Playbook

for Redressal and Prevention of

RANSOMWARE

pnb

CYBER AND INFORMATION SECURITY DIVISION (CISD)

INDEX

“A secure cyberspace is a shared responsibility.”

HOW TO USE PLAYBOOK ?

Ransomware cyber incident, unlike most other cyber incident puts organisation on a countdown timer. Decisions need to be made quickly in a careful and orderly manner to address the cyber incident. Any delay and wrong step in the decision making process can result in an unwanted situation, public disclosure, loss of data, damage to cyber/IT infrastructure and adverse publicity, all resulting in loss of business.

The Playbook focuses on containment of Ransomware cyber incidents, analysis and recovery of data from incident. The Playbook provides "Do's and Don'ts" to prioritise the action and engage right experts, IT personnel and process during detection, mitigation and recovery from such cyber incidents. Comprehensive analysis and incident response for Ransomware incident is covered in this PNB's playbook.

WHAT IS RANSOMWARE ?

Ransomware is a type of malicious software deployed by cyber attackers, also known as threat actors, to infiltrate and infect computing devices. Once installed, it encrypts data, locks access to systems, and often damages IT infrastructure. The attackers then demand a payment, referred to as a "ransom," in exchange for restoring access and decrypting the data.

In many cases, ransomware operators also exfiltrate sensitive information and demand additional ransom payments to prevent the public disclosure of the stolen data. Such incidents can severely disrupt business operations and damage an organisation's reputation.

Ransomware typically spreads through phishing emails, malicious links or downloads, compromised websites, social media platforms, messaging apps, or infected USB and other removable media. Attackers often exploit vulnerabilities in IT systems and take advantage of poor cybersecurity awareness among staff, employees, and users to gain access and deploy ransomware.

Timely detection, user awareness, and robust cybersecurity practices are key to defending against ransomware threats. A proactive approach to prevention is far more effective than dealing with the consequences of an attack.

How It Affects Organizations, Especially Banks

Banks are particularly vulnerable to ransomware attacks due to their being critical infrastructure and having sensitive data. Such attacks can disrupt services, lead to data breaches and cause significant financial loss and loss of customer confidence.

Operational Disruption

Ransomware can shut down critical systems, making it impossible to perform daily operations like processing transactions or accessing customer data.

Financial Losses

Banks may lose money through ransom payments, downtime, remediation costs and potential regulatory fines.

Reputation Damage

A ransomware attack can erode customer trust, especially if sensitive data is exposed.

Regulatory Impact

Banks operate in highly regulated environments. A breach can lead to investigations, penalties and loss of licenses or certifications.

Data Breach Consequences

Many ransomware variants now also steal data before encryption. This can result in data leakage, identity theft and class-action lawsuits.

HOW DOES RANSOMWARE INCIDENT OCCUR ?

‘Ransomware’ incidents occur similar to other “Malware” based cyber incidents. The first step of any ‘Ransomware’ incident is to get the “Malware” installed on the computing device/IT infrastructure. The technique and mode of or initial access and installation/hosting used by the Perpetrators/Adversaries include the following.

a) Phishing: Phishing is a cyber incident that entices the user to click on or open a malicious link or file generally sent through emails. The malicious links are also posted on web sites and social media web sites. Often these links/ files come through a mass email that appears to be legitimate service like the one from office staff or the senior management or known Govt. Service, when someone/user click the link, the Perpetrator/Adversary execute commands using the credential of the device/IT infra to the perpetrators. The clicking of malicious links takes the user to another malicious computer hosting the “Ransomware Malware”. Through this process the malware is transferred, installed and hosted in the user device/IT infra.

b) The Perpetrator/Adversary also use the above-mentioned techniques to transfer or build a ‘backdoor’ into the user’s device/IT infra. Such ‘backdoors’ are used later on to transfer ‘Ransomware’ to extract the data, build part of encryption key, encrypt the data and lock the user’s device /IT infra.

c) Drive-by download: The user downloads Ransomware by visiting a malicious website. On the site they click on the download link, which provides the Perpetrators an entry into the system where malware can be installed to begin a Ransomware incident.

d) Malvertising: Malvertising uses legitimate online advertisements to lure users and replaces the software code with malicious software code that leads to downloading malware. A user will click on the 'Above Link' and is there after taken to a malicious website or directly downloaded malware.

