Annual Report 2018 (BGD E-GOV CIRT Annual Report)

Compiled by

BGD e-GOV CIRT

Published on: June 2019

Published and distributed by:

BGD e-GOV CIRT under LICT Project

Bangladesh Computer Council (BCC), ICT Division,

Ministry of Posts, Telecommunication & Information Technology,

BCC Bhaban, E-14/X, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207

Tel: +88-02-818-1392 | Fax: +88029124626

E-mail: info@cirt.gov.bd

BGD e-GOV CIRT Website: www.cirt.gov.bd

Message from Minister

The Internet has become the most powerful and widely available communication medium which spreading daily. Governments, corporations, bank, hospitals and schools conduct their day-to-day business over the Internet. With such widespread use the data that resides on and flows across the network varies from banking and securities transactions to medical records, proprietary data, and personal correspondence.

While the world is moving toward an era, which requires involvement of people and technology 24x7, and almost majority of our country's population use the Internet, a well-defined structure and management of cyber security must be in place nationwide. The role of BGD e-GOV CIRT under the supervision of LICT is considered to be of great importance to Cyber Security.

Executive Summary

Bangladesh Computer Council (BCC) established BGD e-GOV CIRT in the last quarter of 2015. BGD e-GOV CIRT started providing incident handling services in February 2016. This is the first report of BGD e-GOV CIRT that summarizes activities and results achieved during 2016. It provides an insight into what the CIRT has been seeing, learning, and responding to, focusing on specific areas of change or new knowledge obtained. Furthermore, this document contains mitigation and remediation advice to assist organizations in preventing and responding to cyber threats. For a more comprehensive overview, this report should be read in conjunction with the GoBISM (Government of Bangladesh Information Security Manual).

The main message that derives from BGD e-GOV CIRT activities during 2016 is that current hype associated with the proliferation of threat intelligence" can be a distraction from what really matters: the motivation to allocate effort and resources to improving cyber security posture by implementing technical controls. If we are relying on threat intelligence to respond to threats already discovered, it is too late for us and our organizations.

In 2019, BGD e-GOV CIRT will continue to improve its cyber security capabilities and extend services in support of all government organizations and especially to the 25 Critical Information Infrastructures that have been identified. It will continue coordination efforts with industry and government partners to mitigate cyber risks through timely and effective sharing of situational awareness information and focused mitigation plan.

A new responsibility for the team in 2019 is to assist government organizations with their risk assessments.

Other goals for 2019 include improving and expanding BGD e-GOV CIRT incident response technical teams and tools, which will provide greater value during incident response and assessment activities. The team will also continue to refine and update training offerings that will allow government organizations to better meet the demands of challenging and evolving technical issues in cyber security.

Mission Statement

The mission of Bangladesh e-Government Computer Incidents Response Team, BGD e-GOV CIRT is "to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh, which will make these programs more efficient and reliable."

Major activities:

- Manage cyber security in Bangladesh government's e-Government network and related infrastructure;
- Serve as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders;
- Make efforts to establish national cyber security incident management capabilities in Bangladesh.

To achieve this goal, BGD e-GOV CIRT during the first stage of its development will:

- Monitor the network for the events that affect security of the government network;
- Carry out investigations and containment measures for cyber security events in order to minimize data loss or service disruption in the government network and e-services;
- Help to solve security related issues in National Data Center (NDC) including provision of obligatory instructions for BCC personnel to secure NDC information resources;
- Carry out preventive measures in order to minimize disruptions of secure operations of the government network and e-services;
- Participate in international and national cyber security initiatives;
- Promote and strengthen cyber security environment by developing, collaborating and maintaining relationships with other CIRTs and organizations in the country and abroad;
- Support capacity building of the existing manpower of BCC to establish national CIRT.

Constituency

Constituency of BGD e-Gov CIRT are all governmental institutions of Bangladesh. Constituency sector is “government” and constituency type are “mixed” (internal and external). Part of the constituency is using National Data Center (NDC) located at Bangladesh Computer Council (BCC) where host their IT resources and services. BGD e-GOV CIRT supervises the following Autonomous System numbers, IP address space and domain names associated with the NDC:

- AS63932
- bcc.gov.bd
- bcc.net.bd
- 43.229.12.0/22
- 103.48.16.0/22
- 114.130.54.0/23
- 180.211.213.0/24

The constituency range and description will be continuously checked and updated to ensure that all ICT resources which should be protected are covered by the designed and implemented incident management services.

Services

There are two types of services provided by BGD e-GOV CIRT.

Proactive Services

- Security assessments

  BGD e-Gov CIRT is constantly doing vulnerability assessments and penetration testing on assets located at the National Data Center as well as these activities can be provided to the constituency on a special official request

- Configuration and maintenance of security tools, applications, infrastructures, and services

  BGD e-Gov CIRT maintains described set of security tools primarily used for logs collection and archive for assets located in the National Data Center which allow to trace incidents when they occur.

- Intrusion detection

  BGD e-Gov CIRT collects cyber security threat information (compromises, accessible vulnerabilities) from various external feeds, filters and distributes them among the constituency.

- Security consulting

  BGD e-Gov CIRT provides advice and guidance on the best security practices to implement for constituents' business operations.

- Awareness building

  BGD e-Gov CIRT seeks opportunities to increase security awareness through developing articles, posters, newsletters, web sites, social media or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

- Cyber Sensor

  Detecting intrusion, suspicious activity & development of methodology of assessing maturity level of Critical Information Infrastructure in Bangladesh government IP network, thus sensor network is being implemented.

Reactive Services

- Cyber security incident handling

  BGD e-GOV CIRT will receive information regarding cyber security incidents, triage incidents and coordinate response. Possible activities related to incident handling include:

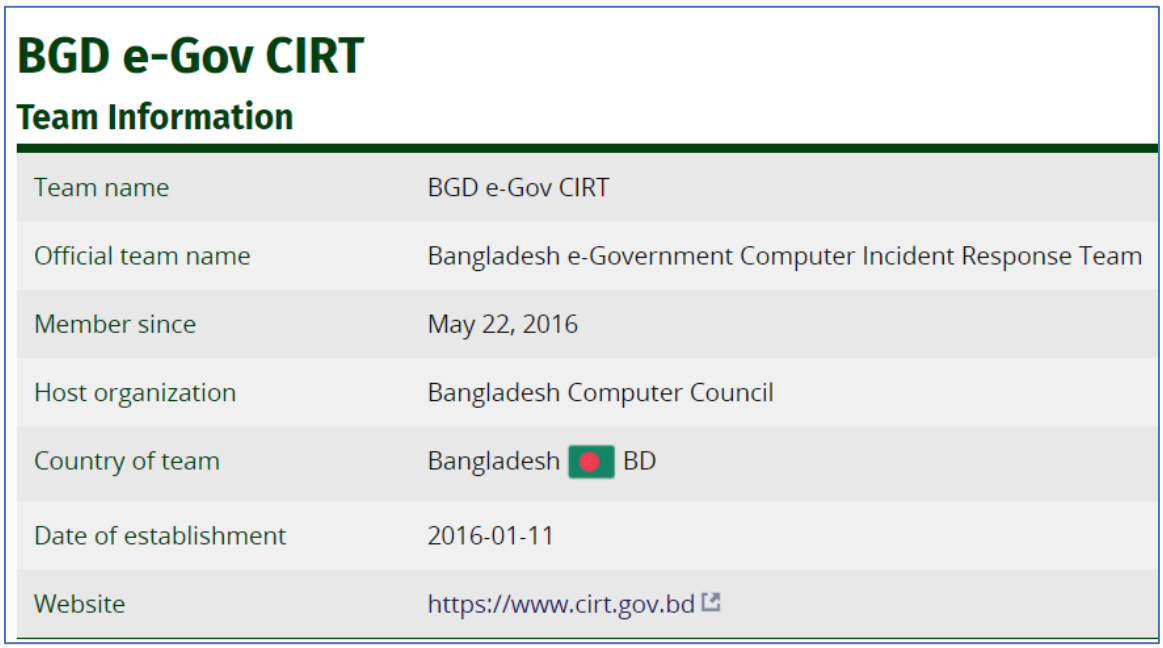
  - Reporting
  - Coordination
  - Incident response support
  - Incident analysis and evidence collection

International Membership

Forum of Incident Response and Security Teams (FIRST.Org)

FIRST is the global. FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

https://www.first.org/members/teams/bgd_e-gov_cirt



BGD e-Gov CIRT

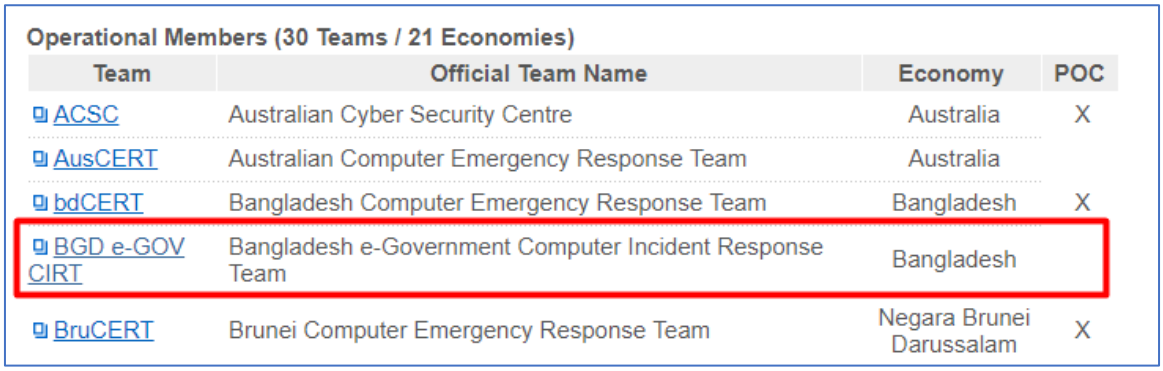
Team Information

Team name	BGD e-Gov CIRT
Official team name	Bangladesh e-Government Computer Incident Response Team
Member since	May 22, 2016
Host organization	Bangladesh Computer Council
Country of team	Bangladesh BD
Date of establishment	2016-01-11
Website	https://www.cirt.gov.bd

Asia Pacific Computer Emergency Response Team (APCERT)

APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation.

https://www.apcert.org/about/structure/members.html



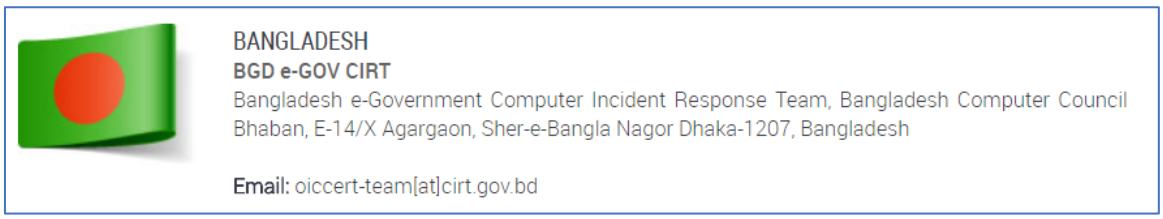
Operational Members (30 Teams / 21 Economies)

Team	Official Team Name	Economy	POC
ACSC	Australian Cyber Security Centre	Australia	X
AusCERT	Australian Computer Emergency Response Team	Australia	
bdCERT	Bangladesh Computer Emergency Response Team	Bangladesh	X
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team	Bangladesh	
BruCERT	Brunei Computer Emergency Response Team	Negara Brunei Darussalam	X

Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)

The purpose of OIC-CERT is to encourage and support the smooth collaboration and cooperation between CERTs among the OIC member countries and other CERT stakeholders as required.

https://www.oic-cert.org/en/allmembers.html#.XMFPfUiFNPY



BANGLADESH

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team, Bangladesh Computer Council Bhaban, E-14/X Agargaon, Sher-e-Bangla Nagor Dhaka-1207, Bangladesh

Email: oiccert-team[at]cirt.gov.bd

TF-CSIRT Trusted Introducer

The Trusted Introducer Service - a.k.a. TI - was established by the European CERT community in 2000 to address common needs and build a service infrastructure providing vital support for all security and incident response teams.

https://www.trusted-introducer.org/directory/teams/bgd-e-gov-cirt.html

BGD e-GOV CIRT
Bangladesh e-Government Computer Incident Response Team

Accredited
since 28 Nov 2018

Fields describing the team

Team Details

Official Name	Short Name	Country
Bangladesh e-Government Computer Incident Response Team	BGD e-GOV CIRT	Bangladesh

Established	Host Organisation
11 Jan 2016	Bangladesh Computer Council

International Collaboration

Indian Computer Emergency Response Team

The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security threats like hacking and phishing. BGD e-GOV CIRT is working very closely with Indian Computer Emergency Response Team (CERT-In) and they have signed a MoU as well On "Cooperation in the area of Cyber Security" between Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Ministry of Post, Telecommunication and IT and Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, India on April 2017, During Prime Minister Sheikh Hasina's Visit to India (Link of that news). BGD e GOV CIRT is Member of IoT Security Working group, Secure Digital Payment Working Group of CERT-In as well.

Anti-Phishing Working Group (APWG)

The Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies.

Norway Registers Development (NRD)

NRD Companies are a global information technology and consulting group of companies specialized in governance and economic digital infrastructure development.

International Council of E-Commerce Consultants (EC-Council)

EC-Council is the world's largest cyber security technical certification body. They operate in 145 countries globally and we are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (C|HFI) courses.

Team Cymru

Team Cymru was formed in 1998 to learn the "who and why" of malicious Internet activity. This focus on attribution resulted in the uncovering of the "what, when, where, and how" of online malevolence.

CERT Polska

CERT Polska is Computer Emergency Response Team which operates within the structures of Scientific and Academic Computer Network or NASK – a research institute which conducts scientific activity, operates the national .pl domain registry and provides advanced IT network services.

