Malware traffic analysis
Case: Analysis of 2024-11-26 - TRAFFIC ANALYSIS EXERCISE: NEMOTODES
Daniel Cruz
7/28/25

Summary

This project analyzes a PCAP file containing malicious HTTP and TCP traffic associated with the IP address 194.180.191.64. A total of 132 connections were identified, with many HTTP POST requests to http://194.180.191.64/fakeurl.htm and numerous TCP sessions over port 443.

The behavior shows malware attempting Command and Control (C2) communication, using techniques like abusing HTTPS ports and retransmissions with payloads.Observed Indicators of Compromise (IOCs).

This analysis demonstrates my ability to investigate malware traffic, extract meaningful IOCs, and perform real world packet analysis using Wireshark and threat intelligence tools like VirusTotal.

Tools

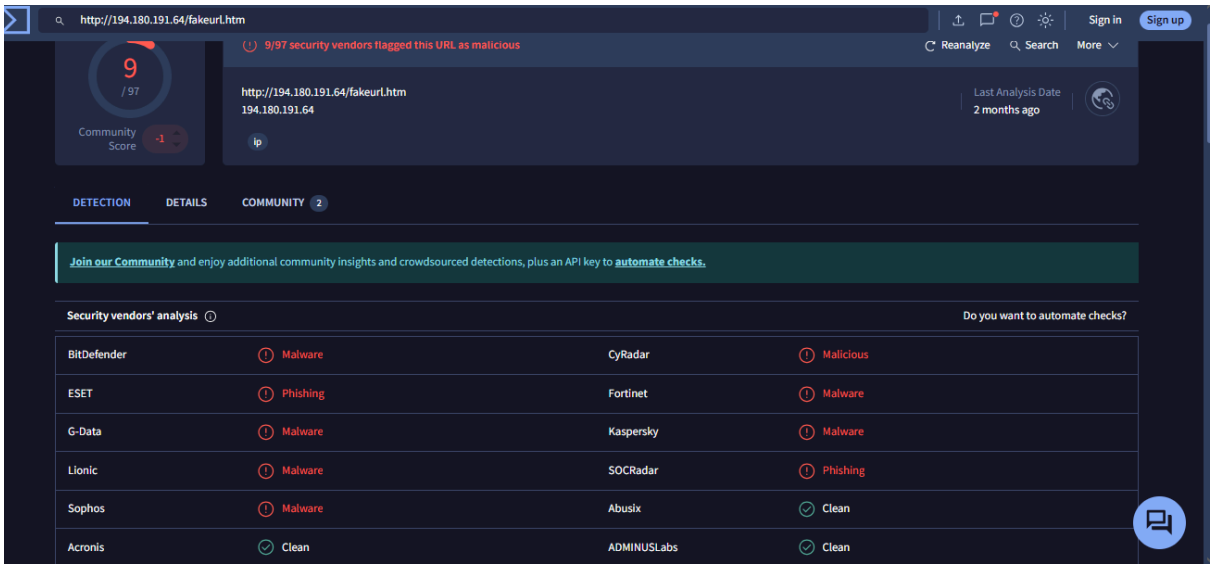
1. malware-traffic-analysis.net
Download PCAP files with known infections or attack traffic.
Study pretagged incidents (phishing, malware, C2 beacons).
Practice realworld analysis with expected outcomes.

