individual traffic analysis challenge 1

trevor achtermann

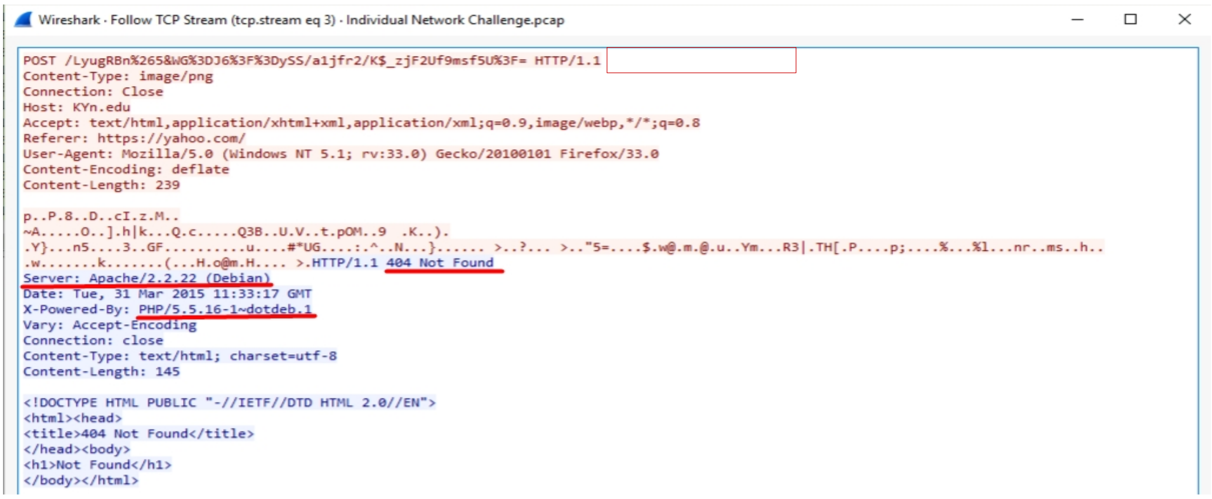
indicators and technical details

date \ time	identifier	comment
2015-03-31 11:32:18	185.91.175.64 GET /jsaxo8u/g39b2cx.exe From: 10.200.2.252	Host 10.200.2.252 downloaded suspicious file from IP 185.91.175.64
2015-03-31 11:33:29 2015-03-31 11:32:36 2015-03-31 11:33:18 2015-03-31 11:34:35 2015-03-31 11:32:19 2015-03-31 11:42:40	199.201.121.169 188.120.225.17 107.191.46.222 45.55.154.235 185.91.175.64 5.135.28.104	Suspicious IP's contacted by Host machine All connections occurred after the download
2015-03-31 11:34:00 2015-03-31 11:33:18	TCnu.YcVBf/ hLX%2C4AVZGlqL/zp2 Host: wxIAJN2OB.org LyugRBn%265&WG%3DJ6%3F%3DySS/ a1jfr2/K$_zjF2Uf9msf5U%3F= Host: Kyn.edu	Suspicious URL's contacted by Host machine

executive summary

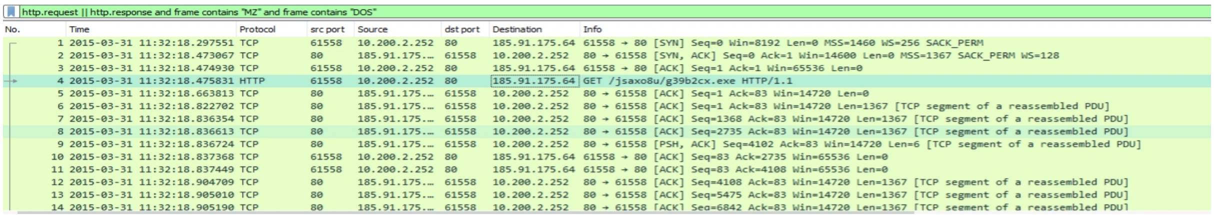
on march 31 2015 at 11:32:18 a suspicious executable [jsaxo8u/g39b2cx.exe] was downloaded by the host at 10.200.2.252. The file was served by IP 185.91.175.64 , an Apache server running on Debian Linux

technical summary



Wireshark · Follow TCP Stream (tcp.stream eq 3) · Individual Network Challenge.pcap

