Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ClickFix distributing Vidar Stealer via WordPress targeting Australian infrastructure

Published: 7 May 2026

Table of contents

Overview

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has observed ClickFix associated activity leveraging WordPress hosted infrastructure to distribute the Vidar Stealer malware. This activity is targeting Australian infrastructure and organisations across multiple sectors. The campaign uses compromised WordPress websites to redirect victims to malware delivery mechanisms. This advisory provides an overview of the activity, an assessment of the threat, observed indicators, detections and recommended mitigations.

Background

ClickFix is a sophisticated social engineering technique observed since early 2024. It supports a range of malicious outcomes, including credential theft and financial compromise, through malware distribution.

ASD's ACSC has detected several variants of this attack. Notably, the large-scale Traffic Distribution System infrastructure detected in 2025, which was observed redirecting users to a ClickFix endpoint, among other attacks.

Since early 2026, ASD's ACSC has become aware of a number of attacks targeting Australian networks, using websites belonging to legitimate Australian businesses as a part of the ClickFix attack vector.

The technique leverages deceptive verification prompts via fake CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), to convince users to execute malicious commands or scripts. This user-driven execution bypasses some preventative security controls and enables the delivery of malware (Vidar in this campaign), increasing the likelihood of successful compromise across Australian networks.

Vidar Stealer is a well-known information stealing malware capable of exfiltrating credentials, browser data, cryptocurrency wallets, and system information, which may subsequently be used to facilitate follow-on malicious activity. Vidar Stealer primarily targets Windows systems.

Technical details

The ClickFix attack typically begins with an adversary injecting a malicious payload delivery domain into the compromised website. The injected payload domain loads JavaScript code from an external API server. This code overwrites the content of the legitimate page, presenting a fraudulent Cloudflare verification prompt.

The malicious JavaScript code retrieves additional content from the API server, including a PowerShell command, which is copied to the user's clipboard. Once the user selects the "Verify you are human" checkbox, a pop-up is displayed instructing the user to manually execute the copied command with administrative privileges.

Analysis of ClickFix-associated activity (in Windows environments) indicates that the obfuscated PowerShell command executed by the user contains a malware delivery URL, hosted on the same payload domain used to inject malicious ClickFix content into the compromised website. Upon execution, the command retrieves and launches the Vidar Stealer malware with minimal user visibility.

Once deployed, Vidar Stealer employs defence-evasion techniques, including self-deletion of the initial executable, enabling the malware to persist and operate primarily in memory. This behaviour reduces the effectiveness of forensic techniques.

Following installation, the malware establishes regular command-and-control (C2) communications. Initial C2 infrastructure is retrieved via dead-drop URLs, which commonly leverage publicly accessible services such as Telegram bots and Steam profiles to hinder detection and takedown efforts. Subsequent beaconing activity consists primarily of HTTP/S POST requests that exfiltrate stolen credentials and other sensitive information.

Observed MITRE ATT&CK techniques associated with ClickFix activity detected by, and reported to, ASD's ACSC are detailed in the Appendix.

Mitigations

ASD's ACSC recommends government entities, organisations, businesses and individuals implement the following guidance, aligned with ASD’s Information security manual, to reduce the risk of compromise by a ClickFix attack.

Application control

- Restrict execution of unauthorised or unapproved applications, including downloaded executables and scripts.
- Prevent execution of untrusted binaries delivered via browser-initiated activity.
- Limit the ability for user-initiated scripts (e.g. PowerShell) to launch secondary payloads.

Relevance: Prevents execution of Vidar Stealer and follow-on tooling delivered via ClickFix.

Patch applications

- For website administrators, ensure WordPress, plugins, themes, browsers, and scripting engines are fully patched and up to date.
- For website administrators, remove unused, unsupported, or deprecated WordPress plugins and themes.
- Prioritise patching of internet-facing applications.

Relevance: Reduces exploitation of WordPress vulnerabilities used for initial website compromise.

User application hardening

- Consider restricting browser-based scripting (ie. JavaScript) and iframe execution to allow-listed websites only.
- Block or limit clipboard write access from browser-based JavaScript and untrusted web content.

Relevance: Directly mitigates ClickFix techniques that rely on clipboard manipulation and browser-based social engineering.

Restrict administrative privileges

- Ensure users with administrative privileges are restricted from executing scripts or commands unless explicitly required.
- Enforce least-privilege principles and review privileged account usage regularly.

Relevance: Reduces impact of ClickFix instructions that prompt users to run commands as administrators.

Patch operating systems

- Ensure operating systems are kept fully patched with the latest security updates.
- Apply patches promptly to endpoints and servers, particularly those exposed to the internet.

