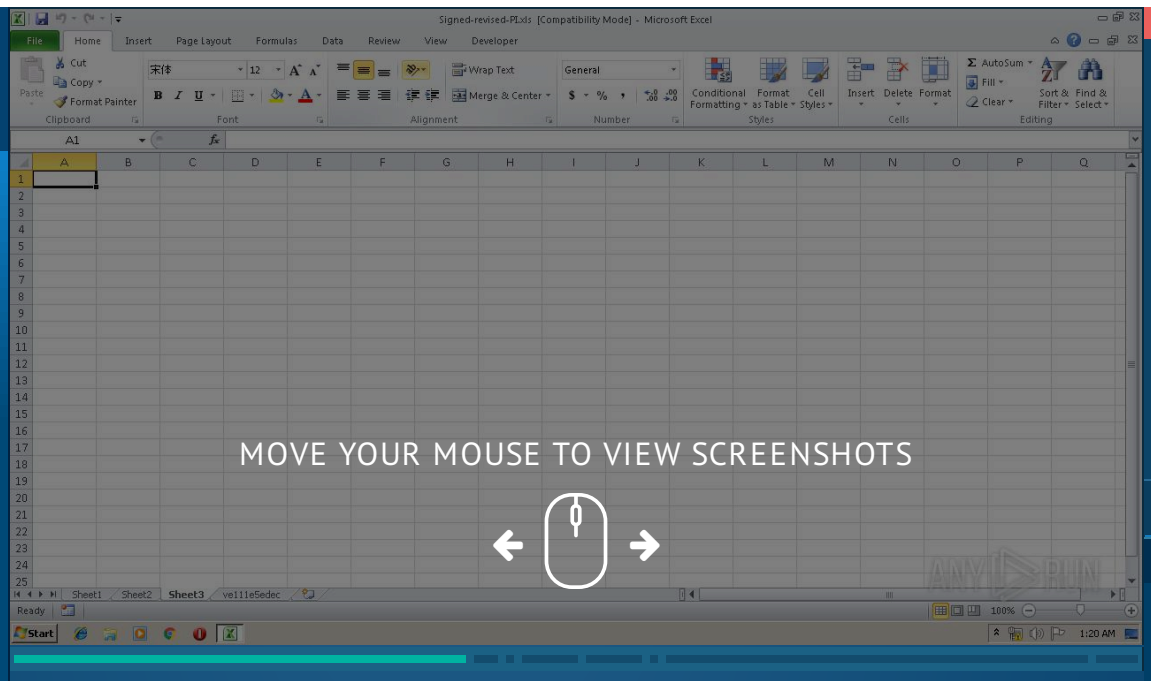

Malicious activity

Signed-revised-PI.xls

MD5: C081E4AA1FBEC4857E88E4FBF91FE90E
Start: 29.07.2019, 02:19 Total time: 45 s

Win7 32 bit
Complete

macros | macros-on-open | keylogger | agenttesla | evasion | trojan | rat

Indicators:

Tracker: Agent Tesla, Keylogger, Remote Access Trojan, 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

3864		EXCEL.EXE	/dde	1k	541	96
2764	WMI	powershell.exe	-WindowStyle Hidden function t63df7d { para...	1k	529	234
3504		csc.exe	/noconfig /fullpaths @"C:\Users\admin\AppData\Loc...	463	0	72
1080		cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OUT:...	95	0	24
2276		v4bc6f.exe	PE	636	351	84
2804		bin.exe	PE agenttesla	1k	94	100
3524		v4bc6f.exe	PE	61	0	38
3800		ipconfig.exe		80	0	25
584		cmd.exe	/c del "C:\Users\admin\AppData\Roaming\v4bc6f.exe"	59	6	24

HTTP Requests 1 | Connections 4 | DNS Requests 3 | Threats 3 — Filter by PID, name or url — PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
36161 ms	GET | 200: OK	?	2804	bin.exe		http://checkip.amazonaws.com/	

Info [2804] bin.exe Reads settings of System Certificates

Try community version for free! Register now