CNCERT/CC

Issue 10 2013

Mar 4-10

Weekly Report of CNCERT

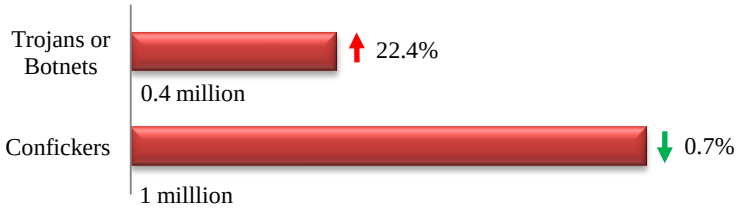
Key Findings

Infected Computers in Mainland China	• 1.4 Million	↑ 5.6%
Defaced Websites in Mainland China Defaced gov.cn	• 6,508 • 616	↓ 1.6% ↑ 24.9%
Backdoored Websites in Mainland China Backdoored gov.cn	• 2,092 • 97	↓ 7.9% ↓ 5.8%
Phishing Webpages Targeting Websites in Mainland China	• 927	↑ 11.2%
New Vulnerabilities Collected by CNVD High-severity Vulnerabilities	• 113 • 30	↓ 31.5% ↓ 36.2%

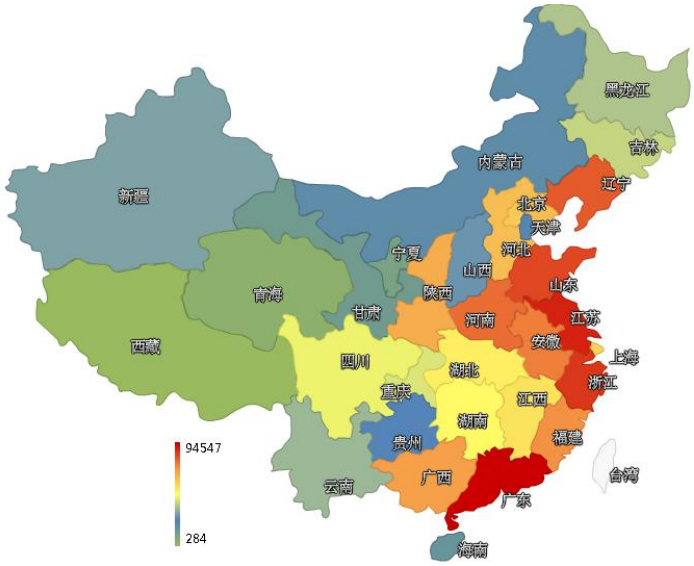
= marks the same number as last week; ↑ marks an increase from last week; ↓ marks a decrease from last week

Malware Activities

The infected computers in mainland China amounted to nearly 1.4 million, among which about 0.4 million were controlled by Trojans or Botnets and about 1 million by Confickers.



The map on the left illustrates distribution of the computers controlled by Trojans or Botnets in mainland China. The regions in red are most seriously affected. This week, the top 3 were Guangdong province, Jiangsu province and Zhejiang province.



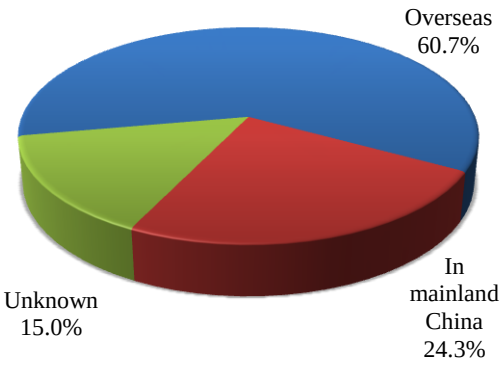
TOP3

Guangdong province	• about 95,000 (21.8%)
Jiangsu province	• about 31,000 (7.1%)
Zhejiang province	• about 26,000 (6%)

