NEWSLETTER

January 2017

National Critical Information Infrastructure Protection Centre

VOLUME 1 ISSUE 1

NCIIPC Newsletter

January 2017

स्वच्छ भारत
एक कदम स्वच्छता की ओर

Inside This Issue

Government of India notified the creation of NCIIPC through a gazette notification on 16th January 2014

Message from NCIIPC Desk

Welcome to the first issue of the NCIIPC monthly newsletter. This newsletter has been introduced with the intention to provide information and updates from around the world dealing with protection of critical information infrastructure.

Government of India notified the creation of NCIIPC through a gazette notification on 16th January 2014. We are celebrating our 3rd foundation day on 16th January 2017, which will also mark the launch of this issue.

In this issue, we have brought news snippets like the return of Shamoon attack on Saudi Arabian organizations, Banks suffering due to an old vulnerability, and, data theft of around one billion Yahoo users. Critical vulnerabilities have been reported in IBM Tivoli Storage Manager, Netgear routers, Siemens IP cameras, NTP daemon, Moxa SoftCMS web server and Adcon Telemetry Gateway Base Station. Security App brings you 'Sysmon', an app by Microsoft to monitor and log system activity.

Taking a step towards information security, NCIIPC and BPCL jointly organised a one day workshop on “Cyber Security and Critical Information Infrastructure Protection” for Oil and Gas industry, at BPCL Regional Office, Noida, on 30th November 2016. The workshop was attended by about 35 officials from Oil and Gas industry. The event helped in spreading awareness about the importance of cyber security practices.

Towards strengthening the information security and resiliency of the Power sector, NCIIPC and India Smart Grid Forum conducted a survey on the information security posture of the Generation, Transmission & Distribution utilities. Based on the findings a “Manual for Cyber Security in Power systems” was prepared by ISGF.

We also present to you an interesting brief on Indian Critical Information Infrastructure Threat Landscape depicting the frequency of incidents, the impacted cities, attack vectors and source of malicious traffic.

News Snippets

Pakistan Intelligence Agencies Spying on Indian Security Forces through Malwares in Mobile Apps

December 15, 2016

Source: India Today

Ministry of Home Affairs (MHA) has indicated that Pakistan Intelligence Agencies are spying on Indian Security Forces by sending malwares through mobile apps such as 'Top Gun' (Game App), 'mpjunkie' (Music App), 'vdjunky' (Video app) and 'Talking Frog' (Entertainment App). The Indian Security forces have been sensitized about ISI using dubious applications on smart phones. Besides, government has circulated a Computer Security Policy and Guidelines to all the ministries/departments on taking steps to prevent, detect and mitigate cyber attacks, which includes, sanitization of staff and officers, and, a Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation. A similar incident was reported earlier this year where an app called 'SmeshApp' was removed by Google from its official Play Store for spying on the Indian Army.

Government has circulated a Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.

Banks under Attack by old Vulnerability in InPage Suite

November 23, 2016

Source: securelist.com

Denis Legezo, while researching a new wave of attacks, has found an interesting target based upon various MSOffice exploits such as CVE-2012-0158. This file had an extension ".inp", which is InPage document. InPage is a publishing and text processing software, mostly popular with Urdu and Arabic speaking users. The file contained a shellcode, which appeared to decrypt itself and further decrypt an EXE file embedded in the document. The sectors for the victims include both financial and governmental institutions.

InPage is an interesting vulnerable software selection as it is widely used within the Urdu/Arabic speaking population.

The threat actors often use more than one malicious document. Between the various phishing campaigns, one particular attack stood out. The targets of this attack were banks in Asia and Africa. During spear phishing, the actors attached InPage files as well as .rtf and word documents with old popular exploits. Several different versions of key loggers and backdoors written mostly in Visual C++, Delphi and Visual Basic were found. Best defense against these exploits is to make sure you have an internet security suite capable of catching exploits.

Organizations in Saudi Arabia reportedly hit by New Shamoon Attacks

December 1, 2016

Source: darkreading.com

The malware, dubbed Shamoon 2, has caused extensive damage at four of the targeted organizations, but defensive measures prevented a similar outcome at the other two organizations, the report said.

