INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:04 UTC

ACSC Flags Active ClickFix Campaign Delivering Vidar Stealer via Compromised WordPress Sites

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0287
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	WordPress sites (vulnerable themes and plugins), Windows endpoints, users exposed to Cloudflare-branded lure pages
Published	2026-05-07T14:00:59
Discovery Source	Rss

Executive Summary

Australia's Cyber Security Centre has confirmed an active campaign targeting Australian organizations and critical infrastructure, in which attackers compromise WordPress websites to trick employees into manually running malicious commands on their Windows machines. Those commands install Vidar Stealer, malware that silently harvests passwords, browser session tokens, cryptocurrency wallets, and sensitive files. Any organization whose employees access the internet on Windows endpoints faces credential theft risk, with particular exposure for teams accessing external WordPress-hosted content.

Technical Analysis

Threat actors compromise WordPress sites via vulnerable themes and plugins, injecting pages that impersonate Cloudflare CAPTCHA or browser verification prompts (CWE-1021: UI Redress; CWE-693: Protection Mechanism Failure). Victims are instructed to open the Windows Run dialog or PowerShell and paste a pre-loaded command from the clipboard (T1204.002, Malicious File, T1059.001, PowerShell). The command retrieves and executes Vidar Stealer, an infostealer typically distributed via MaaS infrastructure, that exfiltrates browser-stored credentials (T1555.003), session cookies (T1539), cryptocurrency wallet files (T1555), and arbitrary sensitive files via C2 channels (T1041) that may use legitimate web services for staging (T1102). Initial access relies on exploitation of vulnerable WordPress plugins and themes (T1190) and compromised supply-chain-adjacent infrastructure (T1195.002). Payload obfuscation (T1027, T1027.011) reduces static detection efficacy. No CVE is associated with the social engineering vector; the WordPress compromise vector exploits unpatched plugins and themes rather than a single named vulnerability. ACSC has published IoCs. Attribution is to unidentified ClickFix campaign operators leveraging the Vidar Stealer ecosystem. CWE

references: CWE-1021, CWE-693.

Action Checklist

1. Containment: Block known ACSC-published IoCs (domains, IPs, hashes) at DNS, proxy, and EDR layers immediately. Restrict outbound PowerShell network calls via Windows Defender Attack Surface Reduction rule: Block process creations originating from PSExec and WMI commands (ASR rule GUID: d1e49aac-8f56-4280-b9ba-993a6d77406c). Limit clipboard-paste execution where technically feasible (this may be aspirational depending on endpoint security tooling available).
2. Detection: Search EDR telemetry and Windows Event Logs for: PowerShell execution with encoded or Base64 arguments (Event ID 4104), Run dialog activity spawning powershell.exe or cmd.exe (Event ID 4688 with parent explorer.exe), and outbound connections to domains matching ACSC-published IoC lists. Query SIEM for typical stealer C2 patterns (T1102): HTTP POST to non-standard ports and connections to Telegram API or Steam community infrastructure, confirmed in this campaign per Microsoft threat intelligence. Review proxy logs for access to compromised WordPress domains in the IoC feed.
3. Eradication: Audit and patch all WordPress installations (themes, plugins, core) under organizational management or vendor control. Remove or disable unrecognized plugins. For any endpoint flagged in detection, isolate, image, and rebuild; Vidar Stealer establishes persistence and exfiltrates before most users notice. Rotate all credentials stored in browsers on affected endpoints immediately, prioritizing privileged accounts, VPN credentials, and cloud console logins.
4. Recovery: Validate remediation by re-running detection queries against cleaned endpoints after 24 hours. Confirm no outbound C2 traffic persists. Force re-authentication for all accounts whose credentials may have been harvested; treat all browser-stored passwords on affected machines as compromised. Enable MFA on all externally accessible systems if not already active. Monitor for account anomalies (new device logins, geographic outliers, privilege escalation attempts) for 30 days post-incident.
5. Post-Incident: This campaign succeeded because users could manually execute arbitrary commands in PowerShell without a technical barrier. Conduct a control gap review covering: user awareness of ClickFix-style lures, PowerShell execution policy enforcement (Constrained Language Mode or execution policy set to AllSigned/RemoteSigned), application of Windows ASR rules, and DNS filtering coverage. Update phishing simulation exercises to include clipboard-paste lure scenarios. Verify WordPress asset inventory is complete; shadow IT WordPress sites are a common gap.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if credential harvest is confirmed on any endpoint with access to regulated data (PII, PHI, financial records) or privileged infrastructure accounts — Vidar's documented exfiltration of browser-stored credentials and session tokens may trigger mandatory breach notification obligations under the Australian Privacy Act (Notifiable Data Breaches scheme), and stolen session tokens for cloud consoles or VPN gateways represent an active, ongoing lateral movement risk requiring executive-level containment authorization.

