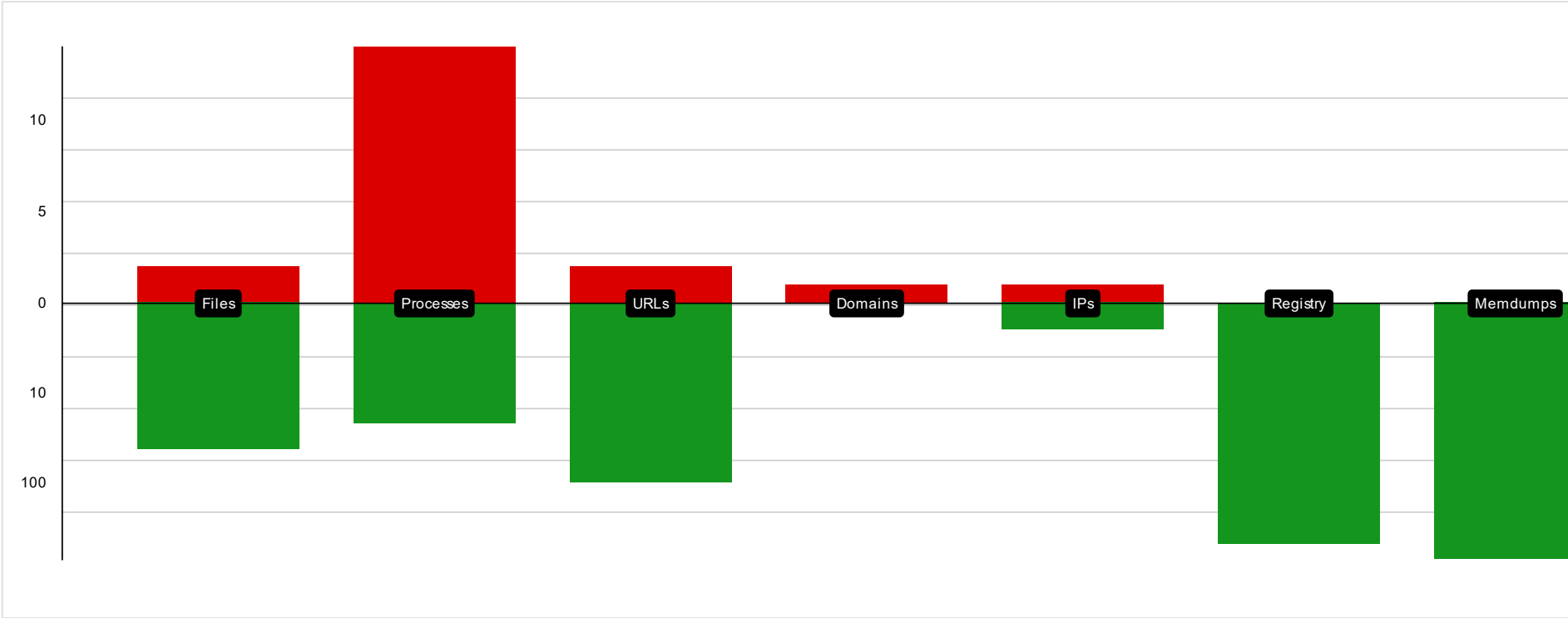


IOCR



Files

File Path	Type	Category	Malic...	Dow...	
A Letter before court 4.docx	Microsoft OOXML	initial sa...			▼
C:\Users\user\AppData\Local\Temp\cha...	PE32+ executable (DLL) (GUI) x86-64, for MS Windows	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	data	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	data	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	data	modified			▼
C:\Users\user\AppData\Local\Microsoft\...	XML 1.0 document, UTF-8 Unicode text, with very long l...	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	JPEG image data, JFIF standard 1.01, aspect ratio, de...	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	ms-windows metafont .wmf	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	HTML document, ASCII text, with very long lines	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	Targa image data - Map - RLE 5 x 65536 x 0 "004"	dropped			▼
C:\Users\user\AppData\Local\Microsoft\...	HTML document, ASCII text, with very long lines	dropped			▼

There are 34 hidden **files**, click here to show them.

Processes



Path	Cmdline	Malic...	
C:\Program Files (x86)\Microsoft Office...	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Em...		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\control.exe	'C:\Windows\System32\control.exe' '.cpl:123',		▼

There are 25 hidden **processes**, click here to show them.


URLs

Name	IP	Malic...	
http://hidusi.com/e8c76295a5f9acb7/m...	23.106.160.25		▼
http://hidusi.com/e8c76295a5f9acb7/si...	23.106.160.25		▼
https://api.diagnosticsdf.office.com	unknown		▼
https://login.microsoftonline.com/	unknown		▼
https://shell.suite.office.com:1443	unknown		▼
https://login.windows.net/72f988bf-86f1...	unknown		▼




https://insertmedia.bing.office.net/imag...	unknown		▼
https://cdn.entity.	unknown		▼
There are 91 hidden URLs , click here to show them.			

Domains

Name	IP	Malic...	
hidusi.com	23.106.160.25		▼





















IPs

IP	Domain	Country	Malicious	
23.106.160.25	hidusi.com	United States 		▼
192.168.2.1	unknown	unknown 		▼

Registry

Path	Value	Malic...	
C:\Program Files (x86)\Microsoft Office...) +		▼
C:\Program Files (x86)\Microsoft Office...	* +		▼
C:\Program Files (x86)\Microsoft Office...	LastBootTime		▼
C:\Program Files (x86)\Microsoft Office...	k'+		▼
C:\Program Files (x86)\Microsoft Office...	RemoteClearDate		▼
C:\Program Files (x86)\Microsoft Office...	Last		▼
C:\Program Files (x86)\Microsoft Office...	FilePath		▼
C:\Program Files (x86)\Microsoft Office...	StartDate		▼
C:\Program Files (x86)\Microsoft Office...	EndDate		▼
C:\Program Files (x86)\Microsoft Office...	Properties		▼
There are 475 hidden registries , click here to show them.			

Memdumps

Base Address	Regiontype	Protect	Malic...	Down...	
306A000	unkown	page read and ...			▼
2F90000	heap default	page read and ...			▼
30BE000	unkown	page read and ...			▼
9F0000	heap private	page read and ...			▼
AC0000	heap default	page read and ...			▼
293307E0000	unkown	page read and ...			▼
99E000	unkown	page read and ...			▼
300E000	unkown	page read and ...			▼
11DA000	heap default	page read and ...			▼
123B000	unkown	page read and ...			▼
There are 711 hidden memdumps , click here to show them.					

