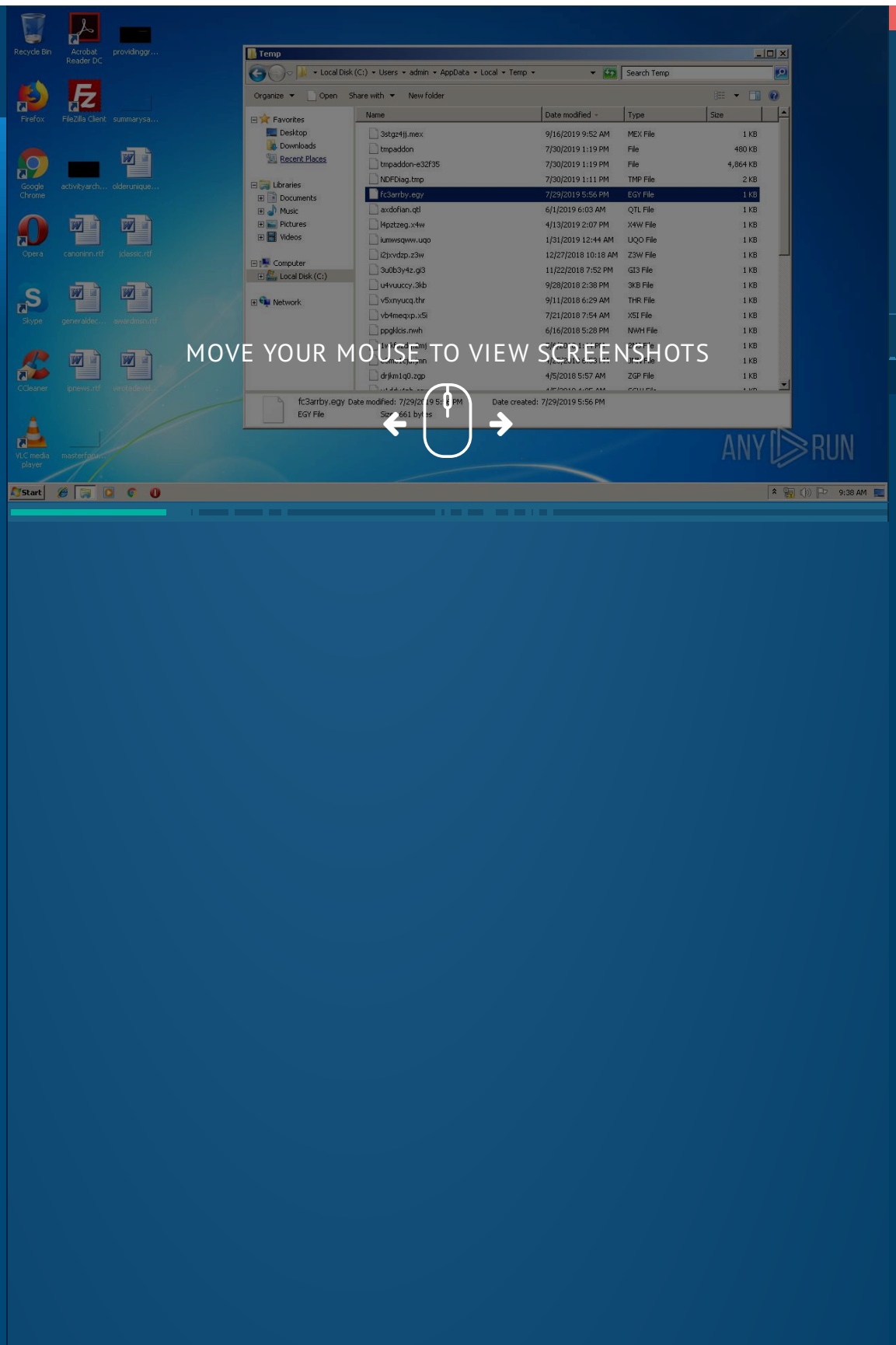

Malicious activity

suspected_formbook.exe

MD5: 949E9B782F6EC2B9D325D97BF93E9493
Start: 20.09.2019, 10:36 Total time: 180 s

Win7 32 bit Complete

trojan formbook stealer

Indicators: Tracker: Formbook, 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

276 SUS explorer.exe formbook 3k 632 212
2980 suspected_formbook.exe PE 49 0 28
3492 NETSTAT.EXE formbook 593 11 51
2240 cmd.exe /c del "C:\Users\admin\AppData\Local\Temp\s... 59 6 24
2284 Firefox.exe formbook 321 0 98
3372 firefox.exe 207 1 78
2248 firefox.exe 16k 122 272
3388 firefox.exe -contentproc --channel="2248.0.886644779... 535 0 176
2936 firefox.exe -contentproc --channel="2248.3.177219693... 5k 19 198
3420 firefox.exe -contentproc --channel="2248.13.42298528... 649 198 188
2500 firefox.exe -contentproc --channel="2248.20.91023290... 629 17 184
2752 pingsender.exe https://incoming.telemetry.mozilla.or... 797 44 158
3528 0pqftI0wnn.exe PE 46 0 28
3616 rundll32.exe 89 0 52
3104 COM Copy/Move/Rename/Delete/Link Object 169 39 58

HTTP Requests 17 | Connections 30 | DNS Requests 66 | Threats 24 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
35005 ms	GET | 302: Found	?	276	explorer.exe		http://www.victorcollege.com/h336/?_...	1
58554 ms	GET | 404: Not Found	?	276	explorer.exe		http://www.loveshe.ink/h336/?_DfXfV=...	3
60596 ms	POST | No Response	?	276	explorer.exe		http://www.loveshe.ink/h336/	3
60601 ms	POST | No Response	?	276	explorer.exe		http://www.loveshe.ink/h336/	
76980 ms	GET | No Response	?	276	explorer.exe		http://www.blueskyplusindicator.com/h...	
80052 ms	POST | No Response	?	276	explorer.exe		http://www.blueskyplusindicator.com/h...	3
80056 ms	POST | No Response	?	276	explorer.exe		http://www.blueskyplusindicator.com/h...	
82101 ms	GET | 200: OK	?	2248	firefox.exe	?	http://detectportal.firefox.com/succes...	

Info [2752] pingsender.exe Reads settings of System Certificates

Try community version for free! Register now