CNCERT/CC

Issue 19 2018

May 7-May 13

Weekly Report of CNCERT

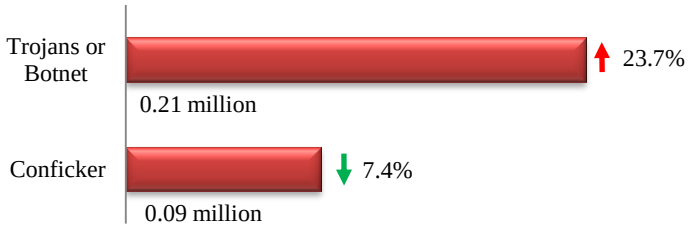
Key Findings

Infected Computers in Mainland China	• 0.30 Million	↑ 12.5%
Defaced Websites in Mainland China	• 1,092	↑ 5.0%
Defaced gov.cn	• 33	↓ 5.7%
Backdoored Websites in Mainland China	• 942	↑ 13.4%
Backdoored gov.cn	• 28	↑ 33.3%
Phishing Webpages Targeting Websites in Mainland China	• 1,430	↓ 9.4%
New Vulnerabilities Collected by CNVD	• 260	↑ 6.6%
High-risk Vulnerabilities	• 62	↓ 21.5%

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

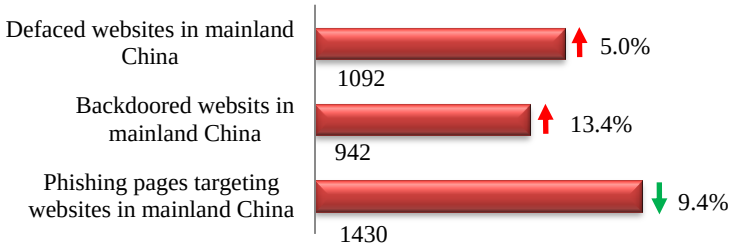
Malware Activities

The infected computers in mainland China amounted to about 0.30 million, among which about 0.21 million were controlled by Trojans or Botnets and about 0.09 million by Confickers.

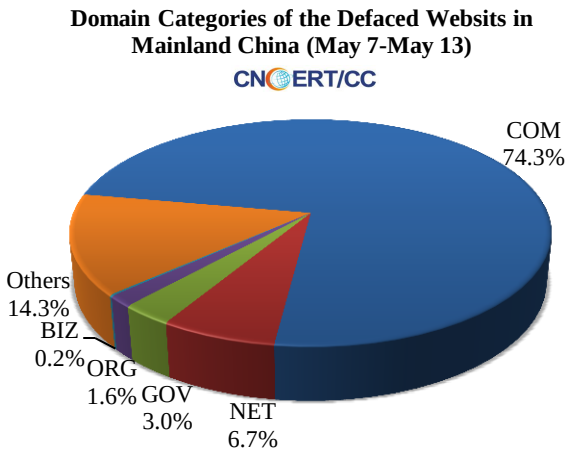


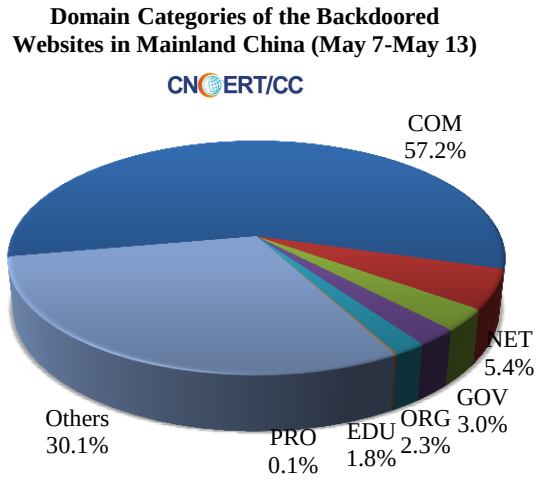
Website Security

This week, CNCERT monitored 1,092 defaced websites, 942 websites planted with backdoors and 1,430 phishing web pages targeting websites in mainland China.



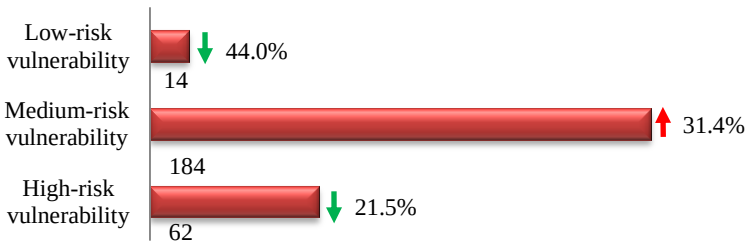
This week, the defaced government (gov.cn) websites totaled 33 (3.0%), a decrease of 5.7% from last week. Backdoors were installed into 28 (3.0%) government (gov.cn) websites, which decrease by 33.3% from last week. The fake domains and IP addresses targeting websites in mainland China reached 540 and 282 respectively, with each IP address loading about 5 phishing web pages on average.



