OIC-CERT
Computer Emergency Response Team

OIC-CERT 2021
ANNUAL REPORT

Organization of the Islamic Cooperation
Computer Emergency Response Team

This page is intentionally left blank

Title	The OIC-CERT Annual Report 2021
Ref	OICCERT-4-RPT-01-ANNUALRPT-v1
Date	6 Jun 2022

The OIC-CERT Permanent Secretariat

CyberSecurity Malaysia
Level 7 Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor
MALAYSIA

Tel: +60 (0) 3 8800 7999
Fax: +60 (0) 3 8008 7000
https://www.oic-cert.org

Copyright Statement

Acronyms

AI	Artificial Intelligence
AI C4	AI Cloud Service Compliance Criteria Catalogue
AITI	Authority for Info-communications Technology Industry (BN)
APAC	Asia Pacific
ARCC	Arab Regional Cyber Security Centre (OM)
BCC	Bangladesh Computer Council
BSI	The British Standards Institution
CA	Certifying Authority (BD)
CCA	Controlling of Certifying Authority (BD)
CCW	Cyber Crime Wing (PK)
CEH	Certified Ethical Hacker Certificate
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CNII	Critical National Information Infrastructure
CIS	Commonwealth of Independent States
CISSP	Certified Information Systems Security Professional Certification
CSB	Cyber Security Brunei
CSC	Cyber Security Council (AE)
CSIRT	Computer Security Incident Response Teams
CSM-ACE	Cyber Security Malaysia - Awards, Conference & Exhibition
CTF	Capture the Flag
DDOS	Distributed Denial of Service Attack
DG	Director General (PK)
EGNC	E-Government National Centre (BN)
FIA	Federal Investigation Agency (PK)
FIRST	Forum in Incident Response and Security Teams
GCC	Gulf Cooperation Council
GCI	Global Cybersecurity Index (ITU)
ICT	Information and Communication Technology
ICTA	Information and Communication Technologies Authority (TR)
IP	Internet Protocol address
ISG	Institute of Higher Management (TN)
IT	Information Technology
ITU	International Telecommunication Union
ITU-ARCC	ITU Arab Regional Cyber Security Centre
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Providers
KPK	Khyber Pakhtunkhwa (PK)
LEA	Law Enforcement Agency
MEA	Middle East & Africa
MOOC	Massive Open Online Courses
MoU	Memorandum of Understanding
MTCIT	Ministry of Transport, Communications, and Information Technology (OM)
MTCP	Malaysian Technical Cooperation Programme
My5G	5G Security Test Lab (MY)
NATO	North Atlantic Treaty Organization
NCA	National Cybersecurity Authority (SA)
NCCA	National Cyber and Crypto Agency (ID)
NCSI	National Cyber Security Index (BD)
OIC	Organization of the Islamic Cooperation
OIC-CERT	Organization of the Islamic Cooperation – Computer Emergency Response Team
OSCE	Organization for Security and Co-operation in Europe
PKI	Public Key Infrastructure
PSIRT	Product Security Incident Response Team
SIEM	Security Information & Event Management
SME	Small and Medium Enterprise
SOC	Security Operation Centre
SUE	State Unitary Enterprise (UZ)
TDRA	The Telecommunications and Digital Government Regulatory Authority (AE)
TI	Trusted Introducer (TR)
UN	The United Nation

The OIC-CERT

The Organization of the Islamic Cooperation – Computer Emergency Response Team

The OIC-CERT was established through the Organization of the Islamic Cooperation (**OIC**) Resolution No 3/35-INF *Collaboration of Computer Emergency Response Team* (**CERT**) *Among the OIC Member Countries*. It was passed during the 35th Session of the Council of Foreign Ministers of the OIC in Kampala Uganda on 18-20 June 2008.

In 2009 through the Resolution No 2/36-INF *Granting the Organization of the Islamic Cooperation – Computer Emergency Response Team an Affiliated Institution Status*, the OIC-CERT became an affiliate institution of the OIC during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic on 23-25 May 2009

Vision

Envisioning the OIC-CERT to be a leading cybersecurity platform to make the global cyberspace safe

Mission

A platform to develop cybersecurity capabilities to mitigate cyber threats by leveraging on global collaboration

Objectives

- Strengthening the relationship of CERTs among the OIC member countries, OIC-CERT partners, and other stakeholders in the OIC community
- Encouraging the sharing of cybersecurity experience and information
- Preventing and reducing cyber-crimes by harmonizing cybersecurity policies, laws, and regulations
- Building cybersecurity capabilities and awareness amongst the OIC-CERT member countries
- Promoting collaborative research, development, and innovation in cybersecurity
- Promoting global cooperation with international cybersecurity organizations
- Assisting the OIC-CERT member countries in establishing and developing their national CERTs

Membership

As of Dec 2021, the OIC-CERT has a network and strategic collaboration with 55 members from 27 OIC countries. This alliance is further supported through the presence of 6 Commercial Members, 5 Professional Members, 2 Fellow Member, 1 Affiliate Member, and 1 Honorary Member

Full Members

These are CERTs, Computer Security Incident Response Teams (**CSIRT**s) or similar entities that are located and/ or having the primary function within the jurisdiction of the OIC-CERT member countries that is wholly or partly owned by the government with the authority to represent the country's interest

1 **Azerbaijan** - Azerbaijan Government CERT (CERT.GOV.AZ)

2 **Bangladesh** - Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
3 **Brunei Darussalam** - Brunei Computer Emergency Response Team (BruCERT)
4 **Cote D'Ivoire** - Cote D'Ivoire Computer Emergency Response Team (CI-CERT)
5 **Egypt** - Egypt Computer Emergency Response Team (EG-CERT)
6 **Indonesia** - Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Centre (Id-SIRTII/CC)
7 **Iran** - Iran Computer Emergency Response Team (IRCERT)
8 **Jordan** - Jordan Computer Emergency Response Team (JO-CERT)
9 **Kazakhstan** - Kazakhstan Computer Emergency Response Team (KZ-CERT)
10 **Kuwait** - Kuwait National Cyber Security Centre (NCSC-KW)
11 **Kyrgyzstan** - Computer Emergency Response Team of Kyrgyz Republic (CERT-KG)
12 **Libya** - Libyan Computer Emergency Response Team (Libya-CERT)
13 **Malaysia** - CyberSecurity Malaysia
14 **Morocco** - Moroccan Computer Emergency Response Team (maCERT)
15 **Nigeria** - Consultancy Support Service Limited (CS2)
16 **Oman** - Oman National Computer Emergency Response Team (OCERT)
17 **Pakistan** – National Response Centre for Cyber Crimes (NR3C)
18 **Qatar** - Qatar Computer Emergency Response Team (Q-CERT)
19 **Saudi Arabia** - Saudi Arabia Computer Emergency Response Team (CERT-SA)
20 **Somalia** - Somalia Computer Emergency Response Team (SomCERT)
21 **Sudan** - Sudan Computer Emergency Response Team (SudanCERT)
22 **Syria** - National Agency for Network Services
23 **Tunisia** - National Agency for Computer Security (tunCERT)
24 **Turkey** - National Cyber Security Incident Response Team (TR-CERT)
25 **United Arab Emirates** - UAE Computer Emergency Response Team (aeCERT)
26 **Uzbekistan** - Uzbekistan Computer Emergency Response Team (UzCERT)

General Members

These are other related government organizations, non- governmental organizations or academia that deals with cybersecurity matters. However, these entities do not have the authority to represent the country's interest

1 **Bangladesh**
- BangladeshCERT
- Bangladesh Computer Emergency Response Team (bdCERT)

2 **Iran**
- Isfahan University of Technology Computer Emergency Response Team (IUTcert)
- Amirkabir University of Technology Computer Emergency Response Team (AUTcert)
- Sharif University of Technology Computer Emergency Response Team (SharifCert)
- Shiraz University ICT Center (SUcert)
- Maher Center
- APA Ferdowsi University of Mashhad CERT (APA-FUMcert)

- APA University Bojnord CERT (APA-UBCERT)

3 **Kazakhstan**
- Center for Analysis and Investigation of Cyber-Attacks (CAICA)

4 **Kyrgyzstan**
- Computer Emergency Response Team (cert.ict kg)

5 **Malaysia**
- Universiti Teknikal Malaysia Melaka (UTeM)

6 **Pakistan**
- Pakistan Information Security Association (PISA-CERT)

7 **Turkey**
- Turkey Cyber Security Incident Response Team (CSIRT)

8 **Uganda**
- Uganda Computer Emergency Response Team (UG-CERT)

Affiliate Members

These are not-for-profit organizations that deals with cybersecurity matters from non OIC-CERT member countries

The United States
- Team Cymru

Commercial Members

These are industrial or business organizations that deals with cyber security matters from the OIC and non-OIC member countries

1 South Korea
- Duzon

2 Singapore
- CERT-GIB

3 United Arab Emirates
- Huawei (HWT)

4 Oman
- Insight Security Operation Centre (**SOC**)

5 Malaysia
- Serba Dinamik Group Berhad

6 Turkey
- Turkcell Cyber Defence Center

Professional Members

1 Malaysia
- Hatim Mohammad Tahir
- Prof. Dr. Rabiah Ahmad (Universiti Teknikal Malaysia Melaka)
- Abdul Fattah Mohamed Yatim (Teknimuda (M) Sdn Bhd)
- Dr. Sofia Najwa Binti Ramli (Universiti Tun Hussein Onn)

2 Yemen
- Dr. Abdulrahman Ahmad Abdul Muthana (Smart Security Solutions)

Fellow Members

These are individual who are considered as co-founders of the OIC-CERT and have actively represent their organization as an OIC-CERT member for a minimum period of 5 years

1 Prof. Nabil Sahli - National Agency for Computer Security

2 Assoc. Prof. Colonel (R) Dato' Ts. Dr. Husin Bin Jazri - Serba Dinamik Group Berhad

Honorary Members

Individuals or organizations who has demonstrated extraordinary contribution, support, and exemplary leadership to the OIC-CERT

Saudi Arabia

The Organization of the Islamic Cooperation

CONTENT

AZERBAIJAN

Azerbaijan Government CERT (CERT.GOV.AZ)

(Full Member)

HIGHLIGHTS OF 2021

- Recorded and handled 4674 incidents
- Provided 205 audit/ penetration test for required government bodies
- Updated some bugs and mailing issues in the Organization of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) Membership Portal
- Agreement to have new languages to be integrated into SIM3 model
- Prepared Azerbaijani version of SIM3 model
- Portals Interface Blacklist updated
- Signed a Memorandum of Understanding (**MoU**) to manage a Cyber Hygiene pilot project for 10,000 local users

- Conduct training for all government organizations in Azerbaijan on cybersecurity
- Published 2 series of Information Security Journal for government bodies and distributed for free

- Participated in various local and international conferences, meetings, and courses such as the OIC-CERT, Forum in Incident Response and Security Teams (**FIRST**), CyberTech, North Atlantic Treaty Organization (**NATO**), and Organization for Security and Co-operation in Europe (**OSCE**)

Summary of Major Activities

Incident Response

CERT.GOV.AZ assisted the system administrators in handling the technical and organizational aspects of the cyber incidents. The agency will aid or advice with respect to the following aspects of the incident management

Incident Triage

- investigating whether indeed an incident occurred
- determining the extent of the incident

Incident Coordination

- determining the initial cause of the incident (the vulnerabilities)
- facilitating contact with other sites which may be involved
- making reports to other Computer Emergency Response Team (**CERT**)/ Computer Security Incident Response Teams (**CSIRT**)
- composing announcements to users, when applicable

Incident Resolution

- removing the vulnerabilities
- liquidation of consequences of the incident
- evaluating possible additional actions while considering the cost and risk
- aid in evidence collection and data interpretation when needed
- CERT.GOV.AZ collects statistics concerning incidents and will notify the community if required to assist in protecting against known cyber-attacks

Proactive Activities

Information services

The CERT.GOV.AZ publishes advisories for events and incidents that are considered of special importance to the users in the constituency. The information is disseminated via various channels (web, Really Simple Syndication (RSS) feeds, mailing lists etc)

Training services

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

ABOUT CERT.GOV.AZ

Introduction

CERT.GOV.AZ helps in computer and network security incident handling and provides incident coordination functions for all incidents involving digital systems and networks located in the state sector of the Azerbaijan Republic

RFC-2350 - *http://cert.gov.az/en/pages4/rfc-2350.html*

Promo - *https://www.youtube.com/watch?v=tYqPc-lzd54*

Host Organisation

Special State Protection Service of Azerbaijan

Special Communication & Information Security State Agency Azerbaijan Government CERT (CERT.GOV.AZ)

Establishment

20 Apr 2008

Resources

Government

Constituency

The constituency of CERT.GOV.AZ – all networks and the users allocated in state sector of the Azerbaijan Republic

Contacts

Representative mail. *rep@cert.gov.az*
Group mail. *team@cert.gov.az*
General use. *info@cert.gov.az*
Tel. +994 12 435 28 25
Fax. +994 12 435 28 31.

PLANS FOR 2022

- Publish a national sandbox platform for the users
- Prepare an Arabic version of the SIM3 model
- Continue collaboration with the CERTs internationally

BANGLADESH

BGD e-GOV CIRT

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- BGD e-GOV CIRT has successfully organized the National Cyber Drill, Inter University Cyber Drill, and Cyber Drill for Financial organizations
- Bangladesh has improved its rank to 32nd among 160 countries on the National Cyber Security Index (**NCSI**) in 2021
- 873 cybersecurity incidents registered in the tracking system

Achievements

- BGD e-GOV CIRT has successfully participated in the *OIC-CERT Cybersecurity Drill 2021* and achieved 2nd position (OM)
- BGD e-GOV CIRT published the *Cyber Threat Landscape Report 2021*
- *Bangladesh Cyber Security Strategy 2021-2025* has been released
- *IT Audit Manual v1.0* is published

ABOUT ORGANIZATION/ AGENCY

Introduction

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CERT of Bangladesh (N-CERT). Currently the responsibilities include receiving, reviewing, and responding to computer security incidents and activities. Under the Government of People's Republic of Bangladesh, BGD e-GOV CIRT reviews and takes the necessary measures to resolve the issue with broad cybersecurity ramifications, conducts research and development, and provides guidance on security vulnerabilities. BGD e-GOV CIRT also works with various government units, Critical Information Infrastructures (**CII**), financial organizations, law enforcement agencies, academia, and civil society to help to improve the cybersecurity defence of Bangladesh

Establishment

The process to establish BGD e-GOV CIRT started in November 2014 and the team starts operation in February 2016

Resources

Currently there are 16 people working in BGD e-GOV CIRT

Constituency

Constituencies of BGD e-GOV CIRT are all the governmental, semi-governmental, autonomous bodies, ministries, and institutions of Bangladesh. Currently BGD e-GOV CIRT is acting as National CERT of

Bangladesh with a mandate to serve the whole of Bangladesh

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

National Cyber Drill organizing team

- Arranged the *National Cyber Drill 2021*
- Arranged the *Inter University Cyber Drill 2021*
- Arranged the *Financial Cyber Drill 2021*
- A day long workshop on BGD e-GOV CIRT operations for the Information and Communication Technology (**ICT**) Division, Ministry of Post, Telecommunications, and Information Technology

A day long workshop for ICT division about cybersecurity

- Launching ceremony for the *Bangladesh Cyber Security Strategy* and *CII Information Security Guideline 2021*
- Seminar on *Digital Forensic Laboratory Guideline*

Launching ceremony of the Bangladesh Cyber Security Strategy and CII Information Security Guideline 2021

Events involvement

- Participated in the *3rd World Data Forum* (UN) in Switzerland (CH)
- Conducted training session for Department of Women Affairs on basic cybersecurity, digital security acts, and cyber awareness

Training session at BIBM

- Conducted a training session for *Bangladesh Institute of Bank Management* on cybersecurity, cybersecurity strategy, and cyber awareness
- Conducted training session for *Youth for Digital Awareness* on cybersecurity awareness

Achievement

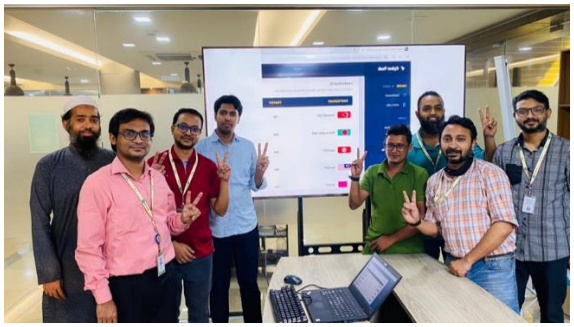
- Provided 70 cyber sensor analysis reports (from Jan 2021 - Dec 2021) to multiple CII

- *Cyber Threat Intelligence Report* provided to 74 government and non-government organizations
- *Malware Threat Intelligence Report for Bangladesh Context – 2021* has been prepared and published
- 218 cybersecurity advisories and news have been published on BGD e-GOV CIRT website to inform people about cybersecurity
- Publishing a monthly cybersecurity magazine for the stakeholders
- *Ransomware Prevention & First Response Guideline (Version 2.0)* has been prepared and published
- *Security Advisories & Alerts for Apache Log4j vulnerability* has been published
- BGD e-GOV CIRT published *Cyber Threat Landscape Report 2021*
- Bangladesh is ranked 53rd in the Global Cybersecurity Index (**GCI**)
- Bangladesh ranked 32nd position on NCSI
- *Information Security Guideline for CII* is published
- *Malware Threat Intelligence Report for Bangladesh Context – 2021* is published
- *Bangladesh Cyber Security Strategy 2021-2025* has been released
- *IT Audit Manual v1.0* is published
- In 2021, a total of eight (8) Information Technology (**IT**) security audits were performed
- Digital Forensic service provided to six (6) organizations with a total number of 16 cases and 160 evidence

2022 PLANNED ACTIVITIES

- Arrange cyber drills for different sectors
- Perform risk-based audit for CIIs
- Provide training about Industrial Control System (ICS) in the public sector
- Perform vulnerability assessment and penetration testing on financial sectors
- Training and workshop about cybersecurity for government organizations
- Provide regular cyber sensor analysis reports (intrusion, suspicious activities) to CII where the cyber sensors were deployed

Honourable Minister of Maldives visiting CIRT premises



Cyber drill team for the 9th Arab Regional & OIC-CERT Cyber Drill 2021

The Controller of Certifying Authorities
(General Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- Controlling Activities of Certifying Authority (**CA**)
- Issuing, suspending, and repealing CA license according to ICT Act 2006 (Amendment 2013) and ICT (CA) Rules 2010
- Leading and Maintaining of Public Key Infrastructure (**PKI**) activities
- Making rules, guidelines, and regulations for PKI and controlling its standard
- Submitting investigation reports before the Cyber Tribunal after investigating cyber-crimes under the ICT Act, 2006
- Constituting audit firm for auditing IT
- Prescribing rate of digital signature certificate according to IT (CA) rules, 2010
- Build up awareness about digital signature certificates and cyber security

Achievements

Cybersecurity trainings have been provided to 89,085 female students of class 8th-10th standard from 1,325 schools all over Bangladesh. Through this workshop, the cyber-crimes, relevant laws, security strategies on social network platforms, ways to avoid crimes, explanations of the related laws, helping agencies to file complaints, and specific procedures have been informed

Mr. Zunaid Ahmed Palak, Honourable State Minister of the ICT Division, Govt. of People's Republic of Bangladesh presiding over an online awareness training session for girls on digital security

Mr. Farhad Hossain, Honourable State Minister of Public Administration, Govt. of People's Republic of Bangladesh presiding over an online awareness training session for girls on digital security

