Sri Lanka Computer Emergency Readiness Team | Coordination Centre

Annual Report 2017

CONTENTS

ABOUT SRI LANKA CERT|CC

INTRODUCTION

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the national centre for cyber security in Sri Lanka, mandated to protect the nation's information infrastructure and to coordinate protective measures against, and respond to cyber security threats and vulnerabilities.

ESTABLISHMENT

As the national CERT of Sri Lanka, Sri Lanka CERT|CC acts as the central hub for cyber security of the nation. It is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks.

Sri Lanka CERT was established on 1st of July 2006 as a subsidiary of Information and Communication Technology Agency of Sri Lanka (ICTA). ICTA is the Government Agency responsible for the development of IT Infrastructure and Policy in Sri Lanka and is under the Ministry of Telecommunications and Digital Infrastructure financed by the Government of Sri Lanka.

WORKFORCE

The Sri Lanka CERT|CC has a total staff strength of fourteen team members consisting of the Chief Executive Officer, Director Operations, Principal Information Security Engineer, Senior Information Security Engineer, Research and Policy Development Specialist, Associate Information Security Engineer, five Information Security Analysts, two Associate Information Security Analysts, an officer in charge of Human Resources and Administrative work and a driver/office assistant. This team is supported by five undergraduate interns.

All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council Certified Ethical Hacker (CEH) and Certified Hacking Forensics Investigator (CHFI), Cisco CCNA and CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)[2].

CONSTITUENCY

Sri Lanka CERT's constituency encompasses the entire cyber community of Sri Lanka (private and public-sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government. Based on the availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

ACTIVITIES & OPERATIONS

INCIDENT HANDLING SUMMARY

Sri Lanka CERT|CC being the national contact point for all cyber security related matters, receives numerous incident reports/complaints relating to the country's national cyber-space from both domestic and international partners.

The types of incidents received by Sri Lanka CERT include incidents related to Facebook and social networks, web mail compromise, phishing, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems, and intellectual property violations.

This report presents an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the year of 2017. Based on the said date, following observations can be made;

- Majority of the reported incidents fall in to the category of social media related incidents. Among the social media incidents, Facebook related incidents were the highest.
- Financial frauds targeting local importers and exporters have seen an increase over the past several years. Financial frauds on local importers and exporters have increased more than 100% when compared to 2016.
- There has been an increase in the spread of ransomware and malicious software during the year of 2017, where sensitive data belonging to both individuals as well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.
- A significant number of phishing attacks targeting financial sector organizations were recorded in 2017.
- The number of intellectual property violation incidents shows a decrease in 2017.
- Not a single DoS/DDoS attacks were reported to Sri Lanka CERT during the year 2017.

The above findings lead to the following conclusions:

- Cyber criminals are changing their strategies in order to obtain more financial gains. Social engineering methods are widely adopted and ransomware is becoming a major threat to many organizations and individuals.
- Cyber security has to be recognized as a responsibility not only of organizations but also of every citizen, and each and every citizen has to contribute to ensure a secure online environment.
- Social media related incidents increased exponentially. Therefore, education and awareness among general public is important to ensure secure and ethical usage of social media sites.
- Making the general public, private and public-sector organizations aware of the various types of cyber threats is essential in order to ensure that people gain benefits of the Internet rather than become victims in the cyber world.

INCIDENT HANDLING STATISTICS

Cyber-security related incidents reported to Sri Lanka CERT have increased in the year 2017 compared to previous years. In 2017, a total of 3907 incidents were reported to Sri Lanka CERT. This is a 66.89% increase in comparison to the previous year.