Thousands of computers belonging to Saudi Arabia's General Authority of Civil Aviation and at least five other organizations in the country have reportedly been rendered unusable in a destructive wave of cyber attacks in November. The attacks involved the use of Shamoon, a malware tool that made headlines four years ago for erasing the hard disks of more than 30,000 computers at petroleum giant Saudi Aramco. The malware, dubbed Shamoon 2, has caused extensive damage at four of the targeted organizations, but defensive measures prevented a similar outcome at the other two organizations, the report said. Shamoon, which some vendors refer to also as Disttrack, is a malware designed to erase a computer's Master Boot Record and Volume Boot Record thereby rendering the system unusable. Palo Alto Networks said that the malware itself consists of three components: a dropper, a communications piece, and the disk wiper. It is designed to spread to as many systems as possible on a local network, typically using stolen credentials belonging to network and system administrators at the target organizations. The new version of Shamoon also has the same commercial disk drive that was used for disk wiping in the original version down to the same trial license key, said vendors that reviewed the new version this week. Since that original trial key only had a 30-day validity period in August 2012, the new malware resets systems' clocks on infected systems back to August 2012 so the wiper can work.

Ministry of Power committed to Safeguarding National Power Grids from Cyber Attacks

November 17, 2016

Source: Power Ministry

Critical setups at POWERGRID and POSOCO have been certified against ISO-27001 Information Security Management System (ISMS) Standard.

Under directions received from National Critical Information Infrastructure Protection Centre (NCIIPC) and Indian Computer Emergency Response Team (CERT-in), Ministry of Power has taken steps to sensitize all critical organisations under them. The underlying information infrastructure has been audited by third-party agencies accredited by CERT-in and have been hardened to ward off any attacks. Critical setups at POWERGRID and POSOCO have been certified against ISO-27001 Information Security Management System (ISMS) Standard. Further, 'CERT-Transmission' has been identified for coordinating cyber security preparedness in the sector.

Data Associated with more than a Billion Yahoo User Accounts Stolen

December 14, 2016

Source: yahoo.tumblr.com

Yahoo believes that in August 2013 an unauthorized third party stole data associated with more than one billion user accounts. The intrusion associated with theft could not, however, be identified. This incident is likely to be different from the incident disclosed by Yahoo on 22nd September 2016. The stolen user account information may have included names, email addresses, telephone numbers, date-of-birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. It is believed that an unauthorized third party accessed Yahoo proprietary code to learn how to forge cookies.

The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. Company is notifying the affected account holders, and has invalidated the forged cookies. Yahoo has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft disclosed on 22nd September 2016.

It is believed that an unauthorized third party accessed Yahoo proprietary code to learn how to forge cookies.

Yahoo has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft disclosed on 22nd September 2016.

BHEL implements Information Security Management System

November 16, 2016

Source: cio.in

The implementation of smarter electric power distribution grids and other new technologies have led to increased connectivity as well as complexities at BHEL. To cater to the emerging complexities, a qualified information security team was created to implement an enhanced security system, incident management system, user awareness campaigns, and support best practices within the organization. The project had a three-pronged approach. First, the company formed a unified IT team at the corporate and unit levels. Second, the teams were given thorough inputs for capability building, and carrying out the vulnerability assessment and penetration tests for BHEL's critical servers. Third, the top level policy, for information security, was signed and approved by the CMD.

Since the implementation, BHEL has been able to proactively collaborate with Standardization Testing and Quality Certification, NTRO, CERT-IN and NCIIPC. The company also aligned with governmental initiatives like Country Wide Crisis Management and has formulated a Crisis Management Plan.

Since the implementation, BHEL has been able to proactively collaborate with Standardization Testing and Quality Certification, NTRO, CERT-IN and NCIIPC.

Vulnerability Watch

Command Injection Vulnerability in IBM Tivoli Storage Manager FastBack Server Identified

November 16, 2016

Source: cisco.com

Vulnerability in IBM Storage Manager Tivoli FastBack Server could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system. An attacker could exploit this vulnerability to execute arbitrary commands with system privileges, which could result in a complete system compromise. IBM has confirmed this vulnerability and released updated software. To exploit this vulnerability, an attacker would need access to a trusted, internal network in which the targeted device may reside. Administrators are advised to apply the appropriate updates, to allow only trusted users to access local systems and to monitor affected systems.

An attacker could exploit this vulnerability to execute arbitrary commands with system privileges, which could result in a complete system compromise.