Konnakotha - Voice of Daughter's (*https://konnakothacca.gov.bd*) a specialized web portal has been developed to maintain connection with the female students after the school awareness program. This idea came from an innovative, creative idea of this agency. This is a platform for teenage girls in Bangladesh to talk openly about cyber-crimes, problems faced, and the possibilities to share information which is new in the country. The portal regularly uploads pictures, videos, Frequently Asked Questions (FAQs) and upcoming training news from events held in each district. As a result, the students from one district can get

support from the training activities of other districts. An e-book on cyber-crime awareness has been inserted here. The type of cyber-crime, punishment, related laws, and remedies against cyber-attacks are described here. As a result, the students can easily download and save the content for future use when needed

Konnakotha - The most creative aspect of *Voice of Daughter's* is the district ambassadors. The ambassadors elected from different districts are connected to each other via the portal thus they can report the cyber thoughts and problems of teenagers in their respective districts directly by contacting the Controlling of Certifying Authority (**CCA**) office. Students register on this portal, create accounts, and stay connected. As a result, their identities are not revealed. They can freely share their thoughts with the highest security authority. Students are regularly asked various questions and answers about cybersecurity by a team of cyber experts. So far 20,093 students have visited this portal (till 15 January 2022)

- 669 government officials have been provided training on digital signature certificates and digital signature certificates
- A Digital Forensic Lab was established to control and investigate cyber-crimes and PKI systems was upgraded. Through this lab, cases are received from the Cyber Tribunal for investigation and reports made on the findings

Digital Forensic Lab was inaugurated by Mr. Sajeeb Wazed, Honourable Adviser on ICT to the Prime Minister of Bangladesh

- Establishing a world-class PKI system and ensuring cybersecurity using digital signature certificates for online transactions and information sharing
- The CCA Office as a Route CA and recognized as an international organization and achieved 06 Webtrust Seal
- A website called *KonnaKotha* has been launched compiling all the training materials including all the recordings, Q&A sessions, tutorials, training e-books titled *Awareness of Girls in Digital Security*
- A Disaster Recovery Centre has been set up for data recovery
- The e-Sign Guideline 2020 has been formulated to introduce user-friendly electronic signatures instead of dongle-based digital signatures, following which CA organizations including the Bangladesh Computer Council (**BCC**) have introduced electronic signatures

ABOUT THE ORGANIZATION/ AGENCY

Introduction

Aiming to achieve the goal of establishing e-commerce, e-transaction, and e-Governance in the

country as the basis for building the aspiration of Digital Bangladesh and the implementation of Information and Communication Technology Act 2006 (amended 2013), CCA Office was established as an attached office of the Information and Communication Technology Division. Digital Signature was introduced in 2012 under the ICT Act 2006 and it is gradually spreading to the whole country. Under Section-8 of the ICT Act 2006, the usage of Digital/ Electronic Signature and Records is recognized by all the Government offices

Establishment

The CCA Office is an organization under the Information and Communication Technology Division of the Ministry of Posts, Telecommunications, and Information Technology. The CCA Office is established under the Information and Communication Technology (Amended) Act, 2006 on May in 2011

Resources

Government

Constituency

Dhaka

ACTIVITIES & OPERATIONS

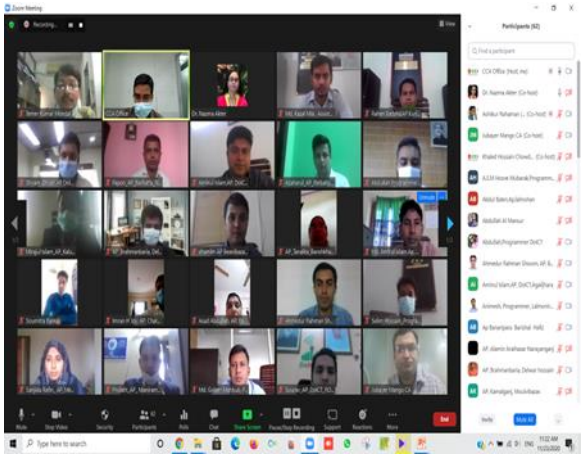
Events Organized by the Organization/ Agency

- To organize awareness seminars and training on digital signature
- To organize awareness training aimed at making the female students aware of digital security
- Conducting innovation related workshops and in-house trainings

Achievement

CA License

Five (5) private organizations and two government organization (BCC and Bangladesh Bank) have been licensed as CA. These seven (7) companies/ organizations have completed their own technical process and have been providing digital signature certificates and related services to various government and private organizations and to interested individuals. e-TIN (Tax Identification Number), the Registrar of Joint Stock Companies (RJSC), banks and the National University of Bangladesh are now using digital signature certificates in some of their online activities. The a2i[1] has started using digital signature certificates on test basis in the e-Nothi[2]



Trainees participating in online digital signature training

[1] *A flagship programme of the Digital Bangladesh agenda*

[2] *E-filing to simplify public service delivery and governance management*

Digital Signature & Training

As part of the activities of Information and Communication Technology Policy 2009, 2015, 2016, the CCA office provides training and certificates on digital signature among the government officials of various ministries, departments, and agencies including district/ upazila[3] level government officials. The CCA office is imparting training on digital signature every year to raise awareness on the use of digital signatures. To make government officials aware of digital signature, training on digital signature has been provided to 27,777 people since 2013. In addition, a roadmap has been prepared to expand the use of digital signatures and application of digital signatures in various e-services

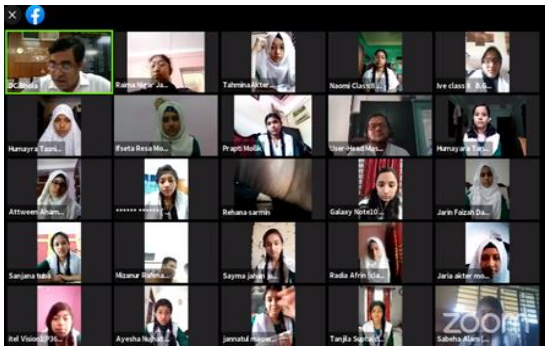
Establishment of Digital Forensic Lab & PKI System

The Digital Forensic Lab was established to control and investigate cybercrimes. and the PKI systems was upgraded. Through this lab, reports are being sent after investigating the cases received from the cyber tribunal. By establishing a world-class PKI system, cybersecurity would be ensured using digital signature certificates for online transactions and information sharing

A Disaster Recovery Centre has been set up for data recovery

Cyber Security Awareness Training for Girls

Awareness workshops on cybersecurity awareness for women empowerment were conducted in 1,325 schools of eight (8) divisions across the country to make women aware about cybercrime and security. In these workshops, about 89,085 students of the 8th to 10th grade received cybersecurity related practical training that explained about cybercrimes, related laws, the safety strategies on social network platforms, the way to get rid of crime, about the agencies to get help, and specific procedures to complain. In the current fiscal year (2021-2022), 15,962 girls were trained with the original 10,000 of targets and these activities are ongoing



Trainees participating in online awareness training for girls on digital security

Publication

A public awareness booklet entitled *Digital Security and Awareness* has been prepared by the CCA Office. The booklet already received a certificate of registration from the Copyright Office of the Ministry of Culture. The booklet is being distributed among students in grades 8 to 10 through an awareness workshop titled *Digital Security Awareness for Girl's Empowerment*

[3] *An administrative region in Bangladesh, functioning as a sub-unit of a district*

Laws & regulations

Information Technology Rules 2010, Cybercrime and Investigation rules have been drafted for Cybercrime, Cybersecurity Strategic Guidelines, Time Stamping Services Guidelines for Certifying Authorities 2020, Intractability Guidelines, Auditing Guidelines, Bangladesh Root CA Certifications Practice Statement (CPS) 2020, Digital Certificate Interoperability Guideline 2018, and Recruitment Rules (Controller, Deputy-Controller and Assistant Controller) 2012, and Recruitment Rules (Employees) 2012 has been formulated

The e-Sign Guideline 2020 has been formulated to introduce user-friendly electronic signatures instead of dongle-based digital signatures following which the CA organizations including the BCC have introduced electronic signatures

Innovation

Customer Data Verification System through National Identification (NID) Verification for Obtaining Digital Signature. VPN connection has been established with the NID database of the Election Commission for verification of user information for the purpose of using digital signature

A website called *KonnaKotha* has been launched compiling all the training materials including all the recordings, Q&A sessions, tutorials, e-books of the training titled *Awareness of Girls in Digital Security*

Leave Management Software, Training Calendar Automation Software, CA License Distribution Automation System & E-Evidence Software have been created

CCA Office as Route CA recognized as an International Organization and Achieved the Webtrust Seal

The CCA Office under the Department of Information Technology has gained recognition as an international standard institution for issuing electronic signature certificates. This was recognized by the Chartered Professional Accountant, Canada. After completing the web trust audit conducted by the CA Browser Forum, the CPA Canada awarded CCA Office the Route CA Certificate of Bangladesh on 25 Jun 2020 with three and five more on 10 Nov 2020. Guarantees to achieve quality of service delivery, these are Webtrust Seal for CA, Baseline Requirement Secure Socket Layer (BR-SSL) and Extended Validation Secure Socket Layer (EV SSL), Code Signing and Extended Validation Code Signing. By obtaining these Webtrust seals, the CCA Office has been processing to store the Bangladesh Root CA Certificate in various browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera, etc.) and operating systems (Microsoft, iOS, Android, etc.). As a result, digitally signed certificates of domestically valid licensing certifying authorities will be considered as acceptable in the international market

Webtrust seals obtained by CCA office

There are generally 5 types of Webtrust seals for certifying authority

- BR-SSL
- Webtrust seal for Certification Authorities
- EV-SSL
- Code Signing (CS)
- Extended Validation Code Signing (EV-CS)

2022 PLANNED ACTIVITIES

- Establishment of Security Operation Centre (**SOC**)
- Provide training and awareness on the practical aspects of using digital signature certificates and e-sign
- Provide awareness training to girls on digital security
- Networking device & e-Sign Equipment Installation
- Formulation of *Electronic Know Your Customer (e-KYC) Guidelines*
- Formulation of Application Programming Interface (API) Guidelines

BRUNEI DARUSSALAM

BruCERT

(Full Member)

ABOUT THE ORGANIZATION/ AGENCY

Introduction

Cyber Security Brunei (**CSB**) is the national cybersecurity agency of Brunei Darussalam, serving as an administrator that monitors and coordinates national efforts in addressing cybersecurity threats and cybercrime. It operates under the Ministry of Transport and Infocommunications (**MTIC**), with the Minister of MTIC as Minister-in-charge of cybersecurity

CSB provides cybersecurity services for the public and private sectors in Brunei Darussalam. These cybersecurity services are intended to ensure the following interests

- Increase awareness on cyber threats in the public and private sectors, especially the protection of the CII in Brunei Darussalam

- Improve the ability to respond to cyber incidents through effective cyber crisis management
- Enhance law enforcement capabilities in addressing cyber threats through the services of the National Digital Forensics Laboratory
- Increase public awareness on cyber threats

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

BruCERT Services

- 24 x 7 security related incidents and emergency response from BruCERT
- 24X7 security related incidents and emergency response onsite (Deployment response is 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 from BruCERT website. BruCERT constituents will receive alerts through email and telephone as well as the defence strategies in mitigating IT security related issues
- Promote security awareness program to educate and increase public awareness and understanding of information security and technical know-how through education workshops, seminars, and trainings
- Coordinating with other CERTs, 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

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

BruCERT Workforce

BruCERT currently has a strength of 66 staff (100% local) of which a majority specializes in IT while the rest are in administration and technical support. The staff has undergone training on various IT and security modules, such as A+, N+, Linux+, Server+, Security+, Security Certified Network Professional (SCNP), Security Certified Network Architect (SCNA), Certified Internet Web Professional (CIW), Certified Ethical Hacker (**CEH**), Cisco Certified Network Associate (CCNA), Certified Information Systems Security Professional (**CISSP**), BS7799 Implementer, and SANS Institute trainings such as Global Information Assurance Certification(GIAC) Reverse Engineering Malware (GREM), GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic

Analyst (GCFA), GIAC Penetration Tester (GPEN), where most of BruCERT workforce has gained certifications in

BruCERT Constituents

BruCERT works closely with government agencies, one (1) major ISPs and various numbers of vendors

Government Ministries and Departments

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

E-Government National Centre

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

AITI

Authority for Info-communications Technology Industry of Brunei Darussalam (**AITI**) is an independent statutory body to regulate, license, and develop the local ICT industry and manage the national radio frequency spectrum

AITI has appointed the Information Technology Protective Security Services (ITPSS), an IT local security company to become the national CERT in dealing with incident response in Brunei

Royal Brunei Police Force and other Law-Enforcement Agencies

BruCERT has been collaborating with Royal Brunei Police Force (RBPF) and other Law-Enforcement Agencies (**LEA**s) to resolve computer-related incidents through the Digital and Mobile Forensic services

Unified National Network

Unified National Network (UNN), the main Internet service provider and BruCERT have been working together to engage information sharing of Internet-related statistics and the current situation of IT environment in Brunei

BruCERT Contact

BruCERT welcomes reports on computer security related incident. Any computer related security incident can be reported to

Telephone: (673) 2458001
Facsimile: (673) 2458002
Email: *cert@brucert.org.bn*

BRUCERT OPERATION IN 2021

Incidents Response

In 2021, BruCERT had received a lot of reports from the public as well as from

BruCERT security intelligent sensors. Malware infections are the most common cyber threats in Brunei Darussalam and there are few cases involving Ransomware. There is an increase in reconnaissance as well as root level intrusion in Brunei. The statistic of the security incident is shown as Figure 1

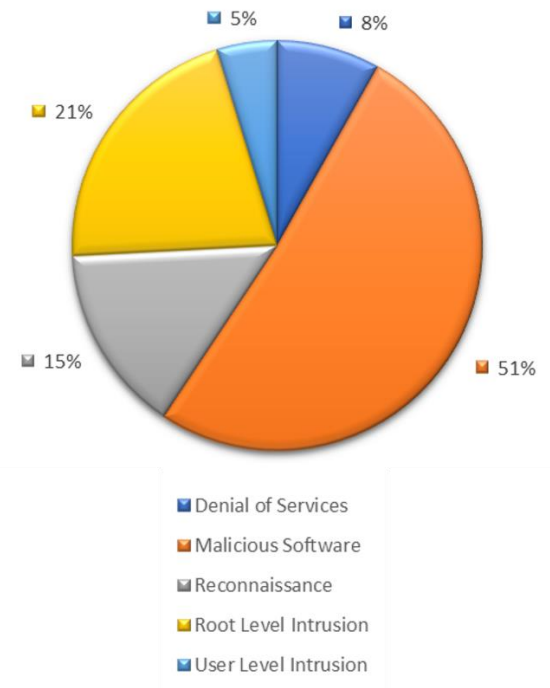


Figure 1 BruCERT Stastics 2021

Table 1 Incident type and counts

Types of Attack	Count
Denial of Services	309
Malicious Software	1939
Reconnaissance	562
Root Level Intrusion	798
User Level Intrusion	180

BruCERT Honey Pot

The most abused port number is 1900 which is the UPnP followed by port number 445, which in this case used by SAMBA (**SMB**). The third most abused port is port number 1433 which is used by Microsoft SQL Server for database management. It is assumed the attack on SMB might came from *WannaCry Ransomware*, trying to exploit the vulnerability

Table 2 Most Attacked Destination Ports 2021

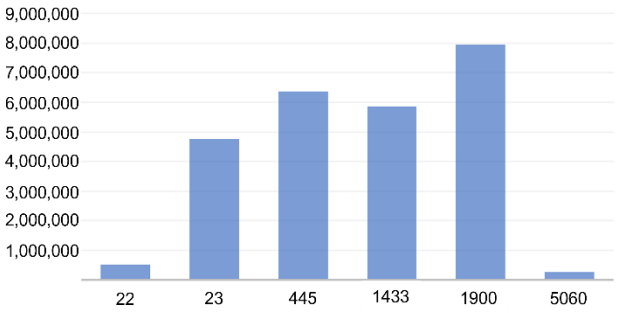


Table 3 Port Attack Counts

Port No:	Count
22	514,573
23	4,768,959
445	6,368,525
1433	5.863,661
1900	7,943,676
5060	273,847

The BruCERT honeypot managed to capture some of the malware hashes, in Figure 2 and Table 4, it shows the summary of the most detected malware in BruCERT Honeypot

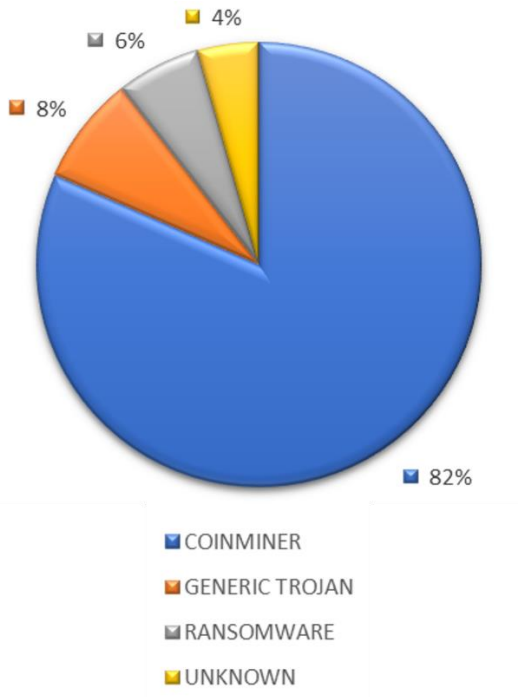


Figure 2 Top Malware Detected 2021

Table 4 Most detected Malware 2021

MALWARE TYPE	TOTAL
COINMINER	35,740
GENERIC TROJAN	3,445
RANSOMWARE	2,674
UNKNOWN	1,942
TOTAL	**43,801**

BRUCERT ACTIVITIES IN 2021

Seminars/Conferences/Meetings/Visits

BruCERT attended and presented at various seminars, conferences and meetings related to the field of ICT security but most of the meetings are done virtually

INDONESIA

National Cyber & Crypto Agency (NCCA)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

The Covid-19 pandemic, which began in 2020, has established a new operational pattern that relies heavily on online communication between employees in the daily work. As people are getting used to the new pattern, the second wave of Covid-19 hit Indonesia in the middle of the year that disrupt the operations due to personnel falling ill, as well as other related activities that had to be postponed

However, despite this condition, the National Cyber and Crypto Agency (**NCCA**) still carry out its activities, especially in international cooperation to increase the capacity of the Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Centre (**Id-SIRTII/ CC**) as the national CSIRT. In addition to participating in training activities and various cyber exercises organized by the international community, NCCA also organized similar activities by getting the participation of other countries in making them a success

Achievements

The major achievement in 2021 for NCCA, especially Id-SIRTII/ CC as the National CSIRT, is to establish regional CSIRTs within the country. In 2020, NCCA has establish 15 CSIRTs in the government sector, and 45 more CSIRTs in government and CII sector in 2021

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The government agency which has a national responsibility in cybersecurity started with the establishment of Id-SIRTII/ CC on 4th May 2007 by the Minister of Communication and Information Decree number no 26 in 2007. Since the establishment until 2018, Id-SIRTII/ CC assumed the function as the National CSIRT and Coordination Centre for national incident handling and works under the Directorate of Telecommunication of the Ministry of Communication and Information. Based on the Presidential Decree Number 53 in 2017, Id-SIRTII/ CC merged and moved to NCCA (*Badan Siber dan Sandi Negara - BSSN*)

In April 2018, NCCA officially started carrying the strategic roles as the top-level authority for cybersecurity related activities in Indonesia. The agency is directly under the purview of the President, which is the merging of Id-SIRTII/ CC and the National Crypto Agency (*Lembaga Sandi Negara - LSN*)

Id-SIRTII/ CC is currently operating under the Directorate of Cyber Security Operation, NCCA

Establishment

Id-SIRTII/ CC was established on 4 May 2007 and later merged with the National Crypto Agency to develop a new national agency named NCCA, based on the Presidential Decree Number 53 in 2017. NCCA officially started its operation in Apr 2018

Resources

NCCA, as the new national agency, has several main functions such as detection, monitoring, response and mitigation, cooperation, and as the national security operation centre, covering the areas of government, CII, and digital economy

Constituency

- Ministries and Government agencies
- LEAs
- National Defence
- CII Operators
- Cybersecurity communities
- Internet Service Providers (**ISP**)
- Network Access Providers (NAP)
- Local Internet Exchange Operators
- Other Sector CERT/ CSIRT in Indonesia

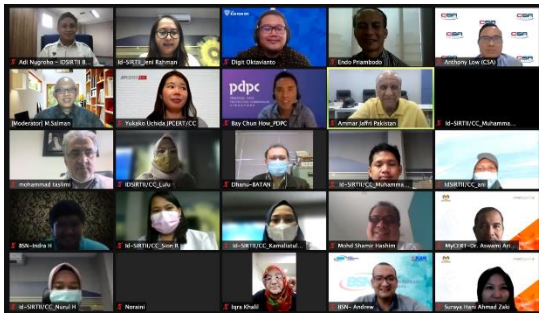
ACTIVITIES AND OPERATION

Events organized by the organization / agency

In 2021, Indonesia is still carrying out the task as Deputy Chair of OIC-CERT, also has a role in maintaining strategic pillar on Capacity Building. We held a webinar entitled "Data Breach: Mitigation and Lesson Learned" which became a big topic in 2021 due to the large number of major data breach cases that occurred both in Indonesia and globally. In this webinar, NCCA invited panelists from various countries, namely Japan and Singapore, as well as the Indonesian National Police, and cyber security activist from Indonesia. In the second semester, NCCA also held a technical workshop with the theme Malware Analysis, which was presented by a lecturer from the National Cyber and Crypto Polytechnic of Indonesia, which is an official university that operates under NCCA to produce graduates who are ready to work at cybersecurity field in NCCA.

