

Weekly Report of CNCERT

Key Findings



Malware Downloads in Chinese Mainland	• 43.7 Million	↓ 17.2%
Infected Computers Controlled by Trojans or Botnets in Chinese Mainland	• 1.13 Million	↓ 29.8%
Defaced Websites in Chinese Mainland	• 21	↓ 98.4%
Defaced gov.cn	• 1	↓ 92.3%
Backdoored Websites in Chinese Mainland	• 497	↑ 3.5%
Backdoored gov.cn	• 0	
Phishing Webpages Targeting Websites in Chinese Mainland	• 76	↓ 10.6%
New Vulnerabilities Collected by CNVD	• 231	↓ 52.9%
High-risk Vulnerabilities	• 39	↓ 74.2%

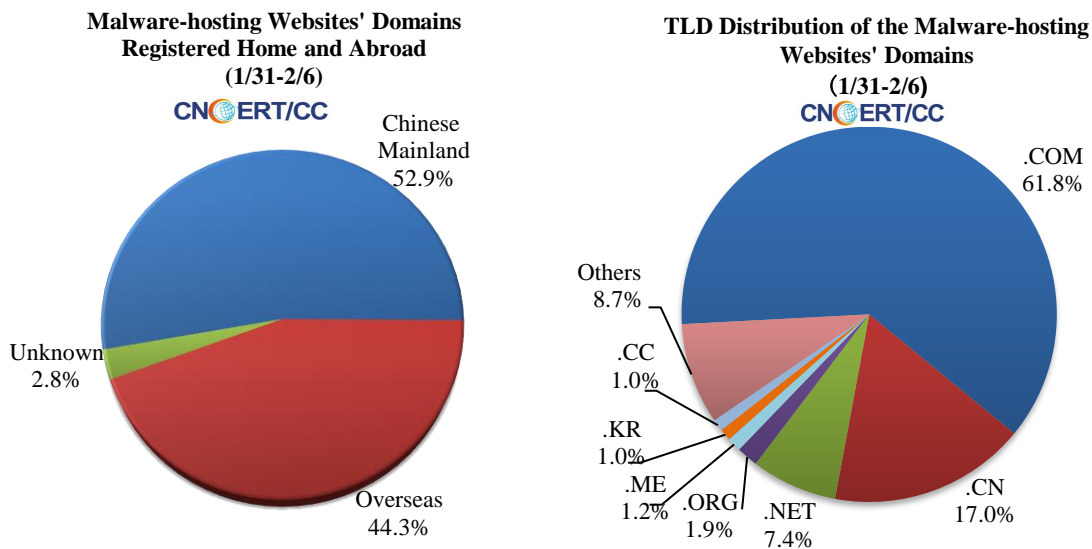
marks the same number as last week;
 marks an increase from last week;
 marks a decrease from last week

Malware Activities

The malware downloads and infected computers controlled by Trojans or Botnets in Chinese Mainland amounted to about 43.7 million and 1.13 million.



The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 1,078 domains and 4,217 IP addresses. Among the 1,078 malicious domains, 44.3% of them were registered abroad, 61.8% of their TLDs fell into the category of .com. Among the 4,217 IP addresses, 68.0% were registered abroad. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain, and 166 were accessed directly via IPs.



In terms of the malicious domain names and IPs either monitored by CNCERT or sourced from the reporting members, CNCERT has actively coordinated the domain registrars and other related agencies to handle them. Moreover, the blacklist of these malicious domains and IPs has been published on the website of Anti Network-Virus Alliance of China (ANVA).

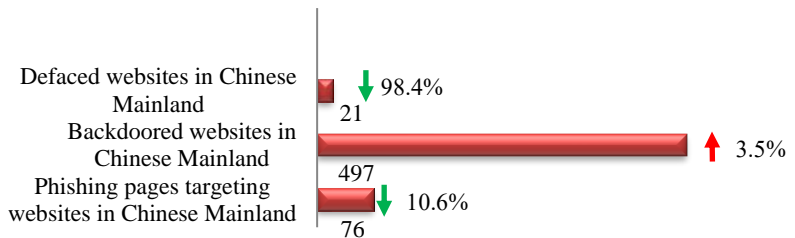
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

<http://www.anva.org.cn/virusAddress/listBlack>

Anti-Network-Virus Alliance of China (ANVA) is an industry alliance that was initiated by Network and Information security Committee under Internet Society of China (ISC) and has been operated by CNCERT.

