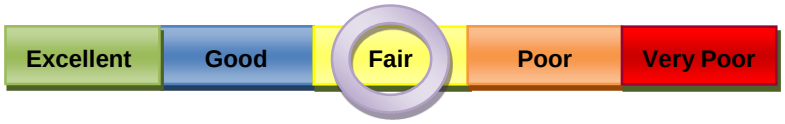
CNCERT/CC

Issue 17 2020

Apr 20-Apr 26

Weekly Report of CNCERT

Key Findings

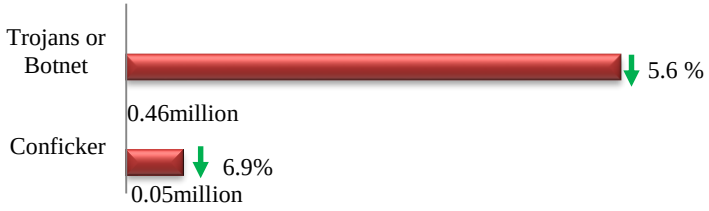


Infected Computers in Mainland China	• 0.51Million	↓ 17.1%
Defaced Websites in Mainland China	• 4,265	↓ 44.7%
Defaced gov.cn	• 23	↓ 20.7%
Backdoored Websites in Mainland China	• 1,138	↓ 22.4%
Backdoored gov.cn	• 1	↓ 88.9%
Phishing Webpages Targeting Websites in Mainland China	• 227	↑ 15.2%
New Vulnerabilities Collected by CNVD	• 533	↑ 27.2%
High-risk Vulnerabilities	• 253	↑ 24.0%

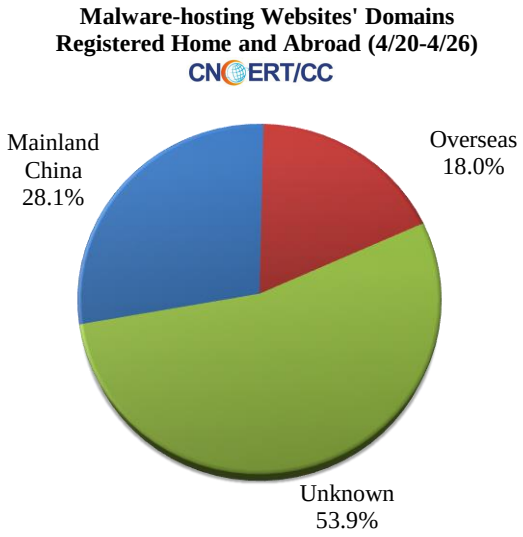
= *marks the same number as last week;* ↑ *marks an increase from last week;* ↓ *marks a decrease from last week*

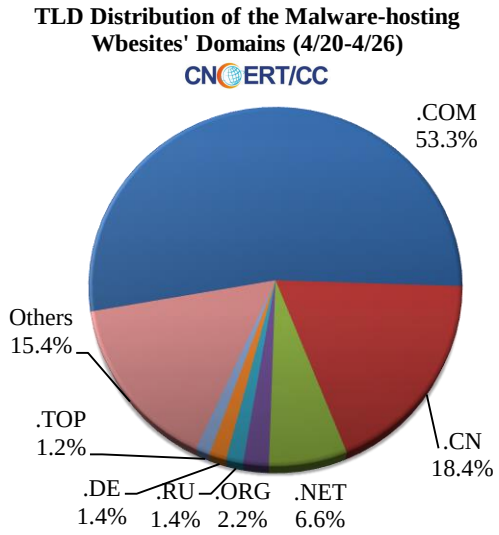
Malware Activities

The infected computers in mainland China amounted to about 0.51 million, among which about 0.46 million were controlled by Trojans or Botnets and about 0.05 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 835 domains and 3,931 IP addresses. Among the 835 malicious domains, 18.0% of them were registered abroad, 57.4% of their TLDs fell into the category of .com. Among the 3,931 IP addresses, 57.4% were registered abroad. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain name, and only 272 were accessed directly via IPs.





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).

