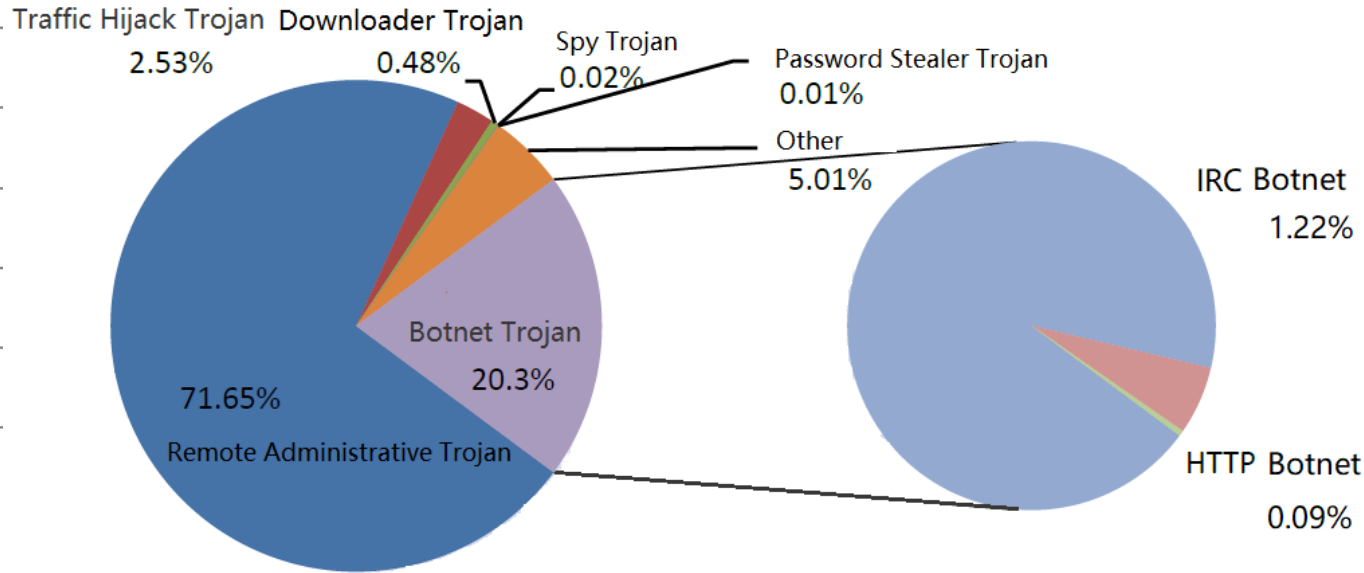
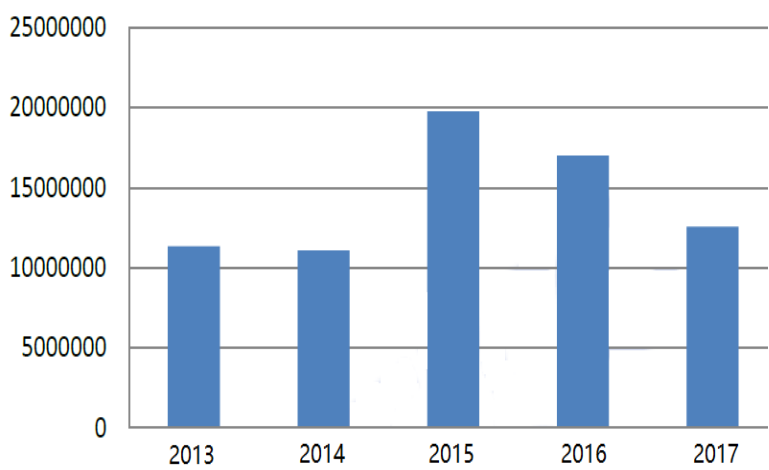


Cyber Attacks and Countermeasures

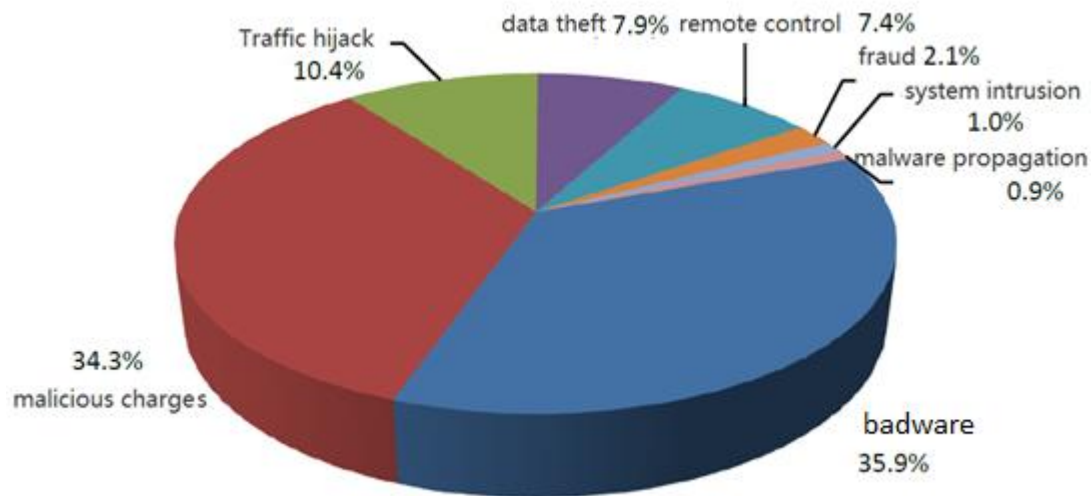
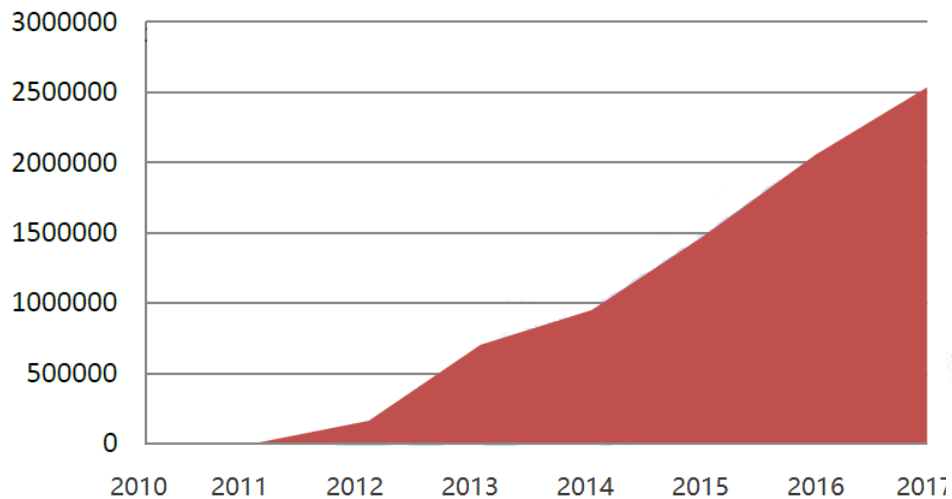
Yunwei Zhao
CNCERT/CC, CHINA
28/08/2018



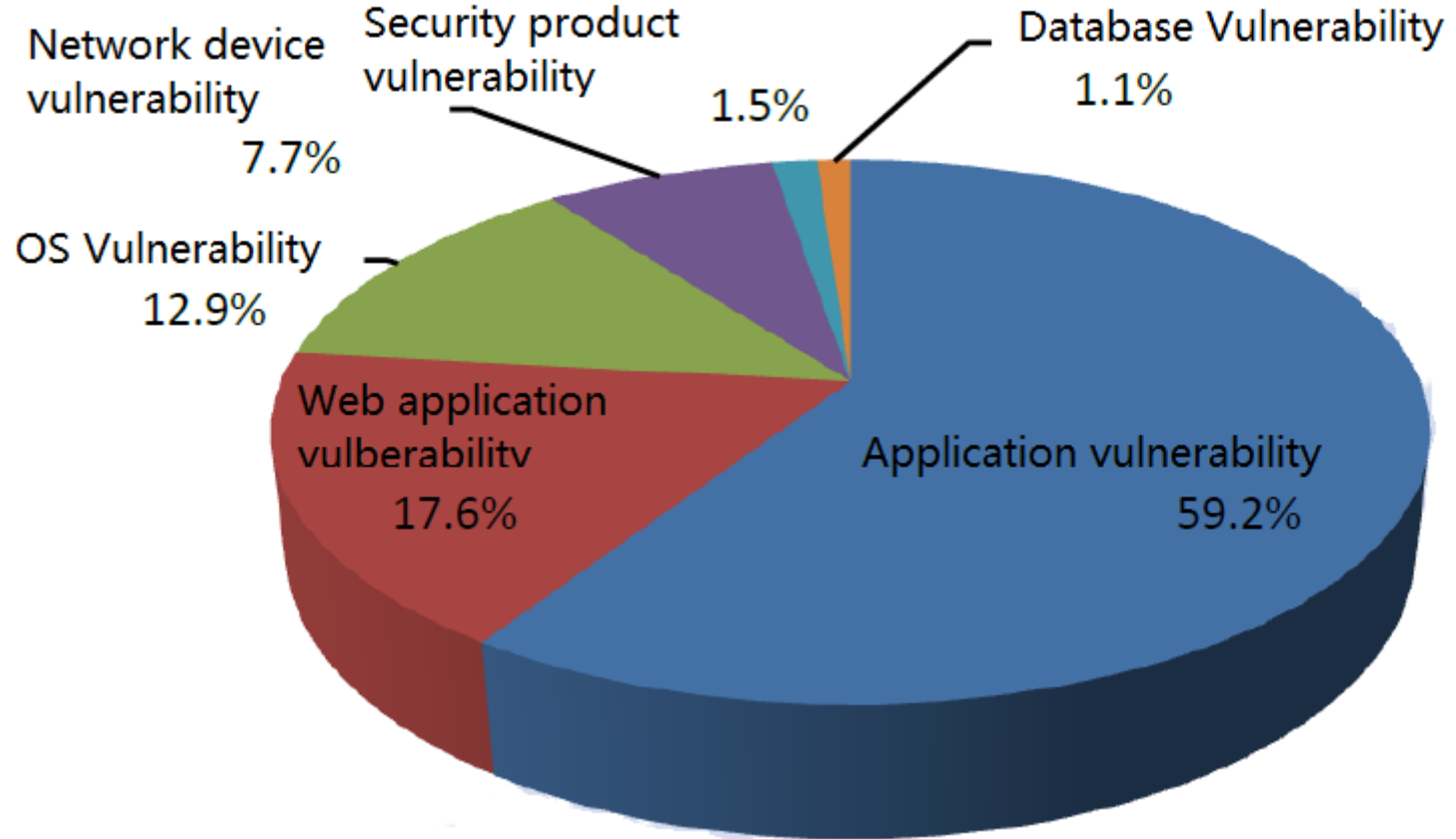
Computer Malware



Mobile Internet Malware



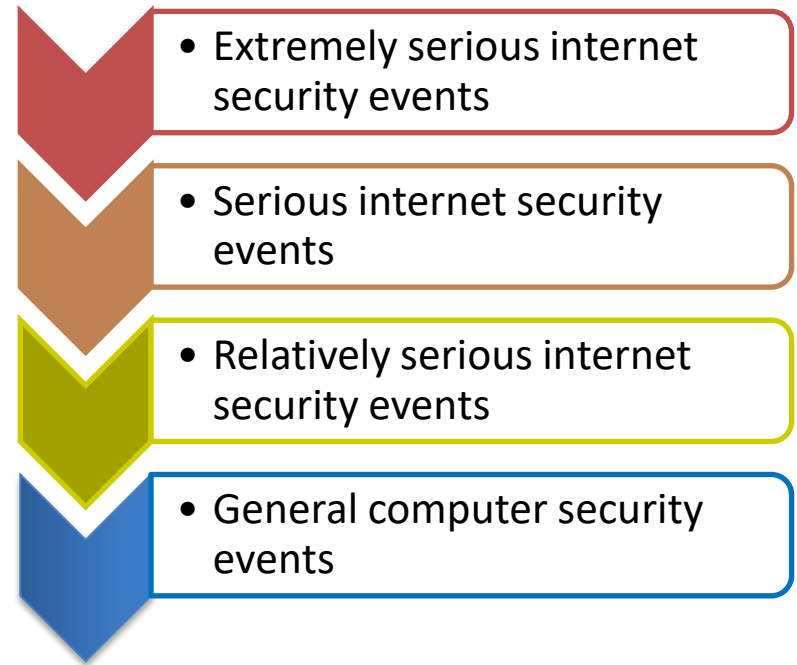
Connected Intelligent Devices Malware



Emergency Response Plan for Internet Security Incidents

- Scope:
 - pernicious procedural incidents
 - cyber attacks
 - information destruction
 - equipment failure
 - disastrous events
 - ...

- Four Scales:



Emergency Response Process

Detection

apply a variety of ways to detect the latest vulnerabilities, viruses, network attacks and other network security risks



Early Warning

Four Scales: red, orange, yellow and blue



Emergency Response

Four scales: extremely serious, serious, relatively serious and general computer security events.

Emergency Response Process of “Wannacry”