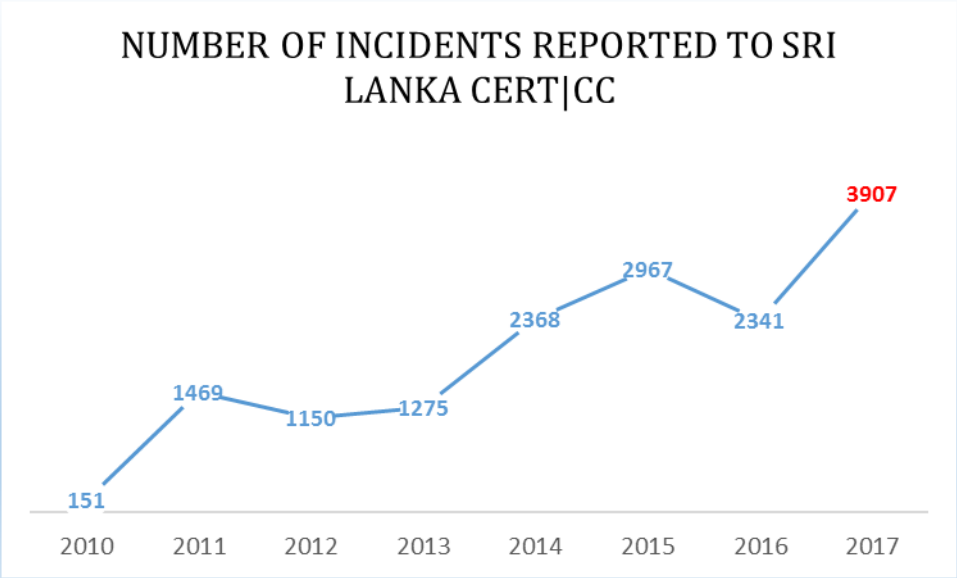

Figure 1. Growth of the number of incidents reported

Type of Incident	Number of Incidents
Phishing	42
Abuse/Hate/Privacy Violation	29
Ransomware	15
Scams	32
Malicious Software issues	24
Financial Frauds	35
Web site Compromise	25
Hate/ Threat emails	14
Intellectual Property violation	06
Unauthorized Access	-
DoS/DDoS	-
Social Media related incidents	3685
Total	3907

