CNCERT/CC

Issue 17 2018

Apr 23-Apr 29

Weekly Report of CNCERT

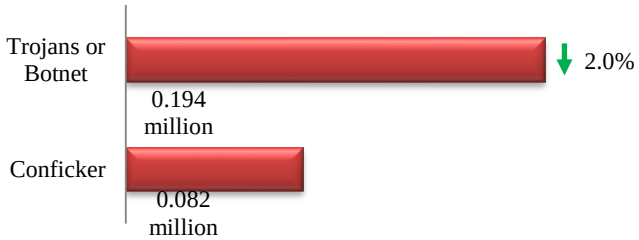
Key Findings

Infected Computers in Mainland China	• 0.276 Million	
Defaced Websites in Mainland China Defaced gov.cn	• 978 • 23	↓ 22.7% ↓ 30.3%
Backdoored Websites in Mainland China Backdoored gov.cn	• 1,046 • 18	↓ 19.2% ↓ 50.0%
Phishing Webpages Targeting Websites in Mainland China	• 821	↓ 2.5%
New Vulnerabilities Collected by CNVD High-risk Vulnerabilities	• 400 • 136	↑ 61.3% ↑ 70.0%

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

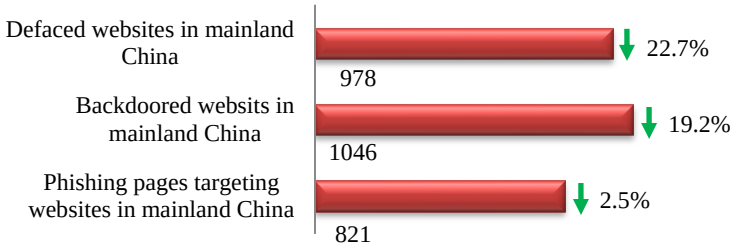
Malware Activities

The infected computers in mainland China amounted to about 0.276 million, among which about 0.194 million were controlled by Trojans or Botnets and about 0.082 million by Confickers.



Website Security

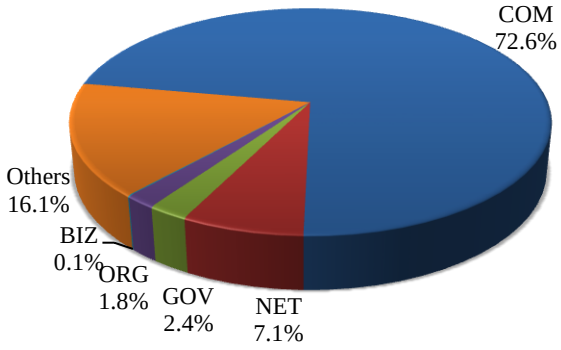
This week, CNCERT monitored 978 defaced websites, 1,046 websites planted with backdoors and 821 phishing web pages targeting websites in mainland China.



This week, the defaced government (gov.cn) websites totaled 23 (2.4%), a decrease of 30.3% from last week. Backdoors were installed into 18 (1.7%) government (gov.cn) websites, which decrease by 50.0% from last week. The fake domains and IP addresses targeting websites in mainland China reached 372 and 136 respectively, with each IP address loading about 6 phishing web pages on average.

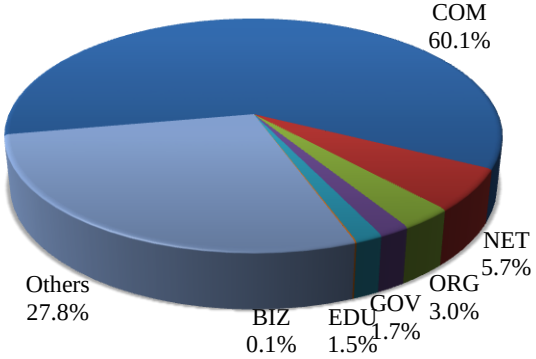
Domain Categories of the Defaced Websits in Mainland China (Apr 23-Apr 29)

CNCERT/CC



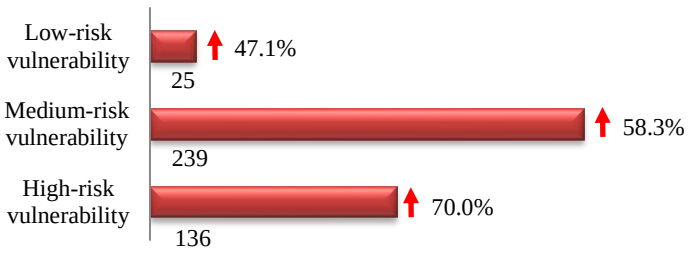
Domain Categories of the Backdoored Websites in Mainland China (Apr 23-Apr 29)

