Hawkeye Lab

Analysis report | 1.48.03

DEMO

LAB SIMULATION

HIGH (0/100) - 100 deducted Recovered from Lab staging - not a live incident.

TARGET	DWM	GENERATED	MODE
Notepad.exe | PID 26152	dwm.exe | PID 9908	2026-09-01 21:50:23	Demo | staged scene

ANALYSIS

This report is from a Lab demo (-demo).

Lab simulated high-risk behavior against the target. Detection recovered that scene.

Evidence is in DETECTION below.

Automated detection is a first look. Several checks need follow-up; they are not a verdict.

Checks also run against dwm.exe: risk software uses that process for anti-screenshot / anti-capture.

Demo note : Lab staged the scene; deductions show what detection recovered.

Staged scene (recovered)

Target Injection and integrity

- Unsigned module detected (Check 1). Lab inject_sim.
- Inline hooks detected (Check 5). Lab inline_hook_sim.
- User-mode RWX page detected (Check 16). Lab apages_sim.

DWM Injection and integrity

- Unsigned module detected (Check 2). Lab inject_sim.
- Inline hooks detected (Check 6). Lab inline_hook_sim.
- User-mode RWX page detected (Check 17). Lab apages_sim.

Cross-process and physical memory

- Cross-process read/write detected (Check 10). Lab cprw_sim.
- Physical page read detected (Check 18). Lab phyread_sim.
- MmMapIoSpace mapping detected (Check 19). Lab mapio_sim.

Anti-screenshot / hidden windows

- Hidden window detected (Check 11). Lab hidden_windows_sim.
- Hidden-from-capture Visual detected (Check 12). Lab hidden_visuals_sim.

Kernel executable pages

- Kernel thread OEP detected (Check 7). Lab apages_sim.
- ETW kernel page hit detected (Check 13). Lab apages_sim.
- Target ukexec detected (Check 14). Lab ukexec_sim.
- DWM ukexec detected (Check 15). Lab ukexec_sim.
- Kernel RWX page detected (Check 20). Lab apages_sim.

Needs confirmation (first look, not a verdict)

- Check 20 consecutive pages
- Check 9 CFG dispatch
- Check 4 busy-process certificates

No findings

- Check 3 System driver certificates: none
- Check 8 Hidden process/thread: none

APPENDIX | DETECTION

Machine evidence for the analysis above. Same content as the text report.

```
[Certificate Verification]
[Check 1] Target process module certificates (suspicious DLL injection)
  Status     : COMPLETED
  Modules    : 152 (PE: 152)
  Findings   : 1
  Breakdown  : no_path=0, missing=0, unsigned=1, broken=0
  Details:
    [ 1] [UNSIGNED]    C:\Hawkeye Lab\sim\HawkUnsignedStub.dll
  Assessment: Risk code runs in the target process context.
              Suspicious injection-type risk code may be present.
```

- 5

```
[Check 2] dwm.exe module certificates (anti-screenshot staging)
  Status     : COMPLETED
  Modules    : 99 (PE: 99)
  Findings   : 1
  Breakdown  : no_path=0, missing=0, unsigned=1, broken=0
  Details:
    [ 1] [UNSIGNED]    C:\Hawkeye Lab\sim\HawkUnsignedStub.dll
  Assessment: Suspicious modules detected in dwm.exe.
              Anti-screenshot techniques may be involved.
```

