Weekly Report of CNCERT

CNCERT/CC

Key Findings

| Excellent | Good | Fair | Poor | Very Poor |

Malware Downloads in Chinese Mainland   ↓ 0.5%

Dec.7th 2025   Dec.14th 2025   Dec.21st 2025   Dec.28th 2025   Jan.4th 2026

Top 5 Families of Propagated Malware

- Malware.a variant of Linux.Mirai
- Backdoor.Linux.Mirai.r
- Trojan.Multi.Zapchast.b
- Malware.a variant of Linux.Mirai.A Trojan
- Trojan.Linux.Mirai.1

Backdoored Websites in Chinese Mainland

↑ 81.8%

Dec.7th 2025   Dec.14th 2025   Dec.21st 2025   Dec.28th 2025   Jan.4th 2026
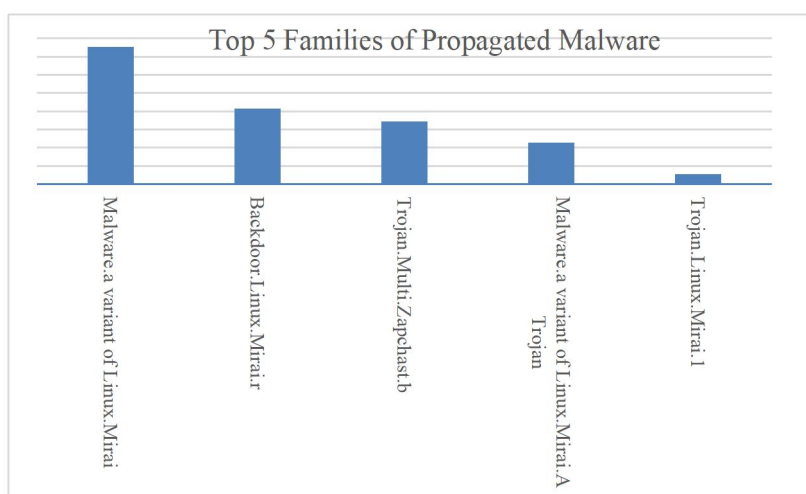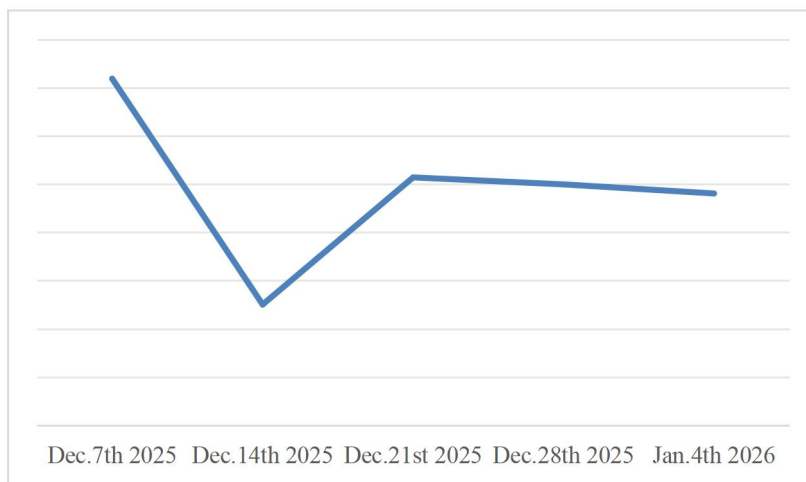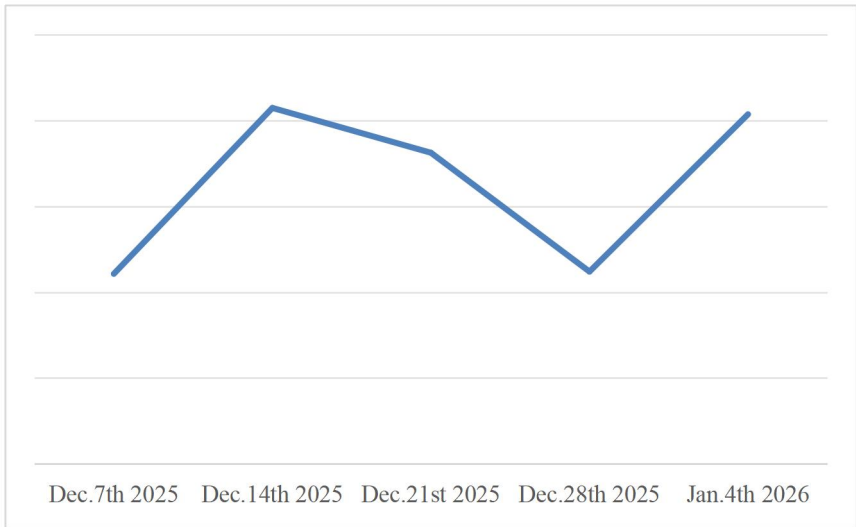
Distribution of Backdoored Websites in Chinese Mainland by Type

