Asia and the Pacific Regional Dialogue:CIRTs and Lessons Learned from COVID -19 Crisis

Radhika Orari
BtCIRT

Outline

- Introduction of National CIRT, mandate, key activities

- Threat Landscape at the time of COVID-19

- Areas of Collaboration & Recommendations

Introduction of National CIRT, Mandate, Key activities

Started Operation in April 2016

- ITU assisted in study to assess formation of national CIRT Assessment for Bhutan.
- Institutionalize BtCIRT with financial support from World Bank

Mandate:

- Serve as a trusted and central coordination point of contact at national level
- More proactive role at the Government level

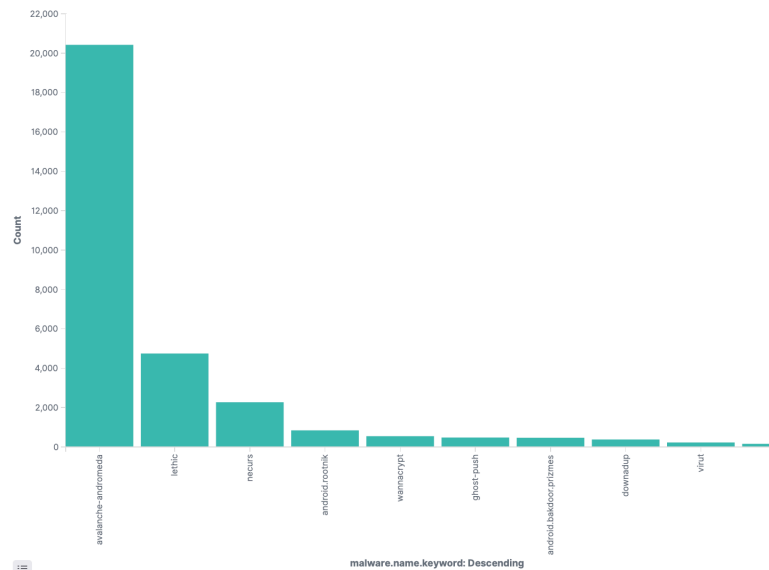## Key Activities:

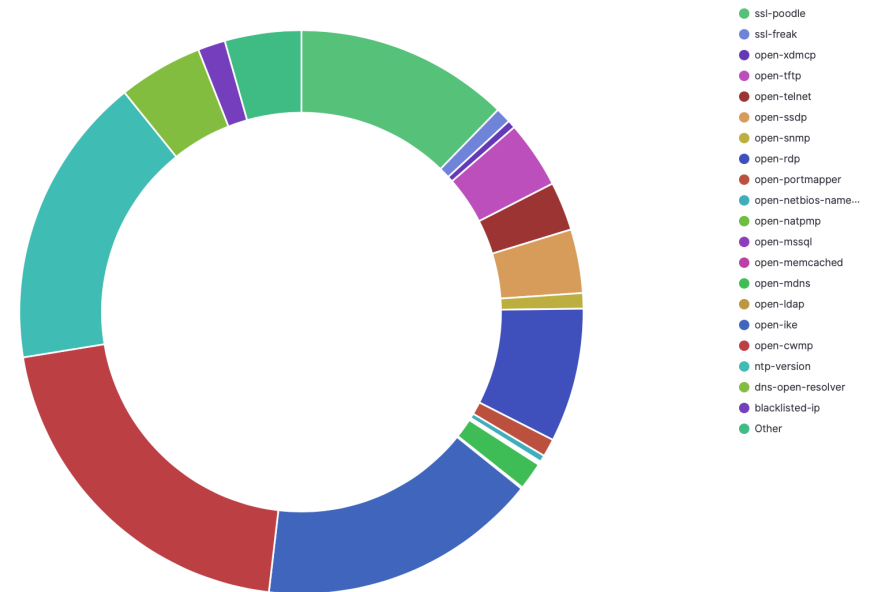**Enhance Cyber security**

Coordinate information

Monitor/Manage cyber threat

BtCIRT
Bhutan Computer Incident Response Team

Proactive Monitoring

Top 10 malware infections

Common vulnerable services

Legend:
- ssl-poodle
- ssl-freak
- open-xdmcp
- open-tftp
- open-telnet
- open-ssdp
- open-snmp
- open-rdp
- open-portmapper
- open-netbios-name...
- open-natpmp
- open-mssql
- open-memcached
- open-mdns
- open-ldap
- open-ike
- open-cwmp
- ntp-version
- dns-open-resolver
- blacklisted-ip
- Other

HoneyNet

URL	Source IP	Count
http://193.228.91.124:80/uih7U8JY7Of7Y8O9d6t68IT67R8y76t7823tg8weuq/pwnNet.x86	193.228.91.124	26
http://134.122.17.29:80/Pandoras_Box/pandora.x86	134.122.17.29	6
http://27.122.56.147:50505/bins/limit.x86	47.251.41.89	1
http://45.80.153.243/GhOul.sh	95.111.254.164	1
		34

loggedin.keyword: Descending – Count
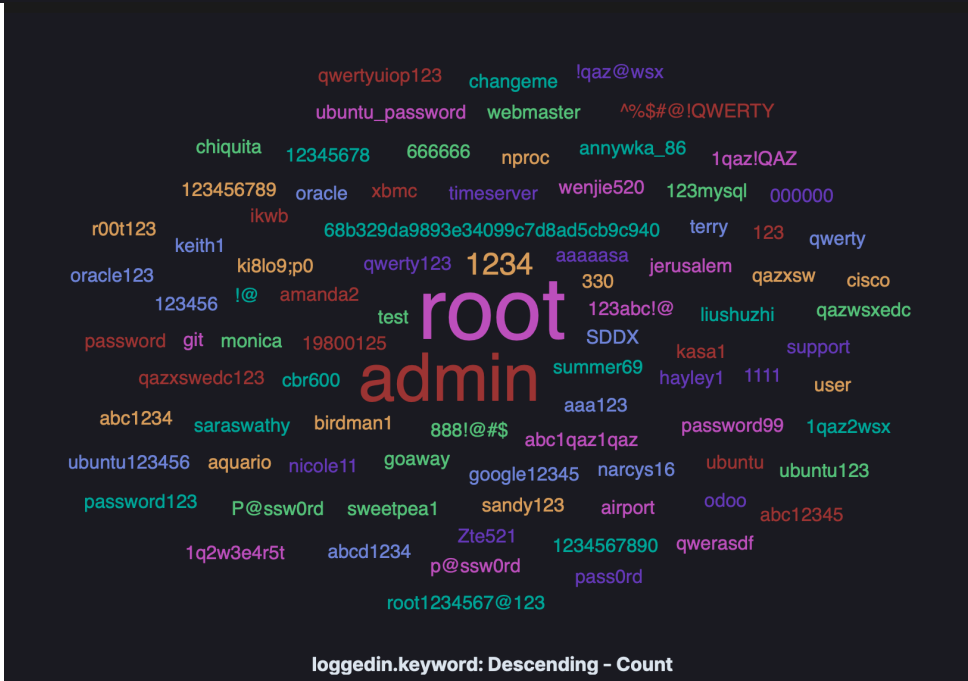
Threat Landscape at the time of COVID-19

Incidents

- Fake news
- Social media account hacks
- Website hacks
- Scam

Risks & Vulnerabilities
- Panic due to fake news
- Vulnerable home networks
- Shift in learning environment
- Rapid deployment of Apps
- Lack of real time monitoring
- Heavy dependence on ICT
- Information sharing vs Privacy

Response

- Awareness through media
- Timely advisories on current threats and best practices
- Developed SOPs for WFH
- Prioritize protection of critical services

Challenges

- Low reporting rate
  - Victims unaware of incident
  - Do not report out of fear
- Taking down false news
- Compromised accounts Recovery
- Lack of artifacts
- Who over how Investigation
- Piracy and related threats to it

Capacity & Capability Development

- Coordination and Collaboration

- Capacity Development

- Awareness and Advocacy

Thank You

Contact @ btcirt@btcirt.bt