Hawkeye Lab

Analysis report | 1.48.03

LIVE

LIVE TARGET

LOW (97/100) - 3 deducted

TARGET	DWM	GENERATED	MODE
Notepad.exe | PID 26152	dwm.exe | PID 9908	2026-09-01 21:53:20	Live | target system

ANALYSIS

Live detection against the target. 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.

Kernel executable pages

- ETW kernel page hit detected (Check 13).
- Kernel RWX page detected (Check 20).

Needs confirmation (first look, not a verdict)

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

No findings

- Check 1 Target module certificates: none
- Check 2 dwm.exe module certificates: none
- Check 3 System driver certificates: none
- Check 5 Target inline hooks: none
- Check 6 dwm.exe inline hooks: none
- Check 7 Kernel thread OEP: none
- Check 8 Hidden process/thread: none
- Check 10 Cross-process read/write: none
- Check 11 Hidden windows: none
- Check 12 Hidden Visuals: none
- Check 14 Target ukexec: none
- Check 15 dwm.exe ukexec: none
- Check 16 Target user-mode RWX pages: none
- Check 17 dwm.exe user-mode RWX pages: none
- Check 18 Physical page read: none
- Check 19 MmMapIoSpace mapping: 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    : 151 (PE: 151)
  Findings   : 0
  Breakdown  : no_path=0, missing=0, unsigned=0, broken=0
  Result     : none
```

```
[Check 2] dwm.exe module certificates (anti-screenshot staging)
  Status     : COMPLETED
  Modules    : 97 (PE: 97)
  Findings   : 0
  Breakdown  : no_path=0, missing=0, unsigned=0, broken=0
  Result     : none
```

```
[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: 52
  Scanned    : 49 process(es) (excluded PID 4, Hawkeye, target, dwm.exe)
  Suspicious : 3 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 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    : 151 scanned, 0 skipped
  Hits       : 0 byte diff(s) across 0 module(s)
  Result     : none
```

```
[Check 6] dwm.exe inline hook scan (anti-screenshot / overlay staging)
  Status     : COMPLETED
  PID        : 9908
  Modules    : 97 scanned, 0 skipped
  Hits       : 0 byte diff(s) across 0 module(s)
  Result     : none
```

```
[Kernel Thread Entry Point Detection]
[Check 7] System (PID 4) kernel thread OEP scan (!threads -pid:4; regions 5/9)
  Status     : COMPLETED
  PID        : 4 (System)
  Threads    : 324 enumerated
  Findings   : 0 high-risk kernel OEP(s) in region 5 or 9
  Result     : none
```

```
[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)
  Status     : COMPLETED
  Target     : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Threads    : 161 sampled on CPU
  Findings   : 0 accessor process(es) with cross-process access
  Result     : none
```

```
[Hidden Window Detection]
[Check 11] Hidden window / anti-capture scan (!hidden_windows)
  Status     : COMPLETED
  Windows    : 0 hidden window candidate(s)
  Findings   : 0
  Result     : none
```

```
[Hidden Visual Detection]
[Check 12] Hidden-from-capture Visual scan (!hidden_visuals)
  Status     : COMPLETED
  DWM PID    : 9908
  Visuals    : 0 hidden-from-capture candidate(s) (raw scan)
  Findings   : 0 non-DWM process Visual(s) with readable owning PID
  Result     : none
```

```
[ETW Kernel Code Page Detection]
[Check 13] ETW live sampling -- high-risk kernel executable pages (!etw -all)
  Status     : COMPLETED
  Samples    : 15566 ETW RIP hit(s)
  Threads    : 278 thread(s) sampled
  Kernel RIP : 4682 kernel address(es) examined (>0xFFFF000000000000)
  Findings   : 1 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 0xFFFFF801762A0000 ([image region], RWX)
         context : TID 4272  PID 13924
         path    : C:\Hawkeye Lab\Hawkeye.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.
```

- 1

```
[User-Accessible Kernel Executable Page Detection]
[Check 14] Target process ukexec scan (!ukexec -pid:<target>)
  Status     : COMPLETED
  Process    : PID 26152  C:\Program
  Files\WindowsApps\Microsoft.WindowsNotepad_11.2607.14.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe
  Pages      : 0 user-accessible kernel executable page(s) scanned
  Findings   : 0
  Result     : none
```

```
[Check 15] dwm.exe ukexec scan (!ukexec -pid:<dwm>)
  Status     : COMPLETED
  Process    : PID 9908  C:\Windows\System32\dwm.exe
  Pages      : 0 user-accessible kernel executable page(s) scanned
  Findings   : 0
  Result     : none
```

```
[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     : 13 driver page(s); 0 user finding(s)
  Pass 2     : 15 driver page(s); 0 user finding(s)
  Skipped    : 15 kernel page(s); 0 MEM_IMAGE page(s) (ZwQueryVirtualMemory)
  Findings   : 0 non-image user-mode RWX active page(s)
  FP/SIMD    : 0 floating-point/SIMD instruction(s) total across reported page(s)
  Result     : none
```

