Team 10(최준헌, 박해원, 정세화)

# Homework: 2nd PRoject

* Analysis of the association of established datasets based on infringement indicators

# outline

|  |  |
| --- | --- |
|  | It checks whether normalized data sets using artifacts extracted through intrusion incident-based malicious code performed by applying the FP-growth algorithm can be used for algorithms such as correlation analysis, machine learning, and artificial intelligence. |

* Based on the data set previously built in Project 1, the association analysis is performed focusing on the classification and year of infringement incidents.
* Through the FP-growth algorithm, each dataset or two or more datasets are combined to generate various rules.

# Table sorting according to the SUPPORT value & Rules according to the table

|  |  |
| --- | --- |
| #1 | Malware name: Downloader |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'TCP'}) | | 1.0 | frozenset({'TCP', 'MD5'}) | | 1.0 | frozenset({'MD5', 'TCP', 'HTTP'}) | | 1.0 | frozenset({'TCP', 'HTTP'}) | | 1.0 | frozenset({'MD5', 'HTTP'}) | | 1.0 | frozenset({'MD5'}) | | 1.0 | frozenset({'HTTP'}) | | 0.9444444444444440 | frozenset({'c:\\', 'TCP', 'HTTP'}) | | 0.9444444444444440 | frozenset({'c:\\', 'TCP'}) | | 0.9444444444444440 | frozenset({'c:\\', 'MD5', 'TCP', 'HTTP'}) | | 0.9444444444444440 | frozenset({'c:\\', 'TCP', 'MD5'}) | | 0.9444444444444440 | frozenset({'c:\\', 'MD5', 'HTTP'}) | | 0.9444444444444440 | frozenset({'c:\\', 'MD5'}) | | 0.9444444444444440 | frozenset({'c:\\', 'HTTP'}) | | 0.9444444444444440 | frozenset({'c:\\'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', '80.0', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'80.0', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'80.0', 'TCP'}) | | 0.8333333333333330 | frozenset({'80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'80.0', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'MD5', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'80.0'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'MD5', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', 'MD5', '80.0', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0', 'TCP', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0', 'TCP', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0', 'TCP'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', '80.0'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'HTTP', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', 'MD5', 'REG\_SZ', 'HTTP'}) | | 0.7777777777777780 | frozenset({'c:\\', 'REG\_SZ', 'TCP'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ', 'TCP'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ', 'MD5'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ', 'HTTP'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.7222222222222220 | frozenset({'80.0', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.7222222222222220 | frozenset({'80.0', 'MD5', 'REG\_SZ', 'HTTP'}) | | 0.7222222222222220 | frozenset({'REG\_SZ', 'TCP', 'HTTP', '80.0', 'MD5'}) | | |

