

Weekly Report of CNCERT

Key Findings

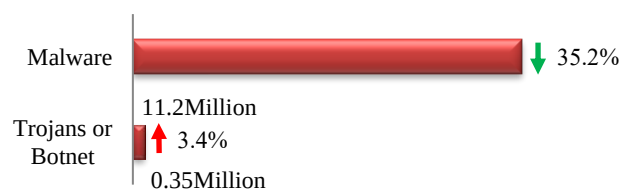


Times of transmission of malware in mainland China	• 11.2 Million	↓ 35.2%
Infected Computers Controlled by Trojans or Botnets in Mainland China	• 0.35 Million	↑ 3.4%
Defaced Websites in Mainland China	• 1,840	↓ 46.7%
Defaced gov.cn	• 9	↓ 59.1%
Backdoored Websites in Mainland China	• 522	↓ 2.8%
Backdoored gov.cn	• 2	=
Phishing Webpages Targeting Websites in Mainland China	• 385	↓ 83.7%
New Vulnerabilities Collected by CNVD	• 679	↑ 10.0%
High-risk Vulnerabilities	• 120	↓ 41.2%

- = marks the same number as last week; ↑ marks an increase from last week; ↓ marks a decrease from last

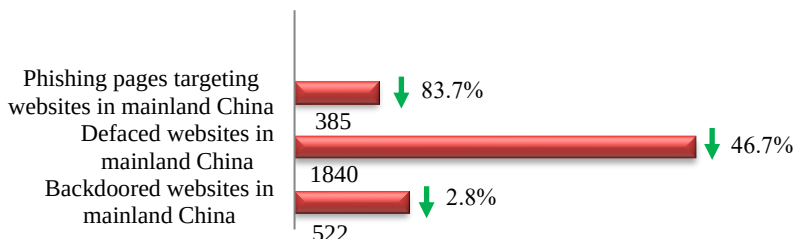
Malware Activities

The Times of transmission of malware and infected computers controlled by Trojans or Botnets in mainland China amounted to about 11.5million and 0.35 million.



Website Security

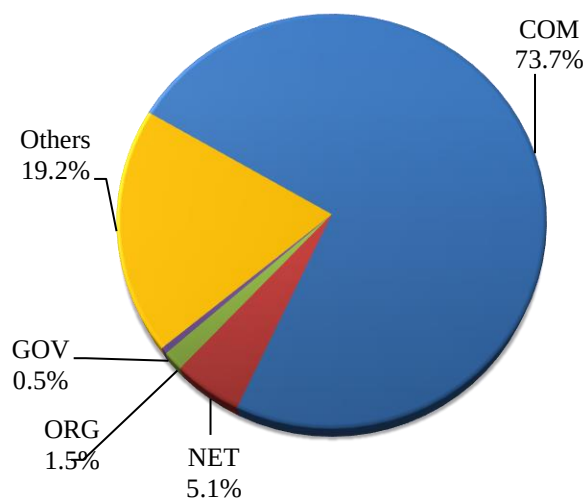
This week, CNCERT monitored 1,840 defaced websites in mainland China and 522 websites planted with backdoors and 385 phishing web pages targeting websites in mainland China.



This week, the defaced government (gov.cn) websites totaled 9 (0.6%), a decrease of 59.1% from last week. The backdoors were installed into 2 government (gov.cn) websites.

