**Ransom Playbook**

**Scope**

This Playbook covers various type of Ransom we could be faced with. The most common being Ransomware but we try to also account for other types.

It was built to be run in parallel with the **Malware Playbook**.

**1. Preparation**

**Summary**

- Create and maintain a list of

- all domains owned by Organisation.

- This can prevent you from taking actions against our own domains

- all people that can register domains

- Create email template

- to notify all employees of ongoing phishing campaign against the organisation

- to contact hosting organisation for domain(s) take down

- to inform 3rd party to take actions against phishing on their infra (Microsoft, Amazon, etc.)

- Ensure that:

- Mail anti-malware/anti-spam/anti-phish solutions are in place.

- Users know how to report phishing

- Detection exists for office documents spawning processes

- PowerShell

- CMD

- WMI

- MSHTA

- Etc.

- Perform dry drills to ensure all aspects of the Playbook are working

- After publication

- At least once a quarter

- Test/Validate:

- Internal Contact and Escalation Paths

- Review threat intelligence for

- threats to the organisation,

- trends for the sector,

- common patterns

- newly developing risks and vulnerabilities

- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following

- IR Playbooks to highlight information security risks faced by employees, including:

- Phishing attacks and malicious emails;

- Ransomware;

- Reporting a suspected cyber incident.

**Tool Access and Provisioning**

**Tools**

Please referrer to [DCOT Handbook]