|  |  |
| --- | --- |
| #2 | Malware name: Ransom |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'TCP'}) | | 1.0 | frozenset({'MD5'}) | | 1.0 | frozenset({'TCP', 'HTTP'}) | | 1.0 | frozenset({'MD5', 'HTTP'}) | | 1.0 | frozenset({'TCP', 'MD5'}) | | 1.0 | frozenset({'MD5', 'TCP', 'HTTP'}) | | 1.0 | frozenset({'HTTP'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'TCP', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_AUTO\_START', 'TCP', 'HTTP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'TCP', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'TCP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'HTTP'}) | | 0.9333333333333330 | frozenset({'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'MD5'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'HTTP'}) | | 0.9333333333333330 | frozenset({'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.9333333333333330 | frozenset({'SERVICE\_AUTO\_START'}) | | 0.9333333333333330 | frozenset({'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.8666666666666670 | frozenset({'c:\\', 'HTTP', 'MD5'}) | | 0.8666666666666670 | frozenset({'c:\\', 'TCP', 'HTTP', 'MD5'}) | | 0.8666666666666670 | frozenset({'c:\\', 'TCP', 'MD5'}) | | 0.8666666666666670 | frozenset({'c:\\', 'TCP', 'HTTP'}) | | 0.8666666666666670 | frozenset({'c:\\', 'HTTP'}) | | 0.8666666666666670 | frozenset({'c:\\', 'TCP'}) | | 0.8666666666666670 | frozenset({'c:\\', 'MD5'}) | | 0.8666666666666670 | frozenset({'c:\\'}) | | 0.8 | frozenset({'TCP', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'MD5', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'80.0', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'MD5', '80.0', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'80.0', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.8 | frozenset({'MD5', '80.0', 'HTTP'}) | | 0.8 | frozenset({'80.0', 'TCP', 'HTTP'}) | | 0.8 | frozenset({'80.0', 'TCP', 'MD5'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'MD5', '80.0', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'SERVICE\_AUTO\_START', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.8 | frozenset({'80.0', 'TCP', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'MD5', '80.0', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'SERVICE\_AUTO\_START', 'TCP', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'MD5', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'MD5', '80.0', 'TCP', 'HTTP'}) | | 0.8 | frozenset({'SERVICE\_AUTO\_START', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'80.0', 'MD5'}) | | 0.8 | frozenset({'SERVICE\_AUTO\_START', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'SERVICE\_AUTO\_START', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'80.0', 'TCP'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'HTTP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'80.0', 'HTTP'}) | | 0.8 | frozenset({'c:\\', 'MD5', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'c:\\', 'MD5', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'MD5', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'TCP', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'HTTP'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'80.0'}) | | 0.8 | frozenset({'c:\\', 'TCP', 'HTTP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'HTTP', 'MD5'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.8 | frozenset({'80.0', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'HTTP', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'MD5', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'MD5'}) | | 0.8 | frozenset({'c:\\', 'SERVICE\_WIN32\_OWN\_PROCESS', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'HTTP', '80.0', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', '80.0', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', '80.0', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'TCP', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'HTTP', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'TCP'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'MD5', 'c:\\', '80.0', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'TCP', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'TCP', 'SERVICE\_AUTO\_START'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | 0.7333333333333330 | frozenset({'c:\\', 'TCP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS'}) | | 0.7333333333333330 | frozenset({'MD5', 'c:\\', '80.0', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', '80.0', 'TCP', 'HTTP'}) | | 0.7333333333333330 | frozenset({'c:\\', 'SERVICE\_AUTO\_START', 'TCP', 'HTTP', '80.0', 'SERVICE\_WIN32\_OWN\_PROCESS', 'MD5'}) | | |