Recovery Notes	After endpoint rebuild and credential rotation, treat all browser-stored session tokens on affected machines as compromised — not just passwords — and force token invalidation across all SaaS platforms and cloud consoles, as Vidar specifically harvests session cookies that allow authentication bypass even after password resets. Monitor for 30 days post-incident for account anomalies including new device registrations, impossible-travel sign-ins, and privilege escalation attempts against any account whose credentials were stored on an affected endpoint. Validate WordPress remediation completeness by re-running WPScan against all organizational WordPress instances at 7-day and 30-day intervals, as this ACSC campaign actively retargets organizations with partially patched or shadow IT WordPress assets.
Forensic Artifacts	Windows Security Event Log (evtx) — Event ID 4688 process creation chains showing explorer.exe spawning powershell.exe with Base64-encoded arguments, and Event ID 4104 (PowerShell Script Block Logging) containing the full decoded ClickFix payload delivered via clipboard paste; these confirm the user-executed initial access vector specific to this campaign. | Browser credential store files — Chrome `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` (SQLite), Edge `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data`, and Firefox `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json` — Vidar Stealer directly targets these paths; timestamp metadata on these files confirms whether access occurred during the suspected compromise window. | Vidar dropper and configuration artifacts in `%TEMP%` and `%APPDATA%\Roaming` — Vidar typically stages its executable and an embedded or downloaded configuration file (containing C2 addresses, exfiltration targets, and module list) in user-writable temp directories; these files should be imaged and submitted to a sandboxed detonation environment (e.g., Any.run or Hybrid Analysis) for full behavioral analysis. | Network traffic logs showing outbound connections to Steam community profile URLs (`steamcommunity.com/profiles/*`) or Telegram Bot API endpoints (`api.telegram.org`) — Vidar uses these legitimate platforms for C2 configuration retrieval (MITRE T1102), making them appear benign in basic firewall logs; correlating these connections with the PowerShell execution timestamp confirms C2 staging activity. | WordPress web server access logs (Apache `/var/log/apache2/access.log` or Nginx `/var/log/nginx/access.log`) on any organizational or vendor-managed WordPress installations — look for POST requests to vulnerable plugin endpoints or wp-admin paths immediately preceding the injection of the Cloudflare-branded ClickFix lure page, which establishes the attacker's initial compromise vector and the full scope of affected WordPress assets.

Per-Action IR Details

Containment — Block known ACSC-published IoCs (domains, IPs, hashes) at DNS, proxy, and EDR layers immediately. Restrict outbound PowerShell network calls via Windows Defender Attack Surface Reduction rule: Block process creations originating from PSExec and WMI commands (ASR rule GUID: d1e49aac-8f56-4280-b9ba-993a6d77406c). Prevent clipboard-paste execution in Run/PowerShell where possible via Group Policy.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without enterprise DNS filtering, deploy Windows Hosts file blocks for ACSC-published Vidar C2 domains on all endpoints via a PowerShell GPO startup script: `Add-Content C:\Windows\System32\drivers\etc\hosts '0.0.0.0 '`. For ASR without Defender for Endpoint licensing, enforce PowerShell Constrained Language Mode via GPO

registry key: `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\__PSLockdownPolicy = 4`. Block clipboard-initiated execution by disabling the Windows Run dialog via GPO: `User Configuration > Administrative Templates > Start Menu and Taskbar > Remove Run menu from Start Menu`. Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (Process Create) filtering on `powershell.exe` and `cmd.exe` with parent `explorer.exe`.