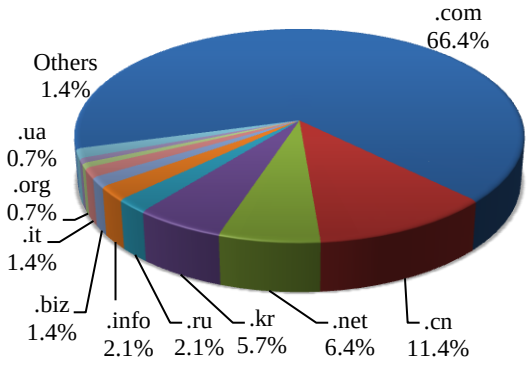
CNCERT captured a great number of new malware samples this week. 33 new malware names were identified, and 1 new malware family was detected.

The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 140 domains and 262 IP addresses. Among the 140 malicious domains, 60.7% were registered overseas and 66.4% of their TLDs fell into the category of.com. Among the 262 malicious IPs, 54.2% were located in mainland China and 45.8% were overseas. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain names, and only 98 were accessed directly via IPs.

Malware-hosting Websites' Domains Registered Home and Abroad (Mar 4-10)



TLD Distibution of the Malware-hosting Websites' Domains (Mar 4-10)



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).

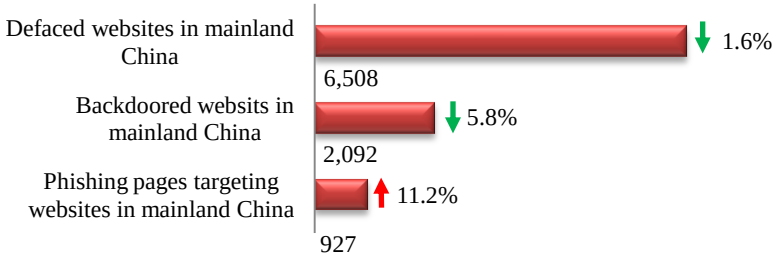
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

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.

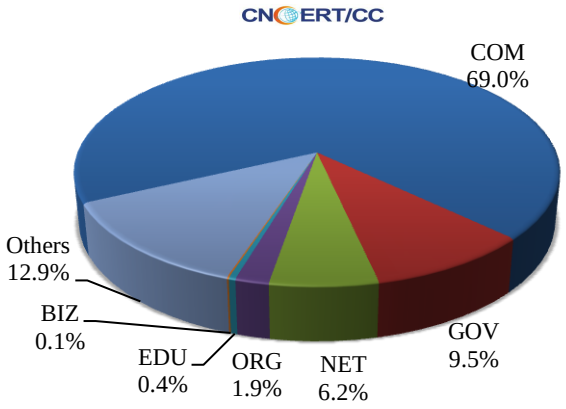
Website Security

This week, CNCERT monitored 6,508 defaced websites, 2,092 websites planted with backdoors and 927 phishing web pages targeting websites in mainland China.

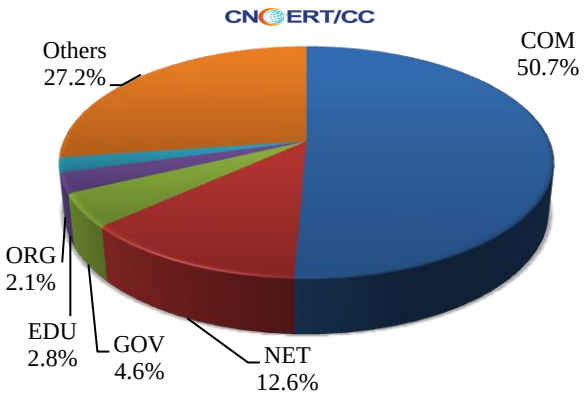


This week, the defaced government (gov.cn) websites totaled 616 (9.5%), an increase of 24.9% from last week. Backdoor were installed into 97 (4.6%) government (gov.cn) websites, which reduced by 5.8% from last week. The fake domains and IP addresses targeting websites in mainland reached 605 and 310 respectively, with each IP address loading about 3 phishing web pages on average.

