



The screenshot displays the 'Win7 32 bit Complete' interface, which is a tool for analyzing malicious activity. The top section shows the file name '5042_30_2019_5-40359273.doc' and its MD5 hash '9600328A14AB247BBE1B1BA6B543E2E3'. The start time is '30.09.2019, 15:46' and the total time is '60 s'. Below this, there are buttons for 'macros', 'macros-on-open', 'generated-doc', 'emotet-doc', and 'emotet'. The 'Indicators' section shows a list of indicators, including 'Emotet'. The 'Tracker' section shows 'Emotet'. The 'Get sample' button is highlighted. The 'IOC' button is also visible. The 'MalConf' button is present. The 'Restart' button is shown. The 'Text report' button is visible. The 'Graph' button is present. The 'ATT&CK' button is shown. The 'Summary' button is highlighted. The 'Export' button is visible. The 'CPU' section shows a bar chart of CPU usage. The 'Processes' section shows a list of processes, including 'WINWORD.EXE', 'powershell.exe', and 'ntvdm.exe'. The 'Filter by PID or name' button is present. The 'Only important' checkbox is checked. The 'WINWORD.EXE' process is highlighted. The 'powershell.exe' process is highlighted. The 'ntvdm.exe' process is highlighted. The 'Summary' button is highlighted. The 'Export' button is visible. The 'CPU' section shows a bar chart of CPU usage. The 'Processes' section shows a list of processes, including 'WINWORD.EXE', 'powershell.exe', and 'ntvdm.exe'. The 'Filter by PID or name' button is present. The 'Only important' checkbox is checked. The 'WINWORD.EXE' process is highlighted. The 'powershell.exe' process is highlighted. The 'ntvdm.exe' process is highlighted.

Win7 32 bit Complete

5042_30_2019_5-40359273.doc

MD5: 9600328A14AB247BBE1B1BA6B543E2E3

Start: 30.09.2019, 15:46 Total time: 60 s

macros macros-on-open generated-doc emotet-doc emotet

Indicators: Tracker: Emotet

Get sample IOC MalConf Restart

Text report Graph ATT&CK **Summary** Export

CPU

Processes Filter by PID or name ☒ Only important

2800 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\5042_3... 3k 1k 116

3100 WMI powershell.exe -enco PAAjACAAaAB0AHQAcABzADoALwAvA... 1k 556 230

4012 ntvdm.exe -i1 436 0 50

HTTP Requests

0

Connections

1

DNS Requests

1

Threats

0

Filter by PID, name or url

PCAP

	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
NETWORK								
FILES								
DEBUG								

No data

Warning [3100] powershell.exe Executes application which crashes

Try community version for free!

Register now