- 5

```
[Check 3] System (PID 4) driver module certificates
  Status     : COMPLETED
  Modules    : 223 (PE: 223)
  Findings   : 0
  Breakdown  : no_path=0, missing=0, unsigned=0, broken=0
  Result     : none
```

```
[Check 4] Busy process module certificates (system-wide injection sweep)
  Status     : COMPLETED
  Busy processes: 62
  Scanned    : 59 process(es) (excluded PID 4, Hawkeye, target, dwm.exe)
  Suspicious : 4 process(es)
  Details:
    [ 1] Suspicious modules in devenv.exe (PID 11972). Please verify.
         [UNSIGNED]
         C:\Users\38105\AppData\Local\Microsoft\VisualStudio\16.0_be33bc00\Extensions\14wghjs0.uh5\x86\tree-sitter.dll
         [UNSIGNED]
         C:\Users\38105\AppData\Local\Microsoft\VisualStudio\16.0_be33bc00\Extensions\14wghjs0.uh5\x86\tree-sitter-cpp.dll
    [ 2] Suspicious modules in CrossDeviceService.exe (PID 12948). Please verify.
         [UNSIGNED]    C:\Program Files\WindowsApps\MicrosoftWindows.CrossDevice_1.26071.84.0_x64__cw5n1h2txyewy\LibNanoAPI.dll
    [ 3] Suspicious process: PID 21128  C:\Program Files\Clash Verge\clash-verge.exe
         [UNSIGNED]    C:\Program Files\Clash Verge\clash-verge.exe
    [ 4] Suspicious process: PID 25532  C:\Program Files\Clash Verge\verge-mihomo.exe
         [UNSIGNED]    C:\Program Files\Clash Verge\verge-mihomo.exe
  Assessment: Please confirm these busy-process certificate results by hand.
              Automated detection is a first look, not a verdict. This sweep is not the staged target.
```

- 2

```
[Inline Hook Detection]
[Check 5] Target process inline hook scan (code integrity)
  Status     : COMPLETED
  PID        : 26152
  Modules    : 152 scanned, 0 skipped
  Hits       : 19 byte diff(s) across 1 module(s)
  Details:
    Module: C:\Hawkeye Lab\sim\HawkUnsignedStub.dll  base=0x7ff8cfb60000
      [ 1] 0x7ff8cfb61006  rva=0x1006 (15 bytes)  mem=0x90 file=0xcc
      [ 2] 0x7ff8cfb6103e  rva=0x103e  mem=0x90 file=0xcc
      [ 3] 0x7ff8cfb611a5  rva=0x11a5 (2 bytes)  mem=0x90 file=0xcc
      [ 4] 0x7ff8cfb6135d  rva=0x135d (2 bytes)  mem=0x90 file=0xcc
      [ 5] 0x7ff8cfb6139d  rva=0x139d (2 bytes)  mem=0x90 file=0xcc
      [ 6] 0x7ff8cfb614a6  rva=0x14a6  mem=0x90 file=0xcc
      [ 7] 0x7ff8cfb61519  rva=0x1519 (2 bytes)  mem=0x90 file=0xcc
      [ 8] 0x7ff8cfb615d6  rva=0x15d6  mem=0x90 file=0xcc
      [ 9] 0x7ff8cfb61649  rva=0x1649 (2 bytes)  mem=0x90 file=0xcc
      [10] 0x7ff8cfb61695  rva=0x1695 (2 bytes)  mem=0x90 file=0xcc
      [11] 0x7ff8cfb616d5  rva=0x16d5 (2 bytes)  mem=0x90 file=0xcc
      [12] 0x7ff8cfb617c5  rva=0x17c5 (2 bytes)  mem=0x90 file=0xcc
      [13] 0x7ff8cfb61852  rva=0x1852  mem=0x90 file=0xcc
      [14] 0x7ff8cfb61939  rva=0x1939 (2 bytes)  mem=0x90 file=0xcc
      [15] 0x7ff8cfb61cb5  rva=0x1cb5 (2 bytes)  mem=0x90 file=0xcc
      [16] 0x7ff8cfb61cc4  rva=0x1cc4 (11 bytes)  mem=0x90 file=0xcc
      [17] 0x7ff8cfb61d12  rva=0x1d12  mem=0x90 file=0xcc
      [18] 0x7ff8cfb61d1b  rva=0x1d1b (10 bytes)  mem=0x90 file=0xcc
      [19] 0x7ff8cfb61d32  rva=0x1d32 (19 bytes)  mem=0x90 file=0xcc
  Assessment: Inline hook modifications detected in the target process.
              In-memory code may differ from on-disk module images.
```