|  |  |
| --- | --- |
| #3 | Malware name: Exploit |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'TCP'}) | | 1.0 | frozenset({'80.0', 'REG\_SZ', 'MD5'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP', 'MD5'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP', 'HTTP'}) | | 1.0 | frozenset({'80.0', 'TCP', 'REG\_SZ'}) | | 1.0 | frozenset({'TCP', 'HTTP', 'MD5'}) | | 1.0 | frozenset({'80.0', 'TCP', 'MD5'}) | | 1.0 | frozenset({'80.0', 'TCP', 'HTTP'}) | | 1.0 | frozenset({'MD5', 'REG\_SZ', 'HTTP'}) | | 1.0 | frozenset({'80.0', 'REG\_SZ', 'HTTP'}) | | 1.0 | frozenset({'80.0', 'MD5'}) | | 1.0 | frozenset({'MD5', '80.0', 'HTTP'}) | | 1.0 | frozenset({'REG\_SZ'}) | | 1.0 | frozenset({'80.0', 'TCP', 'REG\_SZ', 'MD5'}) | | 1.0 | frozenset({'80.0', 'TCP', 'REG\_SZ', 'HTTP'}) | | 1.0 | frozenset({'80.0', 'TCP', 'HTTP', 'MD5'}) | | 1.0 | frozenset({'MD5', '80.0', 'REG\_SZ', 'HTTP'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 1.0 | frozenset({'80.0', 'HTTP'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP', 'HTTP', 'MD5'}) | | 1.0 | frozenset({'80.0'}) | | 1.0 | frozenset({'80.0', 'REG\_SZ'}) | | 1.0 | frozenset({'TCP', 'HTTP'}) | | 1.0 | frozenset({'MD5'}) | | 1.0 | frozenset({'80.0', 'TCP'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP'}) | | 1.0 | frozenset({'REG\_SZ', 'MD5'}) | | 1.0 | frozenset({'REG\_SZ', 'HTTP'}) | | 1.0 | frozenset({'TCP', 'MD5'}) | | 1.0 | frozenset({'MD5', 'HTTP'}) | | 1.0 | frozenset({'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'HTTP', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', 'STD\_INPUT\_HANDLE', 'winword.exe', 'HTTP'}) | | 0.8333333333333330 | frozenset({'MD5', '80.0', 'winword.exe', 'HTTP'}) | | 0.8333333333333330 | frozenset({'MD5', 'STD\_INPUT\_HANDLE', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'TCP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', 'REG\_SZ', 'winword.exe', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'HTTP', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'HTTP', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', '80.0'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'STD\_INPUT\_HANDLE', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'TCP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'TCP'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'TCP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'TCP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ', 'TCP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ', 'TCP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'TCP', 'HTTP', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'TCP', 'HTTP', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'REG\_SZ', 'TCP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'TCP', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'TCP', 'REG\_SZ'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', '80.0'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'HTTP'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'HTTP'}) | | 0.8333333333333330 | frozenset({'winword.exe', 'STD\_INPUT\_HANDLE', 'MD5'}) | | 0.8333333333333330 | frozenset({'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'winword.exe', '80.0', 'MD5'}) | | 0.8333333333333330 | frozenset({'MD5', 'STD\_INPUT\_HANDLE', 'HTTP'}) | | 0.8333333333333330 | frozenset({'MD5', 'winword.exe', 'HTTP'}) | | 0.8333333333333330 | frozenset({'REG\_SZ', 'winword.exe', 'TCP', 'HTTP', 'STD\_INPUT\_HANDLE', '80.0', 'MD5'}) | | |