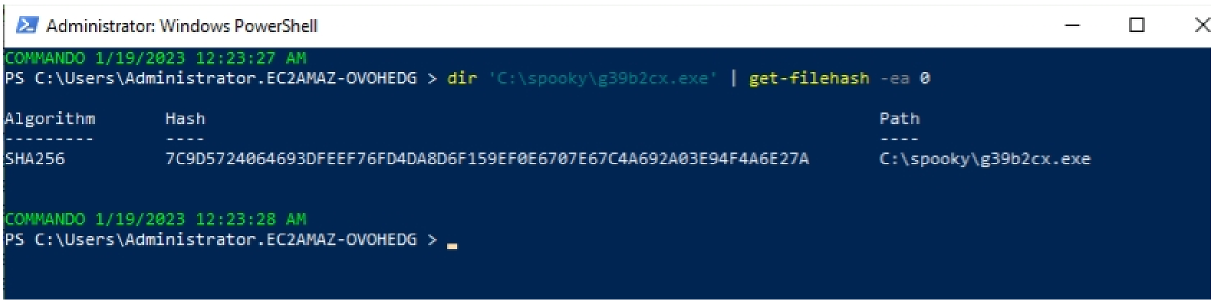
```
POST /LyugRBn%265&WG%3DJ6%3F%3DySS/a1jfr2/K$_zjF2Uf9msf5U%3F= HTTP/1.1
Content-Type: image/png
Connection: Close
Host: KYn.edu
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://yahoo.com/
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:33.0) Gecko/20100101 Firefox/33.0
Content-Encoding: deflate
Content-Length: 239

p..P.8..D..cI.z.M..
~A.....O..].h|k...Q.c.....Q3B..U.V..t.pOM..9  .K..).
.Y}...n5....3..GF..........u....#*UG....:.^..N...}...... >..?... >.."5=....$.w@.m.@.u..Ym...R3|.TH[.P....p;....%...%l...nr..ms..h..
.w.......k.......(...H.o@m.H.... >.HTTP/1.1 404 Not Found
Server: Apache/2.2.22 (Debian)
Date: Tue, 31 Mar 2015 11:33:17 GMT
X-Powered-By: PHP/5.5.16-1~dotdeb.1
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 145

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
</body></html>
```



http.request || http.response and frame contains "MZ" and frame contains "DOS"

```
No.  Time                        Protocol src port Source          dst port Destination    Info
   1 2015-03-31 11:32:18.297551 TCP      61558    10.200.2.252    80       185.91.175.64  61558 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
   2 2015-03-31 11:32:18.473067 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PERM WS=128
   3 2015-03-31 11:32:18.474930 TCP      61558    10.200.2.252    80       185.91.175.64  61558 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   4 2015-03-31 11:32:18.475831 HTTP     61558    10.200.2.252    80       185.91.175.64  GET /jsaxo8u/g39b2cx.exe HTTP/1.1
   5 2015-03-31 11:32:18.663813 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=1 Ack=83 Win=14720 Len=0
   6 2015-03-31 11:32:18.822702 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=1 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
   7 2015-03-31 11:32:18.836354 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=1368 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
   8 2015-03-31 11:32:18.836613 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=2735 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
   9 2015-03-31 11:32:18.836724 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [PSH, ACK] Seq=4102 Ack=83 Win=14720 Len=6 [TCP segment of a reassembled PDU]
  10 2015-03-31 11:32:18.837368 TCP      61558    10.200.2.252    80       185.91.175.64  61558 → 80 [ACK] Seq=83 Ack=2735 Win=65536 Len=0
  11 2015-03-31 11:32:18.837449 TCP      61558    10.200.2.252    80       185.91.175.64  61558 → 80 [ACK] Seq=83 Ack=4108 Win=65536 Len=0
  12 2015-03-31 11:32:18.904709 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=4108 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
  13 2015-03-31 11:32:18.905010 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=5475 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
  14 2015-03-31 11:32:18.905190 TCP      80       185.91.175.…    61558    10.200.2.252   80 → 61558 [ACK] Seq=6842 Ack=83 Win=14720 Len=1367 [TCP segment of a reassembled PDU]
```

