Weekly Report of CNCERT

CNCERT/CC

Key Findings

Excellent	Good	Fair	Poor	Very Poor

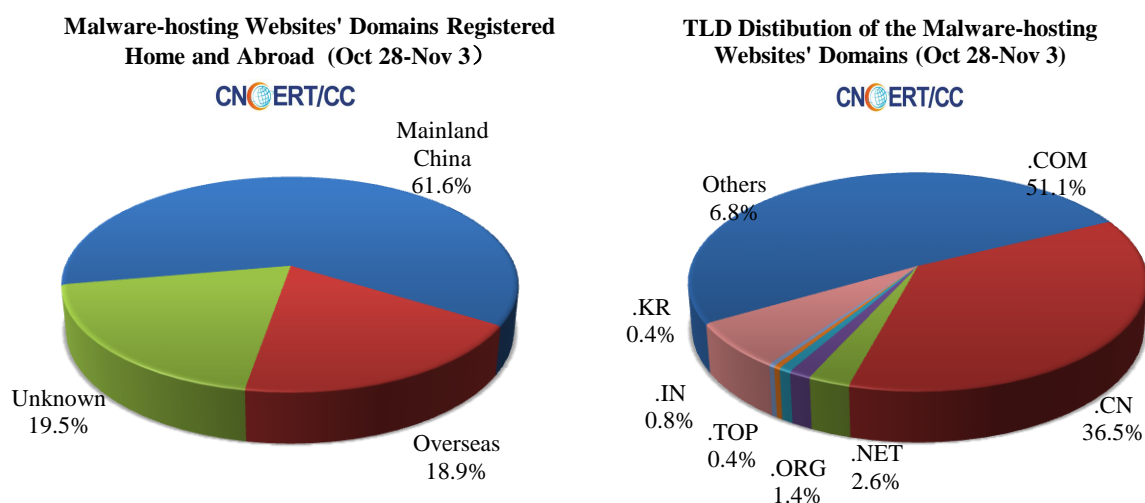| Infected Computers in Mainland China	• 0.62Million	↑ 5.5%
Backdoored Websites in Mainland China **Backdoored gov.cn**	• 2,975 • 73	↓ 4.6% ↑ 128.1%
Phishing Webpages Targeting Websites in Mainland China	• 1884	↑ 229.4%
New Vulnerabilities Collected by CNVD **High-risk Vulnerabilities**	• 478 • 92	↓ 0.2% ↓ 26.4%

═ *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 0.62 million, among which about 0.54 million were controlled by Trojans or Botnets and about 0.08 million by Confickers.

Trojans or Botnet ↑ 4.9%
0.54million

Conficker ↑ 9.4%
0.08million
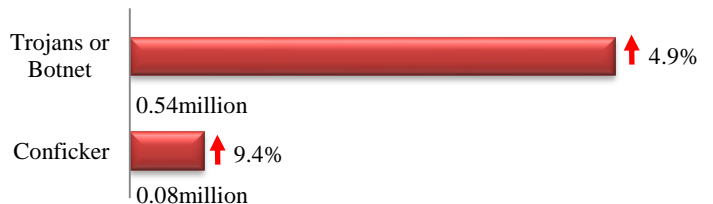
The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 3,291 domains and 2,712 IP addresses. Among the 3,291 malicious domains, 18.9 % were registered overseas and 51.1% of their TLDs fell into the category of.com. Among the 2,712 malicious IPs, 45.9% were overseas. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain names, and only 414 were accessed directly via IPs.

Malware-hosting Websites' Domains Registered Home and Abroad（Oct 28-Nov 3）

CNCERT/CC

- Mainland China 61.6%
- Overseas 18.9%
- Unknown 19.5%

TLD Distibution of the Malware-hosting Websites' Domains (Oct 28-Nov 3)

CNCERT/CC

- .COM 51.1%
- .CN 36.5%
- .NET 2.6%
- .ORG 1.4%
- .TOP 0.4%
- .IN 0.8%
- .KR 0.4%
- Others 6.8%

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 2,975 websites planted with backdoors and 1,884 phishing web pages targeting websites in mainland China.

