Weekly Report of CNCERT

CNCERT/CC

Key Findings

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

Times of Transmission of Malware in Mainland China **Infected Computers Controlled by Trojans or Botnets in Mainland China**	• 50.3 Million • 0.68 Million	↑ 1.8% ↓ 28.9%
Defaced Websites in Mainland China **Defaced gov.cn**	• 1,315 • 7	↑ 31.1% ↑ 133.3%
Backdoored Websites in Mainland China **Backdoored gov.cn**	• 1,161 • 48	↓ 2.0% ↑ 140.0%
Phishing Webpages Targeting Websites in Mainland China	• 413	↓ 49.9%
New Vulnerabilities Collected by CNVD **High-risk Vulnerabilities**	• 430 • 113	↓ 37.5% ↓ 44.6%

= *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 50.3 million and 0.68 million.

Malware ↑ 1.8%

50.3 Million

Trojans or Botnet ↓ 28.9%

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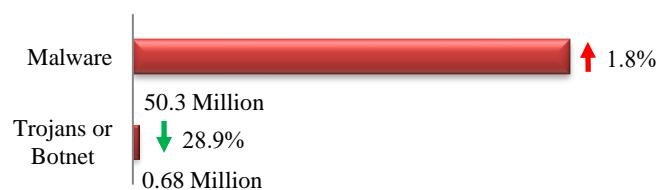
In terms of the malicious domain names and IPs either monitored by CNCERT or sourced from the reporting members, CNCERT has actively coordinated the domain registrars and other related agencies to handle them. Moreover, the blacklist of these malicious domains and IPs has been published on the website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

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

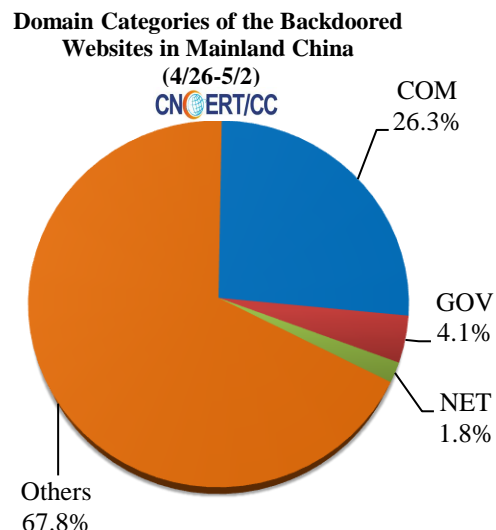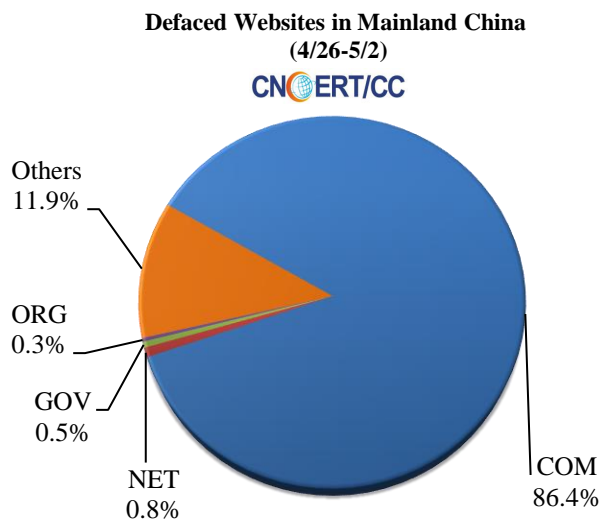http://www.anva.org.cn/virusAddress/listBlack

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 1,315 defaced websites in mainland China and 1,161 websites planted with backdoors and 413 phishing web pages targeting websites in mainland China.