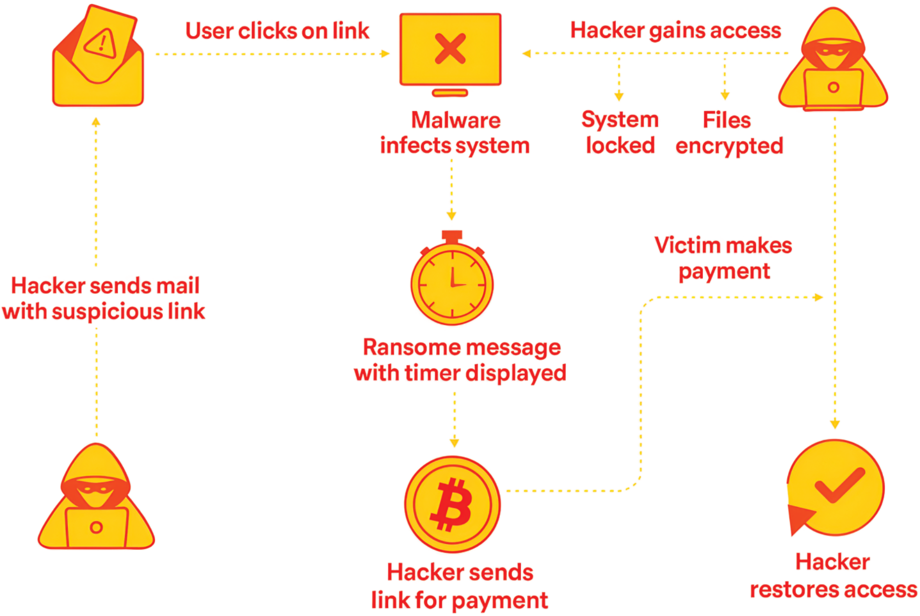
e) Exposed Services and other default ports: Exposed services, like Remote Desktop Protocol (RDP), allow access to the system and are a route for downloading Ransomware. Perpetrators and Adversaries exploit vulnerability in these services or extract passwords using different techniques to get access to the device/Infra and release 'Ransomware' into the target network.

f) Removable Media: The 'Ransomware' links are embedded within removable storage devices such as USB drives or pen drives. Removable media, such as pen drives, when connected to the device or network media, replicate the ransomware within the computer system. The ransomware rapidly encrypts information stored on the device or within the IT infrastructure.

g) Third parties and Managed Service Providers (MSP) are often exploited in phishing attacks. MSP/ User credentials are utilized to send spoof emails, leading users to permit the transfer, installation, and hosting of malware on the device/IT infrastructure.

h) Ransomware as a Service (RaaS): It's an organised model, which provides Ransomware capabilities to would-be criminals who do not have the skills or resources to develop Ransomware/Malware on their own. Perpetrators buy Ransomware kits on the dark web from malicious developers. The developers are entitled to a portion of the ransom if the incident is resolved successfully.

HOW RANSOMWARE WORKS ?



ANATOMY OF A RANSOMWARE ATTACK

1. Initial Access

How attackers gain entry into the network:

- Phishing Emails with malicious attachments/links
- Exploiting Vulnerabilities in unpatched software (RDP, VPNs, web apps)
- Stolen Credentials bought from dark web marketplaces
- Drive-by Downloads from compromised websites

2. Execution

Once inside the system:

- Drops malicious payload (ransomware executable)
- Uses PowerShell or scripts to evade antivirus
- Often runs in memory to avoid detection

3. Command & Control (C2) Communication

- Connects with attacker-controlled servers
- Receives instructions for next steps
- May download additional tools (e.g., Mimikatz, Cobalt Strike)

4. Lateral Movement

Spreads across the network:

- Exploits Active Directory for privilege escalation
- Uses Windows admin tools (PsExec, WMI)
- Maps network drives and critical servers

5. Data Exfiltration (Double/Triple Extortion)

➲ Steals sensitive data before encryption

➲ Uploads to external servers controlled by the attacker

➲ Used as leverage: “Pay or we leak your data”

6. Encryption

➲ Files are encrypted using strong algorithms (e.g., AES, RSA)

➲ File extensions are changed

➲ Drops a ransom note with payment instructions

7. Extortion

➲ Demands ransom via cryptocurrency (usually Bitcoin or Monero)