Collaboration with other CERTs

Sharing knowledge from other CERT organization regarding cyber security best-practices, information security standards and took advantage in information security, BGD e-GOV CIRT has collaborate with various organizations in international CERT community:

Local Partners

1. Bangladesh Computer Council
2. Bangladesh Police
3. Bangladesh Bank

International Partner

1. FIRST
2. OIC-CERT
3. APCERT
4. CERT-IN
5. CERT
6. TEAM CYMRU
7. CERT.PL
8. LITNET CERT
9. APWG
10. ANUBIS NETWORKS
11. SHADOW SERVER
12. CREST
13. EC COUNCIL
14. TF-CSIRT

- Attend on “56th TF-CSIRT Meeting & FIRST Regional Symposium for Europe”.
- Attend on “2017 APISC Security Training Course”.
- Attend on “29th Annual FIRST Conference in Puerto Rico".
- Attend on “OIC-CERT Annual Conference 2017 in Baku, Azerbaijan”.
- Attend on “APCERT Annual General Meeting & Conference 2017 in New Delhi, India”.
- Attend on “55th TF-CSIRT Meeting”.
- Attend “Regional Cyberdrill for CIS” at Baku, Azerbaijan in 2018.
- Attend “Fintech Indonesia 2018” at Jakarta, Indonesia in 2018.
- Attend “Security Scape Bangalore” India in 2018.

1. Incident Handling Unit

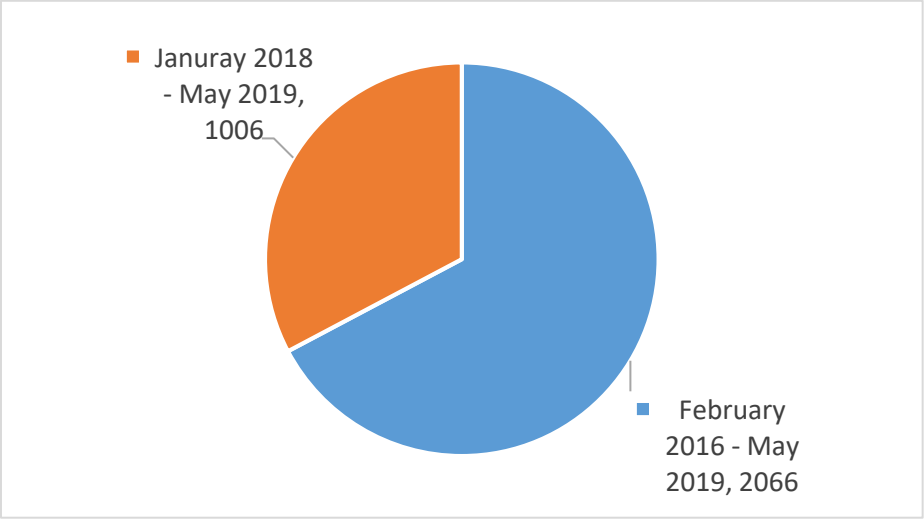
BGD e-GOV CIRT will receive information regarding cyber security incidents, triage incidents and coordinate response. Possible activities related to incident handling include:

- Reporting
- Coordination
- Incident response support
- Incident analysis and evidence collection

PRESENT STATISTICS OF BGD e-GOV CIRT

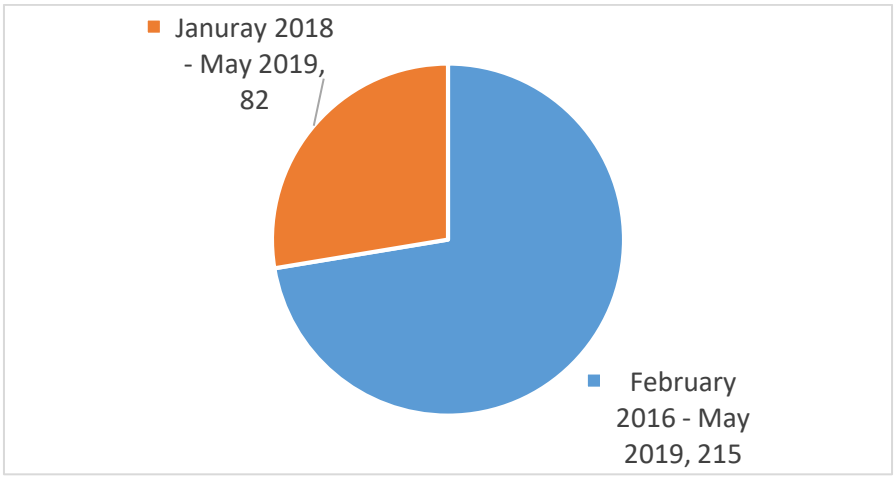
Incident Handling and Coordination:

- From January 2018 to May 2019 total number of Registered Incident Handling & Coordination tickets are 1006.
- From February 2016 to May 2019 total number of Registered Incident Handling & Coordination tickets are 2066.



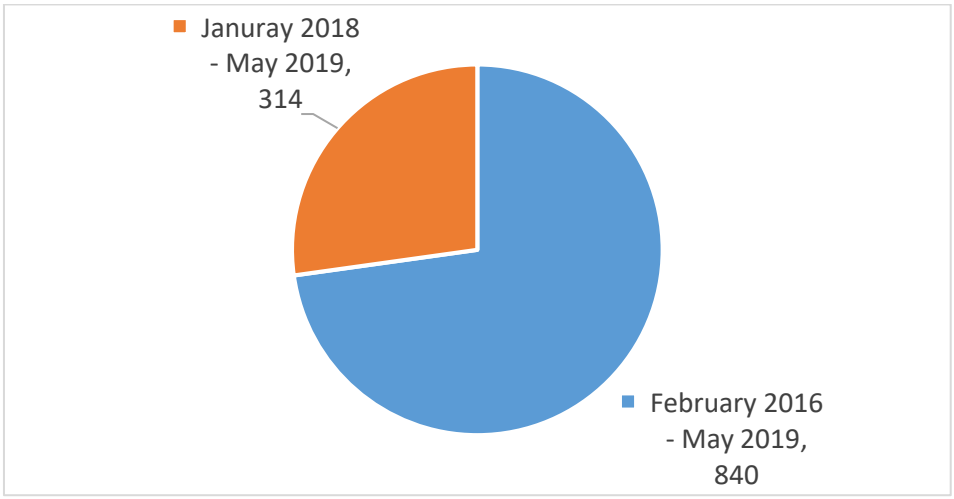
Incident response to Govt. Organizations

- From January 2018 to May 2019 total 82 Incident responses have been provided to Bangladesh Government organizations.
- From February 2016 to May 2019 total 210 Incident responses have been provided to Bangladesh Government organizations.

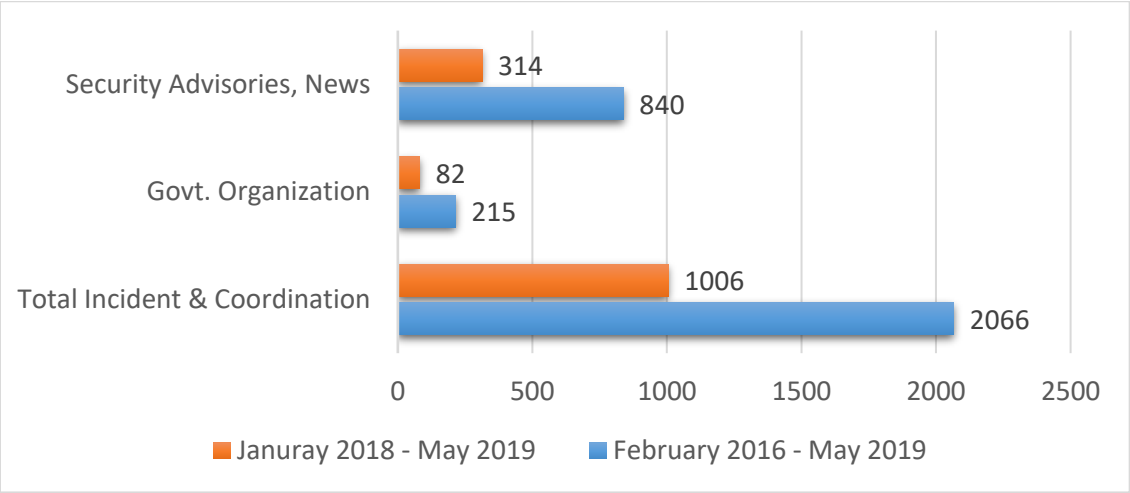


Security Advisories & News:

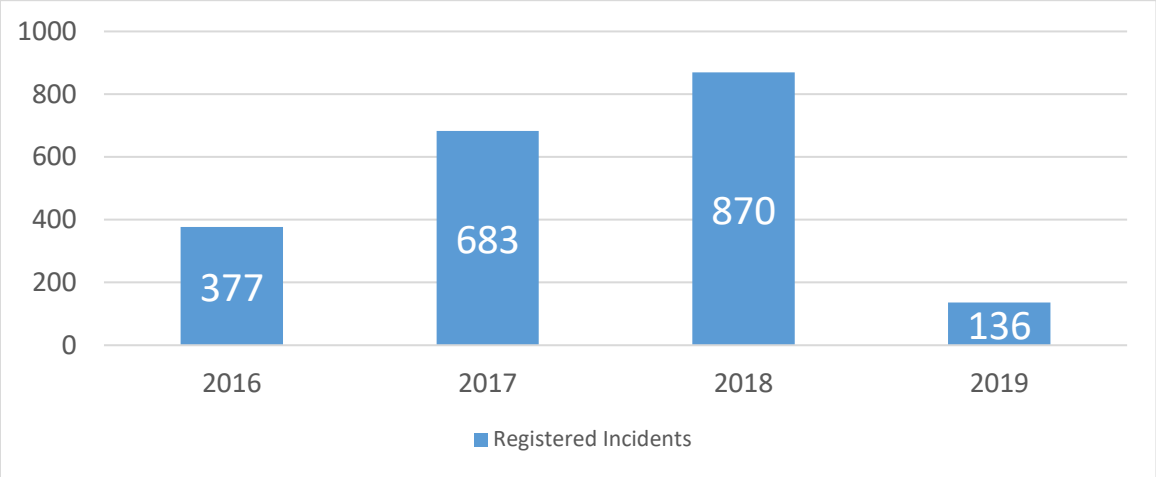
- From January 2018 to May 2019 Total number of published Security Advisories, Alerts & News on CIRT web media are 314.
- From February 2016 to May 2019 Total number of published Security Advisories, Alerts & News on CIRT web media are 840.



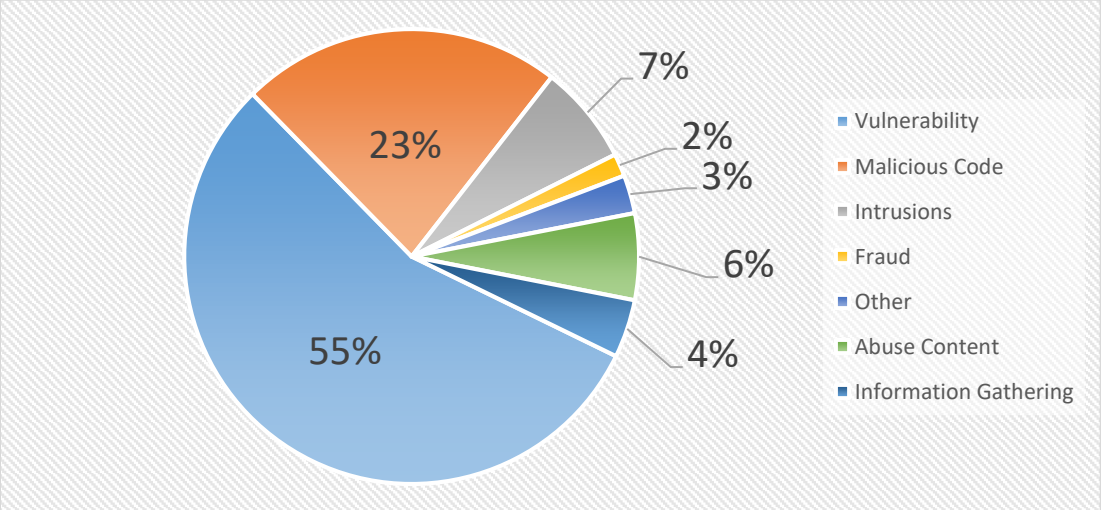
Overall Statistical view



Incidents per year



Incidents Classification



Activities

EVENTS ORGANIZED BY THE ORGANIZATION

BGD e-GOV CIRT's First Anniversary Conference

Cyber Security Drills & CERT Games

International Cyber Security Conference 2018

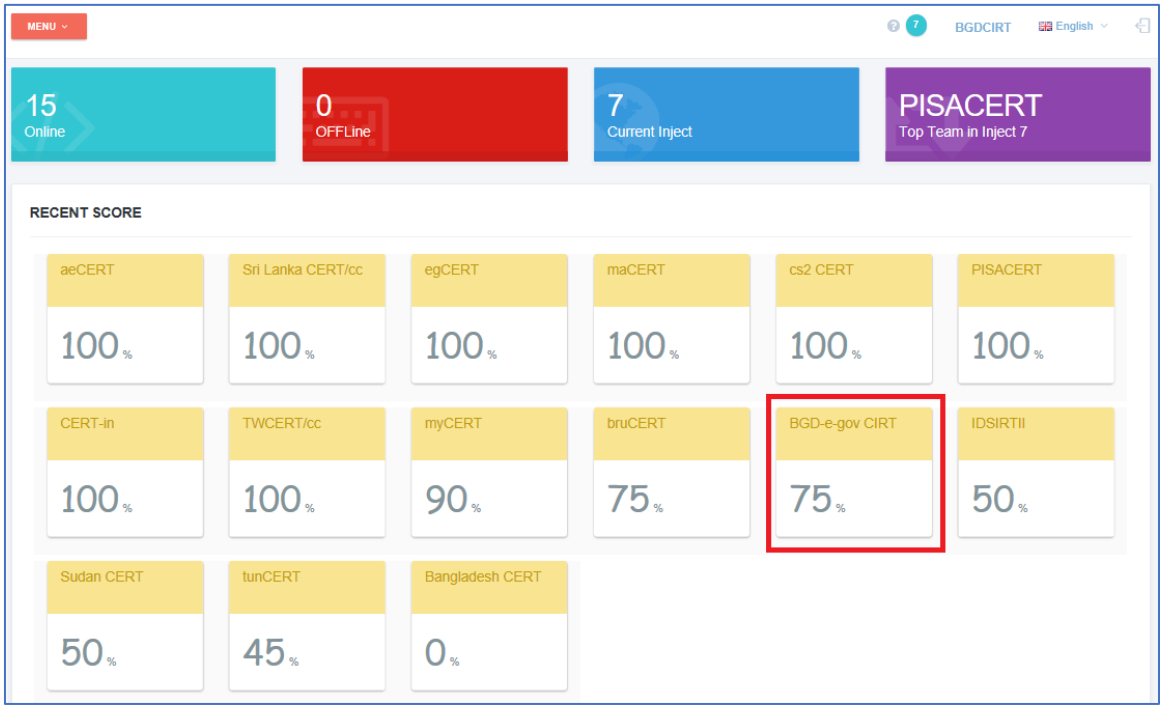
Applicability of International Law on State Behavior in Cyberspace Course", from 20-24 May 2019, at George C. Marshal European Center for Security Studies, Program on Cyber Security Studies, The College of International and Security Studies, Garmisch-Partenkirchen, Germany.

