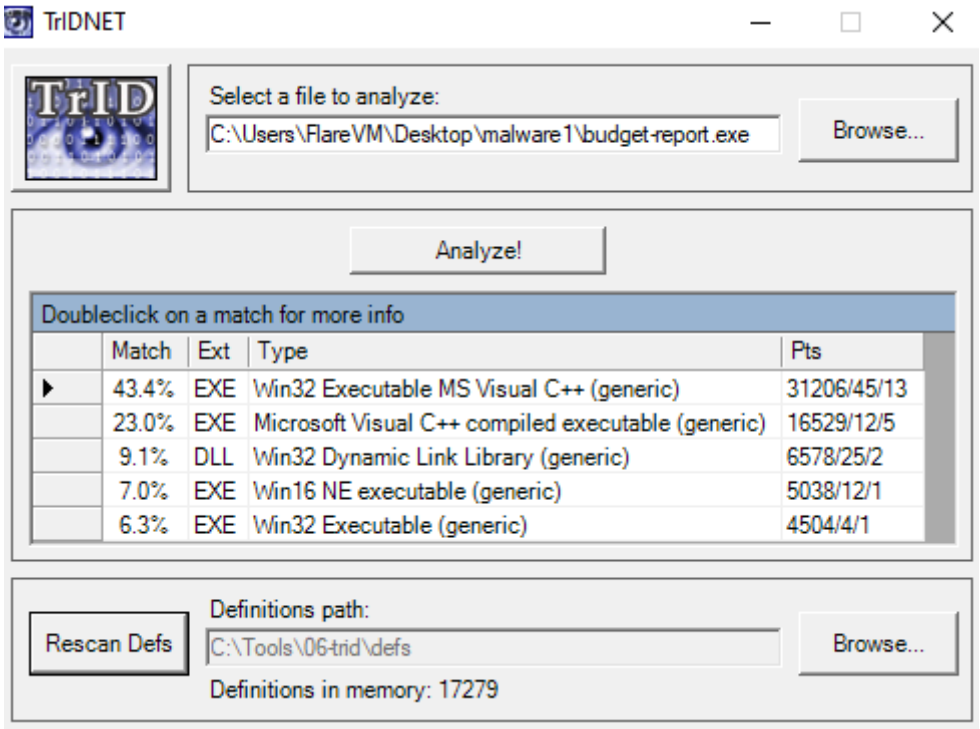
Here is my write-up for the file “budget-report”. The objective here is to find indicators of compromise/evidence that we are dealing with a malicious file.

Static Analysis

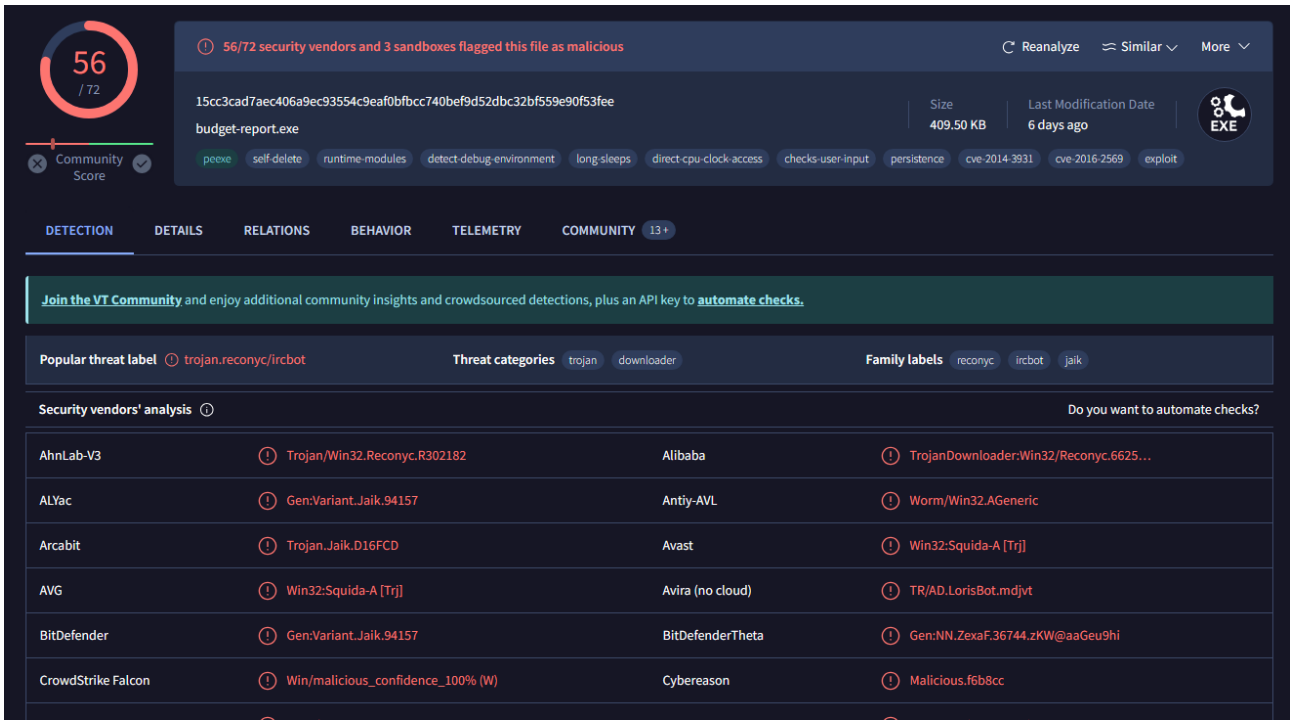
The first suspicious fact is that the file has a .pdf icon but it is really a .exe file.

