statistic.exe

Hash Values:

Using HashMyFiles,

MD5 : c601360ddcef92172c5381947d1d4598

SHA1: 1225c32ebd5aeb03e2204a4b7b7b371c91eb559a

SHA256: 74533fd0e75cb96032d71463946ff6c3822e3c3a7fb72d79703108eeaf393983

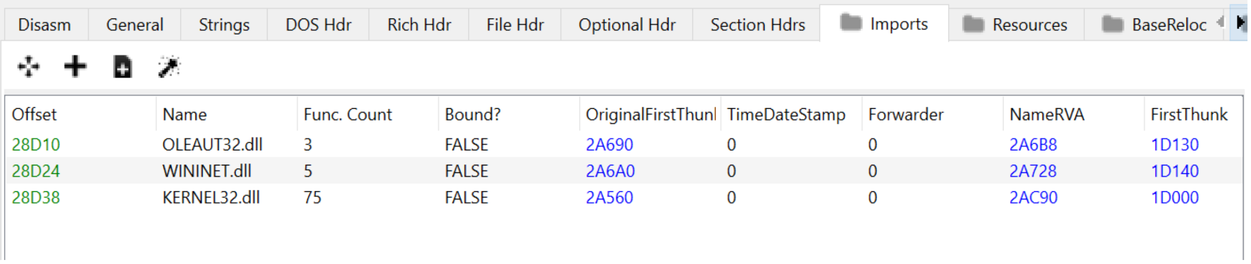
File Type:

Using Detect it Easy,

PE32, compliled using Microsoft Visual C/C++(2019)

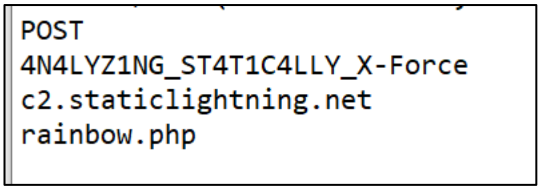
Due to the file being a PE32, the PE-bear tool will be used for more information.

Under the Imports tab, the Windows API functions the sample will use are listed:



Offset	Name	Func. Count	Bound?	OriginalFirstThunl	TimeDateStamp	Forwarder	NameRVA	FirstThunk
28D10	OLEAUT32.dll	3	FALSE	2A690	0	0	2A6B8	1D130
28D24	WININET.dll	5	FALSE	2A6A0	0	0	2A728	1D140
28D38	KERNEL32.dll	75	FALSE	2A560	0	0	2AC90	1D000

Notable Strings from Strings Tool:



```
POST
4N4LYZ1NG_ST4T1C4LLY_X-Force
c2.staticlightning.net
rainbow.php
```

Flag : 4N4LYZ1NG_ST4T1C4LLY_X-Force