Domain Categories of the Defaced Websits in Mainland China (Mar 4-10)

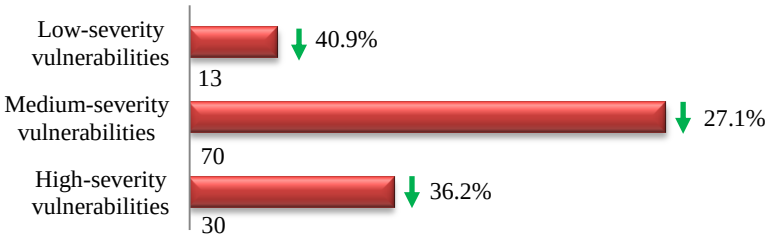


Domain Categories of the Backdoored Websites in Mainland China (Mar 4-10)

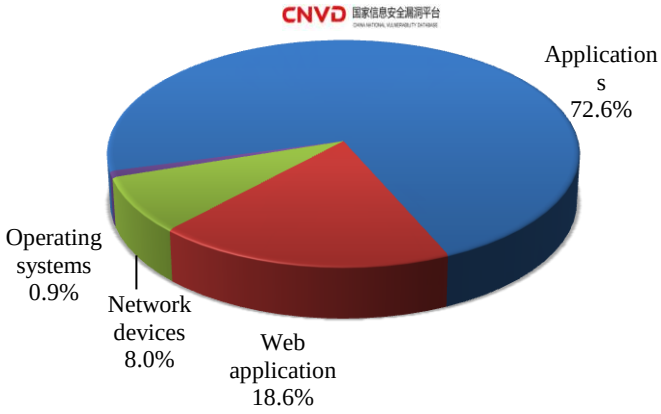


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 113 new vulnerabilities. This week's overall vulnerability severity was evaluated as low



Objectives Affected by the Vulnerabilities Collected by CNVD (Mar 4-10)



Applications were most frequently affected by these vulnerabilities collected by CNVD, followed by the web application and the network devices

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

The URL of CNVD for Publishng Weekly Vulnerability Report

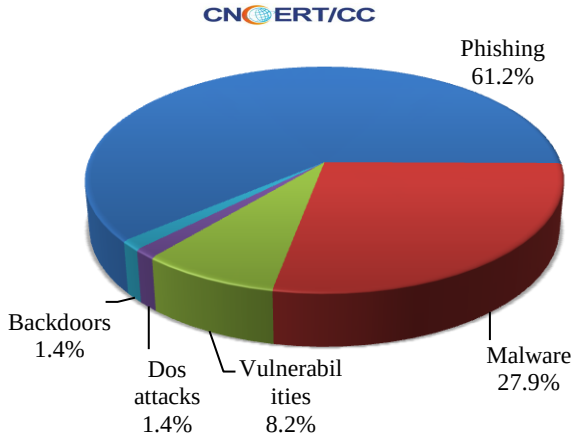
http://www.cnvd.org.cn/publish/main/47/index.html

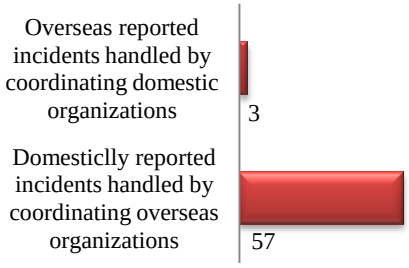
China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

Incident Handling

This week, CNCERT has handled 147 network security incidents, 60 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

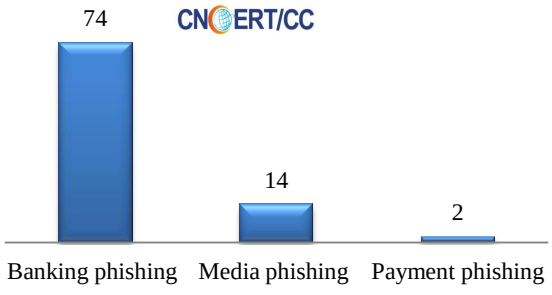
Types of the Incidents Handled by CNCERT (Mar 4-10)



