CNCERT/CC

Weekly Report of CNCERT

Issue 38 2017

Sep 11-Sep 17

Key Findings

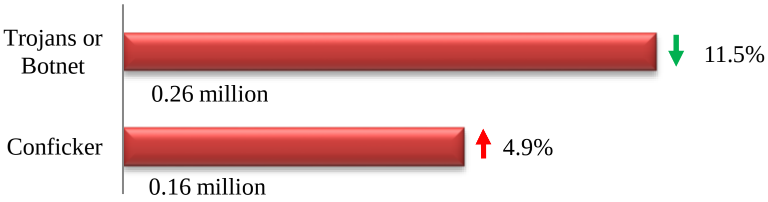
Excellent [✓ Good] Fair Poor Very Poor

Infected Computers in Mainland China	• 0.42 Million	↓ 5.7%
Defaced Websites in Mainland China Defaced gov.cn	• 2,066 • 53	↓ 17.8% ↓ 3.6%
Backdoored Websites in Mainland China Backdoored gov.cn	• 917 • 54	↑ 20.2% ↑ 63.6%
Phishing Webpages Targeting Websites in Mainland China	• 297	↓ 21.4%
New Vulnerabilities Collected by CNVD High-risk Vulnerabilities	• 450 • 178	↑ 34.3% ↑ 89.4%

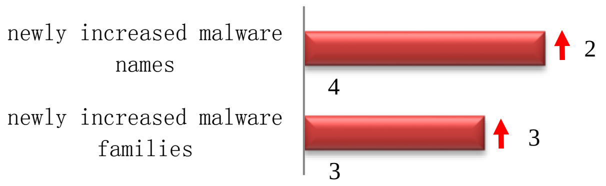
= *marks the same number as last week;* ↑ *marks an increase from last week;* ↓ *marks a decrease from last week*

Malware Activities

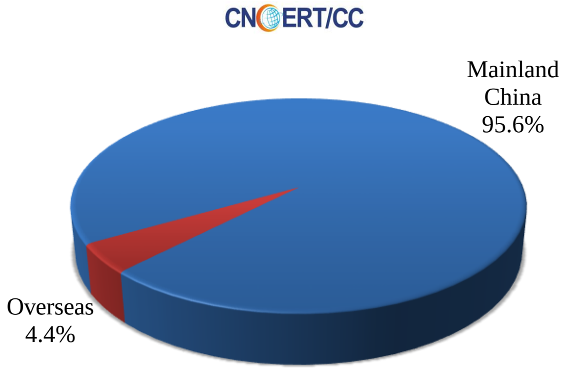
The infected computers in mainland China amounted to about 0.42 million, among which about 0.26 million were controlled by Trojans or Botnets and about 0.16 million by Confickers.

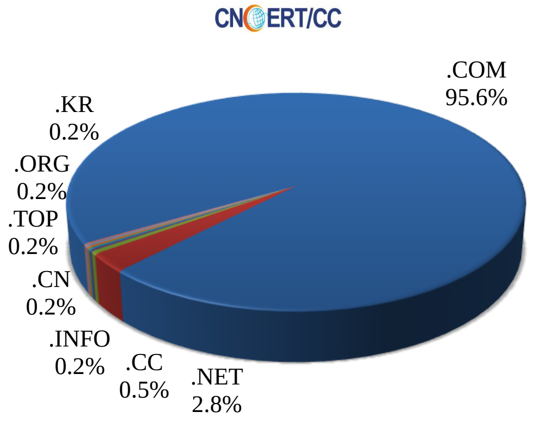


CNCERT captured a certain number of new malware samples this week. 4 new malware names were identified, and 3 new malware families were identified.



The malware-hosting websites is the jumping-off place for malware propagation. The malware-hosting websites monitored by CNCERT this week involved 435 domains and 410 IP addresses. Among the 435 malicious domains, 4.4% were registered overseas and 95.6% of their TLDs fell into the category of.com. Among the 410 malicious IPs, 2.4% were overseas. Based on our analysis of the malware-hosting website's URLs, the majority of them were accessed via domain names, and only 4 were accessed directly via IPs.


Malware-hosting Websites' Domains Registered Home and Abroad (Sep 11-Sep 17)


TLD Distibution of the Malware-hosting Websites' Domains (Sep 11-Sep 17)

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).

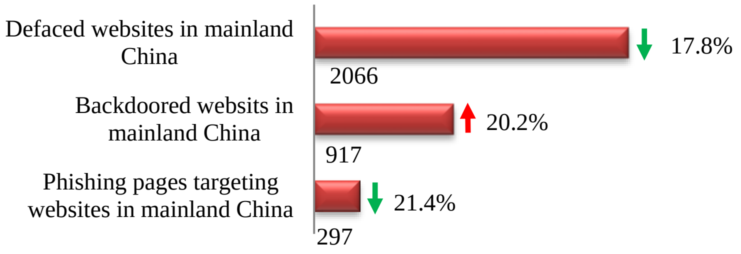
The URL of ANVA for Publishing the Blacklist of Malicious Domains and IPs.

