CNCERT/CC

Issue 16 2019

Apr 15-Apr 21

Weekly Report of CNCERT

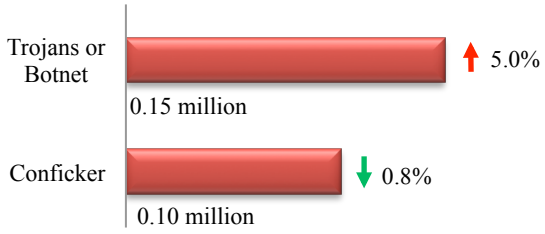
Key Findings

Infected Computers in Mainland China	• 0.25 Million	↑ 2.6%
Defaced Websites in Mainland China Defaced gov.cn	• 1054 • 8	↑ 105.9% =
Backdoored Websites in Mainland China Backdoored gov.cn	• 1321 • 35	↑ 25.0% ↓ 600.0%
Phishing Webpages Targeting Websites in Mainland China	• 2,641	↓ 6.8%
New Vulnerabilities Collected by CNVD High-risk Vulnerabilities	• 230 • 94	↑ 70.4% ↑ 104.3%

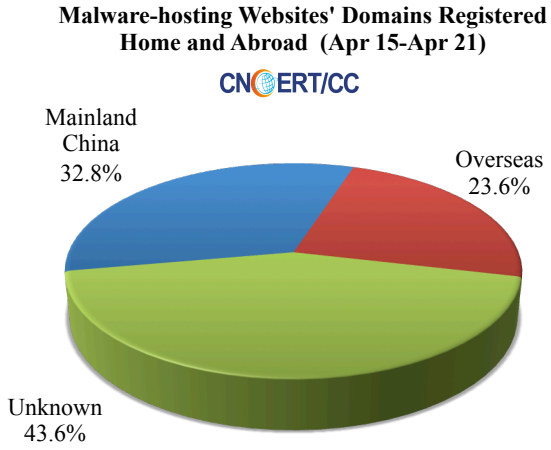
= *marks the same number as last week;* ↑ *marks an increase from last week;* ↓ *marks a decrease from last week*

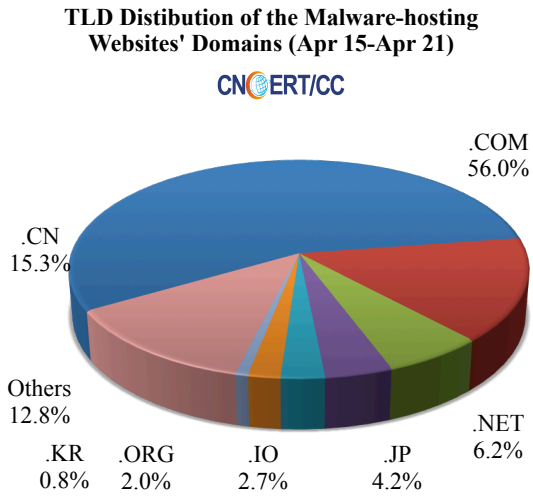
Malware Activities

The infected computers in mainland China amounted to about 0.25 million, among which about 0.15 million were controlled by Trojans or Botnets and about 0.10 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 3,885 domains and 3,672 IP addresses. Among the 3,885 malicious domains, 23.6% were registered overseas and 56.0% of their TLDs fell into the category of.com. Among the 3,672 malicious IPs, 40.2% were overseas. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain names, and only 405 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).

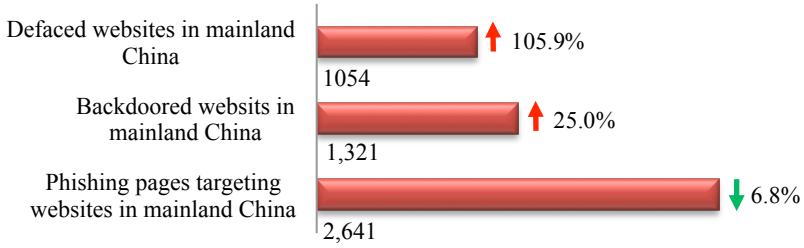
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