Events involvement

- Collaborated with Carnegie Mellon University to conduct a technical training for Id-SIRTII/CC personnel with theme "Unhiding Hidden Cobra" (15 February)
- Participated in APCERT Training: Implementing IoT Security Testing (23 February)
- Participated in NISC: International Cybersecurity Exercise 2021 (25 February)
- Conducted a webinar for "Indonesia Cybersecurity Monitoring Annual Report 2020" publishing (1 March)
- Participated in Japan-US Industrial Control System Cybersecuirty Week FY2020 year 2021 (8 March)
- Conducted a Technical Assistance for Regional Government CSIRT (30 March)
- Participated in FIRST Regional Virtual Lightning Talk Session (1 April)
- Conducted OIC-CERT Webinar "Data Breach: Mitigation and Lesson Learned" (29 June)



OIC-CERT Webinar "Data Breach: Mitigation and Lesson Learned"

- Participated in APCERT Drill Test 2021 (25 August)
- Participated in SingCERT ASEAN CERT Incident Drill (ACID) 2021 (8 September)
- Participated in OIC-CERT Cybersecurity Drill "Enhance Cyber Security Readiness" 2021 (28 September)
- Participated in Carnegie Mellon University "Training of Trainer: Creating and Managing CSIRT" (2 November)
- Participated in ITU Cyber Drill (4 November)
- Participated in Taiwan Cyber Offensive and Defensive Exercise (CODE) 2021 (16 November)

- Conducted OIC-CERT Technical Workshop "Malware Analysis" (17 November)

OIC-CERT Technical Workshop 2021 - Malware Traffic Analysis

- Hosted APCERT Training "Wireless Network Security" (7 December)
- Conducted Coordination Forum of Indonesian Gov-CSIRT (8 December)
- Participated in CIT-CERT/CC Pakistan (C4P) Conference 2021 as panellist (16 December)

Id-SIRTII/CC participated on CIT-CERT/CC Pakistan (C4P) Conference 2021

- Participated in Egyptian First International Cyber Drill (22 Dec 2021)

Achievement

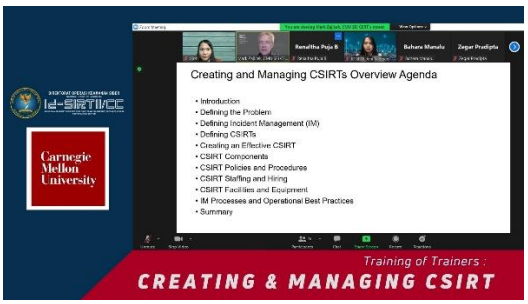
To optimize national incident response, Indonesia has actively established a number of regional CSIRTs for central government, ministries, regional governments, and critical infrastructrure sector. In 2020, NCCA has establish 15 CSIRTs in government sector, and 45 more CSIRTs in government and critical infrastructure sector in 2021.

NCCA also conducted various activities to develop the established CSIRTs to gain their personnel's skill and awarenes, such ad cyber drill, technical assistance, webinar, etc.

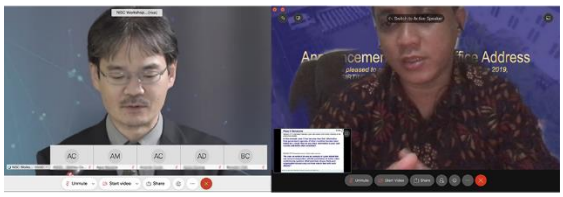
2022 PLANNED ACTIVITIES

In line with the mission on establishing regional CSIRTs which become one of our major focus, it leads to a plan on how a cybersecurity institution like NCCA and Id-SIRTII/CC as a National CSIRT, gain a good relationship with regional agencies, especially with private sector and critical infrastructure sector, to collaborate in cybersecurity and to establish their own CSIRTs.

Based on this objective, we plan to hold a series of activities that gather ideas and experiences from various countries in collaborating with relevant sectors in their respective countries in an effort to improve their national cyber security. As we know, as a national agency engaged in cybersecurity, it is really essential to gain public trust and build collaboration with the private sector, especially the critical infrastructure sector.

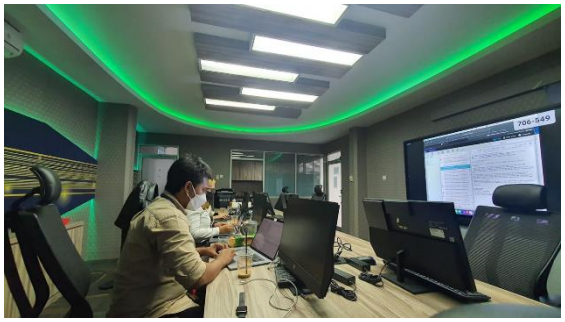


Training of Trainer: "Creating Managing CSIRT" collaboration with Carnegie Mellon University (CMU)



IDSIRTII Participated in NISC: International Cybersecurity Exercise 2021

Regional Gov-CSIRT Technical Assistance 2021



APCERT Cyber Drill: "Supply Chain Attack Through Spear-Phishing - Beware of Working from Home"

OIC-CERT Cyber Security Drill "Enhance Cyber Security Readiness" 2021

KYRGYZSTAN

Computer Emergency Response Team of Kyrgyz Republic (CERT-KG)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- making proposals for the development of a cybersecurity policy
- coordination of activities for the organizations, centres for responding to computer incidents (departmental, industry, and others)
- To ensure security and identified cybersecurity - identify, prevent, and suppress computer attacks
- respond to computer incidents
- identification, prevention, and suppression of possible threats and cybersecurity
- making suggestions for improving the legislation of the Kyrgyz Republic in the field of IT and cybersecurity
- participation in the development of international treaties for the Kyrgyz Republic in the field of security and cybersecurity
- ensuring the fulfilment of obligations in the field of international relations

participation in which is carried out by the Kyrgyz Republic
- Accomplishment of tasks in accordance with the regulatory legal acts of the Kyrgyz Republic

Achievements

- As part of the implementation of the roadmap for the implementation of the Digital Transformation Concept *Digital Kyrgyzstan 2019-2023*, CERT-KG was formed into the Coordination Centre for Ensuring Cybersecurity for the Kyrgyz Republic
- By the Order of the Government of Kyrgyz Republic No. 380-r of 23 November 23, 2020, the Interdepartmental Commission of the Commission on Information and Cybersecurity was established, which is a consultative and advisory body formed to create conditions and coordinate actions of state bodies and local self-government bodies in the field of information and cybersecurity, acting on a permanent basis
- The Coordination Centre for Cybersecurity of the State Committee for National Security of the Kyrgyz Republic (**CERT-KG**) conducts several technical measures to detect and mitigate computer attacks on the information systems of state bodies of the Kyrgyz Republic

ABOUT THE ORGANIZATION/ AGENCY

Introduction

CERT-KG was established to improve the national infrastructure for coordinating and ensuring cybersecurity of the Kyrgyz Republic

Establishment

CERT-KG was established on 21 May 2020

Resources

Government

Constituency

CERT-KG all networks, information resources and users located in the information space of the Kyrgyz Republic

ACTIVITIES & OPERATION

Events organized by the organization/ agency

In the spring of 2021, CERT-KG conducted the first national cyber exercise *Digital Kyrgyzstan 2021* for government officials

2022 PLANNED ACTIVITIES

- Launch of the Incident Response Platform project
- Organize and hold training courses and seminars for employees of state bodies of the Kyrgyz Republic
- Development of standards in the field of IT
- Conducting cyber exercises for government agencies
- Establishment of a training centre

Computer Emergency Response Team of Ministry of Digital Development of Kyrgyz Republic (CERT.ICT.KG)
(General Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

The Computer Emergency Response Team - CERT.ICT.KG was created recently in 2021 as a state and sectoral team to support and help state organizations and other relevant entities

The main efforts and activity of the team aimed at protecting the government information resources and safe digital transformation

ABOUT THE ORGANIZATION/ AGENCY

Introduction

CERT.ICT.KG is a General Member of the OIC-CERT and is a department of the Ministry of Digital Development of Kyrgyz Republic and acting as the state computer emergency team. The Ministry is a regulator in the field of communications and the authorized state body in the field of digital transformation

CERT.ICT.KG was established under the Ministry of Digital Development in Jun 2021. In Sep 2021 became a General Member of OIC-CERT

CERT.ICT.KG provides cybersecurity services for the public and the information & communication sectors in Kyrgyz Republic. Together with the Coordination Centre of Cybersecurity, CERT.ICT.KG forms and develops the national cybersecurity policy, promoting cyber hygiene, and maintains the cybersecurity of state information resources

Constituency

State and public organizations, ICT community

ACTIVITIES & OPERATION

Event organized by the organization

In Sep 2021 organized the Digital Week in Kyrgyz Republic with participation from international organizations, companies, and digital ministries of Kazakhstan and Uzbekistan. As part of this event, a bilateral meeting was held with the Centre for Analysis and Investigation of Cyber Attacks of Kazakhstan (CAICA)

Bilateral meeting with CIACA (Kazakhstan) in Digital Week

Event involvement

Participated as a speaker in the First National Cybersecurity Conference and Drill in Apr 2021

Achievements

CERT.ICT.KG developed the National Cybersecurity Strategy and participated in the development of the National Information Security Concept

CERT.ICT.KG in National Cyber Training

In Dec 2021 created the State Agency for Personal Data Protection under the Cabinet of Ministers

Participate in the development of a draft law on cybersecurity

2022 PLANNED ACTIVITIES

- In strengthening and improving international collaboration and cooperation in cybersecurity, CERT.ICT.KG planned to sign MoUs with cert teams from the Commonwealth of Independent States (**CIS**) and Asia Pacific region
- Implementation of a joint project with International Telecommunication Union (**ITU**) and the World Bank to strengthen the capabilities of CERT.ICT.KG

Bilateral meeting with Kaspersky Lab representative

As a speaker in national cyber training

Participation in cyber training

Presenters of CERT.ICT.KG

MALAYSIA

CyberSecurity Malaysia
(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

22 Feb - 4 Mar 2021 - Participated in the APRICOT 2021/ APNIC 51 virtually

11 – 14 May 2021 - Participated in the 20th Annual AusCERT Information Security Conference virtually

24 - 25 May 2021 - Participated in the 16th Annual Technical Meeting for CSIRTs with National Responsibility virtually

6 – 9 Jun 2021 - Participated in the 33rd FIRST Annual Conference virtually

21 – 30 Jun 2021 - Conducted a capacity building training under the Malaysian Technical Cooperation Programme (**MTCP**) attended by selected APCERT members titled *Certified Penetration Tester" Technical Training* (*Session 1*)

5 – 14 Jul 2021 - Conducted a capacity building training under the MTCP attended by selected APCERT members titled *Certified Penetration Tester Technical Training* (*Session 2*)

25 Aug 2021 - Participated in the APCERT Cyber Drill 2021 with the theme *Supply Chain Attack Through Spear-Phishing – Beware of Working from Home*

13 – 16 Sep 2021 - Participated in the APNIC 52 virtually

28 Sep 2021 - Co-organised the OIC-CERT Cyber Drill with Oman National CERT

1 Oct 2021 - Chaired the APCERT Annual General Meeting (AGM) conducted virtually

23 - 24 Nov 2021 - Organised the OIC-CERT 13th Annual Conference & 9th Arab Regional Cybersecurity Summit 2021 (virtual) with the theme *CERTs in an Evolving Cyber Security Landscape*

14 – 16 Dec 2021 - Organised the Cyber Security Malaysia - Awards, Conference & Exhibition (**CSM-ACE**) 2021 in Cyberjaya, Malaysia

Achievements

Incident Handling Reports and Abuse Statistics

CyberSecurity Malaysia receives reports from various parties within its constituency such as home users, private sectors, government sectors, security teams from abroad (foreign CERTs), Special Interest Groups, as well as through the internal proactive monitoring by CyberSecurity Malaysia

CyberSecurity Malaysia through MyCERT had proactively produced 13 advisories and 18 alerts in 2021 to inform its constituency on issues relating to cybersecurity. The specific list of the advisories, alerts and summary reports can be viewed at *https://www.mycert.org.my/portal/advisories2020*

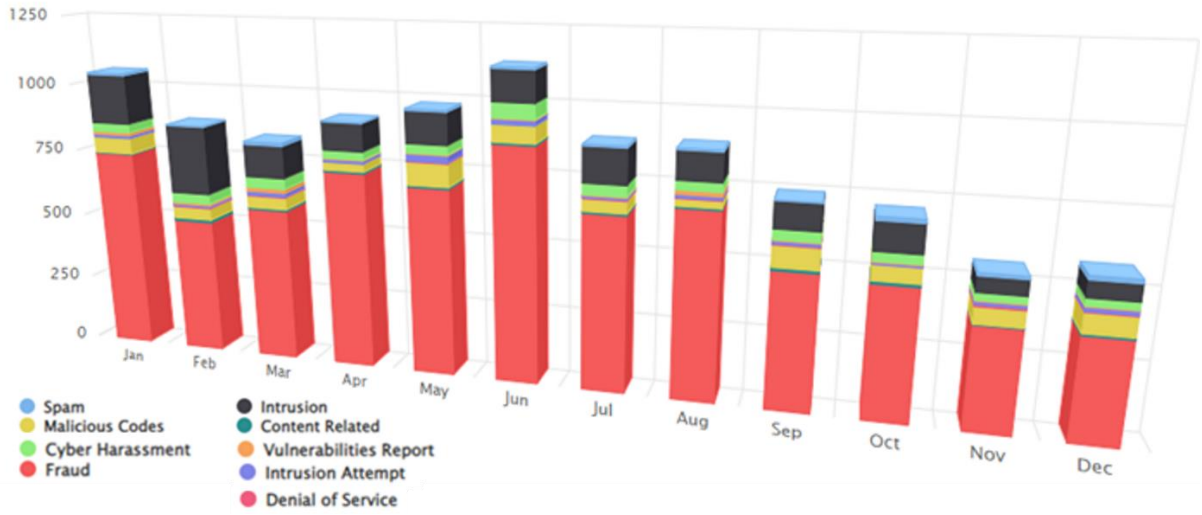


Figure 3 Reported incidents based on General Incident Classification Statistics 2021

Most of the incidents reported were related to fraud and followed by intrusion. Figure 3 shows the reported incidents managed by CyberSecurity Malaysia

Further information on incidents reported to CyberSecurity Malaysia can be viewed at: *https://www.mycert.org.my/portal/statistics-2021*

Cyber Threat Research Centre

The Cyber Threat Research Centre (**CTRC**) operates a distributed research network for analysing malware and cybersecurity threats. The centre had also established collaboration with trusted parties and researchers in sharing threat research information

Other activities by the centre includes

- Conducting research and development work in mitigating malware threats
- Producing advisories on the latest threats
- Threat monitoring via the distributed honeynet project
- Partnership with universities, other CERT's and international organisations

Lebahnet Project

LebahNET is a Honeypot distributed system where a collection of honeypots is used to study on how the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism set up to mimic a legitimate site to ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at *https://dashboard.honeynet.org.my/*

The URLs of the LebahNET project are

- LebahNET portal at *https://dashboard.honeynet.org.my/*

- Kibana portal at *https://es.honeynet.org.my/s/public/app/canvas#/workpad/workpad-5e83726d-0125-4bfd-a8e9-88b6e844ce24/page/1*
  by using guest authentication
  Username: guest
  Password: guest2021

ABOUT THE ORGANIZATION/ AGENCY

Introduction

CyberSecurity Malaysia is the national cybersecurity specialist agency under the Ministry of Communications and Multimedia Malaysia having the vision of being a globally recognised National Cyber Security and Specialist Centre. Some of the services provided are

- Cybersecurity Emergency Services
  - Security Incident Handling
  - Digital Forensic
- Security Quality Management Services
  - Security Assurance
  - Information Security Certification Body
- Cybersecurity Professional Development and Outreach
  - Info Security Professional Development
  - Outreach
- Cybersecurity Strategic Engagement and Research
  - Government and International Engagement
  - Strategic Research
- Industry and Research Development

Establishment

CyberSecurity Malaysia started with the formation of the Malaysian Computer Emergency Response Team (**MyCERT**) on 13 Jan 1997 under the Ministry of Science, Technology, and Innovation. In 2018, with the restructuring of the government administration, CyberSecurity Malaysia was transferred to the Ministry of Communications and Multimedia Malaysia. CyberSecurity Malaysia is committed in providing a broad range of cybersecurity innovation led services, programmes, and initiatives to help reduce the vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in the cyber space

Resources

CyberSecurity Malaysia services include predictive, detective, responsive, and corrective capabilities as well as recovery. This agency provides technical solutions and services to the Government of Malaysia among which are LEAs, ministries, regulatory bodies and government agencies, private organisations, and the Internet users in Malaysia

CyberSecurity Malaysia's scope of specialised cybersecurity services are as follows

- Cyber Security Responsive Services
- Cyber Security Proactive Services
- Outreach and Capacity Building
- Strategic Study and Engagement
- Industry and Research Development

Constituency

CyberSecurity Malaysia's constituency is the Internet users in Malaysia. Cybersecurity incidents within Malaysia that are reported either by the Malaysian public or international organisations will be resolved by assisting the complainants with technical matters. If an incident involves international cooperation, CyberSecurity Malaysia will request trusted parties in respective countries or constituencies, of which the origin of the case, to assist in resolving the security issues

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

Online Trainings

There were several online trainings organized by CyberSecurity Malaysia which are as follows