2017 5/12 20:20, WannaCry was found to be on a large scale, and the emergency response level was upgraded to “extremely serious” response scale.

2017/5/13 Publish the official announcement about Wannacry.

2017 5/14 15:00, CNCERT releases emergency response manuals and ransomware spread is under control.



2017 5/13 CNCERT coordinates domestic main network security enterprises (An Tian, 360) to analyze the samples

2017 5/13 jointly work on defense tools against WannaCry

2017/5/14 CNCERT Continue to monitor “Wannacry”, especially new attack methods and malicious samples

APCERT Data Exchanger (ADE)

APCERT DataExchanger (ADE) - an information sharing platform .

(<https://dataexchanger.apcert.org>).

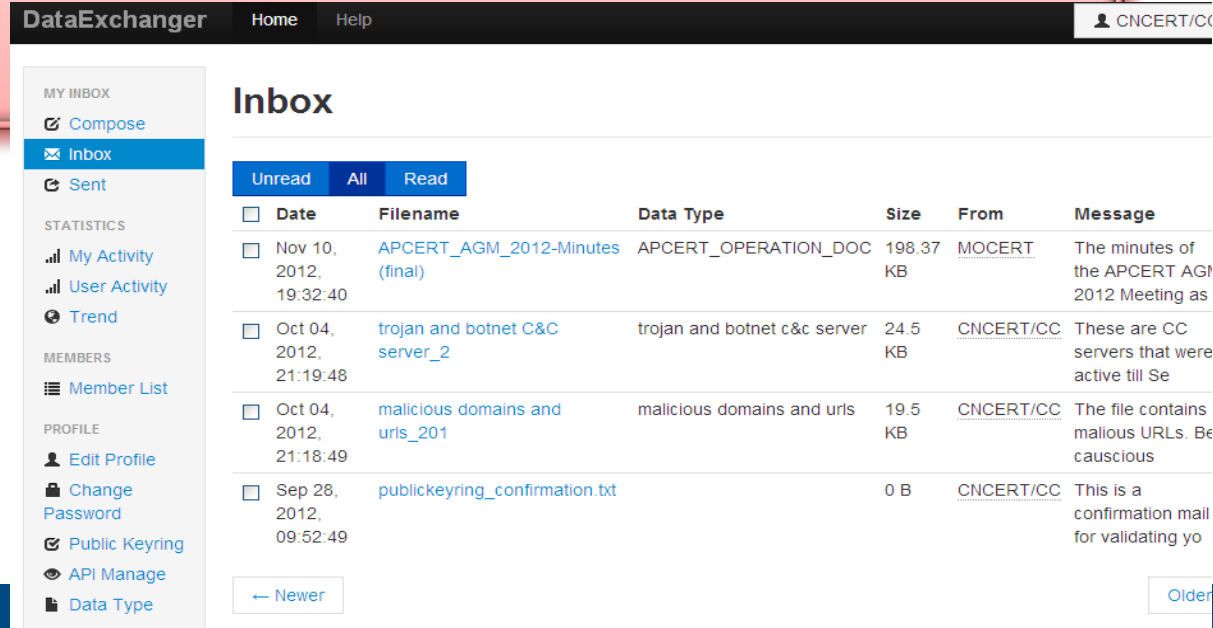
28 teams has registered. 23 teams are using it.