Name	Date modified	Type	Size
budget-report.exe	07/02/2018 07:53	Application	410 KB

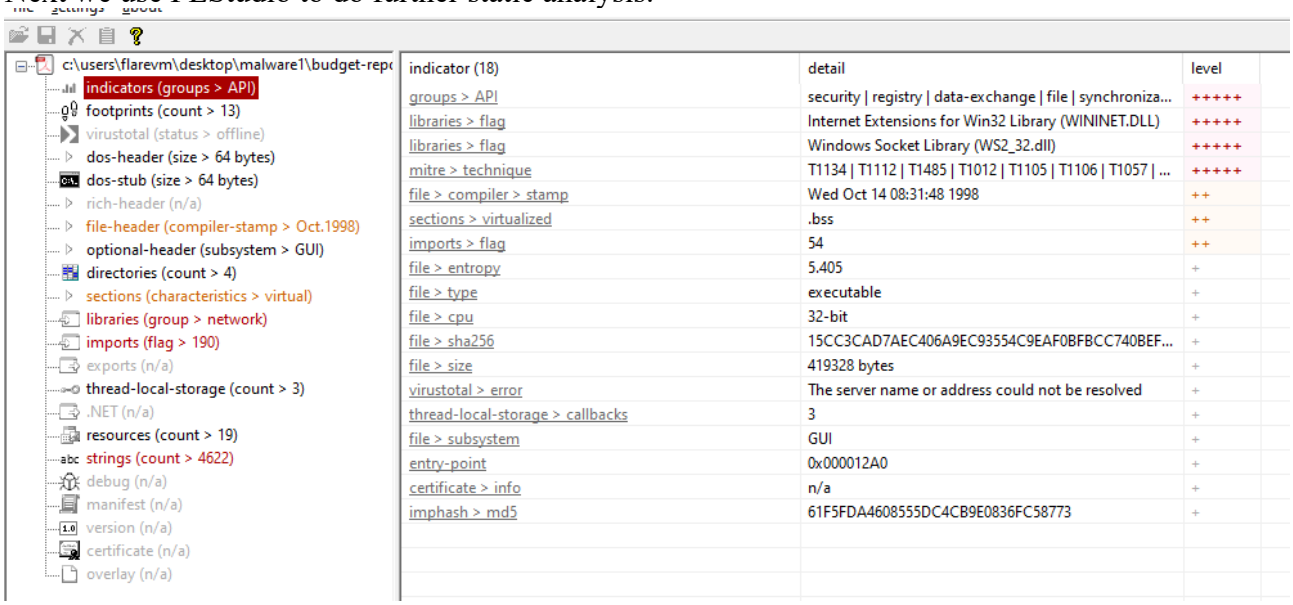
TrIDNET confirms it:



After confirming that we are dealing with an .exe file, the next step is to perform hash analysis. When a hash is created and tested in virustotal the following result is given, a 56/72 result on virustotal for Trojan.



Next we use PEStudio to do further static analysis.



PEStudio finds multiple high level signs of malicious code, one of which is registry which makes me believe the malware is trying to achieve persistance by adjusting the registry of the host system.