- 21 – 30 Jun 2021 – The MTCP *Certified Penetration Tester* (Session 1) Technical Training virtually
- 5 – 14 Jul 2021 – The MTCP *Certified Penetration Tester* (Session 2) Technical Training virtually
- 9 – 12 Aug 2021 - Forensic Training Program for Asia Pacific University (**APU**) virtually
- 28 – 29 Aug 2021 - *The Certified Cybersecurity Awareness Educator* (**CCASE**) Training Program virtually
- 23 Sep 2021- *Global Digital Security and Forensic in the New Norm* Webinar
- 23 Dec 2021 - *People, Process and Technology Certification: An Instrument of Compliance* Webinar

The OIC-CERT 13th Annual Conference & 9th Arab Regional Cybersecurity Summit (Virtual)

Session 2 on "Technical (Emerging technologies – Compliance, and Security Risks" at the 13th Annual Conference & 9th Arab Regional Cybersecurity Summit

Due to COVID-19 pandemic, this annual event was conducted virtually via YouTube Live from 23 to 24 Nov 2021. The conference was hosted by the National Cybersecurity Authority (**NCA**) of the Kingdom of Saudi Arabia and co-hosted by the OIC-CERT Permanent Secretariat and ITU Arab Regional Cyber Security Centre (**ITU-ARCC**). At the event, 12 papers were presented by speakers from various countries i.e., Brazil, Indonesia, Malaysia, Oman, Russia, Saudi Arabia, Sri Lanka, Tunisia. During this conference, the OIC-CERT Chair also has announced the winners of the OIC-CERT Global Cybersecurity Award

Malaysian Technical Cooperation Programme

CyberSecurity Malaysia in collaboration with the Ministry of Foreign Affairs Malaysia successfully organised 2 training sessions entitled *Certified Penetration Tester* from 21-30

Jun and 5-14 Jul 2022 under the MTCP

The MTCP was formulated based on the belief that the development of a country depends on the quality of its human resources. Developing capabilities in the cybersecurity area is essential for developing countries to ensure less dependency on foreign countries and at the same time nurture self-reliance to protect their digital citizens

Opening ceremony of the "Certified Penetration Tester" for MTCP

In relation to this, the training programme leverages on state-of-the-art cybersecurity knowledge from domain experts and experience practitioners. *Certified Penetration Tester* is a hands-on training and certification programme that enable the participants to manage the vulnerability assessment and penetration test for their clients

24 participants from the following OIC-CERT and ASEAN countries attended the training

Bangladesh	Jordan
Brunei Darussalam	Kyrgyzstan
Indonesia	Libya
Thailand	Morocco
Vietnam	Nigeria
Iran	Uzbekistan

OIC-CERT 5G Security Working Group

In 2021, the 1st edition of the OIC 5G security framework plan was developed exclusively for the OIC community globally, the basis for heralding in the new Islamic Golden Age. Hence, the OIC-CERT 5G Security Working Group (**WG**) has been established as proposed by Huawei, a commercial member of the OIC-CERT. The WG consists of 10 members i.e., Bangladesh, Brunei Darussalam, Indonesia, Pakistan, Somalia, Tunisia, Malaysia, Morocco, Oman, and UAE. Huawei and Malaysia are the co-lead for the WG

The OIC-CERT Board Meeting No. 02/2021 has agreed to the establishment of the OIC-CERT 5G Security WG with the following objectives

- Identifying 5G cybersecurity risks taking in account the different perspectives from the stakeholders and maintaining a risk register
- Developing recommendations for members, a 5G security standard that be a reference model for member states to develop their own National 5G cybersecurity standards
- Developing recommendations for an OIC level 5G security framework that harmonise the requirements to allow for cross-recognition among OIC member states
- Develop an Information Sharing and Analysis Centre (**ISAC**) capability for CERT response in the era of 5G and Cloud Computing for OIC-CERT member states

Several meetings were conducted in 2021 and a series of workshops in selected countries will be organized in 2022

Events involvement

CyberSecurity Malaysia is actively participating in cybersecurity events such as trainings, seminars, conferences, and meetings. The agency has contributed its competencies in the following events

Cyber Drills

CyberSecurity Malaysia participated in three (3) international cyber drills in 2021 namely the APCERT Drill, ASEAN CERT Incident Drill (ACID), and the OIC-CERT Drill

As in the previous years, CyberSecurity Malaysia was involved in co-organizing international cyber drills for the OIC-CERT. In 2021, Malaysia collaborated with Oman in organising the drill with the theme, *Enhance Cyber Security Readiness*. The objective of this drill is to get a more realistic experience in anticipating and handling some incidents related incidences and analysis of malwares

Social Media

In 2021, CyberSecurity Malaysia received continuous invitations to speak in events regarding cybersecurity at the local radio and television stations. CyberSecurity Malaysia also actively disseminates cybersecurity concerns through social media such as Facebook and Twitter, which as of now the Facebook Page has about 54,046 followers and the CyberSecurity Malaysia Twitter has 7,175 followers

Achievement

OIC-CERT Malware Research and Coordination Facility

This is a collaborative effort of the OIC-CERT, APCERT and other organisations from various countries. The project is an initiative by CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT. In 2021, 12 issues of the Malware Trend Report have been published and 2 new members joined the project.

The project is using Lebahnet, which is a Honeypot distributed system where a collection of honeypots is used to study on how the exploits functioned as well as to collect malware binaries. Honeypots are computer software mechanism set up to mimic a legitimate site to ensnare malicious software into believing that it is a legitimate site which is in a weak position for attacks. Honeypot allows researchers to detect, monitor, and counter malicious activities by understanding the activities done during the intrusion phase and attacks' payload. It can be viewed at *https://dashboard.honeynet.org.my/*

OIC-CERT Global Cybersecurity Award

The OIC-CERT Global Cybersecurity Award is an initiative by the OIC-CERT to encourage international collaboration in the cybersecurity domain. The OIC-CERT Award recognizes innovative cybersecurity

projects from around the world, not bound by country or region, that contribute to the uplifting of the ummah wellness while promoting the digital realm

The theme for 2021 is *Cybersecurity Innovation Towards Society Prosperity and Wellbeing*. The committee received seven (7) nominations from entities representing governments, private sector, international and regional institutions, civil society, and academia. The 2021 winners and project are as follows

- FNS(M) Sdn. Bhd., Malaysia - *Making the World a Safer Place with Passwordless Blockchain Secure Authentication*
- Huawei Technologies Co., Ltd, Kingdom of Saudi Arabia - *The Dera' Training Initiative*

Research Papers

CyberSecurity Malaysia actively contributed research papers to journals and conference proceedings. Following are some of the papers published

- *Mobile Malware Classification for Social Media Application*. Published in IEEE Xplore Digital Library
- *Using Text Annotation Tool on Cyber Security News: A Review*. Published in IEEE Xplore Digital Library
- *Method for Generating Test Data for Detecting SQL Injection Vulnerability in Web Application*. Published in IEEE Xplore Digital Library
- *Ransomware Entities Classification with Supervised Learning for Information Text*. Published in IEEE Xplore Digital Library
- *Feature Extraction and Selection Method of Cyber Attacks and Threat Profiling in Cybersecurity Audit*. Published in IEEE Xplore Digital Library
- *TAGraph Knowledge Graph of Threat Actor*. Published in IEEE Xplore Digital Library
- *OTPAF: A Security Requirement Conceptual Model of Cloud SAAS for Malaysian Government Based on Common Criteria*. Published in IEEE Xplore Digital Library
- *Cloud Service Provider Security Readiness Model: The Malaysian Perspective*. Published in IEEE Xplore Digital Library
- *An Attribution of Cyberattack using Association Rule Mining (ARM)*. Published in The Science and Information Organization
- *A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies*. Published in ACM Digital Library
- *Cryptojacking Classification Based on Machine Learning Algorithm*. Published in ACM Digital Library
- *The Capabilities that Terrorist Possess in the Digital Age*. Published in Özgür Öztürk Dakam Yayinlari
- *S-Box Construction Based on Linear Fractional Transformation and Permutation Function*. Published in MDPI
- *Secure Information Hiding Based on Random Similar Bit Mapping*. Published in International

Association of Computer Science and Information Technology

- *Slid Pairs of the Fruit-80 Stream Cipher*. Published in Institute of Information Technology
- *Mitigating Insider Threats: A Case Study for Data Leakage Prevention*. Published in Academic Conferences and Publishing International Limited
- *OS Kernel Malware Detection through Data Characterization of Memory Analysis*. Published in Academic Conferences and Publishing International Limited
- *A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Dataset, Open Challenges and Recommendations*. Published in MDPI
- *Fraudulent e-Commerce Website Detection Model Using HTML, Text and Image Features*. Published in Springerlink
- *Malware Behaviour Profiling from Unstructured Data*. Published in Springerlink
- *Findings Annihilator(s) via Fault Injection Analysis (FIA) on Boolean Function of LILI-128*. Published in Engineering and Technology Publishing
- *Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT*. Published in IEEE Xplore Digital Library
- *Randomness Analysis on Lightweight Block Cipher, PRESENT*. Published in Science Publications

International Roles

Amongst the international roles and contributions by CyberSecurity Malaysia are

- The Permanent Secretariat of the Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), where the major role is to facilitate cooperation and interaction among the members countries
- The lead for the Capacity Building Initiatives in the OIC-CERT
- The Chair of the APCERT
- Member of FIRST
- The Convenor for the APCERT Malware Mitigation Working Group – addressing malware infection among Internet users and cyber threat general issues. The main objectives are to provide an overview of the cyber threats landscape by doing collaborative research to mitigate the cyber threats and sharing regular reports or data on malware attacks and focus on the impact analysis and remedial action

2021 PLANNED ACTIVITIES

CyberSecurity Malaysia strives to improve service capabilities and encourage local Internet users to report cybersecurity incidents to the Cyber999 cyber incident reference centre. The development of new and better reporting channels and further promotion of services through the mass media are aspects that will proactively be intensified

To encourage a safer cyber environment, CyberSecurity Malaysia realises the need to work together with the local and international cybersecurity organisations through the establishment of formal relationship arrangements such as MoUs and agreements

This agency will continue to organise national events such as the CSM-ACE, which is an annual event providing awareness, training and awards to information security professionals, and the National ICT Security Discourse to boost the cybersecurity awareness among the youth. At the international arena, CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT, continues to spearhead the collaboration and organise international events such as the OIC-CERT Annual Conferences and trainings

With such understanding, CyberSecurity Malaysia supports newly established local and international CSIRT by providing consultation and assistance especially in becoming members to the international security communities such as the APCERT, FIRST and OIC-CERT

OMAN

Oman National CERT (OCERT)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- Cybersecurity cooperation and alliances
- Participated in the virtual campaign (Aman), which was organized by the Omani Association for Information Technology, held on 18 Jan 2021
- Participated in the virtual conference entitled *Cyber Security Conference for main sectors in the Middle East* as a strategic partner, held on 1- 2 Feb 2021

Cybersecurity for Critical Assets for MENA

- Chaired the 1st virtual meeting of 2021 for the Board of Directors of the OIC-CERT to approve the action plan, held on 2 Feb 2021
- Celebrated the Safer Internet Day (SID 2021) in cooperation with three (3) local institutions in the Sultanate (A-Seeb International School, the Omani Association for People with Hearing Disabilities, and a photography technician) on 8 – 9 Feb 2021
- Chaired the annual meeting of the ITU- Arab region Study Group 17 (SG17RG-ARB).
- The Arab Regional Centre for Cyber Security signed a memorandum of cooperation with a British company, QG Media, to participate as a strategic partner in the event *Cyber Security Conference for Basic Sectors in the Middle East*
- Organized the 2nd virtual workshop entitled *Internet Infrastructure Security and Information Sharing* in cooperation with the Humanitarian Dialogue (HD), held on 22 Mar 2021
- The Director General of the National Centre for Cyber Security received the *Most Influential Cyber Security Award* from Infosec Global in the category of Executives and Leadership
- ITU-ARCC in partnership with the Centre for Humanitarian Dialogue in organizing the 3rd workshop on *Confidence Building Measures and Information Exchange in the Middle East*, held in Geneva on 24-25 Aug 2021 (CH)
- Developed the 2018-2020 Annual Report for the Arab Regional Cybersecurity Centre and published in the ARCC website
- Participated as speaker in the meeting of the ITU for the American and Arab regions and presented the paper titled *Cyber resilience and Information Infrastructure Protection* on 23 Sep 2021
- Organizing the 1st virtual hackathon in the Sultanate of Oman, in cooperation with Oman Arab Bank
- The Sultanate, represented by the Arab Regional Centre for Cyber Security, participated in organizing the ITU Virtual Global Cyber Drill with a scenario entitled *Forensic Analysis of Memory* on 5 Nov 2021

ITU Global Cyber Drill 2021

- Organized the 9th Cyber Drill for Arab countries and the member countries of the OIC-CERT under the theme *Strengthening Cyber Security Readiness* on 28 Sep 2021

Organized The 9th Arab Regional & OIC-CERT Cyber Drill 2021

- ITU-ARCC and OIC-CERT have jointly organized the 9th Regional

Conference & the OIC-CERT 13th Annual Conference, hosted by the NCA on 23-24 Nov 2021

13th Annual OIC-CERT conference and 9th Arab Regional Cybersecurity Summit

- Participation in the organization and arbitration of the Global Cybersecurity Award of the OIC-CERT

OIC-CERT Global Cybersecurity Award 2021

Achievements

Cybersecurity Programs

Consultation and Guidance

- 51 number of security consultations (technical and non-technical) were provided to various government agencies
- 108 hours was consumed to provide the consultation services
- The number of change requests received and dealt with reached to 99 requests

Consultations provided to academicians and researchers in the field of cybersecurity such as providing the necessary information for the preparation of research, statistics of threats and incidents that have been dealt with

- The number of requests received 23 requests
- The number of hours consumed to provide the service is 38 hours

Cybersecurity Innovation

- Participated in the Innovation Challenge 2.0, in cooperation with the Oman Arab Bank
- Created cybersecurity small and medium enterprises (**SME**s) database that includes 120 companies
- Developed a database that contains government and private agencies that support freelancing
- Organized the SAS Cybersecurity Accelerator Program (2nd batch)
- Organized virtual awareness workshop titled with *Freelancing in cybersecurity* and targeting academia and job seekers
- Organized *Out of the box* competition for the Ministry of Transport, Communications, and Information Technology (**MTCIT**) employees
- Organized *Innovate Oman Program* in partnership with the UK Digital Hub in Oman, and in cooperation with Plexal and Cylon

Cybersecurity projects

- Delivered 7 awareness workshops in cybersecurity for the government entities
- Conducted an awareness session about *e-mail security* for the government sector
- Organized a specialized training program for tax authority employees

on the skills of dealing with the Internet and networks
- Organized a specialized workshop in cybersecurity for government sector employees in Aug 2021
- Conducted a session entitled *Countering Cyber Attacks* for MTCIT employees on 14 Apr 2021
- Delivered 2 virtual awareness workshops on cybersecurity and electronic extortion. The workshops targeted the employees of the Ministry of Agricultural Wealth, Fisheries, and Water Resources on 4 May 2021
- Participated in a discussion paper on electronic extortion and smart phone applications for members of the Al-Samoud Base Special Forces in Sep 2021

Cybersecurity Awareness sessions for schools

- Delivered 3 awareness sessions to the students

Participation in TV and radio programs

- Conducted 4 TV and 7 radio interviews giving awareness about cybersecurity
- Organized an awareness month on cybersecurity under the slogan *Be Tech-Smart* in cooperation with Al-Shabiba Radio, focusing on several main pillars
- Smart technology and overcoming the art of hacking
- Innovation in cybersecurity and the future of digital technologies
- The importance of developing competencies in cybersecurity

Cybersecurity events

- Organized the International Safer Internet Day with participation of 130 governmental and educational institutions
- Organized a cybersecurity workshop for job seekers (independent services)
- Hosted and organized a virtual symposium entitled *Trends in innovation and development in cybersecurity* targeting talented youth and SMEs on 19 Apr 2021
- Conducted a workshop entitled *Impacts of the Pandemic on Digital Societies: The Rise of Smart Cyber Crimes* targeting students and employees of the University of Nizwa
- Delivered a workshop in cooperation with the College of Sharia Sciences in the Governorate of Muscat
- Organized the 7th National Cyber Drill
- Participation with worksheets in 6 virtual events
- Delivered a working paper on cybersecurity at a regional conference - *IDC IT Security Roadshow* on 24 May 2021
- Participated in COMEX 2021, by delivering a presentation in cybersecurity virtually on 30 May 2021
- Participated in a working paper on the importance of cybersecurity considering the development of electronic applications, at the Arab Virtual Forum for Innovation and the Future, on 2 May 2021
- Participated in presenting a working paper in a virtual discussion session

on keeping pace with cybersecurity with technological development in the 13th Annual Conference of OIC-CERT

- Delivered 3 virtual workshops on: cybersecurity, protecting children on the Internet, and electronic extortion, as part of the activities of the workshop program and the participation of the MTCIT in (COMEX 2021) during the period from 30 May to 8 Jun 2021

Managing Cyber Risks and Incidents

- Mitigating 1,300 security incidents by the team, which targeted governmental, private institutions and individuals
- 29,331,939 the number of attempts of cyber-attacks in cyber space, deliberate on the networks and systems
- Conduct 10 comprehensive security assessments for government agencies
- Conduct 111 security assessments for government websites
- 10 security vulnerabilities were discovered and reported from the government agencies
- 610 security vulnerabilities were discovered in the government websites
- The team at the National Laboratory for Digital Forensic dealt with 103 digital cases, which included 367 digital evidences from computers, mobile phones, and external storage disks

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The Oman National Computer Emergency Readiness Team (**OCERT**) was established in 2010 to serve as a trusted focal point of contact on any ICT security incidents in the Sultanate of Oman focusing on cyber safety and security, capacity building, and promoting cybersecurity awareness to serve the public and private sector organizations, Critical National Information Infrastructure (**CNII**) as well as individuals

Resources

- CNII Protection team
- Cybersecurity Programs 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 Cybersecurity Centre team

Launched the 5G Security Working Group during in collaboration with Huawei

Participating in the ITU Interregional virtual Meeting for Americas and Arab Regions

The 9th Arab Regional & OIC-CERT Cyber Drill 2021

PAKISTAN

National Response Centre for Cyber Crimes (NR3C)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- Served as OIC-CERT 5G Security WG Member
- Online participation in the OIC-CERT training on *Browser Security*
- Online participation in the OIC-CERT training on *Data Classification of Confidential Data*
- Online participation in the OIC-CERT training on *Global Digital Security and Forensic in the New Norm*
- Online participation in the OIC-CERT training on *Utilizing NG-SIEM to Secure Your Environment (LogRhythm)*
- Online participation in the OIC-CERT training on *Phishing Emails Incident Response*
- Online participation in the OIC-CERT training on *Physical Security*

- Online participation in the OIC-CERT training on *EG|CERT Medico Governmental Case*
- NR3C focal person participated in a Conference *Cybersecurity in 21st Century* held at the Institute of Management Sciences Peshawar
- FIA CCW participated in the OIC-CERT Webinar 2021 *Data Breach: Mitigation and Lesson Learned*
- FIA CCW participated in the OIC-CERT 2021 Cybersecurity Drill.
- FIA CCW speaker delivered lectures in a conference on Cybersecurity in 21st Century at the Institute of Management Sciences (IMSciences) Peshawar
- FIA CCW Officer participated in the OIC-CERT workshop 2021 on *Malware Traffic Analysis*