PARTICIPATION ON INTERNATIONAL CYBER DRILL

OIC-CERT Cybersecurity Drill 2018

BGD e-GOV CIRT team has participated in the OIC-CERT Drill 2018. The team has successfully completed all the activities regarding the event and scored 75% with a very competitive response time.

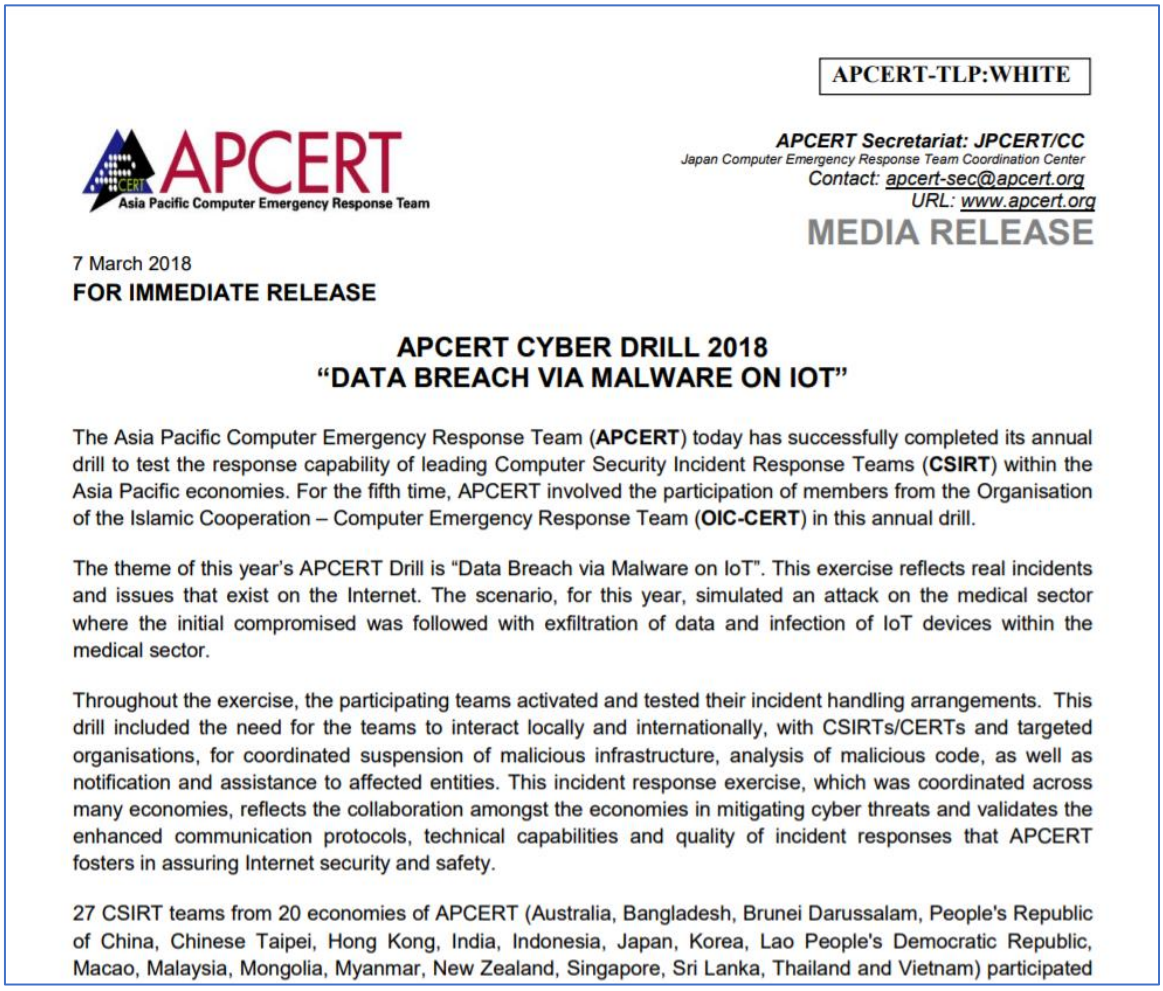
https://www.cirt.gov.bd/bgd-e-gov-cirt-has-successfully-participated-on-oic-cert-cybersecurity-drill-2018-with-75-score/



APCERT Cyber Drill 2018

BGD e-GOV CIRT has successfully participated in the APCERT Drill 2018 and completed all the activities regarding the event.

- https://www.cirt.gov.bd/bgd-e-gov-cirt-has-successfully-participated-on-apcert-cyber-drill-2018/
- https://www.apcert.org/documents/pdf/APCERTDrill2018PressRelease.pdf



APCERT-TLP:WHITE

APCERT
Asia Pacific Computer Emergency Response Team

APCERT Secretariat: JPCERT/CC
Japan Computer Emergency Response Team Coordination Center
Contact: apcert-sec@apcert.org
URL: www.apcert.org

MEDIA RELEASE

7 March 2018
FOR IMMEDIATE RELEASE

APCERT CYBER DRILL 2018
"DATA BREACH VIA MALWARE ON IOT"

The Asia Pacific Computer Emergency Response Team (**APCERT**) today has successfully completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (**CSIRT**) within the Asia Pacific economies. For the fifth time, APCERT involved the participation of members from the Organisation of the Islamic Cooperation – Computer Emergency Response Team (**OIC-CERT**) in this annual drill.

The theme of this year's APCERT Drill is "Data Breach via Malware on IoT". This exercise reflects real incidents and issues that exist on the Internet. The scenario, for this year, simulated an attack on the medical sector where the initial compromised was followed with exfiltration of data and infection of IoT devices within the medical sector.

Throughout the exercise, the participating teams activated and tested their incident handling arrangements. This drill included the need for the teams to interact locally and internationally, with CSIRTs/CERTs and targeted organisations, for coordinated suspension of malicious infrastructure, analysis of malicious code, as well as notification and assistance to affected entities. This incident response exercise, which was coordinated across many economies, reflects the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities and quality of incident responses that APCERT fosters in assuring Internet security and safety.

27 CSIRT teams from 20 economies of APCERT (Australia, Bangladesh, Brunei Darussalam, People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand and Vietnam) participated

CYBER THREAT INTELLIGENCE DASHBOARD

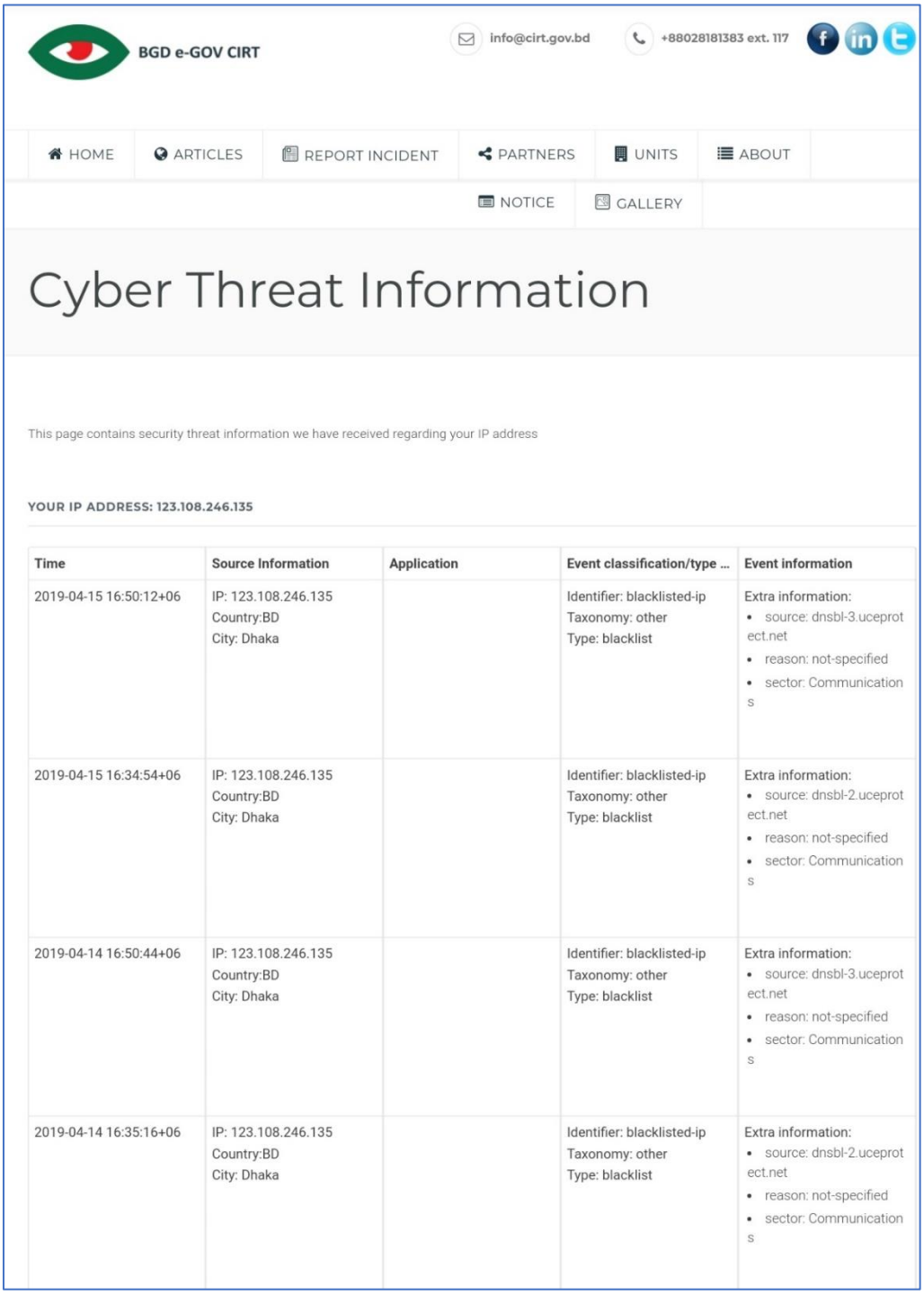
Application was developed and deployed for automated Cyber Threat Intelligence feed aggregation and distributions to the constituents of BGD e-GOV CIRT. The application makes these automated steps:

1. Collects contact information from CIDB system,
2. Collects IP address space information from CIDB system,
3. Collects feed event information from IntelMQ repository,
4. Sends aggregated threat intelligence information to the constituent's contacts once per day. For message delivery, RTIR system is being used to track all possible further communications.

CYBER THREAT INFORMATION

WordPress plugin was created to retrieve information from IntelMQ aggregated database to show it to the portal visitors about cyber threats related to their computer IP address.

The webpage is available through the address https://www.cirt.gov.bd/cyber-threat-information/



2. Cyber Sensor Unit

Cyber Sensor Introduction

Detecting intrusion, suspicious activity & development of methodology of assessing maturity level of Critical Information Infrastructure in Bangladesh government IP network, thus sensor network is being implemented.

The major benefit for deploying cyber sensor is "Identify Cyber security threats" inside the organization (where the cyber sensor is placed), for example monitor the IP network activity, finding unwanted traffic in network, suspicious/malware related executables downloads into the network. Cyber sensor also provides fast indexing and graphical review platform to index all events for deeper analysis.

After deployment of cyber sensor, organization have better network visibility for network for detecting cyber threats and intrusion traffic: cyber security analyst, cyber security manager or CISO of the organization can take better cyber security defense strategy.
Total 15 unit of Cyber sensors had installed into 11 selected organizations.

The detail description is as below:
Deploying Cyber Sensors for national critical information infrastructure networks (CII) is important and mandatory element of ensuring National Cybersecurity Resilience. It stems from understanding, that what you cannot see, you cannot protect from.

Cyber Sensors should be utilized by integrated methodologies of technical architectures and processes. The success criteria of properly developed cyber sensors are in the following increasing maturity indicators of success:

1. Cyber Sensors technology is successfully deployed;
2. Threat intelligence and detection of attacks and vulnerabilities are analyzed, and CIRT collects Intelligence, processes, and shares back to CII organizations to improve their posture;
3. Incident detection and handling assistance to CII organizations;
4. Threat intelligence research unit.

