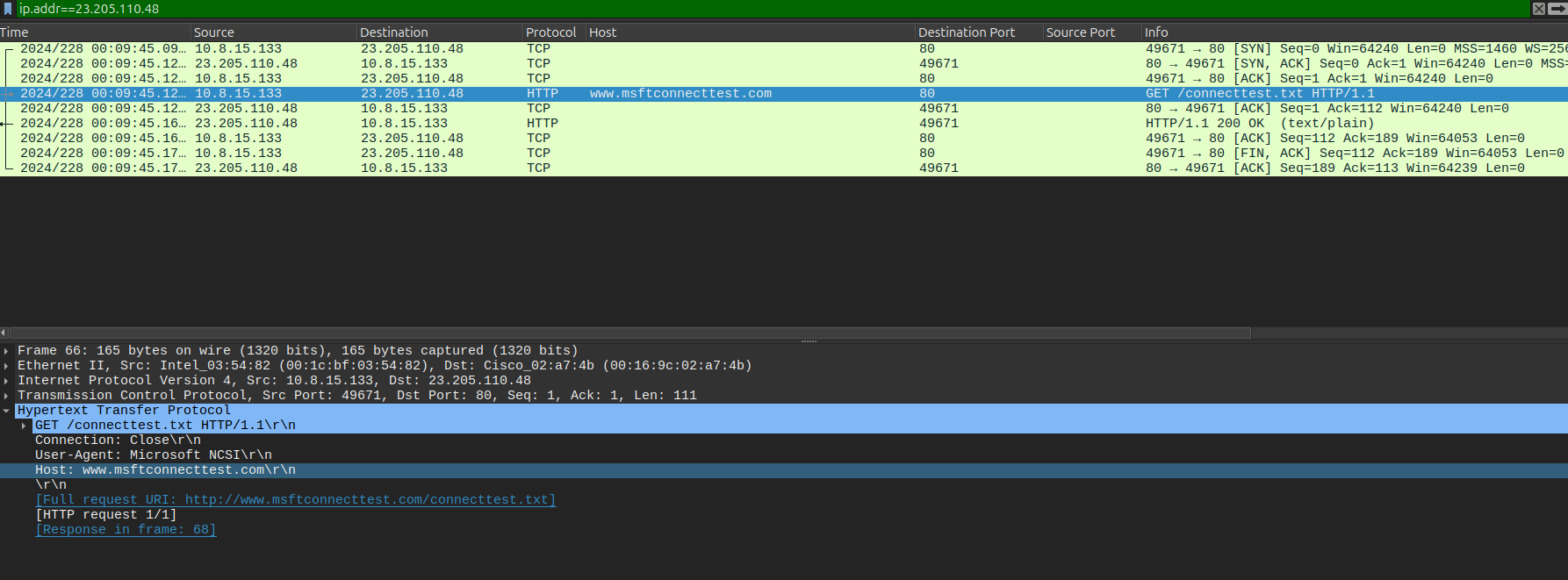
On 2024-08-15 from 00:09 utc an internal host within the local LAN of Ip 10[.]8[.]15[.]133 was observed performing multiple suspicious behaviors indicative of potential compromise or malicious activity. The sequence of events includes attempts to interact with domain infrastructure, encrypted communication with external IPs, anomalous DNS behavior, and download of executable content from a non-standard domain.

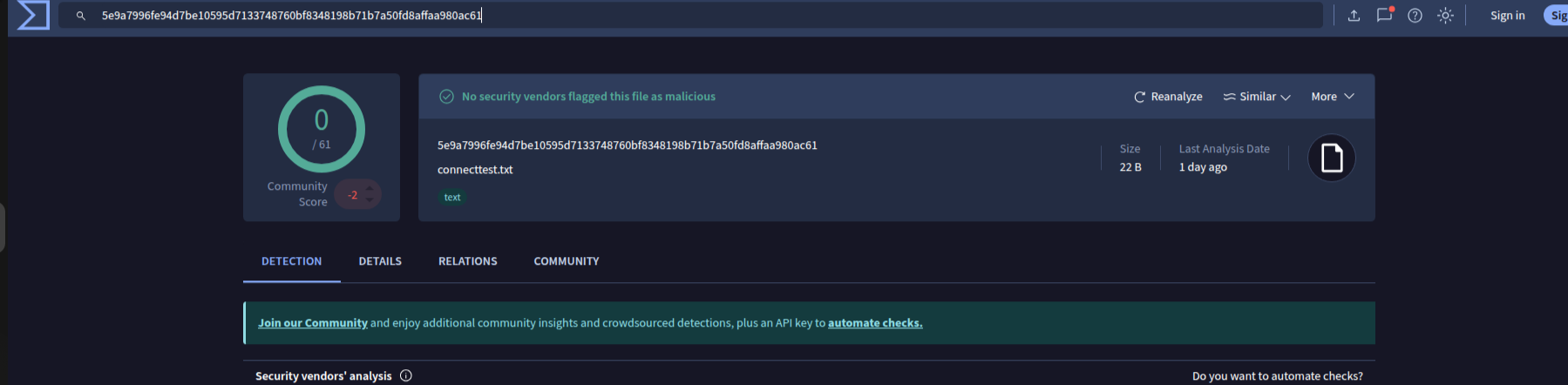
Timeline of events:

Compromised host tries to get information on where wpad is located in the domain

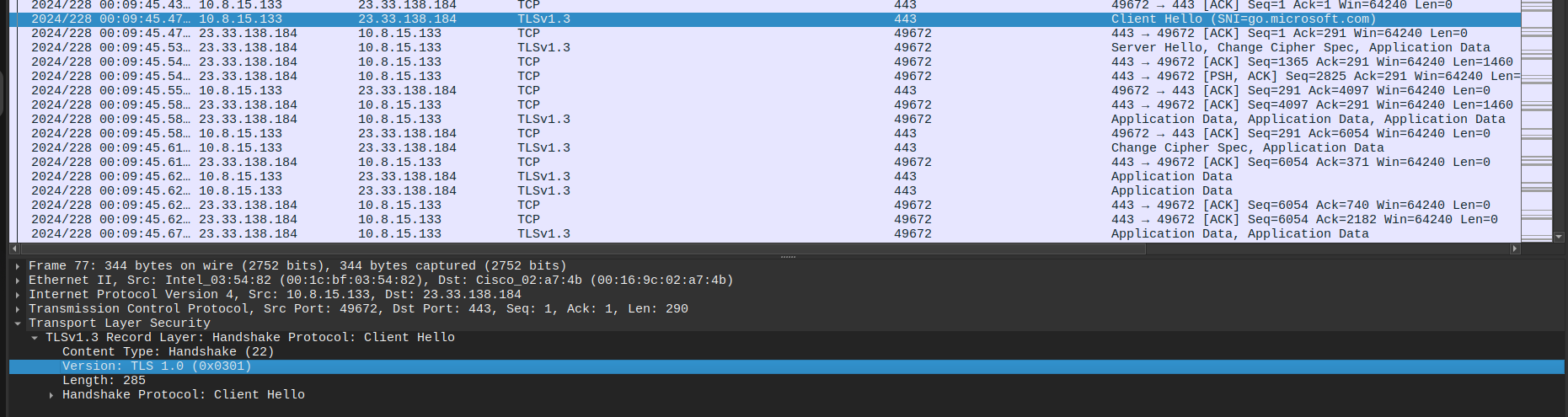


Compromised host get a .txt file from msftconnecttest.com which I not flagged as malicious