Achievements

Muhammad Akram Mughal, Deputy Director of Network Security FIA Cyber Crime Wing (NR3C) contributed in the development of the OIC-CERT 5G Security Framework as a focal person of FIA CCW at the OIC-CERT and an active member of OIC-CERT 5G Security WG

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The National Response Centre for Cyber Crimes (**NR3C**) is the Cyber Crime Wing (**CCW**) of the Federal Investigation Agency (**FIA**). This is a law enforcement agency dedicated to fight cyber-crimes in Pakistan

The inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in the society

It is the only legitimate agency in Pakistan to investigate cyber-crimes and to interact with international law enforcement and cybersecurity bodies

NR3C has expertise in digital forensics, technical investigation, information system security audits, penetration testing and trainings

NR3C since its inception has been involved in capacity building of the officers of police, intelligence, judiciary, prosecutors, and other relevant government organizations. NR3C has also conducted many seminars, workshops and training/ awareness programs for the academia, print/ electronic media, and lawyers

Pre-defined objectives of FIA CCW (NR3C) are

- Digital Crime Investigations
- Information Security Audit
- Advisory Role on Information Security
- Research & Development
- Forensic Analysis of Digital Devices
- Capacity Building and Awareness of Government Departments and Academia
- Investigation & Prosecution of Hi-Tech Crimes

FIA CCW (NR3C) received 16,122 cyber security and cyber-crimes complaints in 2018

FIA CCW (NR3C) received 48,301 cybersecurity and cyber-crimes complaints in 2019

FIA CCW (NR3C) received 94,764 cybersecurity and cyber-crimes complaints in 2020

FIA CCW (NR3C) received approximately 102,356 cybersecurity and cyber-crimes complaints in 2021where 23% of the complaints are Facebook related

The average number of complaints received per month has doubled in just four years

According to official data, 32% of the complaints in 2021 were reported by students, while 25% of them pertained to financial crimes

FIA CCW (NR3C) year wise performance summary is presented in Figure 4

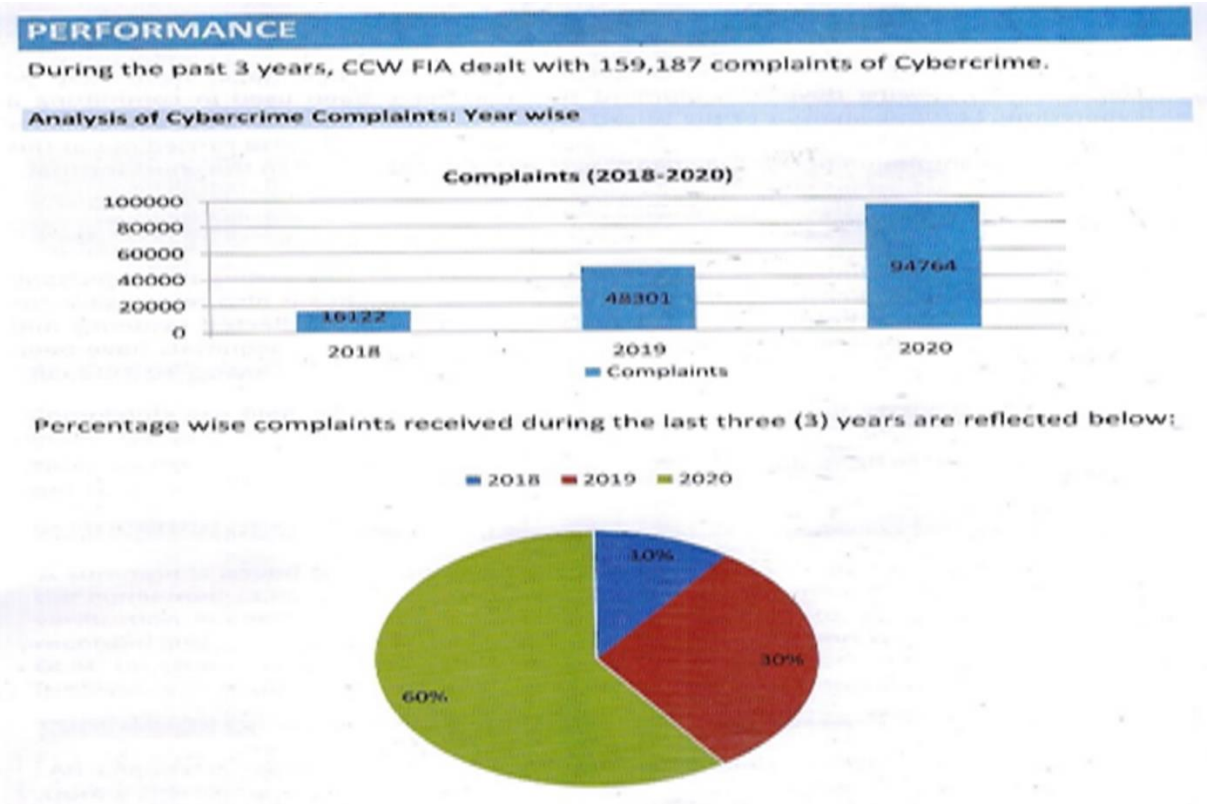


Figure 4 Summary of NR3C performance

FIA CCW (NR3C) received the categories of complaints as shown in Figure 5. It also provides some statistical analysis of each category of cybersecurity and cyber-crimes complaints

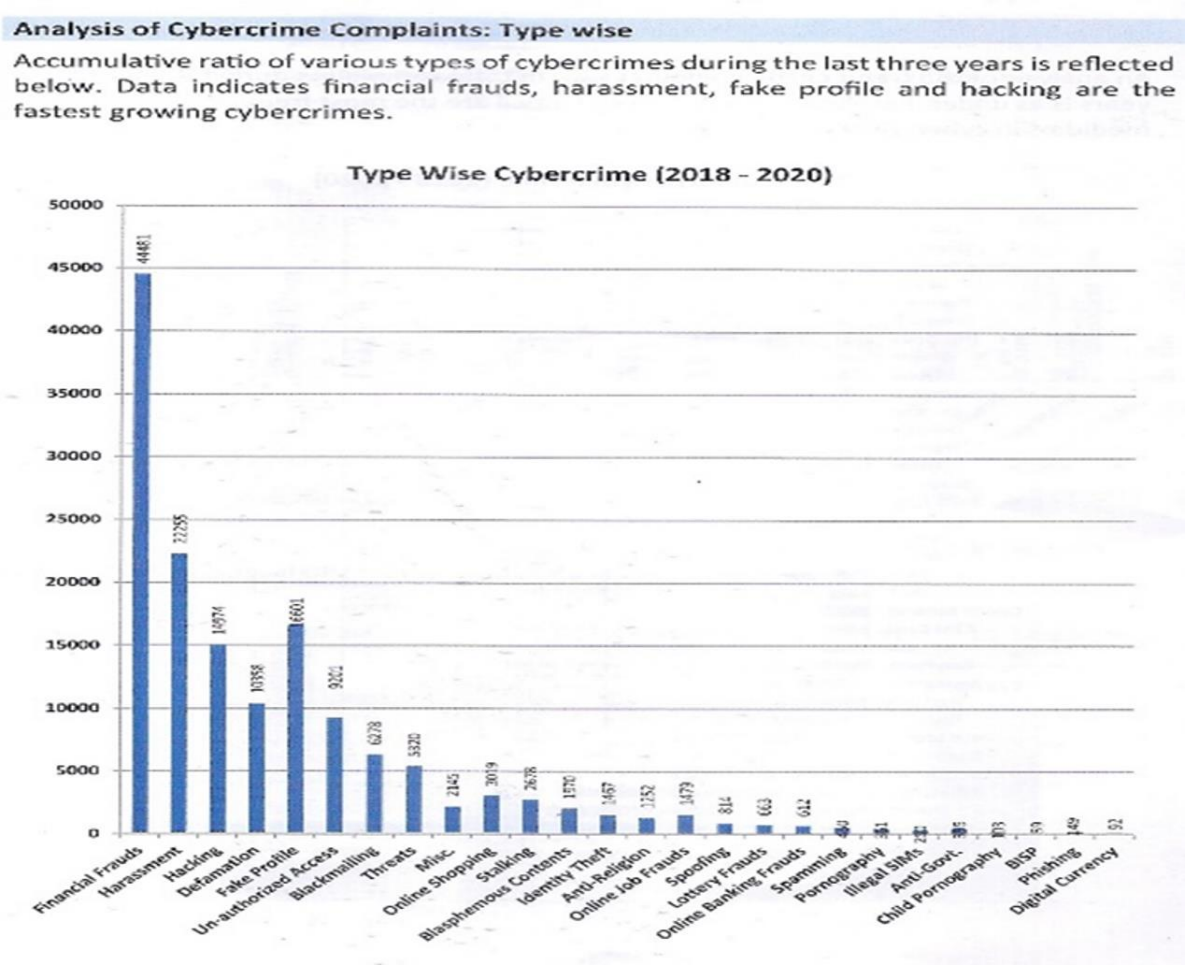


Figure 5 Type of cyber-crime complaints received

Establishment

- NR3C was established in 2007 as the Project
- All officers and the manpower of NR3C was regularized in 2012
- All officers inducted in phase-II of NR3C are in the process of regularization (permanency)
- NR3C's inducted officers in Phase-III are serving as the employees of the Project

Resources

DG of FIA chairing a meeting on FIA CCW performance

NR3C is a state-run wing of the FIA. Resources required to meet the organizational objectives are provided

by the state. Resources allocated/ allotted by the state are financially sponsored through the agency's budget or through the Public Sector Development Programme (PSDP) funded project. In either case NR3C is a state-run organization of Pakistan

DG of FIA briefing on FIA CCW performance

Resources are allocated to meet the organizational objectives. NR3C is a state-run organization and promotes the interests of the State of Pakistan at the national and international level. The NR3C is a full member of the OIC-CERT since its inception in 2009. Therefore, the objectives of NR3C are aligned with the objectives of the OIC-CERT. The total manpower of NR3C comprises of 477 well trained staff

Constituency

Pakistan public, national, and international domain

ACTIVITIES & OPERATION

Events organized by the organization/ agency

- FIA CCW organized seminar on prevention of cyber-crimes
- Launching of the *Cyber Crime Risks, Prevention and Legal Remedies Guidelines* for cyber users
- Launching of awareness campaign by cyber-crime wing. Fifteen (15) teams formed in 15 cyber-crime reporting centres across Pakistan
- FIA CCW participated in the Webinar on *Internet Infrastructure Security and Information Sharing* that was organized by the ARCC and Centre for Humanitarian Dialogue Switzerland
- FIA CCW Peshawar imparted training on Open-source Intelligence (OSINT) to technical officers of the Special Branch Khyber Pakhtunkhwa (**KPK**) Pakistan
- FIA CCW Peshawar imparted training on National Cyber Crime Laws to Deputy Superintendents of Police (DSPs) of KPK Pakistan

Events involvement

- Honourable Director General (**DG**) of FIA addresses the inaugural ceremony in MUET on *International Multitopic IT Conference*
- Honourable DG of FIA participated in INTERPOL conference in Istanbul, Turkey (TR)
- Signing ceremony of an MoU between FIA and the National University of Science & Technology (**NUST**) Islamabad

MoU signing ceremony between FIA CCW & NUST Islamabad

- Federal Ombudsman developed a policy to strengthen the law to control cyber-crimes against children
- Officers of the Basic Military Police (OBMP-124) and Crime Investigation & Detective Course (CIDC-61) call on the DG of FIA, Dr. Sanaullah Abbasi
- Reforms in the FIA Cyber Crime Wing
  - Establishment of a special unit for monitoring & supervision
  - Capacity building and awareness campaign
  - Upgradation of the digital forensic laboratories
  - Human Resource Development (1100 new posts sanctioned).
- A two-day workshop on data collection, management, research & analysis skills by the United Nation Office on Drugs and Crime (UNODC) in FIA Karachi
- Honourable DG of FIA visited the National Radio Telecommunications Corporation Headquarters and showed interest in using their products in FIA CCW. Both Organizations agreed on collaboration in capacity building and hi-tech tools
- Established cooperation between the Nadirshaw Eduljee Dinshaw (NED) University's Cyber Security Centre and FIA CCW
- National Cyber Security Policy of Pakistan was approved and released
- FIA CCW participated in 1st AfricaCERT Cyber Drill

Delegation from NCSC visited FIA HQ, Islamabad

Achievement

FIA CCW (NR3C) Pakistan received and processed 102,356 cyber-crime complaints in 2021

A total of 1,202 cases were registered against cyber criminals under relevant sections of the Prevention of Electronic Crimes Act and over 1,300 suspects were arrested

Financial fraud and forgery topped the list as 427 FIRs were registered and 388 arrests made in this category, followed by the offence of extortion and blackmailing under which 267 cases were registered and 185 people arrested

FIA took new initiatives as the agency introduced e-investigation, getting record and testimony online like email and video calls with security checks, just to provide relief to the common man

Established cyber-patrol unit in FIA CCW (NR3C), particularly in areas of organized crime, pornography, crime against children, women, minorities, and marginalized segments of society

2022 PLANNED ACTIVITIES

- Planning to open a cyber-wing in every district
- To strengthen cyber patrol unit in FIA CCW
- To regularize contractual manpower of FIA CCW
- To conduct seminars on cyber-crime laws, digital forensics, and cybersecurity at all major universities in Pakistan

Pakistan Information Security Association (PISA)
(General Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

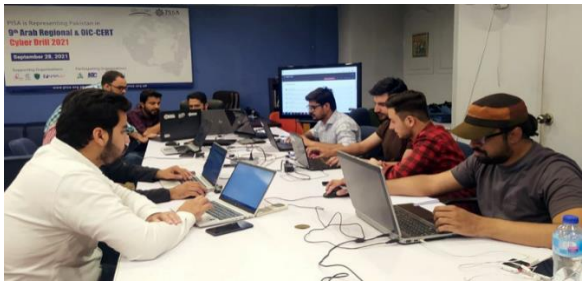
- Silkroad International Conference – 23 Mar 2021

Silkroad International Conference

- International Cyber Security Session by Team Cymru, PISA & CSAP – 28 Jun 2021
- Egyptian Digital Forensic Session, *Medico Governmental Case* by Egypt Government CERT – 28 Jun 2021
- *Data Breach: Mitigation and Lesson Learned* by NCCA of the Republic of Indonesia – 29 Jun 2021
- 1st African International Cyber Drill 2021 – 30 Jun & 1 Jul 2021

1st African International Cyber Drill 2021

- *Need to Build the Capacity of Public and Private Sector Organizations in Developing their Own CERTs, Working with their Sectorial CERT and Communication with National CERT of Pakistan and International CERTs* – 12 Aug 2021
- *Cyber Security as a Part of Sustainable Defence of Pakistan* – 6 Sep 2021
- 9th Arab Regional and OIC-CERT Cyber Drill – 28 Sep 2021



9th Arab Regional & OIC-CERT Cyber Drill

- Conference on *Cyber Security in the 21st Century* – 11 Nov 2021
- *Tracking the Criminals in Cyberspace*, Police Training College Hangu – 9 – 10 Dec 2021
- *Role of CERTs for Cyber Security of National Assets* – 16 Dec 2021

Tracking the Criminals in Cyberspace, Hangu Police Training Centre

- *Tracking the Criminals in Cyberspace*, Punjab Police –19 – 29 Dec 2021

Tracking the Criminals in Cyberspace, Punjab Police

Achievements

In 2021 PISA has completed the following target

- Participated in the International Cyber Drills
- Conducted Seminars/ Workshops on Cyber Security
- Participated in National and International Competition (CTF/ CyberLympics).

Several students and professionals (Universities, law enforcement) have been trained in cybersecurity and information security by PISA

Tracking the Criminal in Cyberspace, Punjab Police

1st African International Cyber Drill

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The Pakistan Information Security Association (**PISA**) is a Not-for-Profit organization working in the information security domain at different levels nationally and internationally. PISA is working with all the relevant stakeholders from the public and private organizations for educational interaction opportunities that enhance the knowledge, skill, and professional growth of the members

The primary goal of PISA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources.

PISA facilitates interaction and education to create a more successful environment for global information systems security and professionals' involvement

Establishment

PISA was establishment in 2005

Resources

- Information Security Experts
- Cybersecurity Experts
- Digital Forensic Experts
- Incident Response Experts
- Penetration Testing Experts
- SOC Specialists
- Information Security Management
- Network Security Specialist

Constituency

Pakistan

ACTIVITIES & OPERATIONS

Events organized by the organization/ agency

- Tracking the Criminals in Cyber Space for Law Enforcement
- Conference on Cybersecurity in the 21st Century for University
- Role of CERTs for Cybersecurity of National Assets for CERTs

Events involvement

- Cyber Security Changing Paradigm, Artificial Intelligence for National Security in Hybrid Warfare
- Participated in International African 2021 Cyber Drill
- Participated in OIC-CERT Cyber Drill
- Represent Pakistan in the OIC-CERT 13th Annual Conference 2020

Achievement

In 2021 PISA have achieved all targets set in 2020. Participated in the international cyber drills and successfully organized seminars and workshops. Provide services to law enforcement, public and private sectors in the following

- Guidelines to minimize Threats of Ransomware
- Identifying and responding to server-level threats
- Security assessments of different infrastructures
- Responding to the cyber incidents

2022 PLANNED ACTIVITIES

- Planned to organize Cyber Secure Pakistan (CSP) International event
- Planned to organize a mega event on Cybersecurity on 21st Century Silk Road (Belt & Silk Road Initiative)
- Planned to organize in-house cyber security drills
- Planned to participate in the International Cyber Security Drills, Capture the Flag (**CTF**) competition, CyberLympics
- Planned to organize cybersecurity/ information security seminar, workshops for universities, government, and private sectors

SOMALIA

Somalia Computer Emergency Response Team Coordination Centre (SomCERT/ CC)

(Full Member)

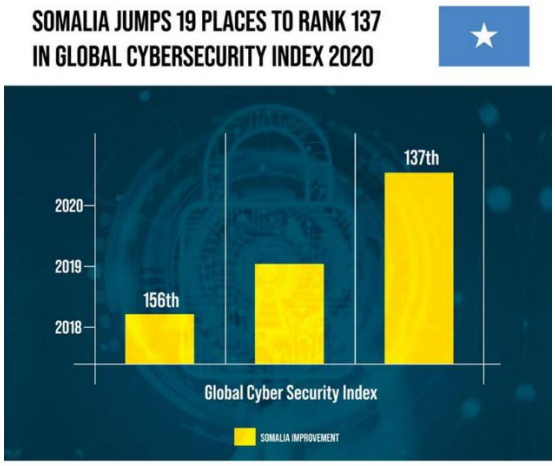
HIGHLIGHTS OF 2021

Summary of Major Activities

- Serve as a trusted point of contact at national level
- Provide cybersecurity incident handling
- Develop policies, procedures, and guidelines
- Provide advice to our constituencies
- Manage and release cybersecurity alters
- Collaborate with the local and international CERTs
- Provide cybersecurity training and awareness

Achievements

- Developed 3-year training and capacity building plan
- Somalia was ranked 137th position in 2020 from 156th in 2018 in the ITU Global Cybersecurity Index (**GCI**)



Somalia's rank in UN's Global Cyber Security Index jumps to 137th in 2020 from 156th in 2018. Somalia ranked 28th in Africa Region, 19th in the Arab States Region, and 137th globally out of 194 countries on ITU Global Cybersecurity Index 2020. Since 2017, #Somalia has been working to put in place legal, regulatory and policy framework in ICT, particularly in cybersecurity.