- 5

```
[Check 6] dwm.exe inline hook scan (anti-screenshot / overlay staging)
  Status     : COMPLETED
  PID        : 9908
  Modules    : 99 scanned, 0 skipped
  Hits       : 19 byte diff(s) across 1 module(s)
  Details:
    Module: C:\Hawkeye Lab\sim\HawkUnsignedStub.dll  base=0x7ff8cfb60000
```

- 5

```
    [ 1] 0x7ff8cfb61006  rva=0x1006 (15 bytes)  mem=0x90 file=0xcc
    [ 2] 0x7ff8cfb6103e  rva=0x103e  mem=0x90 file=0xcc
    [ 3] 0x7ff8cfb611a5  rva=0x11a5 (2 bytes)  mem=0x90 file=0xcc
    [ 4] 0x7ff8cfb6135d  rva=0x135d (2 bytes)  mem=0x90 file=0xcc
    [ 5] 0x7ff8cfb6139d  rva=0x139d (2 bytes)  mem=0x90 file=0xcc
    [ 6] 0x7ff8cfb614a6  rva=0x14a6  mem=0x90 file=0xcc
    [ 7] 0x7ff8cfb61519  rva=0x1519 (2 bytes)  mem=0x90 file=0xcc
    [ 8] 0x7ff8cfb615d6  rva=0x15d6  mem=0x90 file=0xcc
    [ 9] 0x7ff8cfb61649  rva=0x1649 (2 bytes)  mem=0x90 file=0xcc
    [10] 0x7ff8cfb61695  rva=0x1695 (2 bytes)  mem=0x90 file=0xcc
    [11] 0x7ff8cfb616d5  rva=0x16d5 (2 bytes)  mem=0x90 file=0xcc
    [12] 0x7ff8cfb617c5  rva=0x17c5 (2 bytes)  mem=0x90 file=0xcc
    [13] 0x7ff8cfb61852  rva=0x1852  mem=0x90 file=0xcc
    [14] 0x7ff8cfb61939  rva=0x1939 (2 bytes)  mem=0x90 file=0xcc
    [15] 0x7ff8cfb61cb5  rva=0x1cb5 (2 bytes)  mem=0x90 file=0xcc
    [16] 0x7ff8cfb61cc4  rva=0x1cc4 (11 bytes)  mem=0x90 file=0xcc
    [17] 0x7ff8cfb61d12  rva=0x1d12  mem=0x90 file=0xcc
    [18] 0x7ff8cfb61d1b  rva=0x1d1b (10 bytes)  mem=0x90 file=0xcc
    [19] 0x7ff8cfb61d32  rva=0x1d32 (19 bytes)  mem=0x90 file=0xcc
  Assessment: Inline hook modifications detected in dwm.exe.
              Anti-screenshot or overlay manipulation may be involved.
```

```
[Kernel Thread Entry Point Detection]
[Check 7] System (PID 4) kernel thread OEP scan (!threads -pid:4; regions 5/9)
```