➲ Threatens data leak, public exposure, or DDoS (triple extortion)

➲ May offer “customer support” via dark web portals

8. Impact

➲ Downtime of operations

➲ Loss of data / trust / revenue

➲ Reputational damage

➲ May trigger legal, regulatory and compliance issues

Defensive Measures

✓ Patch Management

✓ Endpoint Detection & Response (EDR)

✓ Regular Backups (offline/offsite)

✓ Security Awareness Training

✓ Zero Trust Architecture

✓ Immutable Backup

✓ Network Detection and Automated Responses (NDR)

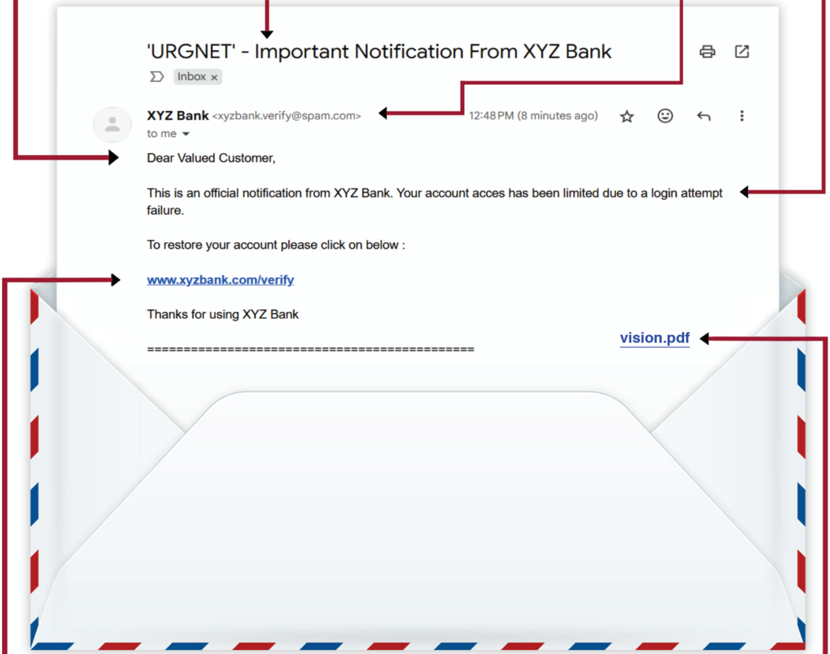
HOW PHISHING EMAIL LOOK LIKE ?

Generic Greetings :
Legitimate companies typically address you by name.

Subject :
Urgent Call to Action, creating a sense of Urgency, Fear and Greed

Look a Like Email ID and Name :
Email addresses that look similar to legitimate ones but contain slight errors

Spelling Error :
Legitimate organizations take care to write professional emails.



'URGNET' - Important Notification From XYZ Bank

XYZ Bank <xyzbank.verify@spam.com>
to me
12:48 PM (8 minutes ago)

Dear Valued Customer,

This is an official notification from XYZ Bank. Your account acces has been limited due to a login attempt failure.

To restore your account please click on below :

www.xyzbank.com/verify

Thanks for using XYZ Bank

vision.pdf

==

Fake Link :
Hover over any link (without clicking it) to see where it leads. Phishing emails often include links that look legitimate at first glance but lead to fake websites.

Attachments :
Phishing emails may include attachments, such as PDFs or ZIP files, which could contain malware or ransomware. Avoid opening attachments unless you are sure about the sender's identity.

TYPES OF RANSOMWARES

Type	Description	Example	Common Attack Vectors	Prevention Methods
Crypto Ransomware	Encrypts files and demands ransom for the decryption key.	WannaCry, CryptoLocker	Phishing emails, malicious attachments, exploit kits	Regular backups, updated antivirus, phishing awareness
Locker Ransomware	Locks the user out of their device or system.	WinLock, Police Trojan	Drive-by downloads, malicious websites	System hardening, updated OS, limited admin rights
Scareware	Uses fake alerts or popups to scare users into paying.	Fake antivirus software	Fake software updates, rogue security software	Use real antivirus, avoid suspicious popups
Doxware / Leakware	Threatens to publish stolen sensitive data unless ransom is paid.	Maze, Doppel Paymer	Phishing, remote desktop protocol (RDP) attacks	Data encryption, access control, network monitoring