**Assets List**

- A list of assets and owner should exist and be available for the following

- Customers Assets

- Owners

- Contacts

- Pre approved/authorized actions

- Organisation Assets

- Owners

- Contacts

- Administrators

- Pre approved/authorized actions

- Type of assets inventory needed

- Endpoints

- Servers

- Network Equipment

- Security Appliances

- Network Ranges

- Public

- Private

- VPN / Out of Band

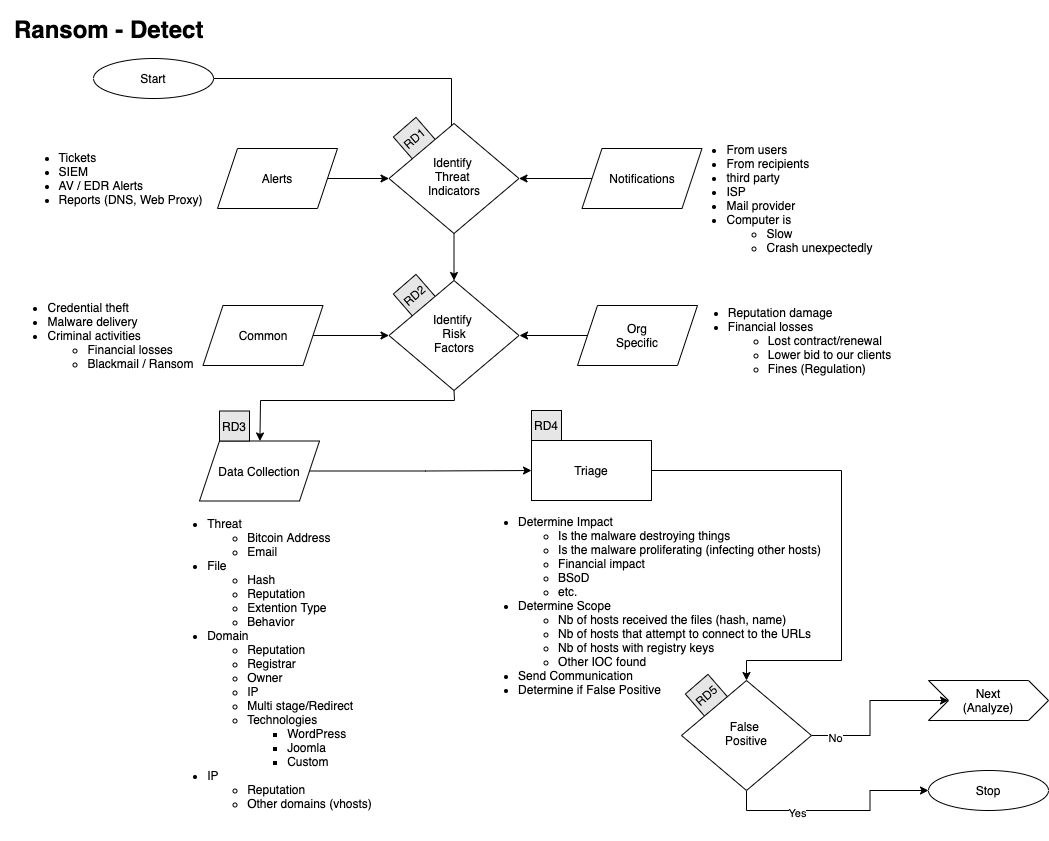
- Employees

- Partners

- Clients

**2. Detect**

**Workflow**



**Identify Threat Indicators**

**Alerts**

Alerts are be generated by different systems. The main sources for alerts are

- Tickets

- SIEM

- Anti-Virus / EDR

- Reports

- DNS

- Web Proxy

- Errors from mail servers

**Notifications**

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)

- Recipients of emails (external)

- Third Parties

- ISP

- Mail Providers

**Identify Risks Factors**

**Common**

- Credential Theft

- Malware Delivery

- Criminal Activities

- Blackmail / Ransom

Company Specific

- Financial Losses

- Lost of contract

- Contract not renewed

- Lower bid to our clients

- Fines

- Regulation

**Data Collection**

This section describes the information that should be collected and documented about the incident.

**Domains**

- Reputation

- Registrar

- Owner

- IP

- Multistage / Redirect

- Technologies of the site

- WordPress

- Joomla

- Custom Page (credential phish)