- Somalia was ranked 28th in the Africa Region and 19th in the Arab Region
- Published the Cybersecurity Capacity Maturity Model (CMM) report of Somalia in collaboration with Cybersecurity Capacity Centre for Southern Africa (C3SA) and Global Cyber Security Capacity Centre (GCSCC) *https://gcscc.ox.ac.uk/cmm-reviews*
- Provided Cybersecurity Awareness training during the Girls in ICT week in collaboration with the Ministry of Communications & Technology (MoCT) and Jamhuriya University of Science and Technology (JUST)

- Participated in developing the documents below with the OIC-CERT 5G Security Working Group

- Part I: Global 5G risk Register and Dictionary
- Part II: Baseline Security Technical Specification
- Part III: Cross-recognition Assurance Methodology

- Attended the GITEX - Global Cyber Security between 17-21 October 2021 at World Trade Centre, Dubai, UAE (AE)
- Participated the Africa Cyber Experts (ACE) Community Consultation Meeting 22 - 24 Nov 2021, The Hague, Netherlands (NL)

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The Somalia Computer Emergency Response Team/ Coordination Centre (**SomCERT/ CC**) is the first national CERT in Somalia. SomCERT/ CC provides cybersecurity incident handling, promoting cybersecurity awareness as well as coordinating cybersecurity issues. SomCERT/ CC collaborates with the government agencies, organizations, telecom operators, CNII providers, academia, ISPs, and other relevant entities to handle cybersecurity incidents in Somalia and various cybersecurity initiatives worldwide. SomCERT/ CC provides timely warning, support, and advisories to all its constituents in preventing and handling cybersecurity incidents

SOMCERT
Somalia Computer Emergency Response Team

Establishment

SomCERT/ CC was established in 2019 by the National Communications Authority of Somalia, as a section under the Cyber Security Department with the objective of securing Somalia's cyberspace and providing an official point of contact to handle cybersecurity incidents for the Internet community

Resources

- Incident Handling and Response Team
- Cybersecurity training and awareness team
- Information Sharing team
- International Coordination team
- Cybersecurity Awareness Campaign Team

Constituency

- Ministries and government agencies
- Law enforcement agencies
- Regulatory bodies
- National defence
- Banks and finance
- ICT, ISP, and telecommunication providers
- Academia
- CNII operators

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

- Provided training about *Incident Handling and Response Process* to the ICT departments of the government institutions
- Conducted Cybersecurity awareness campaign program to the government officials
- Facilitated Girls in ICT Week

- Facilitated and sponsored Somali Network Operators Group (SomNOG5) workshop

Events involvement

- SomCERT/ CC and the National Communications Authority of Somalia hosted the annual celebration of Girls in ICT Day in April 2021 to empower & encourage girls and young women to embrace careers in the growing field of ICT in collaboration with the academia

- Participated in the 9th Arab Regional Cyber Drill 2021 organized by the ITU's Arab Regional Cyber Security Centre (ITU-ARCC) and the 13th Annual Conference 2021 hosted by the NCA of the Kingdom of Saudi Arabia (virtually)
- Participated in the Directorate of National Statistics (DNS) and Internet Corporation for Assigned Names and Numbers (ICANN)- *An introduction to Unique Identifiers and the ICANN Ecosystem* hosted by the United States Telecommunications Training Institute (USTTI) (US)
- Attended the ITU Global Cyber Drill 2021
- Participated in the online training *Data Classification* 27 Jul 2021 hosted by aeCERT
- Participated in FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions, 7-9 Dec 2021

2021 PLANNED ACTIVITIES

- Improving the current National CERT and enhancing the existing capabilities of SOMCERT/ CC
- Develop the National Cybersecurity Strategy and Policy

- Develop Cybersecurity and Cybercrime Legislation
- Develop the National Guidelines for the Protection of National Critical Information Infrastructure
- ISO 27000-series or similar cybersecurity certification for SomCERT/ CC
- Assessment for establishing a cyber forensics laboratory for law enforcement, with estimates and technical specifications
- Establishing the School of Cybersecurity

SYRIA ARAB REPUBLIC

Information Security Centre (ISC)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

Information Security Centre

Background

It is the main centre in the National Agency for Network Services. This centre is the Syrian organizational unit responsible for setting specifications, standards, and all documents related to the security and protection of information and networks. This comprises of websites, best practices and compliance, conducting the necessary and possible research and tests to ensure safe and appropriate working environment, and setting standards for implementing CSIRT to response to emergencies on the network. This include taking all possible preventive and remedial measures and managing work teams to address them

The Information Security Centre performs its tasks and activities through the following departments

- Network and Computer Systems Security Department
- Research Department
- Information Emergency Response Department

The major activities in 2021 was

- Vulnerabilities Assessment - 153 websites, web applications and systems
- Penetration Testing - 44 websites, web, systems, and mobile applications
- Emergency Response - 56 responses
- Workshops - 2 national workshops
- Awareness - 9 awareness plans for both technical and non-technical people
- Approval of new security equipment - 7 approves

These tasks were performed by the local specialist technical team of the Information Security Centre with the professional and standard methods including the related detailed reports

Achievements

- Perform all the initial needs to implement the National Syrian CSIRT
- Successfully prevent many incidents and mitigate the risk of several others
- Managed to arise the security awareness throughout the country
- Document of over 700 vulnerabilities base on the assessments done
- The centre's team has been trained on several important technologies in the field of information security

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The National Agency for Network Services mainly works on regulating the electronic signature services, developing the Syrian CSIRT, managing domain names on the Internet under the two Syrian domains (sy., .Syria), and regulating the use of digital Internet addresses (**IP**s) for computer networks in Syria. In addition, the centre also regulates development of local smart devices applications according to the Syrian cybersecurity national regulation

The centre also oversees everything that would provide an enabling environment for advanced electronic services that contribute to the growth of the national economy and digital transformation

Establishment

The National Agency for Network Services was established under Law No./4 /25 Feb 2009, to organize and coordinate and facilitate work on the information network

Resources

The National Agency for Network Services is a Syrian national authority under the supervision of the Minister of Communications and Technology

Constituency

The National Agency for Network Services undertakes the implementation of Syrian national projects in the fields of information

technology, advanced computing, and national information security

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

- Syrian Capture the Flag (**CTF**) competition

Events involvement

- Modern Cyber Security Regional Conference in Beirut - 22 Jun 2021

2022 PLANNED ACTIVITIES

- Implement the national Syrian CSIRT
- Raise the technical level of the staff through advanced qualitative courses and practical training cases
- Conducting and publishing several advanced research in various fields of information security
- Supervising and following up the preparation and development of relevant security policies in government entities
- Follow up on disseminating information security methodology to government agencies
- Participation in the national and regional events in the fields of information security
- Preparing and presenting workshops in the fields of information security
- Carrying out the tasks of security awareness, early warning of information risks, and security advice
- Providing security assessment, penetration testing, and emergency response services

TUNISIA

National Agency for Computer Security (TunCERT)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- FIRST & AfricaCERT Virtual Symposium for Africa and Arab Region
- National Cyber Drill 2021
- 1st Forum of CERTs and Tunisian SOCs
- October cyber

- Convention National Agency for Computer Security (ANSI[4])/ Institute of Higher Management (**ISG**[5])
- Tunisia Digital Summit

Achievements

- Signature of a contract of collaboration between the National public and private CERTs and SOCs
- A partnership for a master's degree co-constructed with the ISG entitled *Information Systems Security* has been signed

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The National Agency for Computer Security (NACS) (**TunCERT)** carries out general supervision over computer systems and networks appropriated to the diversified public and private organization

Establishment

Law N°5 of 3 Feb 2004 relating to computer security and to the organizations in the field of computer security and laying down the general rules for the protection of computer systems and networks

Resources

75 employees

Constituency

National private and public

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

- FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions
- National Cyber Drill 2021
- 1st Forum of CERTs and Tunisian SOCs

Events involvement

- Plenary sessions and technical workshops in FIRST and AfricaCERT event
- Panel of discussion in Tunisia Digital Summit Event

Achievement

- Signing of chart of consortium between Tunisian CERTs and SOCs
- A partnership for a co-constructed master's degree with ISG

2022 PLANNED ACTIVITIES

- Bug Bounty
- Tender of TunCERT website
- Tender for the Massive Open Online Courses (**MOOC**)

[4] *Agence Nationale de la Sécurité Informatique en Tunisie*

[5] *Institut Superieur de Gestion*

TURKEY

National Cyber Security Incident Response Team (TR-CERT)

(Full Member)

HIGHLIGHTS OF 2021

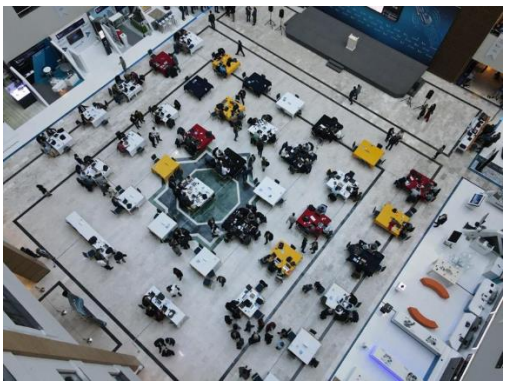
Summary of Major Activities

- Turkey, according to the ITU GCI data used to measure the maturity of countries in cyber security, ranked 6th from 11th in Europe in 2020, and 11th from 20th in the world has achieved success in ranking
- The *National Cyber Shield 2021 Exercise* was held on 12-13 Oct under the coordination of the Ministry of Transport and Infrastructure and hosted by the Information and Communication Technologies Authority (**ICTA**). 135 participants from 36 public institutions and organizations, private sector representatives, and guests participated in the exercise

- The CNA (CVE Numbering Authorities) acceptance process has been completed by TR-CERT. Thus, TR-CERT assigns CVE numbers for security vulnerabilities of third-party software, hardware, and products produced and used in the country. As CNA, the agency also provides process coordination in vulnerability management

Achievements

- 36,761 malicious links (URL, IP, domain) used by malwares and for phishing has been identified, controlled, and blocked from accessing the infrastructure
- 11,656 cybersecurity notifications have been made to the institutions/ organizations/ enterprises
- 5,881 cybersecurity experts from 2,025 CERTs registered with TR-CERT, are coordinated through the CERT Communication Platform established within the organization of TR-CERT
- The FETIH Cyber Training Centre project and applied cybersecurity training laboratory infrastructure works have been completed within the body of TR-CERT, and cyber training and camp activities are organized. With these activities, which have become regular and routine in this framework, it is aimed to train cybersecurity experts in an integrated manner with the ICTA Academy within the body of ICTA and to increase the trained human resources of the country in this field. As of the end of 2021, within the scope of the studies carried out by TR-CERT, online training was given to 3,692 people working in CERTs
- Cooperation activities continue with countries and international organizations in the field of cybersecurity. TR-CERT is a member of organizations such as FIRST, Trusted Introducer (**TI**), Cybersecurity Alliance for Mutual Progress (CAMP), NATO Malware Information Sharing Platform (NATO-MISP). Recently, membership procedures to the OIC-CERT have been completed. Threat intelligence sharing activities with these organizations are continuing. In addition, on behalf of the country, TR-CERT and ICTA contribute to the activities of organizations such as the UN, ITU, NATO, Group of Twenty (G20), Organization for Security and Co-operation in Europe (OSCE), and Organization for Economic Co-operation and Development (OECD) in the field of cybersecurity



ABOUT THE ORGANIZATION/ AGENCY

Introduction

- National Computer Emergency Response Centre (USOM[6], TR-

[6] *Ulusal Siber Olaylara Müdahale Merkezi*

CERT) has established within ICTA to determine threats against national cybersecurity, take measures for reducing or eliminating the impact of cyber-attacks and share information with the defined actors

- The mission of TR-CERT is to protect the Turkish government's cyberspace, along with the critical infrastructures, both public and private, such as the energy production and distribution, water management, telecommunication institutions, and facilities in Turkey

Establishment

TR-CERT was established on the 27 May 2013 within the ICTA, in accordance with the 4th. Clause of the National Cybersecurity Strategy and 2013-2014 Action Plan (Turkish: Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı) issued by the Cabinet of Turkey and published in the Official Gazette of the Republic of Turkey

Resources

TR-CERT benefits from the resources of ICTA which is the national regulatory authority of the Turkish electronic communication sector and has a special governmental budget for national cybersecurity activities

Constituency

TR-CERT is the national CERT of Turkey and its constituency covers the whole country including the public and private sector and also individuals

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

Five (5) national and two (2) international cybersecurity exercises have been carried out under the coordination of our Ministry since 2011, as part of the important steps taken to increase the level of preparedness and incident response capabilities both in the institutions and organizations and at the national level. Finally, the *National Cyber Shield 2021 Exercise* was held on 12-13 Oct under the coordination of the Ministry of Transport and Infrastructure and hosted by ICTA

Events Involvement

TR-CERT continues to participate and contribute to various international cybersecurity exercises such as NATO Locked Shields, NATO Cyber Coalition and NATO Crisis Management Exercise. Some of the other events attended are TR-CERT - CSIRT Advisory Meetings, Energy Sector CSIRTs Meetings

Achievement

- During the pandemic period, the local and national systems AVCI, AZAD, and KASIRGA using artificial intelligence technologies detected 750 fake conference applications and 46,784 weaknesses in remote management services
- With the Sinkhole application, institutions, and organizations accessing malicious links blocked by TR-CERT are detected and

informed. With regular scans on 16 million IP addresses by the ATMACA project, the risks of more than 600 vulnerabilities were proactively prevented

- 133 malware examinations and 612 malware information related to COVID-19 were shared with CERTs. 2,975 harmful droppers and command control centres related to COVID-19 have been blocked

2022 PLANNED ACTIVITIES

- Sectoral Cybersecurity Exercises will be organized
- CERT maturity model will be developed and implemented at national scale
- Cyber Star competitions and cybersecurity training activities will be going on

Turkcell Cyber Defence Centre (TURKCELL CDC)
(Commercial Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

In 2021, Turkcell CDC continued to offer new cybersecurity services for its corporate and individual customers

Threat Intelligence Service (Bozok)

- Turkcell CDC launched a threat intelligence platform called Bozok, which provides up-to-date indicator of compromise (IOC) information, threat actor reports, data leak detection, brand protection, and vulnerability detection services to its corporate customers

Turkcell CDC Bozok Threat Intelligence Service

- BOZOK TI infrastructure is powered by nearly 100 intelligence sources. CDC EYE, dark web, and threat intelligence forums, Pastebin, Github, Twitter, and Virus Total etc
- Detecting data leaks with automation and instant reporting, BOZOK enables the customers to take early action and include threat actor reports specific to advanced APT groups
- BOZOK detects newly opened domains and warns customers against phishing attacks

- It offers a Malware analysis interface to examine files that customers suspect
- Provides information about existing vulnerabilities with the vulnerability centre
- The number of customers increased by 650% in 2021, thanks to the works carried out in this context

Turkcell Security Operation Centre Service

- Turkcell offers a 7x24 SOC services to the customers with the mission of creating added value for the national cybersecurity and the vision of increasing cyber resilience by providing community cybersecurity
- Turkcell produces innovative ideas and develop quality products and services, and keeping customer satisfaction at the highest level
- Apart from the 24/7 monitoring service, there are various trainings by expert cybersecurity engineers to create cybersecurity awareness
- Turkcell provide the customers with monthly reports such as critical vulnerability notifications and security recommendations. As a result of these efforts, the number of our customers increased by 103% in 2021

Digital Security Services

- Turkcell Digital Security Service is a solution designed specifically for Turkcell's mobile internet users. As phishing & fraud attacks continue to become more sophisticated, persistent, and adapting to mobile security defences, demand for phishing & fraud defence solutions is at an all-time high
- Turkcell Digital Security Service ensures the users traffic uses only safe endpoints. This service alerts users for any suspicious connection attempts or links with the help of machine learning and artificial intelligence algorithms. The service also informs the customers, if they are using e-mail and social media accounts that have leaked passwords

Turkcell Security Orchestration, Automation and Response (SOAR) Service

Automation of Security Infrastructure - Turkcell SOAR Webinar 2021

- As a result of digital transformation, both the number of security vulnerabilities and threats to information technology systems are in an increasing trend. Turkcell CDC Security Engineers are experts in their fields and can respond to cyber incidents accurately and quickly using industry standard methodologies

- In this context, Turkcell CDC launched Turkcell SOAR for both Turkcell internal and SOC service customers for faster and safer action by the engineers

Mitre Att&CK Framework Compatibility and Purple Team

- Turkcell examine and test the tactics, techniques, and procedures of advanced attack groups as part of the efforts to comply with the Miter Att&CK framework, which is accepted all over the world
- Considering the motivations, Turkcell are developing rules to detect any anomalies in the systems. With this study, 557 new rules have been written with 90% compliance
- The Purple Team was formed to improve Turkcell's general security, optimize efficiency and effectiveness, and to maximize security
- The team imitate attacks made by advanced attack groups and current attack vectors
- Information and insights about corporate security are reported and shared with all security team managers monthly

Cyber Security Trainings

Various trainings are provided by Turkcell cybersecurity engineers, who are experts in their fields to increase the information security awareness of corporate customers at Turkcell CDC. These trainings are

- Cyber Security 101 and Phishing Training
- Threat Intelligence Training
- SIEM Management Training
- Windows Forensic Tutorial
- Malware Analysis Training

Signalling Security

Within the scope of the signalling security project, Turkcell created an alarm mechanism for anomaly detection with the analyses obtained by collecting electronic signalling traffic

Achievements

- Turkcell's 3 group of companies (Bip, Lifecell Cloud, and Turktell) received ISO 27001 certification for the first time.
- Turkcell CDC CTF teams participated in many Capture the Flag events in 2021 and ranked high. Some of these CTFs are
  - African Cyber Drill (1st place)
  - Battleware (4th place)
  - CTF EGCERT 2021 International Cyber Drill (1st place)

Turkcell Cyber Defence Centre

ABOUT THE ORGANIZATION/ AGENCY

Introduction

Turkcell is a converged telecommunication and technology services provider, founded and based in Turkey. Turkcell CDC is the Cyber Defence Centre of Turkcell. Turkcell CDC provides a variety of services in the information security domain at the national and international scale including threat intelligence, managed security operations centre, and digital forensics & incident response services

Turkcell CDC provides the Digital Security Service for individual Turkcell customers. With this service the customers are protected from various types of phishing and fraud attacks as well as credential leakage

Turkcell CDC is part of the Turkcell Cyber Security Directorate which provides other services in the Cybersecurity domain as well, such as sales, installations, and integrations of network security products, health check services for network security products; penetration and Distributed Denial of Service (**DDOS**) tests, and managed DDOS protection services

Establishment

Turkcell CDC is established in Dec 2015

ACTIVITIES & OPERATIONS

Events Organized by the Organization/ Agency

TURKCELL GNÇYTNK CyberCamp – 2021

Turkcell GNCYTNK CyberCamp 2021

As Turkcell Cybersecurity teams, Turkcell organized the 4th CyberCamp training program in 2021, with 30 students selected from among 3,000 students on Information Security Management, Network Security, Cryptology, Identity and Access Management, Web Application Security, Network and Web Penetration Tests, and SOC Monitoring and Trainings. The camp was held for 2 weeks by Turkcell cybersecurity experts, covering Security Information & Event Management (**SIEM**), Incident Response, Cyber Threat Intelligence, Malware Analysis, and Windows Forensics. With the CTF competition and project assignments, the participants were able to reinforce what they learned

Events involvement

Turkcell CDC members gave presentations and trainings on various cybersecurity issues at Technology Talks, Information Security and Cryptology Conference, Information Security Association, IDC, KVK and Bilişim Summit conferences

