Windows Zero Day Exploited in Cyber Espionage

Overview

This week, Trend Zero Day Initiative (ZDI) discovered that a Windows zero-day vulnerability (ZDI-CAN-25373) has been actively exploited since 2017 by at least 11 state-sponsored hacking groups from North Korea, Iran, Russia, and China.

The flaw allows attackers to execute arbitrary code via manipulated shortcut (.lnk) files, allowing for data theft and cyber espionage. Despite its widespread exploitation, Microsoft has stated it does not meet their criteria for immediate patching.

Affected Products

- All Windows versions – Any system handling shortcut (.lnk) files is vulnerable

ZDI-CAN-25373 exploits Windows shortcut (.lnk) files by embedding hidden command-line arguments that evade detection. This allows attackers to execute arbitrary code on a targeted system without the user's knowledge. The flaw has been actively leveraged in cyber espionage campaigns, with 70% of cases linked to intelligence gathering and data theft, while 20% of observed attacks focused on financial gain.

Various state-sponsored and cybercriminal groups have used this method to deploy malware, including Ursnif, Gh0st RAT, Trickbot, and multiple malware-as-a-service (MaaS) payloads, increasing the risk of system compromise and persistent access.

Microsoft acknowledged ZDI's disclosure of the vulnerability and stated that Microsoft Defender currently detects and blocks related threat activity, with Smart App Control providing additional protection by preventing malicious files from the internet. While Microsoft will not issue a patch, they will "consider addressing it in a future release."

Aspire Protects

- Restrict LNK Execution – Block .lnk files from untrusted locations.
- Apply Group Policy Controls – Disable automatic execution of .lnk files.
- Monitor for Suspicious Activity – Look for cmd.exe or powershell.exe execution from shortcut files.
- Deploy Security Rules – Use YARA rules and network security filters to detect exploitation attempts.
- Limit User Privileges – Apply least-privilege access to prevent system compromise.

TTPs to Watch

Initial Access

- User Execution [T1204] – The attacker may trick users into opening a malicious .lnk file.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute hidden commands via cmd.exe or PowerShell.

Persistence

- Shortcut Modification [T1547.009] – The attacker may use malicious shortcuts to maintain access.

Defense Evasion

- Masquerading [T1036] – The attacker may disguise malicious shortcuts to appear benign.

IoCs

- Suspicious .lnk file activity – Execution of cmd.exe or powershell.exe from a shortcut.
- Hidden command-line arguments – Padded whitespace characters concealing execution commands.
- Malware payloads – Ursnif, Gh0st RAT, Trickbot, and MaaS-linked domains.

Targeted Industries

The vulnerability may impact the following industries/sectors:

- Government
- IT
- MSPs
- Retail
- Manufacturing
- Telecommunications
- Defense and Aerospace
- Finance
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

ZDI-CAN-25373 Windows Shortcut Exploit Abused as Zero-Day in Widespread APT Campaigns | Trend Micro (US)

New Windows zero-day exploited by 11 state hacking groups since 2017