Backdoored websits in mainland China
2,975
↓ 4.6%

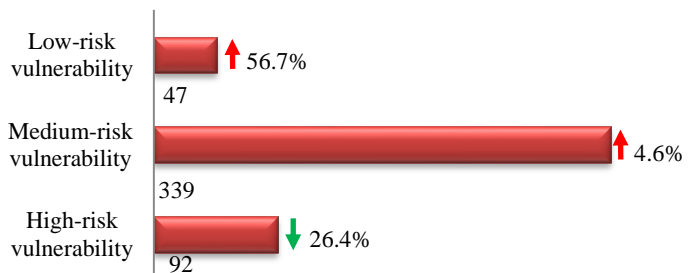Phishing pages targeting websites in mainland China
1884
↑ 229.4%
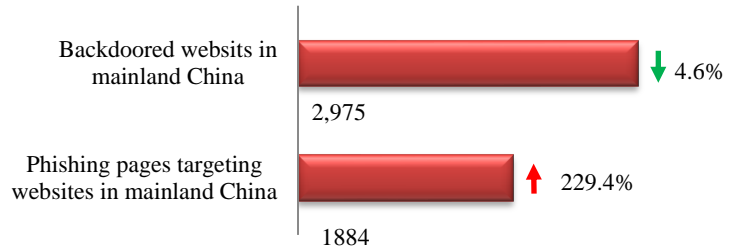
This week, the backdoors were installed into 73(2.5%) government (gov.cn) websites, an increase of 128.1% from last week. The fake domains and IP addresses targeting websites in mainland China reached 1,145 and 385 respectively, with each IP address loading about 5 phishing web pages on average.

Domain Categories of the Backdoored Websites in Mainland China (Oct 28-Nov 3)

CN⊕ERT/CC

COM 69.0%

Others 22.9%

EDU 0.2%

MIL 0.3%

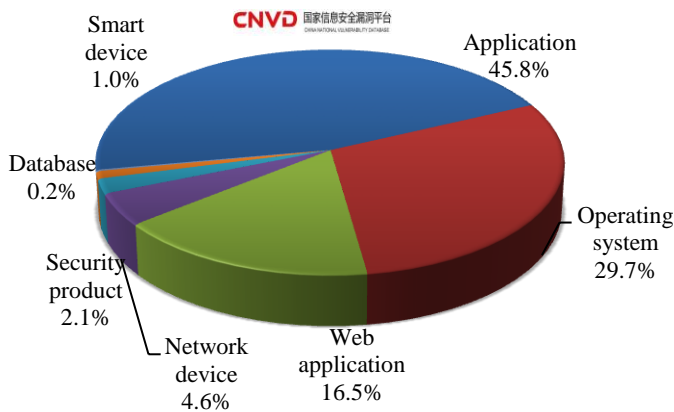ORG 1.7%

GOV 2.5%

NET 3.5%
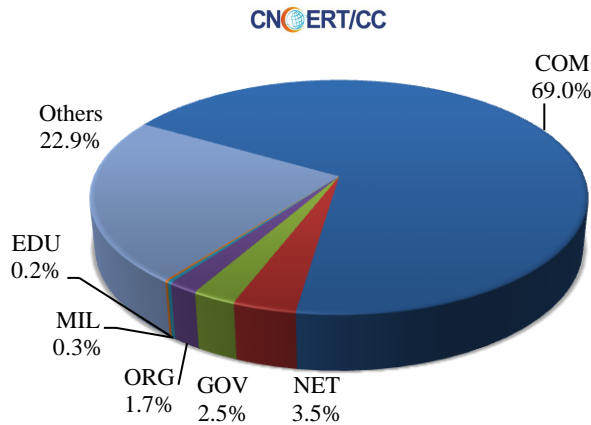
Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 478 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.

Low-risk vulnerability
47
↑ 56.7%

Medium-risk vulnerability
339
↑ 4.6%

High-risk vulnerability
92
↓ 26.4%

**Objectives Affected by the Vulnerabilities Collected
by CNVD (Oct 28-Nov 3)**

- Smart device 1.0%
- Database 0.2%
- Security product 2.1%
- Network device 4.6%
- Web application 16.5%
- Operating system 29.7%
- Application 45.8%

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

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

The URL of CNVD for Publishng Weekly Vulnerability Report

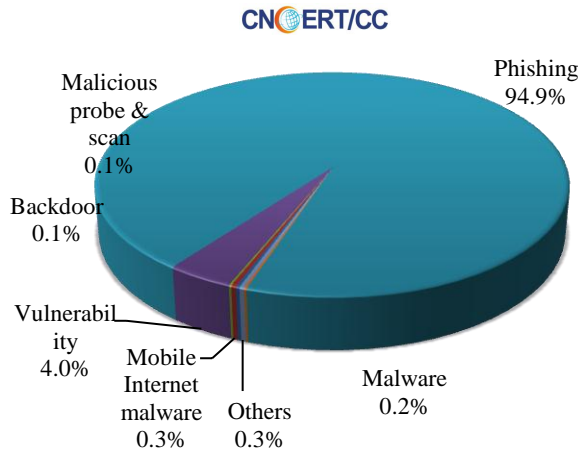http://www.cnvd.org.cn/webinfo/list?type=4

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 1,347 network security incidents, 702 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
(Oct 28-Nov 3)**

- Malicious probe & scan 0.1%
- Backdoor 0.1%
- Vulnerability 4.0%
- Mobile Internet malware 0.3%
- Others 0.3%
- Malware 0.2%
- Phishing 94.9%

Overseas reported incident handled by coordinating domestic organizations — 9
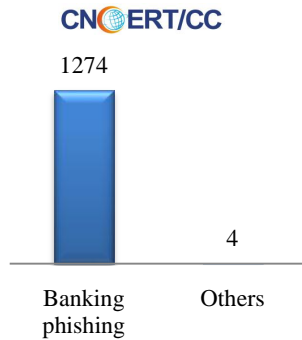
Domesticlly reported incident handled by coordinating overseas organizations — 693
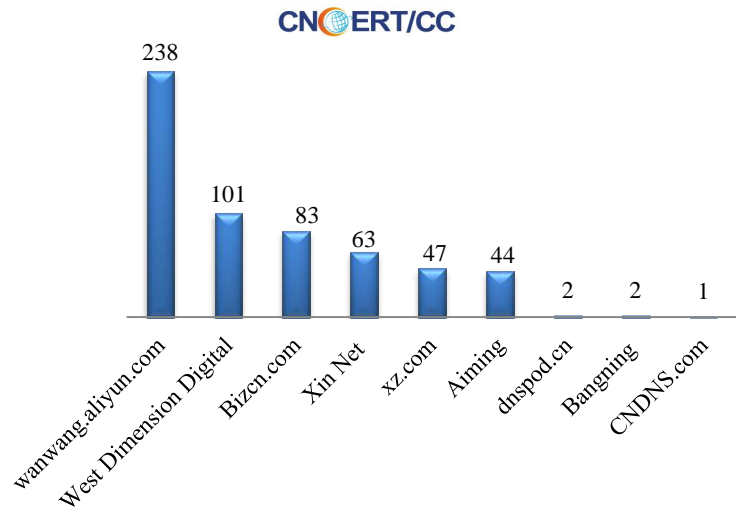
Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 1,278 phishing incidents. Based on industries that these phishing targets belong to, there were 1,274 banking phishing incidents and 4 other incidents..

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (Oct 28-Nov 3)

CNCERT/CC

- Banking phishing: 1274
- Others: 4

CNCERT Coordinated Domestic to Handle Phishing Incidents (Oct 28-Nov 3)

CNCERT/CC

- wanwang.aliyun.com: 238
- West Dimension Digital: 101
- Bizcn.com: 83
- Xin Net: 63
- xz.com: 47
- Aiming: 44
- dnspod.cn: 2
- Bangning: 2
- CNDNS.com: 1

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Oct 28-Nov 3)
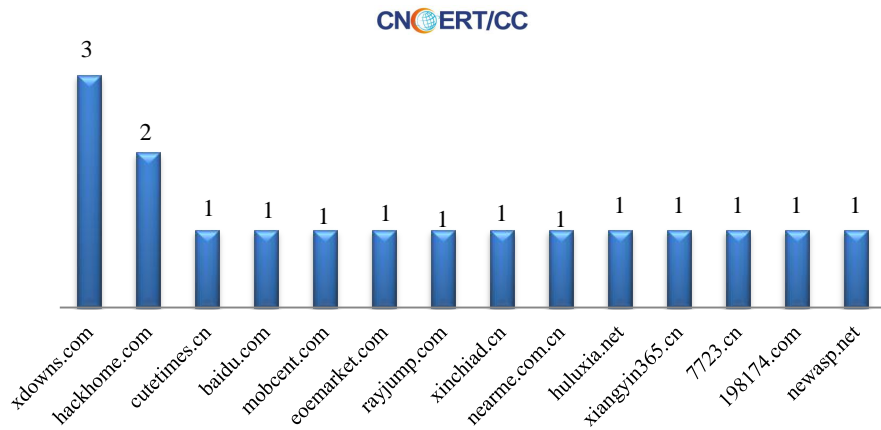
CNCERT/CC

This week, CNCERT has coordinated 14 mobile phone application store and malware-injected domains to handle 17 malicious URL of the mobile malware.

- xdowns.com: 3
- hackhome.com: 2
- cutetimes.cn: 1
- baidu.com: 1
- mobcent.com: 1
- eoemarket.com: 1
- rayjump.com: 1
- xinchiad.cn: 1
- nearme.com.cn: 1
- huluxia.net: 1
- xiangyin365.cn: 1
- 7723.cn: 1
- 198174.com: 1
- newasp.net: 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: Chang Xia

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315