IMPORTANT CYBERSECURITY NEWS: WINDOWS ZERO-DAY EXPLOITED BY MULTIPLE STATE-SPONSORED THREAT ACTORS

Vairav Cyber Security News Report

Date: March 19, 2024

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical zero-day vulnerability (ZDI-CAN-25373) in Microsoft Windows has been actively exploited by 11 state-sponsored threat groups since 2017. This flaw allows attackers to execute hidden malicious commands using crafted .LNK (Windows Shortcut) files. The vulnerability has been leveraged by APT groups from China, Iran, North Korea, and Russia for cyber espionage, data theft, and financially motivated attacks. Despite its exploitation by multiple threat actors, Microsoft has classified the issue as low severity and does not plan to release a fix.

Key Findings:

- Nearly 50% of the known APT groups exploiting this vulnerability originate from North Korea, highlighting collaboration among Pyongyang's cyber units.
- 70% of observed attacks focused on espionage and intelligence gathering, while 20% were financially motivated.
- The flaw has been used to distribute Lumma Stealer, GuLoader, Remcos RAT, and Raspberry Robin, indicating cross-use by cybercriminal and state-sponsored groups.
- ZDI-CAN-25373 remains unpatched, leaving organizations at continued risk of compromise.

INCIDENT ANALYSIS

Researchers from Trend Micro's Zero Day Initiative (ZDI) have identified nearly 1,000 malicious .LNK file artifacts abusing ZDI-CAN-25373. This vulnerability is exploited using hidden command line arguments padded with Line Feed (\x0A) and Carriage Return (\x0D) characters, making detection more difficult.

The vulnerability has been linked to various advanced persistent threat (APT) groups, including:

- Evil Corp (Water Asena)
- Kimsuky (Earth Kumiho)
- Konni (Earth Imp)
- Bitter (Earth Anansi)
- ScarCruft (Earth Manticore)

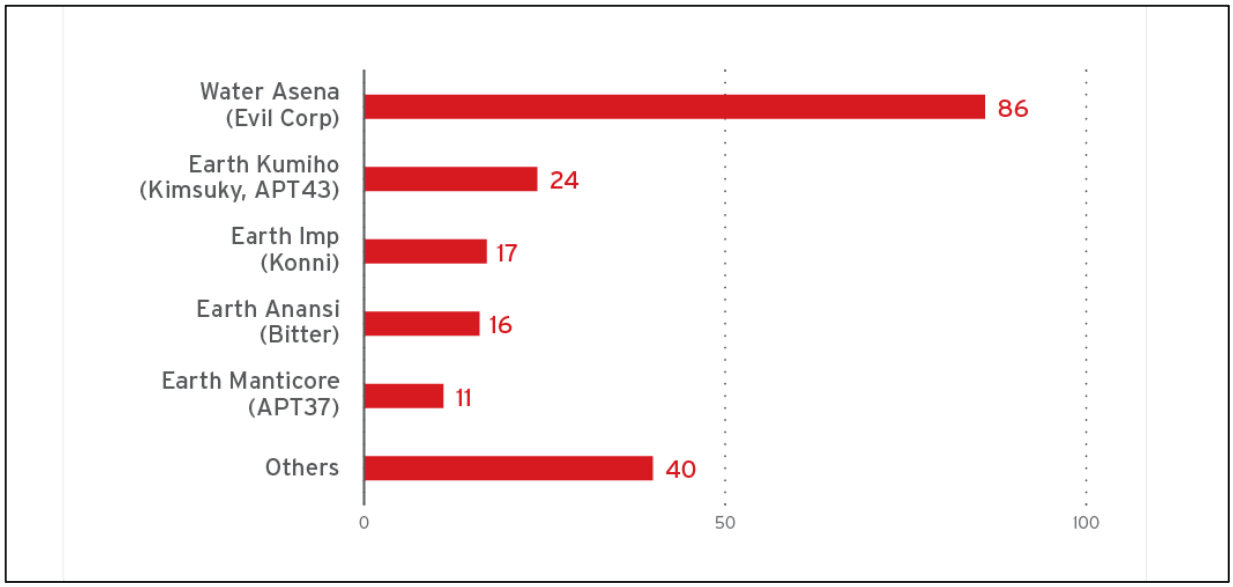

Figure 1: Number of samples from APT groups exploiting ZDI-CAN-25373

Telemetry data reveals that affected sectors include government agencies, financial institutions, think tanks, telecom providers, and defense organizations in the U.S., Canada, Russia, South Korea, Vietnam, and Brazil.