|  |  |
| --- | --- |
| #4 | Malware name: Trojan |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'MD5'}) | | 1.0 | frozenset({'HTTP'}) | | 1.0 | frozenset({'MD5', 'HTTP'}) | | 0.9696969696969700 | frozenset({'c:\\'}) | | 0.9696969696969700 | frozenset({'c:\\', 'HTTP'}) | | 0.9696969696969700 | frozenset({'c:\\', 'MD5'}) | | 0.9696969696969700 | frozenset({'c:\\', 'MD5', 'HTTP'}) | | 0.9393939393939390 | frozenset({'MD5', 'TCP', 'HTTP'}) | | 0.9393939393939390 | frozenset({'TCP'}) | | 0.9393939393939390 | frozenset({'TCP', 'HTTP'}) | | 0.9393939393939390 | frozenset({'TCP', 'MD5'}) | | 0.9090909090909090 | frozenset({'c:\\', 'TCP', 'MD5'}) | | 0.9090909090909090 | frozenset({'c:\\', 'TCP', 'HTTP'}) | | 0.9090909090909090 | frozenset({'MD5', 'c:\\', 'TCP', 'HTTP'}) | | 0.9090909090909090 | frozenset({'c:\\', 'TCP'}) | | 0.8787878787878790 | frozenset({'c:\\', 'REG\_SZ', 'HTTP'}) | | 0.8787878787878790 | frozenset({'REG\_SZ'}) | | 0.8787878787878790 | frozenset({'MD5', '80.0', 'HTTP'}) | | 0.8787878787878790 | frozenset({'c:\\', 'MD5', 'REG\_SZ', 'HTTP'}) | | 0.8787878787878790 | frozenset({'MD5', 'REG\_SZ', 'HTTP'}) | | 0.8787878787878790 | frozenset({'c:\\', 'REG\_SZ', 'MD5'}) | | 0.8787878787878790 | frozenset({'80.0', 'HTTP'}) | | 0.8787878787878790 | frozenset({'REG\_SZ', 'MD5'}) | | 0.8787878787878790 | frozenset({'REG\_SZ', 'HTTP'}) | | 0.8787878787878790 | frozenset({'c:\\', 'REG\_SZ'}) | | 0.8787878787878790 | frozenset({'80.0', 'MD5'}) | | 0.8787878787878790 | frozenset({'80.0'}) | | 0.8484848484848490 | frozenset({'c:\\', '80.0', 'HTTP'}) | | 0.8484848484848490 | frozenset({'c:\\', 'MD5', '80.0', 'HTTP'}) | | 0.8484848484848490 | frozenset({'MD5', '80.0', 'TCP', 'HTTP'}) | | 0.8484848484848490 | frozenset({'80.0', 'TCP', 'HTTP'}) | | 0.8484848484848490 | frozenset({'80.0', 'TCP', 'MD5'}) | | 0.8484848484848490 | frozenset({'c:\\', '80.0'}) | | 0.8484848484848490 | frozenset({'c:\\', '80.0', 'MD5'}) | | 0.8484848484848490 | frozenset({'80.0', 'TCP'}) | | 0.8181818181818180 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'HTTP', 'MD5'}) | | 0.8181818181818180 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.8181818181818180 | frozenset({'c:\\', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8181818181818180 | frozenset({'REG\_SZ', 'TCP', 'MD5'}) | | 0.8181818181818180 | frozenset({'REG\_SZ', 'TCP', 'HTTP'}) | | 0.8181818181818180 | frozenset({'c:\\', 'REG\_SZ', 'TCP'}) | | 0.8181818181818180 | frozenset({'REG\_SZ', 'TCP'}) | | 0.8181818181818180 | frozenset({'c:\\', '80.0', 'TCP'}) | | 0.8181818181818180 | frozenset({'c:\\', '80.0', 'TCP', 'MD5'}) | | 0.8181818181818180 | frozenset({'c:\\', '80.0', 'TCP', 'HTTP'}) | | 0.8181818181818180 | frozenset({'c:\\', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.8181818181818180 | frozenset({'MD5', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.7878787878787880 | frozenset({'80.0', 'REG\_SZ', 'HTTP'}) | | 0.7878787878787880 | frozenset({'c:\\', 'MD5', 'REG\_SZ', '80.0', 'HTTP'}) | | 0.7878787878787880 | frozenset({'80.0', 'MD5', 'REG\_SZ', 'HTTP'}) | | 0.7878787878787880 | frozenset({'c:\\', 'REG\_SZ', '80.0', 'HTTP'}) | | 0.7878787878787880 | frozenset({'c:\\', 'REG\_SZ', '80.0', 'MD5'}) | | 0.7878787878787880 | frozenset({'80.0', 'REG\_SZ', 'MD5'}) | | 0.7878787878787880 | frozenset({'c:\\', 'REG\_SZ', '80.0'}) | | 0.7878787878787880 | frozenset({'80.0', 'REG\_SZ'}) | | 0.7575757575757580 | frozenset({'80.0', 'REG\_SZ', 'TCP'}) | | 0.7575757575757580 | frozenset({'MD5', 'd41d8cd98f00b204e9800998ecf8427e', 'HTTP'}) | | 0.7575757575757580 | frozenset({'d41d8cd98f00b204e9800998ecf8427e', 'MD5'}) | | 0.7575757575757580 | frozenset({'d41d8cd98f00b204e9800998ecf8427e', 'HTTP'}) | | 0.7575757575757580 | frozenset({'c:\\', 'MD5', 'REG\_SZ', 'TCP', '80.0', 'HTTP'}) | | 0.7575757575757580 | frozenset({'REG\_SZ', 'TCP', 'HTTP', '80.0', 'MD5'}) | | 0.7575757575757580 | frozenset({'c:\\', 'REG\_SZ', 'TCP', '80.0', 'HTTP'}) | | 0.7575757575757580 | frozenset({'c:\\', 'REG\_SZ', 'TCP', '80.0', 'MD5'}) | | 0.7575757575757580 | frozenset({'80.0', 'REG\_SZ', 'TCP', 'HTTP'}) | | 0.7575757575757580 | frozenset({'80.0', 'REG\_SZ', 'TCP', 'MD5'}) | | 0.7575757575757580 | frozenset({'d41d8cd98f00b204e9800998ecf8427e'}) | | 0.7575757575757580 | frozenset({'c:\\', 'REG\_SZ', 'TCP', '80.0'}) | | 0.7272727272727270 | frozenset({'c:\\', 'd41d8cd98f00b204e9800998ecf8427e'}) | | 0.7272727272727270 | frozenset({'c:\\', 'd41d8cd98f00b204e9800998ecf8427e', 'HTTP'}) | | 0.7272727272727270 | frozenset({'c:\\', 'd41d8cd98f00b204e9800998ecf8427e', 'MD5'}) | | 0.7272727272727270 | frozenset({'MD5', 'c:\\', 'd41d8cd98f00b204e9800998ecf8427e', 'HTTP'}) | | |

