

Weekly Report of CNCERT

Key Findings

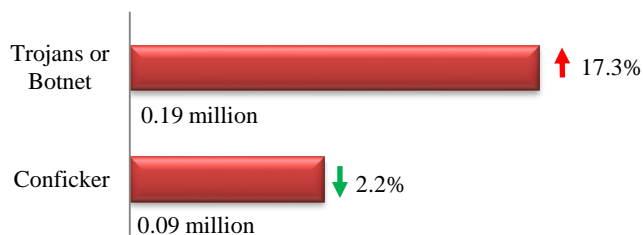


Infected Computers in Mainland China	• 0.28 Million	↑ 10.1%
Defaced Websites in Mainland China	• 466	↑ 90.2%
Defaced gov.cn	• 42	↑ 110.0%
Backdoored Websites in Mainland China	• 645	↓ 27.1%
Backdoored gov.cn	• 10	↑ 11.1%
Phishing Webpages Targeting Websites in Mainland China	• 1,417	↑ 9.8%
New Vulnerabilities Collected by CNVD	• 172	↓ 15.3%
High-risk Vulnerabilities	• 70	↓ 22.2%

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

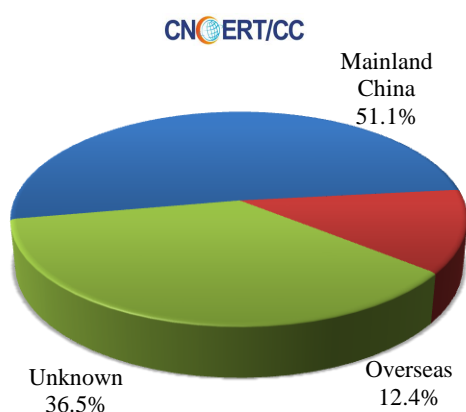
Malware Activities

The infected computers in mainland China amounted to about 0.28 million, among which about 0.19 million were controlled by Trojans or Botnets and about 0.09 million by Confickers.

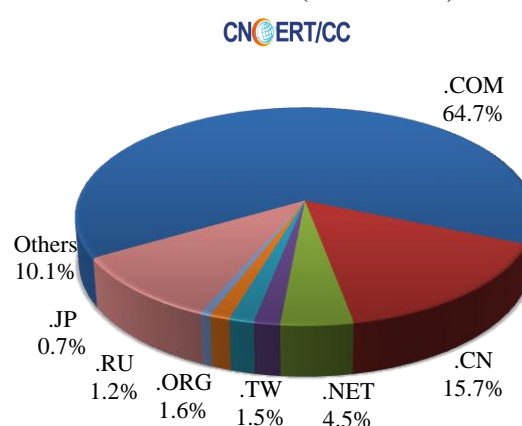


The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 5,573 domains and 6,186 IP addresses. Among the 5,573 malicious domains, 12.4% were registered overseas and 64.7% of their TLDs fell into the category of .com. Among the 6,186 malicious IPs, 52.7% were overseas. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain names, and only 579 were accessed directly via IPs.

Malware-hosting Websites' Domains Registered Home and Abroad (Nov 5-Nov 11)



TLD Distribution of the Malware-hosting Websites' Domains (Nov 5-Nov 11)



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.

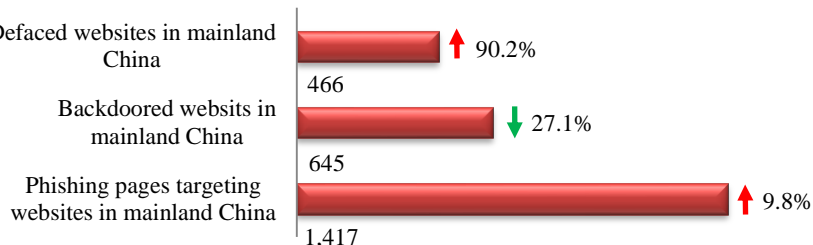
<http://www.anva.org.cn/virusAddress/listBlack>

