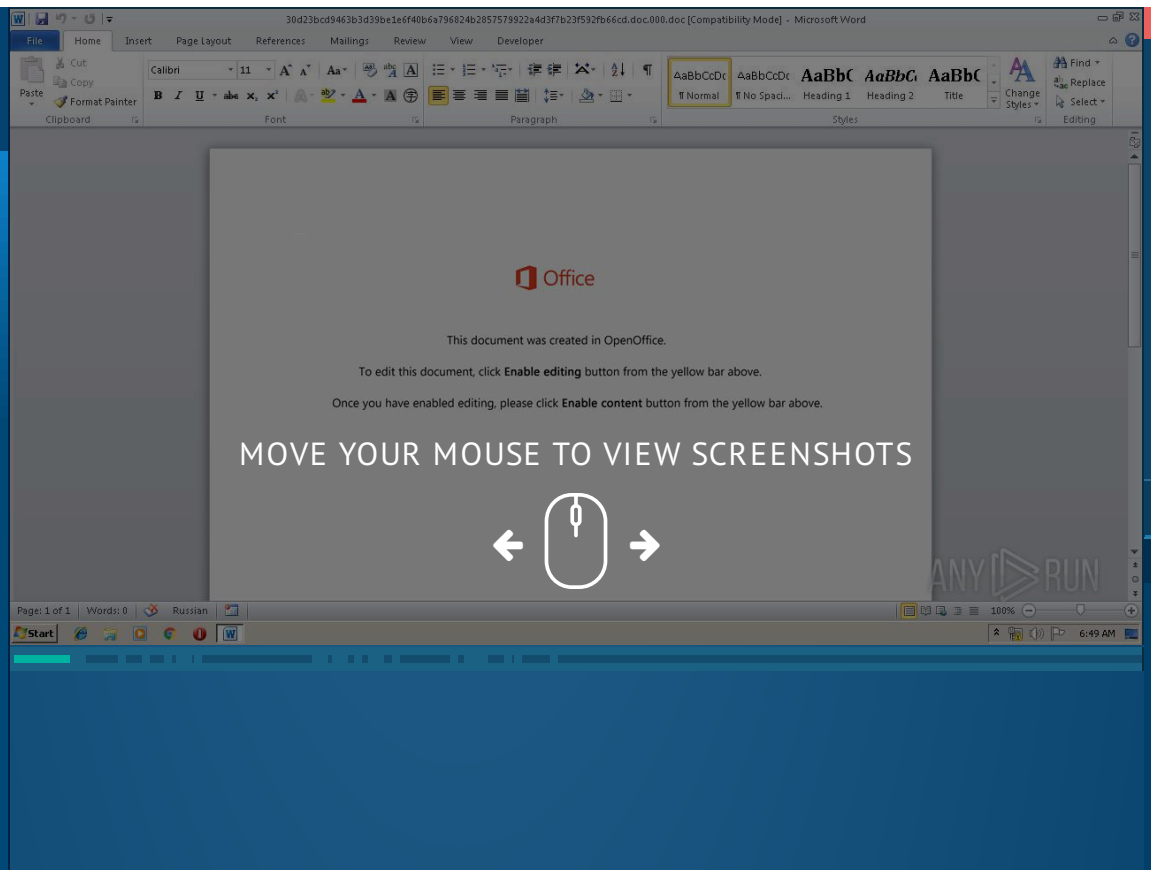

Malicious activity

Win7 32 bit Complete

30d23bcd9463b3d39be1e6f40b6a79682...

MD5: 45432466918693CEC1E63A34FA4999C3

Start: 29.11.2019, 07:48 Total time: 300 s

macros | macros-on-open | generated-doc | loader | trojan | emotet | stealer | emotet-doc

Indicators:

Tracker: Emotet, Loader, Stealer, 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

2240		WINWORD.EXE	/n "C:\Users\admin\AppData\Local\Temp\30d23b...	4k	1k	111
1296	WMI	powershell.exe	-w hidden -enco JABGAGwAeAByAGgAYwBm...	1k	540	218
3356		77.exe	PE	197	0	58
2572		77.exe	PE --800a80a	396	44	86
2884		serialfunc.exe	PE	178	0	58
4068		serialfunc.exe	PE --d6864438 emotet	729	32	142
3220		eUCxd691.exe	PE	179	0	58
3028		eUCxd691.exe	PE --c29cbba6 emotet	393	47	86
2028		serialfunc.exe	PE	155	0	58
3772		serialfunc.exe	PE --d6864438 emotet	394	20	
1992		serialfunc.exe	PE /scomma "C:\Users\a...	805	5	130
320		serialfunc.exe	PE "C:\Users\admin\AppD...	398	86	104
4072		serialfunc.exe	PE "C:\Users\admin\App...	387	115	106
2256		serialfunc.exe	PE /scomma "C:\Users\a...	6k	4	54

HTTP Requests 15 | Connections 11 | DNS Requests 1 | Threats 39 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5125 ms	GET | 200: OK	?	1296	powershell.exe		http://www.quintaesencialghero.com/d...	14
50169 ms	POST | No Response	?	4068	serialfunc.exe		http://77.211.249.124/BnCc9TDt0w	5
83962 ms	POST | No Response	?	4068	serialfunc.exe		http://81.213.145.45:443/uc6bcQ3zKC...	5
118.78 s	POST | No Response	?	4068	serialfunc.exe		http://41.218.118.66/1O63lB	5
129.02 s	POST | 200: OK	?	4068	serialfunc.exe		http://50.63.13.135:8080/1vuqr3Ttq	101
132.57 s	POST | 200: OK	?	4068	serialfunc.exe		http://50.63.13.135:8080/XX4nqxC	1

Danger [3772] serialfunc.exe Changes the autorun value in the registry

Try community version for free! Register now