Table 1. Types of incidents

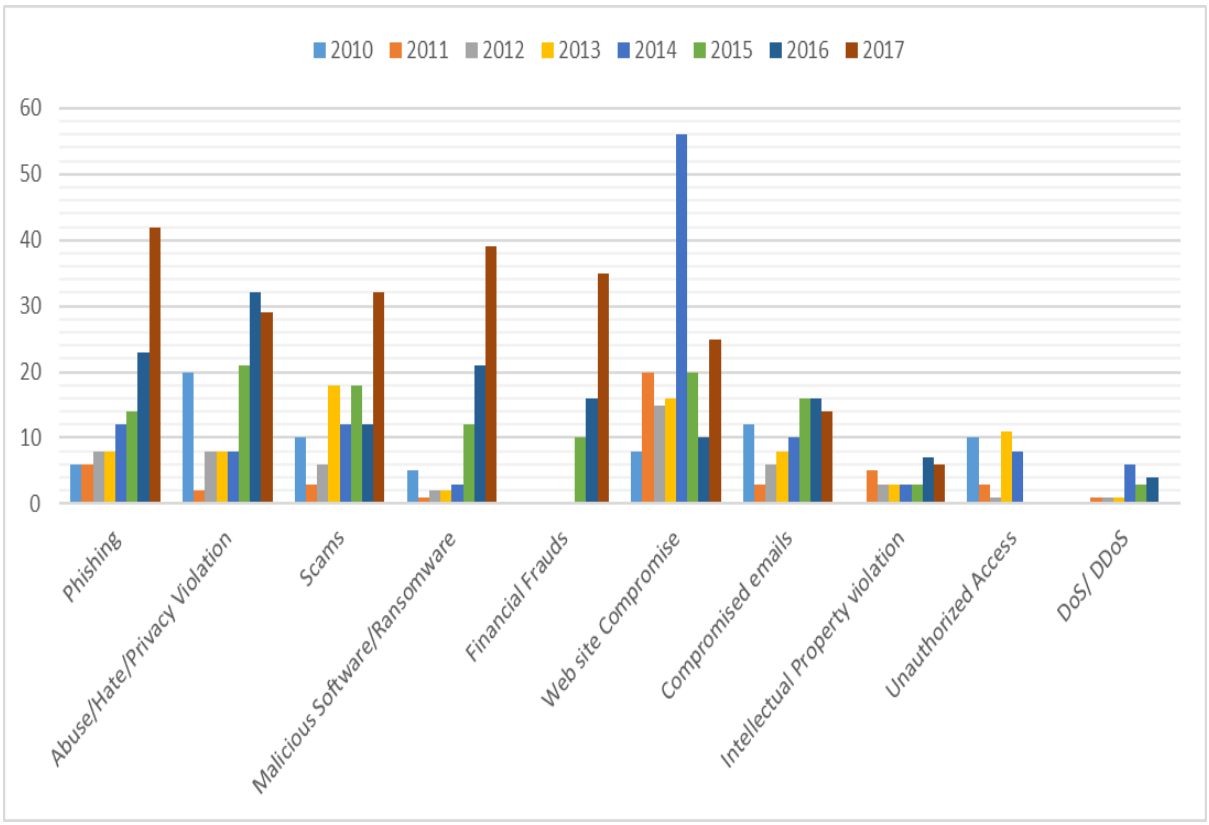

Figure 2. Growth of the types of cyber security incidents

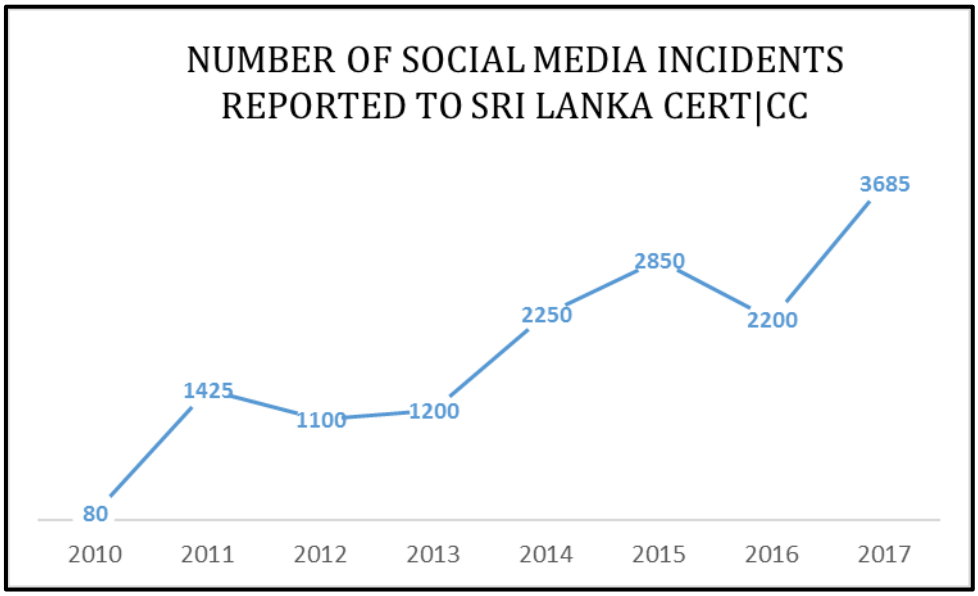

Figure 3. Growth of the social media related incidents

The reported social media related incidents can be categorized as follow.

Social Media Related Incident Types	Number of Incidents
Compromised Accounts	829
Fake Accounts	2018
Phone No Posted	54
Threatening	57
Ransom	1
Email	12
Website	7
Other	241
Porn Video	17
Copyright Violation	7
Photo Abuse	416
Total	3685

Table 2. A classification of the social media related incidents

CONSULTANCY SERVICES

Sri Lanka CERT|CC continues to provide consultancy services for its constituency (government and non-government).

Typical consultancy services provided during the period include;

- Security assessments for more than 40 government ministries/departments/statutory boards web sites.
- Security assessments for several private organizations.
- VAPT Assessments carried out for requested Networks
- Information Systems Security Review for a major government organization.
- Consultancy for a bank on conducting Security Assessments on their systems.
- Consultancy provided for few organizations which were under ransomware attacks.
- Email Header Analysis and security settings reviews for two private companies.
- Consultancy provided for more than 15 website defacement incidents.