The CIRT Sensors established by implementing the following items of the sensors:

- Item-1: Cyber Sensors Management Module (CSMM)
- Item-2: Cyber Sensors Network Module (CSNM)

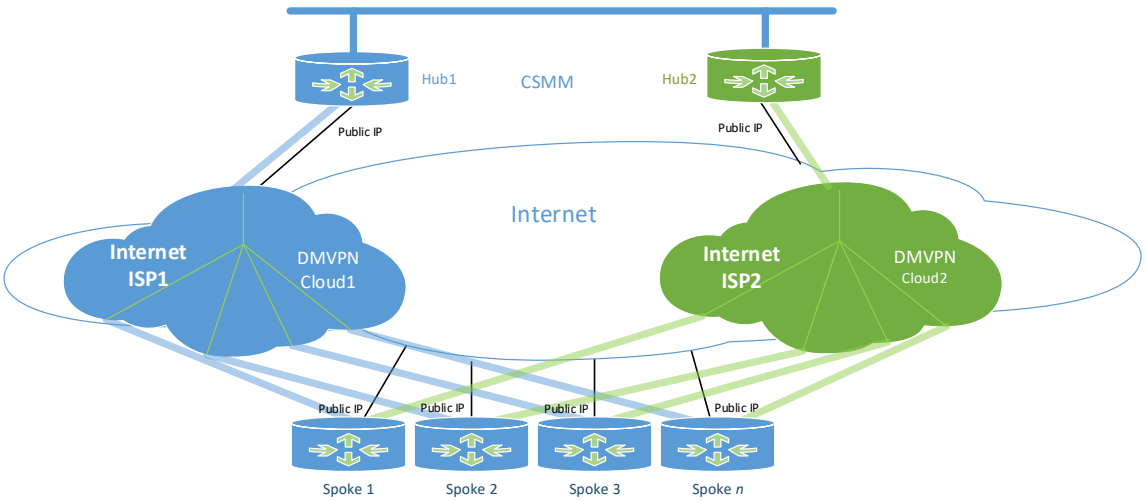
Detailed Functional and Technical Architecture

Technology overview

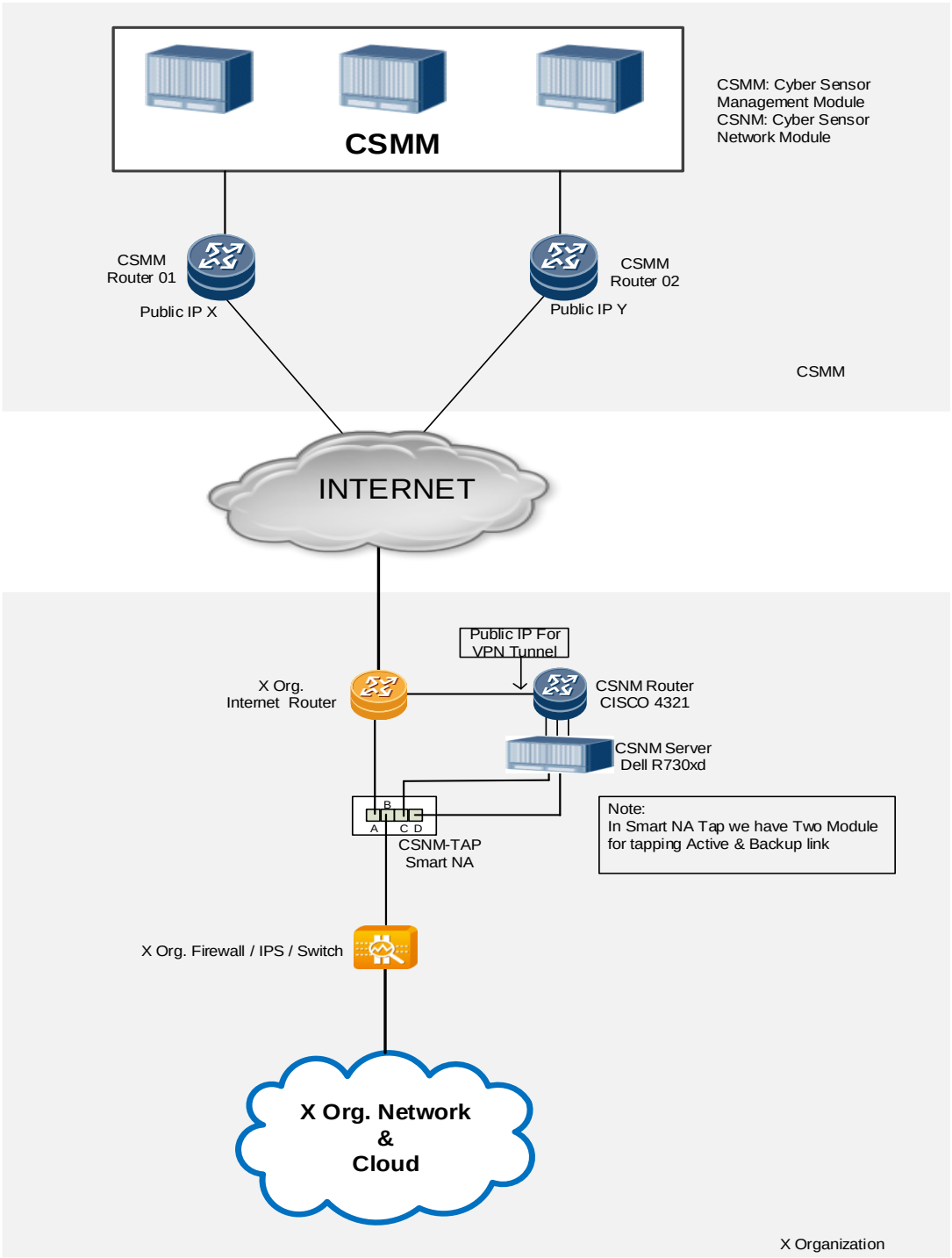
This section defines the reference architecture for implementation of Cyber Sensors into the Critical Information Infrastructure for Cyber Security. It provides technical architectural views for main capabilities of proposed solution and fulfils the scope and requirements specified in the technical proposal. Also it names the most important technologies used in proposed design and explains for what intent whey are used. Some components may already exist in client environment, so they may be changed in favor to utilize current clients' environment and make administration easier.

The core components of proposed Architecture design are:

1. Virtual Private Network (VPN);
2. Cyber Sensors Infrastructure and Services. These infrastructure component and services are covered underneath of proposed design:
   2.1. Network Time Synchronization services (NTP);
   2.2. Domain Name Services (DNS) and Active Directory Services (AD);
   2.3. Distributed implementation of Network Security Monitoring (NSM) using server-sensor model architecture;
   2.4. Virtualization platform;
   2.5. Integration of Threat Intelligence Services;
   2.6. Monitoring Services;



Installation and commissioning of Cyber Sensors into the Critical Information Infrastructure (X Organization) for Cyber Security



Network module contains physical rack with sensing capabilities VPN and data tapping devices:

Cyber sensor operational Dashboard:

Threat Detection Case Study

Threat Detection in BGD e-GOV CIRT sensor Dashboard:

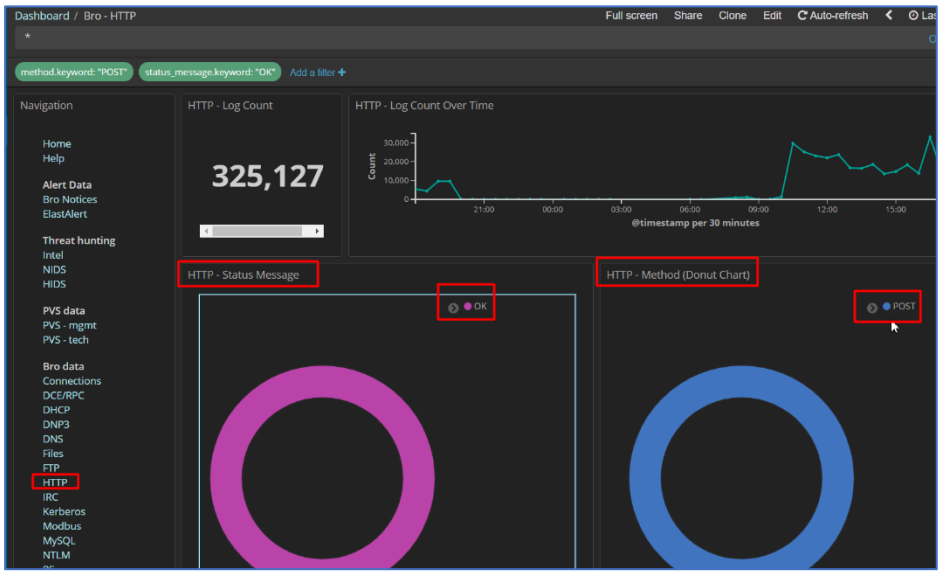
For detecting cyber threat, malware infection, intrusion attempt presently we perform following task:

a. Suspicious HTTP POST Detection from Sensor "HTTP" Section.
b. Suspicious Executable detection in network communication.
c. Suspicious Command Injection detection in overall sensor dashboard available information
d. Infected Host detection
e. Brute-force attack detection

Based on various suspicious communication event, we try to match the information (Specially based on IP address) we will check the IP reputation from various well-known cyber security, malware analysis community information. Each step is listed as below:

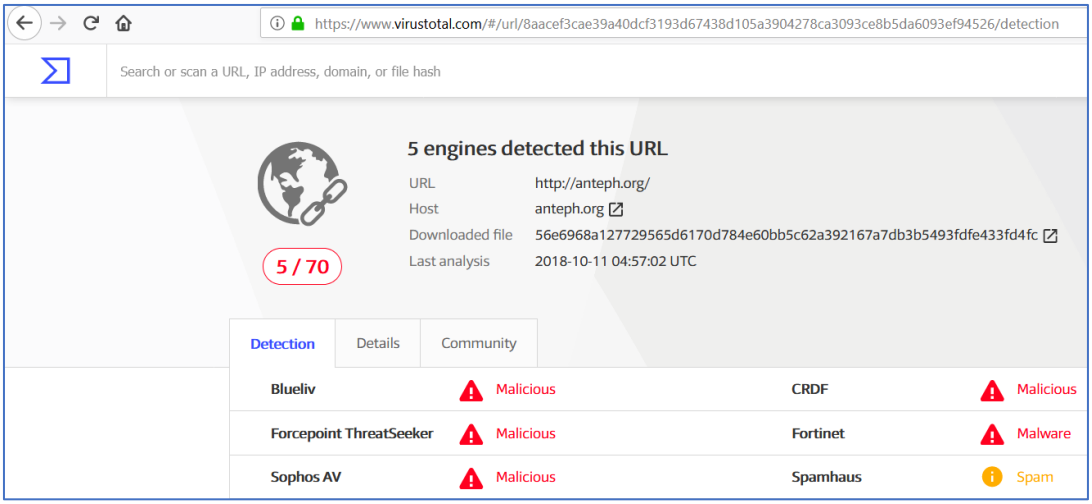
a. Suspicious HTTP POST Detection from Sensor "HTTP" Section.

Step 1: For suspicious HTTP POST detection we need to check the HTTP section. After visit the HTTP section of the dashboard we usually select HTTP Method as POST:

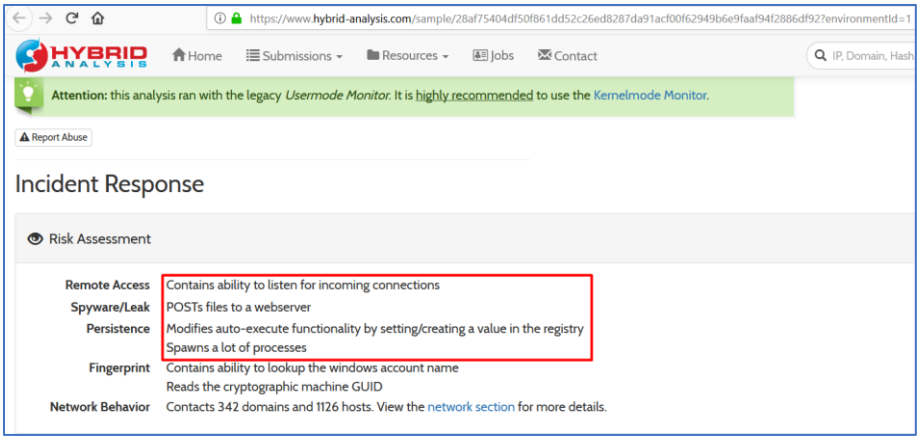


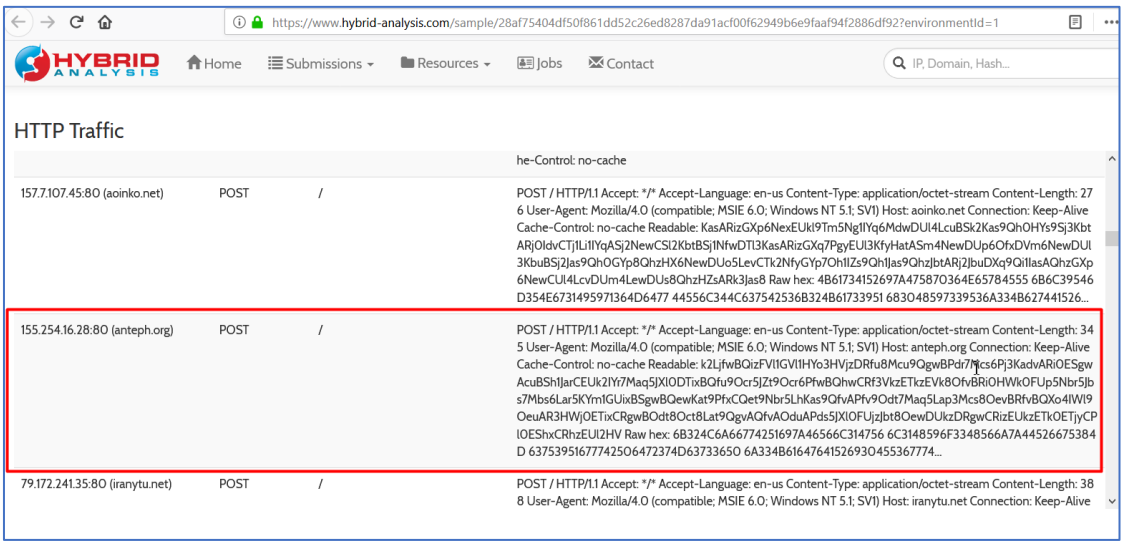
After select the POST method, then we usually investigation manually for detect any suspicious HTTP POST activity, if we detect any suspicious HTTP POST activity, then we need to check the CapME information for further checking as like below:

Step 2: The above CapME information shows the success indication of POST, then we check the URL along with POSTED parameter in well-known community, for example virustotal.com (for check the suspicious domain name reputation), then we found, for example: The related destination domain is listed virustotal.com as malware host.



As per community information, the infected computer system will POST various information to external malware hosting IP and the infected computer system tried to modifies functionality in the registry & spawned lot of process and it also try to write shellcode in infected hosts, there is also high possibility the infected system accepts un-authentication incoming connection from external hosts for example:



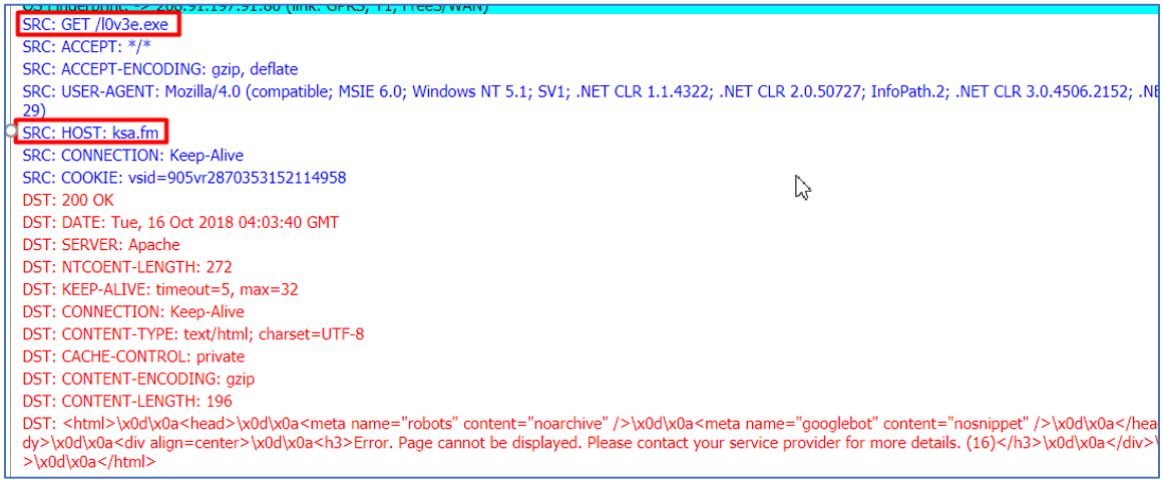


Step 3:

Form the community information & sandbox analysis information, this is clearly indicating this HTTP POST communication is a MALWARE communication.

b. Suspicious Executable detection in network communication.

