BtCIRT Annual Report
(2017)

Table of Content

1. Highlights of 2017

1.1 Summary of major activities

In 2017 BtCIRT has conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted security awareness program targeting end users , developed security baseline and conducted organisational security assessment of some of the organisations.

1.2 Achievements & milestones:

- BtCIRT has conducted end user cyber security awareness covering all 20 district government offices.
- BtCIRT has conducted Security Assessment for Government Data Centre(GDC) and some other critical infrastructures.
- Developed Security Baseline and conducted Information and Network security workshops involving system owners from various critical organisations.
- BtCIRT has placed sensors at GDC to monitor for threats and vulnerabilities since most of the critical system are hosted there.

2. About BtCIRT

2.1 Introduction

Bhutan Computer Incident Response Team (BtCIRT) is a part of Department of Information Technology and Telecom, Ministry of Information and Communication. BtCIRT's mission is to enhance cyber security in Bhutan by enabling cyber security information coordination and by establishing computer security incident handling capabilities within the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

2.2 Establishment

The BtCIRT's mandate has been approved by the Lhengye Zhungtshog/Cabinet vide Government order number C-2/104/310 dated 20th May 2016. However, the team has commenced its operation a month before i.e April 2016.

2.3 Resources

Currently BtCIRT consist of 5 working team members.

2.4 Constituency

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. While BtCIRT services like awareness and reactive services is extended to national level.

3. Activities & Operations

3.1 Scope and definitions:

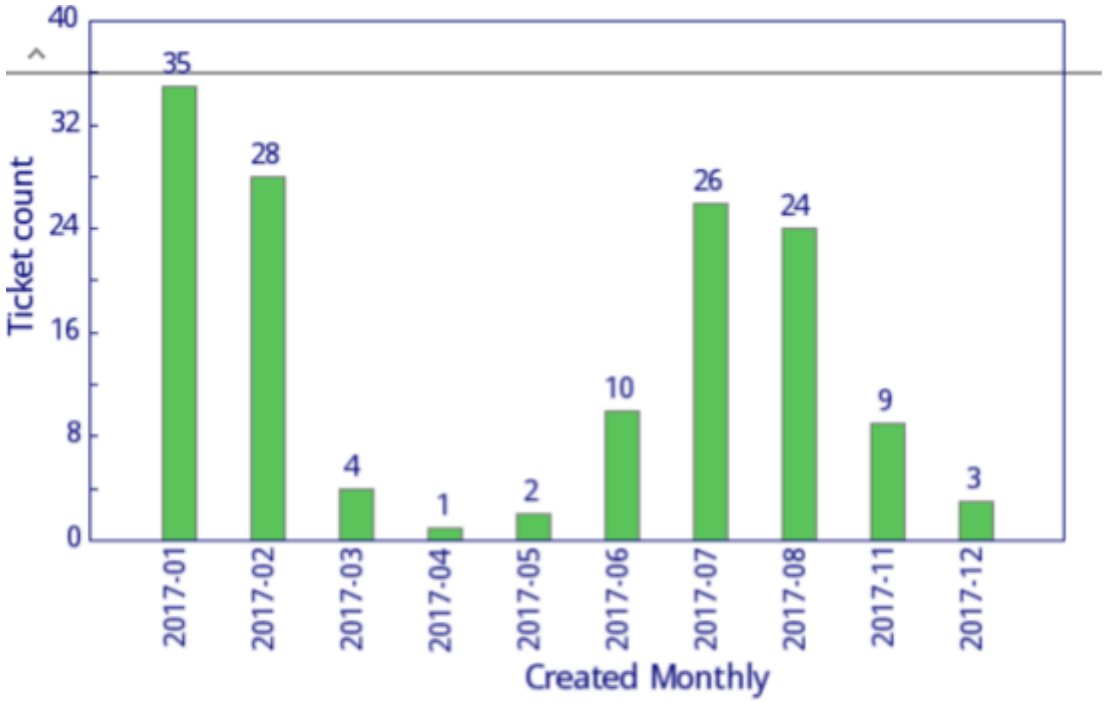
- BtCIRT is mandated to act as central trusted point of national contact in relation to cyber security issues.
- BtCIRT conducts end user awareness at national level and disseminates information on latest threats and vulnerabilities and conducts security workshops related to various cyber security domains .
- BtCIRT actively monitors system hosted in Government Data Centre(GDC) for attacks and vulnerabilities and provides timely report to GDC operating team along with system administrators.
- BtCIRT also conducts periodic security assessment of government systems, while for non-government organisations it provides services on request basis.
- It represents the country in international organisations and forums.

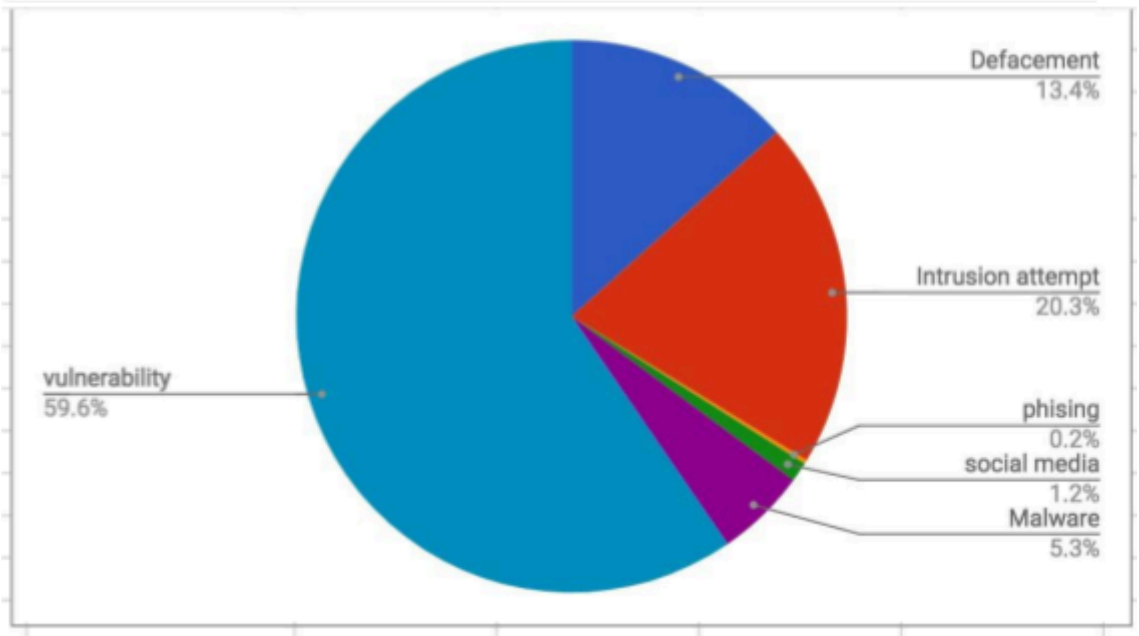
3.2 Incident handling reports:

In 2017 BtCIRT handled 139 incidents of which only 10% was reported by constituents.

3.2.1 General Incident handling statistics:

Following statistics includes Incidents handled monthly and the pie chart represents types of incident handled.

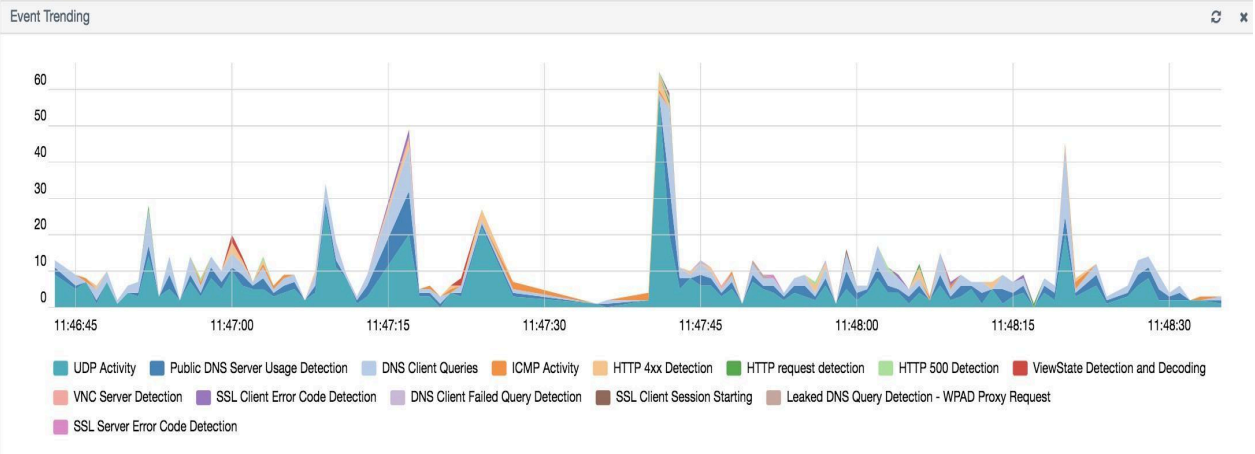




3.2.2 Services to GDC (Government Data Centre)

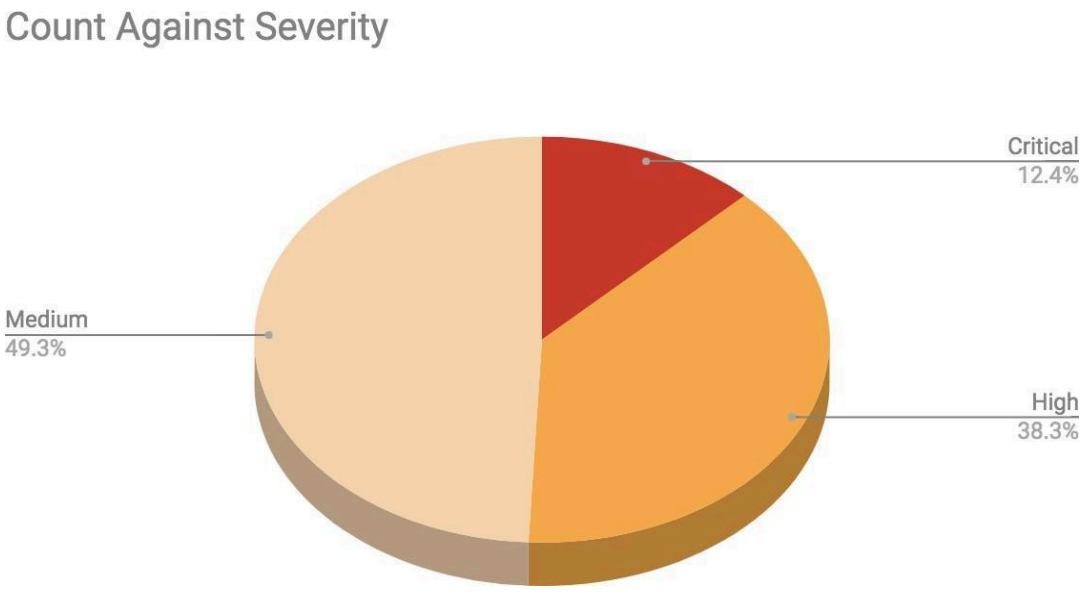
BtCIRT actively monitors Government Data Centre for threats and vulnerabilities in both systems and network and informs GDC team if any issues detected.

3.2.2.1 Monitor system activity for unusual pattern



3.2.2.2 Monitor for Vulnerability and attack pattern:

Vulnerabilities are categorized into “Critical”, “Medium”, “High” and “Low” based on how adverse the impact would be if the vulnerability is exploited. Vulnerability of either Critical, high or medium severity were detected in 42 vulnerable systems.

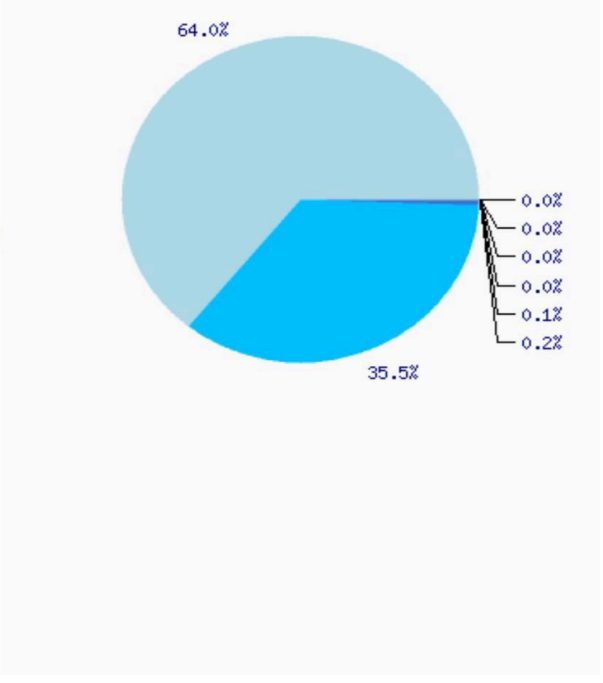


3.2.2.2.1 Top Ten critical Vulnerabilities

☐	CRITICAL	PHP < 7.1.0 Multiple Vulnerabilities	Web Servers	13
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1o / 1.0.2 < 1.0.2c ASN.1 Encoder Negative Zero Value Handling RCE	Web Servers	6
☐	CRITICAL	OpenSSL 1.0.1 < 1.0.1s / 1.0.2 < 1.0.2g RCE	Web Servers	6
☐	CRITICAL	PHP 5.4.x < 5.4.30 / 5.5.x < 5.5.14 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.38 / 5.5.x < 5.5.22 / 5.6.x < 5.6.6 Multiple Vulnerabilities (GHOST)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.43 / 5.5.x < 5.5.27 / 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)	Web Servers	5
☐	CRITICAL	PHP 5.4.x < 5.4.45 / 5.5.x < 5.5.29 / 5.6.x < 5.6.13 Multiple Vulnerabilities	Web Servers	5
☐	CRITICAL	Apache Tomcat 6.0.x < 6.0.45 / 7.0.x < 7.0.68 / 8.0.x < 8.0.32 Multiple Vulnerabilities	Web Servers	3
☐	CRITICAL	Oracle Java SE 6 < Update 115 / 7 < Update 101 / 8 < Update 92 Multiple Vulnerabilities	Web Clients	3
☐	CRITICAL	Oracle Java SE 6 < Update 141 / 7 < Update 131 / 8 < Update 121 Multiple Vulnerabilities	Web Clients	3

3.2.2.2.2 Top attacks types

Alarm	Occurrences
Delivery & Attack — Bruteforce Authentication — SSH	4.103
Delivery & Attack — Bruteforce Authentication — Linux/Unix	2.278
Reconnaissance & Probing — Service discovery — Microsoft Remote Desktop	16
Delivery & Attack — Bruteforce Authentication — Microsoft Remote Desktop	6
Reconnaissance & Probing — Service discovery — VNC	2
Reconnaissance & Probing — Service discovery — SSH	1
Delivery & Attack — WebServer Attack - SQL Injection — Attack Pattern Detection	1
Exploitation & Installation — WebServer Attack — XSS	1



3.3 Publications

3.3.1 Security Advisory and Alerts

BtCIRT provides updates on latest threats and vulnerabilities and provides advisories on known threats and best practices via its website, facebook page and email to government system administrations. Users can also subscribe to receive any Alerts or Articles on to their inbox.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

- BtCIRT has conducted 2 Security Workshops in Information and Security related domain with support from Sri Lanka CERT|CC, APNIC and Asi@Connect.
- BtCIRT has also conducted Security Mock drill involving system owners and critical infrastructure operators.
- BtCIRT has also carried out end user security awareness program covering all 20 district government offices.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT is a member of only two international organisations, Asia Pacific Computer Emergency Response Team(**APCERT**) and Forum of Incident Response and Security Teams(**FIRST**) as of now.

5.2 Capacity building

5.2.1 Seminars & presentations

BtCIRT has attended following conference/Seminars/workshops:

5.2.1.1 AusCERT Annual Conference, 23rd- 26th May, 2017 , Gold Coast, Australia

5.2.1.2 8th APT Cybersecurity Forum (CSF-8), 24-26 October 2017, Dhaka, Bangladesh

6. Future Plans

6.1 BtCIRT is planning to strengthen its vulnerability and threat monitoring system and to conduct awareness programs at schools and colleges.

6.2 We are also looking at enforcing international benchmark like CIS as minimal security requirement for all government systems.

6.3 BtCIRT also looks forward to collaborate with more organisations internally and internationally to strengthen its cooperation.

7. Conclusion:

Year 2017 has been challenging and a learning experience for BtCIRT being the second year of its operation. We look forward to take away mistakes made and improve the services we offer in the year 2018 and strengthen national and international collaboration and cooperation.