# BtCIRT Annual Report
# (2016)

# 1. EXECUTIVE SUMMARY

# 2. About BtCIRT

## 2.1. Introduction

Bhutan started its journey into the cyberspace

Bhutan Computer Incident Response Team (BtCIRT) is a part of Department of Information Technology and Telecom, Ministry of Information and Communications. BtCIRT's mission is to enhance cyber security in Bhutan by enabling cybersecurity information coordination and by establishing computer security incident handling capabilities within the country. The BtCIRT's mandate has been approved by the Lhengye Zhungtshog/Cabinet vide Government order number C-2/104/310 dated 20th May 2016.The team has commenced its operation from April 2016.

## 2.2. Services

### 2.2.1. Reactive services

2.2.1.1. Alerts and warnings

2.2.1.2. Security Incident Handling

2.2.1.3. Incident Analysis

BtCIRT receives information regarding incidents, triage incidents and coordinate response. Activities related to incident handling and analysis include:

2.2.1.4. Evidence Collection

2.2.1.5. Tracing suspicious and malicious activities;

2.2.1.6. Providing mitigation solutions for indicated incidents;

2.2.1.7. Coordinating response activities among related parties;

2.2.1.8. Providing assistance to the affected constituents

### 2.2.2. Proactive services

2.2.2.1. Security event monitoring and security incident detection: BtCIRT proactively monitors security events on the network and uses the collected information to detect malicious activities within governmental network infrastructure.

2.2.2.2. Security vulnerability warnings: BtCIRT collects information regarding security vulnerabilities and communicates with constituents in order to distribute appropriate vulnerability information.

2.2.2.3. Security assessments: BtCIRT uses vulnerability scanners to identify potential threats to the government information and corresponding infrastructure and coordinates appropriate remediation actions in order to minimize or eliminate corresponding security risks.

### 2.2.3. Awareness raising

BtCIRT makes effort in identify gaps in the competence of constituents in order to ensure better understanding and compliance with security best practices, standards and corresponding policies. BtCIRT takes necessary measures to eliminate these gaps and to raise general preparedness for security threats by using different instruments such as meetings, seminars, articles, media and similar methods.

## 2.3. Constituency

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. BtCIRT's extent of responsibilities will constitute organizations using the following IP address space and domain names presently:

- 202.144.144.0/25
- *.bt
- National Critical Infrastructures

# 3. Activities and operations

## 3.1. Security Advisory and Alerts

BtCIRT sends security updates and advisories to its constituents when any vulnerabilities, threads are known or if they are found to be compromised. Email or system (authenticated and authorized) feeds are used to disseminate confidential and internal information (dedicated advisories, alerts, and threat information), while BtCIRT website is used to disseminate public information (advisories, best practices and alerts).

Users can also subscribe to BtCIRT email for any updates directly to their inbox.

To reach maximum users, BtCIRT also updates its facebook page with security news from across the globe, vulnerability update and advisories on how to stay protected.

## 3.2. Incident Response

BtCIRT coordinates computer Incidence response on behalf of the nation.
BtCIRT actively monitors government network for vulnerabilities and malware infections and Constituents are informed via email, calls or live chats of vulnerabilities (such as open ports, misconfigured service and POODLE,) and incidents (such as malware infection, blacklisted ips and compromised web sites) compiled using various online tools and from security feed providers.

