Strings And FLOSS (static string Analysis)

Strings And FLOSS (static string Analysis)

It will Analyze the binary And Show us all the **strings** it can find in the binary

`strings` we can use this command for retriving strings in a binary

`floss` this is an better version of strings made by **fireeye** team.

`floss` can be run with the `-n` argument to specify your desired minimum string length. Sometimes, longer strings can be more useful to an analyst than your ***standard string of len(4)***.

For example : if I want to pull all strings of length 6 or greater, I can issue the following command

```
floss.exe -n 6 [malware_name.exe]
```

After running search for string which make sense like:

- .dll Files
- Powershell objects

- File Paths

```
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
1"1*1h1r1
2'3|3
5=6C6I6O6U6[6b6i6p6w6~6
8"8(8.848:8@8U8j8q8w8
909B9
:F:l:u:{:Y;y;
;F<O<T<g<{<
<#=(=<=F=
>A>K>T>]>r>{>
?!?'?-?3?9???E?K?Q?W?]?c?i?o?u?{?
2N2X2
2)373
4B4M4
5)5@5H5b5
10141D4H4P4
8,808

-----------------------------
| FLOSS UTF-16LE STRINGS (8) |
-----------------------------
jjjj
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
open

--------------------------
| FLOSS STACK STRINGS (1) |
--------------------------
ineIGenu

--------------------------
| FLOSS TIGHT STRINGS (0) |
--------------------------

-----------------------------
| FLOSS DECODED STRINGS (0) |
-----------------------------
```

Floss static Unicode strings Section will give most of the interesting strings.

```
-------------------------------
| FLOSS UTF-16LE STRINGS (8) |
-------------------------------
jjjj
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
http://ssl-6582datamanager.helpdeskbros.local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
http://huskyhacks.dev
ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
open
```

Be Aware !!!!

These String Can be Thrown Intetionally To trick Us .