Set1.pcap

1. 678 packets
2. File transfer Protocol which is a TCP protocol
3. The data is transferred in plain text and usernames and password or any other sensitive information could be disclosed.
4. SFTP(Secure File Transfer Protocol) which does encryption before sending data
5. 192.168.1.8:21
6. Username: jfurgala and password: SophieDanielpourWantsToSueMe
7. 5
8. WTFGirl.jpg , WTFGirl12.jpg , WTFGirl3.jpg , eevee.md , WTFGirl4.jpg
9. Files




WTFGirl.jpg WTFGirl2.jpg WTFGirl3.jpg WTFGirl4.jpg

Note: File eevee.md is attached.

Set2.pcap

10. 76409
11. 2
12. Sets of data:

- [USER: wbgapp31216 PASS: Q827wO6656!nW99_a1 ; 176.58.103.138:80 ; Net-name: LINODE-UK; Https]
- [USER: ventas@wekiguatemala.com.gt PASS: "$Alesgt1.1" ; 74.220.219.141:143; Net-name: BlueHostNetwork-2; domain: https://www.arin.net/; IMAP]

13. All of the users are legitimate i.e. no login/failed access was seen.
14. IP addresses and Host Names

Hosts

#

86 entries.

17.178.96.59 apple.com

169.46.12.72 api.south.kontagent.net

17.253.23.207 cdn-icloud-content.g.aaplimg.com

72.21.206.140 s.amazon-adsystem.com

104.68.97.2 e12930.ksd.akamaiedge.net

52.45.146.29 gregord-elb-298228113.us-east-1.elb.amazonaws.com

169.46.12.74 api.south.kontagent.net

72.21.91.113 cs84.wac.edgecastcdn.net

87.240.165.81 api.vk.com

192.31.80.30 d.gtld-servers.NET

151.101.1.181 prod.taboola.map.fastly.net

151.101.65.181 prod.taboola.map.fastly.net

151.101.129.181 prod.taboola.map.fastly.net

17.142.160.59 apple.com

151.101.193.181 prod.taboola.map.fastly.net

216.115.100.123 fd-geoycpi-uno.gycpi.b.yahoodns.net

104.41.208.54 production-roundrobin.skype-registar.akadns.net

23.203.204.8 e673.e9.akamaiedge.net

172.217.11.170 googleapis.l.google.com

216.115.100.124 fd-geoycpi-uno.gycpi.b.yahoodns.net

23.215.130.192 a1089.d.akamai.net

23.45.86.46 e4478.a.akamaiedge.net

172.217.4.129 googlehosted.l.googleusercontent.com

23.5.251.27 e8218.dscb1.akamaiedge.net

31.13.77.49 mmx-ds.cdn.whatsapp.net

184.24.107.198 e1879.e7.akamaiedge.net

169.46.12.79 api.south.kontagent.net

54.239.17.86 completion.amazon.com

17.125.252.5 sp11p03sa.guzzoni-apple.com.akadns.net

64.4.54.254 cy2.vortex.data.microsoft.com.akadns.net

172.217.11.66 pagead46.l.doubleclick.net

95.213.11.139 api.vk.com

172.217.4.131 gstaticadssl.l.google.com

52.94.224.25 mads.amazon.com

172.217.5.202 googleapis.l.google.com

172.217.5.74 googleapis.l.google.com

115.233.212.147 ps.cname2.igexin.com

104.244.46.231 wildcard.twimg.com

104.244.46.39 wildcard.twimg.com

107.23.77.203 gregord-elb-298228113.us-east-1.elb.amazonaws.com

34.201.64.150 lc80.dsr.livefyre.com

104.27.183.94 warl0ck.gam3z.com

169.46.12.84 api.south.kontagent.net

74.125.28.188 mobile-gtalk.l.google.com

17.139.246.5 mt-ingestion-service-pv.itunes-apple.com.akadns.net

216.58.193.202 googleapis.l.google.com

17.173.66.102 p51-buy.itunes-apple.com.akadns.net

17.139.246.6 mt-ingestion-service-pv.itunes-apple.com.akadns.net

192.33.14.30 b.gtld-servers.NET

208.71.44.30 fd-geoycpi-uno.gycpi.b.yahoodns.net

17.172.224.47 apple.com

17.139.246.7 mt-ingestion-service-pv.itunes-apple.com.akadns.net

208.71.44.31 fd-geoycpi-uno.gycpi.b.yahoodns.net

