**set0.pcap**

1. Microsoft a0:85:fc:de:ab:f5

**set1.pcap**

1. File Transfer Protocol (FTP)
2. FTP is an unencrypted data transfer protocol
3. Secure File Transfer Protocol (SFTP)
4. Destination Server IP: 192.168.1.8
5. Username: penaldo Password: MessiIsTheGoat
6. 5,997 packet files from PC to Server
7. See attached

**set2.pcap**

1. There are 5 total (4 unique) username-password pairs
2. Username-Password pairs:

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | **Password** | **Protocol** | **Legitimate** |
| dmoyes | TheyPlayedWithGreatCharacter | HTTP basic auth | No |
| bwonderchimp | Bloke! | HTTP basic auth | No |
| pret | $string76Minimal | HTTP basic auth | No |
| brodgers | TheyPlayedWithGreatCharacter | HTTP basic auth | Yes |
| brodgers | TheyPlayedWithGreatCharacter | HTTP basic auth | Yes |

1. 2/5 are legitimate credentials, as the others were unauthorized credentials

**set3.pcap**

1. 76,409 packets in the set
2. 2 username-password pairs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Username** | **Password** | **Protocol** | **IP Address** | **Port** |
| [ventas@wekiguatemala.com.gt](mailto:ventas@wekiguatemala.com.gt) | $Alesgt1.1 | IMAP | 10.121.12.153 | 37425 |
| wbgapp31216 | Q827wO6656!nW99\_a1 | HTTP | 10.144.31.242 | 53436 |

1. This user’s credentials are legitimate as given by access to the server when following the TCP stream

A screenshot of a computer

Description automatically generated

1. IP Addresses with domain names

172.217.4.142 clients.l.google.com

172.217.5.74 googleapis.l.google.com

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

169.46.12.69 api.south.kontagent.net

115.233.212.147 ps.cname2.igexin.com

216.58.216.46 connectivitycheck.android.com

104.244.46.231 wildcard.twimg.com

72.21.206.140 s.amazon-adsystem.com

54.239.17.86 completion.amazon.com

169.46.12.88 api.south.kontagent.net

151.101.1.181 prod.taboola.map.fastly.net

169.46.12.74 api.south.kontagent.net

23.203.180.198 e6858.dsce9.akamaiedge.net

216.58.216.4 www.google.com

192.12.94.30 e.gtld-servers.NET

23.203.204.8 e673.e9.akamaiedge.net

192.31.80.30 d.gtld-servers.NET

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

184.24.107.198 e1879.e7.akamaiedge.net

23.215.130.184 a1089.d.akamai.net

23.253.220.65 schemaverse.marcneuwirth.com

169.46.12.93 api.south.kontagent.net

151.101.65.181 prod.taboola.map.fastly.net

169.46.12.79 api.south.kontagent.net

31.13.77.49 mmx-ds.cdn.whatsapp.net

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

172.217.4.131 gstaticadssl.l.google.com

34.201.64.150 lc80.dsr.livefyre.com

104.244.46.39 wildcard.twimg.com

23.45.86.46 e4478.a.akamaiedge.net

172.217.11.66 pagead46.l.doubleclick.net

169.46.12.72 api.south.kontagent.net

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

151.101.129.181 prod.taboola.map.fastly.net

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

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

169.46.12.84 api.south.kontagent.net

172.217.4.129 googlehosted.l.googleusercontent.com

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

169.46.12.70 api.south.kontagent.net

151.101.193.181 prod.taboola.map.fastly.net

172.217.5.202 googleapis.l.google.com

192.26.92.30 c.gtld-servers.NET

17.172.224.47 apple.com

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

216.58.193.202 googleapis.l.google.com

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

115.231.99.203 ps.cname2.igexin.com

192.5.6.30 a.gtld-servers.NET

23.5.251.27 e8218.dscb1.akamaiedge.net

104.27.183.94 warl0ck.gam3z.com

172.217.11.170 googleapis.l.google.com

17.142.160.59 apple.com

104.27.182.94 warl0ck.gam3z.com

169.46.12.68 api.south.kontagent.net

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

192.33.14.30 b.gtld-servers.NET

23.215.130.192 a1089.d.akamai.net

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

172.217.11.74 googleapis.l.google.com

104.68.97.2 e12930.ksd.akamaiedge.net

169.46.12.66 api.south.kontagent.net

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

72.21.91.113 cs84.wac.edgecastcdn.net

17.178.96.59 apple.com

165.227.0.37 vtfbctf.com

218.205.81.155 ps.cname2.igexin.com

87.240.165.81 api.vk.com

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

23.203.233.109 e2546.dsce4.akamaiedge.net

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

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

74.125.28.188 mobile-gtalk.l.google.com

104.244.46.71 wildcard.twimg.com

52.94.224.25 mads.amazon.com

95.213.11.139 api.vk.com

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

1. Don’t use unsecure protocols as done here (FTP, HTTP, IMAP) that expose credentials in plaintext, making them vulnerable to interception. Use instead secure protocols and/or encrypted passwords.