Unauthenticated Command Injection Vulnerability in Multiple Netgear Routers

December 19, 2016

Source: kb.cert.org

Netgear R6200, R6250, R6400, R6700, R6900, R7000, R7100LG, R7300, R7900, R8000, D6220, and D6400 routers and possibly other models contain an unauthenticated command injection vulnerability that may be executed directly or via cross-domain requests. Known affected firmware versions include Netgear R7000 version 1.0.7.2_1.1.93, R6400 version 1.0.1.12_1.0.11, and R8000 version 1.0.3.4_1.1.2. Earlier versions may also be affected. The command injection vulnerability has been assigned CVE-2016-6277. By convincing a user to visit a specially crafted web site, a remote, unauthenticated attacker may execute arbitrary commands with root privileges on affected routers. An unauthenticated LAN-based attacker may do the same by issuing a direct request.

Netgear has begun releasing firmware updates for affected models, as specified in their advisory. For users of models without a firmware fix, the web server may be disabled by running http://<router_IP>/cgi-bin/;killall$IFS'httpd'. After performing this step, the router's web administration will not be available until the device is restarted. Users are advised to leave remote administration disabled to prevent the exploit from WAN. Exploiting these vulnerabilities is trivial. Users who have the option of doing so should strongly consider discontinuing use of affected devices until a fix is made available.

A remote unauthenticated attacker may execute arbitrary commands with root privileges on affected routers.

Netgear has begun releasing firmware updates for affected models.

Vulnerability in Siemens-branded IP cameras from Vanderbilt

November 17, 2016

Source: us-cert.gov

Vulnerability has been identified in Siemens-branded IP cameras from Vanderbilt. This vulnerability could be exploited remotely. A successful exploit of this vulnerability may allow the attacker to obtain administrative credentials. An attacker with network access to the web server could obtain administrative credentials by sending certain requests. CVE-2016-9155 has been assigned and has a CVSS v3 base score of 9.8. An attacker with a low skill would be able to exploit this vulnerability. These products are deployed across several sectors including Commercial Facilities, Healthcare and Public Health, and Government Facilities.

Vanderbilt has released updates to mitigate this vulnerability. Company recommends that users operate the devices within trusted networks and protect network access to the devices with appropriate mechanisms. Siemens also recommends enabling authentication on the web server.

An attacker with network access to the web server could obtain administrative credentials by sending certain requests.

An attacker with a low skill would be able to exploit this vulnerability.

Denial of Service vulnerability in Network Time Protocol daemon (ntpd) CVE-2016-7434

November 21, 2016

Source: dumpco.re, scmagazine.com

NTP (Network Time Protocol) is protocol designed to synchronize the clocks of computers over a network. Security researcher Magnus Klaaborg Stubman has identified vulnerability in Network Time Protocol daemon (ntpd) which allows an unauthenticated user to crash ntpd with a single malformed UDP packet, which cause a null pointer dereference. Vulnerability Note VU#633847 from the developers issued fixes for versions of ntpd prior to v4.2.8p9.

This flaw affects Windows only, the alert stated. Users are advised to upgrade to v4.2.8p9, or later, from the NTP Project Download Page or the NTP Public Services Project Download Page and to "properly monitor ntpd instances, and auto-restart ntpd (without -g) if it stops running."

It allows an unauthenticated user to crash ntpd with a single malformed UDP packet.

SoftCMS is central management software that manages large scale surveillance systems.

A successful exploit could allow an attacker to execute arbitrary commands, as well as gain access to administrative functions

Vulnerabilities in Moxa's SoftCMS Webserver Application

November 17, 2016

Source: us-cert.gov

Zhou Yu and Gu Ziqiang have identified vulnerabilities in Moxa's SoftCMS Webserver Application. The affected product, SoftCMS, is central management software that manages large scale surveillance systems. SoftCMS is deployed across several sectors including Commercial Facilities, Critical Manufacturing, Energy, and Transportation Systems. These vulnerabilities could be exploited remotely. Moxa reports that the vulnerabilities affect the SoftCMS versions prior to Version 1.6. Moxa SoftCMS Webserver does not properly validate input. An attacker could provide unexpected values and cause the program to crash or excessive consumption of resources could result in a denial-of-service condition.