```
[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     : 19 driver page(s); 0 user finding(s)
  Pass 2     : 21 driver page(s); 0 user finding(s)
  Skipped    : 21 kernel page(s); 0 MEM_IMAGE page(s) (ZwQueryVirtualMemory)
  Findings   : 0 non-image user-mode RWX active page(s)
  FP/SIMD    : 0 floating-point/SIMD instruction(s) total across reported page(s)
  Result     : none
```

```
[Physical Page Read Detection (MmCopyMemory)]
[Check 18] Target process phyread scan (!phys_read -pid:<target> -va:<hot>)
  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   : 0 detected hot VA(s)
  Details:
    [1] Round 1/2  notepad.exe PE (0x7ff71bbc0000)
        Not detected within ~0.2s: VA 0x00007FF71BBC0000 scores=0.
    [2] Round 2/2  ntdll.dll PE (0x7ff8e4f20000)
        Not detected within ~0.2s: VA 0x00007FF8E4F20000 scores=0.
```

```
[Kernel I/O Memory Mapping Detection (MmMapIoSpace)]
[Check 19] Target process mapio scan (!map_io -pid:<target> -va:<hot> -cache:<0|1>)
  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   : 0 detected round(s)
  Details:
    [1] Round 1/4  notepad.exe PE (0x7ff71bbc0000) cache:0 (MmNonCached)
        Result     : NOT DETECTED
        Detail     : VA 0x00007FF71BBC0000 [cache:0 (MmNonCached)] - no MmMapIoSpace-style mapping observed (~0.2s window).
    [2] Round 2/4  notepad.exe PE (0x7ff71bbc0000) cache:1 (MmCached)
        Result     : NOT DETECTED
        Detail     : VA 0x00007FF71BBC0000 [cache:1 (MmCached)] - no MmMapIoSpace-style mapping observed (~0.2s window).
    [3] Round 3/4  ntdll.dll PE (0x7ff8e4f20000) cache:0 (MmNonCached)
        Result     : NOT DETECTED
        Detail     : VA 0x00007FF8E4F20000 [cache:0 (MmNonCached)] - no MmMapIoSpace-style mapping observed (~0.2s window).
    [4] Round 4/4  ntdll.dll PE (0x7ff8e4f20000) cache:1 (MmCached)
        Result     : NOT DETECTED
        Detail     : VA 0x00007FF8E4F20000 [cache:1 (MmCached)] - no MmMapIoSpace-style mapping observed (~0.2s window).
```

```
[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)
  Status     : COMPLETED
  Process    : PID 9908  C:\Windows\System32\dwm.exe (kernel VA shared across processes)
  Driver RWX : 22 active page(s) returned by driver
  Skipped    : 0 user-mode page(s)
  Kernel     : 22 page(s) with VA >= 0xFFFF000000000000
  Read fail  : 8 kernel page(s) could not be read for disassembly stats
  Findings   : 22 kernel RWX active page(s)
  Details (one line per page):
    [1] 0xFFFF848B83492000  [specialPoolPaged region]  (page read failed)
    [2] 0xFFFF848B83674000  [specialPoolPaged region]  (page read failed)
    [3] 0xFFFF848B83675000  [specialPoolPaged region]  (page read failed)
    [4] 0xFFFF848B83676000  [specialPoolPaged region]  (page read failed)
    [5] 0xFFFF9A0495200000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:3
    [6] 0xFFFF9A0495400000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
    [7] 0xFFFF9A0495500000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
    [8] 0xFFFF9A0495501000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
    [9] 0xFFFF9A049B900000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:1
   [10] 0xFFFF9A049B901000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
   [11] 0xFFFF9A049B997000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
   [12] 0xFFFF9A04CE200000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
   [13] 0xFFFF9A04CE201000  [nonpaged region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
   [14] 0xFFFFAC8083EAC000  [system region]  (page read failed)
   [15] 0xFFFFAC8083EAD000  [system region]  (page read failed)
   [16] 0xFFFFAC8083EAE000  [system region]  (page read failed)
   [17] 0xFFFFAC8083EAF000  [system region]  (page read failed)
   [18] 0xFFFFAC8088024000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:0
   [19] 0xFFFFAC808F11A000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:2
   [20] 0xFFFFAC8113232000  [system region]  simd:1  invlpg:0  mov_cr3:0  vt:0  junk:14
   [21] 0xFFFFAC8113233000  [system region]  simd:0  invlpg:0  mov_cr3:0  vt:0  junk:13
   [22] 0xFFFFAC81135D9000  [system region]  simd:1  invlpg:0  mov_cr3:0  vt:0  junk:7
  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: 8 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.
```