# AL2025_20 New Windows Zero-Day Exploited by 11 State Hacking Groups Since 2017 (21st March 2025)

**Description**

A newly discovered Windows vulnerability (ZDI-CAN-25373) has been actively exploited by at least 11 state-sponsored hacking groups from North Korea, Iran, Russia, and China since 2017. This zero-day flaw allows attackers to execute arbitrary code on affected Windows systems without detection. Despite its severity, Microsoft has stated that the issue "does not meet the bar for servicing" and has yet to release a patch. Security researchers from Trend Micro's Zero Day Initiative (ZDI) have found nearly 1,000 samples of Shell Link (.lnk) files exploiting ZDI-CAN-25373. The vulnerability primarily facilitates cyber espionage and data theft, with over 70% of observed attacks linked to espionage campaigns.

**Attack Details**

DI-CAN-25373 exploits a User Interface (UI) Misrepresentation of Critical Information (CWE-451) flaw, which allows attackers to manipulate Windows shortcut (.lnk) files to hide malicious command-line arguments. This trick enables malware execution without the user's knowledge.

**Exploitation Method**

- Threat actors embed malicious command-line arguments within .lnk shortcut files.
- Attackers use various whitespace characters (e.g., Space \x20, Horizontal Tab \x09, Linefeed \x0A) to pad command-line arguments, making them invisible in the Windows UI.
- Users who inspect the shortcut file do not see the hidden payload, allowing execution to proceed undetected.
- Successful exploitation allows attackers to run malware such as Ursnif, Gh0st RAT, and TrickBot.

## Notable Threat Groups Utilizing ZDI-CAN-25373

- Evil Corp
- APT43 (Kimsuky)
- Bitter
- APT37
- Mustang Panda

- SideWinder
- RedHotel
- Konni

**Attack Distribution**

While the campaigns have targeted victims worldwide, the primary focus has been on North America, South America, Europe, East Asia, and Australia.

**Remediation**

**Immediate Actions:**

- **Avoid Opening Untrusted Files:** Do not interact with unknown .lnk files, especially those received via email or suspicious downloads.
- **Enable Microsoft Defender:** Ensure Microsoft Defender is updated as it has detections in place for ZDI-CAN-25373-related activity.
- **Use Smart App Control:** This feature provides an extra security layer by blocking malicious files from the internet.
- **Restrict LNK Execution:** Configure Group Policy settings to prevent shortcut file execution from untrusted sources.
- **Monitor for Indicators of Compromise (IOCs):** Regularly check logs and endpoint activity for signs of exploitation.

**Long-Term Protection:**

- **Patch Windows Systems:** While Microsoft has not released a patch, users should stay updated on potential future fixes.
- **Deploy Endpoint Detection and Response (EDR) Solutions:** Advanced EDR tools can help detect and mitigate suspicious activity.
- **Educate Users:** Train employees to recognize and avoid phishing attempts that may deliver malicious .lnk files.
- **Network Segmentation:** Restrict access to sensitive systems to minimize potential damage from an exploited vulnerability.

**Microsoft's Response:**

While Microsoft has yet to assign a CVE-ID to ZDI-CAN-25373, it acknowledges the vulnerability and may address it in a future feature release. In the meantime, users are advised to follow the best security practices to reduce the risk of exploitation.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

**References**


- Gatlan, S. (2025, March 19). New Windows zero-day exploited by 11 state hacking groups since 2017. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-windows-zero-day-exploited-by-11-state-hacking-groups-since-2017/
- The Hacker News. (n.d.). Unpatched Windows Zero-Day flaw exploited by 11 State-Sponsored Threat Groups since 2017. Retrieved from the Hacker News https://thehackernews.com/2025/03/unpatched-windows-zero-day-flaw.html