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

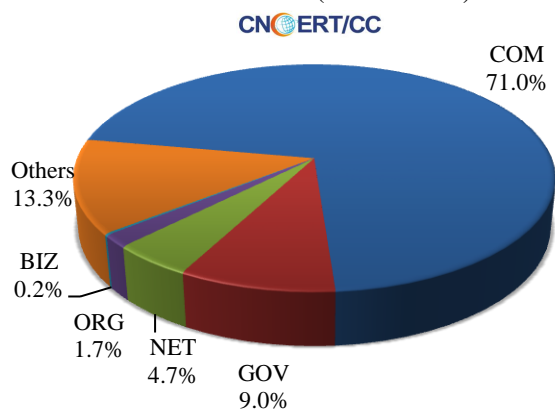
This week, CNCERT monitored

466 defaced websites, 885 defaced websites in mainland China, 466 websites planted with backdoors, 885 backdoored websites in mainland China, and 1,417 phishing web pages targeting websites in mainland China.

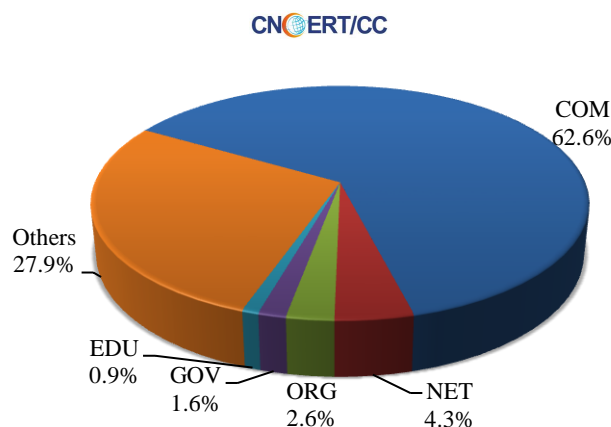


This week, the defaced government (gov.cn) websites totaled 42 (9.0%), an increase of 110.0% from last week. Backdoors were installed into 10 (1.6%) government (gov.cn) websites, an increase of 11.1% from last week. The fake domains and IP addresses targeting websites in mainland China reached 417 and 228 respectively, with each IP address loading about 5 phishing web pages on average.

Domain Categories of the Defaced Websites in Mainland China (Nov 5-Nov 11)

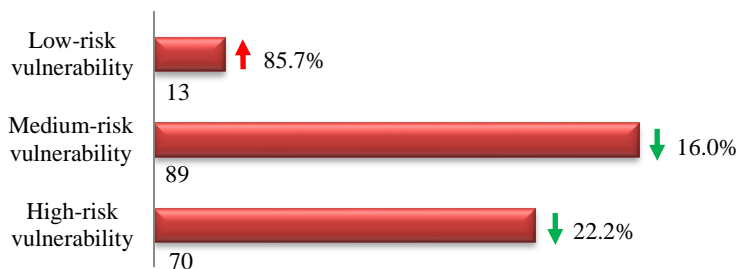


Domain Categories of the Backdoored Websites in Mainland China (Nov 5-Nov 11)

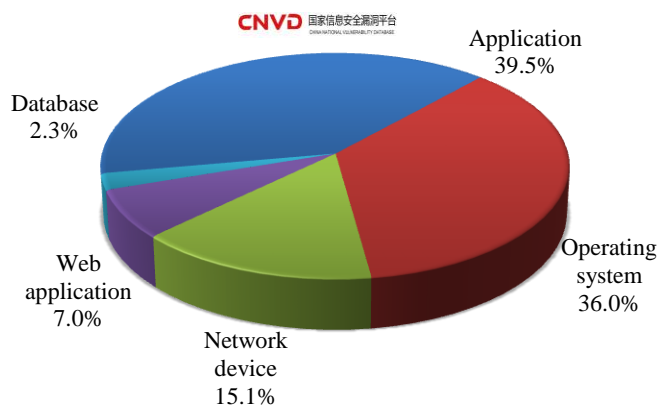


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 172 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (Nov 5-Nov 11)



The Application was most frequently affected by these vulnerabilities collected by CNVD, followed by the Operating system and the Network device.