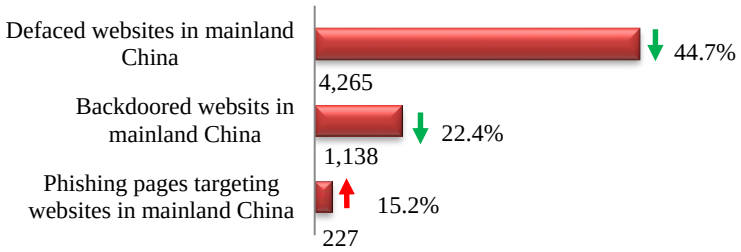
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

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

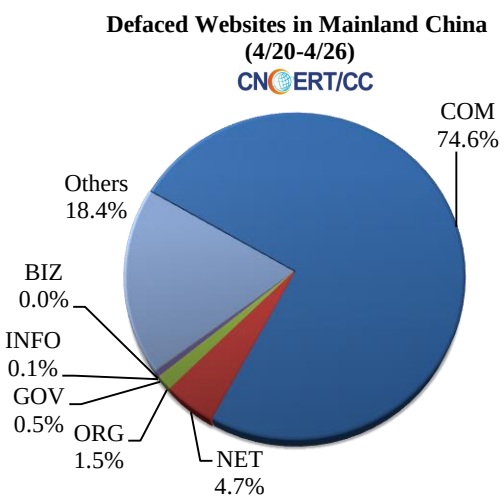
Anti Network-Virus Alliance of China (ANVA) is an industry alliance that was initiated by Network and Information security Committee under Internet Society of China (ISC) and has been operated by CNCERT.

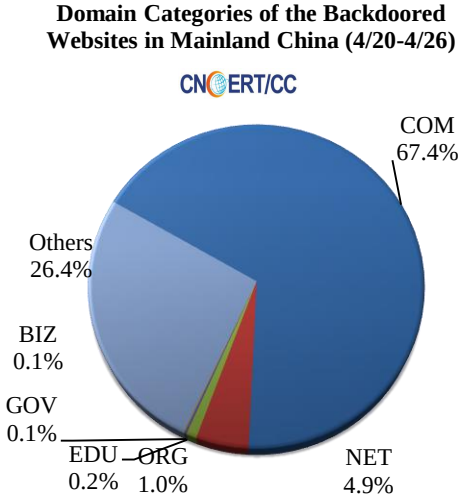
Website Security

This week, CNCERT monitored 4,265 defaced websites in mainland China and 1,138 websites planted with backdoors and 227 phishing web pages targeting websites in mainland China.



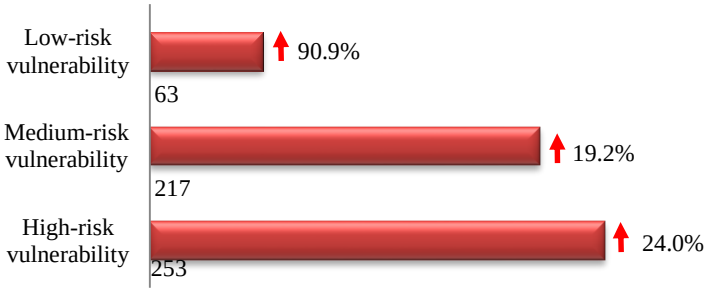
This week, the backdoors were installed into 23(0.5%) government (gov.cn) websites, a decrease of 20.7% from last week. The backdoors were installed into 1(0.1%) government (gov.cn) websites, a decrease of 88.9% from last week.



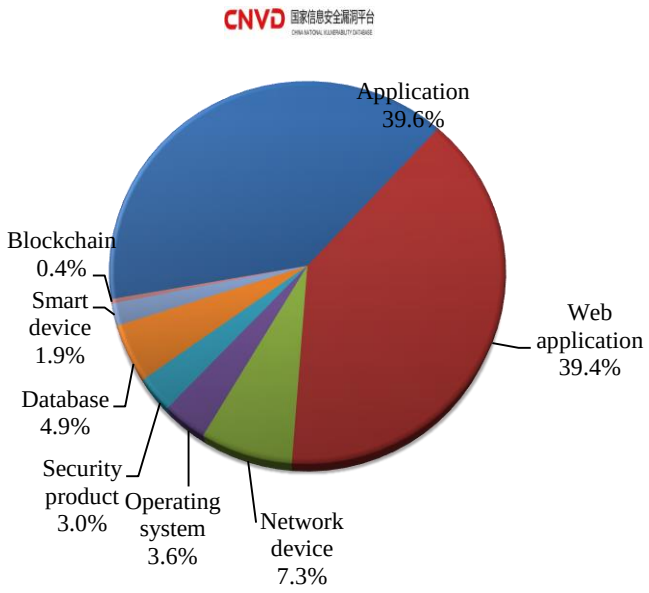


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 533 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (4/20-4/26)



