BtCIRT 2025: Operational Highlights and the Road Ahead

Prepared by BtCIRT
for
BTNOG 12/SANOG 43

GovTech
Bhutan

BtCIRT
Bhutan Computer Incident Response Team

Bhutan Computer Incident Response Team

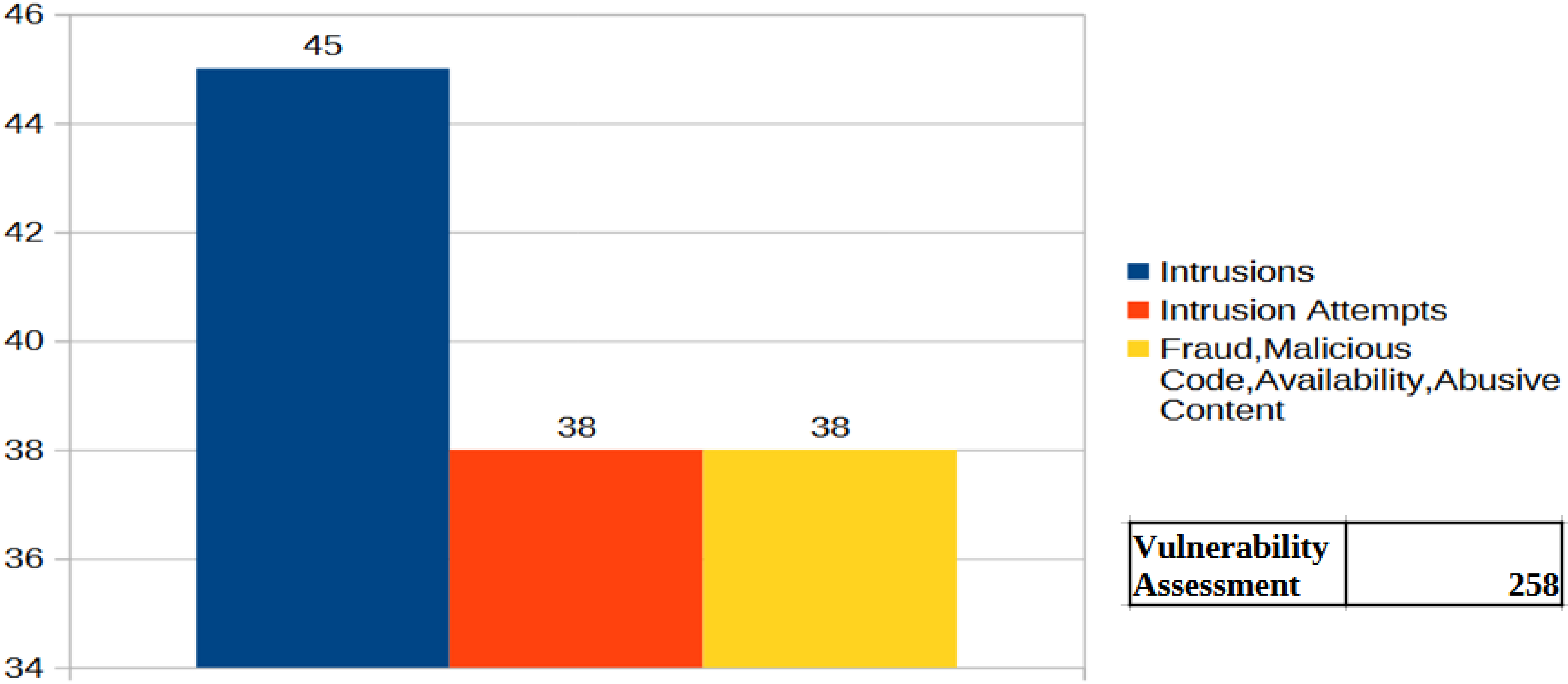
Get to Know Us

- Operationalized since 22nd April 2016
- Visit our Site: **https://www.btcirt.bt/**
- Contact us @ +975-02-338606
- Email for general inquiries here: **info@btcirt.bt**
- Report security incidents here: **cirt@btcirt.bt**
- Visit our Facebook Page: **Bhutan CIRT**

What We Do

- Incident Handling and Analysis
- Cybersecurity Awareness
- Security Assessment and Monitoring
- Cybersecurity Policy and Strategy
- International Cooperation

Incident Records(July 2024-June 2025)



Vulnerability Assessment	**258**

1. Abuse Content

- **Incident**-Request for assistance in removing inappropriate content from social media platforms
- **Solution**:
  - **TikTok:** Clients are advised to report the content directly using TikTok's official in-app reporting system.
  - **Facebook:** In cases involving Facebook, our team engages directly with the platform's support team to facilitate the takedown process.
  - For the individual content takedown we guide the clients how to report by themself to the meta.
- **Challenges:**
  - Social media platforms are based outside our jurisdiction, and response times are often slow.
  - Some platforms do not respond at all, making it difficult to escalate or resolve the issue promptly.
  - Unless the content clearly violates community guidelines, takedown requests are not accepted, regardless of local impact or context.

2. Fraud

- **Incident**: Phishing
- **Solution:**
  - Forced password reset for potentially affected users.
  - Block the phishing domain and URL at the firewall.
  - Request to enable Multi-Factor Authentication (MFA) for all users.
  - Report to domain owner/hosting provider, RIR(Regional Internet Registries)
- **Challenges**: Lack of user awareness, sites mostly hosted outside bhutan.

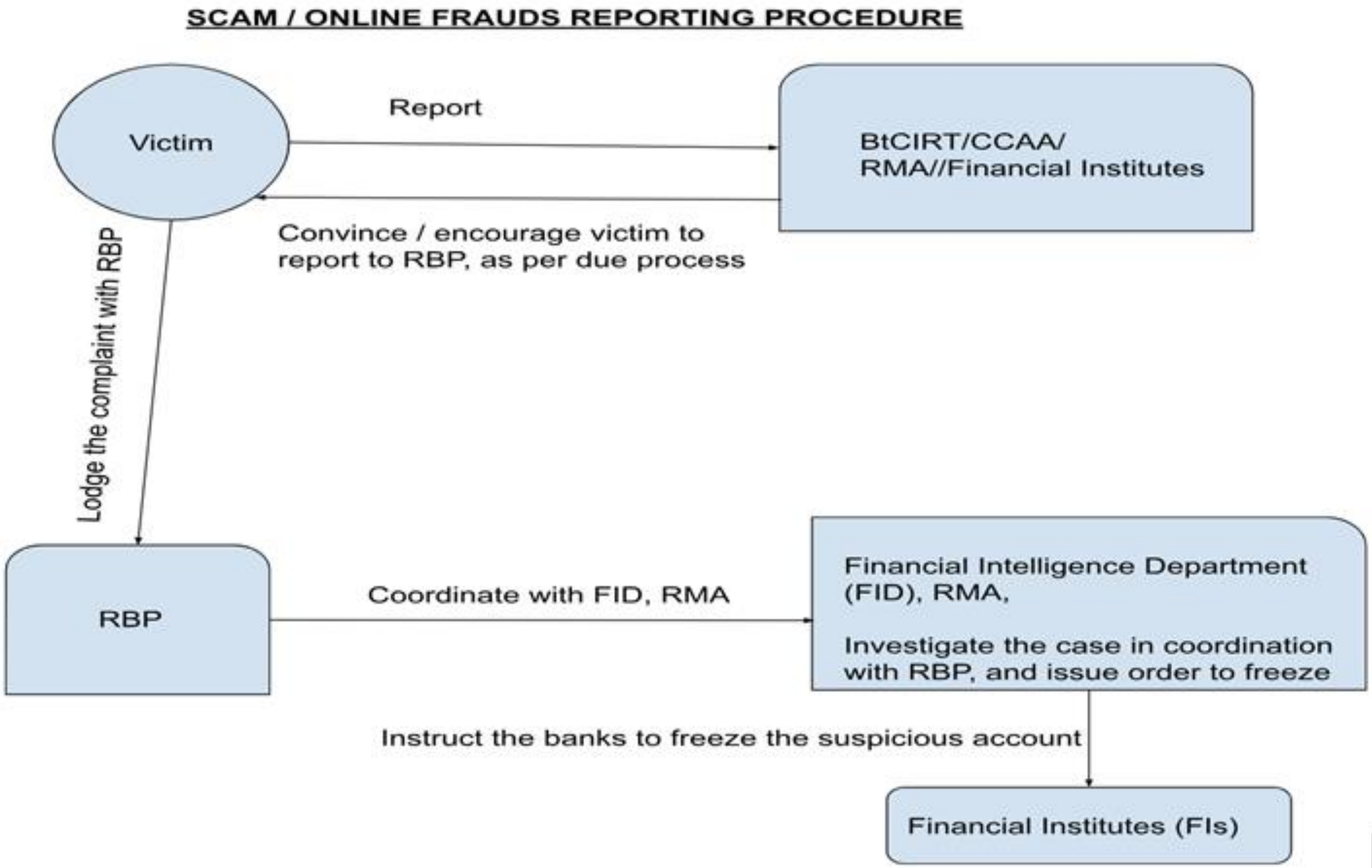
3. Intrusion Attempts:

- **Incident**: SQL Injection
- **Solution**:
  - Input Validation and Sanitization
  - Patch Management
  - Web Application Firewall

4. Intrusion:

- **Incident:** Suspected Compromised IP(exploitation of Cisco IOS XE software)
- **Solution:**
  - Isolate the system from the network to prevent further unauthorized access.
  - Verify whether the device is running Cisco IOS XE software.
  - Conduct a thorough inspection of the device for any suspicious web-based implants or unauthorized modifications.
  - Apply the latest security patches for Cisco IOS XE to mitigate known vulnerabilities.
  - Remove any detected implants or suspicious files and restore the device to a secure configuration.
  - Disable the HTTP server feature on any Internet-facing Cisco IOS XE devices to reduce the risk of web-based exploitation.
  - Review network traffic logs for any unusual activity related to this system.

How BTCIRT helps



SCAM / ONLINE FRAUDS REPORTING PROCEDURE

Victim

Report

BtCIRT/CCAA/
RMA//Financial Institutes

Convince / encourage victim to
report to RBP, as per due process

Lodge the complaint with RBP

RBP

Coordinate with FID, RMA

Financial Intelligence Department
(FID), RMA,

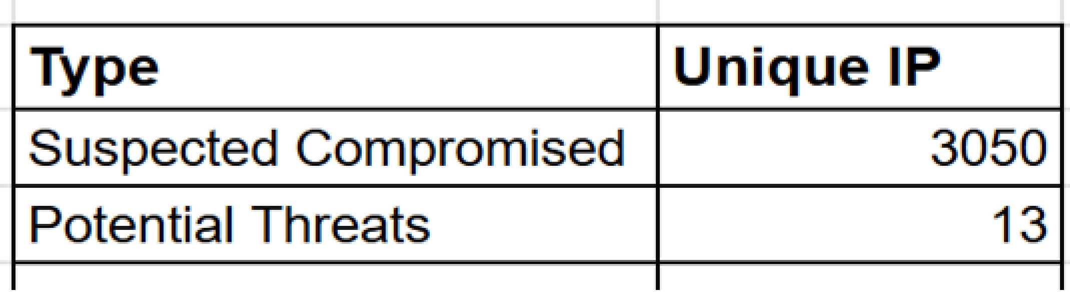
Investigate the case in coordination
with RBP, and issue order to freeze

Instruct the banks to freeze the suspicious account

Financial Institutes (FIs)

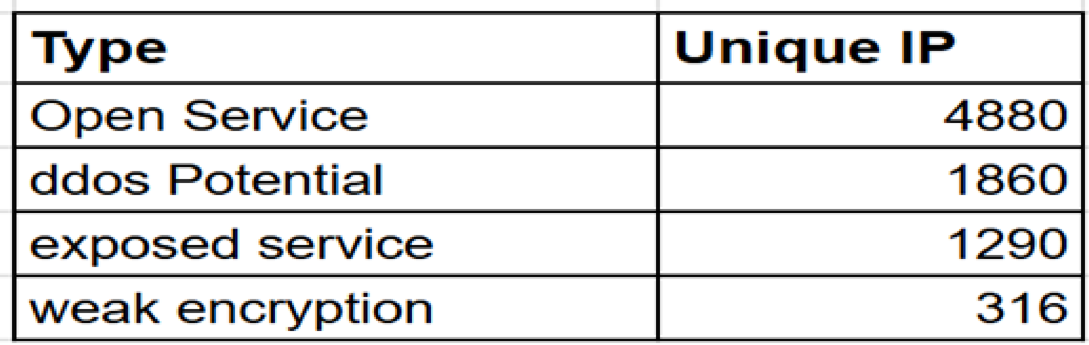
Bhutan Threat Landscape 2025 CyberGreen Statistics, shadowserver

1. Malware



Type	Unique IP
Suspected Compromised	3050
Potential Threats	13

2. Public Exposure



Type	Unique IP
Open Service	4880
ddos Potential	1860
exposed service	1290
weak encryption	316

Recommendation

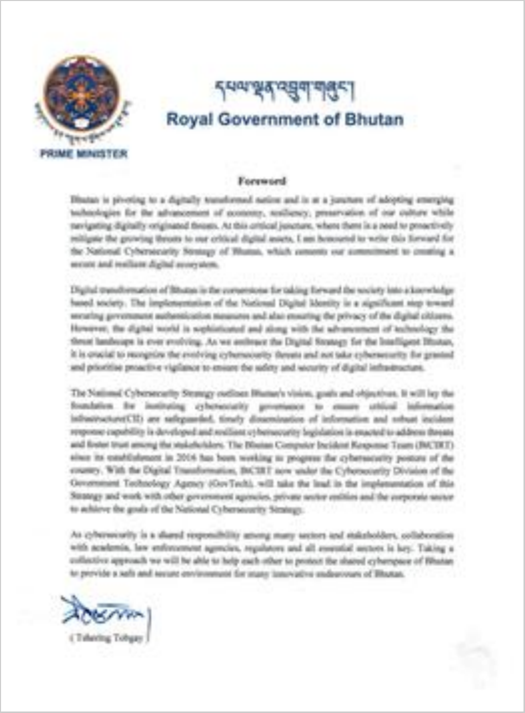
1. Patch HTTP/HTTPS on Cisco IOS XE Devices
2. Disable the Use of Weak Protocols (e.g., Telnet)
3. Avoid exposing SSH services globally to the internet
4. Do Not Keep Service Ports Publicly Accessible (eg., HTTP, HTTPs, SSH, SNMP, VPN)
5. Secure Web Applications
6. Clean and Harden the Network
7. Perform Regular Backups
8. Basically follow Due-diligence

Projects in Progress

National Cybersecurity Strategy - Implementation ([National Cybersecurity strategy](#))

National Cybersecurity Strategy

2024-2029



དཔལ་ལྡན་འབྲུག་གཞུང་།

Royal Government of Bhutan

PRIME MINISTER

Foreword

Bhutan is pivoting to a digitally transformed nation and is at a juncture of adopting emerging technologies for the advancement of economy, resiliency, preservation of our culture while navigating digitally originated threats. At this critical juncture, where there is a need to proactively mitigate the growing threats to our critical digital assets, I am honoured to write this forward for the National Cybersecurity Strategy of Bhutan, which cements our commitment to creating a secure and resilient digital ecosystem.

Digital transformation of Bhutan is the cornerstone for taking forward the society into a knowledge based society. The implementation of the National Digital Identity is a significant step toward securing government authentication measures and also ensuring the privacy of the digital citizens. However, the digital world is sophisticated and along with the advancement of technology the threat landscape is ever evolving. As we embrace the Digital Strategy for the Intelligent Bhutan, it is crucial to recognize the evolving cybersecurity threats and not take cybersecurity for granted and prioritise proactive vigilance to ensure the safety and security of digital infrastructure.

The National Cybersecurity Strategy outlines Bhutan's vision, goals and objectives. It will lay the foundation for instituting cybersecurity governance to ensure critical information infrastructure(CII) are safeguarded, timely dissemination of information and robust incident response capability is developed and resilient cybersecurity legislation is enacted to address threats and foster trust among the stakeholders. The Bhutan Computer Incident Response Team (BtCIRT) since its establishment in 2016 has been working to progress the cybersecurity posture of the country. With the Digital Transformation, BtCIRT now under the Cybersecurity Division of the Government Technology Agency (GovTech), will take the lead in the implementation of this Strategy and work with other government agencies, private sector entities and the corporate sector to achieve the goals of the National Cybersecurity Strategy.

As cybersecurity is a shared responsibility among many sectors and stakeholders, collaboration with academia, law enforcement agencies, regulators and all essential sectors is key. Taking a collective approach we will be able to help each other to protect the shared cyberspace of Bhutan to provide a safe and secure environment for many innovative endeavours of Bhutan.

(Tshering Tobgay)

Projects in Progress

Goal 1: Enhanced cybersecurity Governance

- Institutional Framework Roles and responsibilities of operational level - final draft completed
- National Cybersecurity Risk Assessment - final draft completed.

Goal 2: Cybersecurity legislation framework

- *Information Communication & Media Act 2018* gap analysis with regards to cybersecurity - completed
- Drafted *Critical Information Infrastructure Protection Regulation* of Bhutan

Projects in Progress

Goal 3: Protection of Critical Information Infrastructure

- CII Identification Methodology - endorsed
- List of CIIs-Final draft and in progress for approval

Goal 4: Robust Incident Handling

- Formation of Governmental Security Operations Center (GSOC) - upcoming
- National Cybersecurity Risk Assessment, threat landscape report - upcoming

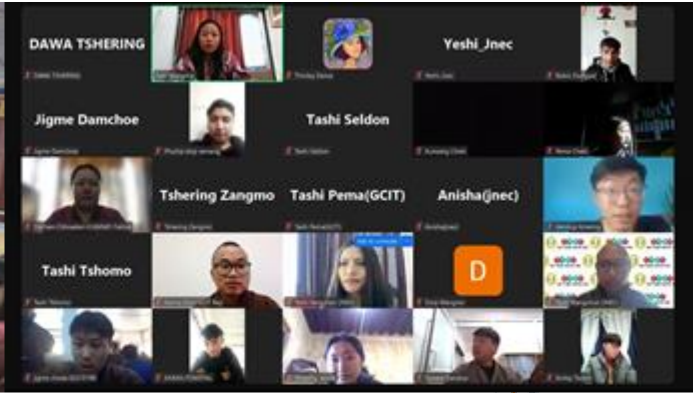
Cybersecurity Events in 2024

Cybersecurity month 2024

Security Workshop

Desups training on pubic cyber awareness

Cyber Hygiene Training



Virtual Capture the flag Challenge in Colleges

GovTech Bhutan

BtCIRT

Thank You