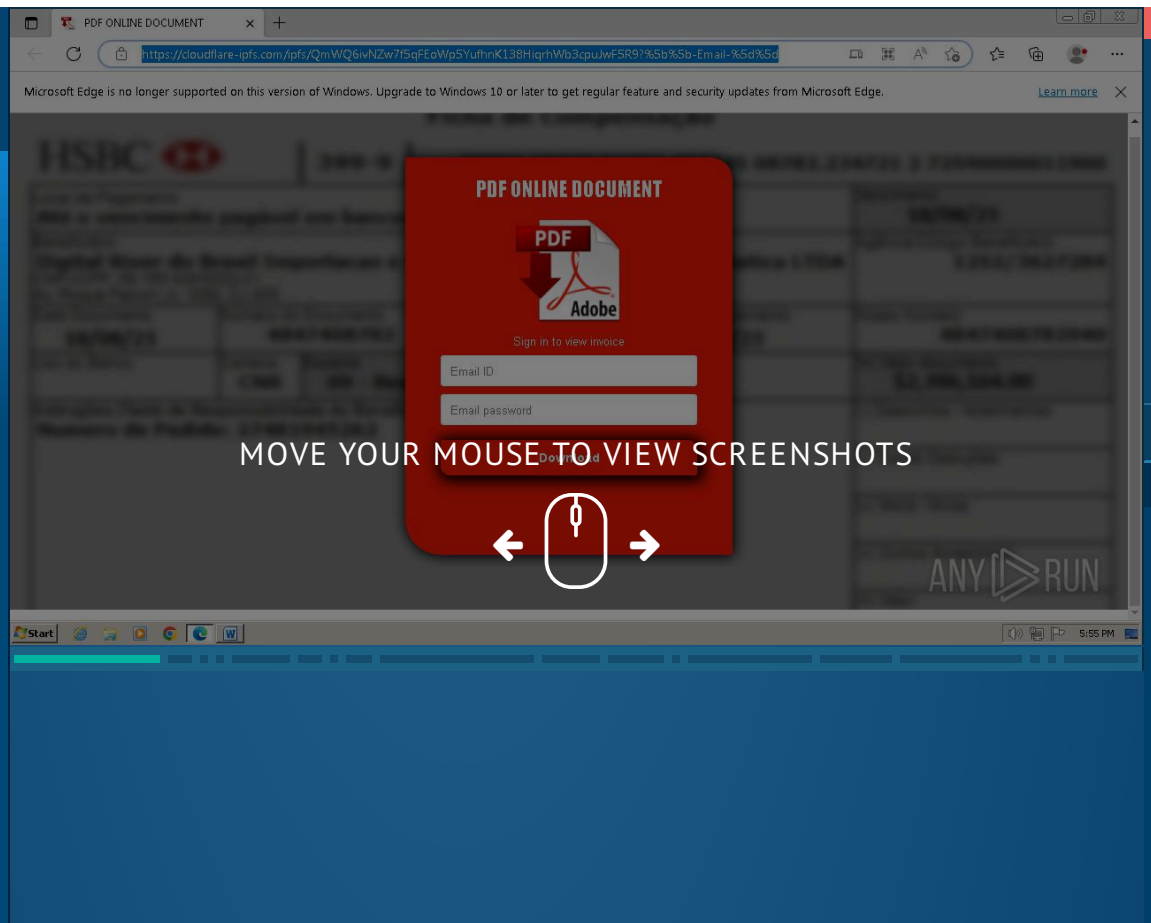

Malicious activity

Invoice.docx

MD5: DB74AF14DB400164A18F2CF195625200

Start: 12.04.2024, 18:54 Total time: 60 s

Win7 32 bit Complete

ipfs phishing

Indicators:

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary (beta) | Export

CPU RAM

Processes Filter by PID or name Only important

3936	WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\In...	4k	12k	150
3724	msedge.exe	--single-argument https://cloudflare-ipfs.com/ipf...	7k	2k	387
1740	msedge.exe	--type=crashpad-handler "--user-data-dir=C:\...	98	23	21
3324	msedge.exe	--type=gpu-process --gpu-preferences=UAAA...	471	93	74
2724	msedge.exe	--type=utility --utility-sub-type=network.mojo... phishing	762	307	56
1308	msedge.exe	--type=utility --utility-sub-type=storage.mojo...	202	37	48
1772	msedge.exe	--type=renderer --lang=en-US --js-flags=--ms-...	368	41	47
3540	msedge.exe	--type=renderer --first-renderer-process --lan...	273	41	47
2620	msedge.exe	--type=gpu-process --gpu-preferences=UAAA...	427	66	76
1796	msedge.exe	--type=utility --utility-sub-type=data_decoder....	238	37	48
2588	msedge.exe	--type=utility --utility-sub-type=data_decoder....	238	37	48
664	msedge.exe	--type=utility --utility-sub-type=entity_extractio...	252	38	50
1020	msedge.exe	--type=utility --utility-sub-type=entity_extracti...	240	37	49
3232	msedge.exe	--type=utility --utility-sub-type=asset_store....	252	37	49
1124	msedge.exe	--type=utility --utility-sub-type=data_decoder....	238	37	48
3900	msedge.exe	--type=utility --utility-sub-type=unzip.mojom....	246	37	48
2828	msedge.exe	--type=utility --utility-sub-type=data_decoder....	238	37	48
1652	msedge.exe	--type=utility --utility-sub-type=unzip.mojom....	253	37	48
2028	msedge.exe	--type=utility --utility-sub-type=data_decoder....	238	37	48
		...lity --utility-sub-type=chrome.mojo...	332	112	57
		...lity --utility-sub-type=chrome.mojo...	332	112	57
		...nderer --disable-gpu-compositing --l...	258	41	47
		...lity --utility-sub-type=entity_extracti...	198	38	50

HTTP Requests 5 | Connections 39 | DNS Requests 39 | Threats 8

Filter by PID, name or url PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
6275 ms	GET | 304: Not Modifi...	?	3936	WINWORD.EXE		http://ctldl.windowsupdate.com/msdo...	
6277 ms	GET | 200: OK	?	3936	WINWORD.EXE		http://ctldl.windowsupdate.com/msdo...	68
7246 ms	GET | 200: OK	?	3936	WINWORD.EXE		http://x1.c.lencr.org/	7
7260 ms	GET | 200: OK	?	3936	WINWORD.EXE		http://x2.c.lencr.org/	29
37368 ms	GET | 304: Not Modifi...	?	1080	svchost.exe		http://ctldl.windowsupdate.com/msdo...	

Danger [2724] msedge.exe PHISHING has been detected (SURICATA)

Try community version for free! Register now

Pricing Contacts FAQ Sign In