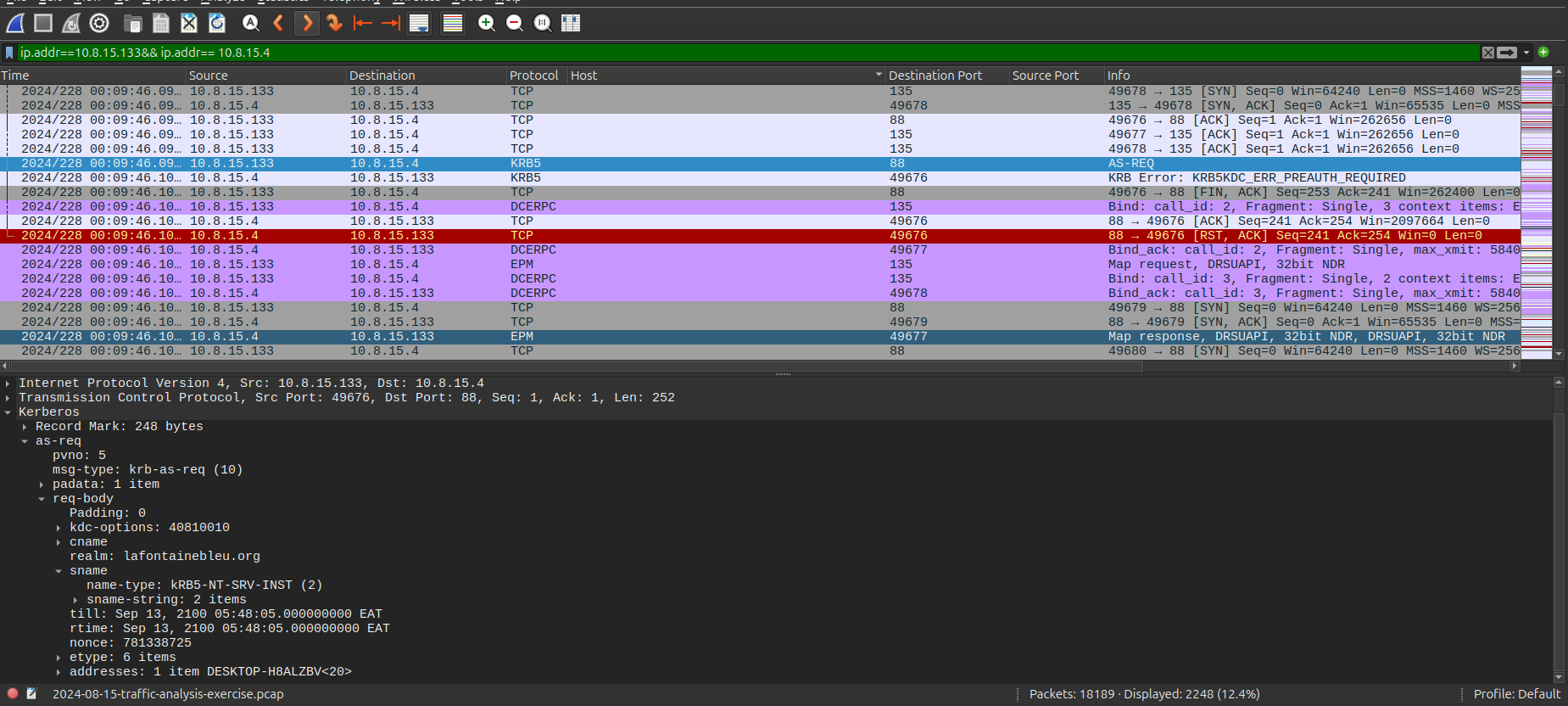




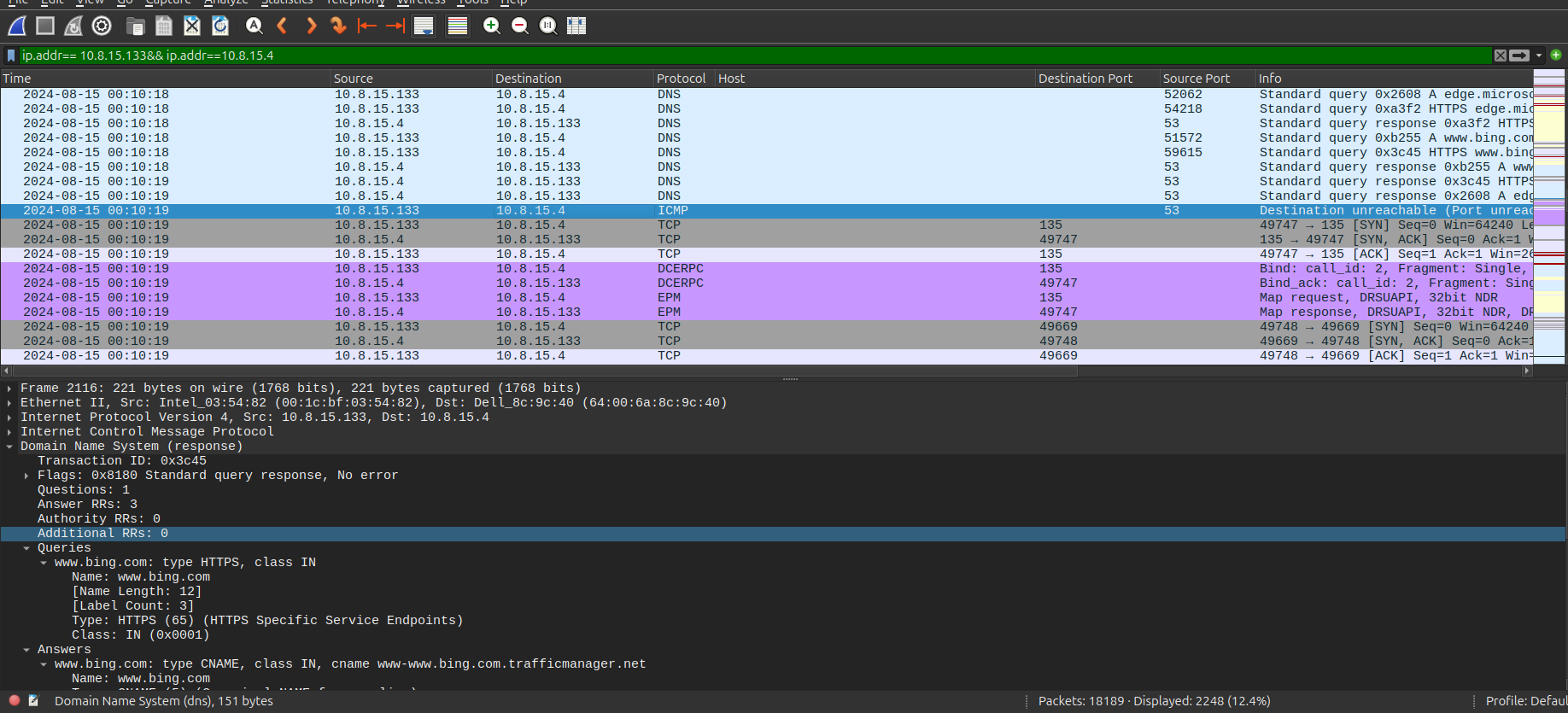
Compromised host does a TLS handshake with an outside Ip which isn’t malicious but TLS 1.0