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

The URL of CNVD for Publishing Weekly Vulnerability Report

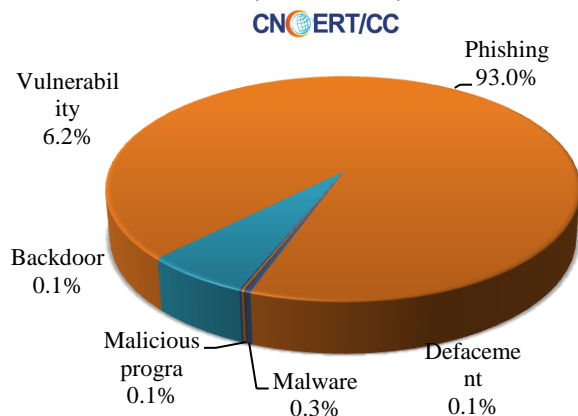
<http://www.cnvd.org.cn/webinfo/list?type=4>

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 705 network security incidents, 260 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 (Nov 5-Nov 11)



Overseas reported incident handled by coordinating domestic organizations

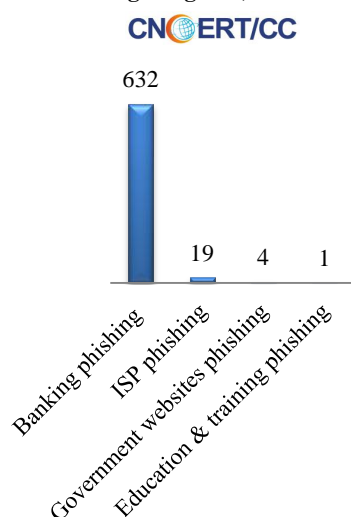
1

Domestically reported incident handled by coordinating overseas organizations

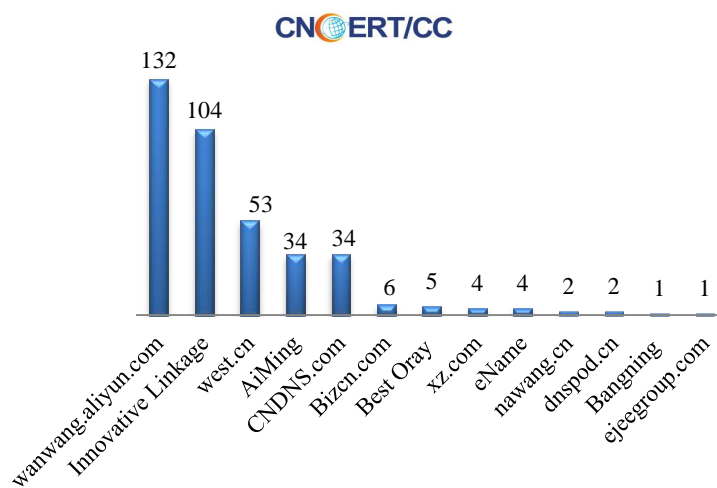
259

Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 656 phishing incidents. Based on industries that these phishing targets belong to, there were 632 banking phishing incidents and 19 ISP phishing incidents.

Phishing Incidents Handled by CNCERT Based on Industries of the Phishing Targets (Nov 5-Nov 11)

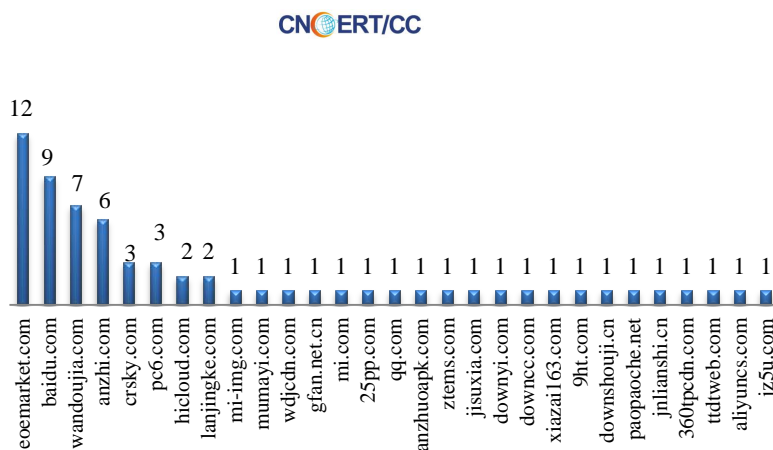


CNCERT Coordinated Domestic to Handle Phishing Incidents (Nov 5-Nov 11)



CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Nov 5-Nov 11)

This week, CNCERT has coordinated 29 mobile phone application store and malware-injected domains to handle 65 malicious URL of the mobile malware.



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: Liu Xiaomin

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158