Evidence: Before implementing blocks, capture a full packet capture (Wireshark/tcpdump) on any suspected endpoint to record live Vidar C2 beacon traffic — Vidar is known to use HTTP POST to non-standard ports and to stage through Telegram and Steam community pages (MITRE T1102). Export current Windows Defender firewall connection logs from `%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`. Pull DNS resolver cache on suspected endpoints via `ipconfig /displaydns` and export to file before DNS blocks are applied, preserving evidence of pre-block resolution attempts to compromised WordPress domains and C2 infrastructure.

Detection — Search EDR telemetry and Windows Event Logs for: PowerShell execution with encoded or Base64 arguments (Event ID 4104), Run dialog activity spawning powershell.exe or cmd.exe (Event ID 4688 with parent explorer.exe), and outbound connections to domains matching ACSC-published IoC lists. Query SIEM for Vidar-associated C2 patterns including HTTP POST to non-standard ports and connections to Telegram or Steam community infrastructure (known Vidar C2 staging channels per MITRE T1102). Review proxy logs for access to compromised WordPress domains in the IoC feed.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, use DeepBlueCLI (`Invoke-DeepBlue.ps1 -log Security`) against collected Windows Security Event Logs to surface Event ID 4688 chains showing `explorer.exe` → `powershell.exe` with Base64 arguments. For Event ID 4104 (PowerShell Script Block Logging), enable it via GPO if not active: `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockLogging = 1`, then parse logs with `Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational' | Where-Object {$_.Id -eq 4104} | Select-String 'base64\|encodedcommand\|iex\|downloadstring'`. For proxy log review, grep web proxy access logs for ACSC IoC domains using: `grep -iF -f acsc_ioc_domains.txt proxy_access.log`. Deploy the Sigma rule `proc_creation_win_powershell_base64_encoded_cmd.yml` (community Sigma repo) against Sysmon Event ID 1 logs using `sigma convert` with the Windows Event Log target.

Evidence: Collect Windows Security Event Log (evtx) from all Windows endpoints in scope before any remediation — specifically preserving Event ID 4688 entries showing process creation chains, and Event ID 4104 from `Microsoft-Windows-PowerShell/Operational` log showing full script block content of the ClickFix-delivered payload. Export browser credential stores prior to any deletion: Chrome vault at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` and Firefox logins at `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json` — Vidar specifically targets these paths and their timestamps confirm harvest timing. Capture network flow logs or proxy logs showing HTTP/HTTPS connections to Steam community profile URLs or Telegram API endpoints, which Vidar uses for C2 configuration retrieval (MITRE T1102 — Web Service).

Eradication — Audit and patch all WordPress installations (themes, plugins, core) under organizational management or vendor control. Remove or disable unrecognized plugins. For any endpoint flagged in detection, isolate, image, and rebuild — Vidar Stealer establishes persistence and exfiltrates before most users notice. Rotate all credentials stored in browsers on affected endpoints immediately, prioritizing privileged accounts, VPN credentials, and cloud console logins.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For WordPress audit without a commercial scanner, run WPScan (free tier: `wpscan --url https://your-site.com --enumerate vp,vt,u`) against all organizational WordPress instances to enumerate vulnerable plugins and themes. For endpoint imaging without enterprise tools, use Winpmem (`winpmem_mini_x64.exe output.raw`) to capture a full memory image of the affected endpoint before rebuild — this preserves in-memory Vidar artifacts and any injected code. For credential rotation tracking, generate a prioritized list via PowerShell: `Get-ChildItem 'HKCU:\Software\Microsoft\Internet Explorer\IntelliForms\Storage2'` and enumerate Chrome's Login Data SQLite file with `sqlite3 "Login Data" "SELECT origin_url, username_value FROM logins;"` to identify exactly which credentials were stored and thus likely harvested.