**Intellectual Property**

- Reputation

- Owner

- Geo Localisation

- Other domains on that IP

**Categorise**

**Categorise**

**Determine type of**

**Triage**

**Determine**

- Impact

- Of

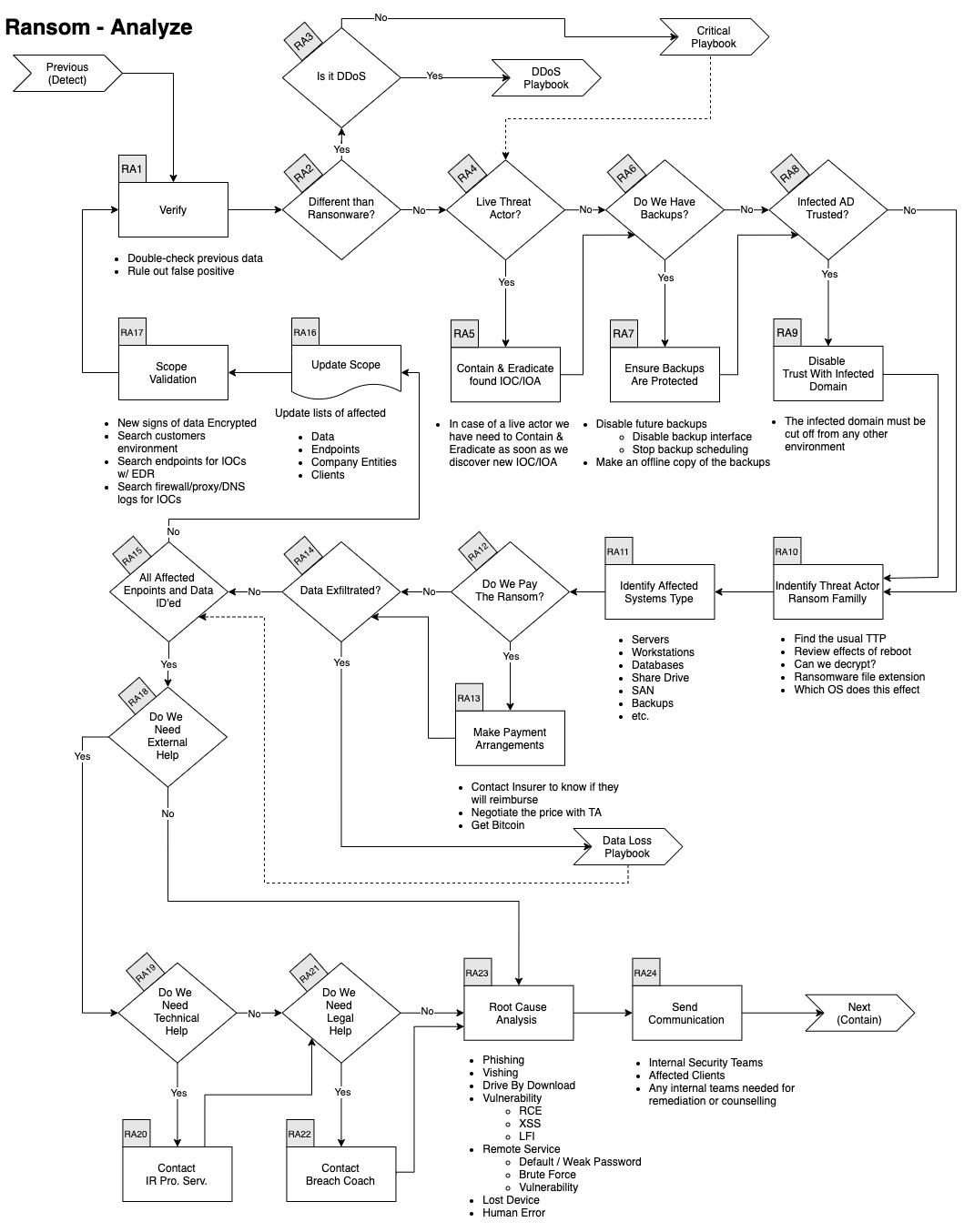
- Financial

- Data loss

- Scope (Nb of people)

**3. Analyse**

**Workflow**



**Verify**

In conjunction with a senior member of the DCOT

- Double check previous data

- Rule out False Positive

**Identify type of Ransom**

The first thing we need to do is understand which type of Ransom we are dealing with.

- Is this a Ransomware?

- Is this a DDoS related Ransom?

- For now, we do not have a DDoS Playbook, so referrer to the **Critical Playbook**

If it's another type, you should follow the **Critical Playbook** and escalate to the DSOC.

**Assess if the Threat Actor is still in the Network**

Depending if the actor has successfully encrypted the data or if they are still actively trying, the speed at which we must act is different.

If the actor is still in the network, the containment effort needs to be taken as fast as possible and the **Contain & Eradicate** actions will be intertwined with the **Analysis**.

**Do We Have Backup**

If we have backups, we must make sure they are protected and not overwritten. Here's some of the steps that needs to be taken:

- Disable future backups

- Disable backup Interface

- Stop backup scheduling

- Make an offline copy of the backup

Is the infected environment (AD) trusted by another environment?

In order to prevent the adversaries to reach other domains that could be linked, we need to

- Disable any Trust from that domain to others

- In some cases, we might need to disconnect the MPLS Link

- This needs management approval, refer to the **Critical Playbook**

**Identify Threat Actor/Ransomware Family**

Using the various artefacts, we need to identify who our adversary is. This will help

- Know the TTP they typically use

- Potentially identify the Initial Access technique

- Understand how they move laterally

- WMI

- PSExec

- RDP

- Etc.

- Understand the effect of a reboot on the machine

- Is there a known decryptor

- This is increasingly less frequent

- Which OS version is targeted

**Things that we can use to identify the adversary:**

- Ransomware note

- Malware payload

- Encrypted file extensions

- Email / Web portal

- Bitcoin addresses

- etc.

