Ransomware, Incident Response and Forensics

Raskin Paul

Understanding the Threat: Ransomware

Ransomware is a type of malicious software that **encrypts a victim's data** or locks access to systems, demanding a ransom—often in cryptocurrency—to restore access.

System Compromise

Attackers gain control through phishing or exploiting vulnerabilities.

Data Encryption

The core attack: data is encrypted, making it inaccessible without the decryption key.

Ransom Demand

A payment, usually in cryptocurrency, is demanded to release the encrypted data.

Organizations face **costly downtime, irreparable data loss, reputational damage**, and severe regulatory penalties.

Ransomware Attack Vectors

Phishing Emails

Deceptive emails trick users into revealing credentials or downloading malware.

Infected USB Drives

Malicious software can spread when infected USB drives are connected.

Malicious Websites

Compromised websites, deceptive ads, or drive-by downloads can infect systems.

Compromised Credentials

Stolen usernames and passwords allow unauthorized access to systems.

Software Vulnerabilities

Exploiting unpatched flaws in software or operating systems allows attackers in.

Preventing Ransomware

Implementing a layered defense strategy is crucial for protecting your organization against modern cyber threats. These practices cover technical controls, user behavior, and continuous monitoring.

User & Email Security

- Avoid suspicious file attachments & links
- Avoid download attachment from spam emails
- Only open emails from known recipients
- Employee training and awareness

Endpoint & Application Control

- Say no to executables, scripts, macros
- Enforce Application Control on endpoints
- Endpoint Detections and Response