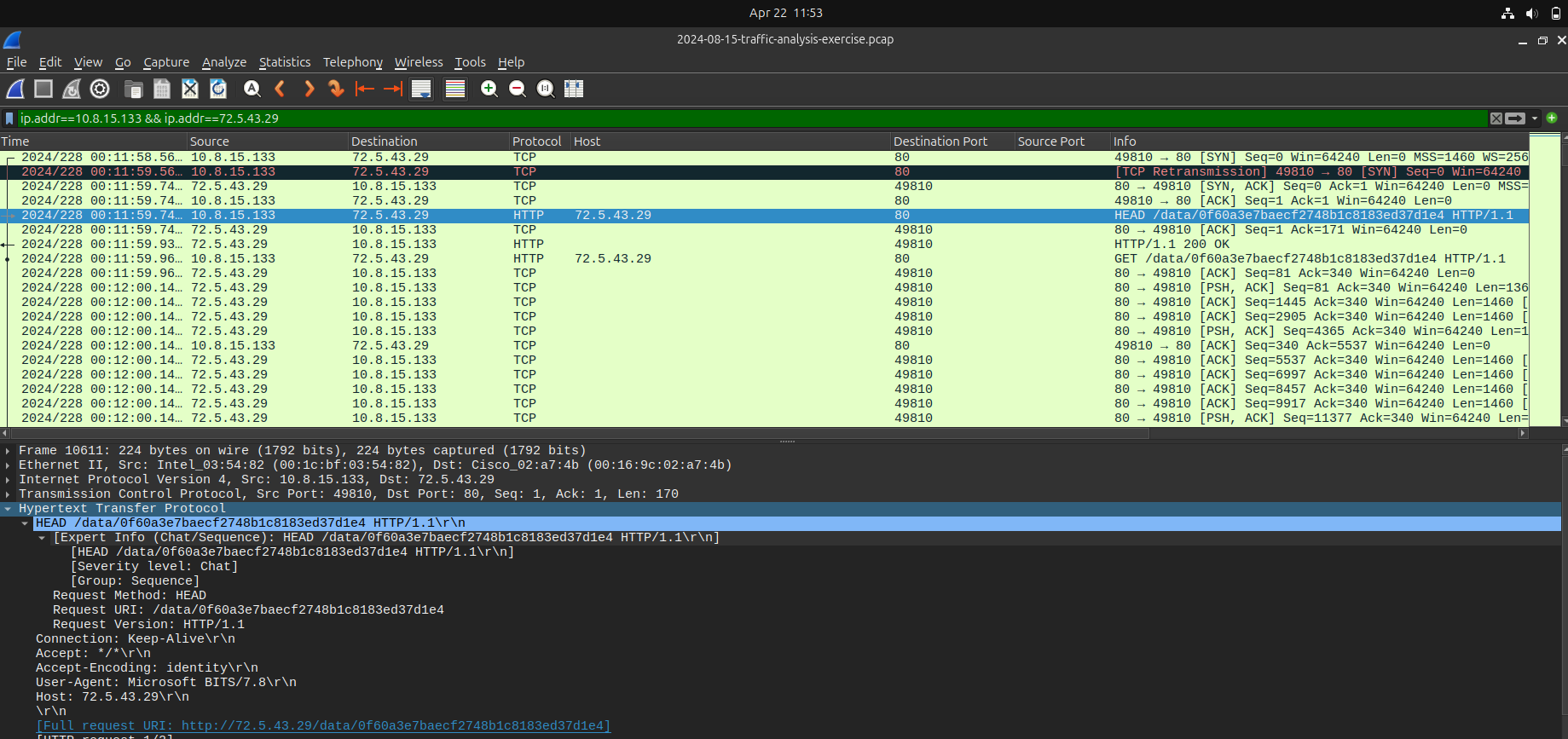
Compromised host does a Kerberos ticket grating service request to access the domain controller



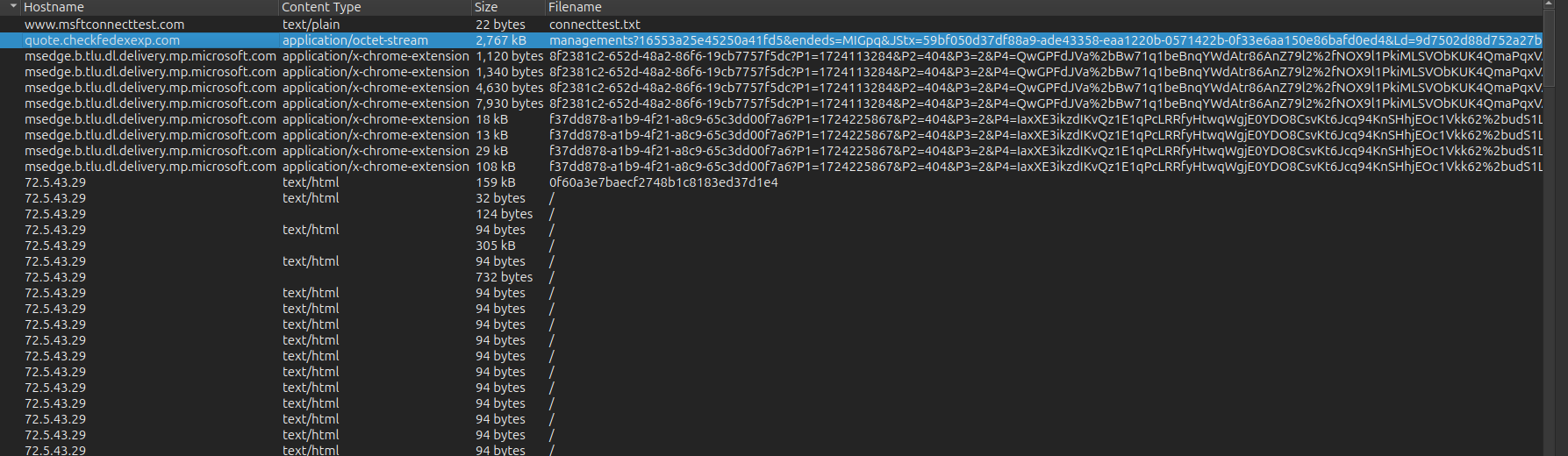
Compromised host replies unsolicited DNS queries to the domain controller through ICMP protocol



