The OIC-CERT is the acronym for the Organization of the Islamic Cooperation – Computer Emergency Response Team. It is an international platform mainly for member states of the Organization of the Islamic Cooperation (OIC) focusing on cyber security and knowledge sharing. This platform encourages and supports the smooth collaboration and cooperation between Computer Emergency Response Teams (CERTs) among the OIC member countries and other stakeholders as required.

The OIC has accepted the establishment of the OIC-CERT in 2008 by approving the resolution on “Collaboration of the Computer Emergency Response Team (CERT) Among the OIC Member Countries” and now this collaboration is an Affiliate Institution of the OIC.

The objectives and scope of the OIC-CERT are:

1. Strengthening the relationships amongst CERTs among the OIC Member Countries, OIC-CERT partners and other stakeholders in the OIC member domain;

2. Encouraging experience and information sharing in cyber security areas;

3. Preventing and reducing cyber crimes, harmonizing cyber security policies, laws and regulations;

4. Building cyber security capabilities and awareness amongst member countries;

5. Promoting collaborative research, development and innovation in cyber security;

6. Promoting international cooperation with international cyber security organizations; and

7. Assisting OIC-CERT member countries in establishing and developing their national CERTs.
MEMBERSHIP

The Full Member - CERTs or CSIRTs or similar entities that are located and/or primary function within the jurisdiction of OIC member countries that is wholly or partly owned by the government with the authority to represent the country’s interest.

Azerbaijan: Azerbaijan Government CERT (CERT.GOV.AZ)
Bangladesh: Bangladesh Computer Emergency Response Team (BangladeshCERT)
Brunei Darussalam: Brunei Computer Emergency Response Team (BrCERT)
Cote D’Ivoire: Cote D’Ivoire Computer Emergency Response Team (CI-CERT)
Egypt: Egypt Computer Emergency Response Team (EG-CERT)
Indonesia: Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC)
Iran: Iran Computer Emergency Response Team (IRCERT)
Jordan: Jordan Computer Emergency Response Team (JO-CERT)
Kazakhstan: Kazakhstan Computer Emergency Response Team (KZ-CERT)
Libya: Libyan Computer Emergency Response Team (Libya-CERT)
Malaysia: CyberSecurity Malaysia
Morocco: Moroccan Computer Emergency Response Team (maCERT)
Nigeria: Consultancy Support Service Limited (CS2)
Oman: Oman National Computer Emergency Response Team (OCERT)
Pakistan: National Response Centre for Cyber Crimes (NR3C)
Saudi Arabia: Computer Emergency Response Team – Saudi Arabia (CERT-SA)
Sudan: Sudan Computer Emergency Response Team (SudanCERT)
Tunisia: National Agency for Computer Security (tunCERT)
United Arab Emirates: UAE Computer Emergency Response Team (aeCERT)

As of December 2016, after two decades of its conceptualisation in 2005, the OIC-CERT now boasts a strong network and strategic collaboration of 28 teams, agencies and establishments from 21 OIC countries. This alliance is further supported through the inception of seven (7) Commercial Members, four (4) Professional Members, one (1) Fellow Member and 1 Honorary Member.
The General Member - Other related government organizations, non-governmental organizations or academia that deals with cyber security matters. However, these parties do not have the authority to represent the country’s interest.

<table>
<thead>
<tr>
<th>Country</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangladesh</td>
<td>Bangladesh Computer Emergency Response Team (bdCERT)</td>
</tr>
<tr>
<td>Iran</td>
<td>Isfahan University of Technology Computer Emergency Response Team (IUTcert)</td>
</tr>
<tr>
<td></td>
<td>Amirkabir University of Technology Computer Emergency Response Team (AUTcert)</td>
</tr>
<tr>
<td></td>
<td>Sharif University of Technology Computer Emergency Response Team (SharifCert)</td>
</tr>
<tr>
<td></td>
<td>Shiraz University ICT Center (SUcert)</td>
</tr>
<tr>
<td></td>
<td>Maher Center</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Pakistan Information Security Association (PISA-CERT)</td>
</tr>
<tr>
<td>Turkey</td>
<td>Turkey Computer Emergency Response Team (TR-CERT)</td>
</tr>
</tbody>
</table>

The Commercial Member - Industrial or business organization that deals with cyber security matters from OIC and non-OIC member countries.

<table>
<thead>
<tr>
<th>Country</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td>DUZON</td>
</tr>
<tr>
<td>Malaysia</td>
<td>FIREEYE MALAYSIA</td>
</tr>
<tr>
<td></td>
<td>InfoSys Gateway Sdn Bhd</td>
</tr>
<tr>
<td></td>
<td>Telekom Applied Business Sdn Bhd (TAB)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Security Response Centre (MSRC)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Intellium Ltd</td>
</tr>
<tr>
<td>Somalia</td>
<td>Telesom</td>
</tr>
</tbody>
</table>

The Professional Member - Individuals who are experts in the information security area.

<table>
<thead>
<tr>
<th>Country</th>
<th>Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malaysia</td>
<td>Assoc. Prof. Hatim Mohammad Tahir</td>
</tr>
<tr>
<td></td>
<td>Prof. Dr. Rabiah Ahmad</td>
</tr>
<tr>
<td></td>
<td>Abdul Fattah Mohamed Yatim</td>
</tr>
<tr>
<td>Yemen</td>
<td>Dr. Abdulrahman Ahmad Abdu Muthana</td>
</tr>
</tbody>
</table>

The Fellow Member - These are individual co-founders of the OIC-CERT and those who use to actively represent their organization as an OIC-CERT member for a minimum period of 5 years.

<table>
<thead>
<tr>
<th>Country</th>
<th>Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunisia</td>
<td>Prof. Nabil Sahli</td>
</tr>
</tbody>
</table>

The Honorary Member - Individuals or organizations who has demonstrated extraordinary contributions, support and exemplary leadership to the OIC-CERT.

<table>
<thead>
<tr>
<th>Country</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saudi Arabia</td>
<td>Organisation of Islamic Cooperation</td>
</tr>
</tbody>
</table>
MEMBERS’ ACTIVITIES

azerbaijan ................................................................. 6
Azerbaijan Government CERT ................................................................. 6

brunei darussalam ................................................................. 8
Brunei Computer Emergency Response Team ................................................................. 8

egypt ................................................................. 12
Egypt Computer Emergency Response Team ................................................................. 12

iran ................................................................. 13
Iran Computer Emergency Response Team ................................................................. 13

malaysia ................................................................. 15
CyberSecurity Malaysia ................................................................. 15

nigeria ................................................................. 21
Consultancy Support Services (CS2) Limited ................................................................. 21

oman ................................................................. 30
Oman National CERT ................................................................. 30

tunisia ................................................................. 34
Tunisia CERT ................................................................. 34

united arab emirates ................................................................. 35
UAE CERT ................................................................. 35

yemen ................................................................. 37
Smart Security Solutions (SmartSec) ................................................................. 37
A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES

CERT.GOV.AZ offers assistance in computer and network security incident handling. It provides incident coordination functions for all incidents involving systems and networks located in the state sector of Azerbaijan Republic. The services provided among others are:

1. Incident Response

CERT.GOV.AZ will assist system administrators in managing the technical and organizational aspects of the incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management.

2. Incident Triage

- investigating whether indeed an incident has occurred; and
- determining the extent of the incident.

3. Incident Coordination

- determining the initial cause of the incident (the used vulnerability);
- facilitating contact with other sites which may be involved;
- making reports to other CERT or Computer Security and Incident Response Team (CSIRT) teams; and
- composing announcements to users, when applicable.

4. Incident Resolution

- removing the vulnerability;
- liquidating the consequences of incident;
- evaluating of possible additional actions taking into account their cost and risk;
- providing assistance in evidence collection and data interpretation when needed; and
- collecting statistics concerning incidents and will notify the community where necessary to assist in protecting against known attacks.

5. Proactive Activities

i. Information services

CERT.GOV.AZ publishes advisories for events and incidents that are considered to be special importance to users in the constituency. Information is disseminated via various channels such as the web, RSS feeds, mailing lists.

ii. Training services

Staffs of CERT.GOV.AZ periodically hold seminars on various aspects of information and network security.

---

1 Rich Site Summary or often called Really Simple Syndication uses a family of standard web feed formats to publish updated information.
B. ACHIEVEMENTS

- Started with the security and management of the .gov.az zone.
- Centralized DNS, hosting, and mail services for the government bodies.
- Have the government organisations to bring the spread out systems hosts and systems from distributed servers around the world into a datacenter which is located in Azerbaijan. The center is supported, penetration tested and monitored by the CERT.gov.az team.
- Prioritized security by implementing penetration testing on government information systems at least twice a year in accordance to regulations accepted by Community of Ministries.
- Combined all government bodies’ IT administration into one ticketing system to enable the registration of incidents and solutions.
- Made available the electronic library and Frequently Asked Question (FAQ) systems to the government bodies within the ticketing system.
- Established international relations with other CERTs and international communities since 2010.
- Became the full member of FIRST\(^2\), CERT CC\(^3\), TF-CSIRT\(^4\), and OIC-CERT.
- Signed Memorandum of Understanding (MoUs) with other countries and laboratories.
- Published Information Security Journal per yearly quarter (4 annually) and spread it to government organisations with no fee.
- As a Steering Committee (SC) of the OIC-CERT.

C. ACTIVITIES AND OPERATIONS

1. Events organized by the organization / agency

- Took part in organising the 1st web security championship "Hackton" in Azerbaijan.
- Organized the Cyber Drills to strengthen and measure the awareness of the government bodies; and
- Organized courses and awareness seminars to the responsible parties within an organisation

2. Events involvement

Took part in many international and local conferences and events providing seminars to educate IT staff, diplomats, and media representatives, to name a few.

3. Achievement

It is found that the level of security / awareness has increased.

D. 2017 PLANNED ACTIVITIES

- Establish relations with other partners; and
- Implement the CERT.gov.az anti-malware project.

E. OTHER INFORMATION

- https://www.youtube.com/watch?v=Z94qVlkgdj8

CERT.GOV.AZ welcome reports on computer security related incidents at:
Telephone: (994) 124352825 / (994) 124352833

---

\(^2\) Forum for Incident Response and Security Team
\(^3\) CERT Coordination Center, a non profit United States federally funded research and development center.
\(^4\) A task force that promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions.
A. ABOUT BRUCERT

INTRODUCTION

The Brunei Computer Emergency Response Team (BruCERT) was established in May 2004. It was formed in collaboration with the Info-communications Technology Industry (AITI), the Ministry of Communication, to become the nation’s first trusted one-stop referral agency in dealing with computer-related and internet-related security incidents in Brunei Darussalam.

1. BruCERT Services

- 24x7 Security Related Incidents and Emergency Response from BruCERT.
- 24x7 On site Security Related Incidents and Emergency Response with the deployment response to be within 2hrs after an incident is received. This service only applies to BruCERT Constituents.
- Broadcast alerts (early warning) of new vulnerabilities, advisories, viruses and security guidelines on BruCERT Web site. BruCERT constituents will receive alerts through email and telephone as well as mitigation strategies in managing the IT security related issues.
- Promote Security Awareness Programs to educate and increase the public awareness and understanding of information security and technical know-how. This is done through education modules, workshops, seminars and trainings.
- Coordinate with other CERT, network service providers, security vendors, government agencies as well as other related organization to facilitate the detection, analysis and prevention of security incidents on the internet.

2. BruCERT Establishment

BruCERT coordinates with the local and international CSIRTs, network service providers, security vendors, law enforcement agencies as well as other related organizations to facilitate the detection, analysis and prevention of security incidents on the Internet.

3. BruCERT Workforce

BruCERT currently has 66 staff (100% local) with the majority specializing in IT while others are in administration and technical support. The staff has undergone training on various IT and security modules, such as A+, N+, Linux+, Server+, Security+, SCNP, SCNA, CIW, CEH, CCNA, CISSP, BS7799.

5 Security Certified Network Professional
6 Sun Certified System Administrator
7 Certified Internet Web Professional
Implementer, and SANS trainings such as GREM, GCIA, GCII, GCFA, and GPEN. Most of the BruCERT workforce has received certifications in these trainings.

4. BruCERT Constituents

BruCERT has established relationship with government agencies, two (2) major Internet Service Providers and numerous vendors.

i. Government Ministries and Departments

BruCERT provide security incident response, managed security services, and consultancy services to the government agencies. Security trainings such as digital forensic, and awareness programs were provided by BruCERT in collaboration with the relevant government agencies.

ii. The E-Government National Centre

The E-Government National Centre (EGNC) provides IT services to all government departments and ministries in Brunei Darussalam. Services such as the IT Central procurement, Network Central Procurement, co-location, ONEPASS (a PKI initiative), co-hosting are provided by EGNC. BruCERT work closely with EGNC in providing incident response and security monitoring since most of the government equipment resided at EGNC.

iii. The Authority for Information and Communications Technology Industry of Brunei Darussalam

The Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is an independent statutory body regulating, licensing and developing the local ICT industry. AITI also manage the national radio frequency spectrum.

AITI has appointed Information Technology Protective Security Services (ITPSS), a local IT security company, to become the national CERT and provide incident response services for Brunei Darussalam.

iv. The Royal Brunei Police Force and other Law-Enforcement Agencies

BruCERT has been collaborating with the Royal Brunei Police Force (RBPF) and other Law Enforcement Agencies (LEAs) to resolve computer related incidents through BruCERT’s Digital and Mobile Forensic Services.

v. TelBru – BruNet

TELBru, the main Internet service provider, and BruCERT have been working together to share information of Internet related statistics and the current Brunei Darussalam IT landscape.

vi. DST

The second largest internet service provider in Brunei.

5. BruCERT Contact

BruCERT welcomed reports on computer security related incident. Any computer security incident can be reported at:

- Telephone: (673) 2458001
- Facsimile: (673) 2458002
- Email: cert@brucert.org.bn
- website: www.brucert.org.bn

B. BruCERT OPERATION IN 2015
1. Incidents Response

In 2015, BruCERT receives a high number of security incident reports from both the public and the private sectors. There were an increasing number of incidents that had been reported to BruCERT, which indicate positive feedbacks from the Brunei community. There was also a decreasing number of website that had been defaced in Brunei. This might be due to the increasing awareness activities by the government and the public sector regarding the importance of information security in maintain the website. Most of the defacement are due to the lack of security controls being placed and lack of security patches updating by the victims. The statistic of the security incidents is shown.

INCIDENT SUMMARY 2015

<table>
<thead>
<tr>
<th>Types of Attacks</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Website</td>
<td>1</td>
</tr>
<tr>
<td>Cyber Harassment</td>
<td>2</td>
</tr>
<tr>
<td>Spam</td>
<td>542</td>
</tr>
<tr>
<td>Scam</td>
<td>9</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>832</td>
</tr>
<tr>
<td>Website defacement</td>
<td>8</td>
</tr>
</tbody>
</table>

Exploits targeted by Malware. Exploits used by the malware and the total number of times it has been used.

2. Summary of BruCERT Honeypot Project

BruCERT had deployed the Honeypot project initiative with TelBru. With this Honeypot, BruCERT can have a better understanding on the current security landscape of Brunei Darussalam’s cyber space.

3. Summary of the Honeypot Activities

The following data shows the overall activities of the Honeypot from January 2015 until December 2015.

Exploits

<table>
<thead>
<tr>
<th>Malicious attacks</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>52</td>
</tr>
</tbody>
</table>

Most attacked Port. Most attacked port and the total number of hits.

Port

<table>
<thead>
<tr>
<th>Destination ports</th>
<th>Description</th>
<th>Total hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>4433</td>
<td>MySQL</td>
<td>175486</td>
</tr>
<tr>
<td>5000</td>
<td>MySQL</td>
<td>182087</td>
</tr>
<tr>
<td>1555</td>
<td>MySQL</td>
<td>129459</td>
</tr>
<tr>
<td>23</td>
<td>www</td>
<td>20536</td>
</tr>
<tr>
<td>115</td>
<td>none</td>
<td>22166</td>
</tr>
<tr>
<td>80</td>
<td>ftp</td>
<td>21353</td>
</tr>
<tr>
<td>6050</td>
<td>none</td>
<td>16773</td>
</tr>
<tr>
<td>22</td>
<td>ssh</td>
<td>16757</td>
</tr>
<tr>
<td>4116</td>
<td>none</td>
<td>15070</td>
</tr>
<tr>
<td>3126</td>
<td>none</td>
<td>15050</td>
</tr>
</tbody>
</table>

Vulnerabilities

<table>
<thead>
<tr>
<th>Destination ports</th>
<th>Descriptions</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>5090</td>
<td>Microsoft Terminal Server (RDP)</td>
<td>CVE-2012-0173 Vulnerabilities provided: attacker with remote access via Remote Desktop Protocol (RDP).</td>
</tr>
<tr>
<td>5090</td>
<td>Universal Plug and Play (UPnP)</td>
<td>CVE-2015-8687 CVE-2013-8685</td>
</tr>
</tbody>
</table>
C. BRUCERT ACTIVITIES IN 2015

1. Seminars / Conferences / Meetings / Visits

BruCERT attended and presented papers at various seminars, conferences and meetings related to the field of ICT security.

On 6th September 2015 until 10th September 2015, four (4) BruCERT delegates attended the Asia Pacific Computer Emergency Response Team (APCERT) and OIC-CERT Annual General Meeting (AGM) and Annual Conference 2015. Both events were done together in Kuala Lumpur, Malaysia, hosted by CyberSecurity Malaysia.

2. Awareness Activities

i. Cyber Battle: Capture the Flag

October 4 & 11, 2015

BruCERT organized Capture the Flag (CTF) competition with the support of AITI. The event was open to citizens and permanent residents of Brunei Darussalam aged 30 years and below. The publicity for the event include a press conference, newspaper ads, social media posts, and online contests through the use of Facebook and Instagram.

14 teams registered for the competition. An elimination round was held on 4 October 2015 at ITPSS to determine the top 10 teams that will compete in the actual event. The final session of the competition was held a week later on 11 October 2015. The top two (2) teams from the competition were selected to represent Brunei Darussalam at the Cyber SEA Games 2015 held in Jakarta, Indonesia, in November 2015.

ii. TechXpo 2015: BruCERT Carnival

Oct 22-25, 2015

BruCERT participated in the 4-day TechXpo 2015 organized by D’Sunlit at the Brunei International Convention Center (ICC). The objective of the participation in the expo was to spread IT security awareness to the public. Prior to the roadshow, BruCERT started advertising the upcoming carnival through social media and providing teasers on what can be expected.

BruCERT had a newly designed booth conducting a carnival with a few activities during the expo. The vibrant look and feel of the booth, the fun activities, and prizes were successful in attracting visitors. A quick survey showed that 90% of the visitors enjoyed their visit to the BruCERT Carnival.

The activities conducted were Password Challenge, Social Media Checkup, Dumpster Diving, and Think Before You Post.

D. CONCLUSION

In 2015, BruCERT observed an improvement in IT security response in both the public and government agencies. Even though incidents reported to BruCERT are still far less compared to other countries, this improvement gives a positive outcome to BruCERT. BruCERT will actively continue to improve its services as the national and government CERT. With the ongoing and upcoming initiative such as BruCERT road shows, security awareness to schools program, and publication of security awareness magazine, will better educate the community on the importance of information security and online safety.

This report also concludes the Honeypot finding for 2015. The is a continuous possible malicious attack or attempt to compromise MySQL database system (port 3306) and MSSQL Microsoft SQL.
Server database management system server (port 1433). Port 23 and 22 were constantly scanned for vulnerabilities followed by port 8080, 135, and 3128.

Egypt Computer Emergency Response Team
Status: Full Member

A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES

• Regular incident handling within the constituency.
• Malware analysis of various types of malware samples.
• Performing penetration testing on the Egypt’s critical infrastructure.
• Several other activities that are related to increasing the level of security in Egypt.

B. ACHIEVEMENTS

• Managed to prevent many incidents and mitigated the risk of several other critical incidents.
• Managed to analyze the effects of various malware samples and developed removal tools for the malwares affecting the constituency.
• Managed to patch many vulnerable critical systems within the constituency.

C. ABOUT THE ORGANIZATION / AGENCY

1. Introduction

The Egypt Computer Emergency Response Team (EG-CERT) was established in April 2009 as part of the National Telecom Regulatory Authority (NTRA).

2. Establishment

EG-CERT is charged with providing computer and information security incident response, support, defense and analysis against cyber attacks and collaboration with government, financial entities and any other critical information infrastructure sectors scoped to Egypt and our mission is to provide an early warning system against malware spreading and massive attacks against the Egyptian critical information infrastructure.

3. Resources

• Incident handling.
• Malware analysis.
• Penetration testing.
• Digital forensics.

4. Constituency

Egyptian National Telecom Regulatory Authority.

D. ACTIVITIES AND OPERATIONS

i. Events organized by the organization / agency

• Regional cyber security summit (RCSS).
• FIRST regional symposium for Arab and Africa region.

ii. Events involvement
Co-organized both events.

iii. Achievement
Both events were very successful and might be conducted annually.

E. OTHER INFORMATION
EG-CERT welcomed reports on computer security related incident. Any computer related security incident can be reported at:
Telephone: (202) 35344243 / (202) 35394444
Facsimile: (202) 35390444
Email: incident@egcert.eg
• Website: www.egcert.eg

Iran Computer Emergency Response Team
Status: Full Member

A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES
• Protecting Children in the Cyber Space.
• Creating CSIRTs in all the provinces of Iran.

B. ACHIEVEMENTS
• Creating a special CSIRT for child online protection.
• Training and awareness toward protecting children in the cyber space.
• Monitoring Botnets and vulnerabilities on national IP spaces.
• Developing Honeynet on national level.
• Training and empowerment in security field by conducting workshops.

C. ABOUT THE ORGANIZATION / AGENCY
The Computer Emergency Response Team Coordination Center.

1. Introduction
This Centre house the Assessing and Analysing Team, Monitoring, Data Gathering and Updating Team, Intrusion Detection and Incident Response Team, and Maintenance and Supporting Team. This Centre cooperates with the national security organizations in order to assure

17 A private computer network infected with malicious software and controlled as a group without the owners’ knowledge.
18 Internet protocol—a method by which data is sent between computers on the Internet.
the security of the cyber space and combating cyber crimes. In addition, the Centre receives vulnerability reports, software and hardware products security flaws from the whole country and provides IPs and ‘.ir’ domains security.

2. Establishment
This Centre is the single point in the Ministry of ICT for cyber space incident handling activities coordination.

3. Resources
This center is a vital subset of Information Technology Organization (ITO) that is supported by the Ministry of Information and Communication Technology (ICT) of Iran.

4. Constituency
This center is under the supervision of the Security Deputy of the Information Technology Organization -Ministry of ICT.

D. ACTIVITIES AND OPERATIONS

1. Events organized by the organization / agency
- The National Workshop on Security of Social Networks.
- Promotion of Security Awareness in the Executive Organizations Workshops in Iranian provinces.

2. Events involvement
- Attending OIC CERT face to face meeting.
- Attending APCERT Annual meeting

The following pictures are from the promotion of security awareness in executive organizations workshop in Iranian province.

E. 2017 PLANNED ACTIVITIES
- Developing Honeynet network (software and hardware).
- Security promotion at the user level via internet space.
- Computer Security Incident Response Teams Reinforcement.
- Provide training contents for Protecting Children in Cyber Space.

F. MORE INFORMATION
IrCERT welcomed reports on computer security related incident. Security incident can be reported to us at:
Telephone: (120) 00005624
Facsimile: (120) 15951122
Email: cert@certcc.ir
Website: www.ircert.com
A. HIGHLIGHTS OF 2016

1. MAJOR ACTIVITIES

16 March 2016       Participated in the APCERT Drill 2016
26 July 2016        Organised the OIC-CERT Cyber Drill 2016
1-10 August 2016    Organised Capacity Building Training under The Malaysian Technical Cooperation Program (MTCP).
27-30 September 2016 The OIC-CERT Technical Workshop in conjunction with CodeBali International Conference
17-19 October 2016  Organised the Cyber Security Malaysia- Awards, Conference & Exhibition (CSM-ACE) 2016
17 October 2016     Visited by Defense Space Agency (DSA), Nigeria
21-26 October 2016  Participated APCERT AGM & Annual Conference 2016, Tokyo, Japan
11-14 December 2016 Organised and participated OIC-CERT 8th AGM & Annual Conference 2016, Jeddah, Saudi Arabia

B. ABOUT ORGANIZATION / AGENCY

1. Introduction
CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Science, Technology and Innovation of Malaysia with a vision of being a globally recognized National Cyber Security and Specialist Centre by 2020.
CyberSecurity Malaysia provides specialized cyber security services as follows:

i. **Cyber Security Emergency Services:**
   - Security Incident Handling
   - Digital Forensic

ii. **Security Quality Management Services:**
   - Security Assurance
   - Information Security Certification Body

iii. **Cyber Security Professional Development and Outreach:**
   - Info Security Professional Development
   - Outreach

iv. **Cyber Security Strategic Engagement and Research**
   - Strategic Engagement Research

2. **Establishment**

The journey started with the formation of the Malaysian Computer Emergency Response Team (MyCERT) on 13 January 1997 as a unit under MIMOS Berhad. The Cabinet Meeting on 28 September 2005, through the Joint Cabinet Notes by the Ministry of Finance and Ministry of Science, Technology and Innovation No. H609/2005 agreed to establish the National ICT Security and Emergency Response Centre, now known as CyberSecurity Malaysia, as a national body to monitor the country’s e-Security aspect. The entity was a spin-off from MIMOS and become a separate agency incorporated as a Company Limited-by-Guarantee under the supervision of the Ministry of Science, Technology and Innovation.

The Malaysian Government gazetted the role of CyberSecurity Malaysia by Order of the Ministers of Federal Government Vol.53, No.13, dated 22 June 2009 (revised and gazetted on 26 June 2013 [P.U. (A) 184] as an agency that provides specialised cyber security services and continuously identifies possible areas that may be detrimental to national security and public safety.

3. **Resources**

i. **MyCERT**

MyCERT operates the *Cyber999 Help Centre*, providing emergency response on computer security and information breached related matters among which are cyber harassment, malware, intrusion, hack attempts.

ii. **Digital Forensics**

CyberSecurity Malaysia has strengthened the technology capabilities and resources which include offering full-fledged digital forensics investigations and examinations in the areas of audio and video forensics. With the aim of providing a clear understanding of the kind of services offered, the trademark “CyberCSI” was introduced to the stakeholders and to the public.

iii. **The National Vulnerability Assessment Centre**

The National Vulnerability Assessment Centre (MyVAC) aims to improve the security posture of the Critical National Information Infrastructure (CNII) through actual assessment or evaluation. This will improve the nation’s ability in defending against cyber threats and exploitation due...
to information systems and technology vulnerabilities.

iv. **Malaysian ICT Security Evaluation Facilities**

The Malaysian ICT Security Evaluation Facilities (MySEF) provides expertise in security evaluation of ICT products and systems. CyberSecurity Malaysia MySEF offers the following evaluation services:

- **Common Criteria (CC) Evaluation Service.**
- **ICT Product Security Assessment (IPSA) Service.**
- **Common Criteria (CC) Protection Profile (PP) evaluation service.**

MySEF is an accredited laboratory under the Laboratory Scheme Accreditation of Malaysia which meets the requirements of MS ISO/IEC 17025.

v. **Information Security Certification Body**

The Information Security Certification Body (ISCB) provides certification services based on international standards and guidelines. The certification services include:

- **Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme.**
- **CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) Scheme.**
- **Malaysia Trustmark for Private Sector (MTPS).**

vi. **Malaysian Common Criteria Evaluation & Certification Scheme**

The Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme is a systematic process of evaluating and certifying the security functionality of ICT products against defined criteria or standards. The missions are:

- To increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard.
- To build consumer's confidence towards Malaysian information security products.

vii. **Security Management & Best Practises**


This includes planning, developing, implementing and monitoring the ISMS processes and Business Continuity Management (BCM).

viii. **Industry Development**

One of the Industry Development initiatives is producing a Cyber Security Industry Directory, which provides a comprehensive listing of the Malaysian companies that offer cyber security related products and services. The Cyber Security Industry Directory connects the ICT security industry players with the business entities and general public on matters related to cyber security.

Another initiative is organising the CyberSecurity Malaysia - Awards, Conference and Exhibition (CSM-ACE). CSM-ACE is an annual public-private-partnership event, and the only 3-in-1 cyber security event in the country that
The OIC-CERT Annual Report 2016

consists of an Awards ceremony, a Conference, and an Exhibition.

ix. Government & International Engagement

The strategic engagement with the Malaysian Government is aimed at identifying and driving various government collaborations, working relations and activities to advocate the cyber security agendas.

On cross border initiatives, CyberSecurity Malaysia engaged in Multilateral Strategic Programmes.

CyberSecurity Malaysia is the co-founder of the Asia Pacific Computer Emergency Response Team (APCERT) and spearhead the formation of The Organisation of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT). Presently CyberSecurity Malaysia is the Steering Committee Member and Deputy Chair of the APCERT and the Permanent Secretariat of the OIC-CERT.

d. Cyber Security Research

CyberSecurity Malaysia developed, coordinate and stimulate continuous research activity in cyber security to ensure compliance with all applicable laws and regulations.

xi. Cyber Security Professional Development

CyberSecurity Malaysia strive to nurture the information security workforce with the required knowledge and skills by providing information security competency and capability courses as well as internationally recognised certifications. As a body entrusted to ensure the security of Malaysia's cyber space, the expertise and services are widely needed to provide training and consultancy on developing CERTs, ISMS, BCM, Wireless Technology, Penetration Testing, SCADA, and Digital Forensics.

xii. MyCyberSecurity Clinic

MyCyberSecurity Clinic is a trustworthy and credible entity for secure data handling and recovery. The clinic, as the specialist for data recovery and sanitization, plays a central role in protecting data while provides an opportunity to safely reuse and recycle the replaced or discarded digital storage devices.

4. Constituency

CyberSecurity Malaysia’s constituency is the Malaysian Internet Users. Incidents within Malaysia that are reported either by the Malaysian public or international organizations will be resolved by assisting the complainants on technical matters. If the incident involves international connection, then CyberSecurity Malaysia will request trusted parties in that
particular country or constituency to assist in resolving the security issues.

C. ACTIVITIES AND OPERATION

1. Events Organized by the Organization / Agency

CyberSecurity Malaysia actively participated in providing support in IT security events by attending various training, seminars/conferences and meetings. CyberSecurity Malaysia staffs contributed their competency to the following events:

a. Cyber Drills

CyberSecurity Malaysia was immensely involved in co-organizing the international drill called OIC-CERT Cyber Drill 2016 with the theme “Cyber Resiliency and Cooperation Against Cyber Threats”. The objective of the drill was to test the procedure and incident handling of participating organization. Six (6) teams from six (6) countries participated in the drill:

Malaysia CyberSecurity Malaysia
Morocco Oman National CERT
Nigeria Moroccan CERT
Oman Nigeria CS2
Tunisia Tunisia CERT
Pakistan PISA-CERT

Apart from the OIC-CERT Cyber Drill, CyberSecurity Malaysia also participated the APCERT Drill 2016.

b. The Malaysian Technical Cooperation Programme

The Malaysian Technical Cooperation Programme (MTCP) emphasizes on the development of human resources through the provision of trainings in various areas which are essential for a country’s development. These areas are the public administration, good governance, health services, education, agriculture, sustainable development, poverty alleviation, investment promotion, ICT and banking.

15 participants from the following OIC-CERT and ASEAN country members attended the training:

- Azerbaijan 2
- Egypt 1
- Indonesia 2
- Jordan 1
- Laos 2
- Morocco 2
- Nigeria 1
- Oman 2
- Pakistan 1
- Philippines 1
c. **Trainings**

Several workshops or hands-on training were conducted by CyberSecurity Malaysia in 2016. The training are:

- Network Security
- Log Analysis
- Information Security Management
- Intrusion Detection Prevention
- Incident Handling & Network Security

2. **Events involvement**

CyberSecurity Malaysia representatives had been invited to participate at various talks at international conferences and seminars. Some of the events were:

- Kaspersky Lab Partner Summit 2016, Bali, Indonesia
- Workshop on Enhancing Port Security Against Terrorism, Sarawak, Malaysia
- Strategic Collaboration in Digital Forensics Quality Management System, Information Technology Authority, Oman, Oman
- 3rd International Conference on Communication and Computer Engineering (ICOCOE 2016), Bandung, Indonesia
- International Conference on ICT in Education 2016, Perak, Malaysia
- Regional Workshop On Undergraduates and Radicalisation, Kuala Lumpur, Malaysia
- NITDA-CERTT Conference and Training, Abuja, Nigeria
- ICT Security Awareness Seminar, Ministry of Education Malaysia
- Amsterdam FIRST Technical Colloquium 2016, Amsterdam, Belanda
- The World Summit of the Information Society (WSIS) 2016, Geneva, Switzerland
- 5th Information Security Summit Spotlight on Cloud, Kuala Lumpur, Malaysia
- 4th International Conference on Information and Communication Technology, Bandung, Indonesia
- Cyber Security Awareness Program for Public Sector, Putrajaya
- 28th Annual FIRST Conference, Seoul, Korea
- ELM SME Seminar, Kuala Lumpur, Malaysia
- International Big Data Analytic Workshop 2016, Johor, Malaysia
- HIMSS Healthcare Cyber Security Symposium 2016, Bangkok, Thailand
- 10th European Conference on Information Systems Management (ECISM), Portugal
- IACSP ASEAN Security Awards & Symposium 2016, Kuala Lumpur
- CODEBALI International Conference, Indonesia
- APT CyberSecurity Forum 7, Cambodia
A. HIGHLIGHTS OF 2016

1. MAJOR ACTIVITIES
   - Development of Cyber-Warriors Roadmap for Defence Space Agency - 2016
   - Development of Nigeria ICT Strategic Roadmap for the Federal Ministry of Communications - 2016
   - Editing and Reviewing of the Nigeria National ICT Strategic Plan for Federal Ministry of Communications - 2016
   - Development of National Information Technology Development Agency (NITDA) IT Strategy and Implementation Plan
   - Resource at the 4 Days Africa Information & Communication Technologies Alliance (AfICTA) Summit, Windhoek, Namibia - 2016
   - Resource Economic Community of West African States (ECOWAS) – ECOWAS Wide-Area Network (ECOWAN) Market Analysis and Business Model validation
   - Resource to the 2016 West Africa Convergence Conference (WACC) 2016, Lagos, Nigeria
   - Resource to HackJos 2016, Jos, Nigeria
   - Resource to the International Conference on Information and Communication Technology and Its Applications (ICTA 2016) Federal University of Technology, Minna, Niger State, Nigeria

D. 2017 PLANNED ACTIVITIES
   - National Cyber Drill (X-Maya): 7 – 9 March 2017
   - CSM-ACE 2017: 9 – 12 October 2017

E. MORE INFORMATION
   CyberSecurity Malaysia welcomed reports on computer security related incident. Any computer related security incident can be reported to us at:
   Telephone: (603) 89926888
   Facsimile: (603) 89926841
   Email: secretariat@oic-cert.org
   - Website: www.cybersecurity.my
• Resource to the Communication Sector 2016 Retreat, Ibadan, Nigeria
• Resource to the West-Africa Telecoms Summit and Exposition 2016, Accra, Ghana
• Resource to eNigeria 2016 Conference
• Nigeria Digital Innovation Conference 2016, Bayero University Kano, Nigeria
• Resource to the Upgrade of Virtual Library - 2015, CERT.ng Bandwidth Renewal (2015) and Virtual Library Bandwidth Renewal - 2015

2. Achievements
• Delivered the Nigeria ICT Roadmap to the Honourable Minister Federal Ministry Of Communications (FMOC)
• Delivered the Roadmap For The Development Of Cyber-Warriors 2017-2022 to the Defence Space Agency (DSA)
• Delivered a 3-Day Cyber Security Workshop on Cyber Security, Cyber-Warfare & Cyber-Forensics at the Nigeria Army School of Signals - 2016
• Facilitated the 2016 Computer Professionals Registration Council of Nigeria (CPRN) Executive Training programme
• Successful interventions at the National Council on Communications Technology
• Successful visit of DSA delegation to Malaysia in October 2016.

B. ABOUT THE ORGANIZATION
1. Introduction
Consultancy Support Services Limited (CS2) is a Cyber Security, e-Library and ICT Policy Consultancy Firm.

2. Establishment
CS2 was Incorporated on 13 February, 2002.

3. Resources

4. Constituency
Public and Private sectors as well as Academia, Media and Non-Governmental Organisations in Nigeria, African and across the globe.

C. ACTIVITIES AND OPERATIONS
1. Events organized by the organization / agency
• APCERT Cyber Drill 2016.
• OIC-CERT Cyber Drill 2016.
• Autopsy Training.

2. Events involvement
• Nigeria Computer Society (NCS).
• Observer Research Foundation (ORF).
• Cyber Security Expert Association of Nigeria (CSEAN).
• Internet Corporation for Assigned Names and Numbers (ICANN).
• African Information and Communication Technologies Alliance (AfICTA)
3. Achievement / Awards

Nigeria Computer Society (NCS)
Federal University of Technology, Minna
CyberSecurity Malaysia
African Information & Communication Technologies Alliance (AfICTA)
Information Technology Association of Nigeria (ITAN)
Greater Height Academy
Diamonds & Dunes Resources Ltd.
African Network Operators Group (AfNOG)

4. Profile Summary

A Cyber Security, e-Library and Policy Consultancy Firm

Mission Statement: “To collaborate with, and empower, our clients by leveraging knowledge.”

Motto: Collaboration. Empowerment.

Our collaborative culture means that we have linkages from around the world that provide the need support required at short notice.

CS2 is peopled by a team of “Resourceful Managers” with strong bias towards the generation, sharing and utilisation of knowledge.

A flat core firm (CS2) that endeavours to empower its people to spin-off specialized firms, which they will operate as entrepreneurs.
D. 2017 PLANNED ACTIVITIES

i. Increased involvement in OIC-CERT, AfICTA, GCSC, ICANN, NCS, CSEAN and related activities.

ii. Implement in-house a cyber forensics capacity development program.

iii. Kickstart the development of Podcast and Vodcast initiatives.

iv. Implement Online testing and certification facilities.

v. Develop multimedia content including tutorials for eLibraries.

vi. Give services in support of Military-Civilian, Law Enforcement and related cyber security initiatives.

vii. Collaborate with the Government Inter-Agency Committee on the implementation of Cybersecurity measures.

viii. Support the following national initiatives:

- Implementation of a Nigeria ICT Roadmap.
- Harmonisation, standardisation and seamless interoperability of national identity systems as well as evolving a Business Model/ Plan defining the rules of engagement governing access of Foundation Identity by Agencies/ organisations providing Functional national identity.
- Development of national frameworks and guidelines to protect Nigerian IT systems from deliberate attack from internal and/ or external forces.
- Implementation of a Nigeria "e"Trustmark to validate the e-Business activates, website security, Apps, Hardware, software, legality and good "e"-Business behaviour.
- Establishment of a cadre of Information Security Professionals with direct reporting line to the Chief Executive of their assigned MDA as well as Office of Head of Information Security for the Nation at NITDA.
- Establishment of local Cybersecurity Certification Authority with International credibility to increase number of Cybersecurity professionals by leveraging the Global Accredited Cybersecurity Education (ACE) Scheme and other partnerships.
- Develop of digital literacy and e-inclusion schemes for under-served communities, including women and girls.
- Increase in compliance and adoption of IPv6 standards.
- Strengthening of ICT departments in our Higher Education Institutions (HEIs).
- Development of a blueprint of common services, policies, standards, procedures and technical components that guide MDAs on IT investment.
a) **Overview: Cybersecurity, Policy, Capacity Building, Consulting**

- CERTT.ng Fusion Centre
- CyFy India 2016
- Nigeria Army School of Signals, Forensics Training 2016
- Cybersecurity Management Training
- Defence Space Agency visit to CyberSecurity Malaysia
- Awareness Activities @ Hillside School 2016
- #ICANN57 Stepdown Meeting

b) **Cybersecurity & Digital Forensics Training**

- Training in Malaysia
- Training in USA
- Training @ CS2 Premises
- Training @ CS2 Premises
- Training @ CS2 Premises
- Training @ CS2 Premises
- Live online Cyber Drill @ CS2 Premises
- Training @ CS2 Premises
c) Provisioning of Digital Forensics Tools

- Forensic Recovery of Evidence Device (FRED)
- Assorted Digital Forensics Tools
- Digital Forensics Lab
- Universal Forensic Extraction Device (UFED)
- Forensic Computer
- Forensic Cable Kit
- Forensic Ultra Kit
- Forensic Write Blockers

d) Capacity Building

- Awareness
- Training
- Facility Tour: CyberSecurity Malaysia
- Facility Tour: Malaysia Space Agency
- Conferences
- Seminars
- Provisioning
- Online Testing
- Partner Development
- Mentoring
e) Cyber Drills

- OIC-CERT Cyber Drill
- OIC-CERT Cyber Drill
- OIC-CERT Cyber Drill
- APCERT Cyber Drill
- APCERT Cyber Drill
- International Interactions
- Computer Professionals Registration Council Training

f) Digitization

- E-Library
- Virtual Library
- Library Automation
- Digital Archiving
- Content Creation
- Podcasting
- VodCasting
- Broadcasting
g) Consulting

Vendor Assessment & Supervision

Project Management

Specifications Development, Compliance, Supervision & Quality Assurance

Event Management

Regional Engagements / ECOWAS EOWAN

Community Information Resource Centers

Community Radio

Computer Ready Smart Building

h) Policy Development

National ICT Policy

Operational Policy

Strategic Planning

Standards

Framework

Guidelines

Roadmap

Masterplan
i) Partner Ecosystem

aeCERT
AfricaCERT
APCERT
BCN
Center for Cybersecurity Nasarawa
CERRT.ng
CISCO
CSEAN

CYAN
Cyber Institute
CyberSecurity Malaysia
Digital Intelligence

Oman CERT
DSA
EFCC
FUT Minna

Huawei
IDSIRTII/CC
IMPACT
Microsoft

ngCERT
Nigeria Army School of Signals
NITDA

OIC-CERT
Pakistan Information Security Association
TBP
Tunisia CERT
A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES

- National drill for Oman government and Critical National infrastructure (CNIs) entities
- Regional Cyber Drill for Arab Region
- Regional Cyber Security Summit
- National Cyber Security Campaign (blackmailing campaign)

B. ACHIEVEMENTS

National Level:

a) Technical achievements:

- Discovered and handled 16,118 real cyber security attempted attacks and 685 malware infections through OCERT Intelligence gathering System resulted from the analysis of millions of attempted attacks against Oman’s cyber space.
- Successfully and comprehensively handled 1744 real cyber security incidents reported by the government, critical national infrastructures (CNIs) and public.
- Published 486 security threat notification and alerts “TNAS” on cyber security threats to OCERT constituents.
- Conducted 15 comprehensive Security Vulnerability Assessments, Penetration Testing and Verification Tests for government organizations and CNII.
- Handled 39 digital forensics cases with 141 evidence devices including computers, mobile, phones, external hard disk and USBs resulted from cyber crime cases in Oman.
- OCERT malware analysis team discovered a vulnerability in Apple system (IOS 10.1, macOS Sierra 10 ), the vulnerability enables the attacker to destroy the victim’s system and as a result, the victim lose all data. Apple announced the vulnerability news and the team's effort in its website.
b) Cyber Security Training and Awareness:

i. Unified Government Information Security Campaign “WAAY”:
   - 93 cyber security awareness sessions were conducted for Information Technology Authority employees.
   - 20 cyber security awareness sessions were conducted to government entities, attended by 1030 people.
   - 2 top management cyber security awareness sessions were conducted.

ii. National Cyber Security Campaign:
   - Conducted an online cybersecurity awareness campaign on cyber blackmailing.
   - Published three online public alerts on Ransomware, Pokémon go and phishing.

iii. Child Online Protection (COP):
   - Participated in the Kids Event for 2 days.
   - Conducted 14 sessions on Child Online Protection for 10 schools.
   - Participated in Ministry of health Awareness day “raising children and adolescents in the digital world”, attended by 100 people.
   - Conducted 9 sessions on Child Online Protection for Information Technology Authority employees.

iv. Specialized Cybersecurity Training:
   - Conducted 4 specialized training on:
     - Technical Security Audit training, attended by 15 people
     - Web security training attended by 18 people
     - Certified Chief Information Security Officer Program attended by 13 people.

v. National Cyber Drill
   Organized a national cyber drill for CNI with the participation of 12 teams (105 players) from 28 different organization.

vi. Ambassador Program:
   - 15 new cyber security ambassadors joined the OCERT ambassadors program (total 589 ambassadors).
• Conducted two technical training on “online investigation”, attended by 41 cyber security ambassadors.

• Conducted hacking competition “Catch Me If You Can” for FOSS group at Sultan Qaboos University for 48 hours.
  - Total Attacks: 17137
  - Total Users: 95

• 12 cyber security awareness sessions were delivered by the ambassadors in different regions of Oman.

• Development of 35 cyber security awareness materials by OCERT ambassadors.

vii. Government Cyber Security Offices

Assisted 10 government entities in establishing their cyber security offices.

viii. Learning Management System

• Activation of 300 online users from different government and CNIS entities.

• Over 45 cyber security materials have been published.

Regional Level:

Gulf Cooperation Council

Drafted a Gulf Cooperation Council (GCC) Cyber Security Strategy and Road map for GCC countries approved by Ministers of ICTs of GCC.

Arab Region:

ITU – Arab Regional Cyber Security Center achievements

• Launching of Arab Regional Cybersecurity Centre (ARCC) website www.arcc.om

• Organized the Annual Regional Cyber Security Summit 2016 in Egypt, with the participation of 35 speakers and 450 delegates from 39 Arab and regional countries.

• Organized a regional cyber drill for Arab CERTs in Tunisia with the participation of 12 teams from 12 different Arab countries.

• Conducted 2 CIRT Trainings, Technical and Management Track for Arab region in Tunisia.

• Participated in the Cyber Security Seminar- Fourth Edition in Morocco, organized by the Ministry of Defense and ma-CERT.

• Conducted the Arab CERTs high level meeting in Tunisia.

• Participated in “Managing Justice Electronically” seminar in United Arab Emirates (UAE).

• Conducted the third Arab meeting in Egypt.

• Participated as Supporting partner in FIRST Arabic and African Regional Symposium in Egypt.
International Level:
- Participated in the OIC-CERT Annual General Meeting & Conference in Saudi Arabia.
- Managed the MOU signing between OIC –CERT and (ISC) 2.
- Participated in CodeBali Conference in Indonesia.
- Participated in the OIC CERT cyber security drill 2016.
- Participated in APCERT cyber drill “An Evolving Threat and Financial Fraud”.
- Signed MoU with Dell Secure Works.
- Signed membership agreement of CAMP initiative under KISA (Korea Internet Security Center).

C. ABOUT ORGANIZATION / AGENCY

1. Introduction
The Oman National Computer Emergency Readiness Team (OCERT) was established to serve as trusted focal point of contact of any ICT security incidents in the Sultanate of Oman focusing on cyber safety and security, capacity building and promoting cyber security awareness and to serve the public and private sector organizations, CNI as well as individuals.

2. Establishment
April 2010.

3. Resources
- Cyber security training and awareness team.
- Threat and risk management team.
- Incident response team.
- Vulnerability assessment and penetration test team.
- Digital forensics team.
- Alliances and cooperation team.
- ITU-Arab Regional cyber security center team.

4. Constituency
- Public ICT users in Oman.
- Government entities and Authorities.
- Critical National Infrastructure sector.

D. 2017 PLANNED ACTIVITIES
- Regional Cyber Drill – (5th -9th March 2017).
- Regional Cyber Security Summit (October 2017).
- National Cyber Drill (December 2017).
- Child online protection (COP) National strategic framework.
- National Campaign.

E. MORE INFORMATION
For more photos, kindly visit below URL’s

i. OCERT Media Center

ii. Arab Regional Cyber Security Center
- http://www.arcc.om/

OCERT welcomed reports on computer related security incidents. Incidents can be reported at:

Telephone: (+968) 24166828
Facsimile: (+968) 24166818
- Website: www.cert.gov.om/
A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES

i. Classification of data: A national project with the objective of setting up a data classification framework, financed by Tunisia Computer Emergency Response Team (TunCERT). The project has been launched since November 2015. The classification of data is a key element in the protection of data.

ii. Implementation of the cycles of training skills in the field of computer security.

iii. Sectorial CERTs: The objective is to encourage the creation of a nucleus of a sectoral CERT.

iv. Saher-Entreprise project: Activate the interaction of TunCERT with its partners at the level of the supervision of the cyber space.

B. ACHIEVEMENTS

All projects are running.

C. ABOUT THE ORGANIZATION

1. Introduction

The National Agency for Computer Security (NACS) through TunCERT carries out the necessary general supervision on the computer systems and networks to the diversified public and private organizations.

2. Establishment

TunCERT

3. Resources

69 employees: 22 engineers; 9 analysts, 9 technicians and 29 administrative staff.

4. Constituency

TunCERT constituency from 2011.
D. ACTIVITIES AND OPERATIONS

1. Events organized by the organization / agency
   - Cyber Security Day.
   - National Cyber Drill.

2. Events involvement
   Regional cyber drill.

3. Achievement
   Progress of the documentation of Cyber Early Warning System (CEWS) phase & testing phase.

E. MORE INFORMATION

TunCERT welcomed reports on computer security related incident security. Any computer related security incident can be reported to us at:

Telephone: (216) 71843200 / (216) 97446170
Facsimile: (216) 71846363
Email: tuncert@ansi.tn
- Website: www.ansi.tn

---

A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES
- Conducted 268 information security awareness sessions and workshops all around United Arab Emirates (UAE).
- Issued 46 security advisories.
- Handled and reported 1054 security incidents.
- Participate in the Safer Internet Day 2016.
- Launch an awareness campaign about Cyber Blackmailing.

B. ACHIEVEMENTS

The launching of a new website for the UAE Computer Emergency Response Team (acCERT) mascot "Salim". The site contains videos, stories, and other awareness materials for different ages. In addition, the website was approved to be the hub for all the awareness materials developed by any entity within the UAE. "Salim becomes the national mascot for Cyber Security in UAE."

Establishing an Information Security Awareness (ISA) committee, that brings together 38 government and private entities to work on awareness projects and initiatives and unify the efforts.

C. ABOUT THE ORGANIZATION / AGENCY

1. Introduction
aeCERT was established to improve the standards and practices of information security. The aim is to protect the IT infrastructure in the UAE from risks and violations in conformity with the UAE Telecommunications Regulatory Authority (TRA) strategy is aimed at supporting and ensuring a safer cyber space for the residents of the UAE, both nationals and expatriates.

2. Establishment

aeCERT was established by the Decree 5/89 of 2008 issued by the Ministerial Council for Services.

3. Resources

aeCERT services include:
- Monitoring and Response.
- Security Quality Services.
- Awareness and Education.

4. Constituency

aeCERT services cover:
- Governmental and Semi-Governmental entities.
- Some of the private entities (especially banks).
- the Public.

D. ACTIVITIES AND OPERATIONS

1. Events organized by the organization / agency
- BlackHat Abu Dhabi 2012
- FireEye Security Summit 2015

2. Events involvement
- GISEC

3. Achievement

- Launching a new website for aeCERT mascot "Salim", that contains videos, stories, and other awareness materials for different ages. In addition, the website was approved to be the hub for all the awareness materials that any entity within the UAE makes, with “Salim” becoming the national character for Cyber Security in UAE.
- Establishing the Information Security Awareness (ISA) committee, that brings together 38 government and private entities to work on awareness projects and initiatives and unify the efforts.

E. 2017 PLANNED ACTIVITIES

A campaign about Social Engineering - Creating the Awareness Management System (AMS) that manages the whole process of creating an awareness program within any organization intelligently.

F. MORE INFORMATION

aeCERT welcomed reports on computer security related incident. Any computer related security incident can be reported at:

Telephone: 800 12 (Toll Free)
Facsimile: (971) 2 6118209
Email: info@tra.gov.ae
Website: www.aecert.ae

21 http://www.blackhat.com/ad-12/
22 https://www2.fireeye.com/FireEye-Summit-Dubai-UAE-EMEA-LP.html
A. HIGHLIGHTS OF 2016

MAJOR ACTIVITIES

- Malware Incident Investigations.
- Research in LTE Security and Privacy:
  - Teaching Information Security related subjects.
- Training Information Security Courses.
- Supervising number of Information Security projects.

B. ACHIEVEMENTS

- Malware Incident has been analysed and report has been delivered to the client.
- A variant of Ransom Virus have been analysed and encrypted data of has been recovered.
- One research paper (LTE user privacy) has been accepted to be published in the International Journal of Computer Networks and Information Security.

C. ABOUT THE ORGANIZATION / AGENCY

1. Introduction
Smart Security Solutions Company (SMARTSEC) is the first company in Yemen to provide Information Security training, consultancy, and Information Security research.

2. Establishment
SMARTSEC was established on October 2010 by Dr.Abdulraman Muthana and a group of Information security professionals.

3. Resources
SMARTSEC includes a number of Information security professionals and researchers. The company has 2 training labs equipped with the necessary facilities in addition to a research lab.

4. Constituency
Information Security fields.

D. ACTIVITIES AND OPERATIONS

1. Events organized by the organization / agency
- Information Security Training.
- Information Security Awareness Programs.
- Information Security Consultantancy.

2. Events involvement
- Information Security Training.
- Information Security Awareness Programs.

3. Achievement
- Training a number of Information Security courses.
- A number of Information Security Awareness programs.
- Malware Incident Investigation reports.

E. 2017 PLANNED ACTIVITIES

Malware Analysis (more specifically Ransomware Viruses).