Bhutan Computer Incident Response Team

Annual Report

2018

Phone: +975-02-338606
Email: info@btcirt.bt or cirt@btcirt.bt

Phone: +975-02-338606
Email: info@btcirt.bt or cirt@btcirt.bt

1. EXECUTIVE SUMMARY

The report captures all essential activities undertaken by BtCIRT in the year 2018. The overall mission of BtCIRT is to enhance cyber security in Bhutan by enabling cybersecurity information coordination and establishing computer security incident handling capabilities within the country. In accord to its mission, BtCIRT has put efforts to fulfill the roles and responsibilities as mandated and entrusted by the Royal Government of Bhutan. The report conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted vulnerability assessment,post incident analysis, workshops, awareness program targeting end users and drafted national cyber security strategy.

2. Activities and Operations

2.1. Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website (www.btcirt.gov.bt) and facebook page (BtCIRT). Last year, BtCIRT published 122 security alerts to disseminate information about the latest threats and vulnerabilities on these platforms.

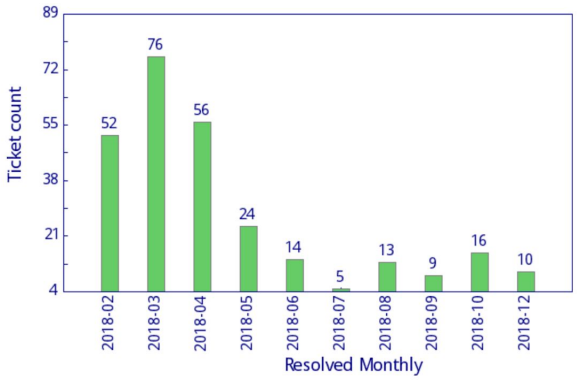
In addition, the team also publishes advisories to assist constituents in resolving the most common threats and vulnerabilities observed in the country derived from regular monitoring of services. 6 security advisories ranging from topic such as ***Meltdown and Spectre*** vulnerability to the ***memcached Reflection/Amplification DDOS*** attack were published during the year. Besides, advisory emails are also sent out to government and critical sector ICT official to notify possible attacks as and when it is detected.

2.2. Incident Management and Response

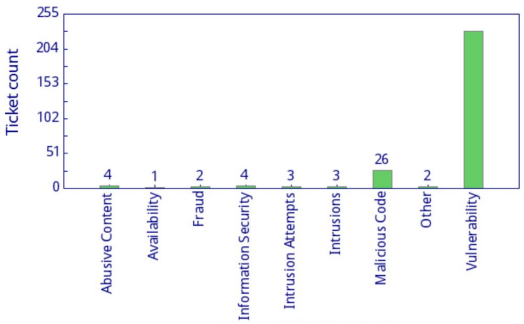
The year saw 8% increase in the incidents reported to BtCIRT as compared to 2017 taking the total of resolved incidents to 275. Possibly, the awareness programs conducted in the dzongkhags at the beginning of the year could have encouraged constituents to report incidents. 50 incidents were reported by constituents.

Even the number of government websites attacks reduced substantially to 5 from 21 in 2017. The migration of government websites to Government Data Center (GDC) could have contributed in the reduction. Unlike other hosting service providers, GDC offers focused security approach to allow more controls of the systems hosted. Close collaboration between GDC and BtCIRT to operate SOC (Security Operation Center) also helps to manage and monitor these websites on daily basis.

The following diagrams provide number of incidents handled on a monthly basis. It also depicts the types of incidents resolved by the team during the year. March was the busiest month for the team with 76 incidents highest recorded in the year. The maximum efforts of the team was spent on vulnerabilities detection and patch followed by removal of malicious codes.



Resolved Monthly	Ticket count
2018-02	52
2018-03	76
2018-04	56
2018-05	24
2018-06	14
2018-07	5
2018-08	13
2018-09	9
2018-10	16
2018-12	10
Total	275

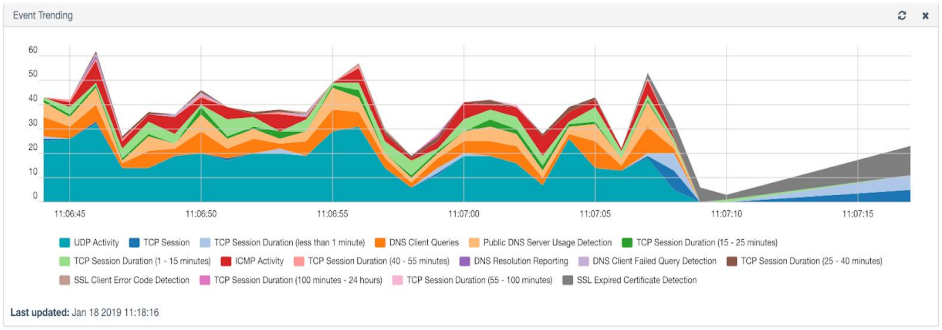


Custom field Classification	Ticket count
Abusive Content	4
Availability	1
Fraud	2
Information Security	4
Intrusion Attempts	3
Intrusions	3
Malicious Code	26
Other	2
Vulnerability	230
Total	275

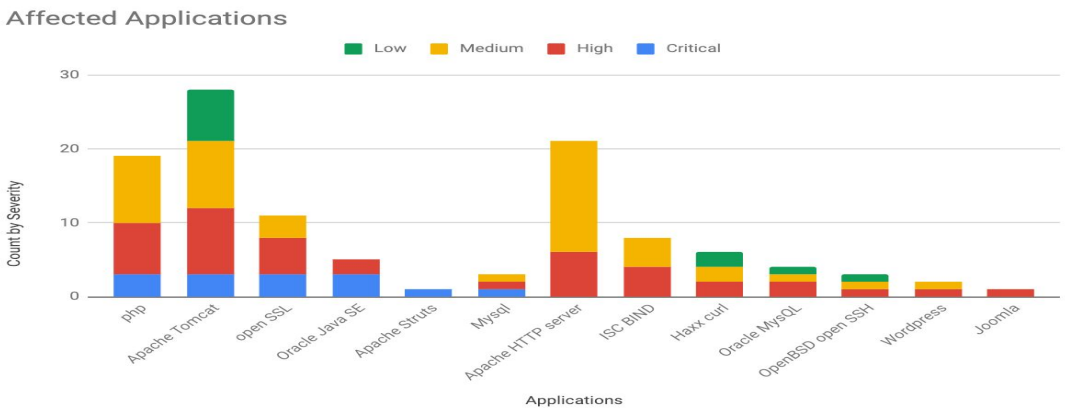
2.3. Collaboration with GDC (Government Data Center)

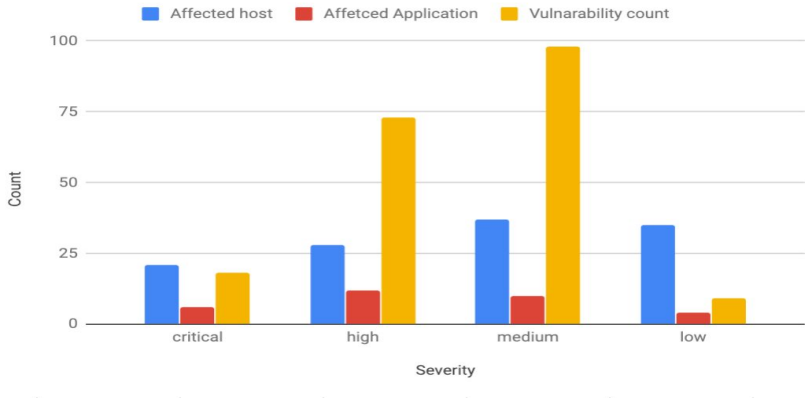
Ever since the establishment of BtCIRT, the team was also identified to function as part of security operation center (SOC) of GDC. The two teams has been working closely on strengthening the security of the data center. It has become ever more critical to safeguard the center with increasing number of government online services migrated to the data center. Today, GDC hosts more than 80 services. These services are the most availed services requiring highest possible uptime with minimal tolerance for disruption.

Last year, BtCIRT installed two screens to proactively monitor Government Data centre for threats and vulnerabilities. The GDC team is notified in the event of any anomalies detected in systems or network. Following diagram is a snapshot of live system taken to demonstrate activities monitored for suspicious patterns, events and trends.



The team also monitors for vulnerabilities detected at the GDC. Vulnerabilities are categorized into "***Critical***", "***High***", "***Medium***" and "***Low***" based on the severity of impact it poses to the service should the vulnerability be exploited. In 2018, 42 systems out of 774 listed servers detected with vulnerabilities of all levels were reported to the GDC team for rectification.





In course of operating SOC, BtCIRT also observed intensive resource usage that caught attention of the SOC team. On further investigation, it was learned that some of the systems were participating in crypto-mining and TOR (The Onion Router) relay. The case was reported to GDC team for rectification and resolutions.

3. Events Organised

3.1. Awareness Program

The BtCIRT successfully conducted cyber security advocacy programs in 12 dzongkhags namely, Samdrup Jongkhar, Pemagatshel, Trashiyangtse, Trashigang, Mongar, Lhuentse, Trongsa, Gasa, Samtse, Haa, Paro and Thimphu. The program was delivered in a mix-mode engaging the participants with live demonstrations and brief presentations on the importance of cyber security.

The program was tailored to meet the cyber security needs of general end users that arise out of their daily occupational and personal engagements. The program covered a wide range of topics such as secure communication using emails and social media services, protection of personal information to avoid social engineering attacks, recognising and identifying phishing emails, and the good habits to become safer Internet users.
The program concluded in January 2018 after deployment of two teams and over two weeks of travels. The program was attended by more than 20 government employees.

3.2. FINCIRT consultative meeting

The alarming rate of scams and attacks targeting financial institutes, service providers and consumers alike has become a serious concern, and also realised the need to institute a specialised cyber security team for the financial sector to protect banking ICT assets from cyber attacks. In recognition of such need, a consultative meeting was convened between the banking institutes and the BtCIRT to identify the areas of collaborations to strengthen the security of banking institutes. The meeting was attended by 10 ICT officials of 6 financial institutes located in Thimphu on April 17, 2018.

The meeting discussed on the level of security measures implemented in each institute. It was learned that most of the institutes has implemented the basic cyber security requirements. Furthermore, the meeting also saw a promising and viable solution to institute a single entity called "FIN-CIRT" (Financial Computer Incident Response Team) that will be solely focused to provide security services to the banking institutes.

3.3. Workshop on Incident Resolution

A workshop was conducted on May 2018 to educate the system owners on the latest vulnerabilities existing in the systems. The workshop was organised to address the capacity gaps faced by the system owners in resolving and patching the detected vulnerabilities. The participants were demonstrated on how vulnerabilities and other issues could be patched and systems secured.

3.4. Workshop on Information and Network Security

A workshop on Information and Network Security was conducted from 12th to 16th November, 2018 with financial and technical support from APT(Asia Pacific Telecommunity) and APNIC (the Asia-Pacific Network Information Centre). The weeklong program was aimed to train system administrators in securing their information systems and network infrastructure and, responding to potential threats and attacks with practical sessions on identifying and defending threats and vulnerabilities. Participants from government agencies, corporations, financial institutions, telecom service providers and other relevant private sector organisations participated.

3.5. Security Incident Mock Drill

As par workshop on information and network security, a day long security mock drill was also conducted to assess the readiness of response capabilities of system and network administrators. The drill was based on plausible cyber security cases and commonly occurred incidents. It also gave stakeholders an opportunity to learn how effective their organisational measure are for testing security vulnerabilities and responding to cyber incidents. While for those who didn't have any measures in place it was an eye opener to go back and start developing ones.

3.6. Drafted Cyber Security Strategy:

Technical assistance was sought from ITU for drafting the National Cybersecurity Strategy in an effort to improve cyber security. Various activities were conducted including consultation and workshops with stakeholder with an aim of developing holistic approach in laying out long-term objectives and a roadmap to achieve identified milestones. It was also aimed at addressing concerns and expectations of stakeholders surrounding cyber security. Along with it, close consultation was done with relevant stakeholder for formulating Online Child Protection programs. A Child Online Protection Survey was also carried out which revealed that students wish for more Cyber Security training programs at school.

3.7. Cyber Security Simulation

On November 27, 2018 Cyber Incident Simulation was conducted with support from the International Telecommunication Union (ITU). The exercise was designed exclusively for heads of government, policy makers and other high ranking figures to increase awareness on cyber security and preparedness to make critical decisions in response to cyber attacks. It was attended by honorable cabinet ministers, secretaries, executive government officials, law enforcement representatives and heads of corporations, private sector organisations and other institutions with critical information infrastructure. The program was moderated by Prof. Marco Gercke from Cybercrime Research Institute, who is also a consultant to ITU.

4. Events attended:

4.1.1. 30th Annual Conference on Computer Security organised by FIRST (Forum of Incident Response and Security Teams).

4.1.2. APT Training Course on Policy on Cyber Security for Safeguarding Public Safety

5. Future Plans:

The following activities is strictly on the agreed plan stipulated for the next six months.

5.1. Considering the importance of secured websites, the team in collaboration with GDC plans to implement SSL certificates in 10 websites and develop a ***how-to*** manual to guide the other system owners to implement similar setup in their websites. So far, most of the agencies have deployed commercial certificates, the two has agreed to implement open source based solution.
5.2. Enhance Honeypot to gather information on attack pattern.
5.3. Conduct workshop on Secure coding

6. Contact:

Address:

Bhutan Computer Incident 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)
You will receive email notifications for any new articles we post if you subscribe through our website.
Get notified as you socialize on facebook by following our page “Bhutan Computer Incident Response Team”