


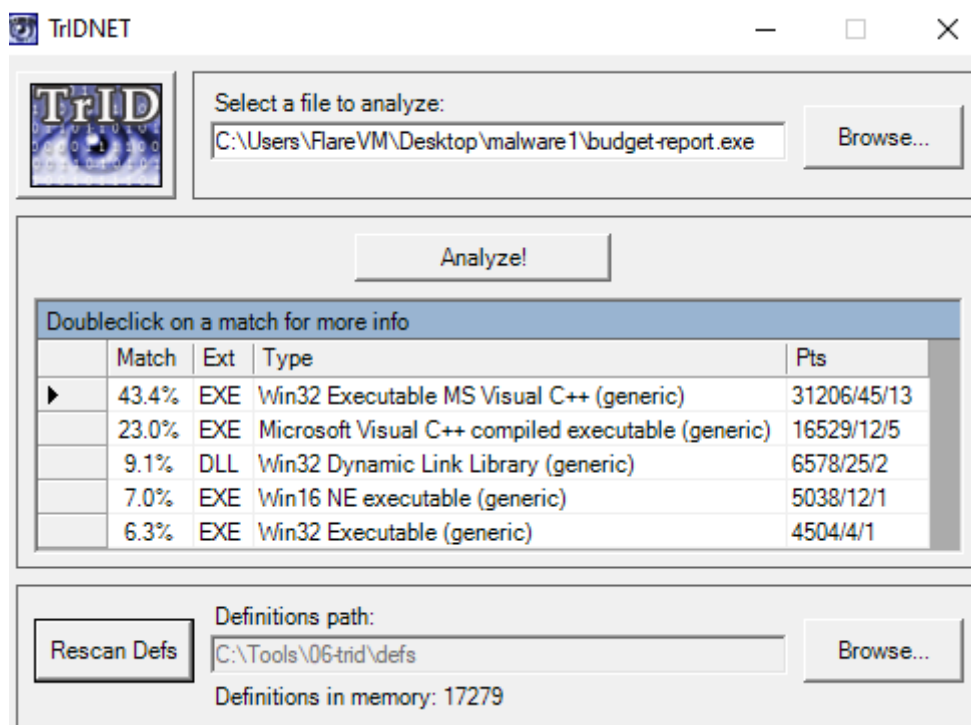
Here is my write-up for the file “budget-report”. The objective here is to find indicators of compromise/evidence that we are dealing with a malicious file.

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.

56 / 72

56/72 security vendors and 3 sandboxes flagged this file as malicious

15cc3cad7aec406a9ec93554c9eaf0bfbc740bef9d52dbc32bf559e90f53fee

Size: 409.50 KB | Last Modification Date: 6 days ago

budget-report.exe

peexe self-delete runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input persistence cve-2014-3931 cve-2016-2569 exploit

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: trojan.reconyc/ircbot | Threat categories: trojan downloader | Family labels: reconyc ircbot jaik

Security vendors' analysis

Vendor	Detection	Vendor	Detection
AhnLab-V3	Trojan.Win32.Reconyc.R302182	Alibaba	TrojanDownloader.Win32/Reconyc.6625...
ALYac	Gen:Variant.Jaik.94157	Antiy-AVL	Worm/Win32.AGeneric
Arcabit	Trojan.Jaik.D16FCD	Avast	Win32:Squida-A [Trj]
AVG	Win32:Squida-A [Trj]	Avira (no cloud)	TR/AD.LorisBot.mdjvt
BitDefender	Gen:Variant.Jaik.94157	BitDefenderTheta	Gen:NN.ZexaF.36744.zKW@aaGeu9hi
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.f6b8cc

Next we use PEStudio to do further static analysis.

c:\users\flarevm\desktop\malware1\budget-rep

indicators (groups > API)

footprints (count > 13)

virustotal (status > offline)

dos-header (size > 64 bytes)

dos-stub (size > 64 bytes)

rich-header (n/a)

file-header (compiler-stamp > Oct.1998)

optional-header (subsystem > GUI)

directories (count > 4)

sections (characteristics > virtual)

libraries (group > network)

imports (flag > 190)

exports (n/a)

thread-local-storage (count > 3)

.NET (n/a)

resources (count > 19)

strings (count > 4622)

debug (n/a)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (n/a)

indicator (18)	detail	level
groups > API	security registry data-exchange file synchroniza...	+++++
libraries > flag	Internet Extensions for Win32 Library (WININET.DLL)	+++++
libraries > flag	Windows Socket Library (WS2_32.dll)	+++++
mitre > technique	T1134 T1112 T1485 T1012 T1105 T1106 T1057 ...	+++++
file > compiler > stamp	Wed Oct 14 08:31:48 1998	++
sections > virtualized	.bss	++
imports > flag	54	++
file > entropy	5.405	+
file > type	executable	+
file > cpu	32-bit	+
file > sha256	15CC3CAD7AEC406A9EC93554C9EAF0BFBC740BEF...	+
file > size	419328 bytes	+
virustotal > error	The server name or address could not be resolved	+
thread-local-storage > callbacks	3	+
file > subsystem	GUI	+
entry-point	0x000012A0	+
certificate > info	n/a	+
imphash > md5	61F5FDA4608555DC4CB9E0836FC58773	+

PEStudio finds multiple high level signs of malicious code, one of which is registry which makes me believe the malware is trying to achieve persistence 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 persistent by creating or "setting" a value in the registry. We see more strange values such as ShellExecute, DeleteFile, WriteFile, WSStartup 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 TracWnd

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.