- 8

```
  Status     : COMPLETED
  PID        : 4 (System)
  Threads    : 325 enumerated
  Findings   : 1 high-risk kernel OEP(s) in region 5 or 9
  Details:
    [ 1] TID=6300  OEP=0xFFFFAC808CE26000  region=9 ([system region])  protect=RWX
         Risk software executing from a kernel thread entry point outside the image region. Entry address: 0xFFFFAC808CE26000,
         kernel region 9 ([system region]), memory protection RWX, TID 6300.
  Assessment: Kernel thread entry point(s) fall outside the image region (regions 5 or 9).
              Risk software may be executing from non-module kernel memory.
```

```
[Hidden Process / Thread Detection]
[Check 8] System-wide hidden process and thread scan (!hidden_process)
  Status     : COMPLETED
  Scope      : system-wide (running vs reported process/thread lists)
  Hidden processes : 0
  Hidden threads   : 0
  Result     : none
```

```
[CFG Guard Dispatch Detection]
[Check 9] Kernel module iguard pit scan (regions 5/9/12)
  Status     : COMPLETED
  Modules    : 234 scanned, 1 with hits
  Findings   : 10 suspicious CFG target(s) in region 5/9/12
  Details:
    [ 1] [ntoskrnl.exe::0xFFFFF801E7E6BF00]->0xFFFF9A0495200000, region 5 [nonpaged region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E7E6BF00
         target : 0xFFFF9A0495200000  |  kernel region 5 [nonpaged region]  |  memory protection RWX
    [ 2] [ntoskrnl.exe::0xFFFFF801E7EEEF00]->0xFFFF9A0495400000, region 5 [nonpaged region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E7EEEF00
         target : 0xFFFF9A0495400000  |  kernel region 5 [nonpaged region]  |  memory protection RWX
    [ 3] [ntoskrnl.exe::0xFFFFF801E7EF0DC0]->0xFFFFF801762A0618, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E7EF0DC0
         target : 0xFFFFF801762A0618  |  kernel region 12 [image region]  |  memory protection RWX
    [ 4] [ntoskrnl.exe::0xFFFFF801E8201850]->0xFFFFF801762A0000, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201850
         target : 0xFFFFF801762A0000  |  kernel region 12 [image region]  |  memory protection RWX
    [ 5] [ntoskrnl.exe::0xFFFFF801E8201858]->0xFFFFF801762A0000, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201858
         target : 0xFFFFF801762A0000  |  kernel region 12 [image region]  |  memory protection RWX
    [ 6] [ntoskrnl.exe::0xFFFFF801E8201860]->0xFFFFF801762A000F, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201860
         target : 0xFFFFF801762A000F  |  kernel region 12 [image region]  |  memory protection RWX
    [ 7] [ntoskrnl.exe::0xFFFFF801E8201888]->0xFFFFF8017D9FC818, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201888
         target : 0xFFFFF8017D9FC818  |  kernel region 12 [image region]  |  memory protection RWX
    [ 8] [ntoskrnl.exe::0xFFFFF801E8201890]->0xFFFFF8017D9FC894, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201890
         target : 0xFFFFF8017D9FC894  |  kernel region 12 [image region]  |  memory protection RWX
    [ 9] [ntoskrnl.exe::0xFFFFF801E8201898]->0xFFFFF8017D9FC8F4, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E8201898
         target : 0xFFFFF8017D9FC8F4  |  kernel region 12 [image region]  |  memory protection RWX
    [10] [ntoskrnl.exe::0xFFFFF801E82018B0]->0xFFFFF8017D9FC96C, region 12 [image region], protection RWX.
         module : C:\WINDOWS\system32\ntoskrnl.exe  |  pit slot (CFG dispatch entry) : 0xFFFFF801E82018B0
         target : 0xFFFFF8017D9FC96C  |  kernel region 12 [image region]  |  memory protection RWX
  Assessment: Please confirm these CFG dispatch results by hand.
              Automated detection is a first look, not a verdict. Load symbols and run this check again for a clearer look.
```

```
[Cross-Process Read-Write Detection]
[Check 10] Target process cross-process memory access (!cross_rw)
```