Defaced websites in mainland China — 1315 — ↑ 31.1%
Backdoored websites in mainland China — 1161 — ↓ 2.0%
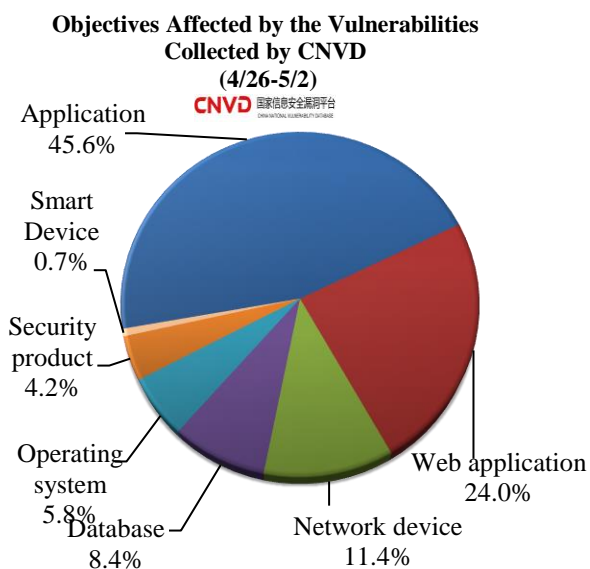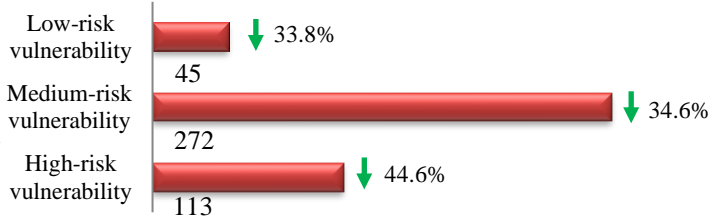Phishing pages targeting websites in mainland China — 413 — ↓ 49.9%
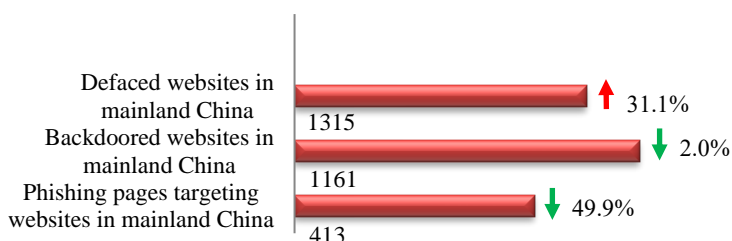
This week, the defaced government (gov.cn) websites totaled 7 (0.5% of domestic websites), an increase of 133.3% from last week. The backdoors were installed into 48 government (gov.cn) websites (4.1% of domestic websites), an increase of 140.0% from last week.

Defaced Websites in Mainland China (4/26-5/2)

CN CERT/CC

- Others 11.9%
- ORG 0.3%
- GOV 0.5%
- NET 0.8%
- COM 86.4%

Domain Categories of the Backdoored Websites in Mainland China (4/26-5/2)

CN CERT/CC

- COM 26.3%
- GOV 4.1%
- NET 1.8%
- Others 67.8%

Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 430 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.

Low-risk vulnerability	↓ 33.8%	
	45	
Medium-risk vulnerability	↓ 34.6%	
	272	
High-risk vulnerability	↓ 44.6%	
	113	

Objectives Affected by the Vulnerabilities Collected by CNVD (4/26-5/2)

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

- Application 45.6%
- Smart Device 0.7%
- Security product 4.2%
- Operating system 5.8%
- Database 8.4%
- Network device 11.4%
- Web application 24.0%

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.
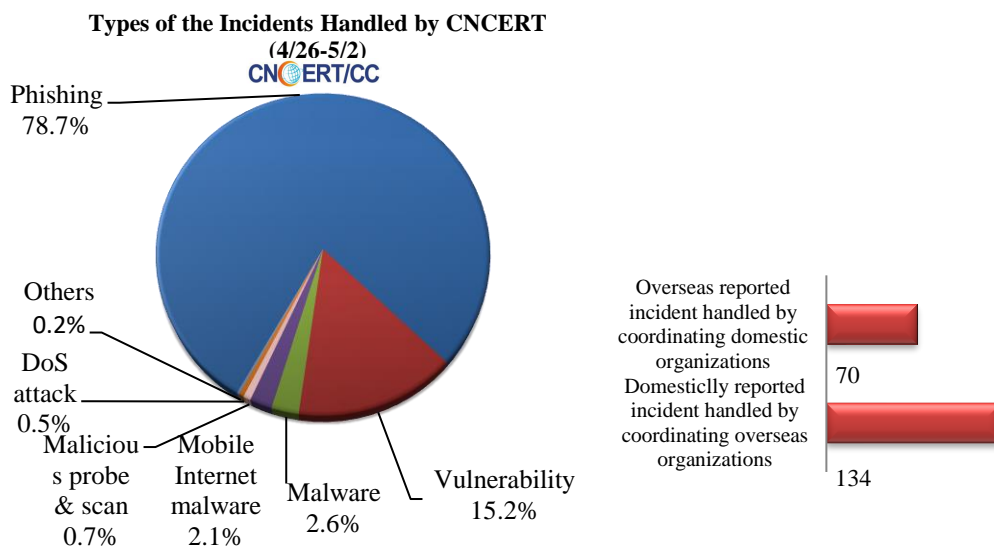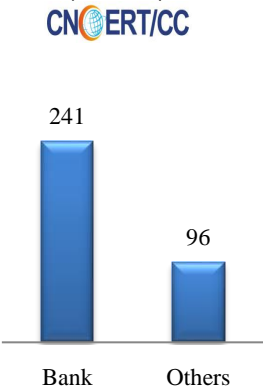
Incident Handling