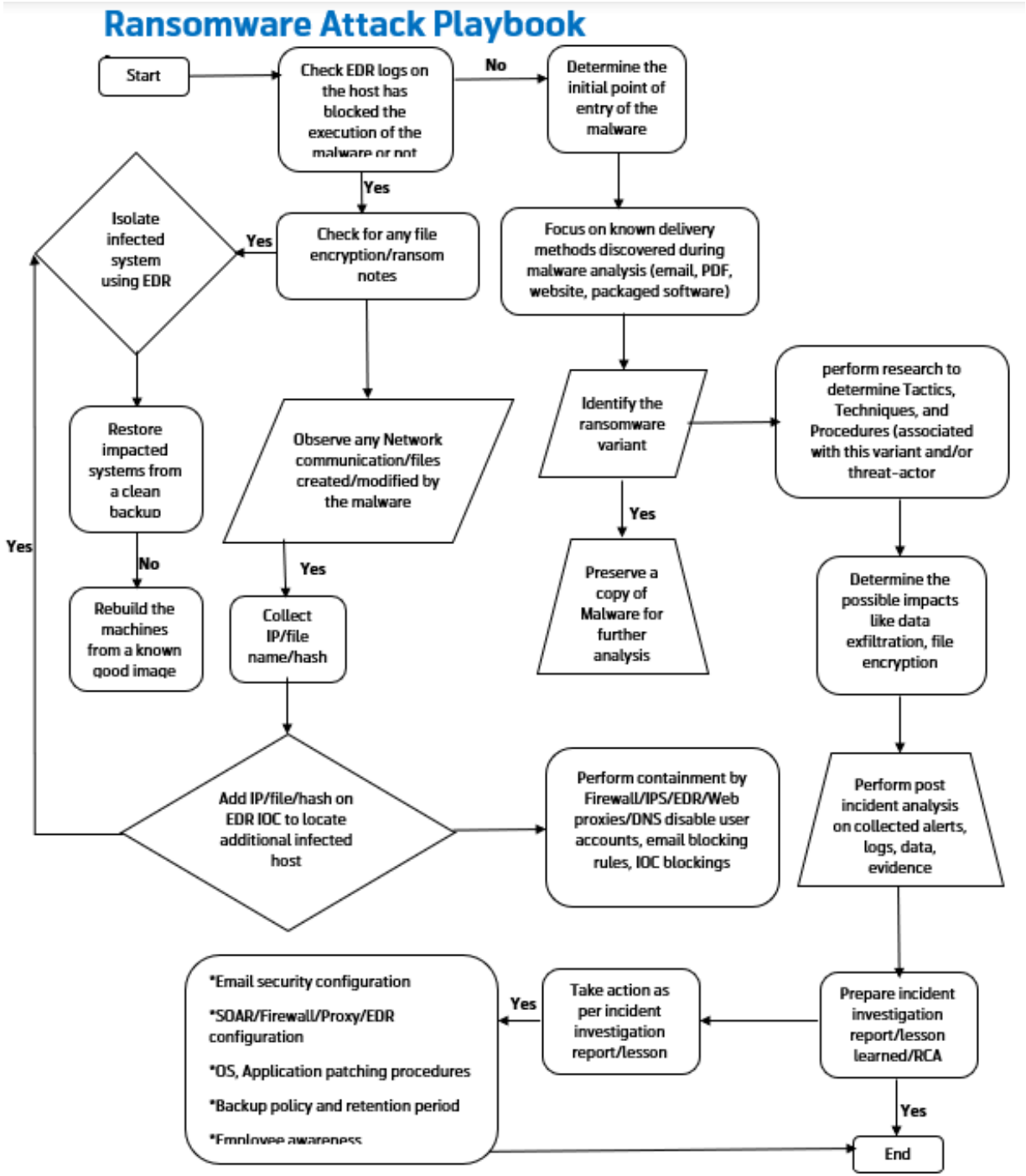
Network & System Hygiene

- Browse carefully
- Remove plugins from browser
- Use ad blocker
- Regular patch updates
- Limit usage of SMB protocol and disable where possible