**Identify Affected Systems Type**

In order to remediate properly and engage the right team(s) we need to understand which type of systems were affected:

- Servers

- OS version

- Kernel

- Workstations

- OS version

- Service Pack

- Databases

- Share Drives

- SAN

- Backups

- Etc.

**Do We Pay the Ransom**

We don’t negotiate with terrorists.

**Was Data Exfiltrated**

If data was exfiltrated we need to refer to the **Data Loss Playbook**

Were All Endpoints and Data Identified?

If we have found new affected endpoints or data go to the next section.

If we have identified all endpoints and data you can jump to

- Update FW, IDS, etc. rules w/ IOCs

- Search endpoints for IOCs w/ EDR

**Update Scope**

- Update lists of

- affected endpoints

- affected Company Entities

- affected clients

**Scope Validation**

Have all the machines been identified?

If you find further traces of phishing or new IOCs go back through this step.

When you are done identifying all compromised:

- Hosts

- Data

You can continue to the next phase.

**Root Cause Analysis**

Identify how this incident happened.

- Phishing Emails

- Voice Phishing

- Drive-by Download

- Vulnerability

- Remote Code Execution

- Cross-Site Scripting

- Remote Services

- Default / Weak Password

- Brute Force

- Vulnerability

- Lost Device

- Human Error

**Send Communication**

Contact any relevant of the following party

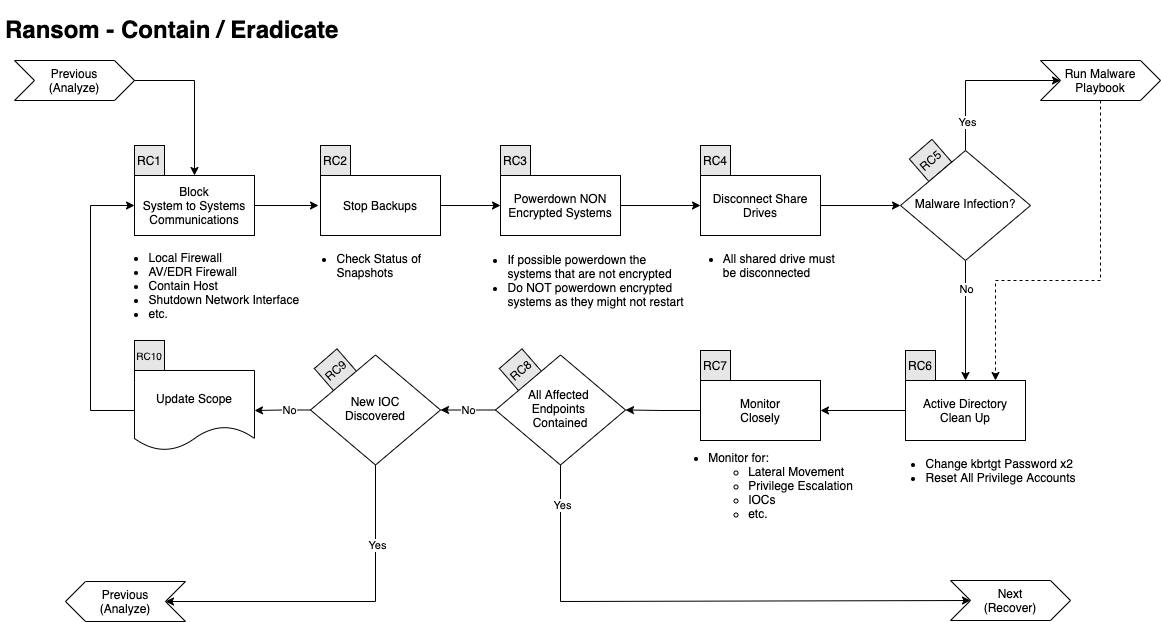
- DSOC

- Affected Clients

- Any internal teams needed for remediation or counselling

**4. Contain / Eradicate**

**Workflow**



**Block Systems to Systems Communications**

The first things we need to do with ransomware is to block systems to systems communication. We can do this using various methods such as:

- EDR containment function

- Local Firewall

- This could be circumvented if the adversary is still on the system

- AV/EDR Firewall

- Shutdown Network Interface

- This mostly apply to VM

- Disable the switch port on the router

- Etc.