Type	Description	Example	Common Attack Vectors	Prevention Methods
RaaS (Ransomware as a Service)	Ransomware provided as a service platform, used by affiliates.	REvil, DarkSide, LockBit 2.0, LockBit 3.0 (a.k.a Akira)	Phishing, RDP exploits, malvertising	Secure endpoints, monitor traffic, threat intelligence
Mobile Ransomware	Targets mobile devices with locking or encryption.	Android. Lockdroid	Malicious apps from third-party stores	Install apps from trusted sources only
Hybrid Ransomware	Combines characteristics of crypto and locker ransomware	NotPetya, Killer 1.0.8	Email attachments, compromised software updates	Comprehensive security policy, layered defence

HANDLING RANSOMWARE

The Do's and Don'ts in a ransomware incident are essential for minimizing and avoiding damage, preserving evidence, and enabling effective mitigation and recovery. Do's and Don'ts also are necessary to enhance the resiliency of IT Infra. An exhaustive list of Do's and Don'ts is provided below.

Do's

I. Identify and Isolate the affected/ suspected system, disabling all external and internal links, IT system and Network.

II. Check if the device (computer, laptop, tablet, or mobile phone) is on or off.

III. If the device is off, do not turn it on.

IV. If the device is on, do not turn it off or shut down.

V. Remove the network cable and disconnect the suspected/ affected device(s) from the network (Wi-Fi, Ethernet etc.) to prevent the Ransomware to spread.

VI. Disconnect all cords and "Devices" connected to affected/suspected system(s).

VII. Unplug the power cord from the device (Please be careful that "Device" is not shut down by using any command, until the cord is removed).

VIII. Remove the battery device in the "Device" and note down the following.

   a) Serial no. of the device and Battery

   b) Host Name

   c) IP Address

   d) Location and Username

IX. Report the incident to team handling cyber incidents.

X. Seize all storage media including USB device(s) which are/was used with the suspected /affected device.

For Incident Response team

I. Shift the affected/suspected system to sandbox or secured environment

II. Obtain snapshot of Device through forensic disk image. Imaging of affected device and its media be created using specialised tools in a sand box. This environment image shall be “bit” level copy and of sector by sector, to capture files, slack spaces and unallocated clusters.

III. Identify the strain and attempt determine the ransomware variant using trusted and reliable decryption tools available through reputable sources “Ransomware” may be partly encrypted to decrypt the software code or encryption key.

IV. **Follow Incident Response Plan** - Execute a pre-established Ransomware response plan, including communication protocols and decision-making authority.

V. **Notify Affected Stakeholders -** If customer data is at risk, inform them according to legal and regulatory requirements.

VI. **Engage Cybersecurity Professionals -** engage expert of providing incident response or forensic analysts to assist with containment and recovery of the “Ransomware”.

VII. Once the threat is contained, restore data from verified, uncompromised backups.

VIII. Save access logs from the suspected/affected system.

IX. Keep all media away from magnets, radio transmitters and other potentially damaging elements.

X. Preserve all the evidence collected from the device for investigation and potential recovery.

XI. Collect instruction manuals, documentation and notes on the configuration of the suspected/affected device.

XII. Document all steps followed and used in the seizure and handling the suspected/affected device including time stamp messages and ransom note.

XIII. Capture volatile data from device as evidence. This includes lists of network connection, processes, login sessions, open files, network interface configuration, and contents of the memory.

XIV. While creating these images, due care should be taken to ensure that the new media has no residual data and is write protectable or write once media.

XV. To ensure that the original image is not modified, it is important to create message digests or hashes for files and directories before and after the analysis to prove the integrity of the original Image.

XVI. At least two full copies of images of media be taken, label them properly and securely store one of the images to be used strictly as evidence.

XVII. All analysis should be conducted on the second copy of the image in order to preserve the original evidence from alteration during examination inadvertently.

XVIII. A standard file system backup can capture information on existing files, which may be sufficient for handling many incidents, particularly those are not expected to lead to prosecution.

XIX. Running carefully chosen commands from the trusted media can collect the necessary information without damaging the evidence.

Don't

I. Do not reset the password till incident is analysed, mitigated and IT systems/ Device is recovered.

II. Do not use the "Device" till further instructions from the authorised official/person/incident resolution team(s).

III. Do not connect infected /suspected Device and storage media to any network and another device without clearance from the authorised person.