When we look at the strings tab you can see the values "RegSetValueEx" which proves that the malware is trying to be persistant by creating or "setting" a value in the registry. We see more strange values such as ShellExecute, DeleteFile, WriteFile, WSAstartup and many more.

encoding (2)	size (bytes)	location	flag (79)	label (292)	group (17)	technique (13)	value
ascii	10	section:.idata	x	import	file	T1105 | Remote File Copy	MoveFileEx
ascii	21	section:.rdata	x	-	network	-	ObtainUserAgentString
ascii	13	section:.idata	x	import	data-exchange	T1115 | Clipboard Data	OpenClipboard
ascii	11	section:.idata	x	import	execution	T1055 | Process Injection	OpenProcess
ascii	16	section:.idata	x	import	security	T1134 | Access Token Mani...	OpenProcessToken
ascii	14	section:.idata	x	import	execution	T1057 | Process Discovery	Process32First
ascii	13	section:.idata	x	import	execution	T1057 | Process Discovery	Process32Next
ascii	14	section:.idata	x	import	registry	T1112 | Modify Registry	RegCreateKeyEx
ascii	14	section:.idata	x	import	registry	T1485 | Data Destruction	RegDeleteValue
ascii	11	section:.idata	x	import	registry	T1112 | Modify Registry	RegFlushKey
ascii	13	section:.idata	x	import	registry	T1112 | Modify Registry	RegSetValueEx
ascii	13	section:.rdata	x	-	network	-	RpcStringFree
ascii	16	section:.idata	x	import	data-exchange	T1115 | Clipboard Data	SetClipboardData
ascii	15	section:.idata	x	import	security	T1134 | Access Token Mani...	SetEntriesInAcl
ascii	17	section:.idata	x	import	file	-	SetFileAttributes
ascii	23	section:.idata	x	import	security	T1134 | Access Token Mani...	SetKernelObjectSecurity
ascii	20	section:.idata	x	import	security	T1134 | Access Token Mani...	SetNamedSecurityInfo
ascii	22	section:.idata	x	import	execution	-	SetProcessAffinityMask
ascii	16	section:.idata	x	import	execution	T1055 | Process Injection	SetThreadContext
ascii	12	section:.idata	x	import	execution	T1106 | Execution through...	ShellExecute
ascii	13	section:.rdata	x	-	-	-	Shell_TrayWnd

So far we have some important IoC's from our static analysis. Lets continue to dynamic analysis and run this malware to see what it does to our system.

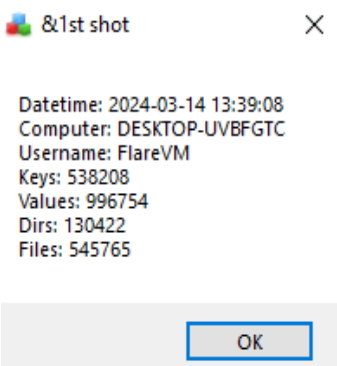
Dynamic Analysis

I setup Fakenet, Procmon and Regshot to capture all necessary traffic for dynamic analysis.

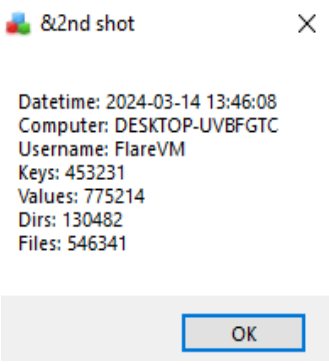
When the file is executed it dissapears immediately, which makes me believes that it removes itself while creating another file (duplicate) of itself somewhere else.

When we compare the first Regshot shot with the second shot we notice some differences in the result.

Regshot 1st shot



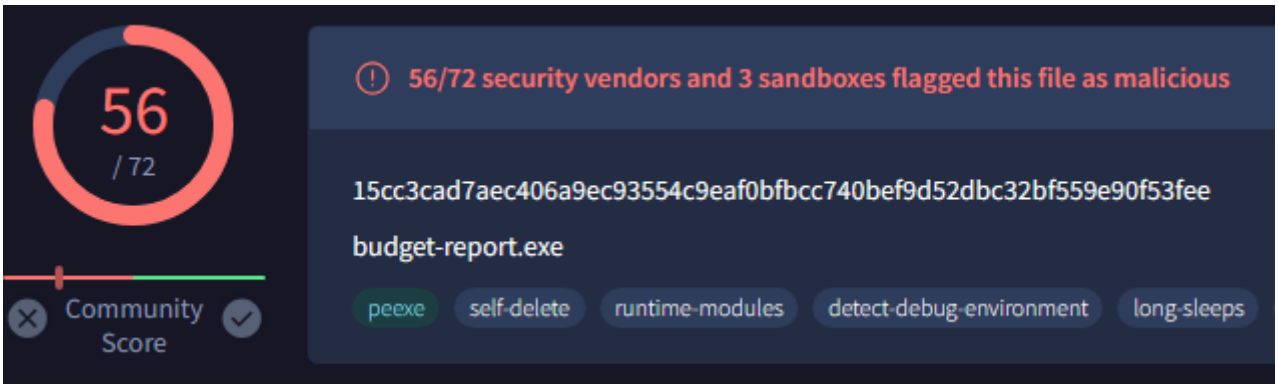
Regshot 2nd shot



When we compare the differences in results in a .txt file we notice that some values were added.