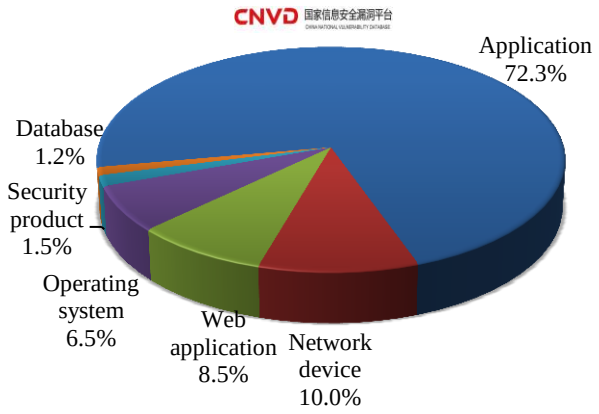


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 260 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (May 7-May 13)



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

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

The URL of CNVD for Publishng Weekly Vulnerability Report

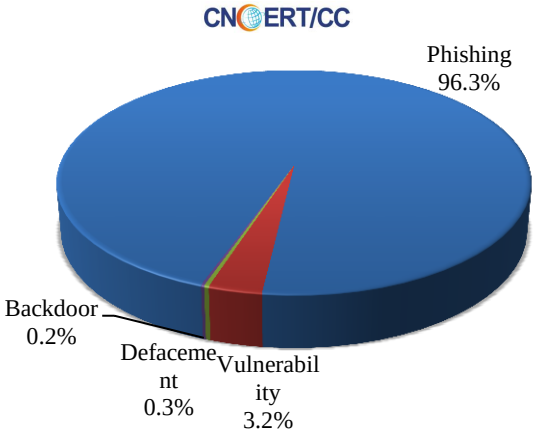
http://www.cnvd.org.cn/webinfo/list?type=4

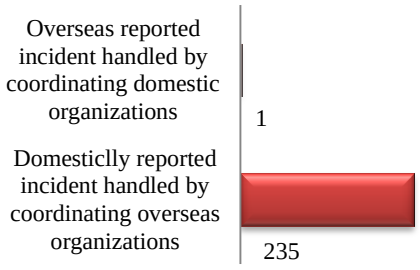
China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

Incident Handling

This week, CNCERT has handled 1,031 network security incidents, 236 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

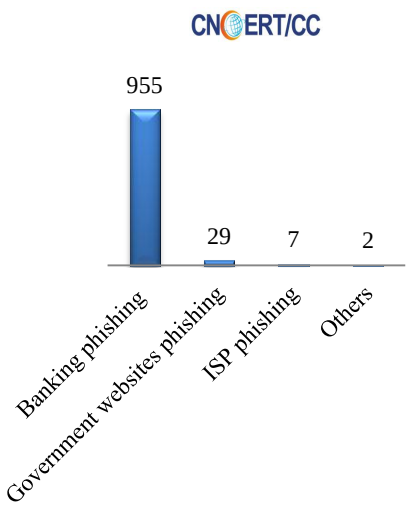
Types of the Incidents Handled by CNCERT (May 7-May 13)



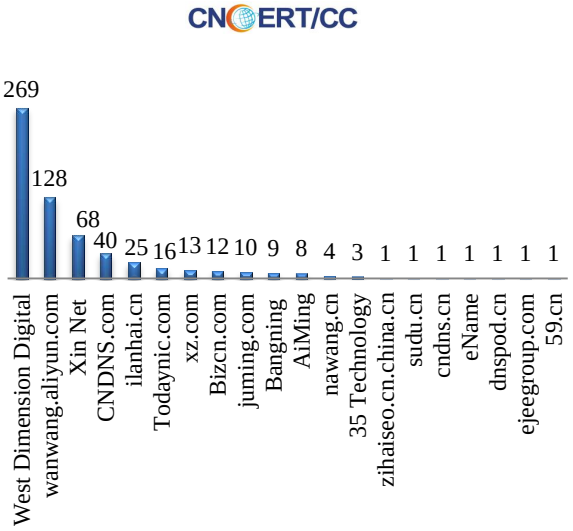


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 993 phishing incidents. Based on industries that these phishing targets belong to, there were 955 banking phishing incidents and 29 government websites phishing incidents.

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (May 7-May 13)

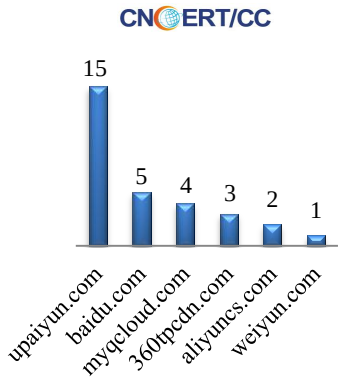


CNCERT Coordinated Domestic to Handle Phishing Incidents (May 7-May 13)



This week, CNCERT has coordinated 6 mobile phone application store and malware-injected domains to handle 30 malicious URL of the mobile malware.

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (May 7-May 13)



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: LI Ting

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158