Pikabot / Pikabot_06.12.2023.txt

pr0xylife Update Pikabot_06.12.2023.txt 6b07f26 · last year History

Code Blame 73 lines (48 loc) · 2.75 KB Raw

```
06.12.2023 | Pikabot | TA577 | 1.1.17-ghost

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

.url https://theonlinepharmacy.ae/equ/?1337
.zip 12b416d6a44e53ce1ddf9f5477281a38fedf8f72fdbc1a9aa2286dd139272f65
.msi 6bb4cdbaef03b732a93559a58173e7f16b29bfb159a1065fae9185000ff23b4b
.dll 70b12617dbbaf60b6a169797cc016eda12b0b18766b6ae48b469b0aed3e73892

.html 1aaf8dfa21057425dcc7a982aba8b0f9a3453e8d3d0eb2274023abfb9a89d8fb (attack chain #2

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

Code Signing Certificate

Organisation:   SOFT BLANKET LTD
Issuer: SSL.com EV Code Signing Intermediate CA RSA R3
Algorithm:      sha256WithRSAEncryption
Valid from:     2023-11-03T20:27:04Z
Valid to:       2024-11-02T20:27:04Z
Serial number:   3aee1200d91ed3572e26a5cf6100d6f1
Thumbprint Algorithm:   SHA256
Thumbprint:      38165af7ef4861e8efdb51657404facee375cf33f50a18f213f104b2e661df57

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

url > zip > msi > dll

msiexec.exe /I C:\Users\Admin\AppData\Local\Temp\Oic.msi

msiexec.exe /V

srtasks.exe ExecuteScopeRestorePoint /WaitForRestorePoint:2

MsiExec.exe -Embedding C387CF83404CAD01F5ACC1D4222D4B0D

rundll32.exe "C:\Windows\Installer\MSI9153.tmp",zzzzInvokeManagedCustomActionOutOfProc


rundll32.exe C:\Users\Admin\AppData\Local\Temp\tmp96E1.dll,Enter

SearchFilterHost.exe

vssvc.exe

**********************************************
HTML attachment url

https://cecvillamaria.org/ae/

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

c2's

154.61.75.156:2078
207.148.103.233:2967
```

Qakbot_BB29_Pikabot_22.05.202...

Qakbot_BB29_Pikabot_23.05.202...

```
57      78.141.222.198:13786
58      210.243.8.247:23399
59      45.63.26.148:2224
60      65.20.77.81:5242
61      154.221.30.136:13724
62
63      HTTPS Checking Traffic
64
65      https://154.61.75.156:2078/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaerationSe
66      https://207.148.103.233:2967/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaeration
67      https://78.141.222.198:13786/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaeration
68      https://210.243.8.247:23399/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaerationS
69      https://45.63.26.148:2224/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaerationSee
70      https://65.20.77.81:5242/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaerationSeet
71      https://154.221.30.136:13724/hostless/6lwGSLU3l36WZlbmu?thrombus=cDXuTGQKb3l&deaeration
72
73      ********************************************
```