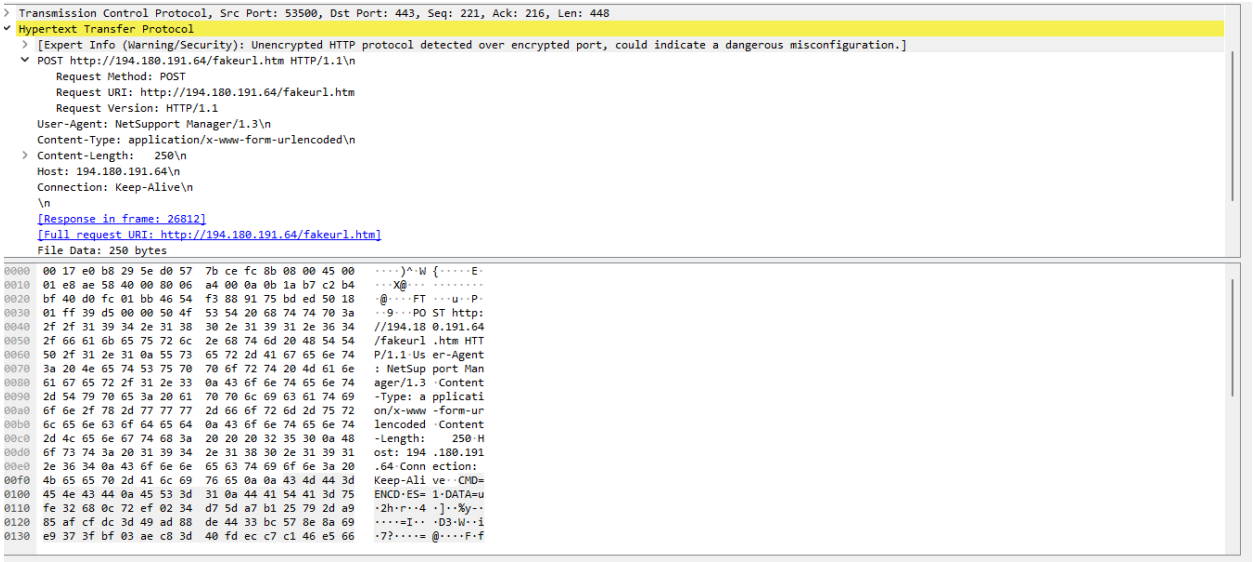
2. Wireshark Primary Packet Analyzer
Identify suspicious HTTP, DNS, TCP, TLS sessions
Reconstruct payloads, downloads, or command-and-control (C2) behavior

3. IP Lookup Tools (e.g. ipinfo.io, abuseipdb.com, virustotal.com, viewdns.info)
Look up source/destination IPs seen in traffic
Identify hosting providers, countries, ASNs
Check if the IP/domain is on a known blacklist
See passive DNS (other domains tied to the same IP)

Pictures


ip.addr == 194.180.191.64
Time Source Destination Protocol Lengtl Info
.8 2052.609467 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=8947 Win=131840 Len=0
.7 2052.336421 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
2 1992.450194 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=8713 Win=132096 Len=0
1 1992.182813 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
8 1932.277956 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=8479 Win=130816 Len=0
7 1932.027567 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
6 1872.233951 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=8245 Win=131072 Len=0
5 1871.966240 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
4 1812.175107 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=8011 Win=131328 Len=0
3 1811.908993 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
0 1752.001631 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=7777 Win=131584 Len=0
9 1751.749616 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
8 1691.957955 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=7543 Win=131840 Len=0
7 1691.690577 10.11.26.183 194.180.191.64 HTTP 288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
8 1631.898929 194.180.191.64 10.11.26.183 TCP 60 443 → 53362 [ACK] Seq=522 Ack=7309 Win=132096 Len=0


http://194.180.191.64/fakeurl.htm
Sign in
Sign up
9/97 security vendors flagged this URL as malicious
Reanalyze
Search
More
9
/ 97
Community Score
http://194.180.191.64/fakeurl.htm
194.180.191.64
ip
Last Analysis Date
2 months ago
DETECTION
DETAILS
COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
BitDefender Malware
CyRadar Malicious
ESET Phishing
Fortinet Malware
G-Data Malware
Kaspersky Malware
Lionic Malware
SOCRadar Phishing
Sophos Malware
Abusix Clean
Acronis Clean
ADMINUSLabs Clean