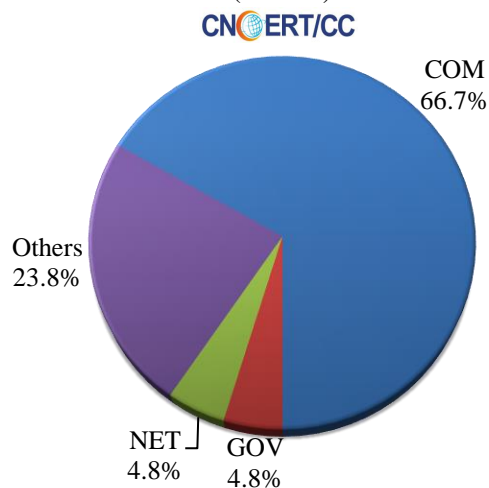
Website Security

This week, CNCERT monitored 21 defaced websites in Chinese Mainland and 497 websites planted with backdoors and 76 phishing web pages targeting websites in Chinese Mainland.

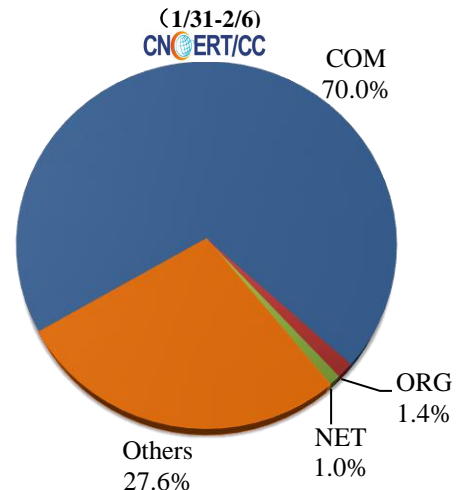


This week, the defaced government (gov.cn) website totaled 1 (4.8% of domestic websites), a decrease of 92.3% from last week. The backdoors were installed into 0 government (gov.cn) website.

Defaced Websites in Chinese Mainland (1/31-2/6)

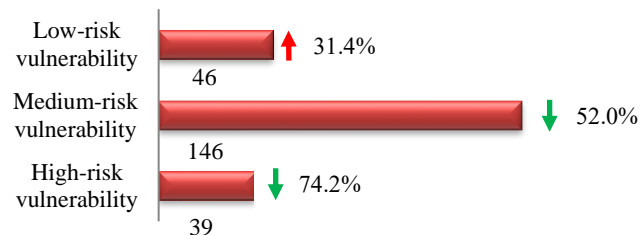


Domain Categories of the Backdoored Websites in Chinese Mainland (1/31-2/6)



Vulnerabilities

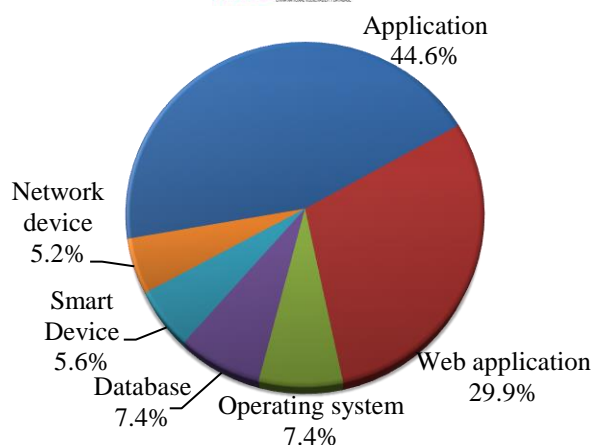
This week, China National Vulnerability Database (CNVD) recorded 231 new vulnerabilities. This week's overall vulnerability severity was evaluated as Medium.



Objectives Affected by the Vulnerabilities Collected by CNVD

(1/31-2/6)

CNVD 国家信息安全漏洞平台



The Application was most frequently affected by these vulnerabilities collected by CNVD, followed by the Web Application, the Operating System and the Database.

For more details about the vulnerabilities, please review CNVD Weekly Vulnerability Report.