A successful exploit could allow an attacker to execute arbitrary commands on the target system, as well as gain access to administrative functions of the application. Also, a specially crafted URL request sent to the SoftCMS ASP Webserver can cause a double free condition on the server allowing an attacker to modify memory locations and possibly cause a denial of service or the execution of arbitrary code. Moxa's suggested mitigation is to update the application (SoftCMS v1.6).

The affected product, A850 Telemetry Gateway Base Station, is a wireless telemetry system.

Vulnerabilities in Adcon Telemetry Gateway Base Station

December 8, 2016

Source: us-cert.gov

Independent researcher Aditya K. Sood has identified a cross-site scripting vulnerability in Adcon Wireless Telemetry's A850 Telemetry Gateway Base Station. This vulnerability could be exploited remotely. Successful exploitation of this vulnerability may affect the integrity of the system. The Web Interface does not neutralize or incorrectly neutralizes user-controllable input before it is placed in the output. This could allow for cross-site scripting. CVE-2016-2274 and CVSS v3 base score of 9.8 has been assigned to this vulnerability.

This product is deployed across several sectors including Commercial Facilities, Critical Manufacturing, Water and Wastewater Systems. Adcon recommends users contact its distributor for information on how to obtain the new firmware version.

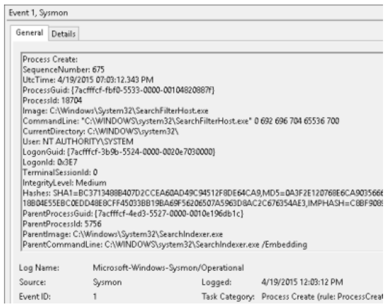
Security App

System Monitor app from Microsoft to Monitor and Log System Activity

November 23, 2016

Source: technet.microsoft.com

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently, by analyzing them, one can identify malicious or anomalous activity and understand how intruders and malware operate on network. *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers. It runs on Windows 7 or higher and Windows Server 2012 or higher.



Snapshot of Sysmon app

Trends

Securing the Digital Economy

December 1, 2016

Source: nist.gov

US Government has established a Commission on Enhancing National Cyber Security to assess the state of nation's cyber security, and developing actionable recommendations for securing the digital economy. The once-bright line between what is critical infrastructure and everything else becomes more blurred by the day. The Internet is one of the most powerful engines for social change and economic prosperity. We need to preserve those qualities while hardening it and making it more resilient against attack and misuse. Partnerships—between countries, between the national government and the states, between governments at all levels and the private sector—are a powerful tool for encouraging the technology, policies, and practices we need to secure and grow the digital economy. The Commission has identified six imperatives for enhancing cyber security -

Imperative 1: Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks

Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy

Imperative 3: Prepare Consumers to Thrive in a Digital Age

Imperative 4: Build Cyber Security Workforce Capabilities

Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age

Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy

The once-bright line between what is critical infrastructure and everything else becomes more blurred by the day.

The Internet is one of the most powerful engines for social change and economic prosperity. We need to preserve those qualities while hardening it and making it more resilient against attack and misuse.

Learning

Cyber-attacks could be used to facilitate the theft of nuclear materials or an act of sabotage resulting in radiological release.

The group identified four overarching priorities that, if implemented, would dramatically reduce the risk of damaging cyber-attacks on nuclear facilities.

Cyber Security at Nuclear Facilities

December 7, 2016

Source: nti.org

Researchers from Nuclear Threat Initiative and SANS recently published a paper on priorities for cyber security at nuclear facilities. Cyber-attacks at nuclear facilities could be used to facilitate the theft of nuclear materials or cause radiological release. The Stuxnet attacks on the Natanz uranium enrichment facility in Iran, the hack of Korea Hydro and Nuclear Power in South Korea, disturbing revelations of malware seeking login credentials found on systems at a German nuclear power plant—demonstrates that the current approach to cyber security at nuclear facilities is falling short, and will soon be insufficient.

To get ahead of this threat, the Nuclear Threat Initiative (NTI) assembled an international group of technical and operational experts with backgrounds in computer security, nuclear safety systems, nuclear engineering, industrial control systems, and nuclear facility operations. This group was tasked with identifying the core elements of a new strategy, then focusing on those elements that would have the greatest possible impact.

The group identified four overarching priorities that, if implemented, would dramatically reduce the risk of damaging cyber-attacks on nuclear facilities. These priorities are: institutionalize cyber security, mount an active defense, reduce complexity, and pursue transformation. Although similar concepts are in use elsewhere, alone and in combination, each of these priorities would provide unique leverage on the threat posed to nuclear facilities.