218.205.81.155 ps.cname2.igexin.com

165.227.0.37 vtfbctf.com

169.46.12.66 api.south.kontagent.net

172.217.11.74 googleapis.l.google.com

17.56.160.246 api.smoot-apple.com.akadns.net

169.46.12.88 api.south.kontagent.net

23.253.220.65 schemaverse.marcneuwirth.com

192.5.6.30 a.gtld-servers.NET

23.203.233.109 e2546.dsce4.akamaiedge.net

169.46.12.68 api.south.kontagent.net

216.58.216.46 connectivitycheck.android.com

192.12.94.30 e.gtld-servers.NET

104.27.182.94 warl0ck.gam3z.com

216.58.216.4 www.google.com

23.203.180.198 e6858.dsce9.akamaiedge.net

169.46.12.69 api.south.kontagent.net

23.215.130.184 a1089.d.akamai.net

172.217.4.142 clients.l.google.com

115.231.99.203 ps.cname2.igexin.com

169.46.12.70 api.south.kontagent.net

192.26.92.30 c.gtld-servers.NET

17.253.23.205 cdn-icloud-content.g.aaplimg.com

104.244.46.71 wildcard.twimg.com

169.46.12.93 api.south.kontagent.net

2001:500:856e::30 d.gtld-servers.NET

2001:503:a83e::2:30 a.gtld-servers.NET

2400:cb00:2048:1::681b:b65e warl0ck.gam3z.com

2001:503:83eb::30 c.gtld-servers.NET

2607:f8b0:4007:804::2002 pagead46.l.doubleclick.net

2400:cb00:2048:1::681b:b75e warl0ck.gam3z.com

2607:f8b0:4007:809::2004 www.google.com

2607:f8b0:4007:800::2003 ssl.gstatic.com

2001:503:231d::2:30 b.gtld-servers.NET

Set3.pcap

15. 3
16. Sets of data:

- [USER: brodgers PASS: TheyPlayedWithGreatCharacter ; 130.64.23.35:80 ; Https; www.eecs.tufts.edu/~cgregg/grades/]
- [USER: dmoyes PASS: IAmAFootballGenius ; 130.64.23.35:80 ; Https; www.eecs.tufts.edu/~cgregg/grades/]
- [USER: aoursler PASS: Id10tExpert ; 130.64.23.35:80 ; Https; www.eecs.tufts.edu/~cgregg/grades/]

17. None of the three plain text username-address pairs were legitimate.
18. I used Ettercap to find the plain text username-password pairs and then selected the unique ones if there were any repeats.
19. Since all the login attempts were done using HTTP protocol so I filtered out the packets containing get request using http.request.method == “GET”. This way I was able to get three packets each containing the username-password credentials and the user’s attempt to login. These packets also contained the location of the corresponding response packet. For each of the user attempt, I opened the corresponding packet which contained the response of that login attempt and found out where it was 401 or a success 200 Ok login.

Set4.pcap

20. The next location of Carmen Sandiego is going to be Africa as mentioned in the lyrics of song the song in a file named ‘blessed’ which is mp4. I determined the information by exporting and checking each http object in set4.pcap and the mp4 file came out to be something containing the next whereabout of Carmen Sandiego.
21. The best way for these people to defend against sniffing is to use a VPN which is a virtual private network and ensure that all the data communication is encrypted. In addition to the use of VPN, a pro tip would be that these people should avoid using HTTP websites and rather prefer to use HTTPS websites which are a lot more secure due to SSL. HTTPS websites ensures data is encrypted when it is sent so that any intruder is not able to see the meaningful content in the data when the data is getting transferred.