INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:15 UTC

TrojPix Raises the Ceiling on Air-Gap Covert Channel Throughput, Physical Controls Remain the Only Defense

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0326
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Air-gapped systems with video output; demonstrated against nine unspecified monitor brands and fifteen unspecified video cable types, no specific vendor products named
Published	2026-07-06T04:50:54
Discovery Source	Rss

Executive Summary

Researchers at Shandong University have demonstrated TrojPix, a covert channel technique that exfiltrates data from air-gapped systems by manipulating on-screen pixel patterns to induce electromagnetic emissions in video cables, achieving throughput of 8.1 Mbps at up to 208 meters under lab conditions, according to The Hacker News. That rate is orders of magnitude above prior research in this class and means a 100 MB file could theoretically be exfiltrated in under two minutes, a threshold that materially changes the risk calculus for classified, critical infrastructure, and high-assurance environments that treated air-gap covert channels as impractically slow. The finding signals that physical isolation alone is no longer sufficient; organizations relying on air gaps as a primary control must re-evaluate whether their physical perimeter, RF shielding posture, and malware-prevention controls are adequate for this revised threat model.

Technical Analysis

TrojPix operates in two stages: first, malware must achieve a software foothold on the air-gapped host to control pixel rendering; second, the malware modulates on-screen pixel patterns in ways that encode data into electromagnetic emissions radiating from the video cable. A receiver positioned up to 208 meters away, no line-of-sight to the screen required, captures and decodes those emissions. The technique requires no hardware implant on the target system, which lowers the operational barrier relative to earlier hardware-based covert channel methods.

The throughput figure of 8.1 Mbps, reported by The Hacker News citing the Shandong University publication, is the central claim that elevates this research above its predecessors. Prior work in the same class, including RAMBO, AirKeyLogger, and PIXHELL, as cited in the item description, operated at kilobits-per-second rates, making them practical only for exfiltrating small artifacts such as cryptographic keys or short text strings over extended dwell time. At 8.1 Mbps, structured datasets, database dumps, or document archives enter the feasible exfiltration window within a single operational window, fundamentally altering the threat model.

Important caveats apply. This research originates from a single academic publication; independent replication has not been publicly confirmed. Lab conditions, controlled RF environment, specific cable types, receiver positioning, may not translate directly to operational environments with ambient RF noise, physical obstructions, or enterprise cable infrastructure. The research was tested against nine unspecified monitor brands and fifteen unspecified video cable types; no specific vendor products are named. No exploitation in the wild has been observed, and no CVE is assigned. The single-source provenance warrants treating the throughput figure as reported, not established fact pending replication.

MITRE ATT&CK mapping aligns the technique to T1020 (Automated Exfiltration), T1029 (Scheduled Transfer), T1041 (Exfiltration Over C2 Channel, applicable to the receiver-side collection), and T1052 (Exfiltration Over Physical Medium). The attack chain's dependency on a prior software foothold means the initial access and persistence stages remain the primary intervention points for defenders. The air-gap covert channel itself is the exfiltration mechanism, not the intrusion vector.

Defensive posture for environments where this threat is relevant centers on three layers: preventing the software foothold (supply chain integrity, removable media controls, strict application allowlisting); physical perimeter controls that limit receiver placement within 208 meters of cable runs (particularly relevant for facilities adjacent to public spaces, parking structures, or shared buildings); and RF shielding of sensitive cable infrastructure. Detection engineering targeting anomalous pixel pattern activity, unusual GPU rendering loads, unexpected display driver behavior, or scheduled screen-content changes correlated with no user session activity, represents an emerging but nascent detection surface.

Action Checklist

1. Step 1: Assess exposure, identify all air-gapped or network-isolated systems in your environment that have video output (monitors, display interfaces, KVM infrastructure); flag those in high-assurance, classified, OT/ICS, or critical infrastructure roles where the confidentiality bar is highest
2. Step 2: Audit software foothold prevention on air-gapped hosts, verify application allowlisting, removable media controls, and supply chain integrity practices; without initial malware access, TrojPix cannot execute; reference NIST AC-3 (Access Enforcement) and MP-7 (Media Use) for removable media governance on air-gapped hosts
3. Step 3: Evaluate physical perimeter controls, assess whether unauthorized personnel or equipment could be positioned within 208 meters of video cable runs, including parking areas, adjacent offices, shared building spaces, or public zones; enforce physical access restrictions per NIST PE-3 (Physical Access Control) and document proximity risk zones
4. Step 4: Review RF shielding posture, for Sensitive Compartmented Information Facilities (SCIFs), classified environments, or critical infrastructure control rooms, confirm that TEMPEST standards or equivalent RF shielding (Faraday caging, shielded cable standards) are current and inspected; reference NIST SP 800-53 PE-2 (Physical Entry) for perimeter access control and PE-3 (Physical Access Control) for cable infrastructure protection