- 50

```
  Status     : COMPLETED
  Target     : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Threads    : 178 sampled on CPU
  Findings   : 1 accessor process(es) with cross-process access
```

```
  Details:
    [ 1] [Hawkeye.exe::PID 13924]->target Notepad.exe (PID 26152), cross-process read-write, total score 304890
         accessor : C:\Hawkeye Lab\Hawkeye.exe  |  [PID:13924 tid:18088 ethread 0xFFFF9A04BCD130C0]  |  score 304890
  Assessment: Hawkeye read the target.
              Expected when Lab stages a cross-process read. Not attributed to an unknown accessor.
  Note: When another process accesses the target, a higher score means more frequent access, and a stronger lead.
        This is a serious risk signal: the target's memory may be getting remote access.
        Re-run this check by hand several times. Recurring hits are high risk; an occasional hit is medium risk.
```

```
[Hidden Window Detection]
[Check 11] Hidden window / anti-capture scan (!hidden_windows)                                    - 30
  Status     : COMPLETED
  Windows    : 1 hidden window candidate(s)
  Findings   : 1
  Details:
    [ 1] [Hawkeye.exe PID 13924] hidden window 0x50A3A detected
         window : Visible: Yes  Iconic: No   Layered: No   Size: 1280 x 800
         path   : C:\Hawkeye Lab\Hawkeye.exe
  Assessment: Hawkeye's own window.
              Lab window / anti-capture staging, not the target.
```

```
[Hidden Visual Detection]
[Check 12] Hidden-from-capture Visual scan (!hidden_visuals)                                      - 30
  Status     : COMPLETED
  DWM PID    : 9908
  Visuals    : 13 hidden-from-capture candidate(s) (raw scan)
  Findings   : 1 non-DWM process Visual(s) with readable owning PID
  Details:
    [ 1] [Hawkeye.exe PID 13924] hidden-from-capture Visual 0x000001EF7A859DD0 detected
         path   : C:\Hawkeye Lab\Hawkeye.exe
  Assessment: Hawkeye's own Visual.
              Lab overlay staging, not the target.
```

```
[ETW Kernel Code Page Detection]
[Check 13] ETW live sampling -- high-risk kernel executable pages (!etw -all)                     - 15
  Status     : COMPLETED
  Samples    : 10867 ETW RIP hit(s)
  Threads    : 171 thread(s) sampled
  Kernel RIP : 954 kernel address(es) examined (>0xFFFF000000000000)
  Findings   : 2 distinct high-risk kernel code page(s) (4 KiB merged)
  Details:
  Note: PID/TID/path below are the thread context at sample time, not ownership of the kernel page.
    [ 1] High-risk executable kernel code page at 0xFFFFAC80A0180000 ([system region], RWX)
         context : TID 2072  PID 4
         path    : System
         samples : 8206
         region  : [system region]
         protect : RWX
    [ 2] High-risk executable kernel code page at 0xFFFFF801762A0000 ([image region], RWX)
         context : TID 22592  PID 23612
         path    : C:\Windows\System32\spool\drivers\x64\3\E_YATISME.EXE
         samples : 1
         region  : [image region]
         protect : RWX
  Assessment: ETW sampling observed execution in a high-risk kernel code page (RX/RWX in [nonpaged]/[system], or RWX in [image]).
              Listed PID/TID/process path reflect the sampled thread context only; concealed kernel hooks or injected pages may
              run under arbitrary process contexts and must not be treated as implicating that process.
```

```
[User-Accessible Kernel Executable Page Detection]
[Check 14] Target process ukexec scan (!ukexec -pid:<target>)                                     - 10
  Status     : COMPLETED
  Process    : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Pages      : 1 user-accessible kernel executable page(s) scanned
  Findings   : 1
  Details:
    [ 1] PID 26152: user-accessible kernel executable page 0xFFFF800000000000 [[unknown region]]
         region : [unknown region]
         module : (unknown)
  Assessment: User-accessible kernel executable page(s) mapped into the target process CR3.