Share 8K+ cyber threat information in past year.

hosts infected by Conficker

hosts infected by Nitol

malicious URLs



The screenshot displays the APCERT DataExchanger (ADE) web interface. The top navigation bar includes 'DataExchanger', 'Home', 'Help', and a user profile icon for 'CNCERT/CC'. The left sidebar contains navigation options: 'MY INBOX' (Compose, Inbox, Sent), 'STATISTICS' (My Activity, User Activity, Trend), 'MEMBERS' (Member List), and 'PROFILE' (Edit Profile, Change Password, Public Keyring, API Manage, Data Type). The main content area is titled 'Inbox' and features a table of messages. The table has columns for 'Unread', 'All', 'Read', 'Date', 'Filename', 'Data Type', 'Size', 'From', and 'Message'. The messages listed are:

Unread	All	Read	Date	Filename	Data Type	Size	From	Message
<input type="checkbox"/>			Nov 10, 2012, 19:32:40	APCERT_AGM_2012-Minutes (final)	APCERT_OPERATION_DOC	198.37 KB	MOCERT	The minutes of the APCERT AGM 2012 Meeting as
<input type="checkbox"/>			Oct 04, 2012, 21:19:48	trojan and botnet C&C server_2	trojan and botnet c&c server	24.5 KB	CNCERT/CC	These are CC servers that were active till Se
<input type="checkbox"/>			Oct 04, 2012, 21:18:49	malicious domains and urls_201	malicious domains and urls	19.5 KB	CNCERT/CC	The file contains malious URLs. Be cautious
<input type="checkbox"/>			Sep 28, 2012, 09:52:49	publickeyring_confirmation.txt		0 B	CNCERT/CC	This is a confirmation mail for validating yo

Navigation buttons for '← Newer' and 'Older →' are visible at the bottom of the inbox list.













Mail List

Mail list

APCERT liaison partner (US-CERT) shared by mailing list (apcert-liaison@apcert.org)

- 100+ emails, including reports about Trojans, Botnets, Vulnerability, Phishing, Ransomware, Spam, and etc.