From the sensor communication event, we detect some executables ware downloaded into internal organization computer system. The executable name is not seeming a valid executable. For example:

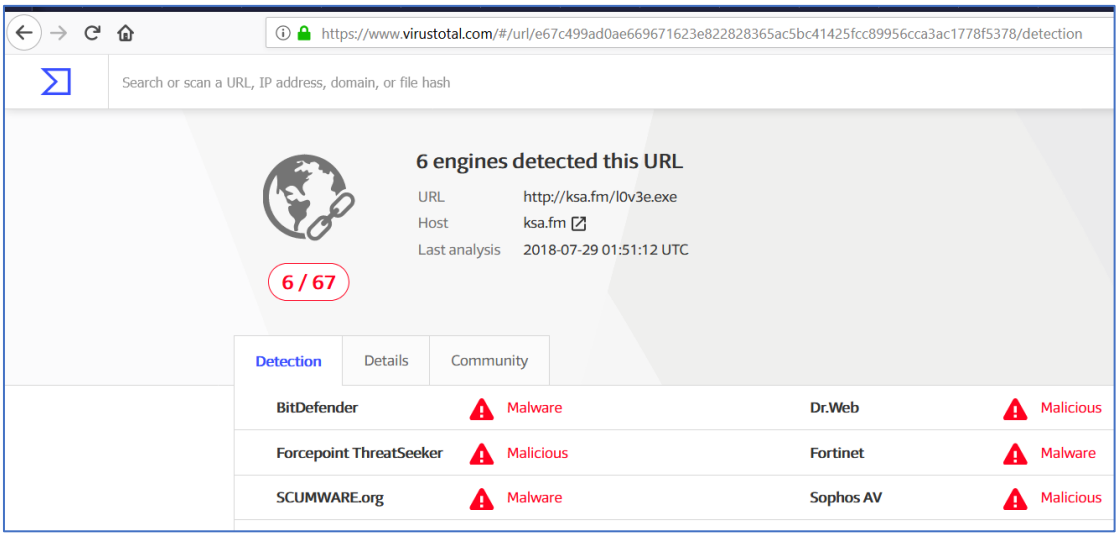


From this commination we detect following information:

Destination IP	**Possible TCP Method**
208.91.197.91(British Virgin Islands) Domain: ksa.fm	HTTP Possible executable name: l0v3e.exe

We can check the reputation of the IP address from available source. We can also check the executable with well-known community for example, virustotal.com.

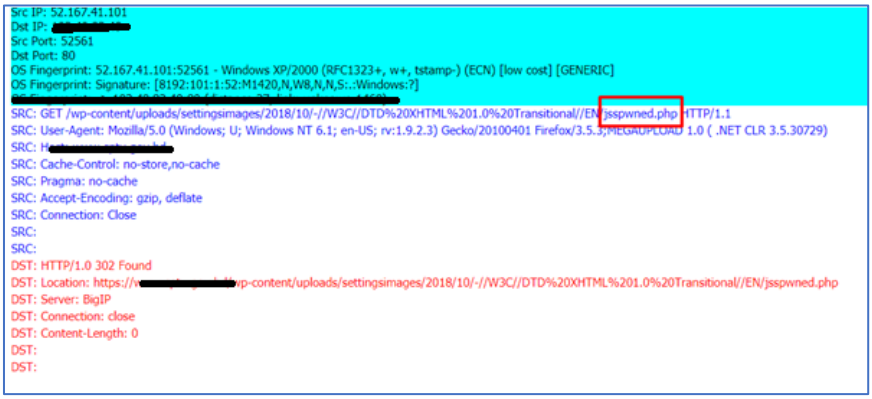
In community this domain and executable considers as malware, for example:

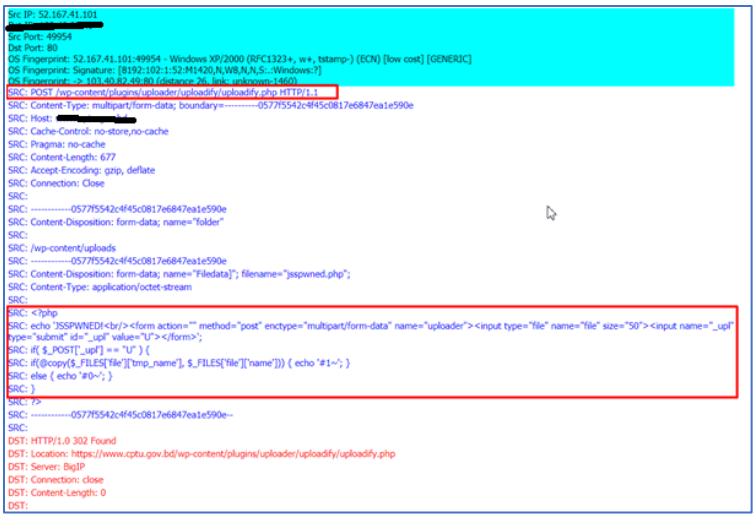


Form the community information, this is clearly indicating this IP communication & downloaded executable is a MALWARE.

c. Suspicious Command Injection detection in overall sensor dashboard available information

From the system available information, we may detect same unusual activity from various IP address and all this IP address try to attack target one system and the activity is considering as Intruder attack, because all of these IP address perform similar task and try to perform "Command Injection" to target system. For example:

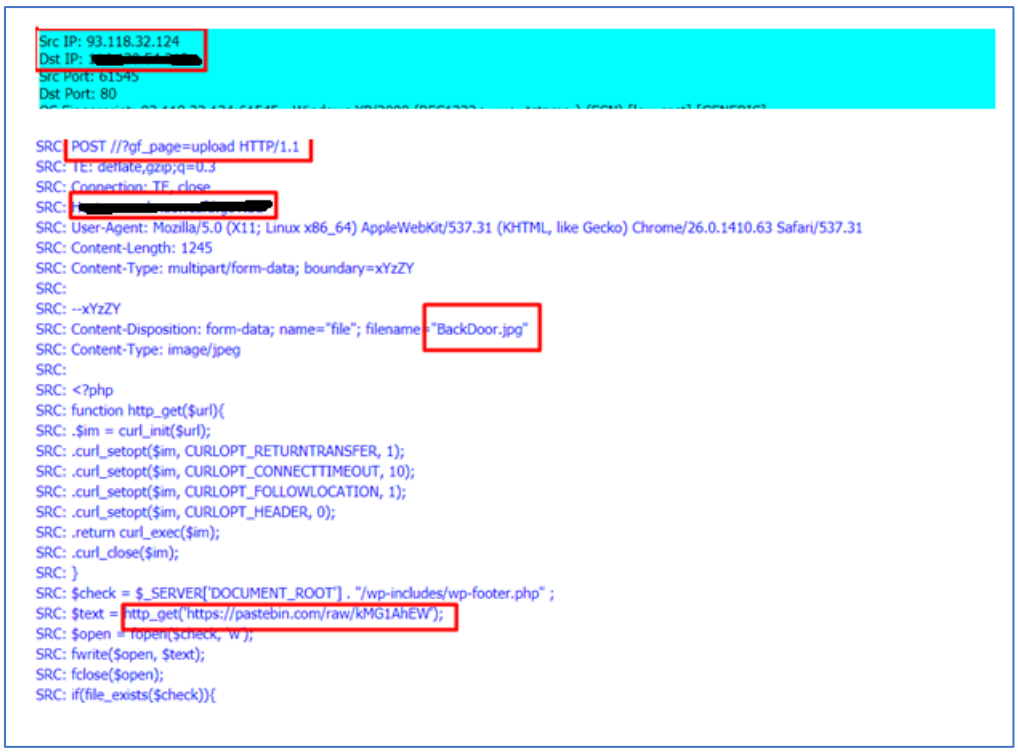




We found same activity from the external source, which we highly suspect this is an intruder team which is targeting the organization. By this way, after detect these types of suspicious activity, we can information to respective organization for taking necessary action/measure.

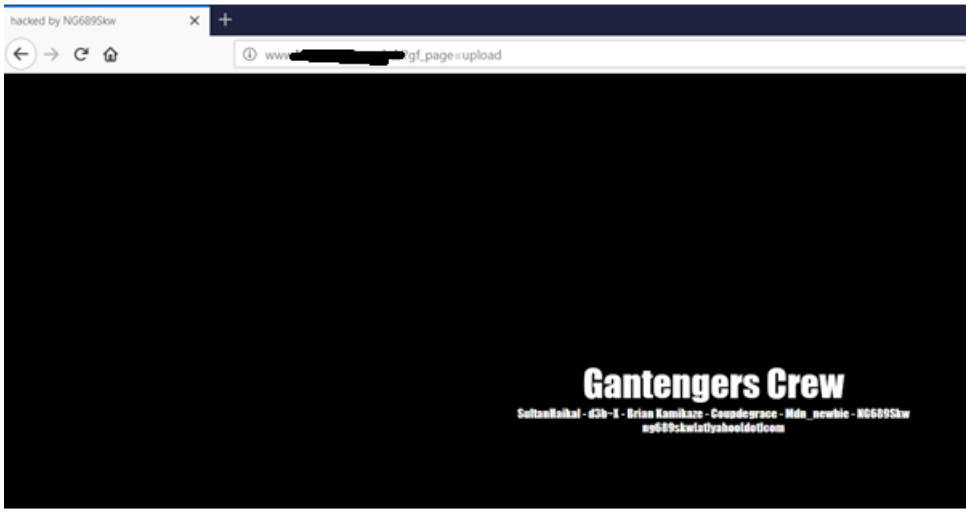
d. Infected Host detection

From the system available information, by analysis various information, we can able to detect infected/compromised host into the network, for example, we detect some suspicious HTTP POST activity and we found some well-known system compromise related keyword (for this case, backdoor):



Then we can visit the respective URL, which is hosted into our trusted network (i.e. Organization network)

We found below possible web based backdoor as like below:



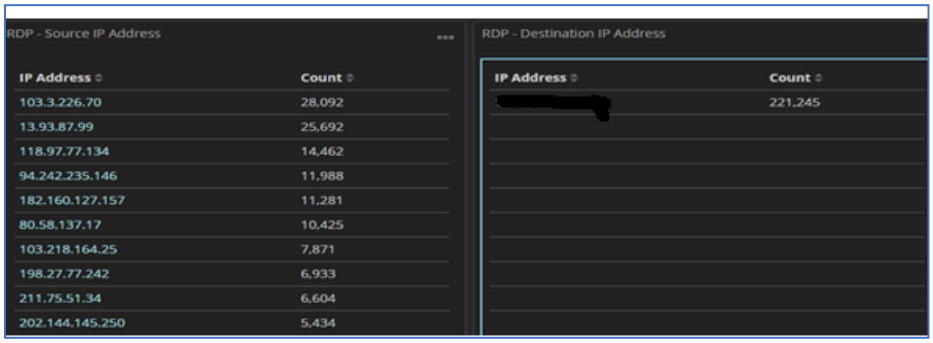
By this way, after detect these types compromise host into network, we can information to respective organization for taking necessary action/measure.

e. Brute-force attack detection

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack is also known as brute force cracking or simply brute force.
If some system expose SSH or RDP activity to external or Internet, it may face brute force attack. For detecting the RDP brute force attack, in the sensor dashboard, we can select RDP and check the RDP failure attempt, which can help us to make decision whether the system fallen under brute force attack or not. For example:

We found from various external IP targeting one system of the organization, the RDP attempt is not in usual number (huge attempt)



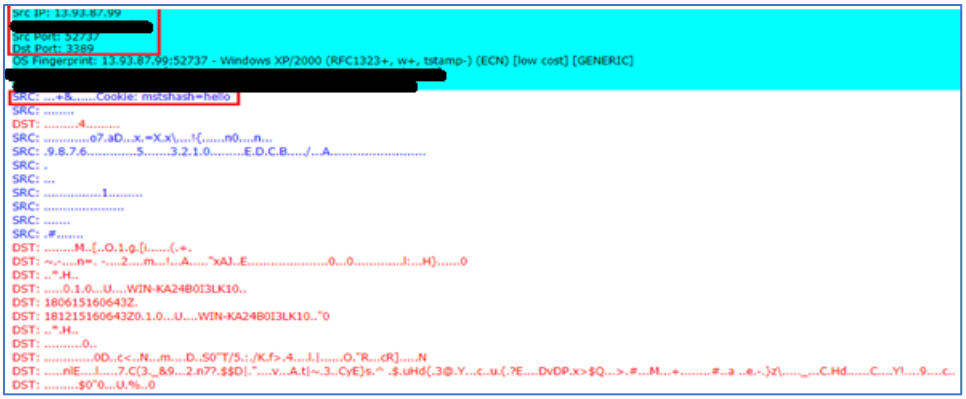
RDP - Source IP Address

IP Address	Count
103.3.226.70	28,092
13.93.87.99	25,692
118.97.77.134	14,462
94.242.235.146	11,988
182.160.127.157	11,281
80.58.137.17	10,425
103.218.164.25	7,871
198.27.77.242	6,933
211.75.51.34	6,604
202.144.145.250	5,434

RDP - Destination IP Address

IP Address	Count
[redacted]	221,245

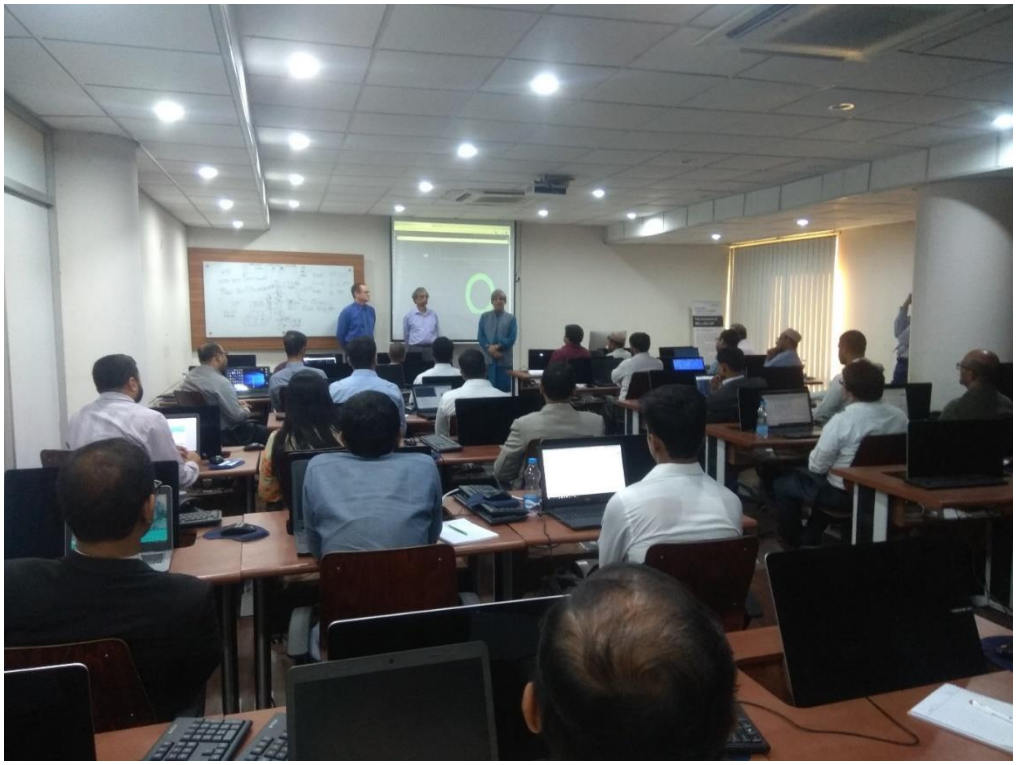
We can check related CapME data for more clarification:



By this way, after detect these types attack we can information to respective organization for taking necessary action/measure.