■ COM ■ NET ■ Others

Phishing Websites Targeting Websites in Chinese Mainland

↓ 50.8%

Dec.7th 2025   Dec.14th 2025   Dec.21st 2025   Dec.28th 2025   Jan.4th 2026

Distribution of Phishing Websites Targeting Websites in Chinese Mainland by Industry

Banks | Securities and Funds | Governments and Institutions
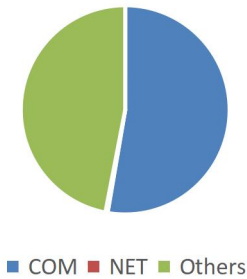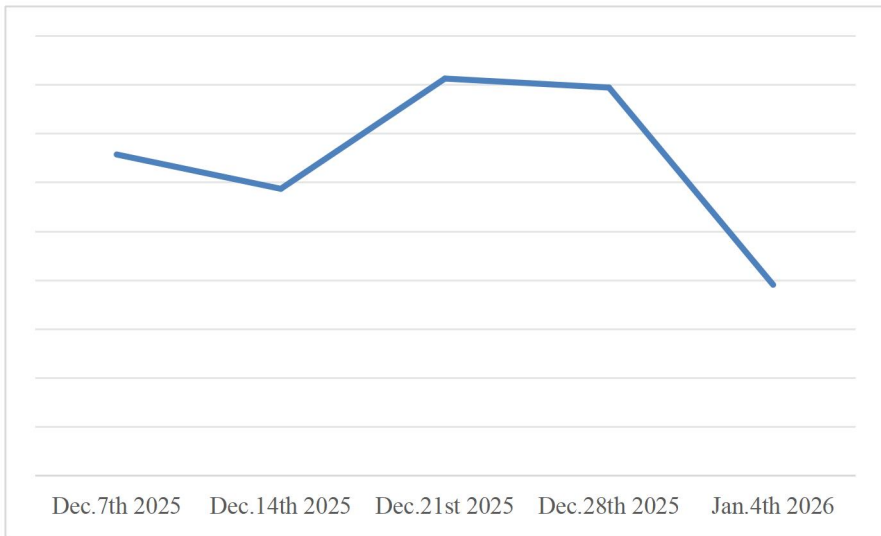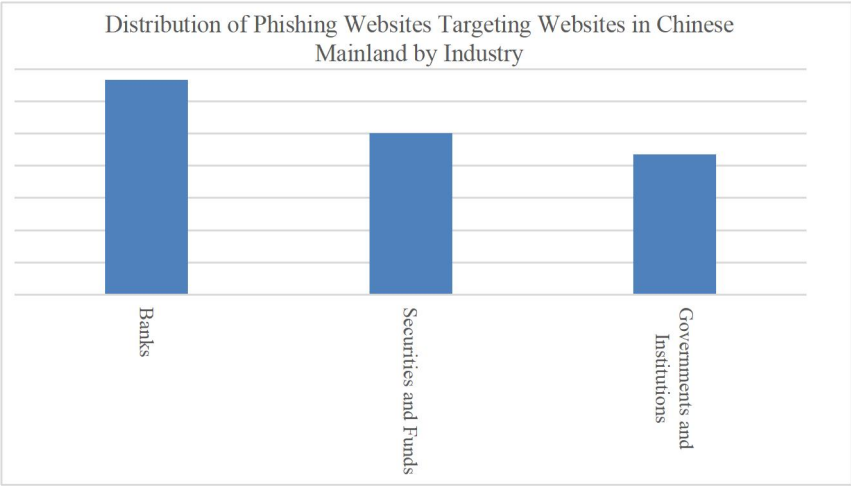
New Vulnerabilities Collected by CNVD