Evidence: Before wiping any flagged endpoint, acquire a forensic image using FTK Imager Lite (free) or `dd` to preserve: Vidar dropper binary typically staged in `%TEMP%`, `%APPDATA%\Roaming`, or user Downloads folder; Vidar persistence mechanism — check `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce` registry keys for any recently added entries pointing to temp or appdata paths; and the Vidar configuration file (often a `.cfg` or unnamed binary dropped alongside the main executable in `%TEMP%`). On the WordPress server side, capture web server access logs (Apache: `/var/log/apache2/access.log`; Nginx: `/var/log/nginx/access.log`) showing the attacker's initial compromise vector — look for requests exploiting vulnerable plugin endpoints (e.g., POST requests to `/wp-admin/admin-ajax.php` or vulnerable theme file upload paths) that preceded the malicious page injection.

Recovery — Validate remediation by re-running detection queries against cleaned endpoints after 24 hours. Confirm no outbound C2 traffic persists. Force re-authentication for all accounts whose credentials may have been harvested — treat all browser-stored passwords on affected machines as compromised. Enable MFA on all externally accessible systems if not already active. Monitor for account anomalies (new device logins, geographic outliers, privilege escalation attempts) for 30 days post-incident.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: Without a SIEM for 30-day anomaly monitoring, configure Azure AD (Entra ID) or on-premises AD audit logging to alert on new device registrations and impossible-travel sign-ins — both are available in free/basic tiers. For MFA enforcement without enterprise SSO, deploy Microsoft Authenticator via Conditional Access (free with Microsoft 365 Business Basic) or use Duo Security's free tier (up to 10 users). Re-run the Sysmon + DeepBlueCLI detection sweep from step 2 at 24-hour and 72-hour marks on rebuilt endpoints to confirm absence of Event ID 4688 PowerShell execution chains. For C2 traffic validation, run a 30-minute Wireshark capture on rebuilt endpoints filtering for `tcp.port != 80 && tcp.port != 443` to identify any unexpected outbound connections that may indicate reinfection or a missed persistence mechanism.

Evidence: Before forcing re-authentication, export Active Directory last-logon timestamps and source IP addresses for all accounts identified as potentially compromised (`Get-ADUser -Filter * -Properties LastLogonDate,LastLogonTimestamp | Export-CSV`) to establish a baseline for detecting post-incident unauthorized use. Capture and preserve Azure AD or on-premises AD sign-in logs covering the full suspected compromise window — Vidar harvests session tokens in addition to passwords, meaning attackers may use stolen tokens to authenticate without triggering password-based alerts. Document the exact set of browser-stored credentials confirmed present on each affected endpoint (from the SQLite export in the eradication step) as this defines the credential rotation scope and may trigger breach notification obligations if regulated data access credentials were harvested.

Post-Incident — This campaign succeeded because users could manually execute arbitrary commands in PowerShell without a technical barrier. Conduct a control gap review covering: user awareness of ClickFix-style lures, PowerShell execution policy enforcement (Constrained Language Mode or execution policy set to AllSigned/RemoteSigned), application of Windows ASR rules, and DNS filtering coverage. Update phishing simulation exercises to include clipboard-paste lure scenarios. Verify WordPress asset inventory is complete — shadow IT WordPress sites are a common gap.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For PowerShell Constrained Language Mode enforcement without enterprise tooling, deploy via GPO registry: `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\__PSLockdownPolicy = 4`; test coverage by running `$ExecutionContext.SessionState.LanguageMode` on endpoints — output must read `ConstrainedLanguage`. For shadow IT WordPress discovery, use Shodan (free community account) or Censys to query `org:"" http.title:"WordPress"` to surface unknown organizational WordPress instances. Build a ClickFix-specific phishing simulation using GoPhish (free, open source) with a scenario replicating the Cloudflare CAPTCHA lure and clipboard-paste execution prompt — measure click-through and execution rates as your baseline metric. Document all control gaps in a formal lessons-learned report per NIST 800-61r3 §4 and assign remediation owners with 30/60/90-day target dates.