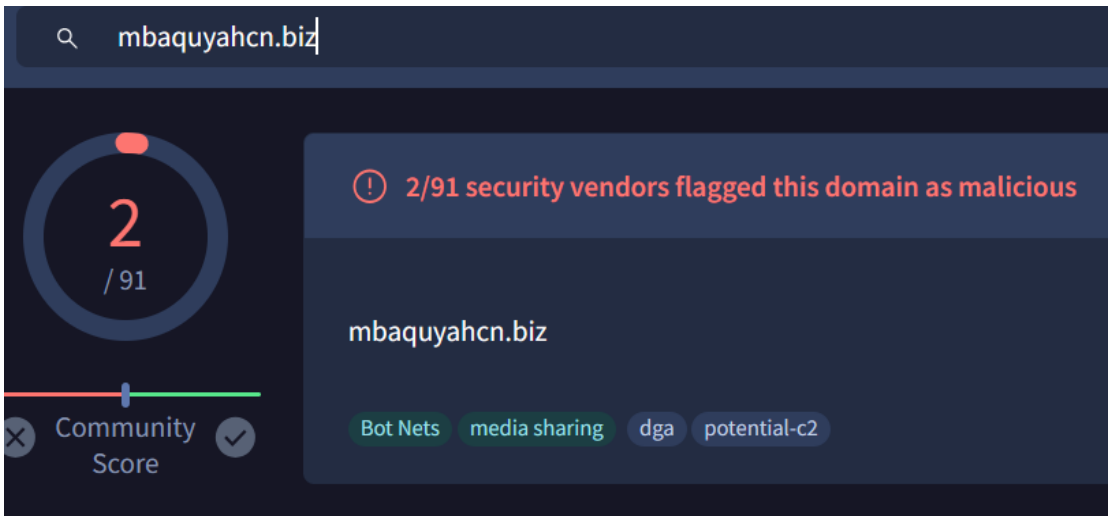
```
\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*12648430: ""C:\Users\FlareVM\AppData\Roaming\12648430\smss.exe""
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\FlareVM\Desktop\malware1\budget-report.exe: 53 41 43 50 01 00 00
\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\FlareVM\Desktop\malware1\budget-report.exe.FriendlyAppName: "budget-report.exe"
_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\FlareVM\Desktop\malware1\budget-report.exe.FriendlyAppName: "budget-report.exe"
```

When we navigate to this new file and test it in virustotal we get the exact same score as the original file, a 56/72. Virustotal also recognizes this new smss.exe file as the original budget-report.exe. We noticed before that the original file got deleted when it was executed, it appears that this new file is the copy.

