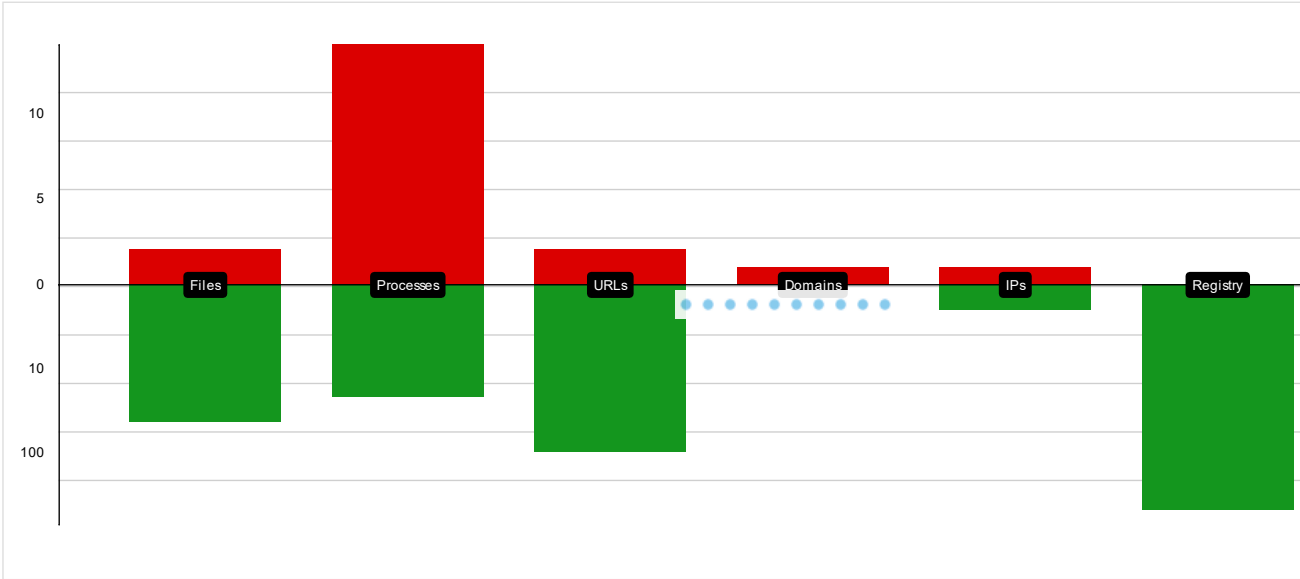


IOCHTML Report



Files

File Path	Type	Cate...	M ...	Do...	
A Letter before court 4.docx	Microsoft OOXML	initial...			▼
C:\Users\user\AppData\Local\...	PE32+ executable (DLL) (GUI) x86-64, fo...	drop...			▼
C:\Users\user\AppData\Local\...	data	drop...			▼
C:\Users\user\AppData\Local\...	data	drop...			▼
C:\Users\user\AppData\Local\...	data	modif...			▼
C:\Users\user\AppData\Local\...	XML 1.0 document, UTF-8 Unicode text, ...	drop...			▼
C:\Users\user\AppData\Local\...	JPEG image data, JFIF standard 1.01, a...	drop...			▼
C:\Users\user\AppData\Local\...	ms-windows metafont .wmf	drop...			▼
C:\Users\user\AppData\Local\...	HTML document, ASCII text, with very lon...	drop...			▼
C:\Users\user\AppData\Local\...	Targa image data - Map - RLE 5 x 65536...	drop...			▼
C:\Users\user\AppData\Local\...	HTML document, ASCII text, with very lon...	drop...			▼
There are 34 hidden files, click here to show them.					

Processes

Path	Cmdline	Ma...	
C:\Program Files (x86)\Micro...	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD....		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼
C:\Windows\SysWOW64\co...	'C:\Windows\System32\control.exe' '.cpl:123',		▼



URLs

Name	IP	Ma...	
http://hidusi.com/e8c76295a...	23.106.160.25		▼
http://hidusi.com/e8c76295a...	23.106.160.25		▼
https://api.diagnosticsdf.offi...	unknown		▼
https://login.microsoftonline....	unknown		▼
https://shell.suite.office.com:...	unknown		▼
https://login.windows.net/72f...	unknown		▼
https://autodiscover-s.outloo...	unknown		▼
https://roaming.edog.	unknown		▼
https://insertmedia.bing.offic...	unknown		▼
https://cdn.entity.	unknown		▼
There are 91 hidden URLs, click here to show them.			

Domains

Name	IP	Ma...	
hidusi.com	23.106.160.25		▼

IPs

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













Registry

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

Memdumps

Base Address	Regiontype	Protect	Ma...	Do...	
306A000	unkown	page read ...			▼



AC0000	heap default	page read ...			▼
293307E0000	unkown	page read ...			▼
99E000	unkown	page read ...			▼
300E000	unkown	page read ...			▼
11DA000	heap default	page read ...			▼
123B000	unkown	page read ...			▼
There are 711 hidden memdumps , click here to show them.					