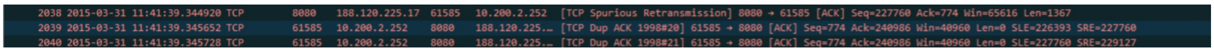
We used powershell to get the filehash on the suspicious exe and it has been determined to be a malicious trojan that makes changes at the registry level to infect \ control the infected machine. The risk to general operations is high, as the scope for this particular worm allows it to potentially breach the network beyond the local machine the file was downloaded to.



Administrator: Windows PowerShell

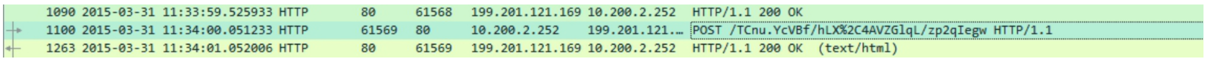
```
COMMANDO 1/19/2023 12:23:27 AM
PS C:\Users\Administrator.EC2AMAZ-OVOHEDG > dir 'C:\spooky\g39b2cx.exe' | get-filehash -ea 0

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          7C9D5724064693DFEEF76FD4DA8D6F159EF0E6707E67C4A692A03E94F4A6E27A       C:\spooky\g39b2cx.exe


COMMANDO 1/19/2023 12:23:28 AM
PS C:\Users\Administrator.EC2AMAZ-OVOHEDG > _
```

After the download, the host machine connected to a number of suspicious and previously unseen IP’s, as noted in the table above. This is concerning because these connections were not occuring before the download.



```
2038 2015-03-31 11:41:39.344920 TCP   8080   188.120.225.17  61585  10.200.2.252   [TCP Spurious Retransmission] 8080 → 61585 [ACK] Seq=227760 Ack=774 Win=65616 Len=1367
2039 2015-03-31 11:41:39.345652 TCP   61585  10.200.2.252    8080   188.120.225.…  [TCP Dup ACK 1998#20] 61585 → 8080 [ACK] Seq=774 Ack=240986 Win=40960 Len=0 SLE=226393 SRE=227760
2040 2015-03-31 11:41:39.345728 TCP   61585  10.200.2.252    8080   188.120.225.…  [TCP Dup ACK 1998#21] 61585 → 8080 [ACK] Seq=774 Ack=240986 Win=40960 Len=0 SLE=227760 SRE=229127
```

The host machine was also reaching out to a variety of suspicious URL’s after the downlaod event, which we have some examples of both in the ITD table as well as in the image below



```
1090 2015-03-31 11:33:59.525933 HTTP   80     61568  199.201.121.169 10.200.2.252   HTTP/1.1 200 OK
1100 2015-03-31 11:34:00.051233 HTTP   61569  80     10.200.2.252    199.201.121.…  POST /TCnu.YcVBf/hLX%2C4AVZGlqL/zp2qIegw HTTP/1.1
1263 2015-03-31 11:34:01.052006 HTTP   80     61569  199.201.121.169 10.200.2.252   HTTP/1.1 200 OK  (text/html)
```

We found these to be suspicious due to the random character strings for both the url and the domain that it is hosted on.

findings and analysis

display_filter	output
Http.user_agent	Displays frames contianing user agent strings in HTTP traffic
http.request || http.response and frame contains "MZ" and frame contains "DOS"	Shows all GET requests and targets frames containing MZ and DOS
Dir ‘C:\spooky\g39b2cx.exe’ | get-filehash -ea 0	Gets the SHA256 hash of the file specified and tells powershell to continue processing and avoid any errors

remediation and recommendation

After review of the traffic assigned, we suggest implementing new company policy to prevent users from encountering these threats through training on proper internet usage and hygiene, as well as endpoint monitoring / intrusion detection protocol in the event any infected machines are used to gain further insight into our network.

We also recommend a forensic investigation of IP 10.200.2.252 as it was the first point of contact for the trojan and could potentially be used to stop further access or even to initiate a response.