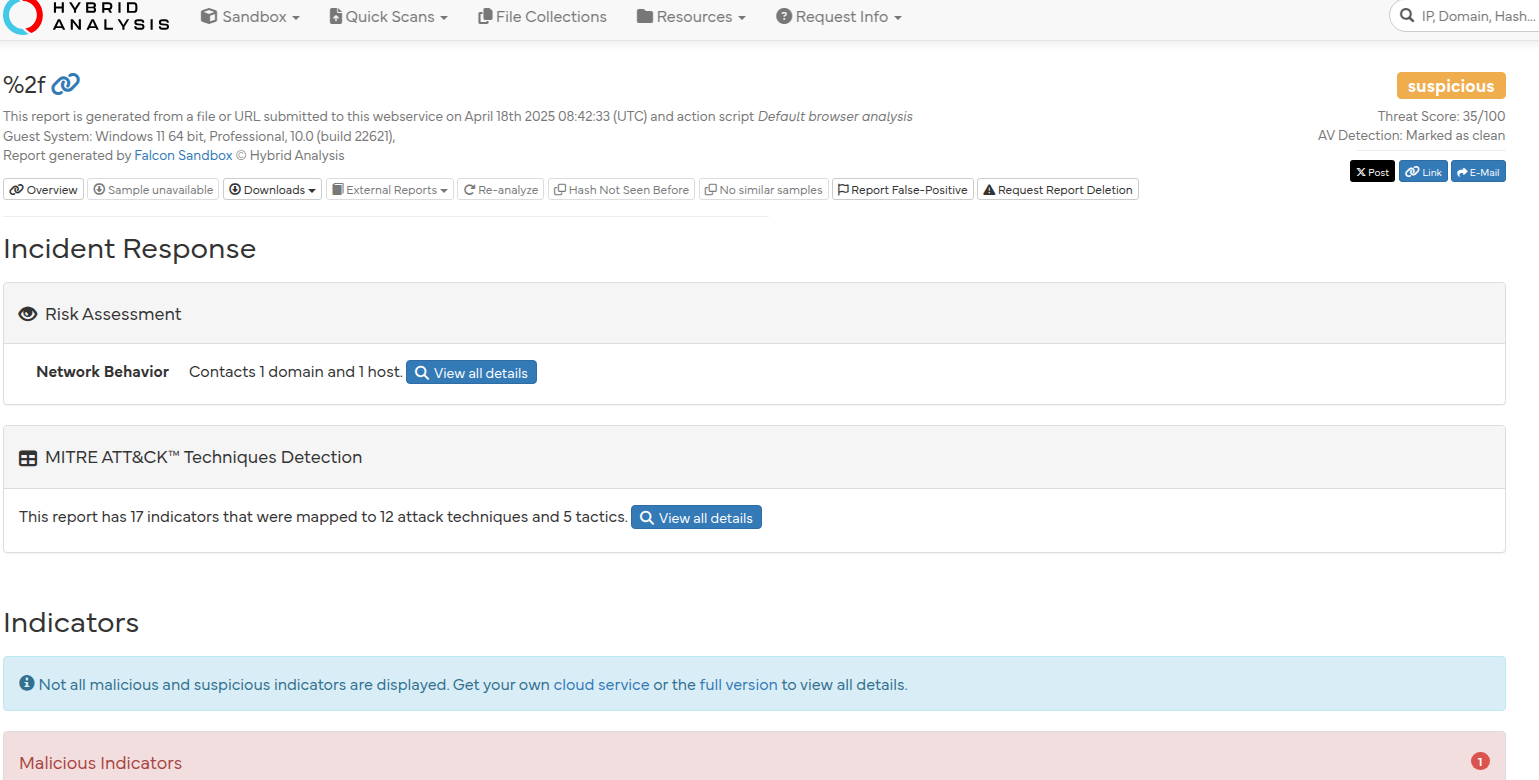
Compromised host visits a malicious domain whose user agent is incorrectly spaced and gets some malicious documents some of which are disguised as html content but are seen to run processes