IV. Do not format/delete/modify any content/data on the device.

V. Do not obtain snapshot of device through back and from file system back-ups.

VI. **Don't pay the ransom (unless absolutely necessary) -** There's no guarantee data will be provided back by the Perpetrators. It may also make you a target again.

VII. **Don't delete or reformat affected systems immediately -** This may erase forensic evidence crucial to investigations or decryptions.

VIII. **Don't use infected backups** - Check and verify backups to ensure they are not compromised before restoring.

IX. **Don't communicate with the Perpetrators directly** - Leave any negotiations or communications (if necessary) to legal and cybersecurity experts.

X. **Don't downplay the incident** - Transparency with stakeholders is critical to trust and compliance.

XI. **Don't reconnect recovery systems prematurely** - Ensure all systems are clean, patched, and secure before reconnecting to the network.

XII. **Don't ignore post-incident review and learning** - Failing to conduct a root cause analysis can leave you vulnerable to future incidents.

PRECAUTIONS AGAINST RANSOMWARE

1. Awareness & Training

☑ Educate employees and users about phishing, malicious attachments and suspicious websites.

☑ Conduct regular security drills and mock phishing campaigns.

☑ Train users to avoid clicking on unknown links and to verify the sender's identity.

2. Strong Email Filtering

Implement advanced email filtering solutions that:

☑ Detect and block phishing and spam emails.

☑ Filter emails with suspicious attachments or links.

☑ Use AI-based detection for unknown threats.

3. Regular Backups & Restoration Plans

☑ Maintain frequent backups of important data (daily or weekly).

☑ Store backups in offline or immutable storage.

☑ Regularly test restoration procedures to ensure data can be recovered quickly.

☑ Use versioning to roll back to uninfected file versions.

4. System & Network Security

☑ Keep all software and operating systems up to date.

☑ Use Next-Gen Antivirus and EDR (Endpoint Detection & Response) tools.

☑ Restrict admin privileges and enforce least privilege access.

☑ Use firewalls, intrusion prevention systems and network segmentation.

☑ Use of Network Detection and Automated Responses (NDR)

6. Use of Multi-Factor Authentication (MFA)

☑ Secure access to sensitive systems and backups using MFA.

☑ Prevent lateral movement by isolating privileged accounts.

STRATEGIC RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS TO COMBAT RANSOMWARE

a. Monitor regulatory updates from both RBI and CERT-In to maintain full compliance.

b. Monitor dark web forums for leaked credentials or early signs of Ransomware targeting.

c. Enforce Multi-Factor Authentication (MFA) for all internal and customer-facing systems.

