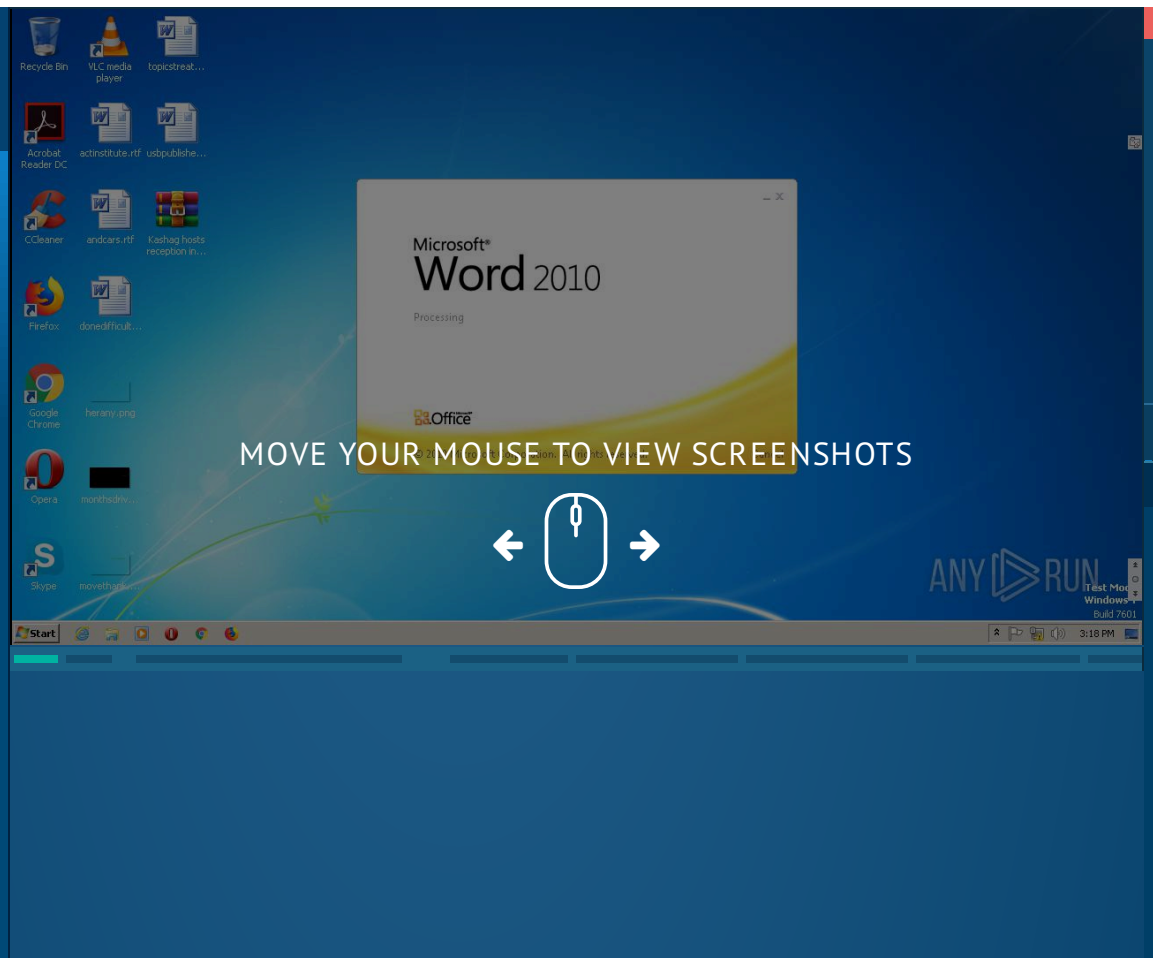

Malicious activity

Kashag hosts reception in honour of the ...

MD5: 1A02B20E9BA6C53B6AA32CCD45C51512

Start: 30.10.2019, 16:14 Total time: 570 s

Win7 64 bit Complete

trojan plugx

Indicators: Tracker: PlugX, Trojan

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

2064	WinRAR.exe	"C:\Users\admin\Desktop\Kashag hosts reception in ...	1k	510	196
1220	cmd.exe	/c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (C:\Users\a...	172	7	30
2272	cmd.exe	/c dir "C:\Users\admin\AppData\Local\Temp\K...	68	7	24
2504	mshta.exe	"C:\Users\admin\AppData\Local\Temp\Rar$D...	514	76	174
2520	cmd.exe	/c dir "C:\Users\admin\Desktop\Kashag hosts r...	60	7	24
2256	WMI 3.exe	PE	263	2	66
2004	unsecapp.exe	PE -app plugx	324	25	78
2564	WMI cmd.exe	/c "C:\Users\admin\AppData\Local\Temp\Kashag ...	326	500	43
2860	WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\Ka...	3k	1k	141

HTTP Requests 9 | Connections 13 | DNS Requests 3 | Threats 12 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
179.43 s	POST | No Response	?	2004	unsecapp.exe		http://103.85.24.186/update?wd=7aaff...	
211.18 s	POST | No Response	?	2004	unsecapp.exe		http://103.85.24.186/update?wd=0928...	
241.90 s	POST | No Response	?	2004	unsecapp.exe		http://103.85.24.186/update?wd=4381...	
403.69 s	POST | No Response	?	2004	unsecapp.exe		http://103.85.24.186:8080/update?wd=...	
405.74 s	GET | 200: OK	?	1540	mscorsvw.exe		http://ctldl.windowsupdate.com/msdo...	
436.46 s	POST | No Response	?	2004	unsecapp.exe		http://103.85.24.186:8080/update?wd=...	
449.77 s	GET | 200: OK	?	1276	mscorsvw.exe	?	http://crl.microsoft.com/pki/crl/produc...	7
449.77 s	GET | 200: OK	?	1276	mscorsvw.exe	?	http://crl.microsoft.com/pki/crl/produc...	5

Danger [2004] unsecapp.exe Connects to CnC server

Try community version for free! Register now