              This indicates possible kernel code injection directly reachable from application mode -- a technique used to
              avoid conventional DLL injection that is easier to detect.
```

```
[Check 15] dwm.exe ukexec scan (!ukexec -pid:<dwm>)                                               - 10
  Status     : COMPLETED
  Process    : PID 9908  C:\Windows\System32\dwm.exe
  Pages      : 1 user-accessible kernel executable page(s) scanned
  Findings   : 1
  Details:
    [ 1] PID 9908: user-accessible kernel executable page 0xFFFF800000000000 [[unknown region]]
         region : [unknown region]
         module : (unknown)
  Assessment: User-accessible kernel executable page(s) mapped into dwm CR3.
              Malware may inject kernel code reachable from dwm to evade conventional application-layer injection detection and
              support anti-screenshot or overlay staging.
```

```
[User-Mode RWX Active Page Detection]
[Check 16] Target process user-mode RWX active page scan (!active_pages -pid:<target> -rx:0, 2 passes merged)
  Status     : COMPLETED
```

```
  Process    : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Scans      : 2 passes merged (deduped by VA)
  Pass 1     : 22 driver page(s); 1 user finding(s)
  Pass 2     : 14 driver page(s); 1 user finding(s)
  Skipped    : 21 kernel page(s); 0 MEM_IMAGE page(s) (ZwQueryVirtualMemory)
  Findings   : 1 non-image user-mode RWX active page(s)
  FP/SIMD    : 1166 floating-point/SIMD instruction(s) total across reported page(s)
  Details:
    [1] heap/private RWX active page 0x000001E977B20000  (HEAP MEMORY)  FP/SIMD=1166
  Assessment: User-mode RWX active page(s) detected in the target process -- likely injected code (heap/private executable
              memory rather than a signed module image).
              Elevated per-page FP/SIMD counts may indicate overlay, rendering, or other graphics-adjacent injected logic. Any
              ZwQueryVirtualMemory protection contradiction is a severe concealment indicator.
```

```
[Check 17] dwm.exe user-mode RWX active page scan (!active_pages -pid:<dwm> -rx:0, 2 passes merged)
  Status     : COMPLETED
  Process    : PID 9908  C:\Windows\System32\dwm.exe
  Scans      : 2 passes merged (deduped by VA)
  Pass 1     : 13 driver page(s); 1 user finding(s)
  Pass 2     : 12 driver page(s); 1 user finding(s)
  Skipped    : 12 kernel page(s); 0 MEM_IMAGE page(s) (ZwQueryVirtualMemory)
  Findings   : 1 non-image user-mode RWX active page(s)
  FP/SIMD    : 1166 floating-point/SIMD instruction(s) total across reported page(s)
  Details:
    [1] heap/private RWX active page 0x000001EF03300000  (HEAP MEMORY)  FP/SIMD=1166
  Assessment: User-mode RWX active page(s) detected in dwm.exe -- likely injected code running outside normal module images.
              This pattern is associated with code staged in dwm for anti-screenshot or overlay-related behavior; review FP/SIMD
              counts per page for graphics-style injected logic.
```

```
[Physical Page Read Detection (MmCopyMemory)]
[Check 18] Target process phyread scan (!phys_read -pid:<target> -va:<hot>)                                    - 50
  Status     : COMPLETED
  Process    : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Hot VAs    : 2
  Rounds     : 2
  Findings   : 2 detected hot VA(s)
  Details:
    [1] Round 1/2  notepad.exe PE (0x7ff71bbc0000)
        DETECTED: VA 0x00007FF71BBC0000 scores=370 in ~0.2s window - concurrent kernel physical read (MmCopyMemory-style).
    [2] Round 2/2  ntdll.dll PE (0x7ff8e4f20000)
        DETECTED: VA 0x00007FF8E4F20000 scores=394 in ~0.2s window - concurrent kernel physical read (MmCopyMemory-style).
  Assessment: Suspicious MmCopyMemory (MM_COPY_MEMORY_PHYSICAL) physical-memory read activity was observed at 2 hot VA(s) in the
              target process: notepad.exe PE (0x7ff71bbc0000), ntdll.dll PE (0x7ff8e4f20000).
              This indicates kernel-side reads of the underlying page frames without normal user-mode virtual reads.