5. Step 5: Develop or update detection logic for anomalous pixel/display activity, work with endpoint security and SIEM teams to identify signals such as unusual GPU rendering activity, unexpected display driver calls, or scheduled screen-content changes during off-hours or outside user sessions; reference NIST AU-2 (Audit Events) and AU-6 (Audit Record Review, Analysis, and Reporting) for log source coverage planning
6. Step 6: Update threat model, incorporate the revised air-gap covert channel throughput envelope into your high-assurance environment threat register; adjust assumed exfiltration dwell-time requirements downward from days/weeks to minutes for this attack class
7. Step 7: Monitor for independent replication, this is a single-source academic publication; track for peer replication, follow-on disclosures, or vendor advisories that would elevate confidence in the throughput claims and trigger a priority reassessment

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate to urgent if a credible peer replication of TrojPix throughput claims is published, if CISA issues a follow-on advisory naming specific affected products, or if physical surveillance indicators (unattended equipment, unauthorized personnel) are discovered within the 208-meter EM intercept envelope of a classified or OT/ICS facility — any of which would indicate movement from theoretical to operationally plausible threat.
Recovery Notes	Recovery for TrojPix is contingent on confirming and eradicating the required software foothold on the air-gapped host, as no exfiltration is possible without a resident payload manipulating display output. After removing any identified malicious process or persistence mechanism, verify display driver integrity against known-good hashes from the OS vendor, confirm application allowlisting policy is enforced and unchanged, and re-run the EM emissions survey (Step 4) to establish a clean-state baseline. Monitor GPU/display driver event logs and Sysmon output for 30 days post-eradication to detect any reinfection attempt through the same initial access vector (removable media or supply chain).
Forensic Artifacts	Running process list with parent-child relationships and loaded display DLLs (dxgi.dll, d3d9.dll, nvapi64.dll) captured from memory before any host isolation — a TrojPix payload would appear as a non-user-initiated process holding display API handles during off-hours or outside active sessions | Windows Sysmon Event ID 1 (Process Create) and Event ID 7 (Image Loaded) logs filtered for display driver DLL loads by unexpected parent processes, covering the period of suspected payload activity on the air-gapped host | Scheduled task registry export (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks) and cron job listings on Linux (/etc/cron.d/, /var/spool/cron/) — TrojPix requires timed or triggered execution to synchronize pixel pattern rendering with receiver operation, making persistence mechanisms a high-value artifact | GPU driver configuration registry keys (HKLM\SYSTEM\CurrentControlSet\Control\Video\) and display adapter device properties for evidence of unauthorized driver modification or parameter injection used to control pixel pattern output | Physical access control logs and CCTV retention for all entry points and exterior zones within 208 meters of identified video cable runs, covering the full suspected dwell-time window — these establish whether a receiver-equipped adversary was physically present during the period the host-side payload could have been active

Per-Action IR Details

Step 1: Assess exposure — identify all air-gapped or network-isolated systems in your environment that have video output (monitors, display interfaces, KVM infrastructure); flag those in high-assurance, classified, OT/ICS, or critical infrastructure roles where the confidentiality bar is highest

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing and maintaining IR capability, including asset inventory and risk identification for high-assurance environments

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-20 (Use Of External Systems)

Compensating: Export asset inventory from an existing CMDB or use a manual spreadsheet audit cross-referenced with physical walk-through of server rooms, OT/ICS control floors, and SCIFs. Use 'Get-PnpDevice -Class Monitor' (PowerShell) on Windows hosts or 'xrandr --query' on Linux to enumerate connected display interfaces per host. A two-person team can complete one facility tier per day using this method.

Evidence: Before acting on flagged systems, record current display topology: capture 'Get-PnpDevice' or 'xrandr' output, note KVM switch model and cable routing diagrams, and photograph physical cable runs. This baseline documents the pre-assessment display state and cable proximity to facility perimeters — the physical geometry that determines TrojPix receiver placement feasibility at up to 208 meters.

Step 2: Audit software foothold prevention on air-gapped hosts — verify application allowlisting, removable media controls, and supply chain integrity practices; without initial malware access, TrojPix cannot execute; reference NIST AC-3 (Access Enforcement) and AC-19 (Access Control for Mobile Devices) for removable media governance

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: implementing controls that prevent the precondition for an attack class, here the software foothold TrojPix requires on the air-gapped host to manipulate pixel rendering

Controls: NIST AC-3 (Access Enforcement), NIST AC-19 (Access Control For Mobile Devices), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: On Windows air-gapped hosts, audit AppLocker or Software Restriction Policy status via 'Get-AppLockerPolicy -Effective | Format-List'. For removable media, confirm Group Policy 'Removable Storage Access' restrictions with 'gpresult /H gp_report.html'. On Linux, verify removable media automount is disabled via 'systemctl status udisks2' and check /etc/udev/rules.d/ for block-device rules. A two-person team can script these checks across all flagged hosts using PSExec or Ansible ad-hoc commands.