Turkcell CDC attended the Turkey Cyber Security Cluster Week and made presentations on various topics such as BOZOK Threat Intelligence and Digital Security Service. Turkcell CDC also attended the CDC's Microfocus Universal Conference in 2021, where Turkcell CDC shared its experiences on the state-of-the-art distributed Extended Security Maintenance (ESM) infrastructure for customers purchasing SOC Service

Achievement

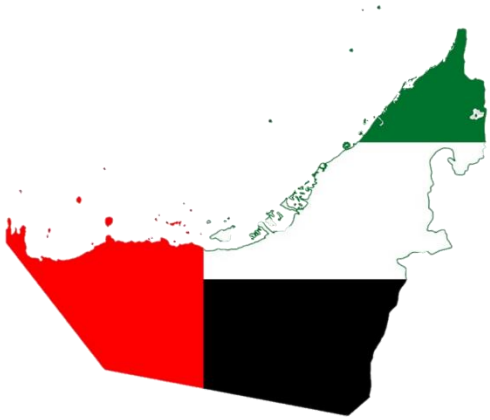
Turkcell group of companies (Bip, Lifecell Cloud, Turktell) received ISO 27001 certification for the first time. Turkcell CDC CTF teams participated in many Capture the Flag events in 2021 and ranked high. Some of these CTFs are: African Cyber Drill 1st place, Battleware 4th place CTF EGCERT 2021 International Cyber Drill 1st place

2022 PLANNED ACTIVITIES

- The Turkcell CDC Sense project is planned to be carried out in the first half of the year. The project to collect the attack activities of aggressive actors with the honeypot systems to be installed in data centres in different continents of the world and turn them into threat intelligence
- Reaching more foreign customers by improving overseas customer engagements
- Efforts to ensure early detection of any cyber-attack by integrating deception technology into the Turkcell network

Turkcell CDC Manager at the 14th Information Security and Cryptology Conference 2021

Turkey Cybersecurity Risk Map



UNITED ARAB EMIRATES

UAE Computer Emergency Response Team (UzCERT)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

Computer emergency response services

- 376 cyber incidents mitigated
- 1,196 sites were monitored against defacement
- Conducted two separate cyber drills covering over thirty federal entities, the cyber drills took place in September and November
- Enhanced and upgraded the aeCERT Advisory System

Cybersecurity awareness services

- 66 awareness sessions provided
- 3,313 people attended awareness sessions
- Raising community awareness of the risks related to the digital world
- Consolidate awareness messages about security best practices

- Building specialized national capacities at a high level of efficiency
- Distributed a cybersecurity awareness monthly packages including infographics, social media posts, and desktop wallpapers

Information quality services

- 12 vulnerability reports prepared
- 37 vulnerability assessment testing
- 35 penetration testing services
- Raw Source scanning service been initiated for federal entities. A coverage of software composition analysis, static application security testing, and interactive application security testing
- Enhanced and upgraded the Mobile Application Testing Lab (MAST), IOS/ Android support, User Interface (UI), and dashboard for entities and more

Compliance services

- Finishing the federal Artificial Intelligence (**AI**) project part 1
  - Release the AI Qualys System for UAE federal entities and registering 43 entities in the system
- Representing UAE in ISO27001 workgroup 1 - Meetings and votes
- Representing the Telecommunications and Digital Government Regulatory Authority (**TDRA**) as a technology expert in court cases

Achievements

- Two cyber drills completed with over a 90% satisfaction rate from the participants
- Enhanced the aeCERT Advisory System which increased the advisory output rate by more than 200%
- Certified ISO 27001 auditor
  - the full team have achieved ISO27001 certification from the British Standards Institution (**BSI**)
- Certified ISO 31000 auditor
  - three members from the team have achieved ISO31000 certification from BSI
- TDRA ISO27001 certification renewal
- More than 63 web applications pen testing/ scanning have been done
- More than 294 vulnerabilities been reported

ABOUT THE ORGANIZATION/ AGENCY

Introduction

https://www.tdra.gov.ae/aecert/en/home.aspx

The National Computer Emergency Response Team (**aeCERT**) launched several initiatives aiming to raise cybersecurity awareness and activate all initiatives that would spread awareness among different groups of society towards the importance of cybersecurity. aeCERT has been established to improve information security standards and practices, protect and support UAE ICT infrastructure from online risks and breaches, and build a secure and protected ICT culture. aeCERT goals include enhancing the cybersecurity law and assisting in the creation of new laws, enhancing information security

awareness across the UAE and building national expertise in information security, incident management, and computer forensics

The Section also provides consultation services to government entities regarding IT management and standards

aeCERT international participation

- Membership in OIC – CERT
- Membership in the Gulf Cooperation Council (**GCC**)- CERT
- Membership in ARCC
- Membership in ITU Child Protection WG
- Member of FIRST

Establishment

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

Resources

aeCERT services

- Computer emergency response services
  - Responding to computer emergencies in federal organizations
  - Providing cyber forensic services through aeCERT's Evidence Lab
  - Infrastructure monitoring services
    - SIEM infrastructure monitoring solution
    - Website defacement monitoring services
  - Providing technical tip documents
  - Anti-phishing email services
- Information quality assurance services
  - Vulnerability assessment services
  - Penetration testing services
- Cybersecurity awareness, guidelines, and training services
  - Federal entity awareness.
  - Public awareness
  - Awareness through the media

Constituency

- Governmental and Semi-Governmental entities
- Some of the private entities (especially banks)
- The Public
- Academic Institutions

ACTIVITIES & OPERATIONS

Events Organized by the Organization/ Agency

- The Protective Shield Cyber Drill – Sep 2021
- The Protective Shield Cyber Drill – Nov 2021

Events involvement

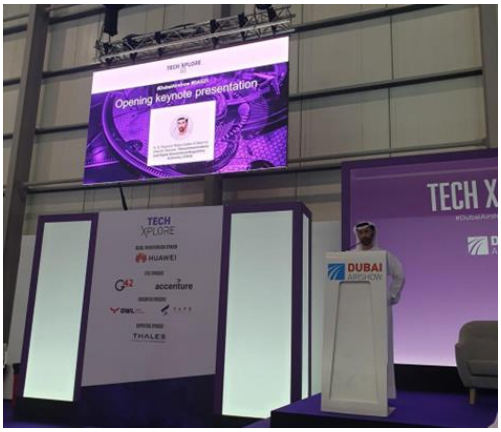
The team was responsible for organizing events including but not limited to vetting and choosing the vendor, overlooking the choice of scenarios, sending out invites, and confirming registrations

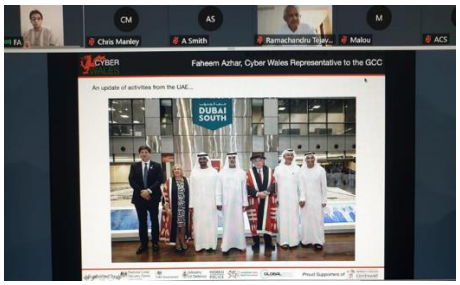
Achievement

- Eight (8) awareness sessions delivered for the OIC-CERT and GCC with the total number of attendees 2,893
- Provided ten (10) training workshops for information security professionals

2022 PLANNED ACTIVITIES

- Conduct a ransomware simulation assessment covering TDRA and federal infrastructure
- Conduct a CTF event for federal entities to hone their security skills
- Provide OIC-CERT with 4 awareness posters monthly which can be white label as end users' needs
- Conduct at least 2 awareness sessions for OIC-CERT





Huawei (HWT), Huawei Tech (UAE) FZ-LLC
(Commercial Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

Following are some of the key activities that Huawei has been delivering last year as part of the key strategy that prioritise security over business and addressing cybersecurity and privacy challenges and opportunities. This are done through management transformation, technological innovation, open cooperation, and fostering a better life for all in the future digital world by offering secure and trustworthy products, solutions, and services where personal data is lawfully used and always protected

Help customers manage security risks through technological innovation

Huawei continues to research, explore, and implement cutting-edge fundamental technologies, such as cryptography, AI trustworthiness, confidential computing, and differential privacy. Furthermore, Huawei accelerate the application of security technology solutions to products, and continue to introduce vulnerability mitigation, advanced threat detection, data protection, and other technologies into the ICT products, improving security and resilience. Take 5G base stations as an example, Huawei deploys a wide range of functions including software integrity check in the boot state, runtime software integrity measurement, and one-click security configuration check providing

security verification, hardening, and detection capabilities

Consolidate privacy governance to respect and protect user privacy

Huawei complies with privacy protection laws and regulations in the countries in which it operates. Since 2016, Huawei has established a unified privacy governance framework in accordance with the EU General Data Protection Regulation (GDPR). With successive personal data protection laws (such as the China's Personal Information Protection Law) being enacted and cross-border data transfer requirements being imposed in different regions/ countries, and has continuously improved the governance architecture and technical capabilities, and incorporated privacy protection and cross-border data transfer requirements into R&D, services, operations, and other aspects. Based on the governance architecture and processes, a series of IT tools and platforms are developed to improve compliance effectiveness and management maturity, and providing transparency, clear compliance processes, and results

Ensure privacy and security of HarmonyOS consumers

HarmonyOS is a next-generation operating system that can run on a wide range of smart devices. At the outset, Huawei emphasized the fundamental importance of consumer privacy and security and implemented a system security architecture and ecosystem management and control framework, to explicitly address these issues

With HarmonyOS, Huawei has built a security architecture for super terminals. It implements hierarchical device security management, trusted device connections, distributed access control, and a security collaboration platform to protect the security of consumers. Furthermore, Huawei has built a HarmonyOS application management and control framework to ensure that applications are protected throughout the lifecycle, including the development, commissioning, release, installation, and operational phases

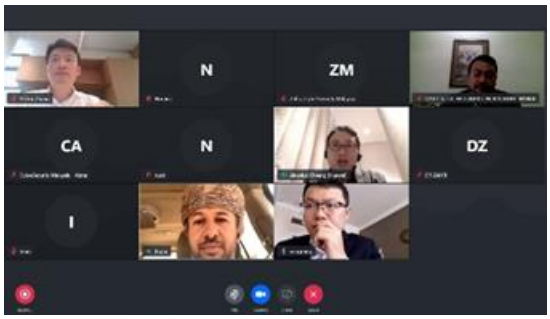
Strengthen cyber security risk management and capability building of the supply chain

Huawei has established a comprehensive ISO 28000 compliant supply chain security management system to identify and control security risks in the end-to-end process from incoming materials to manufacturing and delivery to customers. Huawei has developed industry-leading material security and trustworthiness specifications, security sourcing test standards, and supplier security and trustworthiness maturity standards. Suppliers must pass the security system certification and test before they are admitted

Achievements

- Huawei became a member of the OIC-CERT for the 1st year. Huawei has actively participated in the OIC-CERT 5G Security WG as a co-chair to develop a 5G cybersecurity framework for risk assessment and management, aiming to help member states improve their 5G cybersecurity management

capabilities. The OIC-CERT 5G Security Framework has been developed by multi-stakeholders in the OIC region to effectively identify and capture 5G security threat landscape, distinguish the shared 5G security responsibilities, define 5G security baseline technical specification references, and establish a harmonized and cross-recognized 5G security certification system among OIC member states



- Besides the 5G security working WG, Huawei had also contributed to the 13th Annual Conference and the 9th Arab Regional Cybersecurity Summit 2021 as a speaker
- During this event Huawei Saudi Arabia Rep Office has been honoured with the OIC-CERT Global Cybersecurity Award for 2021. In addition, Huawei was awarded the Middle East & Africa (**MEA**) Business Technology Achievement Awards 2021 during GITEX where Huawei was the winner of the Collaborations and Partnerships Award for the Cybersecurity Partnership with the OIC

- Meanwhile at the International level, in the UAE, Huawei deepened cooperation with the Cyber Security Council (**CSC**) and played an active

role in the construction of the local cybersecurity ecosystem and the improvement of the regional cybersecurity awareness and capabilities. Huawei won the *Cybersecurity Company of the Year* and *Cybersecurity CEO of the Year* awards

In Germany, Huawei supported the Federal Office for Information Security in the release of the AI Cloud Service Compliance Criteria Catalogue (**AI C4**) by providing relevant suggestions based on a use case pilot project. AI C4 is the industry's first security standard for an AI Cloud Service. In Dec 2021, HUAWEI CLOUD OCR service officially passed the AI C4 attestation conducted by an independent agency

In Malaysia, Huawei worked with the national cybersecurity specialist agency, CyberSecurity Malaysia and mobile telecommunications provider Celcom to build a 5G Security Test Lab (**My5G**) improving Malaysia's cybersecurity capabilities and preparing for 5G deployment. At the Cyber Security Malaysia Awards, Conference & Exhibition (**CSM-ACE**) in December, the Ministry of Communications and Multimedia Malaysia released My5G, and Huawei was awarded *Cyber Security Innovation of the Year* by CyberSecurity Malaysia

In Indonesia, Huawei renewed the MoU on cybersecurity with the National Cyber and Crypto Agency (BSSN), reaffirming commitment to the sharing of cybersecurity knowledge, and supporting the program of workforce development on cybersecurity and digital transformation

- Huawei increases investment in third-party independent verification. In 2021, Huawei obtained more than 70 cybersecurity certificates. For example, the 5G base station was the first to obtain NESAS[7]/SCAS[8] 2.0 certification in the industry; HarmonyOS obtained Common Criteria (ISO/ IEC 15408) certification

- Intelligent Automotive Solution Business Unit (IAS BU) was the first to obtain ISO/SAE 21434 certification for automotive cybersecurity; and digital power

[7] *GSMA Network Equipment Security Assurance Scheme*

[8] *5G Security Assurance Specification*

products obtained the IEC 62443 certificate

- In the mobile communications field, Huawei contributed more than 400 cybersecurity proposals to 3GPP[9] and GSMA[10], maintaining a longstanding industry-leading position. Huawei also submitted proposals on remote attestation security architecture, interaction model, YANG data model, and campus Internet of Things (IoT) device access security to international standards organizations, such as the European Telecommunication Standards Institute (ETSI), Internet Engineering Task Force (IETF), ITU-T[11], and Centre for Cyber Security (CCS). These are just some examples of the many continuous contributions made to the development of industry security standards
- For strengthening the supply chain security in 2021, Huawei conducted cybersecurity risk assessments of more than 4000 global suppliers and recorded, tracked, and rectified the issues identified. Huawei signed data processing/ protection agreements (DPAs) with more than 5000 suppliers and implemented privacy protection management requirements for suppliers to ensure compliance. Huawei also optimized the security baselines and verification processes for manufacturing and supply availability and implemented them in the production and delivery processes of new products
- Huawei has also deepened trustworthiness transformation to enhance software engineering capabilities and cyber resilience, and building secure, trustworthy, and quality products and solutions. In 2021, Huawei improved internal off-the-shelf components of trustworthy technologies and product design platforms and implemented the clean code mechanism to continuously improve code quality and to reduce vulnerabilities. Huawei also enhanced threat analysis and trustworthy design, bringing improvements to the security and resilience capabilities of products and solutions. In terms of continuous organizational optimisation, Huawei strengthened the integration and continuous construction of common security capabilities via corporate-level vulnerability management centre based on Product Security Incident Response Team (**PSIRT**) to enhance vulnerability management initiatives. Huawei also integrated the Trustworthiness Enabling Department and IT Equipment Department at the product line level to help implement software engineering capabilities through the IT systems

[9] *3rd Generation Partnership Project*
[10] *GSM Association is an industry organisation that represents the interests of mobile network operators worldwide*
[11] *ITU Telecommunication Standardization Sector*

ABOUT THE ORGANISATION/ AGENCY

Introduction

Huawei is a leading global provider of ICT infrastructure and smart devices. The company has more than 194,000 employees, and operate in more than 170 countries and regions, serving more than three billion people around the world

The vision and mission are to bring digital realm to every person, home, and organization for a fully connected, intelligent world. To this end, Huawei will drive ubiquitous connectivity and promote equal access to networks, bring cloud and artificial intelligence to all four corners of the earth providing superior computing power where you need it, when you need it; build digital platforms to help all industries and organizations become more agile, efficient, and dynamic; redefine user experience with AI, making it more personalized for people in all aspects of their life, whether they're at home, in the office, or on the go

Huawei has operated in the Middle East region for over 20 years now, with Bahrain as our regional headquarters. The UAE is the MEA business centre, where Dubai is one of the six global cybersecurity centres. Huawei has identified and prioritized cybersecurity since 2005 when the Huawei PSIRT is formed. PSIRT manages the receipt, investigation, internal coordination, and disclosure of security vulnerability information related to Huawei offerings and it is an important window to disclose the vulnerability of Huawei products. Huawei PSIRT became a FIRST member in 2010 and adheres to ISO/IEC 29147:2018. Subsequently Huawei published the first cybersecurity white paper in 2012, the second in 2013, the third white paper in 2014, and a fourth in 2016 and our most recent position paper in 2019

Establishment

1987

Resources

Huawei Trust Centre - *https://www.huawei.com/en/trust-center*

Huawei Cloud Trustworthiness Knowledge Base - *https://www.huaweicloud.com/intl/en-us/securecenter/resource.html*

Constituency

Huawei's customers in the global ICT eco-system that Huawei is a part of, covering over 170 countries and regions where Huawei provide products, services, and end-to-end solutions to carrier network clients, enterprise customers, government, and end-user consumers supporting them in their digital transformation journey

2022 PLANNED ACTIVITIES

While Huawei continuing to play an integral part as a responsible and contributing member of the global cybersecurity ecosystem, the company has the following major key initiatives

Deepen the cooperation and development with OIC in terms of cybersecurity

Specifically, based on the achievement of the current OIC-CERT 5G Security Framework, it is essential to establish task forces for adopting it in by the OIC-CERT member states. In detail, this task force would be very useful to convene local stakeholders to establish, control, and maintain local-preferred 5G security technical specifications and standards according to the original 5G security framework. In this way, the 5G boosted digital transformation could be well guaranteed

With the task force, the local 5G security certification system can be established. In most cases, according to the OIC-CERT 5G Security Framework, each certification system is harmonized and mutual recognized among the different countries. With the implementation of cloud computing and cloudification, it is also essential to establish a cloud security working group for a secure cloud development in the OIC region with a controllable, objective, cost effective, and technical manner. By now, such new association could be constructed along with the OIC-CERT 5G Security Working Group's experience

Continuously enhancing secure and trustworthy service operations

Huawei continue to invest in the development of IT-based capabilities for trustworthy operations and digitally ensure transparent and traceable network operations. The company set up an operations trustworthiness lab to strengthen interconnection with global standards organizations and cutting-edge research and continued to build capabilities to address future cyber security challenges. The data security management system for operator service support successfully passed the SOC2 external audit, proving effective lifecycle management of such data. At the same time, Huawei continued with the *Network Safety Day* campaign to increase cybersecurity awareness and risk control, working together with the customers to enhance cyber resilience