Cyber Sensor Training

BGD e-GOV CIRT Provided “Cyber Sensor Operation Training” to nominated persons from CII Organizations.



Cyber Sensor Analysis Report

From August 2018 to May 2019, a total 57 (Fifty-Seven) cyber sensor analysis report provided to 11 (Eleven) Bangladesh Government Critical Information Infrastructure (CII).

3. Digital Forensic Lab Unit

Forensic Lab established on 2018, with the purpose of forensic investigation of digital evidence. It helps the incident handling unit as reactive service after an incident occurs by providing forensic support on evidence included in the incident. Digital Forensic team is also capable of recovery and investigation of material found in digital device including mobile, PC, Drone or any IOT's or computational devices. The objective of CIRT LAB is also to build capacity of students and government officials who are keenly interested in cyber security and digital forensic.

Benefits:

- Helps the incident handling unit as reactive service after an incident occurs by providing forensic support on evidence.
- Build capacity of students and government officials on Cyber Security
- Criminal prosecutors – Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- Civil litigation- Personal and business data discovered on a computer can be used in fraud, harassment or discrimination cases
- Financial Organizations – Evidence discovered on computer can be used to mollify costs
- Law enforcement officials – Rely on computer forensics to backup search warrants and post-seizure handling

CIRT Lab Capabilities:

- Computer Forensic – Can be used to recover important data, deleted logs, any criminal activities which is deleted intentionally. Current capacity:
    - Write Blocker
    - Imager
    - Forensic Analysis Suite
    - Password Breaker

- Mobile Forensic – Mobile device forensic investigation to detect any criminal activities performed in mobile device

- Network Forensic – monitoring and analysis of computer network traffic for the purposes of information gathering of network anomaly, legal evidence, or intrusion detection. **Network forensics** is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Current Capacity:
    - Honeypots
    - Network Data Tapper
    - SSL Decrypting Device

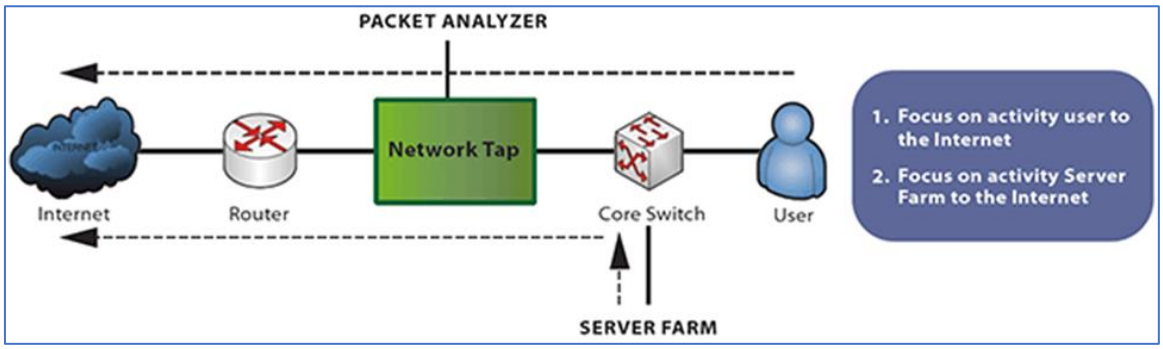


Fig: Network Forensic

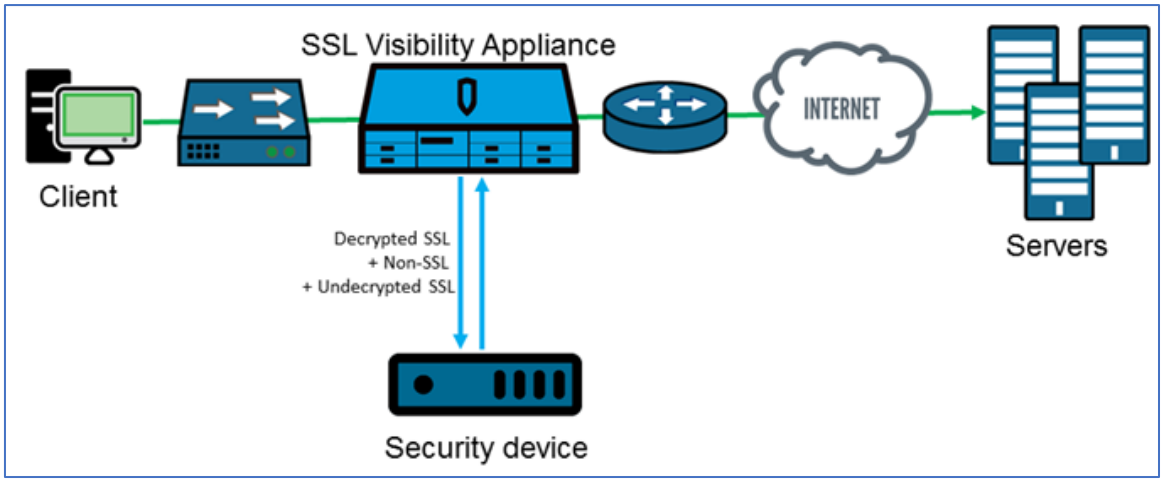


Fig: SSL Decrypting Methodology


Fig: Honeypot Device

Service Workflow follows:

- Evidence Detection
- Evidence Acquisition
- Evidence Analysis/Examination
- Documenting and Reporting

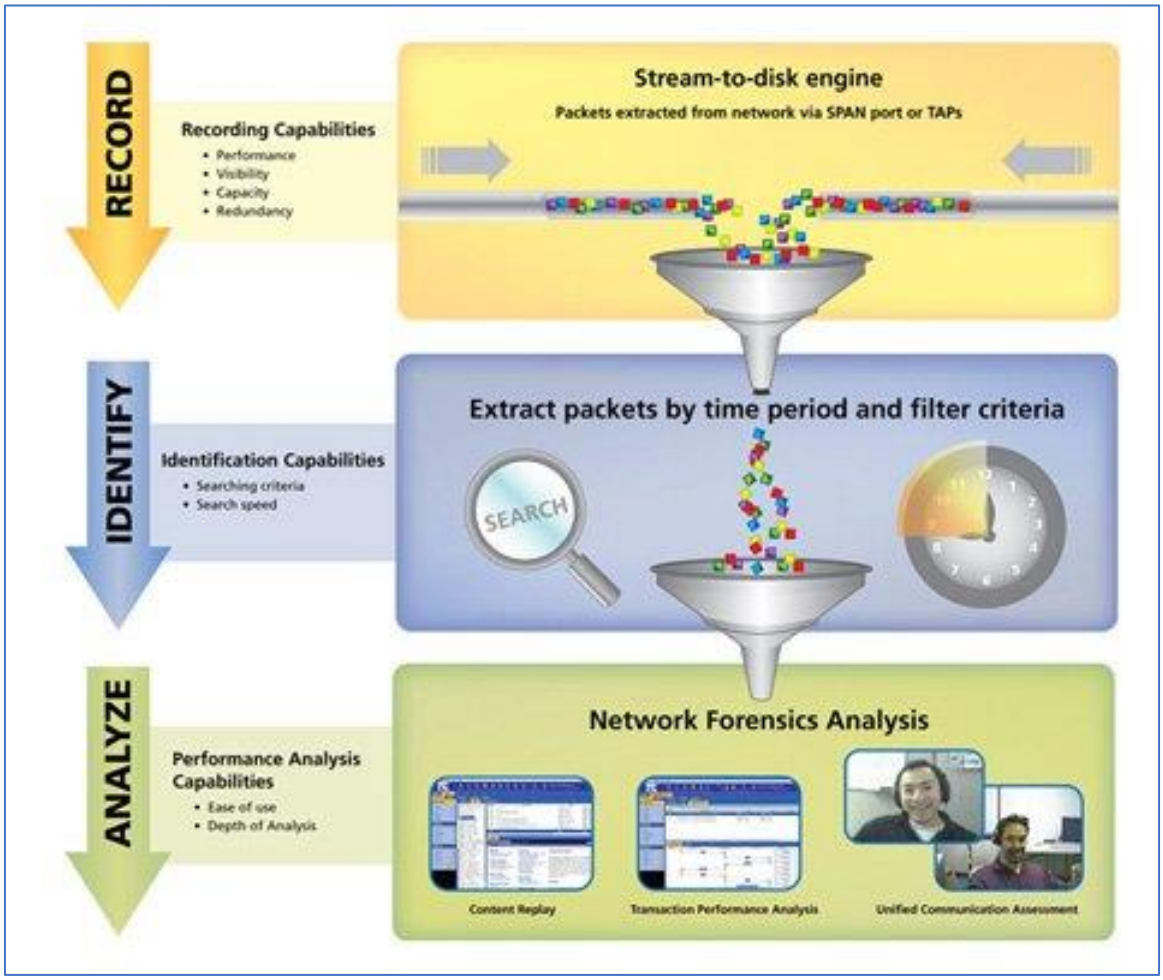


Fig: Digital Forensic Service Workflows

Ongoing Service:

a) Providing monthly threat intelligence report based on network forensic and feed data.

b) Successfully delivered four (4) government cases till January 2019.

Our strengths upon case analysis:

- Data recovery and analysis.
- Image data analysis.
- Email data analysis.
- Ransomware related analysis and data recovery.

Fig: Inauguration of CIRT Lab by Honourable Adviser of ICT

Fig: Inauguration of CIRT Lab by Honourable Adviser of ICT

বঙ্গবন্ধুর সৌহিত্র ও প্রধানমন্ত্রীর তথ্যপ্রযুক্তি বিষয়ক উপদেষ্টা সজীব ওয়াজেদ জয় ২৬ জুলাই ২০১৮ ইং তারিখ বৃহস্পতিবার আগারগাঁওয়ের আইসিটি ভবনে বাংলাদেশে প্রথম সফটওয়্যার টেস্টিং ল্যাব এবং হ্যাকিং প্রতিরোধে 'কম্পিউটার ইন্সিডেন্ট রেসপন্স টিম ল্যাব' এর উদ্বোধনী অনুষ্ঠানে বক্তব্য রাখেন - ইয়াসিন কবির জয়/ফোকাস বাংলা নিউজ

Fig: Inauguration of CIRT Lab by Honourable Adviser of ICT

Fig: Training on EnCase Digital Forensic Analysis

Fig: Honourable state minister in BGD e-GOV CIRT's First Anniversary conference

Fig: BGD e-GOV CIRT member participating in MTCP fellowship – A Malaysian government training scholarship on Cybersecurity

Fig: BGD e-GOV CIRT member participating in MTCP fellowship – A Malaysian government training scholarship on Cybersecurity

Fig: BGD e-GOV CIRT member participating and representing Bangladesh Cyber Security Unit in MTCP fellowship – A Malaysian government training scholarship on Cybersecurity

Fig: BGD e-GOV CIRT member participating APCERT 2018 Annual Conference, Shanghai, China

Fig: BGD e-GOV CIRT member participating in AGM and Voting of APCERT 2018, Shanghai, China

Fig: BGD e-GOV CIRT member participating and presenting Bangladesh Government Cyber Security Unit in 56th TF-CSIRT meeting & FIRST Regional Symposium Europe After being accredited Member

Fig: BGD e-GOV CIRT member receiving fellowship for participating FIRST 2018 Annual Conference, Kualalumpur, Malaysia

4. Cyber Security Strategy & Risk Assessment Framework Development

a. Establishment of Bangladesh cyber threat landscape in order to have a holistic understanding about national cyber threat landscape and better align the objectives of the strategy with national security needs.

Identification of emerging trends in cyber threats and understanding the evolution of cybercrime is very important to national cybersecurity and enables effective responses to cyber risks. There is a number of international or regional cyber threat landscape reports and they provide important insights in the international developments regarding cyber threats. However, each country has its own peculiarities and it is vital to understand national cyber threat landscape to build necessary cyber capabilities and effectively mitigate cyber risks.

Bangladesh national cyber threat landscape report defines top cyber threats to Bangladesh, their relations with threat agents, specific attack vectors used to launch a particular threat and kill chain for it. Each cyber threat is assigned to one of the incident classes used by BCC.

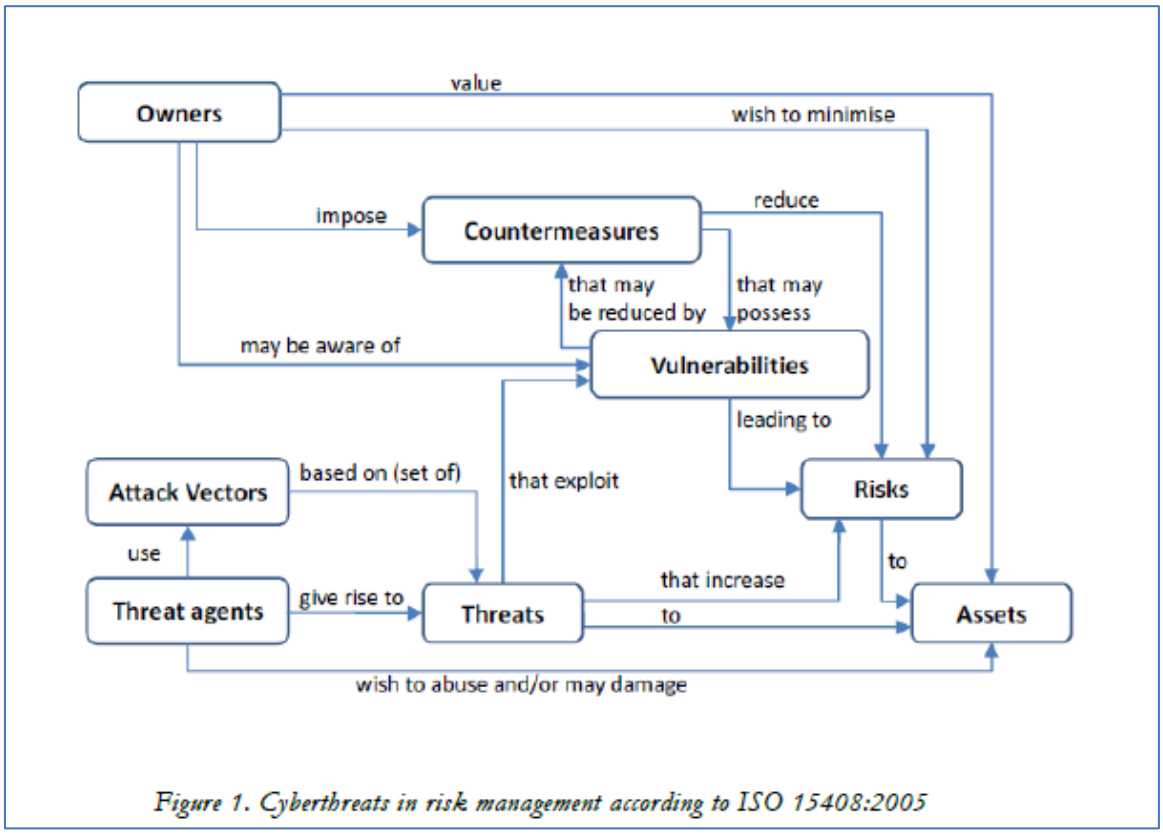


Figure 1. Cyberthreats in risk management according to ISO 15408:2005

For the development of Bangladesh cyber threat landscape, a workshop with different organizations was held on July 2018. Participants of the workshop were introduced to the trends in cyber threat landscape since 2015 and ENISA's top 15 cyber threats for 2017. Based on the results of an anonymous survey of workshop participants, Bangladesh top 15 cyber threats have been identified and are recorded.

Workshop on: cyber threat landscape

b. Assessment of Bangladesh cyber maturity to identify strengths and gaps in a current status of Bangladesh cyber security maturity

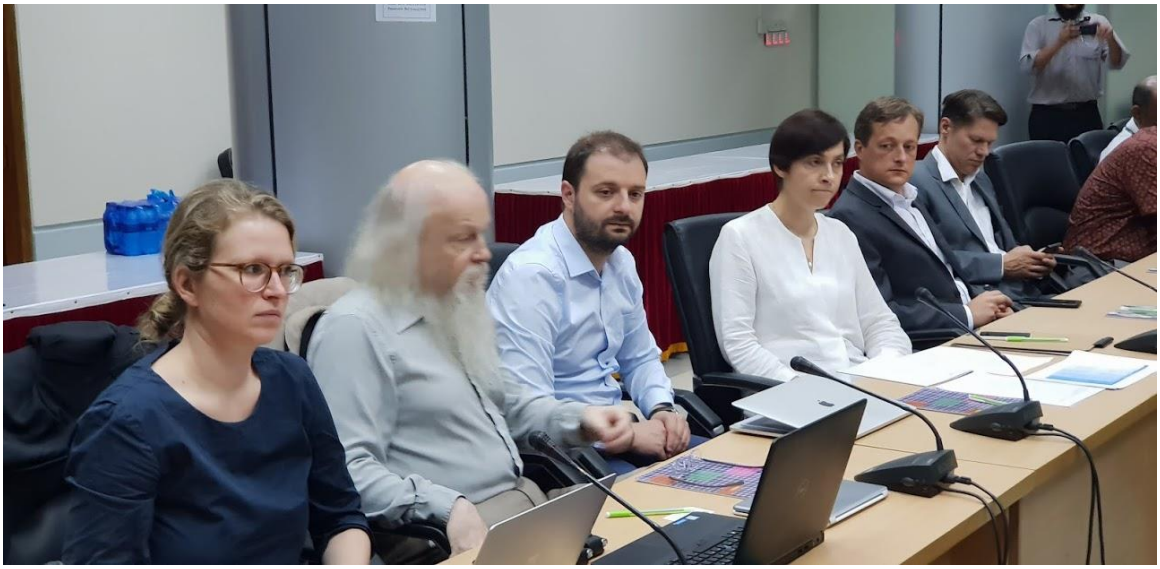
In collaboration with NRD Cyber Security (NRD CS), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') Oxford undertook a review of the maturity of cybersecurity capacity in Bangladesh at the invitation of the Bangladesh Computer Council (BCC). The objective of this review was to enable Bangladesh to gain an understanding of its cybersecurity capacity in order to strategically priorities investment in cybersecurity.

Over the period 2-4 July 2018, the different stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies and the banking sector. Remote follow-up interviews were conducted with representatives from civil society and international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five dimensions of cybersecurity capacity:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organizations, and Technologies

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations.



Roundtable consultations on Bangladesh Cyber Maturity

Cyber Risk Assessment Framework Development

The module envisages a series of activities aimed at establishing cyber risk assessment framework to strengthen the resilience of Bangladesh Critical Information Infrastructure CIIs and provide guidelines for its implementation.

Module activities focused on defining and establishing processes to identify, analyze and manage country-specific risks to Bangladesh CIIs in order to ensure smooth functioning of essential information and communication systems under ordinary circumstances and continuity on a minimum level during critical situations.

All module activities include on-site engagements with the Client, owners of CIIs, transfer of knowledge and awareness raising activities and conducted on the basis of international best practices.

Activities envisaged under this Module are:

a. Development of cyber risk assessment framework for Bangladesh CIIs

Bangladesh critical infrastructures (CI) operate in financial services, telecommunications, energy supply, air transport and government services and are essential for the maintenance of vital society functions, health, safety, security, economic and social well-being of people. Today, information and communication technologies are becoming increasingly important for the functioning of critical infrastructure. Such essential information and communication infrastructures, also referred to as national critical information infrastructures, need to be protected in order to deter, mitigate and neutralize threats, risks or vulnerabilities and minimize the impacts of the incidents should they occur. More smart technology will be introduced to many critical processes in Bangladesh and it will mean increased dependency on data traffic systems and the Internet and ICT disruptions will have a greater impact on various critical services.

Critical information infrastructures can be disrupted by natural disasters, such as floods or earthquakes, or by deliberate attacks of malicious actors. Bangladesh national critical information infrastructures are regular target of cyber-attacks. As ICT knowledge and technology will become more accessible to malicious actors, the likelihood of cyber-attacks in Bangladesh critical infrastructures may increase. Due to inter-dependency of Bangladesh critical infrastructures, the disruption of one critical information infrastructure can have cascading effectives across sectors and paralyze the provision of services in other sectors. The disruption of critical services in Bangladesh ICT/ telecommunication sectors and financial sectors would have most severe cascading effects.

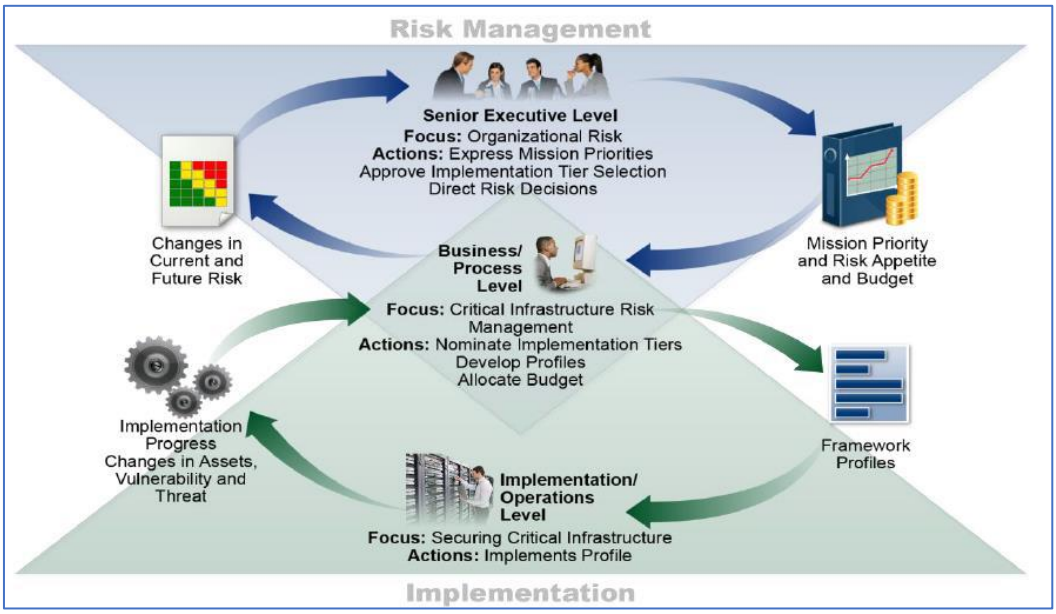
Managing risks is a shared responsibility among all critical information infrastructure stakeholders, including government organizations, industry partners, first responders and nongovernment organizations.

The purpose of cyber risk assessment framework for CIIs is to provide a centralized cyber risk assessment model that will be applicable to all Bangladesh CIIs and will implement a coordinated, all-hazards framework to critical infrastructure risk management. Moving forward with this comprehensive risk management process requires Government of Bangladesh and agencies to collaborate with their critical infrastructure partners, including other industry stakeholders. This framework promotes a common approach to critical infrastructure risk management and owners. Each CII is responsible for applying a risk management approach within its organization.

The framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:20092, ISO/International Electrotechnical Commission (IEC) 27005:20113. Framework's assets identification is prepared applying ENISA's recommendations "Threat Landscape and Good Practice Guide for Internet Infrastructure"4.

Cyber risk assessment framework for CIIs is based on a common flow of information and decisions during risk management process. Figure 1 depicts information and decision flows within an organization at three different levels:

- Executive level
- Business/Process level
- Implementation/Operations level



The executive level communicates to the business/process level:

- the mission priorities
- available resources
- overall risk tolerance

The business/process level:

- uses the information as inputs into the risk management process, and then
- collaborates with the implementation/operations level to communicate business needs and
- create a risk profile

The implementation/operations level:

- communicates the Profile implementation progress to the business/process level

The business/process level:

- uses this information to perform an impact assessment
- reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact

Cyber risk assessment framework presentation to CIIs

b. Conducting risk assessments of CIIs using the developed cyber risk assessment framework in order to validate its effectiveness and suitability.

The objective of the cyber risk assessment of 3 CIIs was to validate the Cyber risk assessment framework and Implementation guidelines for the cyber risk assessment framework developed in the earlier stages of the project which are planned to be used by all Bangladesh CIIs.

During the assessment, cyber risk assessment framework and implementation guidelines for the cyber risk assessment framework were used to identify cyber risk levels of the three selected CIIs and to prepare risk mitigation plans for the unacceptable risks.

The purpose of the cyber risk assessment of 3 CIIs was to provide a detailed high-level assessment on how cyber threats impact their assets and whether implemented risk mitigation measures and security controls are sufficient, effective and practical to contain unacceptable risks.

The scope of the cyber risk assessment was the evaluation of the resilience of critical assets of 3 selected CIIs against Bangladesh cyber and environmental threats list. The report is not

intended to evaluate, disclose and describe all information (documents, processes, functions or systems) of a particular critical infrastructure and is based solely on the information provided by the owners of the CIs.

	Threats	Organisation 1	Organisation 2	Organisation 3	∑ (3 CII)
1	Malware	512	384	128	341
2	Spam	333	444	333	370
3	Failure or Disruption of Communication Networks	325	217	217	253
4	Failure or disruption of third party service providers	269	179	179	209
5	Web application attacks	263	302	175	247
6	Web based attack	261	261	174	232
7	Phishing	346	259	173	259
8	Failure or Disruption of the Power Supply	249	166	166	193
9	Botnets	221	110	110	147
10	Ransomware	310	106	106	174
11	Insider threat	158	106	106	123

Sample report format Risk Assessment

c. Information system establishment for cyber risk assessments and compliance management (CRACM)

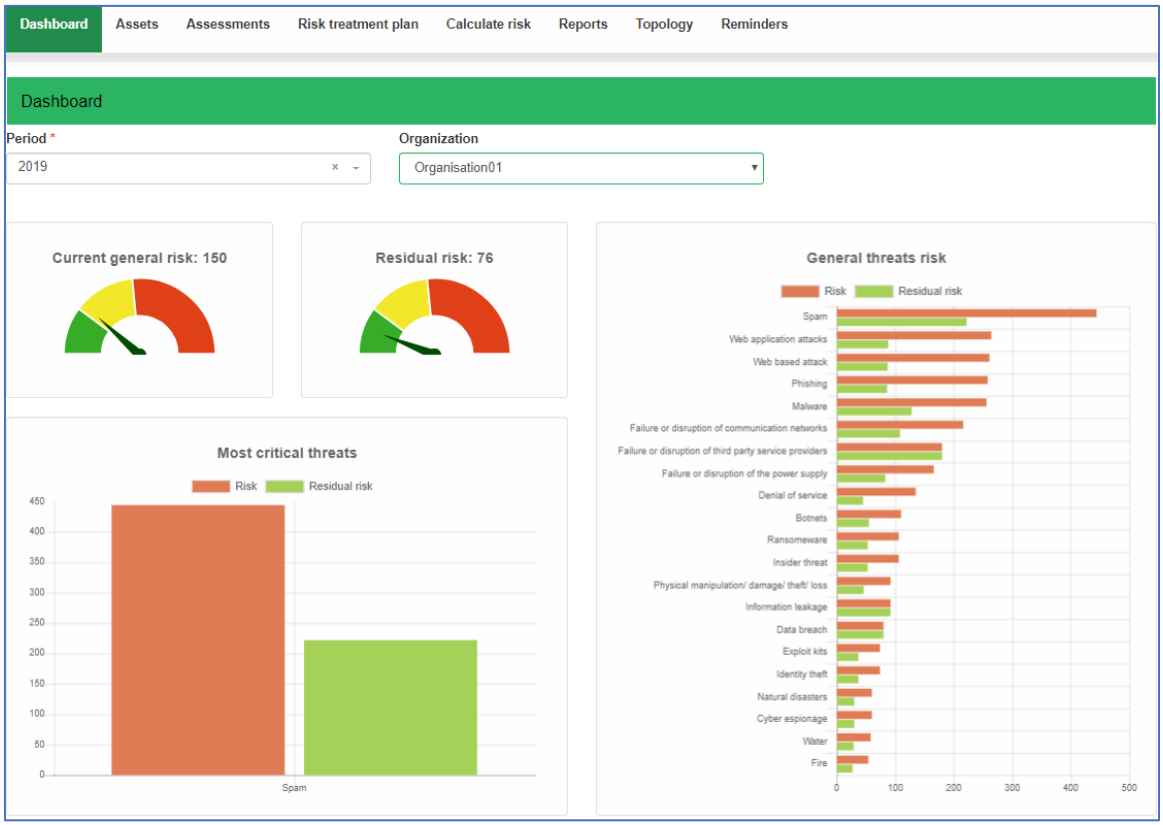
Establishment of CRACM is enable the BCC to be up to date with the current Bangladesh CII cyber security posture, monitor and assess the progress based on the common taxonomy of standards, guidelines and practices and ensure communication with internal and external stakeholders about cyber security risk.

Benefits are:

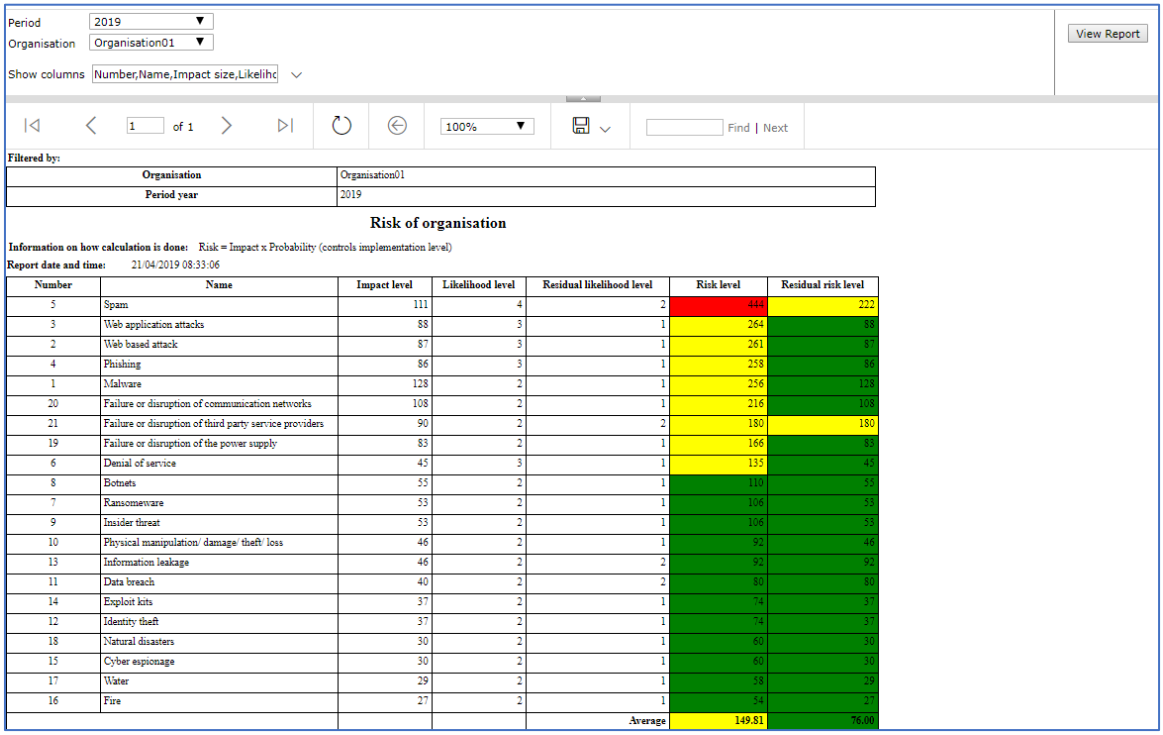
- Organization assets identification
- Bangladesh cyber threats understanding
- Tool for Organization IT controls evaluation (ISO 27001 Monitoring)
- IT risk level calculation
- IT risk treatment plan for organization
- Bangladesh IT risk evaluation

Outcomes

1. Organizations Risk Management Dashboard



2. Report “Risk of organization"



Filtered by:

Organisation	Organisation01
Period year	2019

Risk of organisation

Information on how calculation is done: Risk = Impact x Probability (controls implementation level)

Report date and time: 21/04/2019 08:33:06

Number	Name	Impact level	Likelihood level	Residual likelihood level	Risk level	Residual risk level
5	Spam	111	4	2	444	222
3	Web application attacks	88	3	1	264	88
2	Web based attack	87	3	1	261	87
4	Phishing	86	3	1	258	86
1	Malware	128	2	1	256	128
20	Failure or disruption of communication networks	108	2	1	216	108
21	Failure or disruption of third party service providers	90	2	2	180	180
19	Failure or disruption of the power supply	83	2	1	166	83
6	Denial of service	45	3	1	135	45
8	Botnets	55	2	1	110	55
7	Ransomeware	53	2	1	106	53
9	Insider threat	53	2	1	106	53
10	Physical manipulation/ damage/ theft/ loss	46	2	1	92	46
13	Information leakage	46	2	2	92	92
11	Data breach	40	2	2	80	80
14	Exploit kits	37	2	1	74	37
12	Identity theft	37	2	1	74	37
18	Natural disasters	30	2	1	60	30
15	Cyber espionage	30	2	1	60	30
17	Water	29	2	1	58	29
16	Fire	27	2	1	54	27
				Average	149.81	76.00

5. IT Audit Unit

The mission of IT Audit is to provide an independent, objective assurance and consulting activity designed to add value and improve the organization's operations. IT Audit aims to help the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. BGD e-Gov CIRT's IT Audit team performs extensive IT audit for 3 (Three) Bangladesh Government Critical Information Infrastructure (CII) till May, 2019.

6. Awareness Building

Awareness is the ability to directly know and perceive, to feel, or to be cognizant of events. More broadly, it is the state of being conscious of something. The primary goal of awareness is to reach the message to the end user about the current cyber threat and its mitigation. It is very hard-hitting to reach every people about every incidents of cyber security or cyber threat and aware them continuously.

BGD e-GOV CIRT is also working for awareness of its constituencies. It publishes posters, leaflets, newsletters, web sites that explain security best practices and provide advice on precautions to take.

It publishes awareness article in English as well as local language for better understanding of its stakeholder. It frequently published the reports regarding the assessment of stakeholder application including the vulnerability and weakness. Additionally the quarterly, semi-annual, annual reports are published.

BGD e-GOV CIRT arrange workshops, seminar, and conferences for its constituencies. For preparing the stakeholders it arranges different level training session for different stakeholder. The training helps the stakeholder up-to-date with ongoing security knowledge and potential threats to the information security.

Our Android Mobile App: https://play.google.com/store/apps/details?id=com.cirt.axion.bdcirt

Social Media for awareness:

- Facebook: https://www.facebook.com/bgdegovcirt/
- LinkedIn: https://www.linkedin.com/company/bgdegovcirt
- Twitter: https://twitter.com/bgdegovcirt

High Commissioner of India, Dhaka visits BGD e-GOV CIRT Operations Center

High Commissioner of India, Ms Riva Ganguly Das has visited BGD e-GOV CIRT Security operations center on 19 July, 2019. She visited different components of BGD e-GOV CIRT and got briefed about the daily activities of security operations center, cycler censor activities, cyber range lab and digital forensic lab. Hon'ble state Minister Zunaid Ahmed Palak MP, Secretary of ICT Division N M Zeaul Alam, Executive Director of Bangladesh Computer Council Parthapratim Deb and Project Director of LICT project Md. Rezaul Karim was present at that time.

Fig: Brief on Cyber Sensor Operations

BGD e-GOV CIRT is working very closely with Indian Computer Emergency Response Team (CERT-In) and they have signed a MoU as well On “Cooperation in the area of Cyber Security” between

Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Ministry of Post, Telecommunication and IT and Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, India on April 2017, During Prime Minister Sheikh Hasina's Visit to India (Link of that news). BGD e GOV CIRT is Member of IoT Security Working group, Secure Digital Payment Working Group of CERT-In as well.

Human Resource Development

Development of human resources is essential for any organisation that would like to work with specialized task. Unlike other resources, human resources have rather unlimited potential capabilities which can be used by creating an environment that can continuously identify, bring to surface, nurture and use the capabilities of people. Training is one of the methods to materialize the organization goal.

BGD e-GOV CIRT introduced various specialized training to its employee, stakeholders and its beneficiaries. BGD e GOV CIRT has conducted a number of training to address the shortage of cyber Security professionals in Bangladesh Government Sector.

In total, BGD e-GOV CIRT provided various cyber Security related trainings to 1578 (One thousand Five Hundred & Seventy-Eight) Bangladesh officials.

The main stakeholders of BGD e-GOV CIRT are as follows:

Armed Police Battalion (APBN), Access to Information (A2i), Different Ministries, Secretariat, CID, Bangladesh Air Force, Bangladesh Army, Bangladesh Bank, Bangladesh Bureau of Statistics, Bangladesh Computer Council, Bangladesh Election Commission, Bangladesh Hi-Tech Park Authority, Bangladesh Navy, Bangladesh Police, Bangladesh Supreme Court, Bangladesh Tariff Commission, Bangladesh Telecommunication Regulatory Commission, Bangladesh Telecommunications Company Ltd., Different Bank & Financial Institution, BARC, BARD, BASIS and other government organization.

The statistics of training conducted by BGD e-GOV CIRT are follows:

SL	Training Name	Participant Number
1.	Accounting Fraud Investigation	18
2.	Business Continuity Training	54
3.	Business Intelligence	22
4.	Certified Ethical Hacker (CEH)	45
5.	Certified Secure Computer User	62
6.	Cyber Investigation	84
7.	Cyber Security Training	54
8.	Cybersec First responder	21
9.	E-Government Public Service Transformation	225
10.	Information Management	22
11.	Information Technology Infrastructure Library (ITIL)	33
12.	IT Governance, Data Governance & Protection	105
13.	IT-Project Management Training	40
14.	Managing Technology for e-government	291
15.	OSINT (Analytics)	36
16.	Penetration Testing	84
17.	Social Media Course	18
18.	The Stanford Advanced Project Management (SAPM)	57
19.	Training on Binary Analysis	37
20.	Training on Malware Analysis	37
21.	Training on Managing Digital Forensic Lab	17
22.	Training on Network Traffic Analysis	15
23.	Training on Oxygen Forensic Complete	23
24.	Training on Reverse Engineering	37
25.	Vulnerability Assessment	84
26.	WSO2 API Manager	66
	Total	**1587**

Conferences

The CIRT team of Bangladesh Computer Council is increasingly creating awareness of the need to seriously address the daunting challenges of protecting their information networks, especially those related to national security and critical infrastructures, from any attacker. The cyber-security question needs to be placed within a larger framework of international cooperation, norms, and rules for appropriate and responsible state behavior that will ensure the peaceful use of cyberspace.

On this regard, the government in collaboration with cyber security and tech giants has successfully organized an international cyber security conference on 9 March 2017.

Leveraging ICT for Growth, Employment and Governance (LICT) of ICT Division, US based Fire Eye, CISCO, CA Technologies, Microsoft, One World InfoTech, Europe based NRD AS and Bangladesh Based companies NRD Bangladesh Ltd. & REVE Systems has jointly organized the conference at auditorium of Bangladesh Computer Council (BCC).

Honorable State Minister for ICT Zunaid Ahmed Palak, MP inaugurated the conference, which was attended by over 200 diplomats, government officials and many local and foreign cyber security experts.

Meeting & Seminar

To address the cyber security challenges faced by the Bangladesh government, BGD e-GOV CIRT arranged seven (7) meetings, chaired by the State Minister for ICT Zunaid Ahmed Palak at ICT Division.

Main outcomes of these meeting include:

- Identification and preparation of a list of 25 Critical Infrastructures in Bangladesh;
- Review and approval of the "Government of Bangladesh Information Security Manual";
- Dissemination of the "Government of Bangladesh Information Security Manual" among the identified 25 Critical Infrastructures of the country as well as to other Government organizations & officials;
- Discussion regarding the existing cyber act and the new digital security act;
- Representatives from critical infrastructures shared their ideas and took necessary measures to ensure Cyber Security in their organizations;
- Knowledge sharing session regarding new threats and attack vectors;
- Presentations from Cyber Security Experts.

Conclusion

From the previous data and work experience we can take a supposition that Cyber Attacks within country are rising and the top types of attacks are information gathering, intrusion attempts, and fraud.

With more and more high-profile cyber security incidents being made public, awareness of the importance of cyber security continues to steadily increase. However, while an on-going dialogue is good for Bangladesh, the level of public discussion and understanding would benefit from more informed and considered perspectives.

In order to have a mature discussion in 2019, it is particularly important that we get the language right - calling every incident a ‘hack’ or ‘attack’ is not helpful for a proportion ate understanding of the range of threats and only promotes sensationalism. And treating every adversary as though they are all equally sophisticated and motivated detracts from a balanced perspective of risk and vulnerability.

BGD e-GOV CIRT goals for 2019 include improving and expanding communication as well as incident response capacity of its technical team and associated new tools, which will provide greater value during incident response and assessment activities. The team will continue to refine and update its training offerings that will allow government organizations to better meet the demands of challenging and evolving technical issues in cyber security.