Evidence: Before auditing or modifying any allowlisting or media control policy on a potentially compromised air-gapped host, capture volatile state: run 'Get-Process | Select-Object Name,Id,Path,StartTime' and 'Get-ScheduledTask | Where-Object {$_.State -eq "Running"}' to identify any active TrojPix-class payload that may already be manipulating GPU/display driver calls. TrojPix requires resident malware to trigger pixel pattern rendering; a running unauthorized process with display API hooks is the primary host-side indicator.

Step 3: Evaluate physical perimeter controls — assess whether unauthorized personnel or equipment could be positioned within 208 meters of video cable runs, including parking areas, adjacent offices, shared building spaces, or public zones; enforce physical access restrictions per NIST AC-3 and document proximity risk zones

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: identifying environmental and physical preconditions that enable an attack, specifically the 208-meter receiver standoff distance demonstrated for TrojPix EM emission interception

Controls: NIST AC-3 (Access Enforcement)

Compensating: Conduct a manual proximity survey using a building floor plan overlaid with a 208-meter radius drawn from each video cable run. Mark zones (parking structures, adjacent tenant spaces, public lobbies, exterior walls) that fall within range. Document findings in a simple risk register spreadsheet. No specialized tooling is required; a two-person team with a measuring wheel or laser rangefinder and building schematics can complete a single-facility survey in one working day.

Evidence: This step does not alter live system state and carries no order-of-volatility obligation. However, document the current physical access log baseline before any perimeter changes: pull badge reader access logs for the 90 days prior to the assessment for all entry points within the 208-meter envelope, and capture any CCTV footage retention windows. These records establish whether an adversary with a software-defined radio or purpose-built EM receiver has already been positioned within intercept range during the window a TrojPix payload could have been active.

Step 4: Review RF shielding posture — for Sensitive Compartmented Information Facilities (SCIFs), classified environments, or critical infrastructure control rooms, confirm that TEMPEST standards or equivalent RF shielding (Faraday caging, shielded cable standards) are current and inspected; reference CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) for baseline physical layer documentation

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: verifying that physical and environmental controls adequate to the threat class are in place and current, specifically RF/EM shielding that would neutralize TrojPix's interception channel

Controls: CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For environments without a formal TEMPEST program, conduct a practical shielding gap assessment: use a handheld SDR (e.g., RTL-SDR dongle with GNU Radio, cost under $30) to perform a passive EM emissions survey of video cable runs with a known test pattern displayed on-screen. Detectable signal at facility perimeter or adjacent spaces confirms shielding inadequacy. Document findings with signal strength readings and cable run locations for the risk register.

Evidence: This step does not alter live host state. Before engaging any RF testing equipment near operational systems, record the current display configuration state on all assessed hosts ('xrandr --verbose' or 'Get-DisplayResolution') and note active screen content schedules, as TrojPix emission intensity is directly coupled to pixel pattern content and refresh rate. This baseline allows post-assessment comparison if emissions are later attributed to an active payload rather than normal display operation.

Step 5: Develop or update detection logic for anomalous pixel/display activity — work with endpoint security and SIEM teams to identify signals such as unusual GPU rendering activity, unexpected display driver calls, or scheduled screen-content changes during off-hours or outside user sessions; reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) for log source coverage planning

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: developing threat-specific detection logic and identifying log sources capable of surfacing TrojPix host-side indicators, specifically GPU/display driver manipulation by a resident payload

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Deploy Sysmon with the SwiftOnSecurity baseline config and add a ProcessCreate rule (Event ID 1) filtering on processes invoking display driver DLLs (dxgi.dll, d3d9.dll, nvapi64.dll) from non-standard parent processes, and a FileCreate rule (Event ID 11) for unexpected writes to GPU driver config paths under HKLM\SYSTEM\CurrentControlSet\Control\Video\. On Linux, enable auditd rules for execve calls to /dev/dri/* and framebuffer device nodes. Write a Sigma rule targeting Sysmon EID 1 where ParentImage is not in an approved allowlist and CommandLine references display or render API entry points.

Evidence: Before enabling new logging or modifying Sysmon configuration on a potentially active host, capture current volatile state: dump running process list with parent-child relationships ('Get-CimInstance Win32_Process | Select-Object Name,ProcessId,ParentProcessId,ExecutablePath'), query loaded DLLs for display-related processes using Sysinternals ListDLLs or 'tasklist /m dxgi.dll', and export the current Sysmon operational log. A TrojPix payload would appear as a process with unexpected display API hooks executing during periods of no legitimate user graphical activity.

