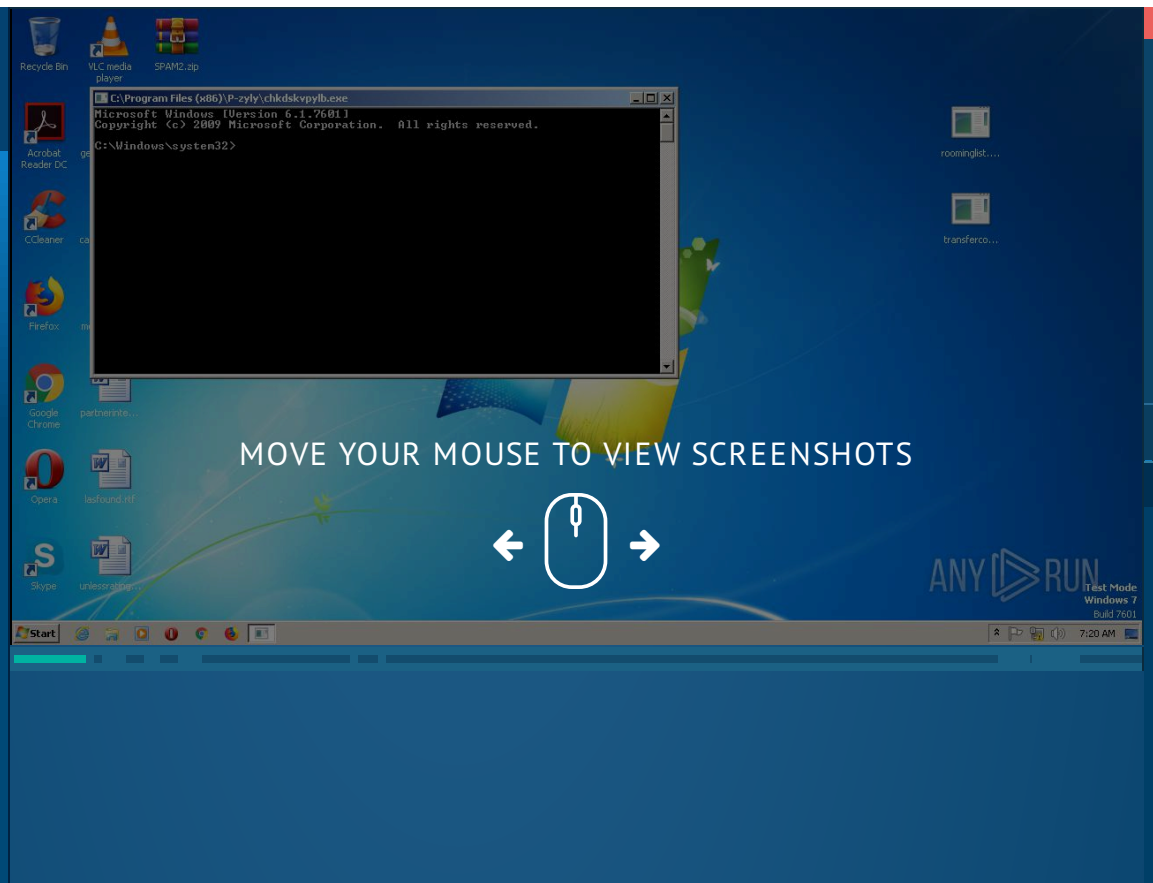

Malicious activity

SPAM2.zip

MD5: 8B76B587FC68D09AB41B72B1D08DBB9B

Start: 23.10.2019, 09:17 Total time: 416 s

Win7 64 bit Complete

trojan formbook stealer opendir

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

- 1936 SUS explorer.exe — formbook — 6k 4k 228
  - 3036 WinRAR.exe "C:\Users\admin\Desktop\SPAM2.zip" — 893 341 172
  - 1788 transfercopy.exe PE — 199 0 102
    - 2816 cmd.exe PE — 70 0 48
      - 1148 ipconfig.exe — formbook — 526 12 69
        - 884 cmd.exe PE — 93 0 50
        - 2064 Firefox.exe — formbook — 317 44 96
  - 1720 roominglist.exe PE — 918 72 206
    - 668 cmd.exe PE /C type nul > "C:\Users\admin\Desktop\ro... — 78 0 50
    - 3028 roominglist.exe PE — 70 0 48
  - 2628 transfercopy.exe PE — 207 0 102
    - 2288 cmd.exe PE — 5 0 6
    - 988 cmd.exe PE — 70 0 48
      - 344 cscript.exe — 122 0 54
        - 1008 roominglist.exe PE — 874 57 208
          - 2800 cmd.exe PE /C type nul > "C:\Users\admin\Desktop\r... — 78 0 50
          - 1812 roominglist.exe PE — 73 0 48
        - 1700 chkdskvpylb.exe PE — 65 0 28
        - 2948 msiexec.exe — 181 0 116
  - 68 0 50
  - e/Link Object — 178 50 58

HTTP Requests 22 | Connections 27 | DNS Requests 17 | Threats 40 | Filter by PID, name or url | PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
85829 ms	GET | No Response	?	1936	explorer.exe		http://www.moonchildenterprises.com...	
133.96 s	GET | 404: Not Found	?	1936	explorer.exe		http://www.pi2023.com/hx332/?8pMx2...	5
136.00 s	POST | No Response	?	1936	explorer.exe		http://www.pi2023.com/hx332/	3
136.01 s	POST | No Response	?	1936	explorer.exe		http://www.pi2023.com/hx332/	
137.05 s	POST | No Response	?	1936	explorer.exe		http://www.pi2023.com/hx332/	10
173.89 s	GET | No Response	?	1936	explorer.exe		http://www.lokmazel.com/hx332/?8pM...	
176.96 s	POST | No Response	?	1936	explorer.exe		http://www.lokmazel.com/hx332/	3
176.97 s	POST | No Response	?	1936	explorer.exe		http://www.lokmazel.com/hx332/	

Danger [2612] cmd.exe Application was dropped or rewritten from another process

Try community version for free! Register now