<input type="checkbox"/>		Publications	[APCERT Liaison] MAR-10069471 – Zeus Encrypted Configuration File (TLP:GREEN) APCERT,US-CERT has released MAR-10069471 – Zeus Encrypted Configuration File (TLP:GREEN). Copies o ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MIFR-10081661-Adware (TLP:GREEN) APCERT,US-CERT has released MIFR-10081661-Adware (TLP:GREEN). Copies of the files are provided for ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MIFR-10082283-Phishing Email (TLP:GREEN) APCERT,US-CERT has released MIFR-10082283-Phishing Email (TLP:GREEN). Copies of the files are provi ...
<input type="checkbox"/>		PublicationsPubli...	[APCERT Liaison] MIFR-10083391 – Zepto Ransomware (TLP:GREEN)(2) APCERT,US-CERT has released MIFR-10083391 – Zepto Ransomware (TLP:GREEN). Copies of the files are ...
<input type="checkbox"/>		PublicationsPubli...	[APCERT Liaison] MIFR-10087696 – Downloader (TLP:GREEN)(2) APCERT,US-CERT has released MIFR-10087696 – Downloader (TLP:GREEN). Copies of the files are provid ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MIFR-10079612 – Trojan (TLP: GREEN) APCERT,US-CERT has released MIFR-10079612 – Trojan (TLP: GREEN). Copies of the files are provided ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MAR-10049853-A DDOS Trojan (TLP:GREEN) APCERT,US-CERT has released MAR-10049853-A DDOS Trojan (TLP:GREEN). Copies of the files are provide ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MIFR-10078251 – PHP Bot (TLP:GREEN) APCERT,US-CERT has released MIFR-10078251 – PHP Bot (TLP:GREEN). Copies of the files are provided ...
<input type="checkbox"/>		Publications, tec...	[APCERT Liaison] Re: MIFR-10080392 – Phishing Email (TLP:GREEN)(2) Dear APCERT, Thank you for the feedback! We always welcome any questions or information you may hav ...
<input type="checkbox"/>		Publications	[APCERT Liaison] MAR-10060020 – Trojan Kovter (TLP: GREEN)



Wiki

MyCERT operates the APCERT wiki (<https://wiki.apcert.org>).

TWNCERT shared the video and documents of APCERT online training.



Home Main Web View Edit Hi Cn CERT

APCERT APCERT WIKI Jump Search English Edit Attach

Tags: create new tag . view all tags

APCERT Official Wiki

With the rapid development of the Internet, many Asia Pacific economies are now increasingly dependent on public network applications such as online banking, online stock trading, e-business, e-government and e-customs. The protection of the various national information infrastructures that make up this new and emerging Asia Pacific e-economy is critical to the region's political and economic stability and security. The need to protect these critical national information infrastructures is also urgent.

Attacks on information infrastructures are increasing in frequency, sophistication and scale. For example, the Code Red II Internet worm integrated characteristics of a computer virus, Trojan, Worm and Hacking activity to propagate quickly across the Internet and infect massive numbers of host computers. Code Red II was fully automated to search for hosts to infect with no respect for national or international boundaries. Subsequent worms such as Nimda also illustrate this recent and concerning trend.

This growing threat in the Asia Pacific region requires a collaborative approach with the various CERT and CSIRT organizations taking the lead role with full support from their respective governments.

To address this urgent need, Asia Pacific Incident Response Teams propose the establishment of a group called Asia Pacific CERT ([APCERT](#)). The Asia Pacific Computer Emergency Response Team ([APCERT](#)) was established in 2003 for cooperation between CERTs in Asia Pacific region. [APCERT](#) would have an

Recent changes in Main web:

- [TWiki User](#)
- [Cn CERT](#)
- [Aus CERT](#)
- [TWiki Admin Group](#)
- [Bd CERT](#)
- [APCERTHistory Document](#)
- [Shamir Mycert](#)
- [Kr CERT](#)
- [Nz NCSC](#)
- [Zahn Yunos](#)
- [Rahayu 2 Mycert](#)
- [APCERTPOCList](#)
- [Jp CERT](#)
- [Web Statistics](#)
- [Site Statistics](#)
- [Id Sirtii](#)
- [more.....](#)