```

```
[Kernel I/O Memory Mapping Detection (MmMapIoSpace)]
[Check 19] Target process mapio scan (!map_io -pid:<target> -va:<hot> -cache:<0|1>)                            - 50
  Status     : COMPLETED
  Process    : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Hot VAs    : 2
  Rounds     : 4 (2 cache types per hot VA)
  Findings   : 4 detected round(s)
  Details:
    [1] Round 1/4  notepad.exe PE (0x7ff71bbc0000) cache:0 (MmNonCached)
        Result     : DETECTED
        Detail     : VA 0x00007FF71BBC0000 [cache:0 (MmNonCached)] - concurrent kernel MmMapIoSpace-style mapping of the target
        page (~0.2s window).
    [2] Round 2/4  notepad.exe PE (0x7ff71bbc0000) cache:1 (MmCached)
        Result     : DETECTED
        Detail     : VA 0x00007FF71BBC0000 [cache:1 (MmCached)] - concurrent kernel MmMapIoSpace-style mapping of the target
        page (~0.2s window).
    [3] Round 3/4  ntdll.dll PE (0x7ff8e4f20000) cache:0 (MmNonCached)
        Result     : DETECTED
        Detail     : VA 0x00007FF8E4F20000 [cache:0 (MmNonCached)] - concurrent kernel MmMapIoSpace-style mapping of the target
        page (~0.2s window).
    [4] Round 4/4  ntdll.dll PE (0x7ff8e4f20000) cache:1 (MmCached)
        Result     : DETECTED
        Detail     : VA 0x00007FF8E4F20000 [cache:1 (MmCached)] - concurrent kernel MmMapIoSpace-style mapping of the target
        page (~0.2s window).
  Assessment: Suspicious MmMapIoSpace kernel I/O memory mapping activity was observed at 4 hot target address round(s).
              Each round probes one MmMapIoSpace cache type (MmNonCached or MmCached). This indicates target page frames were
              temporarily mapped into kernel virtual address space.
```

```
[Kernel RWX Active Page Detection (dwm context)]
[Check 20] dwm.exe process-context kernel RWX active page scan (!active_pages -pid:<dwm> -rx:0, VA >= 0xFFFF000000000000)  - 30
  Status     : COMPLETED
  Process    : PID 9908  C:\Windows\System32\dwm.exe (kernel VA shared across processes)
  Driver RWX : 14 active page(s) returned by driver
  Skipped    : 0 user-mode page(s)
  Kernel     : 14 page(s) with VA >= 0xFFFF000000000000
  Read fail  : 7 kernel page(s) could not be read for disassembly stats
  Findings   : 14 kernel RWX active page(s)
  Details (one line per page):
    [1] 0xFFFF848B83674000  [specialPoolPaged region]  (page read failed)
    [2] 0xFFFF848B83675000  [specialPoolPaged region]  (page read failed)
    [3] 0xFFFF848B83676000  [specialPoolPaged region]  (page read failed)
```

```
  [4] 0xFFFF9A049B922000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
  [5] 0xFFFFAC8088024000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
  [6] 0xFFFFAC808F119000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:4
  [7] 0xFFFFAC80A22CD000  [system region]  simd:136  invlpg:68  mov_cr3:136  vt:201  junk:0
  [8] 0xFFFFAC80A22CE000  [system region]  (page read failed)
  [9] 0xFFFFAC80A22CF000  [system region]  (page read failed)
  [10] 0xFFFFAC80A22D0000  [system region]  (page read failed)
  [11] 0xFFFFAC80A22D1000  [system region]  (page read failed)
  [12] 0xFFFFAC8113232000  [system region]  simd:1  invlpg:0  mov_cr3:0  vt:0  junk:16
  [13] 0xFFFFAC8113233000  [system region]  simd:1  invlpg:0  mov_cr3:0  vt:0  junk:16
  [14] 0xFFFFAC81135D9000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:11
Assessment: Kernel RWX active page(s) observed while scanning dwm.exe. Re-run this check by hand several times.
            Recurring hits on consecutive pages that share the same read error, all-zero data, or identical content may be
            VT/EPT deception. ETW RIP sampling can assist the final call.
Note: 7 page(s) could not be read.
      Re-run this check by hand several times. Recurring hits on consecutive nearby pages that share the same read error,
      all-zero data, or identical content may be VT/EPT deception.
      ETW RIP sampling can assist the final call.
```