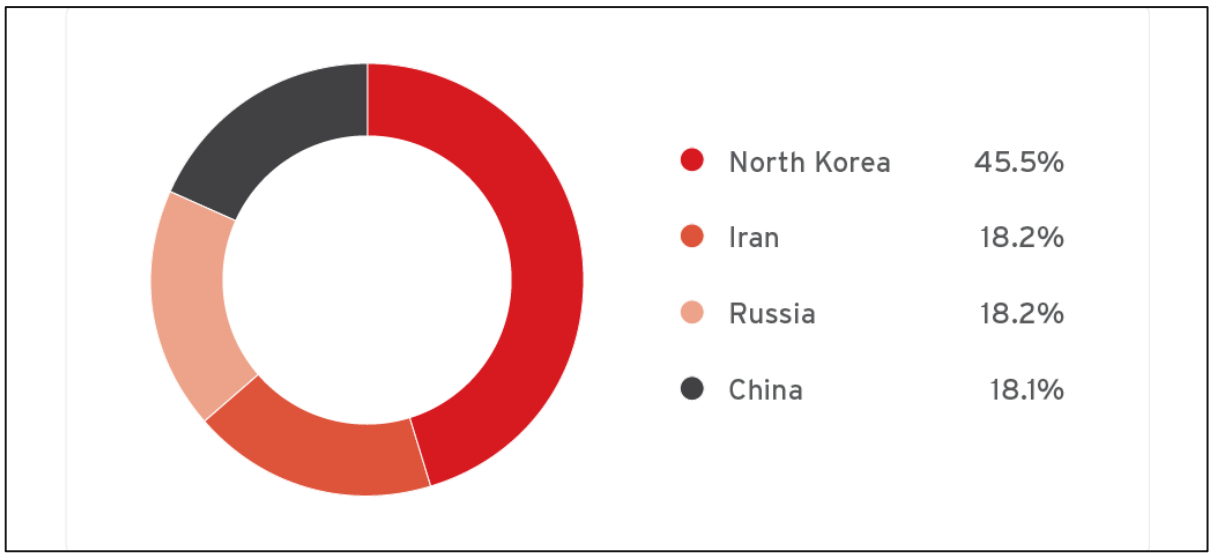

Figure 2: Countries of state-sponsored APT groups exploiting ZDI-CAN-25373

Attackers have used ZDI-CAN-25373 to deploy well-known malware such as Lumma Stealer, GuLoader, Remcos RAT, and Raspberry Robin. The involvement of multiple North Korean APT groups suggests possible collaboration within Pyongyang's cyber operations. These APTs have targeted:

- Government agencies
- Financial institutions (including cryptocurrency-related entities)
- Telecommunications firms

- Military and defense organizations
- Energy and critical infrastructure sectors

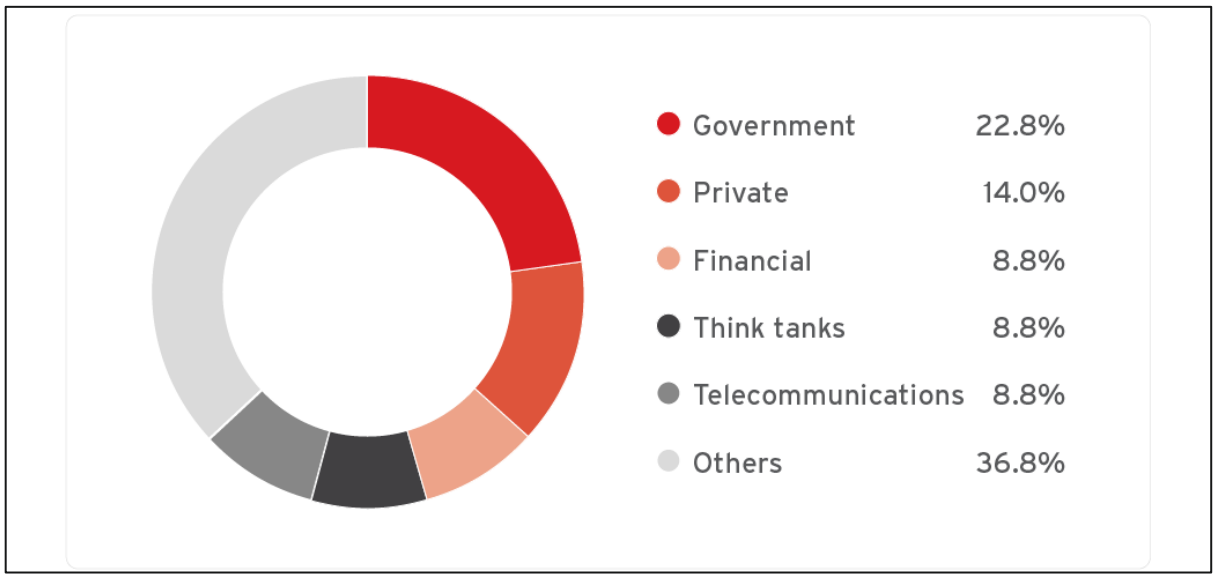

Figure 3: Targeted sectors in exploitation of ZDI-CAN-25373

RECOMMENDED ACTIONS

To mitigate the risks posed by ZDI-CAN-25373, organizations should:

- Block untrusted shortcut files, especially from external sources.
- Implement security monitoring for unauthorized command execution.
- Prevent unauthorized execution of scripts and unknown executables.
- Deploy EDR solutions to detect and respond to malicious .LNK file activity.
- Educate users on phishing techniques involving weaponized shortcut files.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zero-day-exploit.html

https://thehackernews.com/2025/03/unpatched-windows-zero-day-flaw.html

https://www.zerodayinitiative.com/advisories/ZDI-25-148/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com