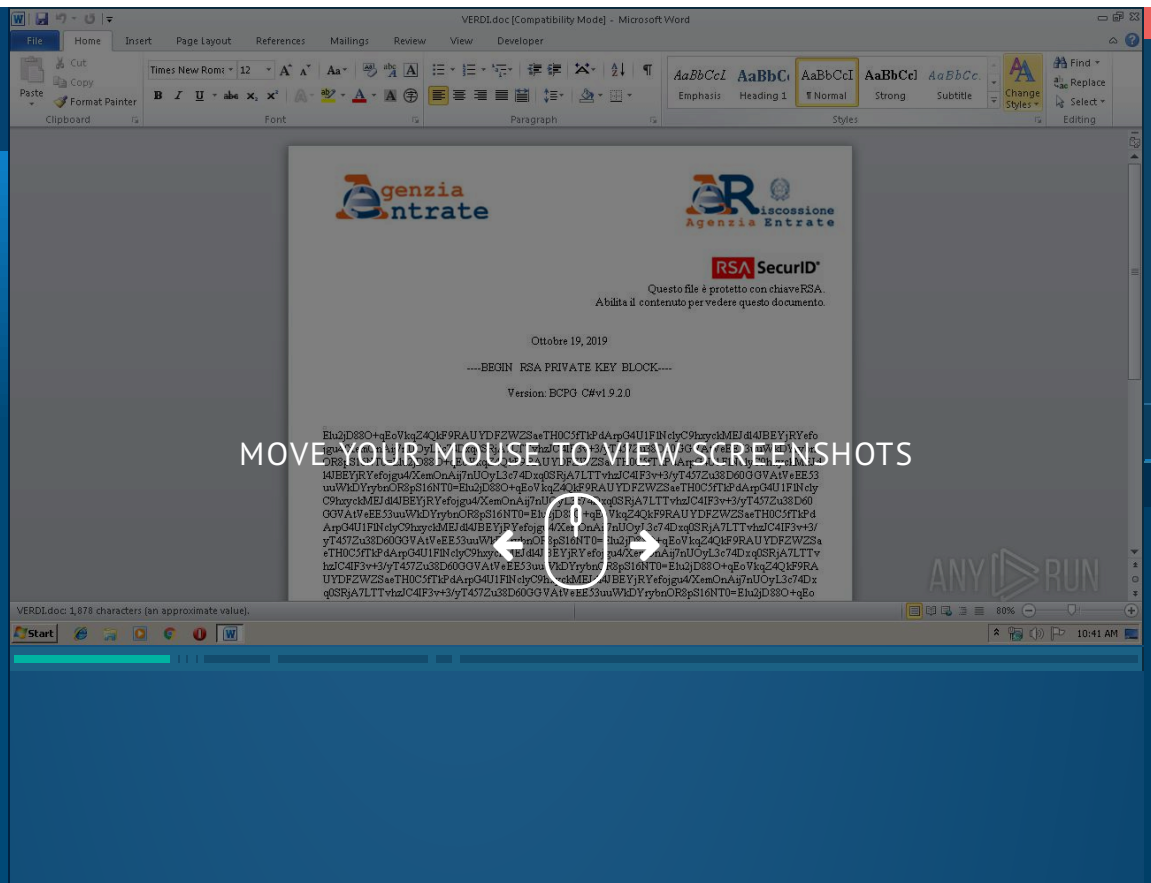

Malicious activity

VERDI.doc

MD5: AD30987A53B1B0264D806805CE1A2561

Start: 29.10.2019, 11:41 Total time: 120 s

Win7 32 bit Complete

macros ransomware maze trojan opendir

Indicators: Tracker: Maze, Ransomware, 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

2416 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Temp\VERDI.d... 3k 1k 296

3180 wupd12.14.tmp PE maze 9k 191 108

1744 wmic.exe shadowcopy delete 339 19 100

1036 wmic.exe shadowcopy delete 329 19 96

HTTP Requests 33 | Connections 28 | DNS Requests 0 | Threats 23 | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
6215 ms	GET | 200: OK	?	2416	WINWORD.EXE		http://104.168.198.208/wordupd.tmp	73
34879 ms	POST | No Response	?	3180	wupd12.14.tmp		http://91.218.114.4/transfer/xclpdu.jsp...	2
34883 ms	POST | 404: Not Found	?	3180	wupd12.14.tmp		http://91.218.114.4/transfer/xclpdu.jsp...	2
34884 ms	POST | No Response	?	3180	wupd12.14.tmp		http://91.218.114.4/ubdnm.action?j=0...	
34886 ms	POST | 404: Not Found	?	3180	wupd12.14.tmp		http://91.218.114.4/ubdnm.action?j=0...	2
34887 ms	POST | No Response	?	3180	wupd12.14.tmp		http://91.218.114.11/create/nii.html	2
34889 ms	POST | No Response	?	3180	wupd12.14.tmp		http://91.218.114.11/jcr.jspx?jv=qj7ypv...	

Warning [3180] wupd12.14.tmp Connects to server without host name

Try community version for free! Register now