Events

Workshop on "Cyber Security & Critical Information Infrastructure Protection"

November 30, 2016

Bharat Petroleum Corporation Limied (BPCL) and NCIIPC jointly organized a one day workshop on "Cyber Security and Critical Information Infrastructure Protection" for Oil and Gas industry at BPCL Regional Office, Noida. The workshop was attended by about 35 officials from Oil and Gas industry. Cmde A. Anand, Director–NCIIPC, talked about the importance of Cyber Security for Critical Information Infrastructure Protection in Oil & Gas Industry. The other topics discussed in the workshop were Cyber Attack Vectors, Identification of Critical Information Infrastructure & Notification as Protected System, Cyber Hygiene & OPSEC. The workshop was inaugurated by Smt. Sushma Rath, Joint Secretary (General)-MOP&NG.

NCIIPC Initiatives

Power and Energy

Power and Energy is one of the most critical sectors for Critical Information Infrastructure Protection. In order to strengthen the information security and resiliency of the Power sector, NCIIPC has taken several initiatives. One of such initiative was Cyber Security Preparedness Survey of Power Sector.

NCIIPC and India Smart Grid Forum (ISGF) undertook a survey of the information security posture of a sample set of the Generation, Transmission & Distribution utilities in order to provide an understanding of the present status, the required secure architecture and existing gaps.

NCIIPC and India Smart Grid Forum undertook a survey of the information security posture of the Generation, Transmission & Distribution utilities in order to provide an understanding of the present status, the required secure architecture and existing gaps.

It was necessary to gain an understanding of the cyber security culture in each organization, commencing from the senior most management, to the actual ground personnel, including those not traditionally associated with cyber security such as Legal or Human Resource Development.

The survey was conducted on a sample set of 7 utilities from the Power Sector. All utilities were provided with the detailed Gap Analysis Report along with recommended practices. Top 10 Findings of the Survey was prepared and submitted to Ministry of Power. This was in turn, circulated to Power Sector organisations for compliance by Ministry of Power.

Based on the findings of the survey a “Manual for Cyber Security in Power systems” was prepared by ISGF focused Cyber Security implementation in Power Sector.

Government

The Government sector includes all the Ministries of Government of India except those already covered in major sectors. NCIIPC had pro actively initiated the process of Identification and Notification of UIDAI-CIDR CII as a "Protected System". Consequent to these efforts, the UIDAI-CIDR CII was notified as a "Protected System” in Dec 2015.

Transport

Transportation Sector includes Railway, Aviation, Road and Shipping. Indian transportation sector is increasingly vulnerable to cyber threats as a result of the growing dependencies on network based industrial control systems, navigation, tracking, positioning and communication systems, as well as the ease with which malicious actors can exploit Information systems.

Long Range Identification and Tracking (LRIT), Ministry of Shipping, is amongst the First system to be declared as "Protected System".

Long Range Identification and Tracking (LRIT) system, Directorate General of Shipping, Ministry of Shipping, is amongst the First system to be declared as "Protected System" on 9th February 2016. Similar initiatives have been taken for other sectoral constituents as well to get systems notified and protected.

