CNCERT/CC

Issue 16 2022

Apr 11- Apr 17

Weekly Report of CNCERT

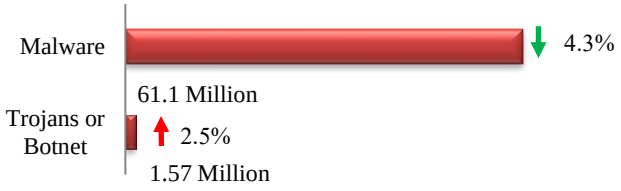
Key Findings

Malware Downloads in Chinese Mainland	• 61.1 Million	↓ 4.3%
Infected Computers Controlled by Trojans or Botnets in Chinese Mainland	• 1.57 Million	↑ 2.5%
Defaced Websites in Chinese Mainland	• 656	↓ 70.5%
Defaced gov.cn	• 0	
Backdoored Websites in Chinese Mainland	• 627	↓ 8.6%
Backdoored gov.cn	• 3	↓ 82.4%
Phishing Webpages Targeting Websites in Chinese Mainland	• 268	↑ 176.3%
New Vulnerabilities Collected by CNVD	• 311	↑ 94.4%
High-risk Vulnerabilities	• 108	↑ 62.2%

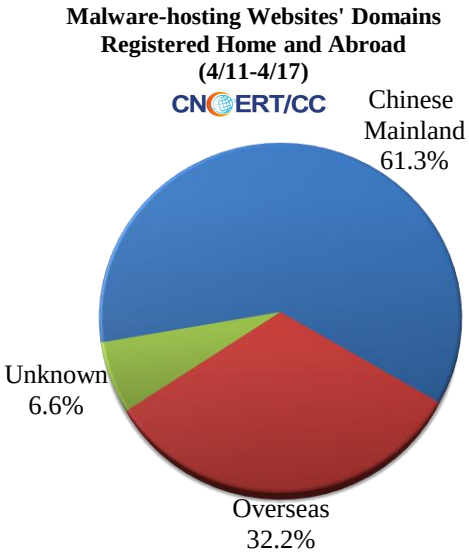
= *marks the same number as last week;* ↑ *marks an increase from last week;* ↓ *marks a decrease from last week*

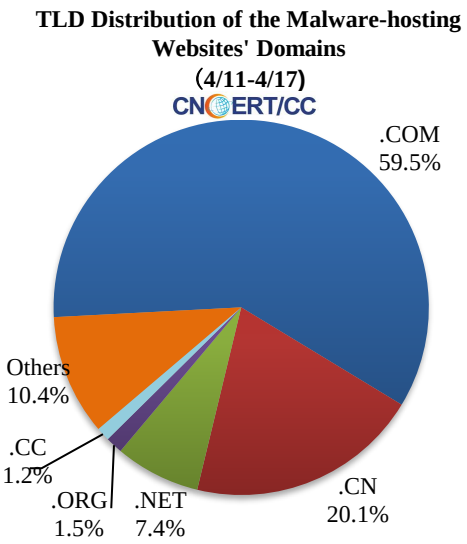
Malware Activities

The malware downloads and infected computers controlled by Trojans or Botnets in Chinese Mainland amounted to about 61.1 million and 1.57 million.



The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 1,020 domains and 4,177 IP addresses. Among the 1,020 malicious domains, 32.2% of them were registered abroad, 59.5% of their TLDs fell into the category of .com. Among the 3,211 IP addresses, 61.1% were registered abroad. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain, and 243 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).

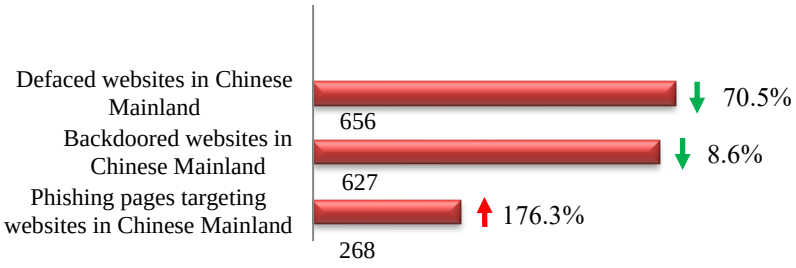
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

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

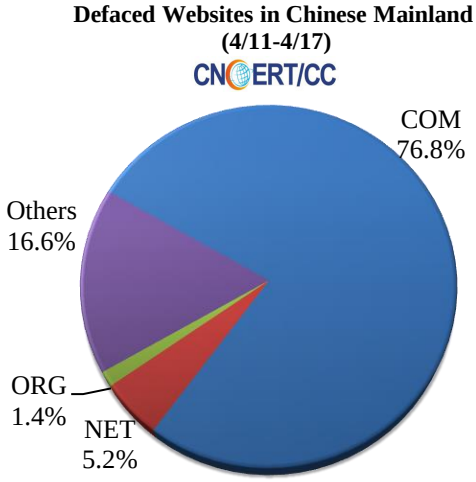
Anti-Network-Virus Alliance of China (ANVA) is an industry alliance that was initiated by Network and Information security Committee under Internet Society of China (ISC) and has been operated by CNCERT.

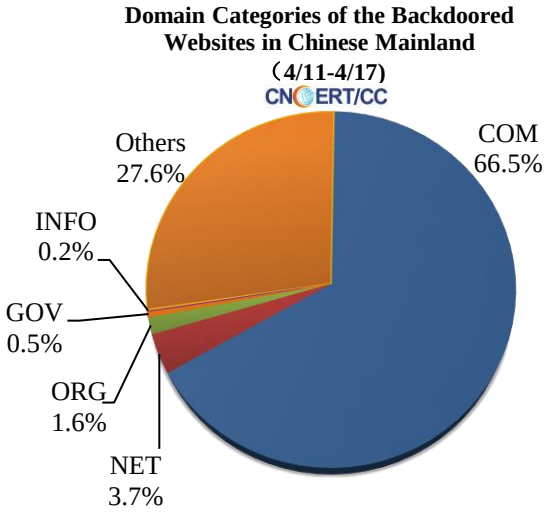
Website Security

This week, CNCERT monitored 656 defaced websites in Chinese Mainland and 627 websites planted with backdoors and 268 phishing web pages targeting websites in Chinese Mainland.



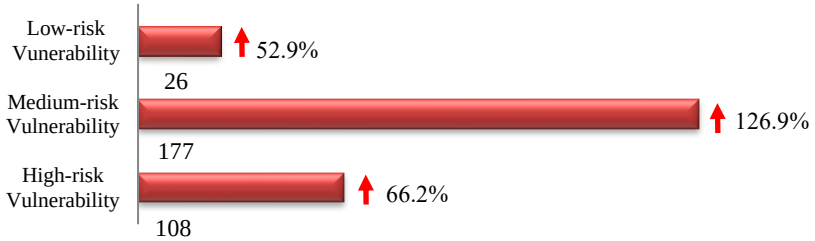
This week, the defaced government (gov.cn) website totaled 0. The backdoors were installed into 3 government (gov.cn) websites (0.5% of domestic websites), a decrease of 82.4% from last week.



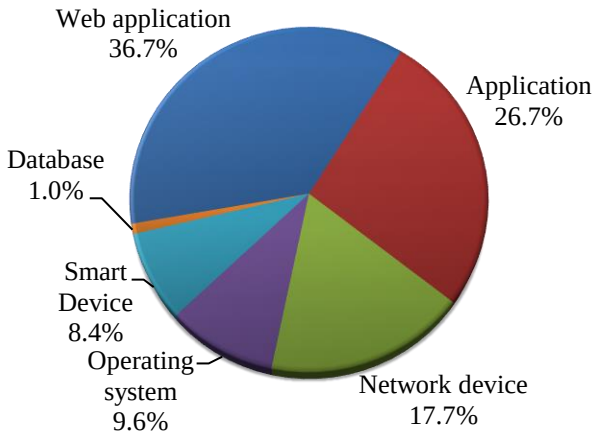


Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 311 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.



Objectives Affected by the Vulnerabilities Collected by CNVD (4/11-4/17)



The Web Application was most frequently affected by these vulnerabilities collected by CNVD, followed by 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

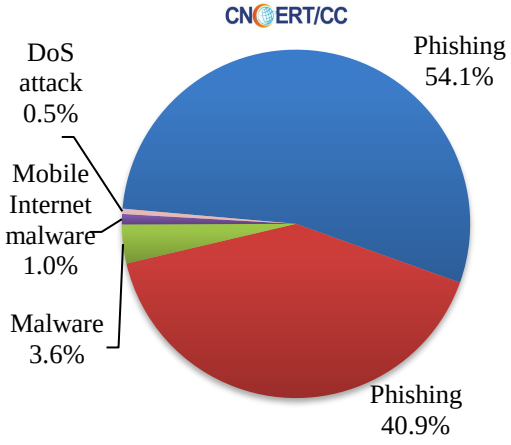
http://www.cnvd.org.cn/webinfo/list?type=4

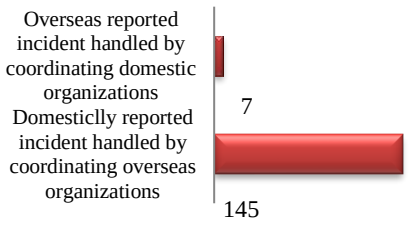
China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

Incident Handling

This week, CNCERT has handled 416 network security incidents, 152 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

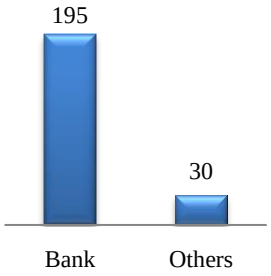
Types of Incidents Handled By Cncert (4/11-4/17）



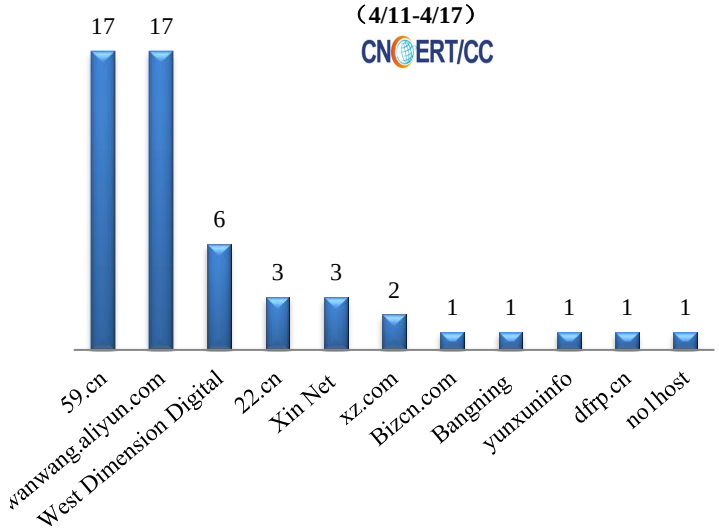


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs, and the other organizations to handle 225 phishing incidents. Based on industries that these phishing targets belong to, there were 195 banking phishing incidents and 30 other incidents.

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (4/11-4/17)

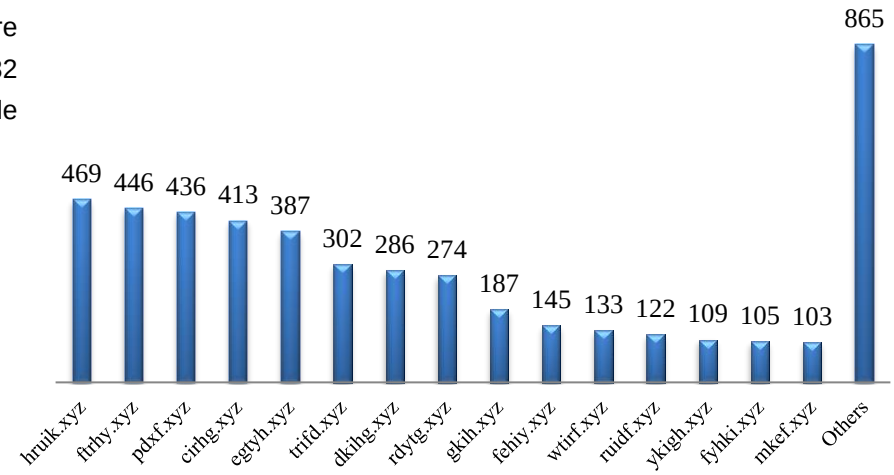


CNCERT Coordinated Domestic Domain Registrars to Handle Phishing Incidents (4/11-4/17)



This week, CNCERT has coordinated 102 platforms which provided malware download to handle 4782 malicious URLs of the mobile malware.

CNCERT Coordinated Platforms to Handle Mobile Malware (4/11-4/17)



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 Chinese Mainland.

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 2021, CNCERT has established "CNCERT International Partners" relationships with 274 organizations from 81 countries or regions.

Contact us

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

Duty Editor: Zhu Tian

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990315