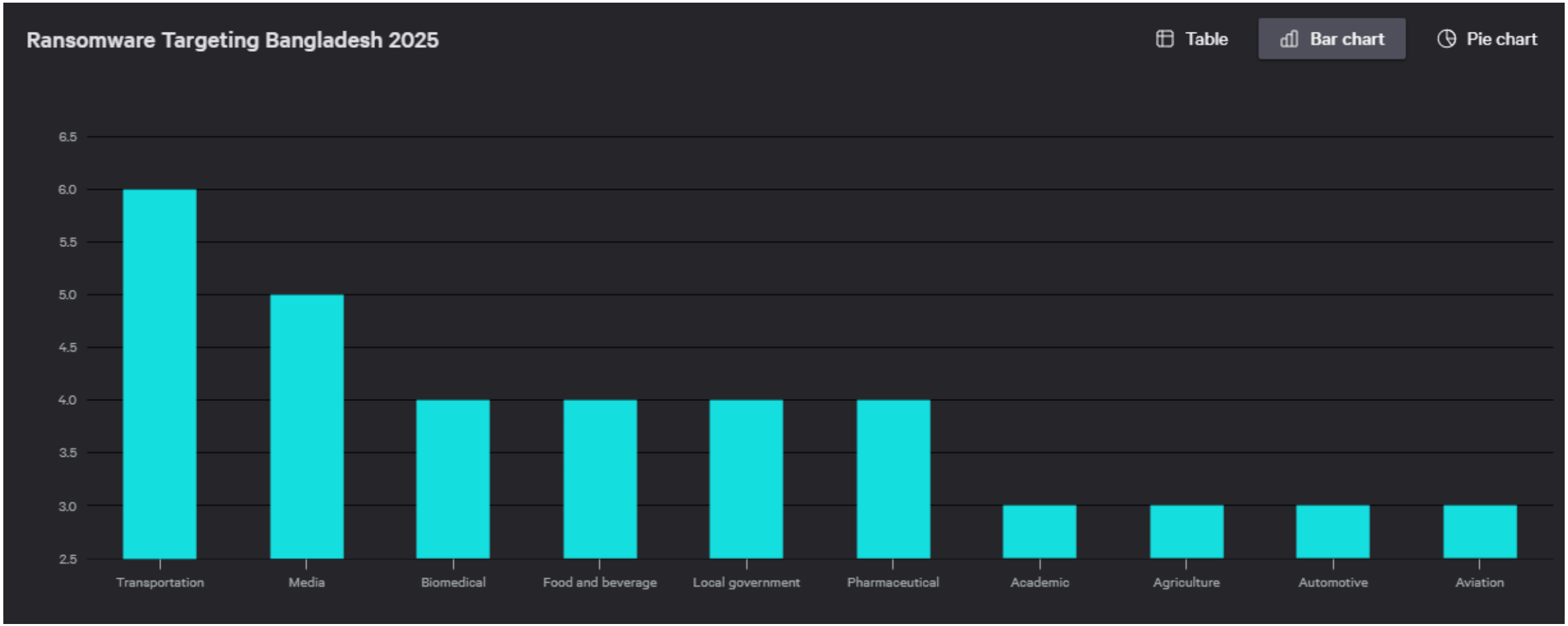
Access & Detection

- Multi-factor authentication
- Ensure least privilege
- SIEM rules multi source log Correlation and Threat Intel IOC for early detection

Ransomware Incident Response Playbook



Industry Wise Ransomware Attack Trends in Bangladesh



Ransomware Threat Landscape by Industry

A breakdown of the most likely ransomware families, along with key indicators and indicators of compromise (IOCs) observed across various critical industries.

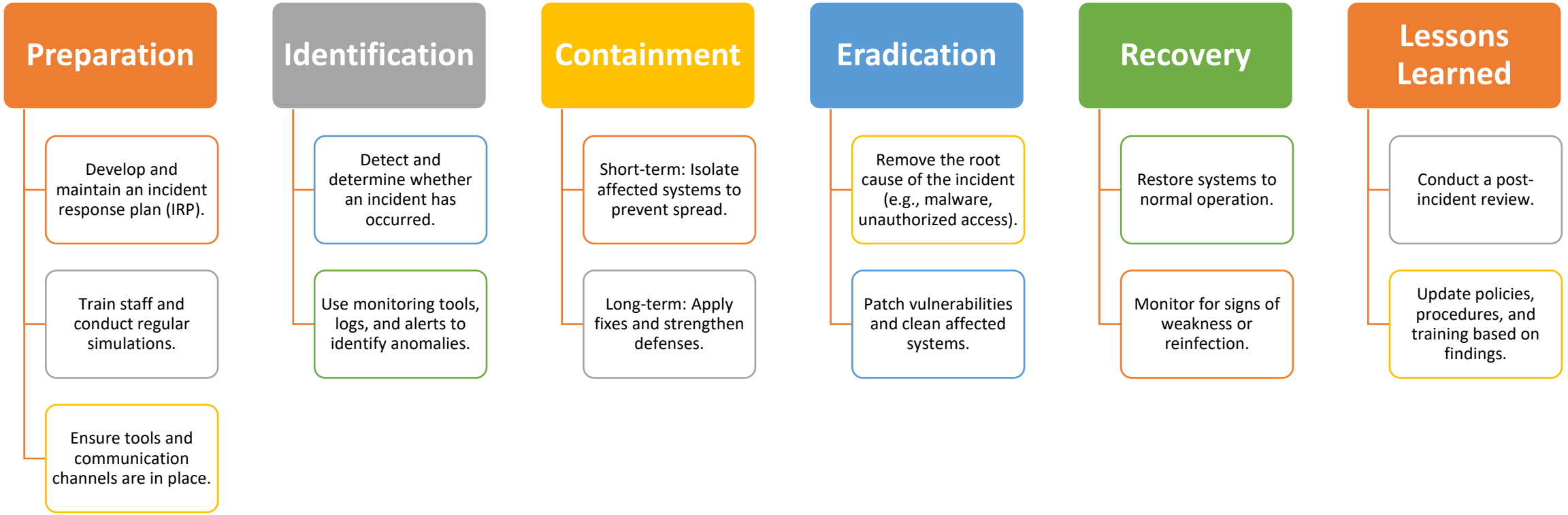
Industry	Likely Ransomware Families	Key Indicators / IOCs
Financial services	LockBit, Clop, ALPHV/BlackCat	Mimikatz credential theft, .lockbit3 extension, ransom note ClopReadMe.txt
Government / public sector	LockBit, ALPHV/BlackCat, Hive	Lateral movement via SMB, GPO misuse for mass encryption
Aviation & transport	LockBit, Conti-style (descendants)	Targeting VMware ESXi hosts, disabling backups
Healthcare	LockBit, Clop	Double extortion (exfiltration + encryption), data leaks
Education	Clop, LockBit	Supply-chain compromise, credential reuse
Energy & utilities	ALPHV/BlackCat, LockBit	Disabling logs, shadow copies, OT network access attempts
Telecom / ISPs	LockBit variants, supply-chain affiliates	Data exfiltration via third-party services, unusual outbound traffic
Manufacturing / logistics	Clop, LockBit	Targeting AD servers, lateral movement to OT networks
Retail / e-commerce / supply-chain software	Clop (supply-chain style), LockBit affiliates	Exploitation of third-party software (MOVEit, GoAnywhere), data exfiltration before encryption

Understanding these industry-specific threats is crucial for developing targeted defense strategies and prioritizing security investments.

Understanding Incident Response

Incident Response is a structured approach to managing and addressing security breaches or cyberattacks. The goal is to handle the situation in a way that limits damage, reduces recovery time and costs, and mitigates the risk of future incidents.

Key Phases of Incident Response



Effective Incident Response

Implement Zero trust principles with Proper Network Segmentation

Ensure Defense in Depth as much as possible

Organizational strategy shall be risk driven rather than alert volume for True Positive Incident Candidate selection.

A solid incident response plan documented with proper communication matrix and automated playbook.

Skilled IR team resources with proper environment knowledge for quick containment, Eradication, Recovery and preventing future incidents.

Availability of logs from all possible Infra and application log sources for better correlation and visibility.

SOC team equipped with Security tools such as EDR, SIEM, SOAR, NDR, CTI, Dark Web Monitoring etc.

Deploy SOAR playbook based automated incident response

Generative and Agentic AI capability for better false positive elimination and faster incident response.

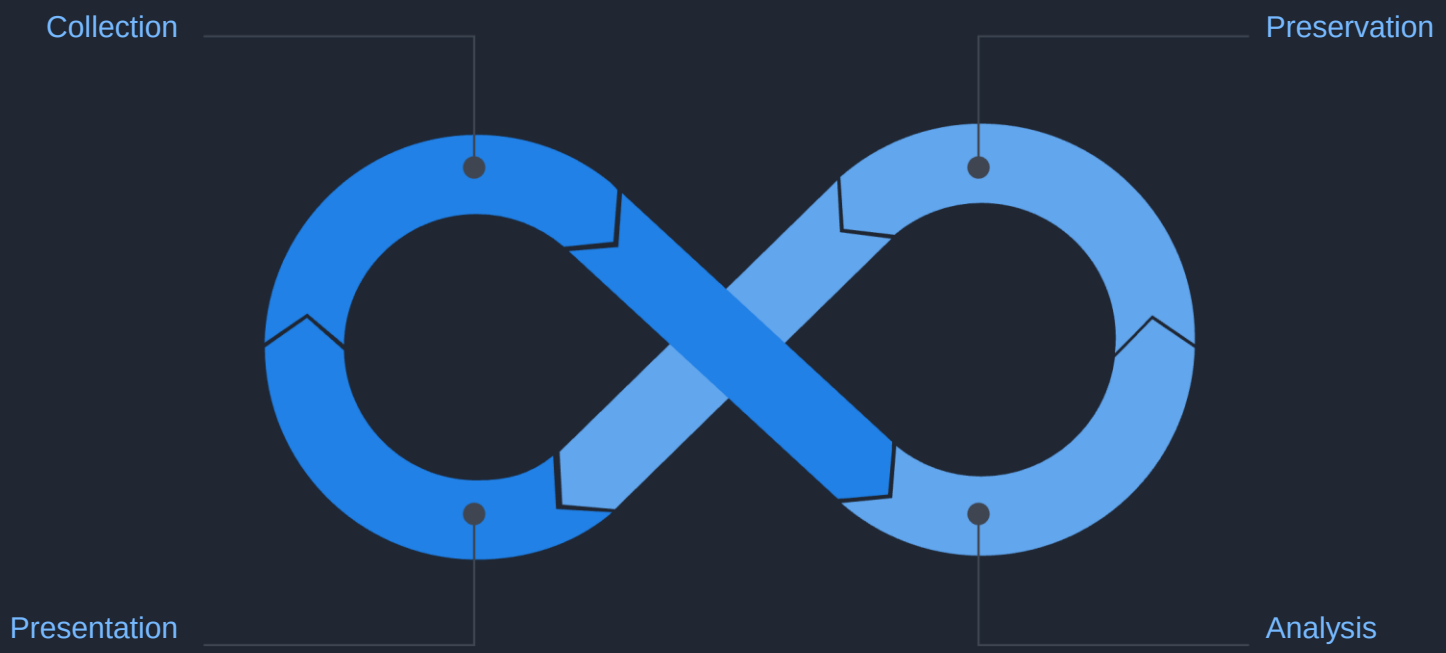
Threat Actors Trend Bangladesh

Name	Known as	Motivations	Capabilities
PUNK SPIDER	REDBIKE, Akira, Storm-1567	Criminal	ransomware
HOOK SPIDER	BenjaminFranklin, pirat-network, Big-Bro, crasty_bro, pirat, Pirat-Networks	Criminal	exploit,informationstealer
FRANTIC TIGER	--	State-Sponsored	credentialharvesting,informationstealer,exploit
SOLAR SPIDER	--	Criminal	--
VETO SPIDER	nixploiter	Criminal	exploit,botnet
STARDUST CHOLLIMA	APT38, HIDDEN COBRA, CryptoCore, TAG-71, Bluenoroff, COPERNICIUM, Sapphire Sleet, Lazarus Group, Dangerous Password, TA444, Alluring Pisces, BeagleBoyz, CageyChameleon, Leery Turtle, CryptoMimic	State-Sponsored,Criminal	--
BITWISE SPIDER	LockBit, LockBitSupp, Fox William Mulder	Criminal	ransomware,informationstealer
HAZY TIGER	Bitter APT, Orange Yali	State-Sponsored	--
RAZOR TIGER	Baby Elephant, Rattlesnake, Operation Origami, APT-Q-39, Sidewinder, APT-C-17, Hardcore Nationalist, T-APT-04	State-Sponsored	--
QUILTED TIGER	Patchwork, Chinastrats, Monsoon, APT-C-09, Dropping Elephant, Orange Athos	State-Sponsored	rat,informationstealer,credentialharvesting
OUTRIDER TIGER	--	State-Sponsored	backdoor,credentialharvesting
OCULAR SPIDER	Knight, RansomHub, Cyclops	Criminal	ransomware
FABLE TIGER	--	State-Sponsored	credentialharvesting, informationstealer, exploit

Forensics

Digital forensics plays a crucial role in cybersecurity and incident response It helps to uncover the truth behind incidents by examining logs, metadata .

It involves collecting, preserving, analyzing, and presenting data from computers, networks, mobile devices, and cloud environments to identify security breaches, insider threats, data exfiltration, or other malicious activities.



Key stages of Forensic investigation

Thank You