This week, CNCERT has handled 428 network security incidents, 204 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 (4/26-5/2)

CNCERT/CC

Phishing 78.7%

Others 0.2%

DoS attack 0.5%

Malicious probe & scan 0.7%

Mobile Internet malware 2.1%

Malware 2.6%

Vulnerability 15.2%

Overseas reported incident handled by coordinating domestic organizations — 70

Domesticlly reported incident handled by coordinating overseas organizations — 134
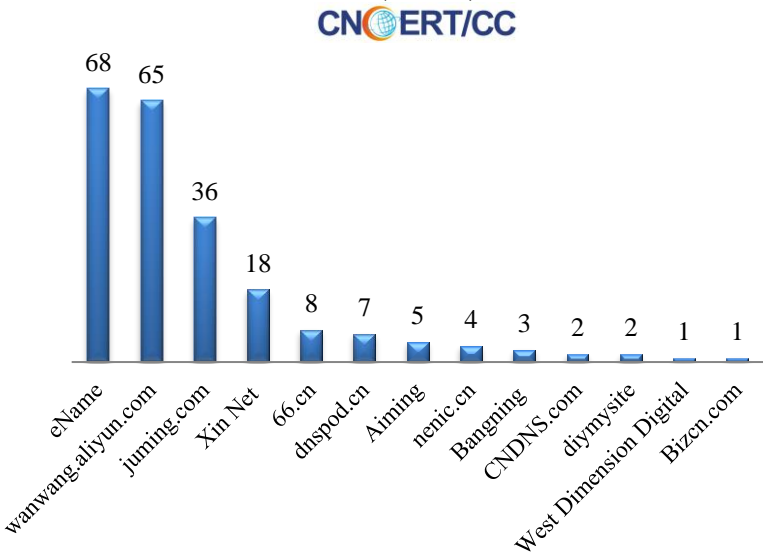
4

Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs, and the other organizations to handle 337 phishing incidents. Based on industries that these phishing targets belong to, there were 241 banking phishing incidents and 96 other incidents.

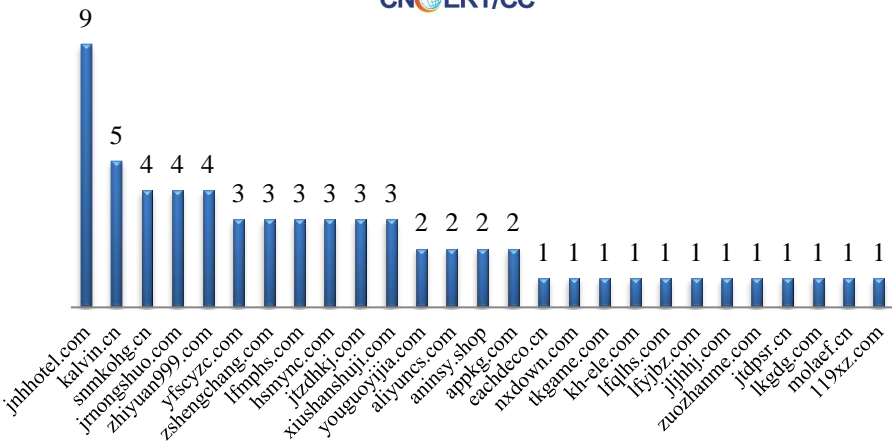**Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (4/26-5/2)**

CNCERT/CC

Bank	Others
241	96

CNCERT Coordinated Domestic to Handle Phishing Incidents (4/26-5/2)

CNCERT/CC

eName	wanwang.aliyun.com	juming.com	Xin Net	66.cn	dnspod.cn	Aiming	nenic.cn	Bangning	CNDNS.com	diymysite	West Dimension Digital	Bizcn.com
68	65	36	18	8	7	5	4	3	2	2	1	1

This week, CNCERT has coordinated 28 mobile phone application stores and malware-injected domains to handle 64 malicious URLs of the mobile malware.

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (4/26-5/2)

CNCERT/CC

jnhhotel.com	kalvin.cn	snmkohg.cn	jrnongshuo.com	zhiyuan999.com	yfscyzc.com	zshengchang.com	lfmphs.com	hsmync.com	jtzdhkj.com	xiushanshuiji.com	youguoyijia.com	aliyuncs.com	aninsy.shop	appkg.com	eachdeco.cn	nxdown.cn	tkgame.com	kh-ele.com	lfqihs.com	lfyjbz.com	jlihhj.com	zuozhanme.com	jfdpsr.cn	lkgdg.com	molaef.cn	119xz.com
9	5	4	4	4	3	3	3	3	3	3	2	2	2	2	1	1	1	1	1	1	1	1	1	1	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: Liu Liwei

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315