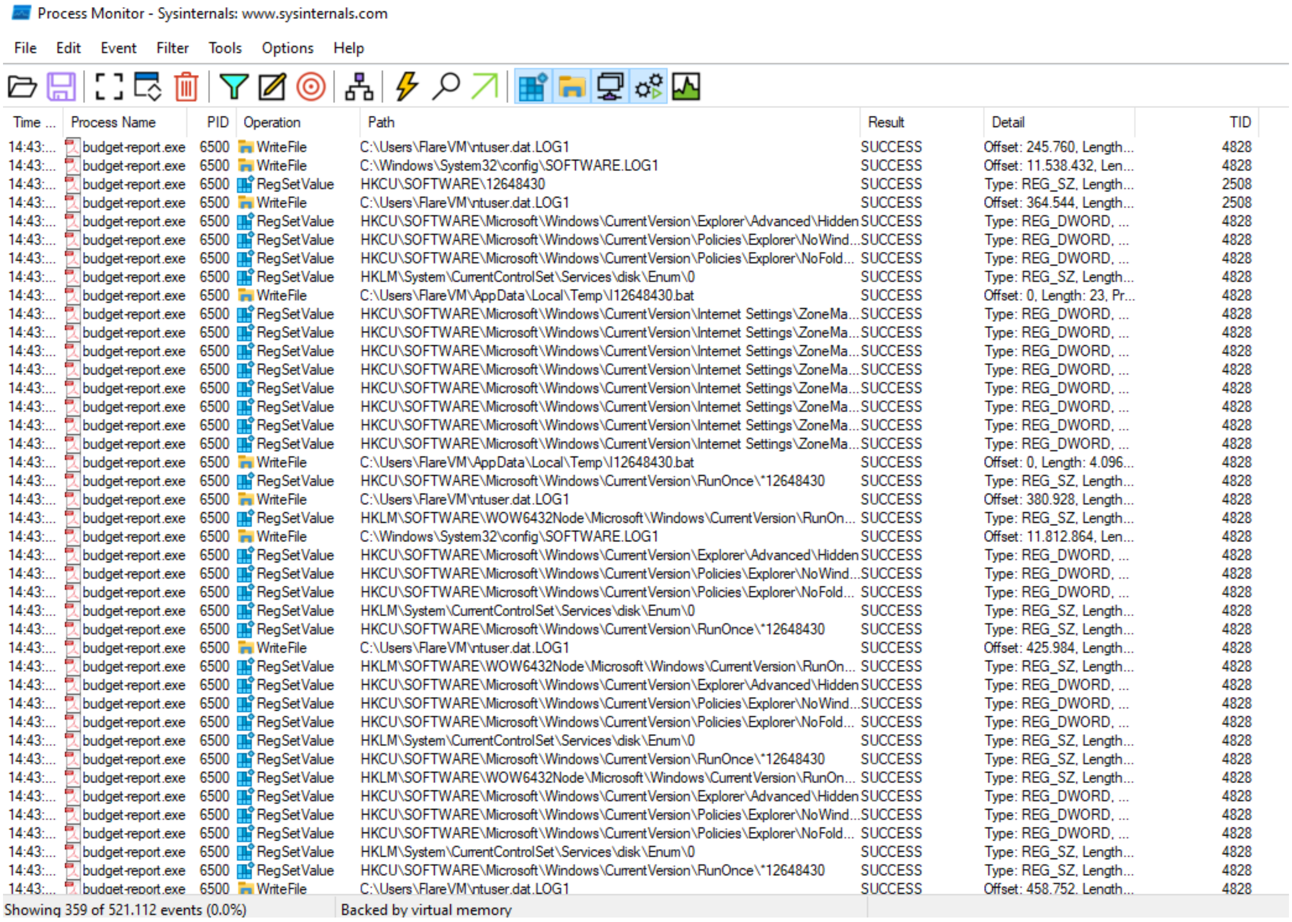


Fakenet created a .pcap file to be analyzed in wireshark.
When we filter on http traffic we notice the following.

Looks like it is trying to send something to an unknown adress ending with .biz, when we search this adress in virustotal we get a 2/92 result for malware, which is another IoC.