Transmission Control Protocol, Src Port: 53500, Dst Port: 443, Seq: 221, Ack: 216, Len: 448
Hypertext Transfer Protocol
[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
POST http://194.180.191.64/fakeurl.htm HTTP/1.1\n
Request Method: POST
Request URI: http://194.180.191.64/fakeurl.htm
Request Version: HTTP/1.1
User-Agent: NetSupport Manager/1.3\n
Content-Type: application/x-www-form-urlencoded\n
Content-Length: 250\n
Host: 194.180.191.64\n
Connection: Keep-Alive\n
\n
[Response in frame: 26812]
[Full request URI: http://194.180.191.64/fakeurl.htm]
File Data: 250 bytes
0000 00 17 e0 b8 29 5e d0 57 7b ce fc 8b 08 00 45 00
0010 01 e8 ae 58 40 00 80 06 a4 00 0a 0b 1a b7 c2 b4
0020 bf 40 d0 fc 01 bb 46 54 f3 88 91 75 bd ed 50 18
0030 01 ff 39 d5 00 00 50 4f 53 54 20 68 74 74 70 3a
0040 2f 2f 31 39 34 2e 31 38 30 2e 31 39 31 2e 36 34
0050 2f 66 61 6b 65 75 72 6c 2e 68 74 6d 20 48 54 54
0060 50 2f 31 2e 31 0a 55 73 65 72 2d 41 67 65 6e 74
0070 3a 20 4e 65 74 53 75 70 70 6f 72 74 20 4d 61 6e
0080 61 67 65 72 2f 31 2e 33 0a 43 6f 6e 74 65 6e 74
0090 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69
00a0 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72
00b0 6c 65 6e 63 6f 64 65 64 0a 43 6f 6e 74 65 6e 74
00c0 2d 4c 65 6e 67 74 68 3a 20 20 20 32 35 30 0a 48
00d0 6f 73 74 3a 20 31 39 34 2e 31 38 30 2e 31 39 31
00e0 2e 36 34 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
00f0 4b 65 65 70 2d 41 6c 69 76 65 0a 0a 43 4d 44 3d
0100 45 4e 43 44 0a 45 53 3d 31 0a 44 41 54 41 3d 75
0110 fe 32 68 0c 72 ef 02 34 d7 5d a7 b1 25 79 2d a9
0120 85 af cf dc 3d 49 ad 88 de 44 33 bc 57 8e 8a 69
0130 e9 37 3f bf 03 ae c8 3d 40 fd ec c7 c1 46 e5 66

Http

HTTP Request Summary
http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)"
Request method:post
Request url: http: / / 194.180.191.64/fakeurl.htm
User agent net support manager /1.3\n
Content type application /x-www-form-urlencoded\n
Host 194.180.191.64

IOCS

Destination IP	194.180.191.64
URL Path	/fakeurl.htm
Protocol	HTTP/1.1
Method	POST
Content Type	application/x-www-form-urlencoded
User Agent	NetSupport Manager /1.3
Host Header	194.180.191.64

Ip flagged on virus total for malware phishing and is malicious NetSupport Manager is a legitimate remote desktop tool, but threat actors often bundle it with droppers such as GuLoader, AgentTesla, or phishing attachment can be used for data theft Remote control C2 communication Surveillance and persistence

TCP

Source: 194.180.191.64
Destination: 10.11.26.183
Src port: 443
Dst port: 53362
Seq: 522
Ack: 10117
Len = 0 (no payload)

Source port 443 is used for HTTPS traffic. This makes sense because it appears right after suspicious HTTP requests automatically making it more suspicious. Malware often abuses ports like 443 to hide C2 traffic from firewalls.

The IP (194.180.191.64) is flagged as malicious on VirusTotal. The HTTP traffic tied to this IP was also marked as dangerous.

Destination port 53362 is suspicious because it's a high ephemeral port. Normally, these are temporarily assigned by client systems but repeated use of this specific port suggests hardcoded behavior or persistence.

These packets (including multiple ACKs with no payload) likely represent failed or blocked C2 communication. The combination of protocol misuse, IP reputation, and abnormal port behavior supports classifying this as malware related TCP activity.

In addition to this there are multiple tcp retransmissions from port 53362 to 443 with len=234 meaning there is payload in this packet this indicates that the host tried to send data but was blocked this further proves that the traffic is malware and intentional

Block the IP 194.180.191.64
Perimeter firewalls
Isolate the affected host
Scan for malware using EDR or antivirus tools
Notify Tier 2/3 analysts or Threat Hunt team