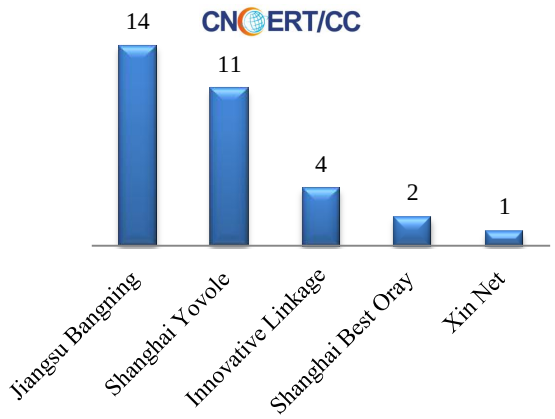


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 90 phishing incidents. Based on industries that these phishing targets belong to, there were 74 banking phishing incidents, 14 media incidents and 2 payment incident.

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (Mar 4-10)

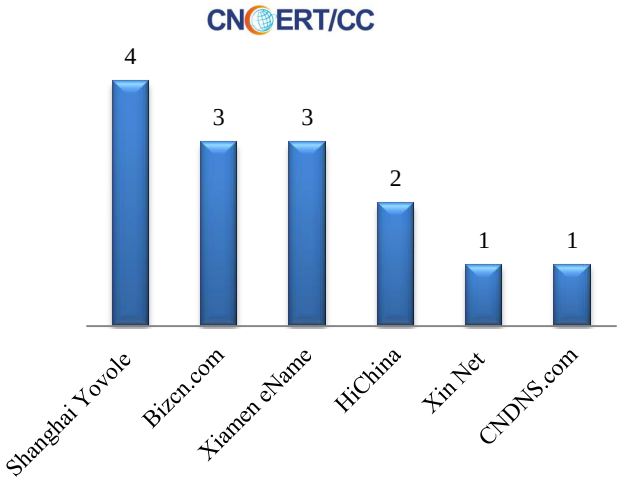


CNCERT Coordinated Domestic Domain Registrars to Handle Phishing Incidents (Mar 4-10)

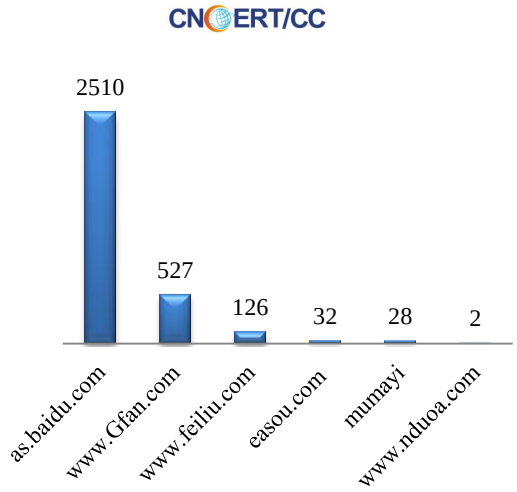


This week, CNCERT has coordinated 1 non-profit internet organization, 6 domestic domain registrars and 6 mobile phone application stores to handle 22 domains hosting malware and 3,225 malicious URLs of the mobile malware.

CNCERT Coordinated Domestic Domain Registrars to Handle Malware (Mar 4-10)



CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Mar 4-10)



About CNCERT

CNCERT or CNCERT/CC is the National CERT organization of China, which is serving as a national-level network security monitoring center, warning center and emergency handling center. It provides supports to the governmental departments for fulfilling their network security-related social management and public service functions, ensures the safe operation of national information infrastructures and undertakes the network security monitoring, early warning and emergency response of control systems. Branches of CNCERT spread in 31 provinces, autonomous regions and municipalities in mainland China.

Contact us

Should you have any comments or suggestions on the Weekly Report of CNCERT, please communicate with our editors.

Duty Editor: GAO Sheng

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn