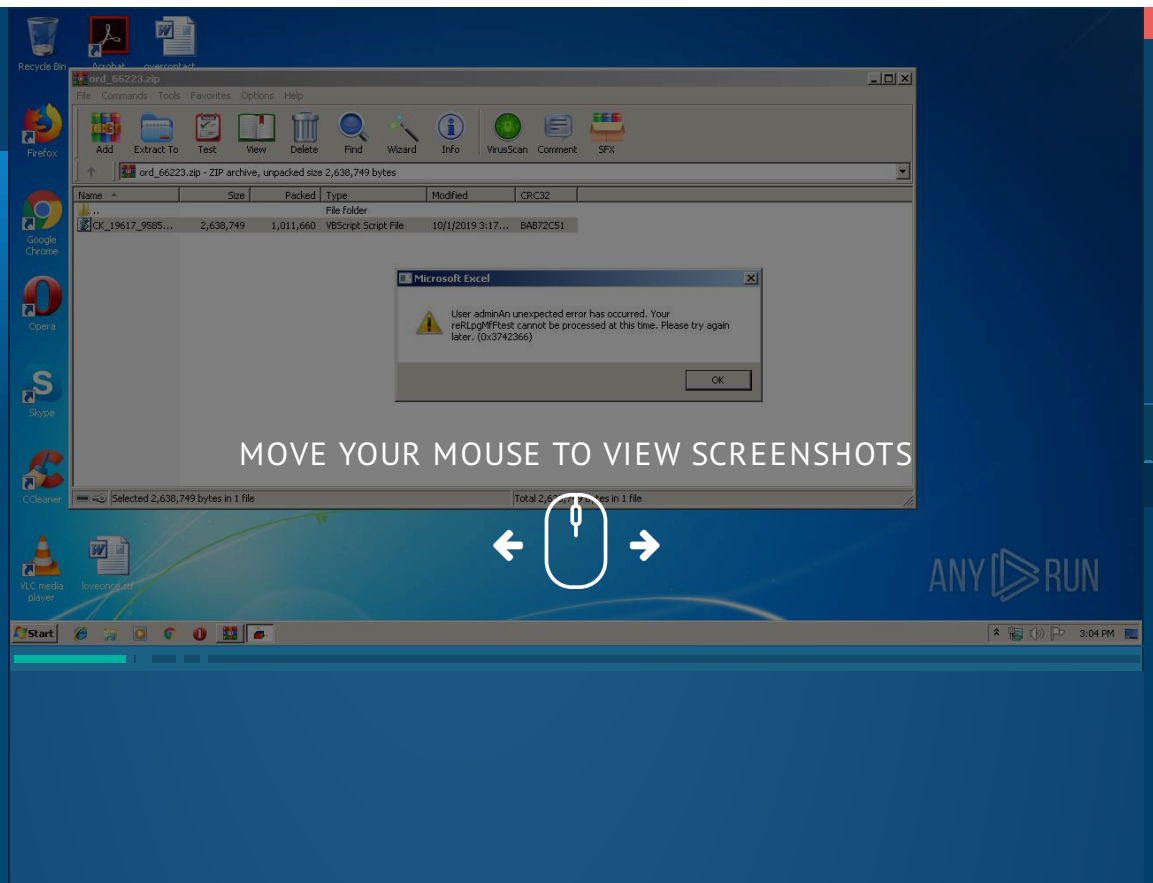

Malicious activity

ord_66223.zip

MD5: 81F39B11A731FDCB71FDADEA1DD8A54F
Start: 01.10.2019, 16:03 Total time: 205 s

Win7 32 bit
Complete

qbot trojan

Indicators: Tracker: Qbot, 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

- 3152 WinRAR.exe "C:\Users\admin\Downloads\ord_66223.zip" — 1k 453 196
  - 3944 WScript.exe "C:\Users\admin\AppData\Local\Temp\Rar$DIa3... — 1k 410 150
    - 960 WMI aNkxbUo.exe PE — qbot 463 65 98
      - 3264 aNkxbUo.exe PE /C — 97 0 64
        - 2188 ytfovlym.exe PE — 130 0 60
          - 2416 ytfovlym.exe PE /C — 96 0 64
          - 3484 explorer.exe — 141 1 47
        - 624 cmd.exe /c ping.exe -n 6 127.0.0.1 & type "C:\Windows\System... — 86 6 26
          - 3808 PING.EXE -n 6 127.0.0.1 — 68 2 44

HTTP Requests 0 | Connections 0 | DNS Requests 0 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content

No data

Danger [3484] explorer.exe Changes the autorun value in the registry

Try community version for free! Register now