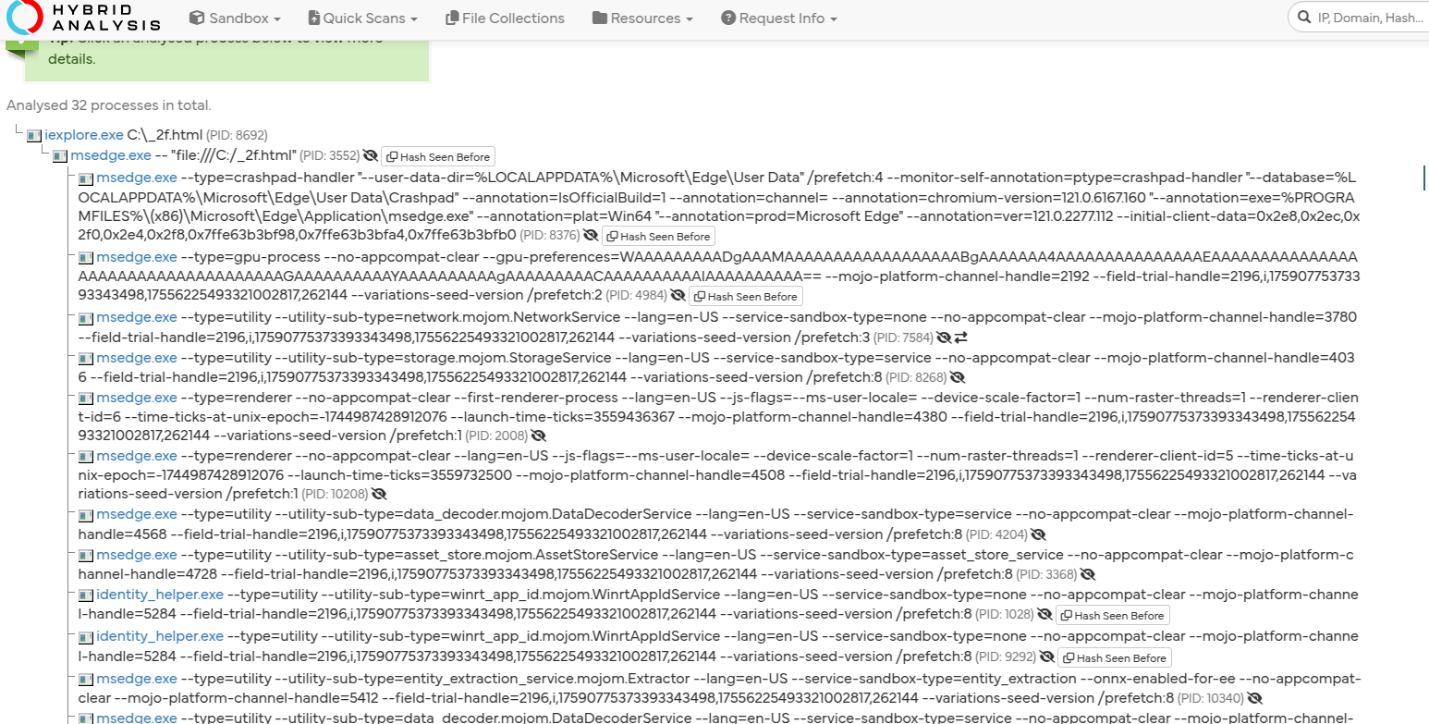




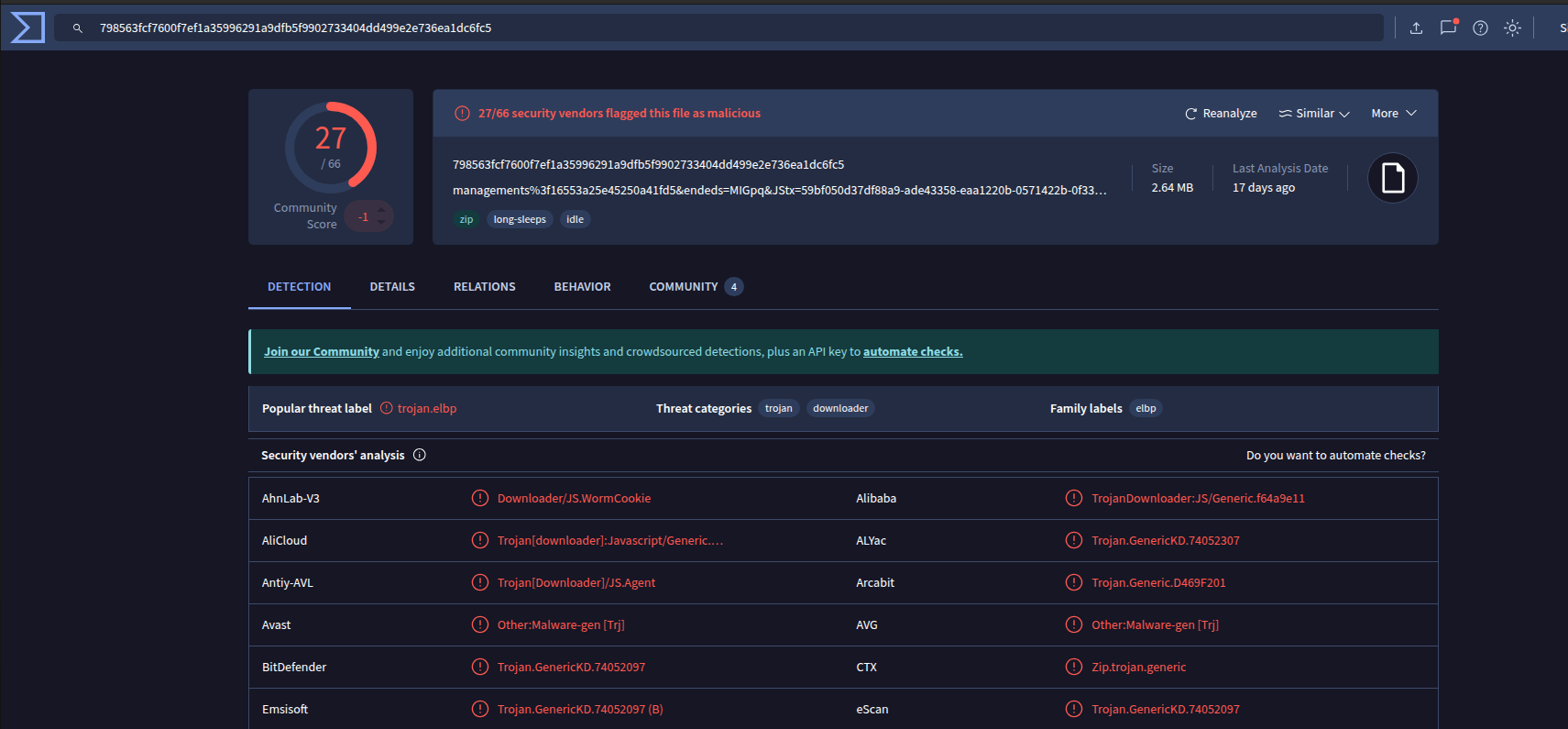


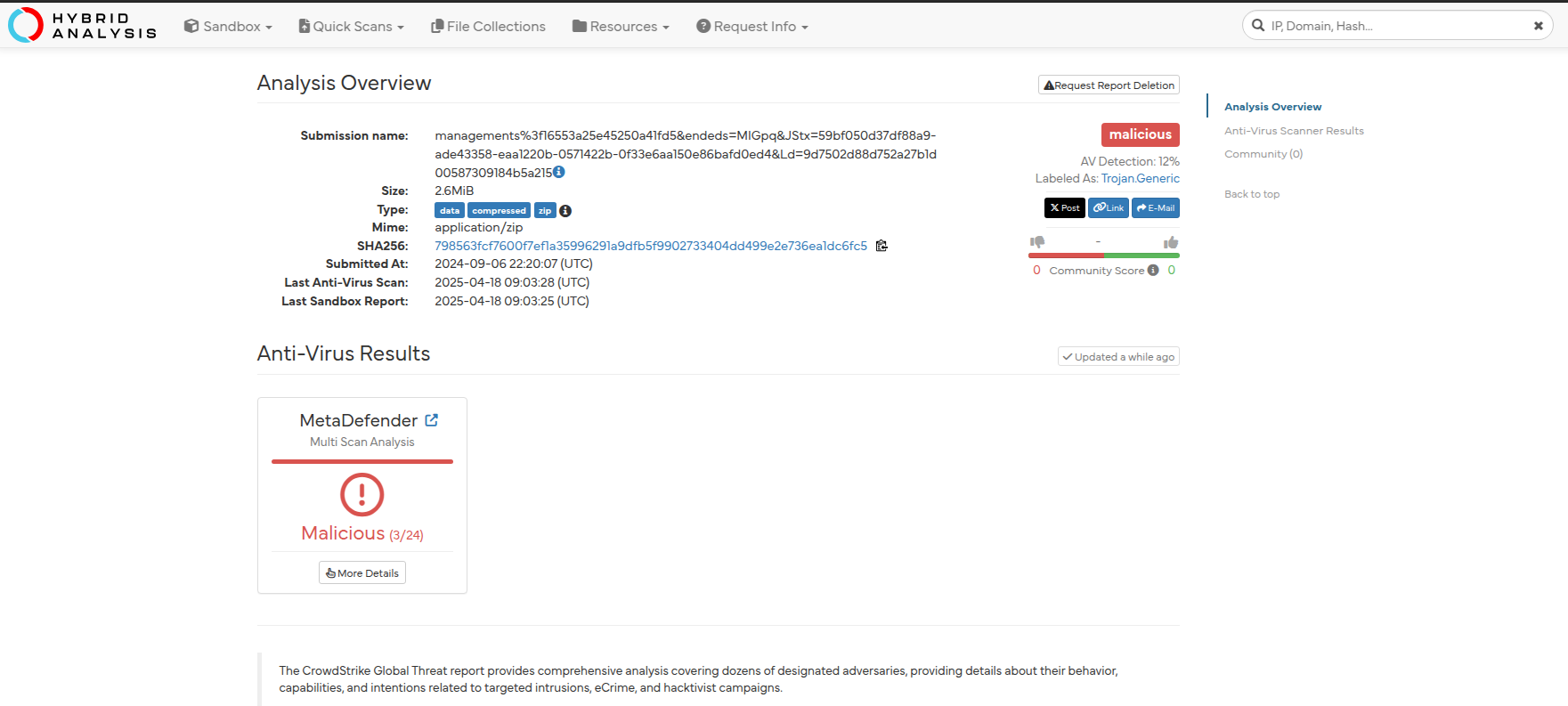
The file (2f%) disguised as html file is flagged as suspicious and seen to run processes on the background.