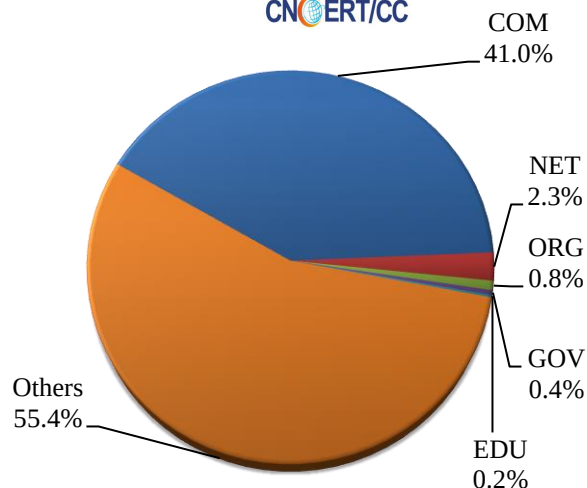
Defaced Websites in Mainland China (3/15-3/21)

CNCERT/CC



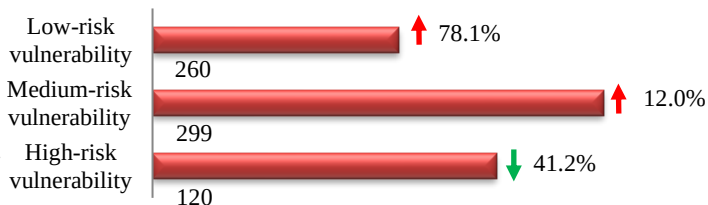
Domain Categories of the Backdoored Websites in Mainland China (3/15-3/21)

CNCERT/CC

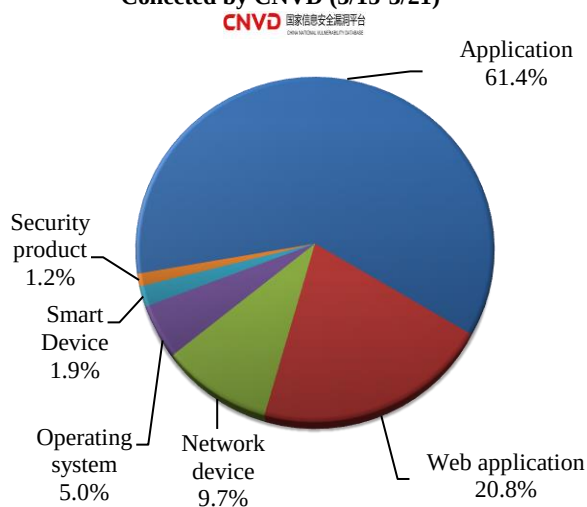


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 679 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (3/15-3/21)



The Application was most frequently affected by these vulnerabilities collected by CNVD, followed by Web application and Network device.

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

The URL of CNVD for Publishing Weekly Vulnerability Report

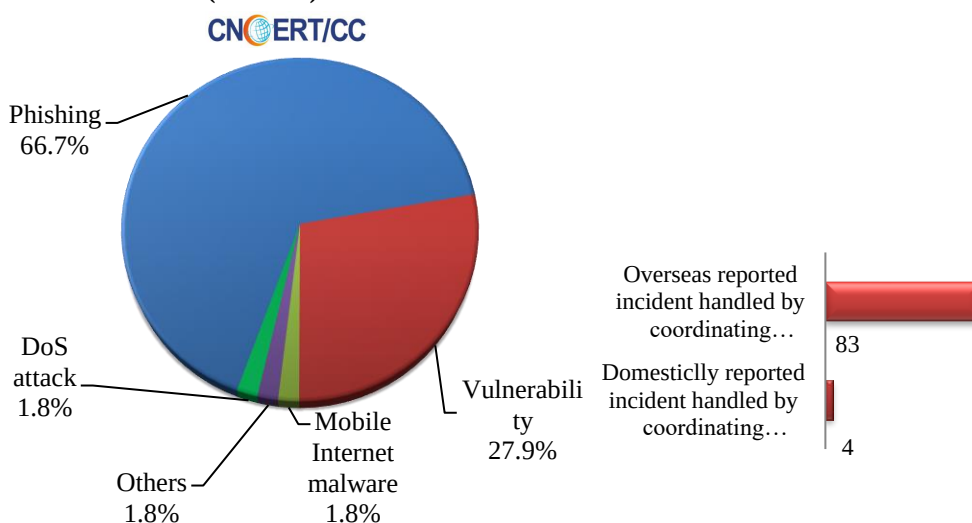
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