↓ 10.0%

Dec.7th 2025   Dec.14th 2025   Dec.21st 2025   Dec.28th 2025   Jan.4th 2026

Types of Vulnerabilities by Risk

■ High Risk ■ Medium Risk ■ Low Risk
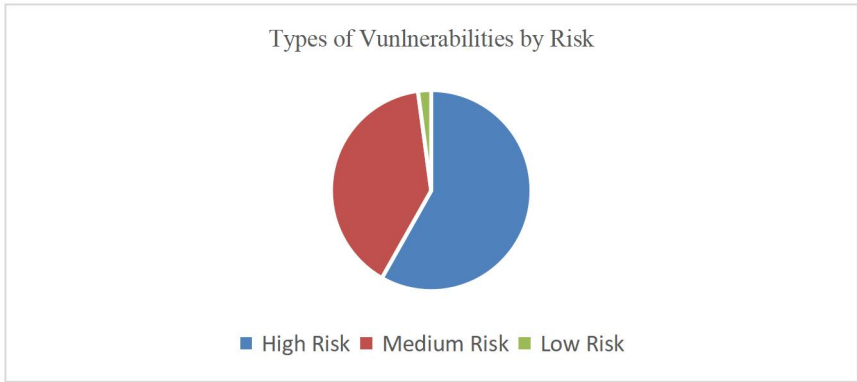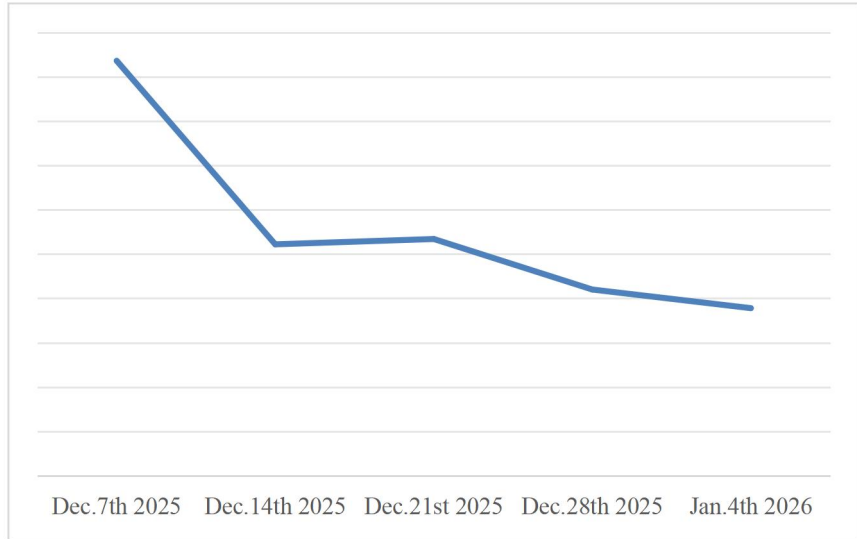
marks the same number as last week; ↑ *marks an increase from last week;* ↓ *marks a decrease from last week*

Incident Handling

This week, CNCERT has handled 196 network security incidents, 63 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners. Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs, and the other organizations to handle 129 phishing incidents.

About CNCERT

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT/CC) was founded in August 2001. It is a non-governmental non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community. As the national CERT of China, CNCERT/CC strives to improve the nation's cybersecurity posture and safeguard the security of critical information infrastructure. CNCERT/CC leads efforts to prevent, detect, alert, coordinate and handle cybersecurity threats and incidents, in line with the guiding principle of "proactive prevention, timely detection, prompt response and maximized recovery". CNCERT/CC also operates the China National Vulnerability Database (CNVD).

CNCERT/CC has its presence in 31 provinces, autonomous regions and municipalities across mainland China. CNCERT/CC coordinates with key network operators, domain name registrars, cybersecurity vendors, academia, civil society, research institutes and other CERTs to jointly handle significant cybersecurity incidents in a systematic way. With an important role in the industry, CNCERT/CC initiated the foundation of Anti Network-Virus Alliance of China (ANVA) and China Cyber Threat Governance Alliance (CCTGA).

CNCERT/CC actively carries out international cooperation in cybersecurity and is committed to establishing the mechanism of prompt response to and coordinative handling of cross-border cybersecurity incidents. As of 2024, CNCERT/CC has established "CNCERT/CC International Cooperation Partnership" with 292 teams in 86 countries and regions. CNCERT/CC is a full member of the Forum of Incident Response and Security Teams (FIRST) and one of the founders of the Asia Pacific Computer Emergency Response Team (APCERT). CNCERT/CC has also actively engaged in activities of APEC, ITU, SCO, ASEAN, BRICS and other international and regional organizations.

Contact us

Should you have any comments or suggestions on the Weekly Report of CNCERT, please contact our editors.

Duty Editor：Lou Shuyi

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82991680