Original Feature Table with Interpretations

1. The original features of the dataset

number	Feature name (Abbreviation)	Feature Name (long)
1	Category	Category
2	pslist.nproc	Number of processes
3	pslist.nppid	# of Parent Processes
4	pslist.avg_threads	Avg # of threads
5	pslist.nprocs64bit	# of 64-bit processes
6	pslist.avg_handlers	Avg handlers
7	dlllist.ndlls	# of dlls
8	dlllist.avg_dlls_per_proc	Avg # of dlls per process.
9	handles.nhandles	# of handles
10	handles.avg_handles_per_proc	Average handles per process.
11	handles.nport	Number of port handles
12	handles.nfile	Number of Filehandles
13	handles.nevent	# of Event handles
14	handles.ndesktop	# of Desktop Handles
15	handles.nkey	# of Key handles
16	handles.nthread	# of thread handles
17	handles.ndirectory	# of directory handles
18	handles.nsemaphore	# of semaphore handles
19	handles.ntimer	# of timer handles
20	handles.nsection	# of section handles
21	handles.nmutant	# of mutant handles

22	ldrmodules.not_in_load	# of modules not in load
23	ldrmodules.not_in_init	# of modules not in init list
24	ldrmodules.not_in_mem	# of modules not in the mem list
25	ldrmodules.not_in_load_avg	#avg
26	ldrmodules.not_in_init	#avg
27	ldrmodules.not_in_mem_avg	#avg
28	malfind.ninjections	# of instances of injected code
29	malfind.commitCharge	# of instances of committed charges
30	malfind.protection	# of instances of protection
31	malfind.uniqueInjections	# of unique injections
32	psxview.not_in_pslist	The sum of hidden processes not in the process list
33	psxview.not_in_eprocess_pool	Sum of hidden processes not in e process pool
34	psxview.not_in_ethread_pool	Sum of hidden processes not in e thread pool
35	psxview.not_in_pspcid_list	The sum of hidden processes is not in the id list.
36	psxview.not_in_csrss_handles	The sum of hidden processes not in csrss handles list.
37	psxview.not_in_session	# of hidden processes not in session
38	psxview.not_in_deskthrd	# of hidden processes not on the desktop

39	psxview.not_in_pslist_false_avg	Avg
40	psxview.not_in_eprocess_pool_false_avg	Avg
41	psxview.not_in_ethread_pool_false_avg	Avg
42	psxview.not_in_pspcid_list_false_avg	Avg
43	psxview.not_in_csrss_handles_false_avg	Avg
44	psxview.not_in_session_false_avg	Avg
45	psxview.not_in_deskthrd_false_avg	Avg
46	modules.nmodules	# of modules
47	svcscan.nservices	# of services in service scan
48	svcscan.kernel_drivers	# of kernel drivers in service scan
49	svcscan.fs_drivers	# of drivers
50	svcscan.process_services	# of process services
51	svcscan.shared_process_services	# of shared processes
52	svcscan.interactive_process_services	# of interactive process services
53	svcscan.nactive	# of inactive services
54	callbacks.ncallbacks	# of callbacks
55	callbacks.nanonymous	# of anonymous callbacks
56	callbacks.ngeneric	# of generic callbacks
57	Class	Classification – Benign or Malware