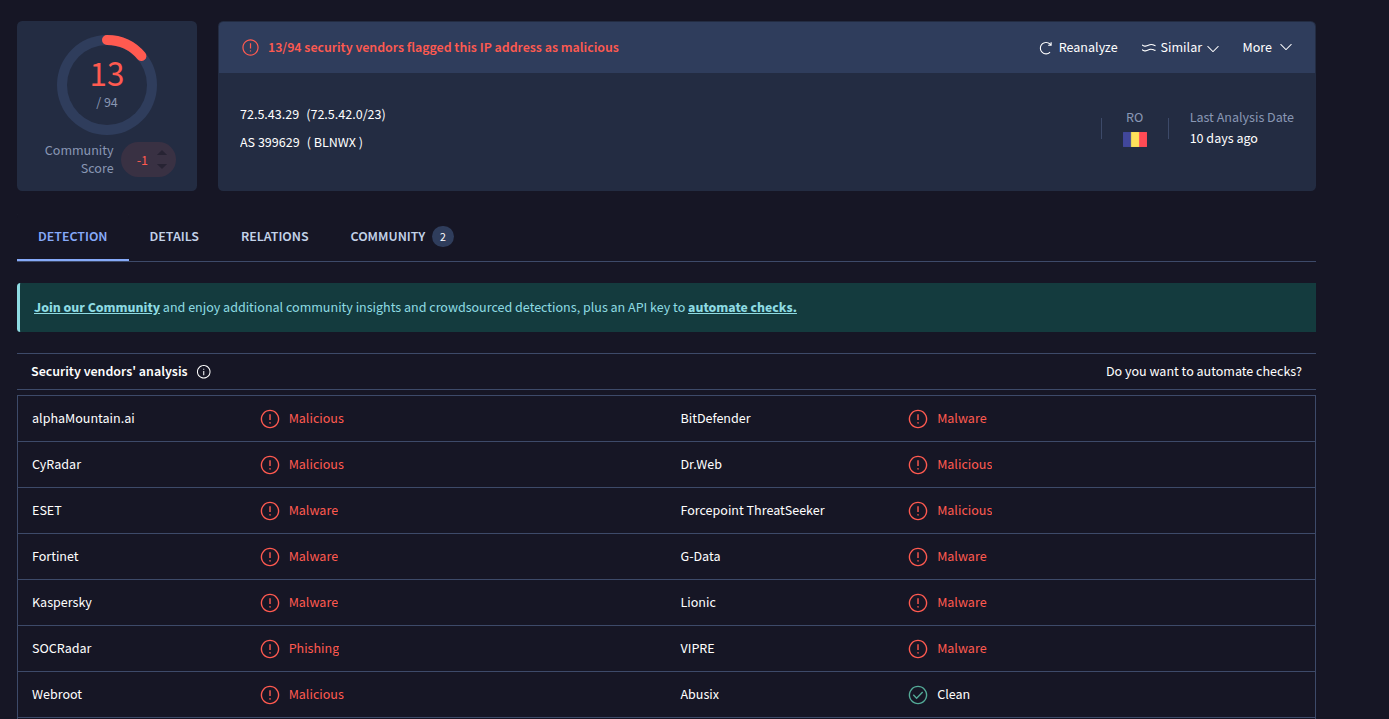


Another file “managements%3f16553a25e45250a41fd5&endeds=MIGpq&JStx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=9d7502d88d752a27b1d00587309184b5a215” is also flagged as suspicious and regarded as a trojan downloader.





The domain host is also flagged as suspicious



Compromised host does a suspicious post to the malicious website

**Systems involved**

|  |  |  |
| --- | --- | --- |
| Host Ip | Role played | Notes |
| 10[.]8[.]15[.]133 | Suspected compromised endpoint | Initiated the incidence |
| 10[.]8[.]15[.]4 | Domain controller | Targeted for Kerberos |
| 72[.]5[.]43[.]29 | External host/server | Malicious documents were retrieved and posted here |
| 23[.]33[.]138[.]184 | External server | TLS V.1 was conducted |

**Indicators of compromise**

* TLS version 1.0 was used which is deprecated
* Kerberos anomaly ticket was until sept 2100
* DNS tunnelling through ICMP protocol
* Incorrect spacing of User Agent: Mozilla / 5.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)
* Files marked as malicious
* External Ips
* Non-standard domain: 72[.]5[.]43[.]29