TRAINING / EDUCATION SERVICES

Sri Lanka CERT|CC continues to conduct and facilitate training programs and education sessions targeting various audiences. This includes Chief Innovation Officers (CIOs), System Administrators, Banking and Telecom Sector Staff, Law enforcement authority staff, Tri-forces, Students, Engineers and the General Public.

1. Awareness Program and Training Sessions

○ Participated for Internet security related discussions.
○ Approximately 25 Awareness and Training sessions conducted for law enforcement officers including police officers and judges on Internet safety, Social media Security, cybercrime and electronic evidence and related incident handling.
○ Newspaper articles
○ Information and Cyber Security alerts communicated through Radio and TV Channels
○ Posters on Internet Safety – Ministry of Education.
○ Carried out awareness sessions in national level events such as “Yowun Puraya”.
○ Internet Security Awareness sessions carried out in three government schools for teachers, students and parents.
○ Conducted two Security Policy Development sessions for Government Officials.
○ Conducted training sessions for private companies on their requests.
○ Several awareness sessions for Principals and Education Administrative officers on Cyber security and internet safety.
○ Eight sessions on “How to be safe on Social Media” for District Child development officers.
○ Judges Training Program – Council of Europe (COE) - Special training on cybercrime and electronic evidence for Nepal Judicial Officers
○ Nine EDUCSIRT Training programs for school teachers on different topics including Information security, Social Media safety and incident handling
○ 1938 Helpline training session on Social Media related incident handling organized by Ministry of Women and Child Affairs
○ E-Leadership training program for Senior Local government officials on Information Security and Cybercrime
○ Carried out several training sessions for Government CIOs.
○ Internet safety and policy development sessions for Officers in Tri Forcers.
○ Around 5 awareness and training sessions for SLAS officers.
○ Awareness Session for undergraduate students in a local private university.

2. Awareness through Electronic/Print Media

o Hiru TV - Cybercrime program (complete 20 episodes out of 56)
o Udhayam TV - Awareness program on cyber security
o Newspaper articles
o Information and Cyber Security alerts communicated through Radio and TV Channels
o Posters on Internet Safety – Ministry of Education.

3. Annual Cyber Security Week 2017

Activities carried out at the Cyber Security Week
o Hacking Challenge
o Cyber Security Quiz for Universities
o Workshops
o 10th Annual National Cyber Security Conference
o Handbook on Security was launched and copies were distributed to conference participants

4. Council of Europe (COE)/GLACY project

Sri Lanka CERT|CC is engaged with a capacity building programme of the Council of Europe, under a project titled Global Action Against Cybercrime (GLACY) and has been engaged in conducting training programs for law enforcement and officials from Judicial service.

- Participated for a workshop on Criminal Justice statistics on cybercrime and electronic evidence (Ghana)
- Advisory mission on CERT capacities, digital forensics lab and public-private cooperation and a Workshop on cybercrime reporting systems and collection and monitoring of criminal justice statistics on cybercrime and electronic evidence in Nuku'alofa, Tonga, - participated as Council of Europe expert, assess and suggested the CERT operations and way forward. In the workshop importance of criminal justice statistics were presented.
- Global Action On Cybercrime Extended – 3 workshops (Singapore)
- T-CY 17th Plenary meeting, GLACY+ Steering Committee meeting, - Participated with Sri Lankan Delegates (Country coordinator, Judiciary and law enforcement agents) to present how the TOT programs were effective and how to sustain the training for judiciary and law enforcement in long term.
- Special training on cybercrime and electronic evidence for Nepal judicial officers with trainers from Sri Lanka Judges' Institute in partnership with Nepal Judicial Academy at Kathmandu, Nepal - Participated as resource person to carryout presentations for the course along with Sri Lankan Judges. Trained 25 Nepal Judges during 5day training program.
- Special training on cybercrime and electronic evidence were conducted in Sri Lanka with the support of Council of Europe, Participated as resource person to carryout presentations for the course along with Sri Lankan Judges (1 High court judge, and 3 for Magistrates). 70+ High courts judges and 180+ magistrates from different parts of the country were the participants in these training programs.