|  |  |
| --- | --- |
| #5 | Malware name: Spy |
| |  |  | | --- | --- | | **support** | **itemsets** | | 0.75 | frozenset({'0.0'}) | | |

|  |  |
| --- | --- |
| #6 | Malware name: Dropper |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'c:\\'}) | | 1.0 | frozenset({'TCP'}) | | 1.0 | frozenset({'REG\_SZ'}) | | 1.0 | frozenset({'c:\\', 'TCP'}) | | 1.0 | frozenset({'c:\\', 'REG\_SZ'}) | | 1.0 | frozenset({'REG\_SZ', 'TCP'}) | | 1.0 | frozenset({'c:\\', 'REG\_SZ', 'TCP'}) | | |

|  |  |
| --- | --- |
| #7 | Malware name: UDS |
| |  |  | | --- | --- | | **support** | **itemsets** | | 1.0 | frozenset({'winword.exe'}) | | 1.0 | frozenset({'winword.exe', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'C:\\Users\\aETAdzjz\\Desktop\\', 'winword.exe', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'winword.exe', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\', 'winword.exe'}) | | 1.0 | frozenset({'winword.exe', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'winword.exe', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'C:\\Users\\aETAdzjz\\Desktop\\', 'winword.exe'}) | | 1.0 | frozenset({'winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'winword.exe'}) | | 1.0 | frozenset({'winword.exe', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'c:\\program files\\microsoft office\\root\\office16\\winword.exe'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'C:\\Users\\aETAdzjz\\Desktop\\', '1112.0'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe'}) | | 1.0 | frozenset({'c:\\program files\\microsoft office\\root\\office16\\winword.exe', '1112.0'}) | | 1.0 | frozenset({'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'winword.exe'}) | | 1.0 | frozenset({'winword.exe', '1112.0'}) | | 1.0 | frozenset({'winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'winword.exe', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe'}) | | 1.0 | frozenset({'"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n'}) | | 1.0 | frozenset({'1112.0'}) | | 1.0 | frozenset({'C:\\Users\\aETAdzjz\\Desktop\\'}) | | 1.0 | frozenset({'1112.0', '"C:\\Program Files\\Microsoft Office\\Root\\Office16\\WINWORD.EXE" /n', 'winword.exe', 'c:\\program files\\microsoft office\\root\\office16\\winword.exe', 'C:\\Users\\aETAdzjz\\Desktop\\'}) | | |

## SOURCE CODES

|  |
| --- |
| import pandas as pd import numpy as np from mlxtend.preprocessing import TransactionEncoder from mlxtend.frequent\_patterns import association\_rules from mlxtend.frequent\_patterns import fpgrowth  dataset\_df = pd.read\_csv('./dataset.csv', index\_col='file\_name')  malware\_type\_dict = {}  # 같은 family\_name을 가진 행끼리 모아서 dictionary 생성 # key: family\_name, value: 해당 family\_name을 가진 row들의 list for row in dataset\_df.iterrows():  # 해당 family\_name과 일치하는 key가 dictionary에 존재하지 않는 경우, 빈 list를 value로 가지는 원소 생성  if not row[1]['Family'] in malware\_type\_dict:  malware\_type\_dict[row[1]['Family']] = pd.DataFrame()   # 해당 family\_name과 일치하는 원소의 value에 row 추가  # row의 type은 tuple이기 때문에, list로 타입변경해줌  malware\_type\_dict[row[1]['Family']] = malware\_type\_dict[row[1]['Family']].append(row[1].drop('Family'),  ignore\_index=True)  # print(malware\_type\_dict)  # 컬럼 전체 데이터가 NaN 경우 column drop # 컬럼 데이터가 한 번씩 나올 경우 column drop  for key, df in malware\_type\_dict.items():  for col in df.columns:  # 컬럼 전체가 NaN인 경우 or 컬럼 데이터가 한 번씩 나올 경우  if df[col].isna().sum() == len(df) or len(df[col].dropna().unique()) == len(df[col].dropna()):  # if key == 'Downloader':  # print(col)  df = df.drop(col, axis=1)  else:  df[col] = df[col].fillna(df[col].mode()[0])   df = df.dropna(axis=0)  malware\_type\_dict[key] = df   for key, value in malware\_type\_dict.items():  print("\n\n===============================================================================================")  print("악성코드 명: {}".format(key)) # Family\_name 출력  print("해당하는 파일 개수: {}".format(len(value))) # 해당 Family\_name을 가진 row의 개수 출력  # print("\n")   # 파일 한 개일 경우 연관성 분석 건너뜀  if len(value) == 1:  continue   dataset\_arr = value.to\_numpy(dtype=str)   # # row 생략 없이 출력  # pd.set\_option('display.max\_rows', None)  # # col 생략 없이 출력  # pd.set\_option('display.max\_columns', None)   pd.set\_option('display.max\_colwidth', 1)   # 연관성 분석  te = TransactionEncoder()  te\_ary = te.fit(dataset\_arr).transform(dataset\_arr)  df = pd.DataFrame(te\_ary, columns=te.columns\_)  result = fpgrowth(df, min\_support=0.7, use\_colnames=True)  print("\n=====연관성 분석=====")  print(result.sort\_values(by=['support'], ascending=False))  # print("\n")  # result\_chart = association\_rules(result, metric="confidence", min\_threshold=0.5)  # print('<result chart>')  # print(result\_chart)  # print('\n') |