

Case1 – Windows:

- Hostname: **Win11-JumpBX**
- Files:
 - o Case1-Windows-KAPE-and-RTW.7z
 - Artifacts:
 - EVTX
 - Artifacts of Execution
 - Browser Artifacts
 - MFT
 - Netstat
 - Autoruns
 - Pslist
 - DNS Cache
 - Services List
 - Common Executable Content in Writable Dirs (w/hash)
 - o Case1-Win11-SPOILERS.7z
- Timeline:
 - o 11/13/2024: download and execution of “mok.exe” (aka Laplink.exe)
 - http://[//]87.120.125.254/img/mok.exe
 - C:\Users\devuser\Downloads\mok.exe
 - o **Case1-Win11-JumpBX-web-and-exe-evtx.xlsx**
 - Review “yellow highlighted rows”
 - evtx-triage-output
 - hayabusa_events_offline
 - BrowserDownloadsView
 - BrowsingHistory
 - Timeline
 - o **Case1-Win11-JumpBX-pslist.xlsx** (review “yellow highlighted rows”)
 - o **Case1-Win11-JumpBX-netstat.xlsx** (review “yellow highlighted rows”)
 - o **Case1-Win11-JumpBX-autoruns.xlsx** (review “yellow highlighted rows”)
- General:
 - PowerShell execution
 - *.lnk files written to Start Menu
 - Reg key value changes
 - TCP/IP C2 (87.120.125.16) xMany

Case2 – Windows:

- Hostname: **Win11-JumpBX**
- Files:
 - o Case2-Windows-KAPE-and-RTW.7z
 - Artifacts:
 - EVTX
 - Artifacts of Execution
 - Browser Artifacts
 - MFT
 - Netstat
 - Autoruns
 - Pslist
 - DNS Cache
 - Services List
 - Common Executable Content in Writable Dirs (w/hash)
 - o Case2-Win11-SPOILERS.7z
- Timeline:
 - o 11/08/2025: Download and execution of “valid.exe”
 - skotes.exe, 2l3440.exe, axplong.exe, splwow64.exe, service123.exe
 - o **Case2-Win11-JumpBX-web-and-exe-evtx.xlsx**
 - Review “yellow highlighted rows”
 - hayabusa_events_offline
 - BrowserDownloadsView
 - Timeline
 - o **Case1-Win11-JumpBX-netstat.xlsx** (review “yellow highlighted rows”)
 - o **Case2-Win11-JumpBX-autoruns.xlsx** (review “yellow highlighted rows”)
 - o **Case2-Win11-JumpBX-mft_filtrlisting_executable_files.xlsx** (review “yellow highlighted rows”)
- General:
 - o DNS entries; DNS domains (Lumma?); opiniene.store
 - o IPs: 185.215.113.43; 89.105.201.183
 - o MFT: Beijing.bat, lots of *.exe's
 - o Tasks: axpong.job, skotes.job