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.

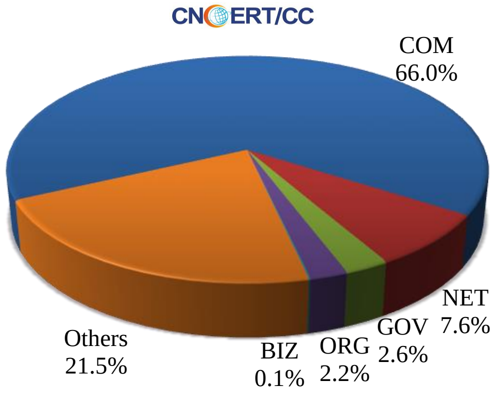
Website Security

This week, CNCERT monitored 2,066 defaced websites, 917 websites planted with backdoors and 297 phishing web pages targeting websites in mainland China.

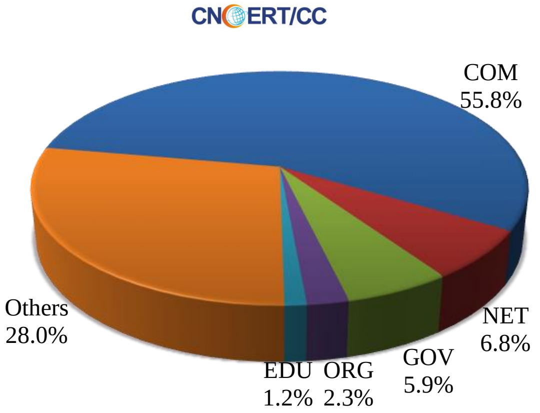


This week, the defaced government (gov.cn) websites totaled 53 (2.6%), a decrease of 3.6% from last week. Backdoors were installed into 54 (5.9%) government (gov.cn) websites, which increase by 63.6% from last week. The fake domains and IP addresses targeting websites in mainland China reached 257 and 122 respectively, with each IP address loading about 2 phishing web pages on average.

Domain Categories of the Defaced Websits in Mainland China (Sep 11-Sep 17)

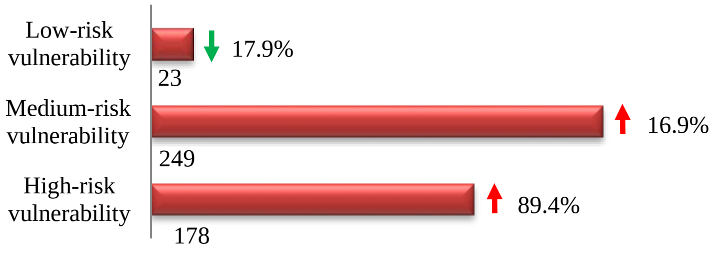


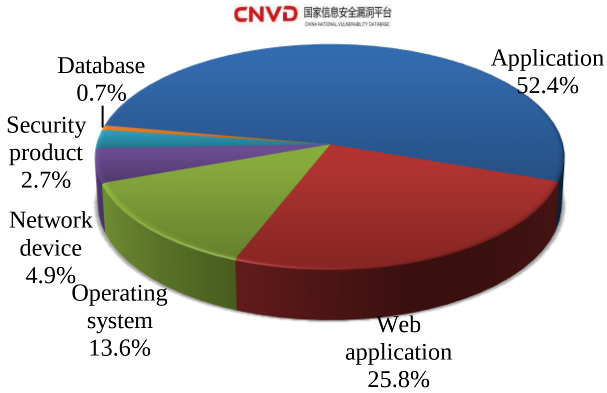
Domain Categories of the Backdoored Websites in Mainland China (Sep 11-Sep 17)



Vulnerabilities

This week, China National Vulnerability Database (CNVD) recorded 450 new vulnerabilities. This week's overall vulnerability severity was evaluated as high.




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

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.

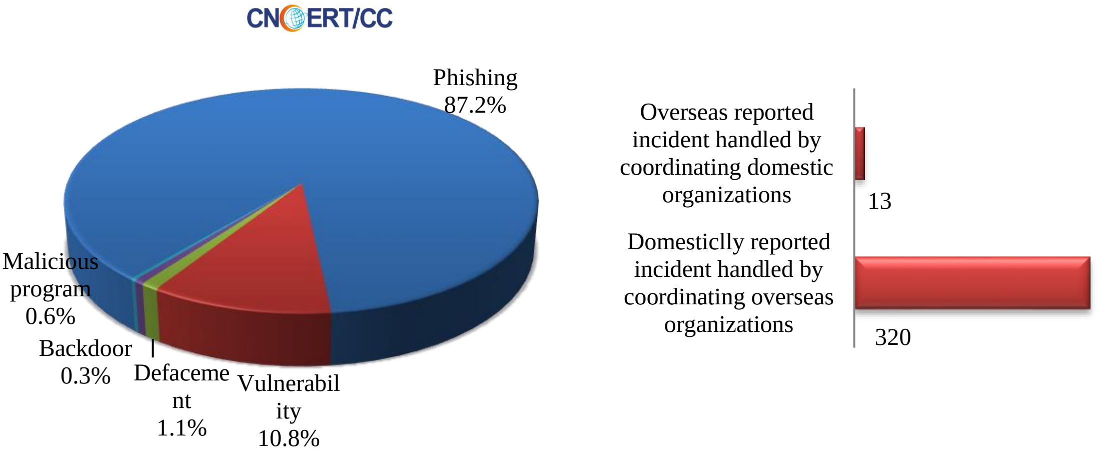
The URL of CNVD for Publishng Weekly Vulnerability Report

