Weekly Report of CNCERT

Key Findings

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

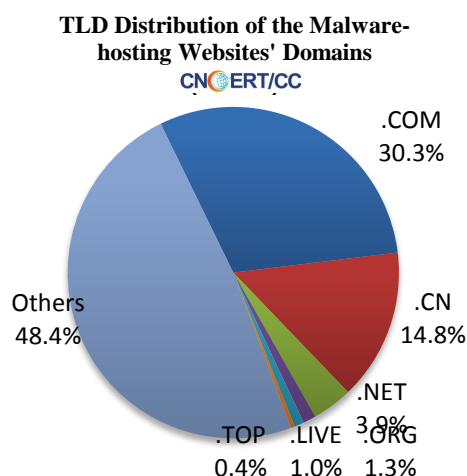|		
Infected Computers in Mainland China	• 0.59Million	↓ 6.5%
Defaced Websites in Mainland China **Defaced gov.cn**	• 7,529 • 27	↓ 17.6% ↓ 40.0%
Backdoored Websites in Mainland China **Backdoored gov.cn**	• 1578 • 3	↑ 2.7% ↑ 200.0%
Phishing Webpages Targeting Websites in Mainland China	• 1570	↑ 57.6%
New Vulnerabilities Collected by CNVD **High-risk Vulnerabilities**	• 554 • 197	↓ 20.7% ↓ 31.6%

= *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 0.59 million, among which about 0.52 million were controlled by Trojans or Botnets and about 0.07 million by Confickers.

Trojans or Botnet ↓ 7.9%
0.52million

Conficker ↑ 5.8%
0.07million
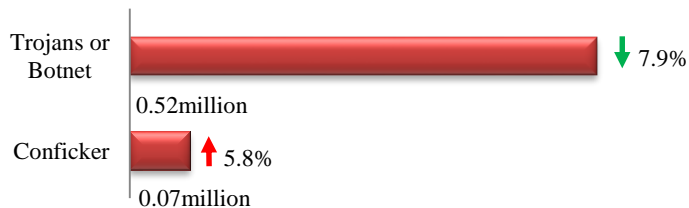
The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 2,311 domains and 6,155 IP addresses. Among the 2,311 malicious domains, 30.3% of their TLDs fell into the category of .com. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain name, and only 338 were accessed directly via IPs.

TLD Distribution of the Malware-hosting Websites' Domains

CN●ERT/CC

- .COM 30.3%
- .CN 14.8%
- .NET 3.9%
- .ORG 1.3%
- .LIVE 1.0%
- .TOP 0.4%
- Others 48.4%

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.*
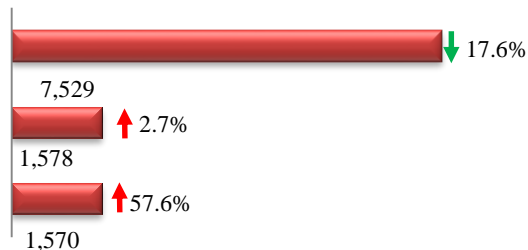
Website Security

This week, CNCERT monitored 7,529 defaced websites in mainland China and 1,578 websites planted with backdoors and 1,570 phishing web pages targeting websites in mainland China.

defaced websites in mainland China
7,529 ↓ 17.6%

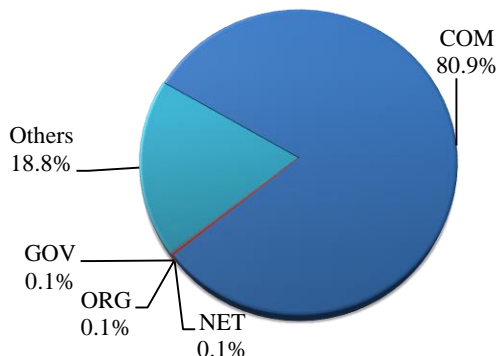Backdoored websits in mainland China
1,578 ↑ 2.7%

Phishing pages targeting websites in mainland China
1,570 ↑ 57.6%

This week, the backdoors were installed into 27(0.4%) government (gov.cn) websites, a decrease of 40.0% from last week. The backdoors were installed into 3(0.2%) government (gov.cn) websites, an increase of 200.0% from last week.
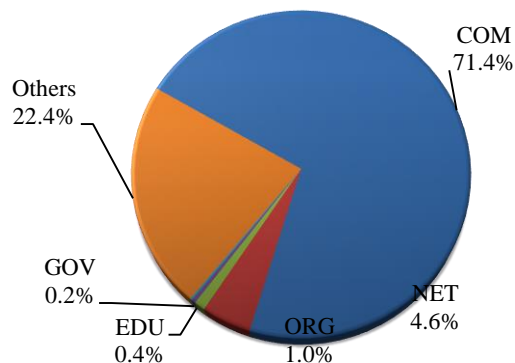
Defaced Websites in Mainland China (3/2-3/8)

CN CERT/CC

COM 80.9%
Others 18.8%
GOV 0.1%
ORG 0.1%
NET 0.1%

Domain Categories of the Backdoored Websites in Mainland China (3/2-3/8)

CN CERT/CC

COM 71.4%
Others 22.4%
GOV 0.2%
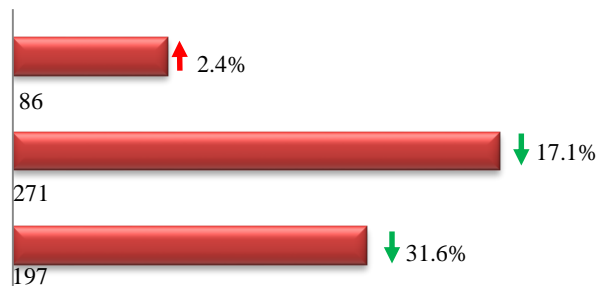EDU 0.4%
ORG 1.0%
NET 4.6%

Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 699 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.
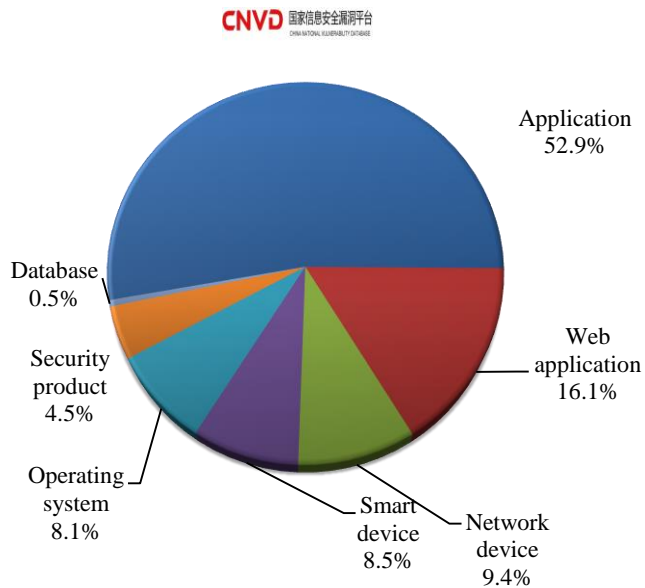
Low-risk vulnerability
86 ↑ 2.4%

Medium-risk vulnerability
271 ↓ 17.1%

High-risk vulnerability
197 ↓ 31.6%

**Objectives Affected by the Vulnerabilities
Collected by CNVD (3/2-3/8)**

CNVD 国家信息安全漏洞平台
CHINA NATIONAL VULNERABILITY DATABASE

Application
52.9%

Database
0.5%

Security
product
4.5%

Operating
system
8.1%

Smart
device
8.5%

Network
device
9.4%

Web
application
16.1%

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 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.
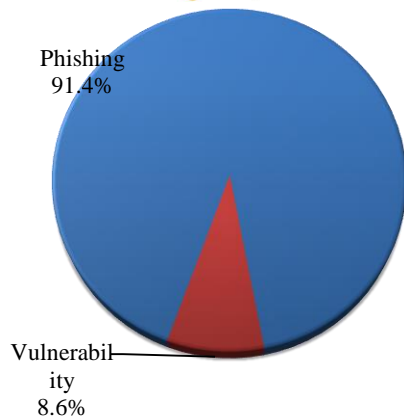
Incident Handling

This week, CNCERT has handled 525 network security incidents, 235 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
(3/2-3/8)

CN<u>C</u>ERT/CC

Phishing
91.4%

Overseas reported
incident handled by
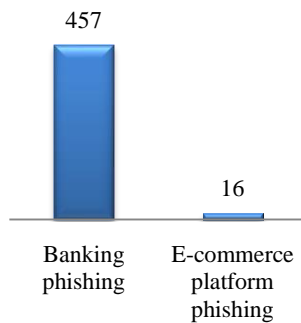coordinating domestic
organizations

2

Domesticlly reported
incident handled by
coordinating overseas
organizations

233

Vulnerabil
ity
8.6%

Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 480 phishing incidents. Based on industries that these phishing targets belong to, there were mainly 457 banking phishing incidents and 16 e-commerce platform incidents.
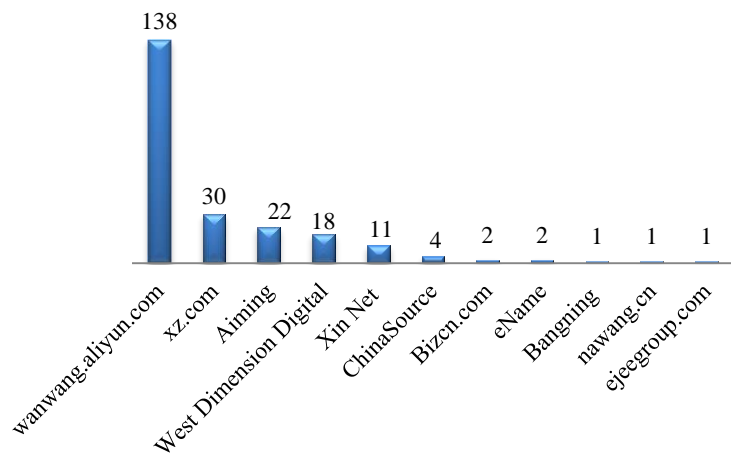
Phishing Incidensts Handled by
CNCERT Based on Industries of the
Phishing Targets (3/2-3/8)

CN<u>C</u>ERT/CC

457

16

Banking
phishing

E-commerce
platform
phishing

CNCERT Coordinated Domestic
to Handle Phishing Incidents (3/2-3/8)

CN<u>C</u>ERT/CC

138

30

22

18

11

4

2

2

1

1

1

wanwang.aliyun.com

xz.com

Aiming

West Dimension Digital

Xin Net

ChinaSource

Bizcn.com

eName

Bangning

nawang.cn

ejeegroup.com

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (3/2-3/8)

CN⊕ERT/CC

This week, CNCERT has coordinated 6 mobile phone application store and malware-injected domains to handle 31 malicious URL of the mobile malware.

Domain	Count
baidu.com	26
aliyuncs.com	19
360tpcdn.com	7
vivo.com.cn	4
59370.com	1
5you.com	1
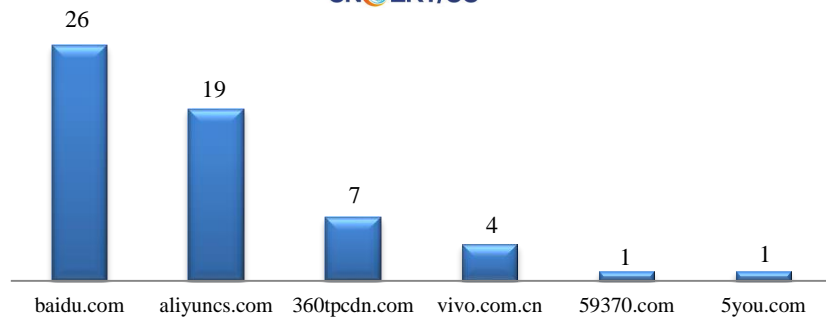
About CNCERT

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: Jia Zixiao

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315