ADE Users

28 teams registered and login the platform

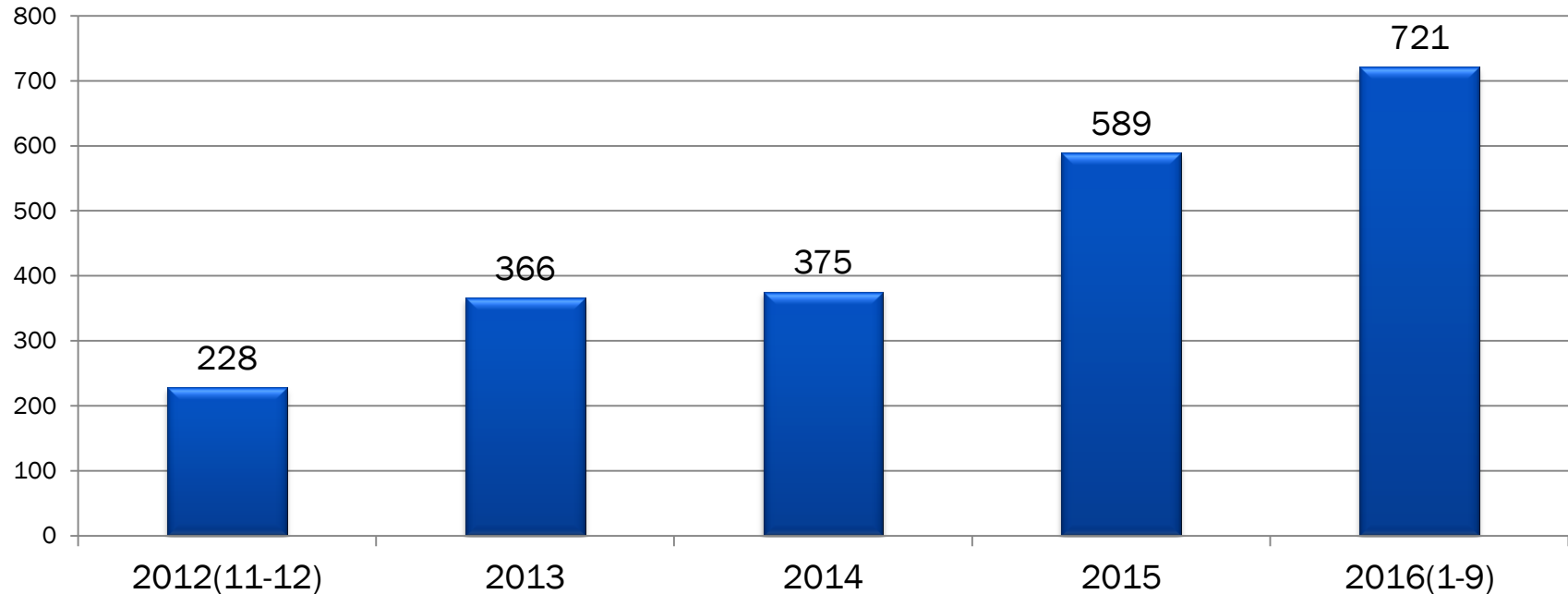
23 teams uploaded their PGP Key and used the platform

AusCERT	BDCERT	BruCERT	CCERT	CERT Australia	CERT-In
CNCERT	EC-CERT	GovCERT.HK	HKCERT	ID-CERT	ID-SIRTII/CC
JPCERT/CC	KrCERT/CC	LaoCERT	mmCERT	MNCERT/CC	MOCERT
MonCERT	MyCERT	NCSC	SingCERT	Sri Lanka CERT CC	TechCERT
ThaiCERT	TWCERT	TWNCERT	VNCERT		

Information Exchange(cont.)

22K+ information shared from Nov 2012 to Sep 2016, including botnets, malicious URLs and vulnerabilities.