Evidence: Retrieve and preserve the full IR case timeline — including first-evidence timestamp, detection timestamp, and containment timestamp — to calculate dwell time and mean time to detect (MTTD) and mean time to respond (MTTR) for this ClickFix/Vidar incident; these metrics are required inputs for the lessons-learned report and for any regulatory breach notification assessment. Preserve copies of the malicious WordPress page source and the ClickFix lure HTML/JavaScript as threat intelligence artifacts — these can be converted to YARA rules targeting the specific obfuscation patterns and clipboard-injection JavaScript used in this ACSC-documented campaign variant for future detection. Archive all ACSC IoC feeds consumed during this incident with their retrieval timestamps to document the intelligence-to-action timeline and identify any lag between ACSC publication and organizational blocking.

Detection Guidance

Primary detection surface is endpoint telemetry. Key signals: (1) powershell.exe or cmd.exe spawned by explorer.exe with command-line arguments containing Base64 strings, IEX (Invoke-Expression), or DownloadString; Windows Event ID 4104 (Script Block Logging must be enabled) and 4688 (Process Creation with command-line auditing enabled). (2) Run dialog activity (Event ID 4688, parent: explorer.exe, image: powershell.exe or cmd.exe), abnormal for most business users. (3) Outbound HTTP/HTTPS connections to domains and IPs in ACSC's published IoC list; check proxy and DNS resolver logs (IoCs available via ACSC Alerts portal at alerts.cyber.gov.au or vendor threat intelligence feeds). (4) Stealer C2 staging behavior (T1102): connections to Telegram API endpoints, Steam community profile pages, or other legitimate web services used as dead-drop C2, flag these when initiated by powershell.exe or newly spawned processes. (5) File system: creation of temp-directory executables or DLLs shortly after PowerShell execution. Cross-reference ACSC IoC feed hashes against endpoint AV/EDR quarantine logs and file creation events. Enable PowerShell Script Block Logging (HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging) if not active; this campaign is invisible without it.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`ACSC advisory IoC feed (see official ACSC advisory for current list)`	ACSC has published accompanying IoCs covering domains, IPs, and file hashes associated with this ClickFix/Vidar campaign. Retrieve directly from the ACSC advisory to ensure currency.	HIGH
DOMAIN	`Telegram API endpoints (api.telegram.org)`	Vidar Stealer uses Telegram as a C2 staging channel (T1102). Outbound connections to Telegram API from powershell.exe or spawned child processes are a behavioral indicator — not a block candidate in isolation, but a high-value detection signal in context.	MEDIUM
DOMAIN	`Steam community profile pages (steamcommunity.com)`	Vidar Stealer has historically used Steam community profiles as dead-drop C2 resolvers (T1102). Connections from non-browser processes to steamcommunity.com warrant investigation.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1056.001** — Keylogging
- **T1102** — Web Service
- **T1566** — Phishing
- **T1539** — Steal Web Session Cookie
- **T1041** — Exfiltration Over C2 Channel
- **T1190** — Exploit Public-Facing Application
- **T1555** — Credentials from Password Stores
- **T1059.001** — PowerShell
- **T1195.002** — Compromise Software Supply Chain
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File
- **T1555.003** — Credentials from Web Browsers
- **T1027.011** — Fileless Storage

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1056.001	Keylogging	Collection
T1102	Web Service	Command-And-Control
T1566	Phishing	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1555	Credentials from Password Stores	Credential-Access

Technique ID	Technique Name	Tactic
T1059.001	PowerShell	Execution
T1195.002	Compromise Software Supply Chain	Initial-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution
T1555.003	Credentials from Web Browsers	Credential-Access
T1027.011	Fileless Storage	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/australia-warns-of-c...	T3
New Threat ALERT! Hackers are exploiting WordPress themes with ...	https://www.facebook.com/thehackernews/posts/-new-threat-alert-hack...	T3
WordPress Had 11,334 Plugin Vulnerabilities Last Year. Cloudflare ...	https://dev.to/adioof/wordpress-had-11334-plugin-vulnerabilities-la...	T3
WordPress Compromises Advance Global Stealer Operation - Rapid7	https://www.rapid7.com/blog/post/tr-malicious-websites-wordpress-co...	T3
Think before you Click(Fix): Analyzing the ClickFix social ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/08/21/think-befo...	T1

Generated 2026-05-07 19:04 UTC by TJS Security Command Center