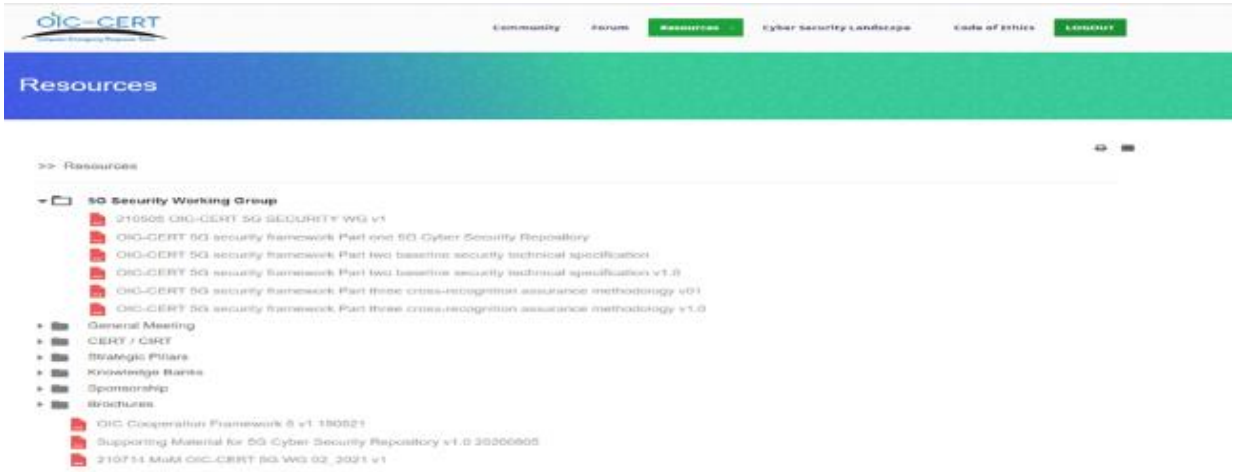
Steadily boosting awareness and professional capabilities among all employees

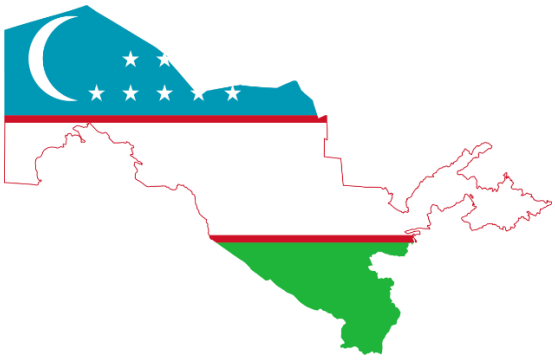
Huawei encourage employees continued participation in external professional cybersecurity and privacy protection certification programs. To date, more than 1,200 employees have obtained industry-recognized certifications, such as CISSP, Certified Information Privacy Professional (CIPP) from the International Association of Privacy Professionals (IAPP), and Certificate of Cloud Security Knowledge (CCSK). Huawei have established a Cyber Security & Privacy Protection Knowledge Centre and released more than 200 MOOC, facilitating the rapid sharing and transfer of knowledge within the organization. To continuously improve the cybersecurity and privacy protection awareness among all employees, the company held the Cyber Security Awareness Month campaign, engaging about 150,000 employees online and offline through different activities. Such activities

included messages from top-level management, expert lectures, knowledge quizzes, CTF contests, cybersecurity technology conferences, and a verification conference

In the pursuit to deliver these activities, we aim to work with various standards organizations, industry alliances, and open-source communities and platforms such as GISEC/ GITEX, which Huawei has already been working with, to jointly work on these projects. Specifically, Huawei will work closely with OIC-CERT to drive realization of these projects and create good cybersecurity artifacts that will benefit the industry globally

Aloysius Cheang, Huawei UAE Global Cyber Security & Privacy Officer, reported to the head of the CSC at the UAE Cyber Security Week





UZBEKISTAN

Uzbekistan Computer Emergency Response Team (UzCERT)

(Full Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

2021 was just as eventful and at the same time difficult as 2020 for both UzCERT and its partners. However, the team remained positive in facing the challenges posed by the new virus strains of the pandemic. UzCERT participated in several online conferences, entered into several joint agreements with international companies, signed a memorandum of understanding, and most importantly, contributed to making UzNET a safe place. UzCERT is grateful to its partners for showing phenomenal flexibilities during these difficult times and for inviting the team to various online conferences. It is really appreciated

Achievements

The UZCERT team took 3rd place in the first international cyber-exercise *CyberDrill 2021* organized by EG/CERT with the support of the OIC-CERT

ABOUT THE ORGANIZATION/ AGENCY

Introduction

The UZCERT services, operating as a structural unit of the State Unitary Enterprise (**SUE**) *Cybersecurity Centre*, is focused on the cooperation and interaction with the operators and providers, as well as the nation's Internet users, and providing the necessary support in responding to cybersecurity incidents. The UZCERT service carries out the necessary analysis of incident artefacts, establishes the causes and consequences of the incident, and prepares recommendations for effective counteraction to computer viruses and hacker attacks. This approach has resulted in a positive trend in information and cybersecurity threats and incidents, through continuous training of employees in the field of computer forensics, malware analysis, and the subscribing to the world's best practices for responding to cybersecurity threats and incidents

Given the cross-border nature of cybersecurity threats and incidents, the service aims to collaborate widely with foreign partners to maximize the opportunities and experience of the world community in the fight against cyber threats and cyber-crimes

The result of this approach is the positive information and cybersecurity dynamics of threats and incidents, which include the continuous training of employees in the field of computer forensics, malware analysis and the

best world practices in responding to cybersecurity threats and incidents

Establishment

The increased attention on the issues on cybersecurity is backed by the Presidential Decree of *On the State Program for implementation of the National Action Strategy on Five Priority Development Areas* signed in 2017, where ensuring further improvement of cybersecurity in the country is one of the most important priorities. The tasks of implementing government initiatives in the field of information and cybersecurity were assigned to the Information Security Centre established in 2013, and later following the government decision in 2019, was transformed into the SUE *Cybersecurity Centre* along with an increase in its roles as the responsible executive of state policy in the field of information and cybersecurity

Resources

Government

Constituency

UZCERT is responsible for providing and supporting information and cybersecurity for all users and resources operating in the national Internet segment (UzNET) of the Republic of Uzbekistan

ACTIVITIES & OPERATIONS

Events Organized by the Organization/ Agency

The SUE *Cybersecurity Centre* regularly conducts seminars and training courses on various issues regarding information security and cybersecurity for authorized employees of the state bodies and institutions of the Republic of Uzbekistan

Event Involvement

- participation in an online conference organized by Expo-Link CodIB LLC (RF) on *Safe Environment* (Forensics)
- participation in an online training on *Using NG-SIEM systems to protect your environment*, organized by the aeCERT under the initiative of the OIC-CERT

participation in an online conference organized by BI.ZONE on *Security Operations Centre* (RU)

- participation in the 10th annual online conference *Cloud & Digital Transformation 2021* organized by ICS-Holding JSC (RU)
- participation in an online training on *Attacks on the supply chain: problems and opportunities*, organized by aeCERT under the initiative of the OIC-CERT
- participation in an online training on *DNSSEC* organized by aeCERT under the initiative of the OIC-CERT
- participation in situational cyber exercises for CERT services/ teams

FIRST Fellowship organized by FIRST

- participation in the 16th Annual CSIRT Technical Meeting (NatCSIRT 2021) organized by Carnegie Mellon University (US)
- participation in an online training on *Protect Your Business* organized by aeCERT under the initiative of the OIC-CERT
- participation as representatives of the Centre in the online meeting of the Group of Experts of the Shanghai Cooperation Organization (SCO) Member States on International Information Security
- participation in an online conference organized by CETC International Co., Ltd on *Cybersecurity Monitoring System and Cyber Training Centre* (CN)
- participation in an online conference organized by Kaspersky Lab on *Actual Cyber Threats in the Central Asian Region* (RU)
- participation in an online training on *Egyptian Digital Judicial Session, Government Case MEDICO* organized by EG/ CERT under the initiative of the OIC-CERT
- participation in an online conference on *Data Leakage: Prevention of Negative Consequences and Analysis of the Experience Gained* organized by NCCA (ID)
- participation in the online cyber-exercise *Africa Cybersecurity Drill 2021*, organized by AfricaCERT, under the initiative of the OIC-CERT

Place	Team	Score
1	Turkcell CDC	4500
2	tunCERT	3600
3	UzCERT	3200
4	BGD e-GOV CIRT	3050
5	bjCSIRT	2500
6	espc-cert	1750
7	TeamX	1100
8	NCCA/ID-SIRTII	900
9	NISSA	850
10	Moinul	500
11	p4	450
12	r003	350
13	sudan cert	100

- participation in 3 online cyber exercises Cyber Polygon, organized by BI.ZONE (RU)
- participation in an online training on Data Classification organized by aeCERT under the initiative of the OIC-CERT
- participation in an online conference on Ensuring Cybersecurity of a Large-scale Sporting Event or an Important Event, organized by the Computer Incident Response Service CNCERT (CN)
- participation in the 16th Annual International Online Conference and Exhibition DPC organized by JSC X-Holding (RU)
- participation in an online conference organized by Kaspersky Lab, representative office in the Asia-Pacific region on Improving Cyber Resilience by Building Cyber Potential (RU)
- participation in an online conference on Computer Forensics Problems of Data Extraction and their Solutions", organized by Meiya Pico (CN)

- participation in an online training on Browser *Security*, organized by aeCERT under the initiative of the OIC-CERT
- participation in an online training on the topic *Global Digital Security and Forensics According to New Criteria/ Norms* organized by CyberSecurity Malaysia, under the OIC-CERT
- participation in the annual online cyber-exercise *Annual OIC-CERT Cyber Drill 2021* organized by the OIC-CERT and Oman National CERT
- participation in an online training on *Physical Security* organized by aeCERT under the initiative of the OIC-CERT
- participation in an online conference on *Malware Traffic Analysis* organized by NCCA under the initiative of the OIC-CERT (ID)
- participation in the online conference in the *13th Annual Conference and 9th Arab Regional Cybersecurity Summit* organized by the NCA under the initiative of the OIC-CERT (OM)
- participation in an online conference on *CyberCrimeCon-2021* organized with the technical support from Group-IB under the initiative of the OIC-CERT (RU)
- participation in the first international cyber exercise *CyberDrill 2021* organized by the EG/ CERT with the support of the OIC-CERT
- participation in an online conference with representatives of the Israel Cybersecurity Agency
- participation in the first consultations on ensuring international cybersecurity of the CIS countries
- participation in the annual symposium FIRST 2021 for the Africa and Arab regions, organized by the African Forum of Incident Response and Security Teams (AfricaCERT), as well as with the OIC-CERT

Achievement

A MoU was signed between a Russian leading cybersecurity company Rostelecom-Solar (Солар Секьюрити-Solar JSOC) and SUE Cybersecurity Centre

2022 PLANNED ACTIVITIES

Presently, the SUE Cybersecurity Centre is actively working on the coordination and signing of MoU with foreign departments and organizations acting as CERT services

To conclude the agreements, in 2021, UZCERT held numerous online meetings with representatives of various foreign companies, both in the public and private sectors

The main goal for 2022 is to continuously develop the cybersecurity field, active cooperation with foreign partners, and signing of MoU with new partners. This include close collaboration with the ITU and the Japanese Computer Incident Response Service (JPCERT/ CC) (JP) who are actively supporting UZCERT team to achieve full FIRST membership status.

YEMEN

Dr Abdulrahman Ahmad Abdu Muthana (SMART SECURITY SOLUTIONS)

(Professional Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- SMS operator & local bank network penetration testing
- Cybersecurity training
- Android apps penetration testing
- Security awareness program training
- Software protection solutions for local software development companies
- Helping SMS operator company to implement ISO 27000 (ISMS) Standard

Achievements

- Penetration testing of different SMS operator companies
- Penetration testing of network infrastructure for a local bank
- Security awareness training for local company staff
- Secure coding training for two software development companies
- Helping SMS operator company to implement ISO 27000 (ISMS) Standard
- providing security solutions for protecting software developed by local software development companies

ABOUT THE ORGANIZATION/ AGENCY

Introduction

Smart Security Solutions Company (SMARTSEC) is the first company in Yemen for providing information security training, consultancy, and information security research

Establishment

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

Resources

SMARTSEC includes several information security professionals and researchers. The company has 2 training labs equipped with facilities and a research lab

Constituency

Information security domain

ACTIVITIES & OPERATIONS

Events Organized by the Organization/ Agency

- Cybersecurity training courses
- Secure coding training programs for software development companies between Oct and Dec 2021

Events involvement

- First conference of Cybersecurity Strategy in Yemen, held in Sanaa, Yemen on 7-9 Jun 2021
- Information Security Training
- Information Security Awareness Programs
- Ransomware Incidents Analysis

Achievement

- Training several Information Security courses (CEH, Computer, and mobile Forensics)
- Several Information Security Awareness Programs for the financial institutes
- Ransomware Virus Investigations

2022 PLANNED ACTIVITIES

Cybersecurity training, helping organizations in Yemen to implement ISO 27000 (IS MS) Standard

SINGAPORE (SG)

CERT-GIB

(Commercial Member)

HIGHLIGHTS OF 2021

Summary of Major Activities

- 18 years of operation since the establishment of Group-IB
- 70000+ hours of hands-on Incident Response
- 1300+ successful investigations of hi-tech cybercrime cases
- Opening of Group-IB Threat Intelligence and Research Centre in the Middle East and Africa (based in Dubai)

- International cooperation with other CERT/ CSIRT teams
- *Carding Action 2021* - Joint operation with Europol's European Cybercrime Centre (EC3)
- *Operation Lyrebird* joint operation with INTERPOL
- *Fraud Family*
- Establishment of Threat Hunting & Investigation Competence Centre partnering with University of Naples Federico II (UNINA) in Italy
- Group-IB becomes the first cybersecurity company to join JTC's Punggol Digital District, Singapore *https://www.group-ib.com/media/gib-pdd/*

Achievements

Product launch

- Atmosphere (Corporate Email Protection)

Analytical and Technical Reports

- Hi-tech crime trends 2021/2022 - *https://www.group-ib.com/resources/threat-research/2021-reports.html#report-1*
- Uninvited Guests - The sale of access to corporate networks
- Corporansom - Threat number one
- Big Money - Threats to financial sector
- Scams and Phishing - The epidemic of online fraud

White papers

- Digital risk insights - *https://www.group-ib.com/whitepapers/digital-risks.html*
- Cost Savings and Business Benefits Enabled by Fraud Hunting Platform
- A Guide to Cyber Threats to the Finance Sector Report
- Lock like a Pro (ProLock Ransomware) - *https://www.group-ib.com/whitepapers/prolock.html*
- Egregor ransomware - The legacy of Maze lives on *https://www.group-ib.com/whitepapers/egregor-ransomware.html*
- The easy first step to your Zero Trust journey - *https://www.group-ib.com/whitepapers/zero-trust-consulting.html*
- Ransomware Uncovered 2020-2021 (Annual Report) - *https://www.group-ib.com/resources/threat-research/ransomware-2021.html*

Annual events:

- CyberCrimeCon 2021 - *https://cybercrimecon.com/*
- Digital Risk Summit 2021 - *https://digitalrisks.group-ib.com/*

- Ransomware Insights 2020-2021 - *https://www.group-ib.com/resources/webinars/ransomware-insights-2020-2021.html*

ABOUT THE ORGANIZATION/ AGENCY

Introduction

CERT-GIB is a Computer Emergency Response Team created by Group-IB, a global cybersecurity company. It launched with the mission to immediately contain cyber threats, regardless of when and where they take place and who is involved

CERT-GIB combines the power of human intelligence with technological prowess to offer the most effective response and remediation actions

Aside from being an OIC-CERT member, CERT-GIB is an accredited member of the Trusted Introducer, a member of FIRST, and a strategic partner of the International Multilateral Partnership Against Cyber Threats (IMPACT)

Establishment

10 Mar 2011

Resources

Human intelligence

More than 60 employees working round the clock to ensure help is provided to any parties that require it

CERT-GIB works closely with Group-IB's Digital Forensics Lab and Threat Intelligence & Attribution and Investigations teams

Proprietary technology

Group-IB Threat Hunting Framework allows CERT-GIB experts to manage incidents effectively and efficiently and reduce time spent on incident analysis

CERT-GIB operations are enhanced with data collected by Group-IB Threat Intelligence & Attribution

Malware analysis further reinforces CERT-GIB's capabilities, as it allows experts to prevent severe data breaches and network infections and detect vulnerabilities within the perimeter

Combined, Group-IB technological capabilities include

- Internal and external threat hunting
- Graph analysis
- Data storage
- Correlation and attribution
- Event analysis

Unmatched expertise

CERT-GIB has spent over 65,000 hours responding to incidents of various complexity all over the globe

Group-IB has conducted extensive research on APT groups, ransomware operators, and general cybersecurity trends across all major industries

Group-IB's combined technological capabilities and human intelligence means the company is always aware of cyber criminals' latest tools, TTPs, and movements

International cooperation

CERT-GIB is part of a global network of CERTs that actively engages in information and intelligence sharing

CERT-GIB also actively collaborates with top-level Russian domains to block dangerous websites

Constituency

Service Provider Customer Base

CERT-GIB's constituency includes organizations from the media, law enforcement agencies, government sector, Internet service providers, private sector, and CII

ACTIVITIES & OPERATION

Events Organized by the Organization/ Agency

- CyberCrimeCon 2021 - *https://cybercrimecon.com/*
- Digital Risk Summit 2021 - *https://digitalrisks.group-ib.com/*
- Advanced Fraud Hunting with Group-IB – Egypt
- Comprehensive Digital Risk Protection for your business - UAE
- Comprehensive Digital Risk Protection for your business – Singapore
- Webinars
  - Digital risks 2021 Scam trends and projections in MEA region
  - Digital risks 2021 Scam trends and projections in the Asia Pacific (**APAC**) region
  - *Building a customer-centric approach to Fraud Prevention*
  - Cyber Response Chain APAC, Europe- Middle East- Africa (**EMEA**), Namibia
  - *The Total Economic Impact of Threat Intelligence*
  - *Warding off REvil: How to keep ransomware gangs out of your company*
  - Treat Day in APAC, Europe
  - Fraud Day APAC, EMEA
  - *Forget-me-not: using memory analysis to search for traces of commodity malware*
  - *Leaks, spies, and blackmail: Insights into modern high-tech crime*
  - *Phishing Attack Investigations and the latest scam trends*

Events involvement

- Secon & eGISEC 2021 – Korea
- Korea Police Expo 2021
- 2nd Global Online Scam Summit

- Cyber Crime Command's Virtual In-Service – Singapore
- Infosec 2021 – Pakistan
- The Financial Services Information Sharing and Analysis Center (FS-ISAC) (EU)
- Positive Hack (PH) Days
- Magnet Summit
- GISEC'21 - UAE, Dubai
- AtHack - Saudi Arabia
- 1st Arab Banking forum - Egypt, Sharm el Sheikh
- GITEX - UAE, Dubai

- Online Banking Forum - Gulf region
- 1st defense and security conference AIDTSEC - Jordan, Amman
- OIC-CERT 13th Annual Conference & 9th Arab Regional Summit Annual Conference (virtual)
- @HACK - Saudi Arabia, Riyadh
- International Conference on Cyber Warfare & Security - Pakistan

Achievement

- Group-IB wins 8 Gold Cybersecurity Excellence Awards 2022 - *https://www.group-ib.com/media/gcea-2022/*
- Group-IB Services included among major cybersecurity companies by Forrester - *https://www.group-ib.com/media/gib-forrester-report-2021/*
- Group-IB Honoured With 5-Star Rating in the 2021 CRN® Partner Program Guide - *https://www.group-ib.com/media/gib-crn-2021/*
- Group-IB was granted Innovation Excellence award for its Digital Risk Protection (DRP), Frost Radar: European Digital Risk Protection (DRP) Market, 2020 *https://www.group-ib.com/media/drp-frost-and-sullivan/*

2022 PLANNED ACTIVITIES

- Digital Risk Summit 2022
- CyberCrimeCon 2022
- High-tech crime trends 2022/ 2023
- Ransomware Uncovered (Annual Report) 2021-2022
- Quarterly Fraud Hunting Day Webinars
- AssetZero product launch - 1 Apr 2022