The statistic of information sharing on per month by ADE



Information Exchange

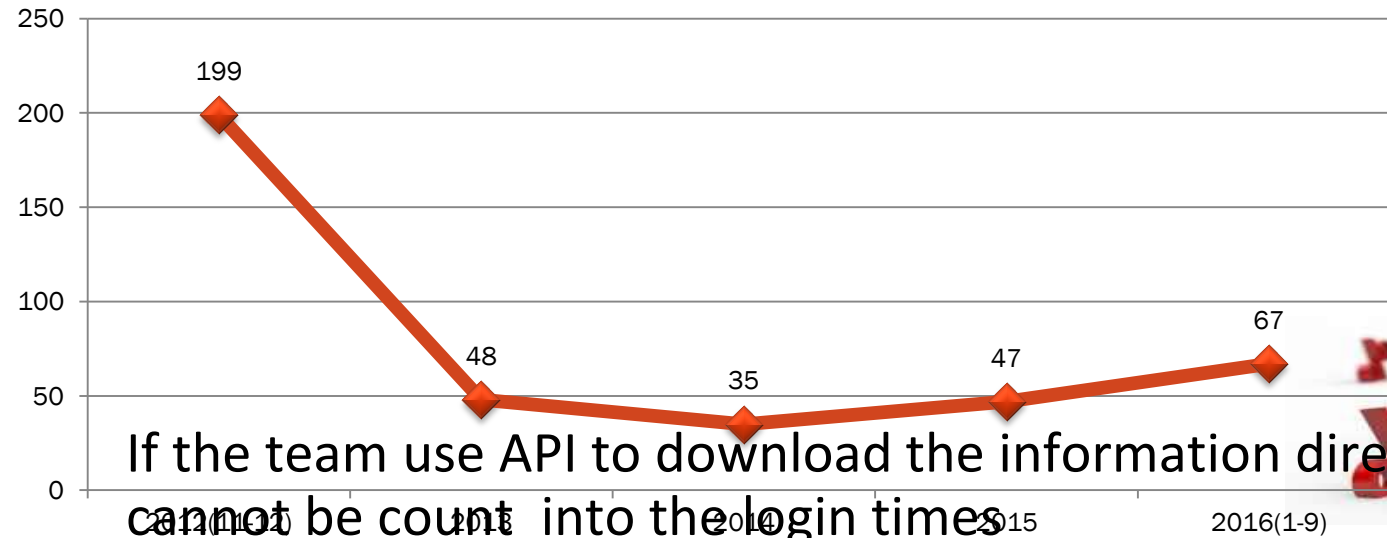
- In Jan-Sep 2016 , the amount of received information for each users.

Organizations	Received information	Organizations	Received information
BDCERT	373	MNCERT/CC	337
BruCERT	292	MOCERT	372
CERT Australia	409	MyCERT	409
HKCERT	418	SingCERT	395
JPCERT/CC	419	Sri Lanka CERT CC	380
KrCERT/CC	414	ThaiCERT	409
LaoCERT	341	TWNCERT	409
mmCERT	318	VNCERT	409

User Activity

Monthly login times from Nov 2012 to Sep 2016.

The monthly statistic of log in times



If the team use API to download the information directly, it cannot be count into the login times



Example of Information Shared by CNCERT/CC - Nitol

Found by Microsoft from some counterfeit versions of Windows OS and announced on Sep. 2012

More than 560 different types of malware hosted on more than 70,000 domains with the potential for targeting millions of hosts



The Official Microsoft Blog

NEWS & PERSPECTIVES

[TechNet Blogs](#) > [The Official Microsoft Blog](#) > [Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain](#)

Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain

13 Sep 2012 12:15 AM

Earlier this week, the U.S. District Court for the Eastern District of Virginia granted Microsoft's Digital Crimes Unit permission to disrupt more than 500 different strains of malware with the potential for targeting millions of innocent people. Codenamed "Operation b70," this legal action and technical disruption proceeded from a Microsoft study which found that cybercriminals infiltrate unsecure supply chains to introduce counterfeit software embedded with malware for the purpose of secretly infecting people's computers. In disrupting these malware strains, we helped significantly limit the spread of the developing Nitol botnet, our second botnet disruption in the last six months.



Nitol – Malicious domains handling

The 3322.org domain is used as the C&C infrastructure for controlling Nitol.

Microsoft had taken over the control of 3322.org domain.

CNCERT helped BitComm and Microsoft to reach a settlement.

The malicious domains were redirected to sinkhole managed by CNCERT.



Thank you for your attention !