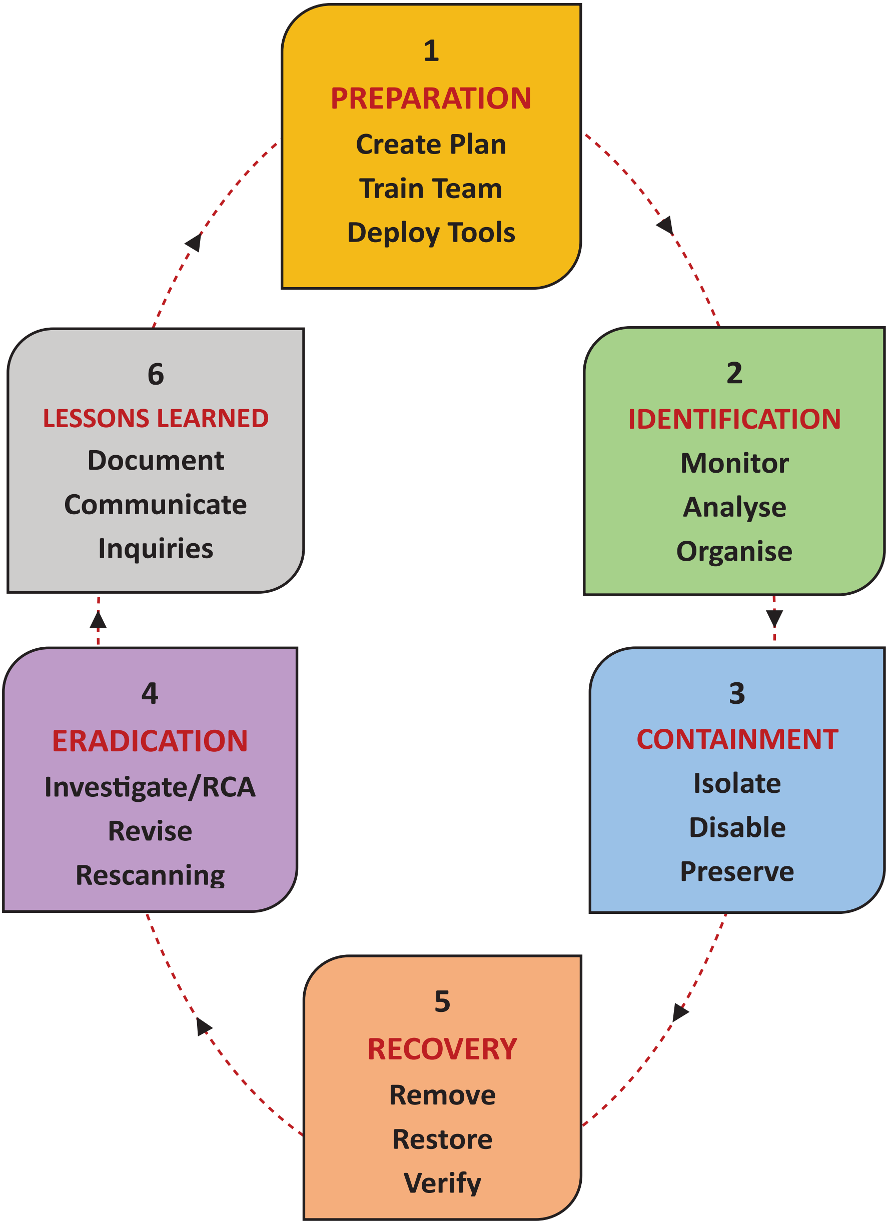
d. Establish robust incident response plans that include ransomware-specific scenarios.

e. Invest in employee training to recognise phishing and social engineering incidents.

f. Ensure contractual clauses with third parties include security compliance and breach notification obligations.

g. Regularly simulate phishing incidents and train teams on Ransomware behaviours.

RANSOMWARE INCIDENT RESPONSE LIFECYCLE



1
PREPARATION
Create Plan
Train Team
Deploy Tools

2
IDENTIFICATION
Monitor
Analyse
Organise

3
CONTAINMENT
Isolate
Disable
Preserve

4
ERADICATION
Investigate/RCA
Revise
Rescanning

5
RECOVERY
Remove
Restore
Verify

6
LESSONS LEARNED
Document
Communicate
Inquiries

COMMON TYPES OF MALWARE

Virus

Attaches to files and spreads when the file is executed.

Worm

Self-replicates and spreads across networks without user action.

Trojan Horse

Disguises as legitimate software but performs harmful actions once installed.

Spyware

Secretly gathers user information and sends it to attackers.

Rootkit

Hides deep in the system to grant remote access or control to attackers.

Adware

Displays intrusive ads and may track browsing behaviour.

Botnet

A network of infected devices controlled remotely to launch attacks.

GLOSSARY OF TERMS

Term / Acronym	Definition
Perpetrator / Adversary	In cybersecurity, a **perpetrator** is the one who directly carries out a malicious act like hacking or data theft. An **adversary** is any individual, group, or nation that poses a threat to digital systems, regardless of whether an attack has occurred
Payload	The part of malware which performs the malicious action, such as encryption or data deletion.
C2 (Command & Control)	Servers controlled by attackers used to send instructions to infected systems.
Zero Trust Architecture	A security model that requires verification for every user and device attempting to access resources, regardless of origin.
Endpoint Detection and Response (EDR)	A cybersecurity solution that monitors endpoints (devices) to detect and respond to threats in real time.
Immutable Backup	Backups that cannot be altered or deleted, even by ransomware or attackers.
Network Detection & Automated Response (NDR)	A security solution that uses AI and behavioural analytics to detect threats on the network level.
Ransomware-as-a-Service (RaaS)	A criminal business model where ransomware tools are sold or rented to affiliates for a share of the profits.
Sandbox	A controlled environment where suspicious files or programs can be safely executed and analysed.
Incident Response Plan (IRP)	A structured approach outlining how to handle and mitigate cybersecurity incidents.
Dark Web	A hidden part of the internet often used for illicit activities, including buying/selling stolen data or malware.