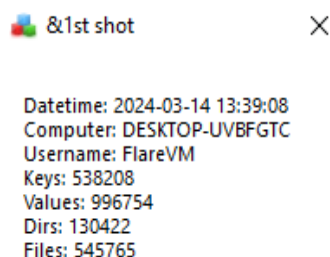
Dynamic Analysis

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

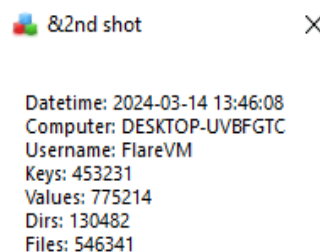
When the file is executed it disappears immediately, which makes me believe that it removes itself while creating another file (duplicate) of itself somewhere else.

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

Regshot 1st shot



Regshot 2nd shot




OK

OK

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.

Process Monitor - Sysinternals: www.sysinternals.com

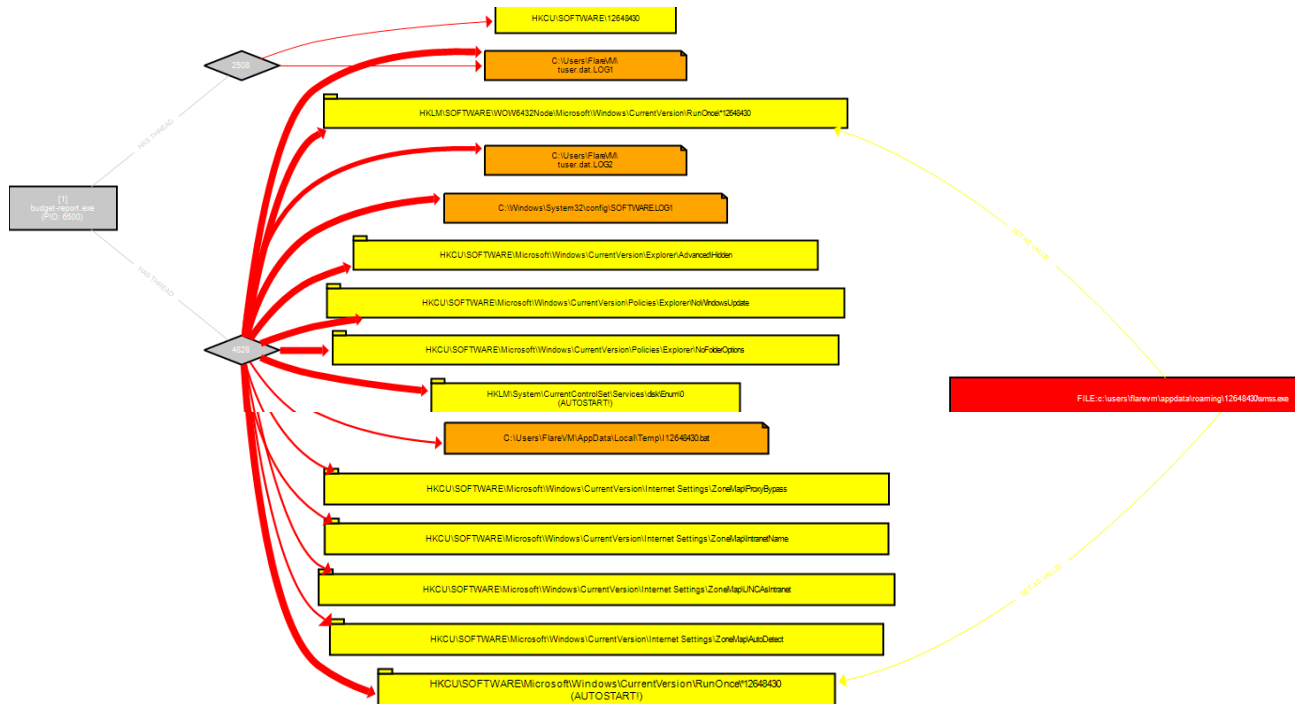
File Edit Event Filter Tools Options Help



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\12648430.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	WriteFile	C:\Users\FlareVM\AppData\Local\Temp\12648430.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 persistence. The red box on the right is indeed the new file we checked earlier, smss.exe, this is also linked to an autostart for persistence.



During the analysis of this sample file it is 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 persistence
- Running the file deleted the original file and created the new persistent 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