CNCERT/CC

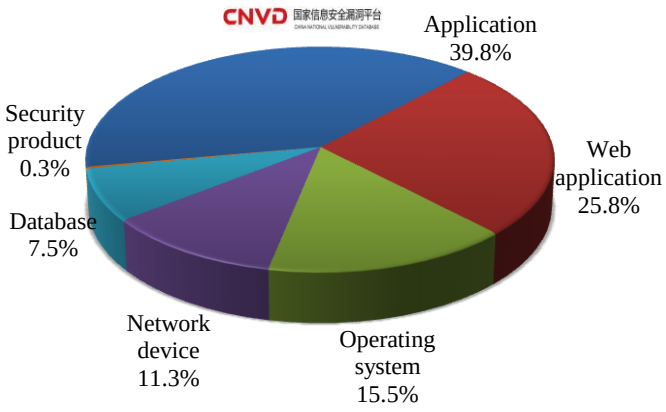


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 400 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (Apr 23-Apr 29)



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

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

The URL of CNVD for Publishng Weekly Vulnerability Report

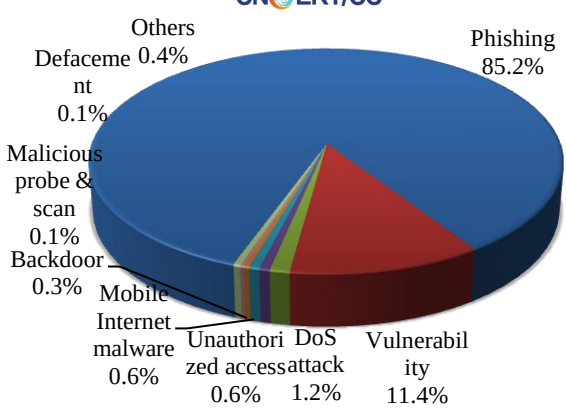
http://www.cnvd.org.cn/webinfo/list?type=4

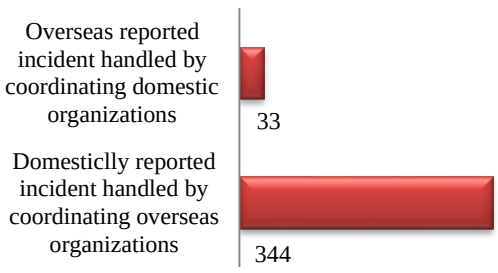
China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

Incident Handling

This week, CNCERT has handled 944 network security incidents, 377 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

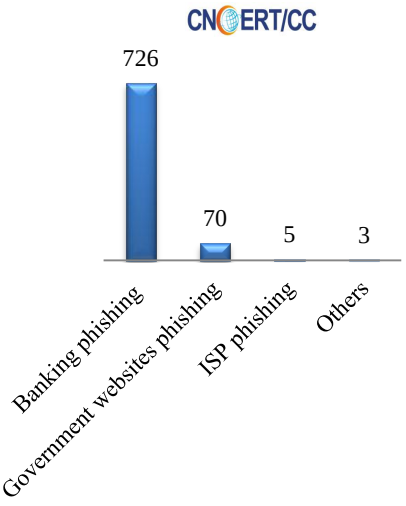
Types of the Incidents Handled by CNCERT (Apr 23-Apr 29)



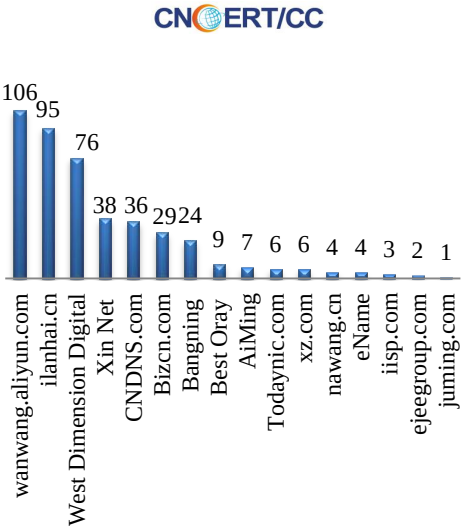


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 804 phishing incidents. Based on industries that these phishing targets belong to, there were 726 banking phishing incidents and 70 government websites phishing incidents.

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (Apr 23-Apr 29)

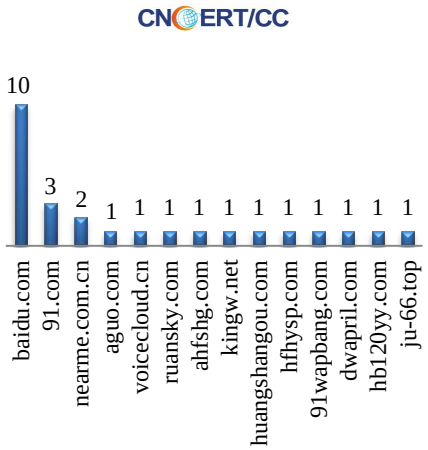


CNCERT Coordinated Domestic to Handle Phishing Incidents (Apr 23-Apr 29)



This week, CNCERT has coordinated 14 mobile phone application store and malware-injected domains to handle 26 malicious URL of the mobile malware.

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Apr 23-Apr 29)



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: LV Lifeng

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158