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

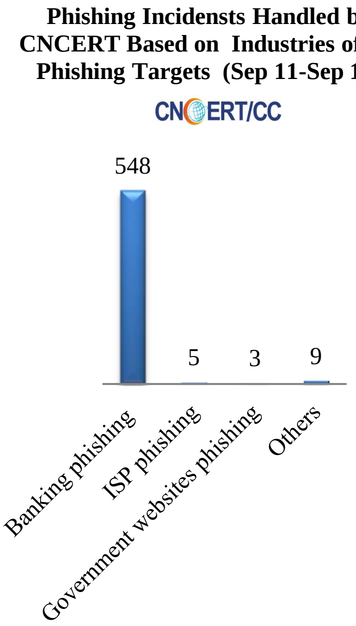
China National Vulnerability Database (CNVD) was established by CNCERT, together with control systems, ISPs, ICPs, network security vendor, software producers and internet enterprises for sharing information on vulnerabilities.

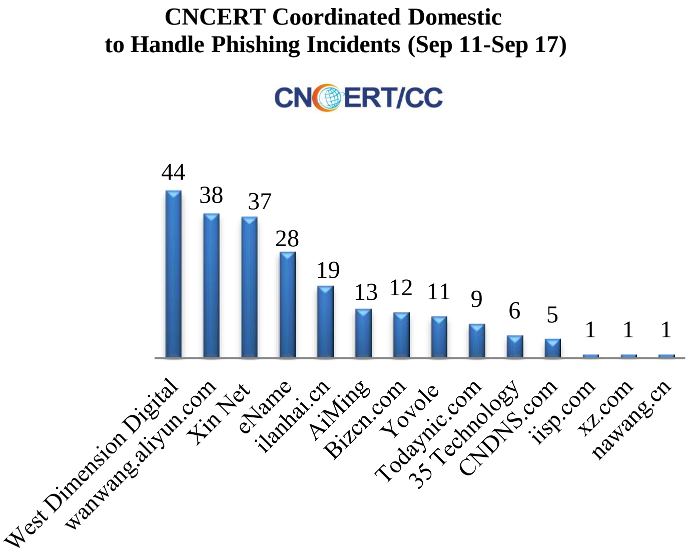
Incident Handling

This week, CNCERT has handled 648 network security incidents, 333 of which were cross-border ones, by coordinating ISPs, domain registrars, mobile phone application stores, branches of CNCERT and our international partners.

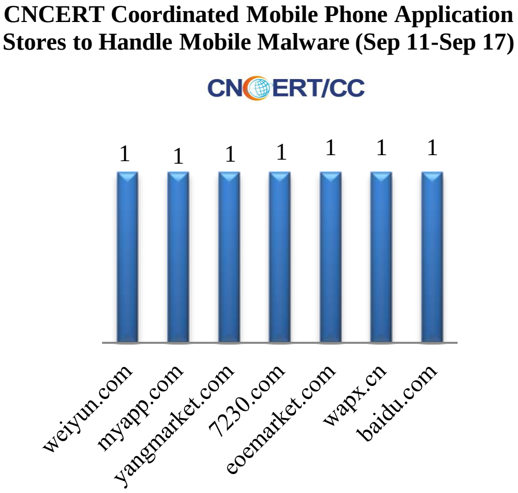

Types of the Incidents Handled by CNCERT (Sep 11-Sep 17)

Specifically, CNCERT has coordinated domestic and overseas domain registrars, international CERTs and the other organizations to handle 565 phishing incidents. Based on industries that these phishing targets belong to, there were 548 banking phishing incidents and 5 ISP phishing incidents.


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


CNCERT Coordinated Domestic to Handle Phishing Incidents (Sep 11-Sep 17)

This week, CNCERT has coordinated 7 mobile phone application stores and malware-injected domains to handle 7 malicious URL of the mobile malware.


CNCERT Coordinated Mobile Phone Application Stores to Handle Mobile Malware (Sep 11-Sep 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 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 2016, CNCERT has established “CNCERT International Partners” relationships with 185 organizations from 69 countries or regions.

Contact us

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

Duty Editor: MA Liya

Website: www.cert.org.cn

Email: cncert_report@cert.org.cn

Tel: 010-82990158