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

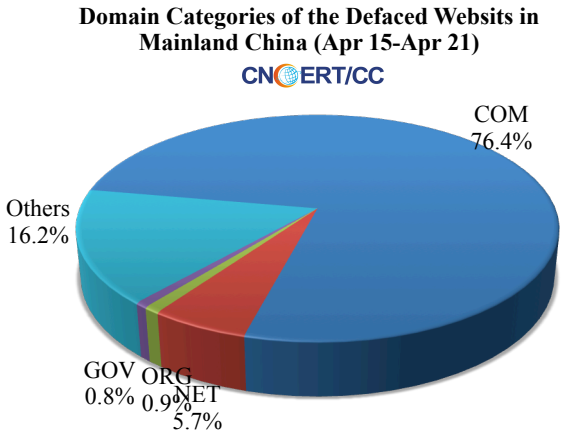
Anti Network-Virus Alliance of China (ANVA) is an industry alliance that was initiated by Network and Information security Committee under Internet Society of China (ISC) and has been operated by CNCERT.

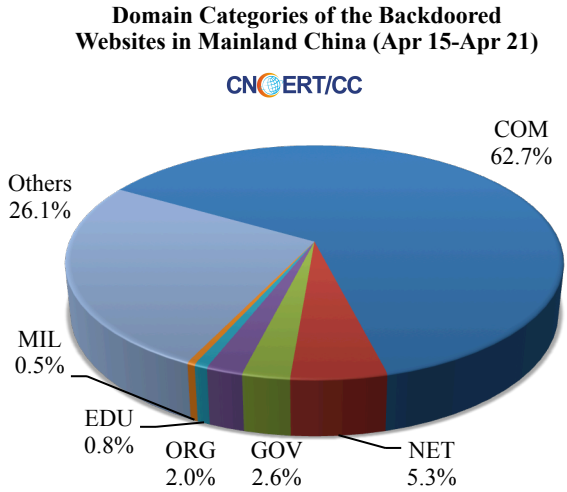
Website Security

This week, CNCERT monitored 1,054 defaced websites, 1,321websites planted with backdoors and 2,641 phishing web pages targeting websites in mainland China.



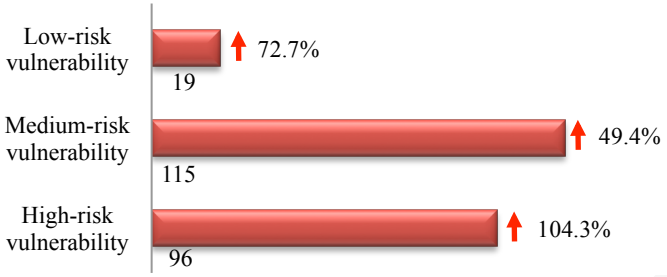
This week, the defaced government (gov.cn) websites totaled 8 (0.8%). Backdoors were installed into 35 (2.6%) government (gov.cn) websites, an increase of 600.0% from last week. The fake domains and IP addresses targeting websites in mainland China reached 803 and 434 respectively, with each IP address loading about 6 phishing web pages on average.

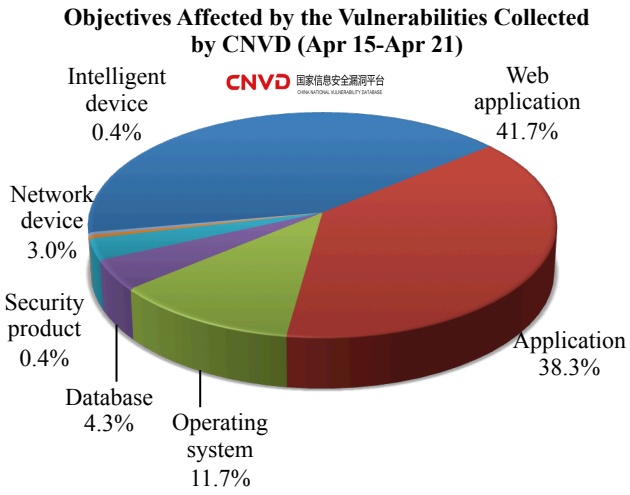




Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 230 new vulnerabilities. This week's overall vulnerability severity was evaluated as medium.





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

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

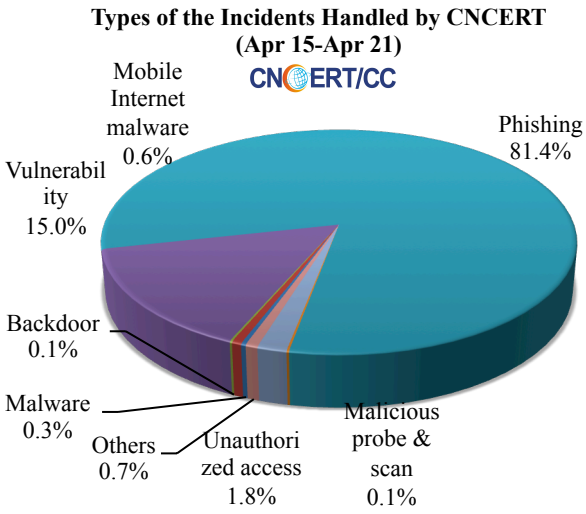
The URL of CNVD for Publishng Weekly Vulnerability Report

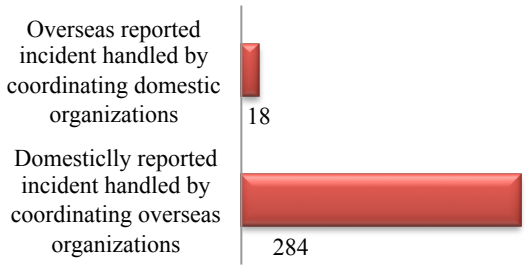
http://www.cnvd.org.cn/webinfo/list?type=4

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

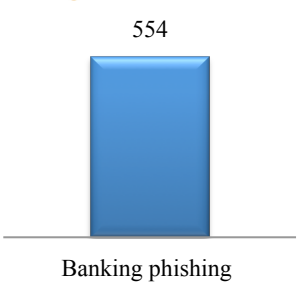
This week, CNCERT has handled 681 network security incidents, 302 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.



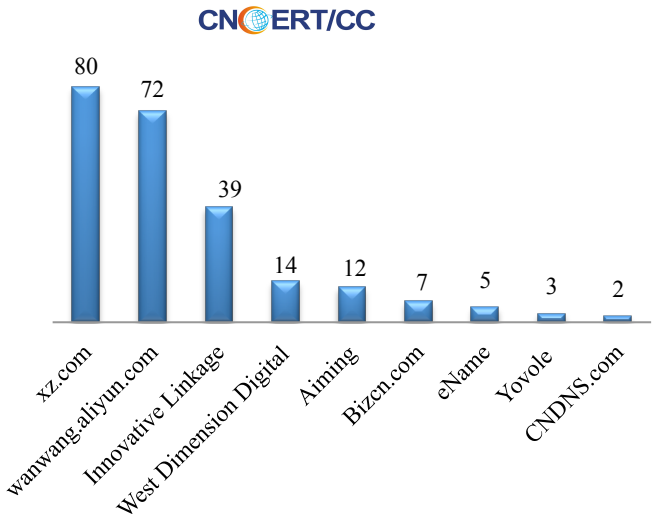


Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 554 phishing incidents. Based on industries that these phishing targets belong to, there were 554 banking phishing incidents.

Phishing Incidensts Handled by CNCERT Based on Industries of the Phishing Targets (Apr 15-Apr 21)

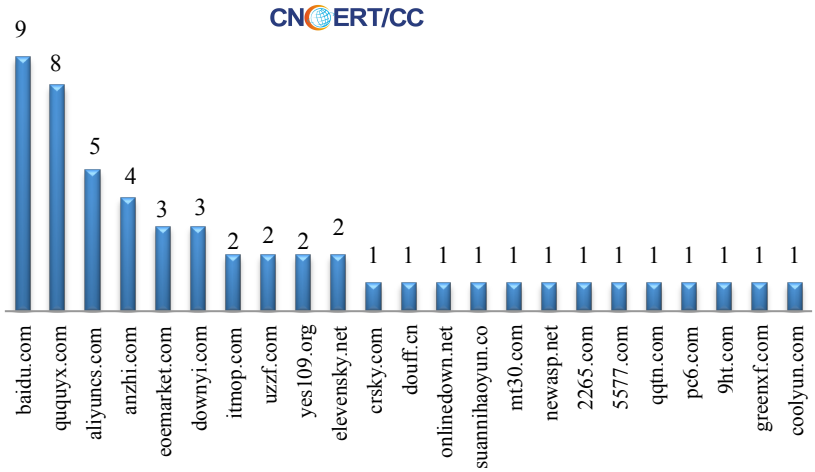


CNCERT Coordinated Domestic to Handle Phishing Incidents (Apr 15-Apr 21)



This week, CNCERT has coordinated 23 mobile phone application store and malware-injected domains to handle 53 malicious URL of the mobile malware.

CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Apr 15-Apr 21)



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: Wang Shiwen

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158