Relevance: Limits post-compromise exploitation and privilege escalation opportunities.

Multi-factor authentication (MFA)

- Enforce phishing-resistant MFA for:
  - Administrative accounts
  - Remote access services
  - Cloud services and externally accessible systems

Relevance: Reduces the impact of credential theft performed by Vidar Stealer by requiring MFA to access sensitive information.

Regular backups

- Maintain regular, tested, and offline backups of critical systems and web content.
- Ensure backup integrity and restoration processes are validated.

Relevance: Supports recovery from website compromise or malware-related incidents.

Network and DNS controls

- Filter inbound and outbound HTTP/S traffic and restrict connections to approved destinations.
- Use protective DNS services to block known malicious domains.

Relevance: Prevents systems from resolving to attacker-controlled domains, including malware distribution sites and C2 infrastructure.

PowerShell controls

- Enforce PowerShell code signing policies.
- Restrict PowerShell from making outbound network connections unless allow-listed.

Relevance: Restricts execution of PowerShell commands for malicious delivery.

Data loss prevention (DLP)

- Monitor for suspicious outbound POST requests and unencrypted data transfers.
- Identify critical sensitive data and implement DLP controls to prevent unauthorised exfiltration of that data.

Relevance: Limits the impact of successful Vidar Stealer infection by detecting or preventing the exfiltration of sensitive data.

Security awareness training

- Educate users on ClickFix-style social engineering.
- Reinforce guidance to never copy, paste, or execute commands from websites or pop-ups.

Relevance: Disrupts attack at the earliest stage by reducing the likelihood of a user executing commands copied from a malicious page.

Appendix

Appendix A – Mitre ATT&CK tactics, techniques and procedures

Mitre ATT&CK Techniques observed in ClickFix incidents detected by and reported to ASD's ACSC in 2026.

Table 1: ClickFix distributing Vidar Stealer techniques for resource development

Technique title	ID	Use	Detection ID
Compromise Infrastructure: Web Services	T1584.006	Adversary leverages legitimate domain infrastructure to use as attack vector.	DET0882
Acquire Infrastructure: Domains	T1583.001	Adversary obtains domains to use for ClickFix attacks, payload delivery and C2 Infrastructure.	DET0892
Obtain Capabilities: Malware	T1588.001	Adversary obtains Vidar Stealer to steal sensitive information.	DET0845
Obtain Capabilities: Exploits	T1588.005	Adversary obtains exploits to compromise legitimate WordPress webpages.	DET0827

Table 2: ClickFix distributing Vidar Stealer techniques for initial access

Technique Title	ID	Use	Detection ID
Drive-By Compromise	T1189	Legitimate website compromised. Adversary utilises built-in web application interface, allowing for insertion of the malicious script and ClickFix iFrame.	DET0176

Table 3: ClickFix distributing Vidar Stealer techniques for execution

Technique Title	ID	Use	Detection ID
Command and Scripting Interpreter: PowerShell	T1059.001	Adversary utilises PowerShell commands to download and deploy a malware executable from the internet.	DET0455
User Execution: Malicious Copy and Paste	T1204.004	Adversary relies upon a user pasting the PowerShell command – which has been copied to their clipboard by a malicious script – into the command line as administrator.	DET0340

Table 4: ClickFix distributing Vidar Stealer techniques for defence evasion

Technique Title	ID	Use	Detection ID
Obfuscated Files or Information	T1027	PowerShell command which is copied to the user's clipboard is heavily obfuscated. This makes detection of the malware delivery URL or analysis of the command difficult.	DET0505
Indicator Removal: File Deletion	T1070.004	Upon execution the file will delete itself and exist in memory to evade detection and prevent analysis of the executable file.	DET0140

Table 5: ClickFix distributing Vidar Stealer techniques for command and control

Technique Title	ID	Use	Detection ID
Application Layer Protocol: Web Protocols	T1071.001	Adversary uses POST requests to carry stolen information to the C2 server while blending in with normal HTTP/S traffic.	DET0027
Web Service: Dead Drop Resolver	T1102.001	Adversary leverages Telegram bots and Steam profiles as dead drop resolvers which contain C2 server details. This masks the network communications to appear legitimate.	DET0058

Table 6: ClickFix distributing Vidar Stealer techniques for exfiltration

Technique Title	ID	Use	Detection ID
Exfiltration Over C2 Channel	T1041	Adversary exfiltrates the data stolen by the Vidar Stealer over an existing command and control channel.	DET0348

Indicators of compromise (IOC)

For a downloadable copy of IOCs observed, see Clickfix-Vidar-IOC (CSV, 6 KB)

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre