Weekly Report of CNCERT

CN ERT/CC

Key Findings

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

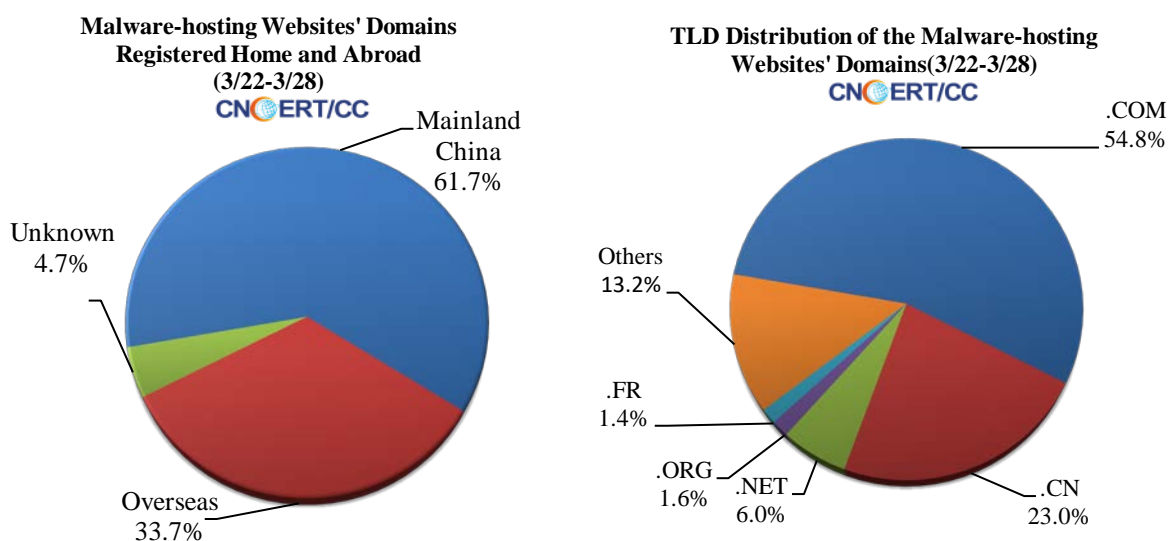|		
Times of transmission of malware in mainland China	• 21.4Million	↑ 92.0%
Infected Computers Controlled by Trojans or Botnets in Mainland China	• 0.38Million	↑ 8.6%
Defaced Websites in Mainland China	• 3,198	↑ 73.8%
Defaced gov.cn	• 13	↑ 44.4%
Backdoored Websites in Mainland China	• 563	↑ 7.9%
Backdoored gov.cn	• 9	↑ 350%
Phishing Webpages Targeting Websites in Mainland China	• 982	↑ 155.1%
New Vulnerabilities Collected by CNVD	• 719	↑ 5.9%
High-risk Vulnerabilities	• 166	↑ 38.3%

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

Malware Activities

The Times of transmission of malware and infected computers controlled by Trojans or Botnets in mainland China amounted to about 21.4 million and 0.38 million.

Malware ↑ 92.0%
21.4Million

Trojans or Botnet ↑ 8.6%
0.38 Million
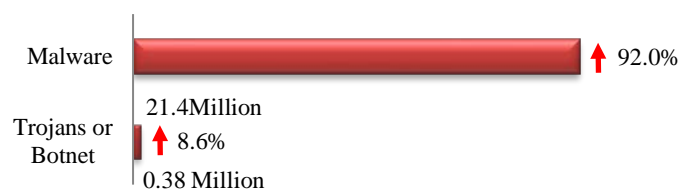
The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 832 domains and 4,408 IP addresses. Among the 832 malicious domains, 33.7% of them were registered abroad, 54.8% of their TLDs fell into the category of .com. Among the 4,408 IP addresses, 40.8% were registered abroad. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain, and 420 were accessed directly via IPs.

Malware-hosting Websites' Domains Registered Home and Abroad (3/22-3/28)
CNCERT/CC

Mainland China 61.7%
Unknown 4.7%
Overseas 33.7%

TLD Distribution of the Malware-hosting Websites' Domains(3/22-3/28)
CNCERT/CC

.COM 54.8%
Others 13.2%
.FR 1.4%
.ORG 1.6%
.NET 6.0%
.CN 23.0%

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 3,198 defaced websites in mainland China and 563 websites planted with backdoors and 982 phishing web pages targeting websites in mainland China.

Phishing pages targeting websites in mainland China
982 ↑ 155.1%

Defaced websites in mainland China
3198 ↑ 73.8%

Backdoored websites in mainland China
563 ↑ 7.9%
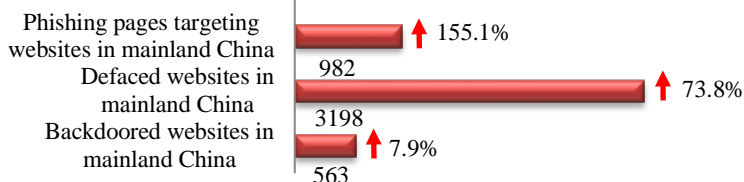
This week, the defaced government (gov.cn) websites totaled 13 (0.6%), an increase of 44.4% from last week. The backdoors were installed into 9 government (gov.cn) websites.
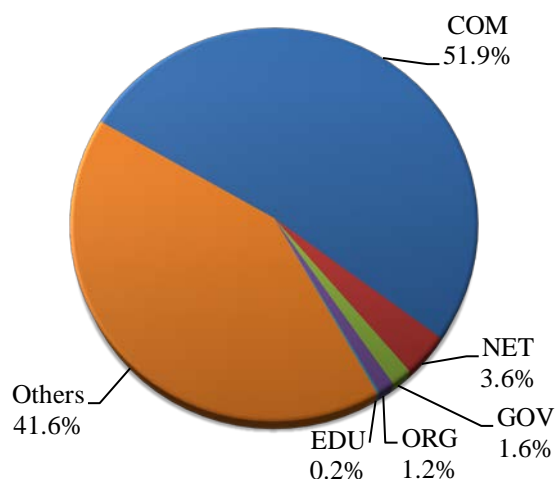
Defaced Websites in Mainland China
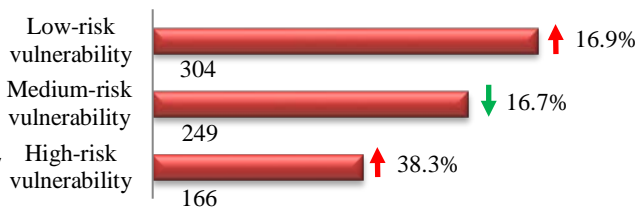**(3/22-3/28)**
CNCERT/CC

COM 74.2%
Others 17.9%
INFO 0.1%
EDU 0.1%
GOV 0.4%
ORG 1.8%
NET 5.6%
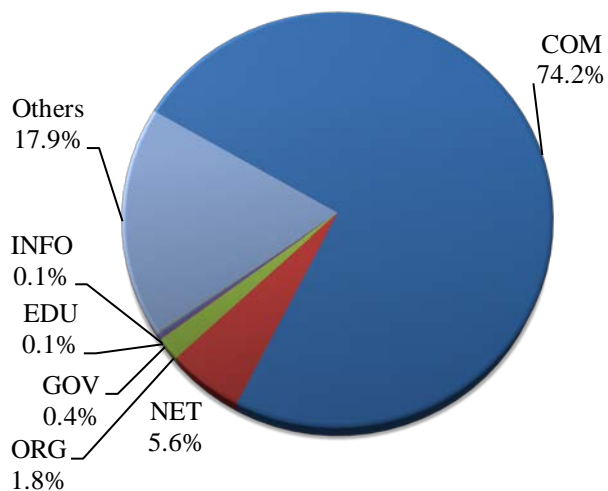
Domain Categories of the Backdoored Websites in Mainland China
(3/22-3/28)
CNCERT/CC

COM 51.9%
Others 41.6%
NET 3.6%
GOV 1.6%
ORG 1.2%
EDU 0.2%

Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 719 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.

Low-risk vulnerability
304 ↑ 16.9%

Medium-risk vulnerability
249 ↓ 16.7%

High-risk vulnerability
166 ↑ 38.3%

Objectives Affected by the Vulnerabilities Collected by CNVD (3/22-3/28)
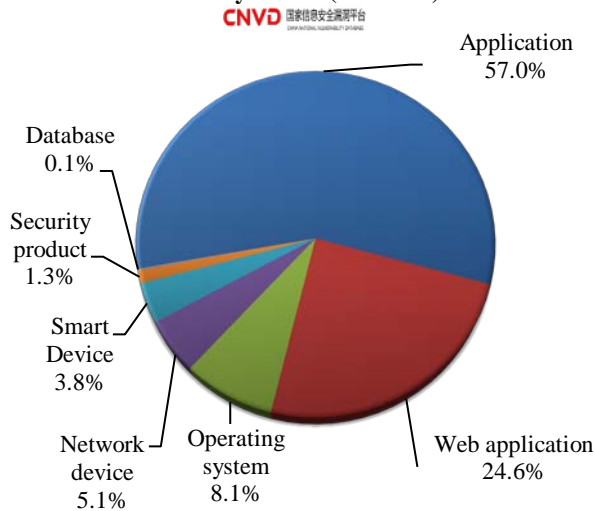
The Application was most frequently affected by these vulnerabilities collected by CNVD, followed by Web application and Operating System.

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

Incident Handling
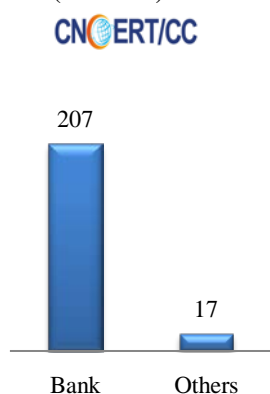
This week, CNCERT has handled 287 network security incidents, 66 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

Types of the Incidents Handled by CNCERT (3/22-3/28)

Overseas reported incident handled by coordinating… 60

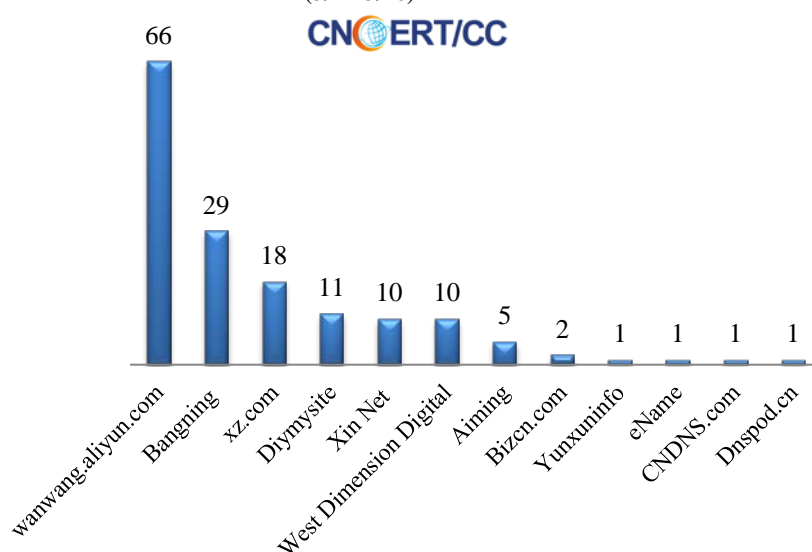Domesticlly reported incident handled by coordinating… 6
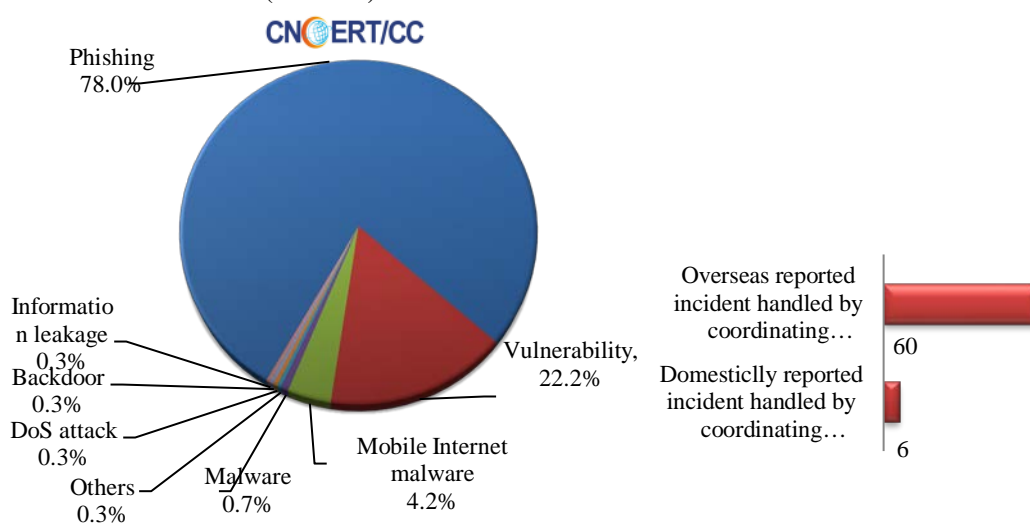
Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 224 phishing incidents. Based on industries that these phishing targets belong to, there were 207 banking phishing incidents and 17 other incidents.
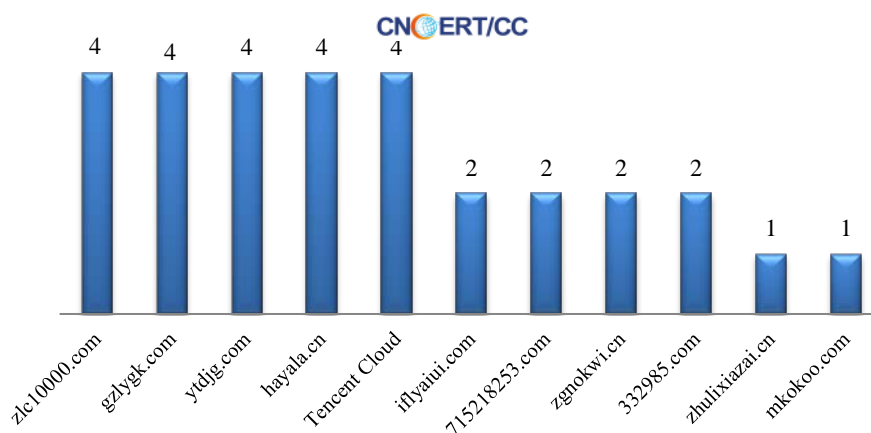
Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (3/22-3/28)

CNCERT/CC

Bank	Others
207	17

CNCERT Coordinated Domestic to Handle Phishing Incidents (3/22-3/28)

CNCERT/CC

wanwang.aliyun.com	Bangning	xz.com	Diymysite	Xin Net	West Dimension Digital	Aiming	Bizcn.com	Yunxuninfo	eName	CNDNS.com	Dnspod.cn
66	29	18	11	10	10	5	2	1	1	1	1

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (3/22-3/28)

CNCERT/CC

This week, CNCERT has coordinated 12 mobile phone application stores and malware-injected domains to handle 30 malicious URLs of the mobile malware.

zlc10000.com	gzlygk.com	ytdjg.com	hayala.cn	Tencent Cloud	iflyaiui.com	715218253.com	zgnokwi.cn	332985.com	zhulixiazai.cn	mkokoo.com
4	4	4	4	4	2	2	2	2	1	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 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: Wang Ying

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315