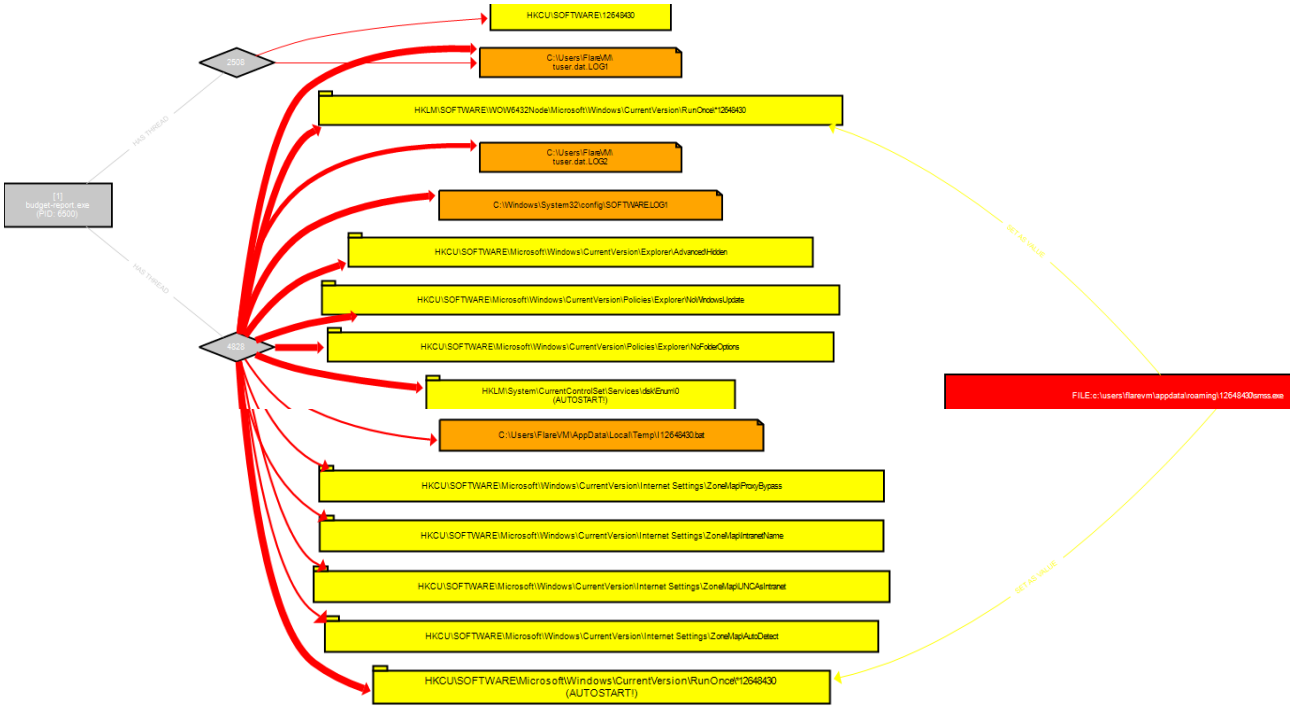
When we filter Procmon to only show results correlated with the malicious file we get the following results. We notice the many WriteFile and RegSetValue actions which are more IoC's. At this point I am very interested in the flow of actions that the malicious file took so I saved this Procmon result as a .csv and opened it in Procdot for a logical flow of actions.



Time ...	Process Name	PID	Operation	Path	Result	Detail	TID
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\ntuser.dat.LOG1	SUCCESS	Offset: 245.760, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Windows\System32\config\SOFTWARE.LOG1	SUCCESS	Offset: 11.538.432, Len...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\12648430	SUCCESS	Type: REG_SZ, Length...	2508
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\ntuser.dat.LOG1	SUCCESS	Offset: 364.544, Length...	2508
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWind...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFold...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\System\CurrentControlSet\Services\disk\Enum\0	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\AppData\Local\Temp\I12648430.bat	SUCCESS	Offset: 0, Length: 23, Pr...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMa...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\AppData\Local\Temp\I12648430.bat	SUCCESS	Offset: 0, Length: 4.096...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*12648430	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\ntuser.dat.LOG1	SUCCESS	Offset: 380.928, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOn...	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Windows\System32\config\SOFTWARE.LOG1	SUCCESS	Offset: 11.812.864, Len...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWind...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFold...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\System\CurrentControlSet\Services\disk\Enum\0	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*12648430	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\ntuser.dat.LOG1	SUCCESS	Offset: 425.984, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOn...	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWind...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFold...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\System\CurrentControlSet\Services\disk\Enum\0	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*12648430	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOn...	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWind...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFold...	SUCCESS	Type: REG_DWORD, ...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKLM\System\CurrentControlSet\Services\disk\Enum\0	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*12648430	SUCCESS	Type: REG_SZ, Length...	4828
14:43:...	budget-report.exe	6500	WriteFile	C:\Users\FlareVM\ntuser.dat.LOG1	SUCCESS	Offset: 458.752, Length...	4828

Showing 359 of 521.112 events (0.0%) Backed by virtual memory

Here is a logical flow of the actions that the malware has taken. We see the starting point of the malware in the gray box on the left, it has a process which executives multiple actions regarding registry keys in the yellow middle section. Several files are created as logfiles, these are LOG1, LOG2 and SOFTWARELOG1, also a .bat file in the orange blocks. We notice there are multiple counts of creating persistance. The red box on the right is indeed the new file we checked earlier, smss.exe, this is also linked to an autostart for persistance.



During the analysis of this sample file it it clear that the file is indeed malicious.
A gathering of the IoC's from this analysis:

Host IoC's

- File pretends to be a .pdf but is really a .exe
- Hash analysis gave a 56/72 on virustotal
- Changes to the registry to achieve persistance
- Running the file deleted the original file and created the new persistant smss.exe file
- Creation of various other files such as LOG1, LOG2, SOFTWARELOG1 and a .bat file

Network IoC's

- Communication with unknown host mbaquyahcn.biz which gave a 2/91 in virustotal