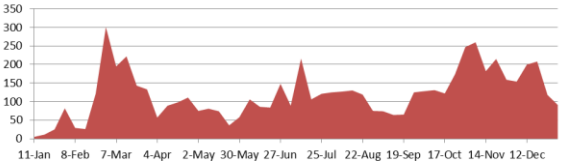


Figure 1: Incidents Reported

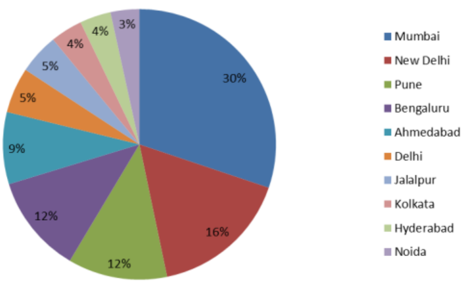


Figure 2: Top Impacted Cities

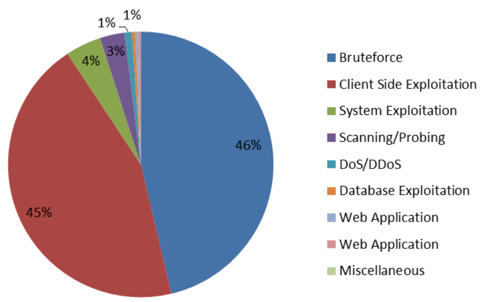


Figure 3: Attack Vectors

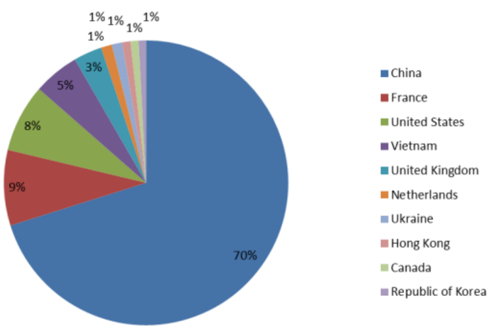


Figure 4: Malicious Traffic Sources

Strategic Public Enterprises

Strategic Public Enterprises include Heavy Industry and Public Sector Units (PSUs). NCIIPC is engaged with 14 CISOs in "Strategic and Public Enterprises" for identification, protection and notification of their CII.

State CII

To protect the CII of States and UTs of the country, NCIIPC has made five zones as Central, East, West, North, and South. Mizoram, Sikkim, Goa and Chhattisgarh have declared their CII as a 'Protected System' under section 70 of IT Act 2000. Assam and Meghalaya have shared the details of Indentified CII with NCIIPC. Haryana and J&K have shown a keen interest for taking all the measures for protecting their cyber space.

Banking, Finance Services and Insurance

Banking sector continues to attract various threat actors including a renewed push by the organized crime groups for taking advantage of the nascent and volatile situation in post-demonetization era. Mobile Banking and various apps must be scrutinized for exploitable vulnerabilities. Ransomware and new variants continue to be of great concern to the sector. There is also an urgent need to evolve sector specific guidelines for handling cyber crises.

Indian Critical Information Infrastructure (CII) Threat Landscape Report 2016

One of the important functions of NCIIPC is to coordinate, share, monitor, collect, analyze and forecast threats for Policy Guidance & Situational Awareness. The present report is a result of valuable data shared by broad range of NCIIPC constituencies. The report is based on total event count of around 7.5 million, related to incidents, threat feeds and vulnerabilities reported from CIIs for the year 2016. It is observed that the maximum number of incidents reported to NCIIPC touches a figure of around 300 towards the end of February month in 2016.

Figure 1 depicts the Cyber Security Incidents that have been reported to NCIIPC for the year 2016. The chart represents the number of incidents reported drawn on the timeline for every week.

Figure 2 indicates that Mumbai has been the top impacted in terms of cyber attack incidents city followed by Delhi and Pune.

Figure 3 depicts that brute force and client side exploitation were the major attack vectors.

Figure 4 presents the share of various kinds of attacks reported. China has been the major source of malicious traffic contributing about 70 percent of total malicious traffic. Figure 4 shows the country wise share of malicious traffic.

Upcoming Events

January

- **NCIIPC Raising Day, New Delhi** Jan 16
- **IoT Tech Expo Global 2017, Olympia, London** Jan 23-24
- **1st ISEA, ASIA Security and Privacy Conference, NIT Surat** Jan 29-Feb 1

JANUARY 2017

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February

- **Cyber Resilience & InfoSeC, Abu Dhabi** Feb 6-7
- **Maximizing Your Leadership Potential Harvard Mumbai India Research Center** Feb 6–9
- **RSA Conference 2017, San Francisco** Feb 13-17
- **SANS Secure India, Bangalore** Feb 20 - Mar 4
- **SC Congress London** Feb 23

FEBRUARY 2017

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28				

March

- **IEEE International Conference on Big Data Analysis, Beijing China** Mar 10-12
- **International Conference on Cryptography, Security and Privacy, Wuhan, China** Mar 17-19
- **Third International Conference on Cryptography And Information Security, Geneva, Switzerland** Mar 25-26

MARCH 2017

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

NCIIPC Helpline

General Help	helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	ir@nciipc.gov.in
Vulnerability Disclosure	rvdp@nciipc.gov.in
Malware Upload	mal.repository@nciipc.gov.in
Website	www.nciipc.gov.in

Feedback/Contribution
Suggestions, feedback and contributions are welcome at
newsletter@nciipc.gov.in