Weekly Report of CNCERT

CNCERT/CC

Key Findings

Excellent	Good	Fair	Poor	Very Poor

Infected Computers in Mainland China	• 0.21 Million	↑	9.6%
Defaced Websites in Mainland China **Defaced gov.cn**	• 638 • 43	↓ ↑	7.5% 4.9%
Backdoored Websites in Mainland China **Backdoored gov.cn**	• 561 • 9	↓ ↓	30.3% 47.1%
Phishing Webpages Targeting Websites in Mainland China	• 1,718	↓	52.7%
New Vulnerabilities Collected by CNVD **High-risk Vulnerabilities**	• 375 • 110	↑ ↑	66.7% 61.8%

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

Malware Activities

The infected computers in mainland China amounted to about 0.21 million, among which about 0.12 million were controlled by Trojans or Botnets and about 0.9 million by Confickers.

Trojans or Botnet
↓ 13.0%
0.12 million

Conficker
↑ 74.9%
0.5 million
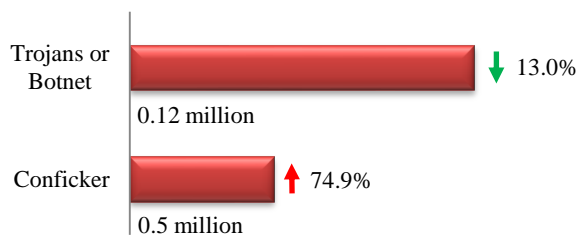
Website Security

This week, CNCERT monitored 638 defaced websites, 561 websites planted with backdoors and 1,718 phishing web pages targeting websites in mainland China.

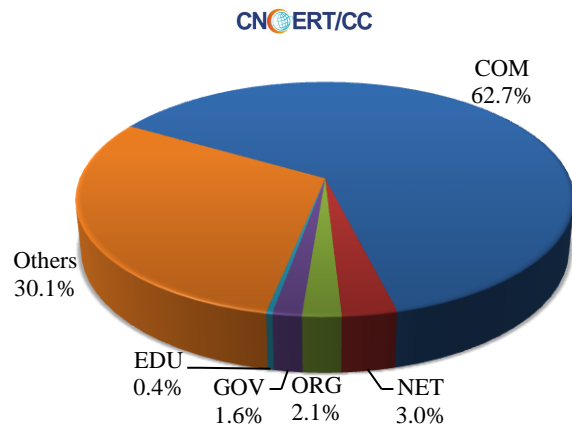|	
Defaced websites in mainland China	↓ 7.5% 638
Backdoored websits in mainland China	↓ 30.3% 561
Phishing pages targeting websites in mainland China	↓ 52.7% 1,718
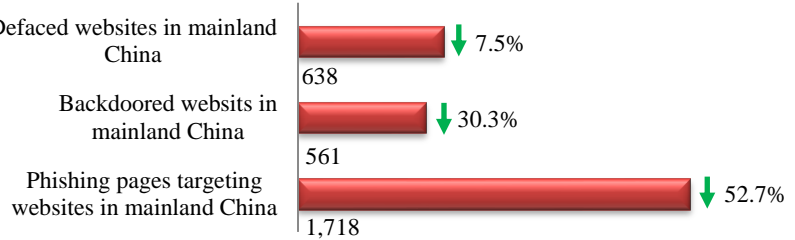
This week, the defaced government (gov.cn) websites totaled 43 (6.7%), an increase of 4.9% from last week. Backdoors were installed into 9 (1.6%) government (gov.cn) websites, a decrease of 47.1 from last week. The fake domains and IP addresses targeting websites in mainland China reached 412 and 221 respectively, with each IP address loading about 109 phishing web pages on average.

Domain Categories of the Defaced Websits in Mainland China (Jan 14-Jan 20)

CNCERT/CC

COM 71.6%
Others 13.3%
BIZ 0.2%
ORG 2.0%
NET 6.1%
GOV 6.7%
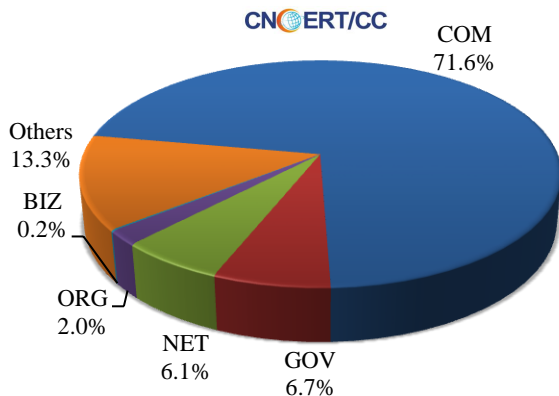
Domain Categories of the Backdoored Websites in Mainland China (Jan 14-Jan 20)

CNCERT/CC

COM 62.7%
Others 30.1%
EDU 0.4%
GOV 1.6%
ORG 2.1%
NET 3.0%

Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 375 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.

Low-risk vulnerability	↑ 66.7% 29
Medium-risk vulnerability	↑ 69.8% 236
High-risk vulnerability	↑ 61.1% 110
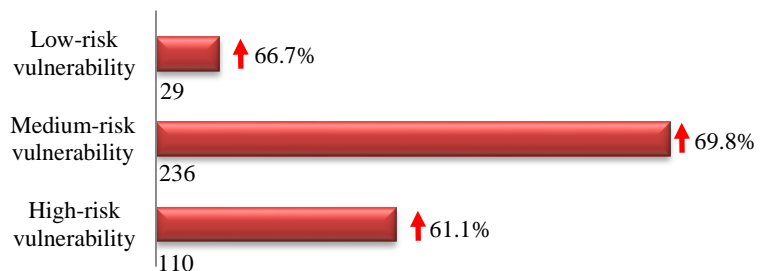
Objectives Affected by the Vulnerabilities Collected by CNVD (Jan 14-Jan 20)
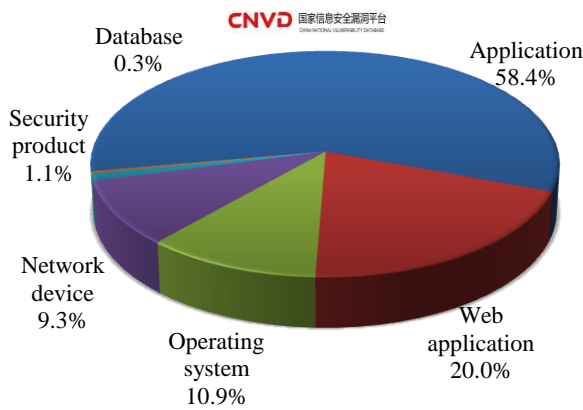
The Application was most frequently affected by these vulnerabilities collected by CNVD, followed by Web Application and Operating system.

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

The URL of CNVD for Publishng 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 658 network security incidents, 341 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 (Jan 14-Jan 20)
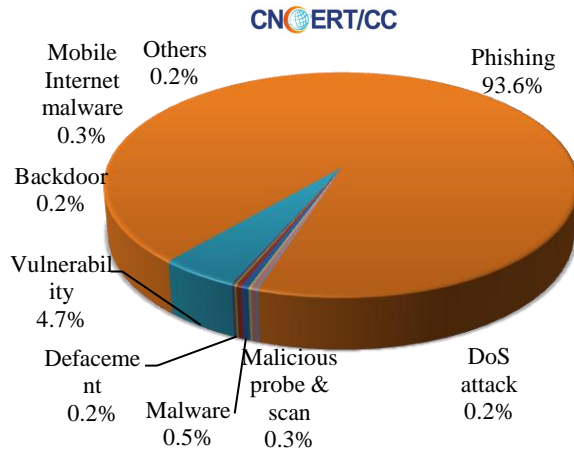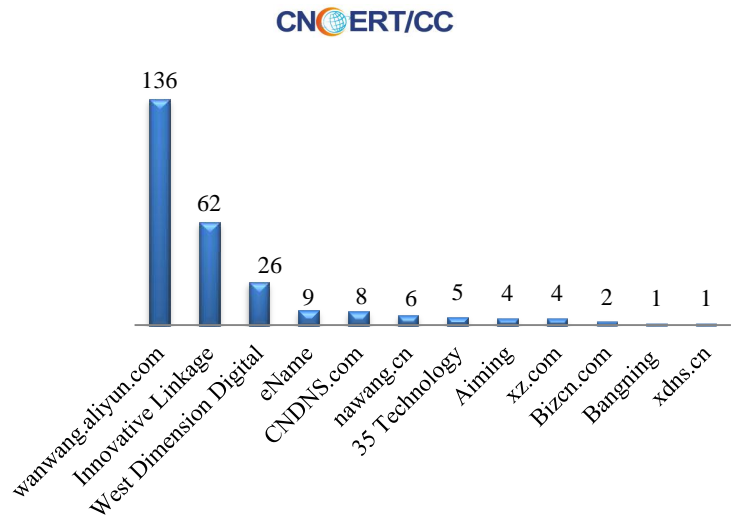
Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 616 phishing incidents. Based on industries that these phishing targets belong to, there were 606 banking phishing incidents and 8 ISP phishing incidents.
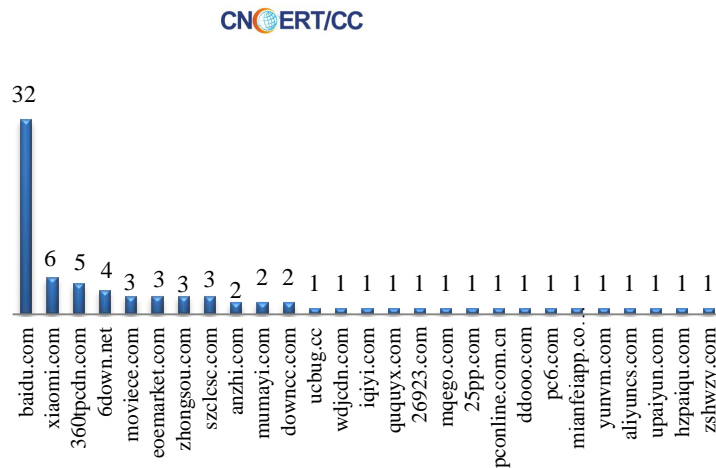
Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (Jan 14-Jan 20)

CNCERT/CC

Category	Count
Banking phishing	606
ISP phishing	8
Government websites phishing	2
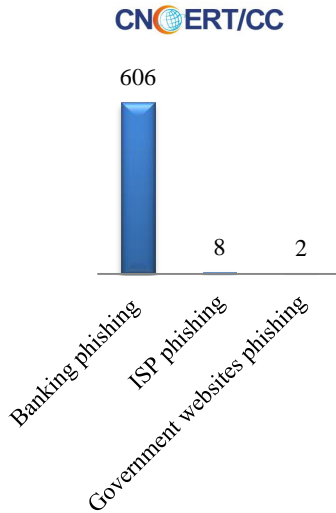
CNCERT Coordinated Domestic to Handle Phishing Incidents (Jan 14-Jan 20)

CNCERT/CC

Registrar	Count
wanwang.aliyun.com	136
Innovative Linkage	62
West Dimension Digital	26
eName	9
CNDNS.com	8
nawang.cn	6
35 Technology	5
Aiming	4
xz.com	4
Bizcn.com	2
Bangning	1
xdns.cn	1

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Jan 14-Jan 20)

CNCERT/CC

This week, CNCERT has coordinated 27 mobile phone application store and malware-injected domains to handle 81 malicious URL of the mobile malware.

Domain	Count
baidu.com	32
xiaomi.com	6
360tpcdn.com	5
6down.net	4
moviece.com	3
eoemarket.com	3
zhongsou.com	3
szclcsc.com	3
anzhi.com	2
mumayi.com	2
downcc.com	2
ucbug.cc	1
wdjcdn.com	1
iqiyi.com	1
ququyx.com	1
26923.com	1
mqego.com	1
25pp.com	1
pconline.com.cn	1
ddooo.com	1
pc6.com	1
mianfeiapp.co...	1
yunvm.com	1
aliyuncs.com	1
upaiyun.com	1
hzpaiqu.com	1
zshwzy.com	1

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 2017, CNCERT has established "CNCERT International Partners" relationships with 211 organizations from 72 countries or regions.

Contact us

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

Duty Editor: Zhu Yunqian

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158