The URL of CNVD for Publishing Weekly Vulnerability Report

<http://www.cnvd.org.cn/webinfo/list?type=4>

China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

Incident Handling

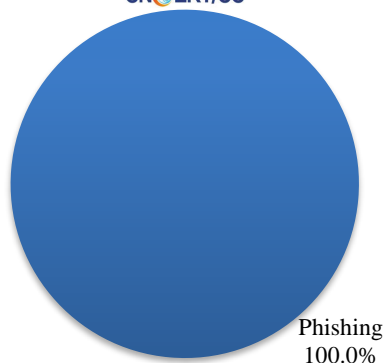
This week, CNCERT has handled 40 network security incidents, 17 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

Types of the Incidents handled by

CNCERT

(1/31-2/6)

CNERT/CC



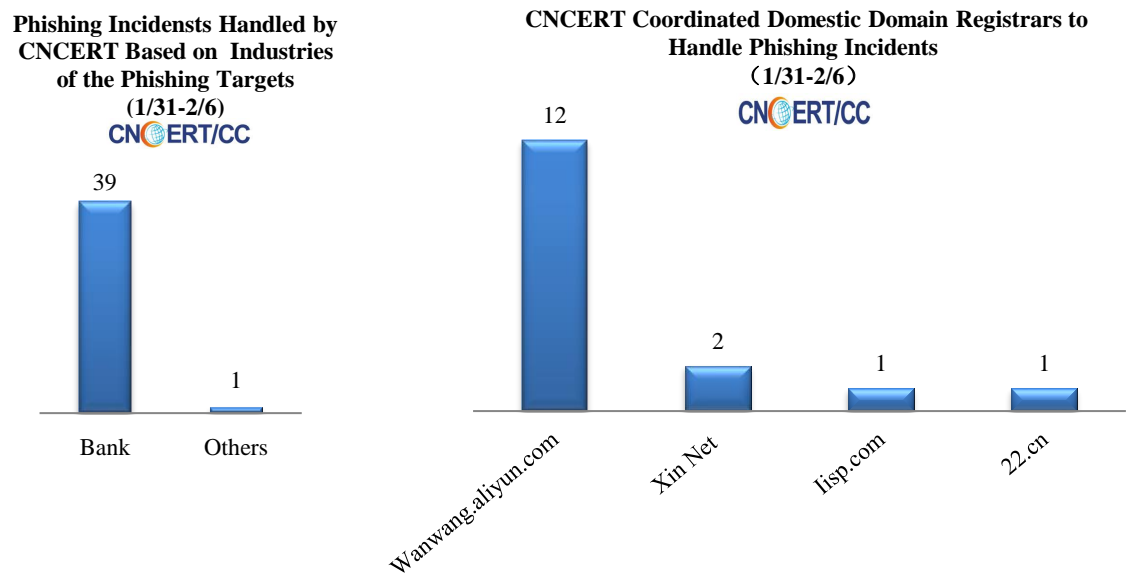
Overseas reported incident handled by coordinating domestic organizations

0

Domestically reported incident handled by coordinating overseas organizations

17

Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs, and the other organizations to handle 40 phishing incidents. Based on industries that these phishing targets belong to, there were 39 banking phishing incidents and 1 other incident.



About CNCERT

The National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT or CNCERT/CC) is a non-governmental, non-profitable organization of network security technical coordination. Since its foundation in Sep.2002, CNCERT has dedicated to carrying out the work of preventing, detecting, warning and handling China network security incidents under the policy of “positive prevention, timely detection, prompt response, guaranteed recovery”, to maintain the safety of China public Internet and ensure the safe operation of the information network infrastructures and the vital information systems. Branches of CNCERT spread in 31 provinces, autonomous regions, and municipalities in Chinese Mainland.

CNCERT is active in developing international cooperation and is a window of network security incidents handling to the world. As a full member of the famous international network security cooperative organization FIRST and one of the initiators of APCERT, CNCERT devotes itself to building a prompt response and coordination handling mechanism of cross-border network security incidents. By 2020, CNCERT has established “CNCERT International Partners” relationships with 265 organizations from 78 countries or regions.

Contact us

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

Duty Editor: Qin Jiawei

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315