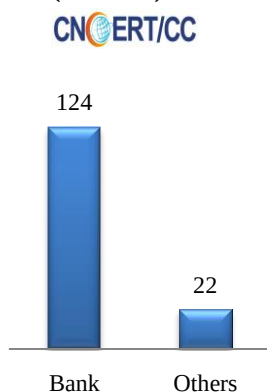
This week, CNCERT has handled 219 network security incidents, 87 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

Types of the Incidents Handled by CNCERT (3/15-3/21)

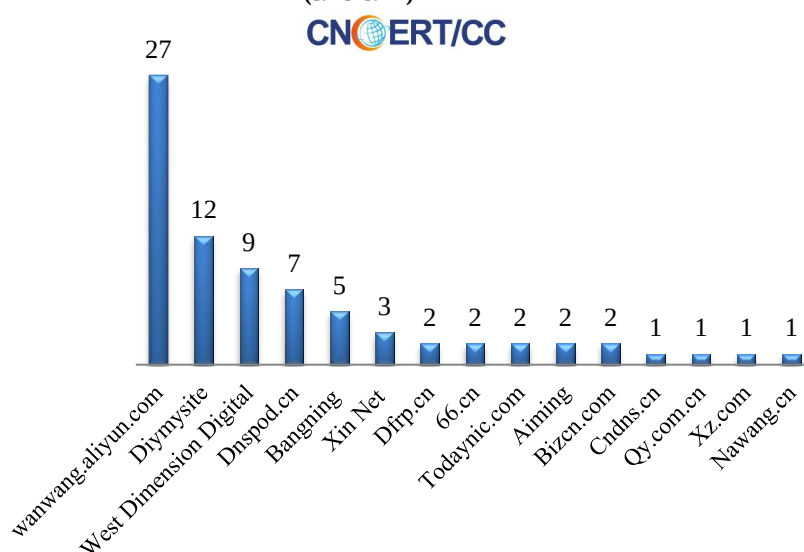


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 146 phishing incidents. Based on industries that these phishing targets belong to, there were 124 banking phishing incidents and 22 other incidents.

Phishing Incidents Handled by CNCERT Based on Industries of the Phishing Targets (3/15-3/21)

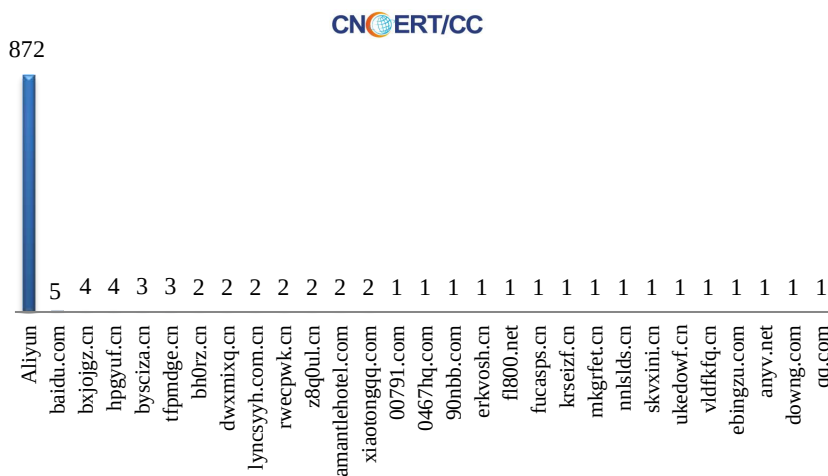


CNCERT Coordinated Domestic to Handle Phishing Incidents (3/15-3/21)



CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (3/15-3/21)

This week, CNCERT has coordinated 28 mobile phone application stores and malware-injected domains to handle 921 malicious URLs of the mobile malware.



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 mainland China.

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: :Wen Jing

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315