Step 6: Update threat model — incorporate the revised air-gap covert channel throughput envelope into your high-assurance environment threat register; adjust assumed exfiltration dwell-time requirements downward from days/weeks to minutes for this attack class

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: using new threat intelligence to update detection capabilities, response assumptions, and security posture; here specifically revising dwell-time and data-volume assumptions for air-gap covert channel exfiltration scenarios

Compensating: Update the existing threat register document (even a spreadsheet) to add a row for 'EM/video covert channel exfiltration' with throughput envelope: 8.1 Mbps max, 208-meter standoff, requiring prior software foothold. Annotate each high-assurance asset row with the revised exfiltration time estimate for its most sensitive data volume (e.g., a 1 GB classified dataset = ~16 minutes at peak claimed rate). Share the update in the next scheduled threat briefing with no additional tooling required.

Evidence: No live-system state is altered by this step; order-of-volatility sequencing does not apply. Reference the Shandong University TrojPix research publication and The Hacker News reporting (2024–2025 timeframe) as the intelligence basis. Document the source, claimed throughput figures (8.1 Mbps, 208 meters), lab conditions, and single-source status in the threat register entry to support future confidence reassessment when peer replication or vendor advisories emerge.

Step 7: Monitor for independent replication — this is a single-source academic publication; track for peer replication, follow-on disclosures, or vendor advisories that would elevate confidence in the throughput claims and trigger a priority reassessment

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrating cyber threat intelligence updates and monitoring for new information that would require revising the organization's response posture or escalating priority for this attack class

Controls: NIST AU-13 (Monitoring For Information Disclosure)

Compensating: Configure a free RSS or keyword alert (Google Alerts, Feedly free tier, or CISA RSS feed at cisa.gov/news) for search terms: 'TrojPix', 'air-gap covert channel video', 'EM exfiltration display cable', and 'TEMPEST covert channel'. Review weekly. Add a standing agenda item in the monthly threat intelligence review to check CISA ICS-CERT advisories and academic preprint servers (arXiv cs.CR category) for follow-on TrojPix research. A single analyst can maintain this watch with under 30 minutes per week.

Evidence: No live-system state is altered by this monitoring step. Maintain a running log of intelligence items collected, including source, date, claimed replication status, and any vendor (monitor manufacturer or video cable vendor) responses. If a vendor advisory naming a specific affected product is published, immediately re-run the Step 1 asset exposure assessment against that product's installed base — at that point physical system state may become relevant and order-of-volatility disciplines apply to any subsequent host investigation.

Detection Guidance

Detection for TrojPix is challenging because the exfiltration occurs via physical electromagnetic side-channel; no network traffic is generated. Detection engineering should focus on the preconditions and behavioral artifacts of the malware foothold stage, not the channel itself.

Endpoint signals to monitor:

- Anomalous GPU or display driver activity: unusual rendering calls, unexpected frame buffer writes, or high-frequency pixel pattern updates correlated with no active user session (AU-2, AU-6)

- Scheduled tasks or processes triggering display output changes outside business hours, particularly on isolated workstations or OT HMI terminals

- Unauthorized removable media insertion events on air-gapped hosts (MP-7; CIS 8.2)

- Application execution anomalies: processes accessing display driver APIs that are not part of the system's approved software baseline

Physical and environmental monitoring:

- RF anomaly detection in sensitive areas: consider deploying spectrum analyzers or TSCM (Technical Surveillance Countermeasures) sweeps for high-value facilities, particularly in frequency ranges associated with video cable emissions

- Physical access logs for areas within 208 meters of cable infrastructure, flag unescorted visitors, contractor access, or after-hours entries (NIST PE-3)

- Periodic inspection of cable shielding integrity for video runs in sensitive zones

Hunting hypotheses (per NIST AU-6):

- Hunt for processes on air-gapped hosts that write to display buffers or invoke GPU APIs without a corresponding logged user session

- Correlate any anomalous display driver crashes or performance spikes with time windows of interest

- On Windows hosts, review Windows Event Log for unexpected DXGI or DirectX subsystem activity outside normal application use

No IOCs (hashes, domains, IPs) are available from the source material for this research-stage technique. Detection at this stage is behavioral, not indicator-based.

Framework Mappings

MITRE-ATTACK

- **T1020** — Automated Exfiltration
- **T1029** — Scheduled Transfer
- **T1041** — Exfiltration Over C2 Channel
- **T1052** — Exfiltration Over Physical Medium

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SC-8** — Transmission Confidentiality and Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security
- **164.312(a)(1)** — Access Control

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1020	Automated Exfiltration	Exfiltration
T1029	Scheduled Transfer	Exfiltration
T1041	Exfiltration Over C2 Channel	Exfiltration
T1052	Exfiltration Over Physical Medium	Exfiltration

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/new-trojpix-attack-leaks-data-fro...	T2
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-07-06 15:15 UTC by TJS Security Command Center