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

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

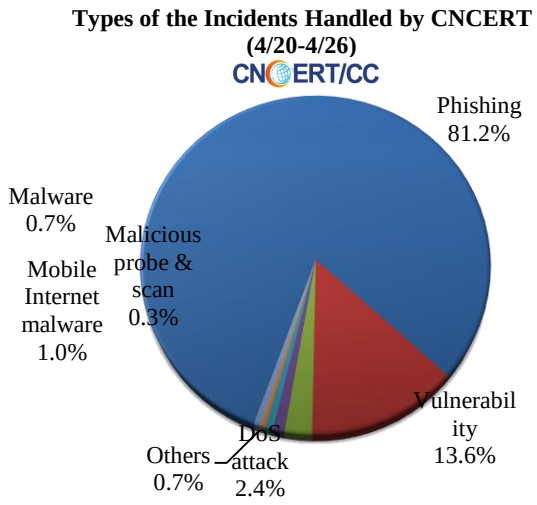
The URL of CNVD for Publishng Weekly Vulnerability Report

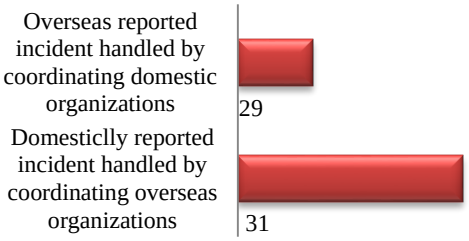
http://www.cnvd.org.cn/webinfo/list?type=4

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.

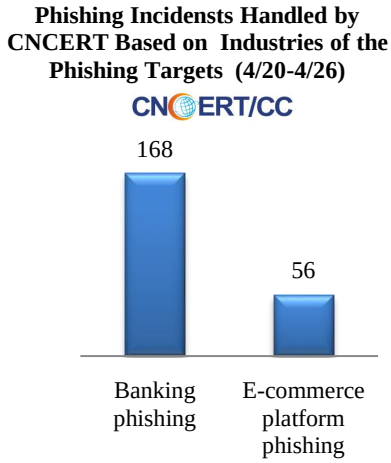
Incident Handling

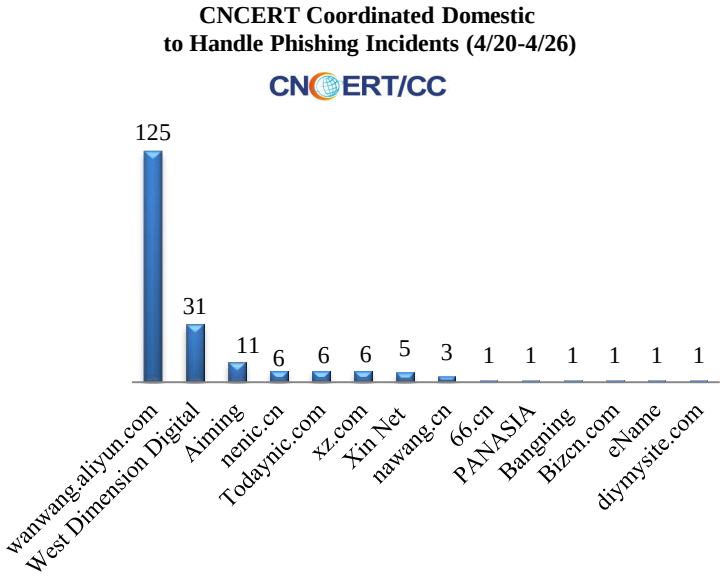
This week, CNCERT has handled 287 network security incidents, 60 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.



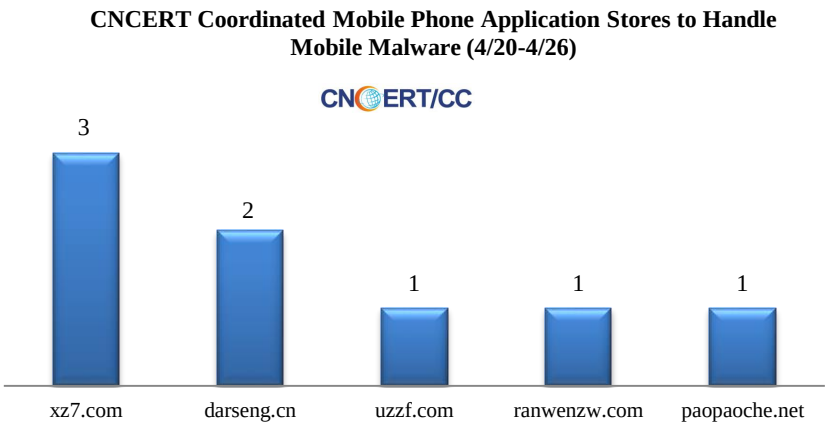


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 231 phishing incidents. Based on industries that these phishing targets belong to, there were mainly 168 banking phishing incidents and 56 e-commerce platform incidents.





This week, CNCERT has coordinated 5 mobile phone application store and malware-injected domains to handle 8 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 2019, CNCERT has established “CNCERT International Partners” relationships with 260 organizations from 78 countries or regions.

Contact us

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

Duty Editor:Zhou Yu

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315