

NCA-23.261026 – National CERT Advisory

Zero-Click Spyware Through Targeted Online Advertisements (AdFection): Potential Risks to Mobile Devices, Networks and Sensitive Information

Overview

National CERT Pakistan has reviewed recent cybersecurity research published by Citizen Lab on 15 October 2026, documenting a sophisticated spyware delivery technique known as “**AdFection**.” The research describes how malicious actors may exploit digital advertising infrastructure to profile users and deliver mercenary spyware through targeted advertisements displayed on websites and mobile applications. Unlike conventional phishing campaigns, this technique may not require a user to click a link, open an attachment or take any other deliberate action. Under certain conditions, a malicious advertisement may deliver code that attempts to exploit vulnerabilities in a browser, application or device.

The Citizen Lab report describes a high-confidence finding that devices at Al Jazeera were targeted and infected with Candiru spyware through this technique. It also discusses the use of advertising infrastructure to reach devices across multiple countries and sectors. However, the appearance of an advertisement or an advertising impression alone does not establish that a device was targeted, exploited or infected. This advisory highlights the potential risks associated with abuse of the digital advertising ecosystem and suggests measures that organizations and individuals may consider to strengthen device security, reduce exposure and improve their ability to detect and respond to suspected spyware activity.

Document Summary

Item	Details
Threat	AdFection: potential spyware delivery through targeted online advertising
Threat category	Mercenary spyware, targeted surveillance and exploitation of digital advertising infrastructure
Potential severity	High impact in targeted cases; actual risk depends on the target, device, software vulnerabilities and attacker capabilities
Potential attack vector	Online advertisements and real-time bidding systems
User interaction	May not be required in a zero-click attack
Potential impact	Unauthorized surveillance, information exposure, device compromise and access to sensitive communications
Relevant systems	Mobile devices, browsers, applications and devices used to access sensitive information
Primary reference	Citizen Lab research published on 15 October 2026

Threat Overview

Potential attack sequence

A campaign using this technique may involve the following stages:

1. **Advertisement delivery:** An advertisement is delivered to a device through an online advertising network or publisher.
2. **Device profiling:** Advertising-related information may be used to distinguish devices or identify users of interest.
3. **Target selection:** Selected devices may be prioritised for further action based on information available to the operator.
4. **Malicious code delivery:** In a targeted case, an advertisement or related infrastructure may deliver code intended to interact with the device, browser or application.
5. **Vulnerability exploitation:** If the device contains a suitable vulnerability, the delivered code may attempt to exploit it.
6. **Potential spyware infection:** Successful exploitation may allow spyware to operate on the device and access information or activities, depending on the capabilities of the malware and the level of compromise.

The sequence may differ between campaigns. The delivery of an advertisement does not, by itself, establish that the later stages occurred.

Significance of Threat

Traditional awareness measures often focus on avoiding suspicious links, attachments and downloads. These remain useful, but they may not prevent every zero-click attack. Targeted spyware campaigns can exploit vulnerabilities without requiring an obvious user action, making software maintenance, secure device configuration, monitoring and specialist incident response particularly important.

Potential Impact

If a device is successfully compromised, the possible consequences may include:

- **Surveillance of communications:** Access to messages, call-related information, contacts or other communications, depending on the spyware's capabilities.
- **Exposure of sensitive information:** Access to files, photographs, account information or other data available to the compromised device.
- **Credential and session risks:** Potential exposure of authentication information or active sessions, depending on the nature and extent of compromise.
- **Device and application compromise:** Unauthorized activity affecting the browser, applications or operating environment.
- **Organizational information exposure:** Risks to sensitive government, corporate, research, media or other institutional information accessed through a targeted device.

- **Targeted monitoring:** Persistent or selective surveillance of individuals considered of interest to an attacker.
- **Follow-on security incidents:** Potential misuse of information obtained from a compromised device to support further attacks.

The actual impact would depend on the exploit used, the device and operating-system version, the privileges obtained and the spyware's capabilities.

Threat Characteristics

Characteristic	Description
Delivery mechanism	Targeted online advertising and associated advertising infrastructure
Possible interaction user	A click or download may not be necessary
Targeting	May involve selection of particular users or devices
Exploitation	May depend on vulnerabilities in the operating system, browser or application
Detection challenges	Activity may not resemble conventional phishing or malware delivery
Evidence exposure of	Advertising impressions alone are insufficient to confirm targeting or infection
Defensive focus	Timely updates, secure configurations, device management, monitoring and appropriate incident response

Indicators of Possible Exposure or Compromise

There may be no obvious user-facing signs of a sophisticated spyware infection. Nevertheless, organizations may wish to consider the following information when assessing a suspected incident:

- A credible device-manufacturer or platform-provider threat notification.
- A relevant alert from a trusted security provider or threat-intelligence source.
- Security-tool alerts indicating suspicious device, browser or application behaviour.
- Unexpected configuration changes, unfamiliar applications or unexplained security-setting changes.
- Unusual account activity or access inconsistent with normal use.
- Forensic findings indicating exploitation, unauthorized access or spyware-related activity.
- Corroborated reporting of a targeted campaign relevant to the device, user or organization.

These observations are not conclusive on their own. Unusual battery consumption, device heating or performance issues, for example, can have many causes and should not automatically be treated as evidence of spyware.

Similarly, the receipt or display of an advertisement does not confirm that a device was targeted or compromised.

Recommended Security Measures

Organizations and individuals may consider the following measures to reduce exposure to spyware and other targeted threats.

- Organizations may consider deploying reputable ad-blockers and browser-level protections to reduce exposure to potentially malicious advertisements. These should complement, rather than replace, other security controls.
- Organizations are encouraged to preserve relevant historical DNS, firewall, proxy, web gateway, EDR and other available security logs to support retrospective exposure assessment and incident investigation.

Device and software security

- Keep operating systems, browsers and applications updated, preferably using automatic updates where appropriate.
- Use devices that continue to receive security updates from their manufacturers.
- Review the availability of relevant security updates and follow the guidance issued by device and software vendors.
- Consider replacing unsupported devices where they are used to access sensitive information.
- Install applications from trusted sources and review application permissions periodically.
- Review device configuration and remove applications or profiles that are no longer needed or cannot be verified.

Account and information protection

- Use strong, unique passwords and multifactor authentication for important accounts.
- Review account recovery options, active sessions and connected devices periodically.
- Consider limiting the amount of sensitive information stored on mobile devices.
- Use organizationally approved secure communication and data-storage arrangements for sensitive work.
- Where feasible, separate high-risk or sensitive activities from routine browsing and general-purpose device use.

Organizational controls

- Maintain an inventory of devices used to access sensitive organizational systems and information.
- Consider mobile device management (MDM) and endpoint security controls appropriate to the organization's risk profile.
- Apply proportionate security requirements to personnel whose roles involve sensitive information or high-value accounts.
- Review browser, application and device security settings against vendor guidance and organizational requirements.

- Consider advertising, web-filtering or network-monitoring controls as supplementary safeguards, while recognising that these may not block every targeted or zero-click attack.
- Include targeted spyware and zero-click exploitation in relevant security-awareness and incident-response planning.

These measures can reduce risk but cannot guarantee protection against a sophisticated, targeted exploit.

Monitoring and Detection

Organizations may wish to strengthen monitoring through a combination of technical controls and established security processes:

- Review alerts generated by endpoint protection, mobile device management and other approved security tools.
- Monitor for unexpected application installations, configuration changes and suspicious device behaviour.
- Track relevant security advisories issued by device manufacturers, operating-system vendors and trusted cybersecurity organizations.
- Review available authentication and account-access logs when a device or user account is suspected of compromise.
- Preserve relevant logs and security alerts in accordance with the organization's retention and incident-response procedures.
- Consider specialist mobile-device forensic analysis where credible indicators suggest a targeted spyware incident.

Routine antivirus scanning or the absence of security alerts should not, by itself, be treated as confirmation that a device is free from sophisticated spyware.

Response to Suspected Compromise

Where a device may have been targeted or compromised, the following response steps may be appropriate:

1. **Assess the concern:** Record the circumstances, relevant alerts, device details and any credible threat notifications.
2. **Seek specialist advice:** In cases involving sensitive information, senior officials, high-risk personnel or critical functions, consider contacting the organization's incident-response team or a qualified digital-forensics specialist.
3. **Consider containment:** Based on the circumstances and expert advice, consider isolating the device or limiting its access to organizational accounts and networks.
4. **Preserve evidence:** Where a formal investigation may be required, seek forensic guidance before resetting the device, deleting applications or making substantial changes that could destroy evidence.

5. **Protect associated accounts:** From a separate, trusted device, consider reviewing account sessions, credentials and recovery settings where account exposure is suspected.
6. **Recover safely:** Restore or replace the device in accordance with the findings and the organization's recovery procedures, and ensure relevant security updates are applied.
7. **Document and report:** Record the assessment, actions taken and findings through the organization's incident-management process.

A factory reset or ordinary antivirus scan may not reliably identify or resolve every sophisticated spyware infection. Recovery decisions are best based on the circumstances and, where warranted, specialist forensic advice.

Platform Threat Notifications and Additional Protections

Some technology providers issue targeted threat notifications when they believe a user may have been individually targeted by sophisticated spyware. Where such a notification is received, it may be helpful to verify it through the provider's official account or support channels rather than relying on links in an unsolicited message.

Apple provides guidance for users who receive Apple threat notifications and offers **Lockdown Mode** for individuals who may face an elevated risk of highly targeted cyberattacks. Organizations using other platforms may wish to consult the relevant manufacturer's official security guidance for comparable protections.

The absence of a threat notification does not establish that a device is free from spyware, and a notification should be assessed in its proper context.

Additional Considerations for High-Value Targets

Organizations managing sensitive information or supporting high-value personnel may wish to consider a risk-based review of their existing arrangements, including:

- Whether devices used for sensitive duties receive timely security updates.
- Whether personnel have a clear process for reporting credible threat notifications or unusual security alerts.
- Whether incident-response plans account for suspected zero-click exploitation and targeted spyware.
- Whether mobile-device forensic support is available when a credible incident warrants specialist investigation.
- Whether sensitive accounts and systems can be accessed from a dedicated, managed device.
- Whether incident-reporting, evidence-preservation and recovery procedures are understood by relevant teams.

The appropriate controls will depend on the organization's threat exposure, operational needs and available resources.



National Cyber Emergency Response Team

Government of Pakistan



Incident Reporting

Organizations that identify credible indicators of spyware activity or a suspected targeted cyber incident may report it through their established incident-response channels and the National CERT reporting mechanism.

National CERT — Pakistan

Incident reporting: <https://pkcert.gov.pk/report-incident/>

Email: cert@pkcert.gov.pk

Telephone: +92-51-9203412

For other advisories, please visit the NCERT website: <https://pkcert.gov.pk/advisories.asp>

References

1. **Citizen Lab**, *Exposing AdFection: Executive Summary*, published 15 October 2026.
2. **Citizen Lab**, *How Discover-Tech Turned Targeted Ads into a Pipeline for Spyware*, technical research report.
3. **Apple Support**, guidance on Apple threat notifications and protections for users at elevated risk.
4. **MyCERT**, advisory on AdFection and targeted spyware, published in October 2026.

PKCERT

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | <https://pkcert.gov.pk/advisories>

Page 7 of 7