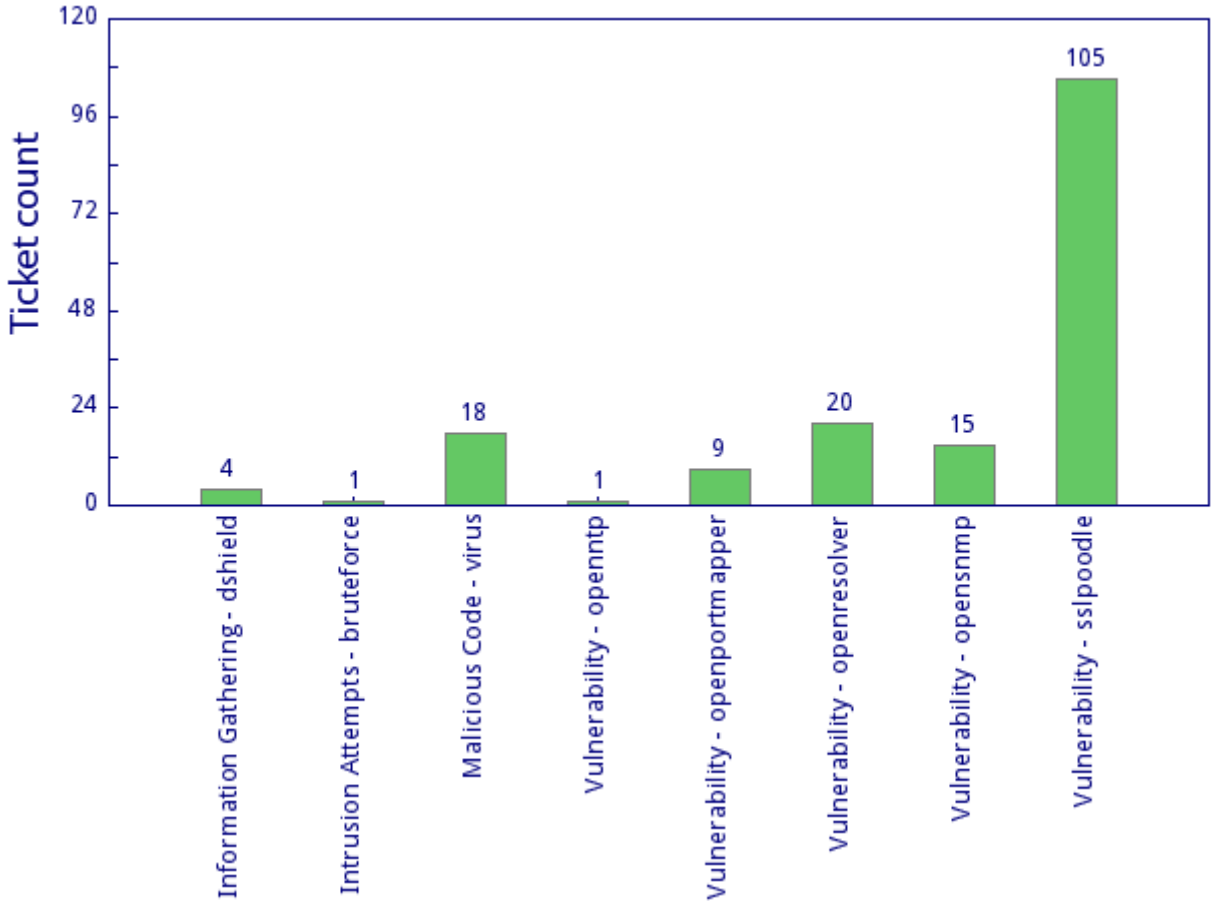
Following chart shows the type and list of incidence initiated by BtCIRT in the last 12 months, with POODLE being the most prevalent vulnerability in government systems. Dorkbot, Conficker, ghost-push and ZeroAccess were some of the common malware infecting the systems.

BtCIRT also monitors for defaced/hacked websites. 51 .bt domains(websites) have been defaced/hacked since January 2016 to January 2017, BtCIRT informed web admins and requested to do the needful with technical support if they requested.

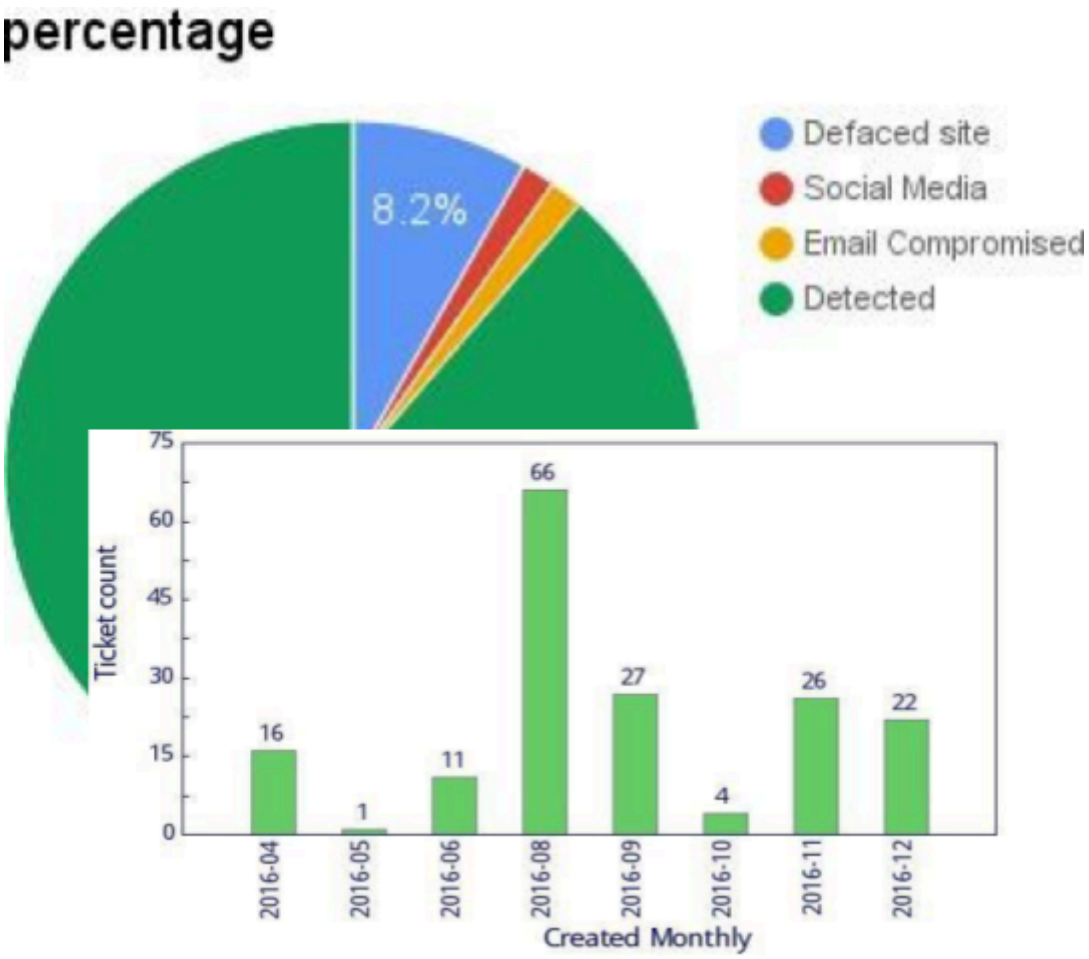
BtCIRT has sent security advisories on how to resolve issues specific to systems, via email to ICT personnel owning the service and also publish general advisories on the BtCIRT website.

A total of 195 incidences were handled of which only 22 case were reported from constituents others were all detected by proactive monitoring

**Incident Tickets Initiated by BtCIRT last 12 months**



BtCIRT also receives incidents from its constituencies via email or call but it counts to only 11.3% of total incident handled of which 8.2% is facebook defacement . Vulnerability assessment was carried out for all the defaced sites and the report with advisory on how to clean was sent.




## 3.3. Vulnerability Report for early warning

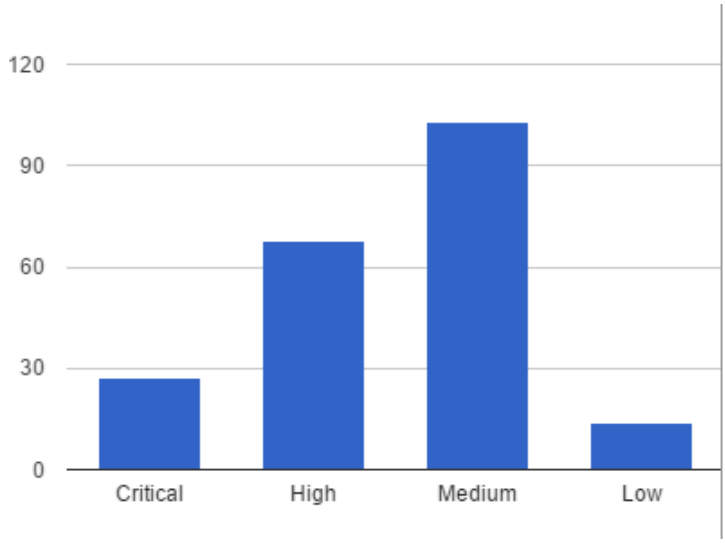
3.3.1. BtCIRT Accesses global IP addresses and blocks assigned to government entities and sends the vulnerability assessment report to its constituencies to enable them to block the back doors if any before the system is compromised.

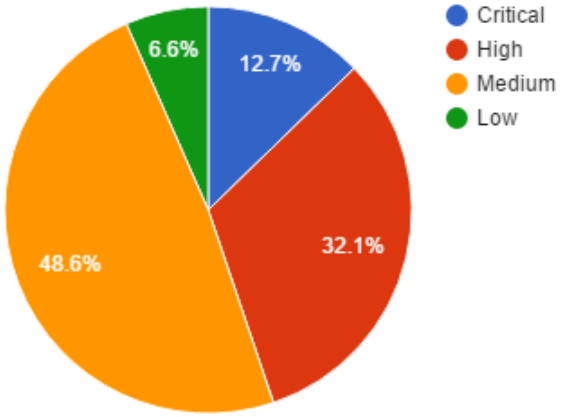
3.3.2. 92 systems/services were assessed for vulnerability since April 2016. From the assessment it was found that most of services are installed once and never updated for instance SSL certificate installed once but never

renewed or the ssl version never updated or for that matter most of the sites are using obsolete PHP version. which does not receive any vendor protection. Another big issue is with insecure coding and configuration.

3.3.3. Following graph shows the types of vulnerabilities and misconfigurations found across various scanned services/systems.

3.3.4. Vulnerabilities are categorized into “Critical”, “Medium”, “High” and “Low” based on how adverse the impact would be if the vulnerability is exploited.




# 4. Events Organised

## 4.1. Workshops:

4.1.1. Digital forensic Training: conducted with a resource person from FIRST more than 15 ICTOs from the government, focal person from RBP, ACC, Technical lecturers from RUB along with BtCIRT members were trained from 26th- 30th March, 2016.

4.1.2. CIRT Operations and Computer Incident Handling: By APNIC member 30+ ICT officials from government, ACC, Banks and CIRT members trained from 19th – 21st April 2016.

4.1.3. Cyber Security Workshop: 31 government officials attended from 15 to 16 September, with resource person from APNIC.

4.1.4. BtCIRT has also conducted meeting with ISPs and Royal Monetary Authority discussing areas of collaboration.

4.1.5. BtCIRT met with officials from OAG, RAA, staff from Application Division on revisiting the IMSP(Information Management Security Policy) and reinforcing the policy document in the government.

## 4.2. Awareness Program:

4.2.1. The team has conducted awareness program for government officials in 7 dzongkhags covering basics security issues like password, email,social media, browsing and handling usb.

4.2.2. As a part of general awareness BtCIRT shares and writes simple and short security tips on its facebook page along with vulnerability update and global cyber news that relates to Bhutan.

4.2.3. Nine advisories have been published on BtCIRT public website since April 2016.

## 4.3. Events attended:

4.3.1. International Conference on Cyberlaw & Cybercrime: attended by one of the RAA employee

4.3.2. APCERT Annual Conference

4.3.3. 6th Cyber Security Forum;

4.3.4. 7th Cyber Security Forum

# 5. International Collaboration

5.1. Processing for APCERT and FIRST membership

# 6. Future Plans:

6.1. Establish Staging room/Lab

6.2. Develop SoPs

6.3. Conduct Awareness program in Schools/Ministries/Agencies/Remaining Dzongkhags

6.4. Nation wide awareness program

6.5. Install tapping device in GDC for incidence monitoring

# 7. Contact:

Address:

Bhutan Computer Incidence Response Team(BtCIRT)
Infrastructure Division
Department of Information Technology and Telecom (DITT)
Ministry of Information and Communications
Thori Lam, Chubachu, Thimphu
Bhutan, Post Box: 482

Phone: +975-02-338606
Email: info@btcirt.bt (for general questions)
Email: cirt@btcirt.bt (for reporting an incident)
In case of sensitive information please use BtCIRT PGP key to encrypt your content.

Working hours: 9:00-17:00, Monday to Friday (BTT/Bhutan Time, UTC+6, no DST)