PUBLICATIONS

Website

The Sri Lanka CERT|CC website publishes security related awareness bulletins for the public through News Alerts, Glossaries, Case Studies, Statistics and FAQs.

E-mails

Sri Lanka CERT|CC disseminates security related information through e-mails to its subscribers.

Newsletters

Sri Lanka CERT|CC continues to publish and circulate The Cyber Guardian e-newsletter to a large number of students, through the SchoolNet- the network connecting secondary schools in Sri Lanka.

Newspapers/media

Sri Lanka CERT|CC continues to educate the general public through the electronic and print media about emerging cyber security threats and vulnerabilities with recommendations on how to safeguard themselves against these attacks.

OPERATIONAL SUPPORT PROJECTS

It was able to conduct a project to acquire cyber security investigation/assessment resources and enhance the capabilities of staff during the year 2017. This project was funded by government of Sri Lanka.

SPECIAL PROJECTS

Project Name	Description and Activities
○ National Certification Authority (In progress)	○ Procurement of Hardware is completed ○ Procurements of software is completed ○ Procurement of two data centre locations for production and backup sites are in progress. ○ Staff trainings are completed. ○ Implementation is started.
○ National Security Operations Center (In progress)	○ This is a joint project with ICTA. ○ Procurement in progress.

○ Activities with EduCSIRT (Sector based CSIRT for Educational Sector. Established in collaboration with Ministry of Education)	○ Development of Training modules is completed ○ Completed two trainings for two batches
○ Cyber Security Project (Funded by UK High Commission)	○ Procurement of Cybercrime investigation resources for Sri Lanka CERT (Encase forensics software and video and image analysis software) ○ User Trainings for staff on forensics software ○ Specific foreign trainings on cyber security provided for Sri Lanka CERT ○ Awareness programmes for government organizations and general public

EVENTS ORGANIZED

SEMINARS & WORKSHOPS

- Cyber Security Week 2017

Since 2008, Sri Lanka CERT|CC has been conducting an annual security awareness programme titled Cyber Security Week (CSW). This international event attracted the attention of the local as well as regional information security professionals. Cyber Security Week 2017 was held in the month of August 2017, and featured a series of events including the following;

- Annual National Conference on Cyber Security 2017 – Securing Critical Infrastructure and Environment.

  - Three full-day Workshops for professionals, namely:
    - Workshop 1 on "Advanced Web Application Security (Hands on)"
    - Workshop 2 on "Incident Response and Internet Security"
    - Workshop 3 on "Ethical Hacking and Forensic Computing"

  - Hacking Challenge: Hacking Challenge is a contest for IT Professionals to attack or defend an actual network within a given timeframe. The participants were Technical Security Professionals, Network Administrators, System Administrators and students following information security post-graduate courses.

  - Cyber Security Quiz: This competition is open only to students of Sri Lankan Universities and other tertiary education institutions. The objective of the quiz is to assess the knowledge and to identify and reward the aspiring young information security professionals.

- Workshop on Development of the National Cybersecurity Strategy.

  - Two Cyber Security Experts from UK were invited to provide insights for the development of a national cyber security strategy,
  - Task Force members and Stakeholders participated for the workshop and shared their ideas for the strategy.

ACHIEVEMENTS

NATIONAL CYBER SECURITY STRATEGY

2016/2017

Sri Lanka CERT|CC commenced work on the first draft of the national cyber security strategy for Sri Lanka in 2016. Stakeholder consultations have been initiated to identify key strategic thrust areas. Following six strategic thrust areas are identified namely;
(1) Establishment of Governance Framework
(2) Enactment and Establishment of Legislation
(3) Policies and Standards, Resilient Digital Government and Infrastructure
(4) Development of Competent Workforce
(5) Raising Awareness and Empowerment of Citizens, and
(6) Development of Public-Private, Local-International Partnerships.

RESEARCH AND POLICY DEVELOPMENT

Sri Lanka CERT strengthened its research arm by recruiting a research team. The team conducted several surveys, such as, Youth's Survey on Social Media Awareness and Public Service Managers Information and Cyber Security Readiness Survey.

CERTIFICATION & MEMBERSHIP

Sri Lanka CERT continues to maintain memberships with following professional organizations;

a) (ISC)2 Colombo Sri Lanka Chapter the local representative organization of International Information Systems Security Certification Consortium.
b) Threat Intelligence from ShadowServer.

NEW SERVICES

Sri Lanka CERT is expecting to deliver cyber security managed services during the year of 2018 and has completed the preparatory work during this year.

INTERNATIONAL COLLABORATION

EVENT PARTICIPATION

- Global Cybersecurity Center for Development (GCCD) Training, Korea. Organized by KISA, CAMP
- Cyber Detection, Eradication and Forensic (Cyber D.E.F) Confirmation - APCERT online training Webinar organized by MyCERT.

- Participated for APISC Security Training Course organized by KISA in Soul, Korea.
- APCERT Annual General Meeting and Conference hosted by CERT-In –New Delhi
- Cyber Offence and Defensive Exercise organized by National Information and Communication Security Taskforce Taiwan, R.O.C.
- International visitor leadership program on "Cyber Security". Organized by US Embassy.
- Participated for USTTI training in Washington, DC.

OTHER ACTIVITIES

- Reporting of malicious IP address details received from International counterparts to local ISPs. The International counterparts consists of CERT Bund - Germany, Microsoft, Shadow Server and APCERT Data Exchanger.
- Continuing with network monitoring project "Tsubame" with JPCERT|CC
- Conducted APCERT webinar on "digital forensics and its importance on CERT day to day operations" for the APCERT members
- Conducted Training for Bhutan government officials on Website Security and Network Security (Bhutan).
- Conducted site visit to Bhutan CIRT as the sponsor for membership of APCERT and FIRST and conducted a training program for Bhutan government officers.

INTERNATIONAL INCIDENT COORDINATION

- APCERT Cyber Security Drill
  - Worked as a member of the organizing committee of APCERT Cyber Security Drill 2017
  - Participated for the drill
- Engagements with CERTs in the Asia Pacific region. Sri Lanka CERT has regular operational engagements with CERTs/Information security organizations in-other regions of the world and commercial establishments and solution providers (such as Facebook, Google, Yahoo) to resolve phishing and identity theft incidents.

FUTURE PLANS

FUTURE PROJECTS

- Development of National Cyber Security Strategy (In progress).
- Development and Implementation of a Security Operations Centre (In progress).
- Establishment of the National Certification Authority (In progress).
- Establishment of sector based CSIRT's (e.g. Telco-CERT).
- Cyber Security Week 2018.

FUTURE OPERATIONS

This section details the changes anticipated in Sri Lanka CERT with regard to staff, equipment and capabilities:

- Sri Lanka CERT shall recruit undergraduate students on internships basis to enhance the information security capabilities of the younger generation.

- Sri Lanka CERT shall continue to operate as a skilled small group of professionals.
- Sri Lanka CERT shall continue to invest on developing the capacity of the staff.

CONCLUSION

As predicted in Sri Lanka CERT's Annual Report of 2016, a significant growth in financial frauds and ransomware attacks targeting small and medium size businesses were observed in 2017.

During this period, Sri Lanka CERT carried out a large number of information and cyber security training and awareness sessions, and the demand for such programs are increasing. All the events organized by Sri Lanka CERT during the period were very successful, well attended and were high in demand. Sri Lanka CERT will continue to conduct the Annual Cyber Security Week and the Annual National Conference on Cyber Security as we have planned.

Furthermore, Sri Lanka CERT aims to complete the development of the National Information and Cyber Security Strategy during the first quarter of 2018

Sri Lanka CERT continues to receive requests from other newly established CERTs/CSIRTs to be their sponsor for membership of APCERT and/or FIRST.

Sri Lanka CERT is currently working with UK Foreign and Commonwealth Office and the Council of Europe to enhance the cyber security posture in the country which may have a significant impact to the other nations. During the year 2017 it was able to complete most of the activities that we had planned to achieve this target.

In addition to securing Sri Lanka's cyberspace, Sri Lanka CERT is committed to building a secure information environment in the Asia Pacific region/world with the help of all the CERTs and information security organizations through APCERT/FIRST.