**Stop Backups**

- Check status of Snapshots

**Power down NON-Encrypted Systems**

- If possible, power down the systems that are not encrypted

- Do NOT power down encrypted systems as they might not restart

**Disconnect Share Drives**

- All shared drive must be disconnected

**Malware Infection**

- If there is a Malware infection run the **Malware Playbook**

**Active Directory Clean Up**

In most cases these actions should be sufficient:

- Change kbrtgt Password twice

- Reset All Privilege Accounts

In cases where we believe Domain Admin account(s) were compromised we have to do the following before the steps above:

- Restore the AD from backup that predate the initial compromised

- If no backup exists:

- Consider rebuilding the AD from scratch.

- Change how we protect sensitive Accounts

The decision to rebuilt from scratch should come from the higher command.

**Monitor Closely**

- Monitor for:

- Lateral Movement

- Privilege Escalation

- IOCs

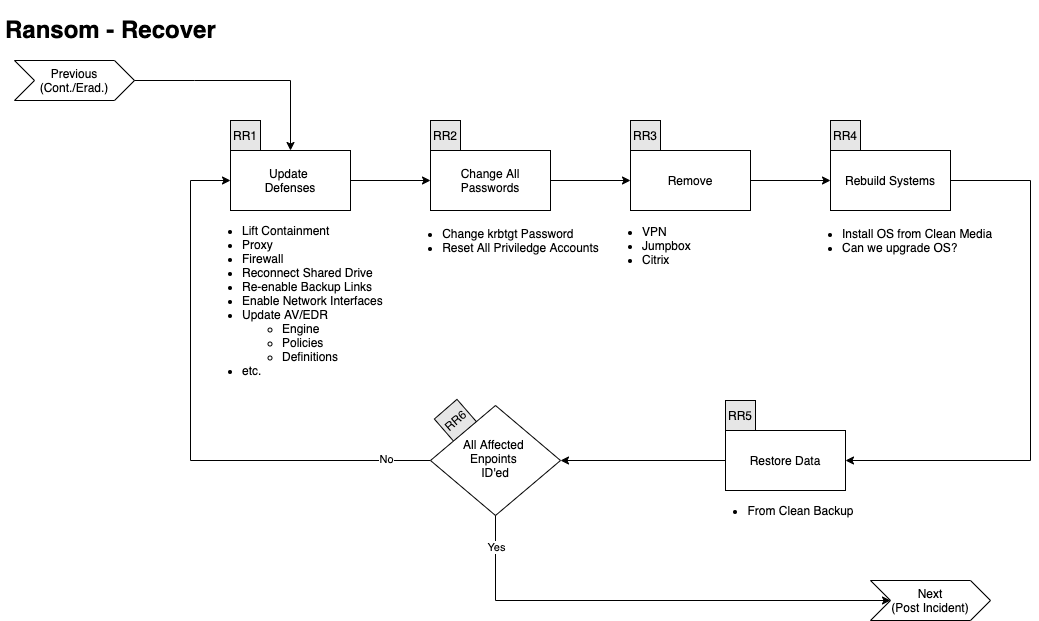
- etc.

**New IOC Discovered**

- Go back to **Ransom Analyse**

**5. Recover**

**Workflow**



**Update Defences**

Determine which of the following actions need to be performed:

- Lift Containment

- Proxy Block

- Firewall Rules

- Reconnect Shared Drives

- Re-enable Backup Links

- Enable Network Interfaces

- Update EDR/AV

- Engine

- Policies

- Definitions

**Change All Passwords**

- Change krbtgt Password

- Reset All Priviledge Accounts

**Remove**

- VPN

- Jumpbox

- Citrix

**Rebuild Systems**

- Install OS from Clean Media

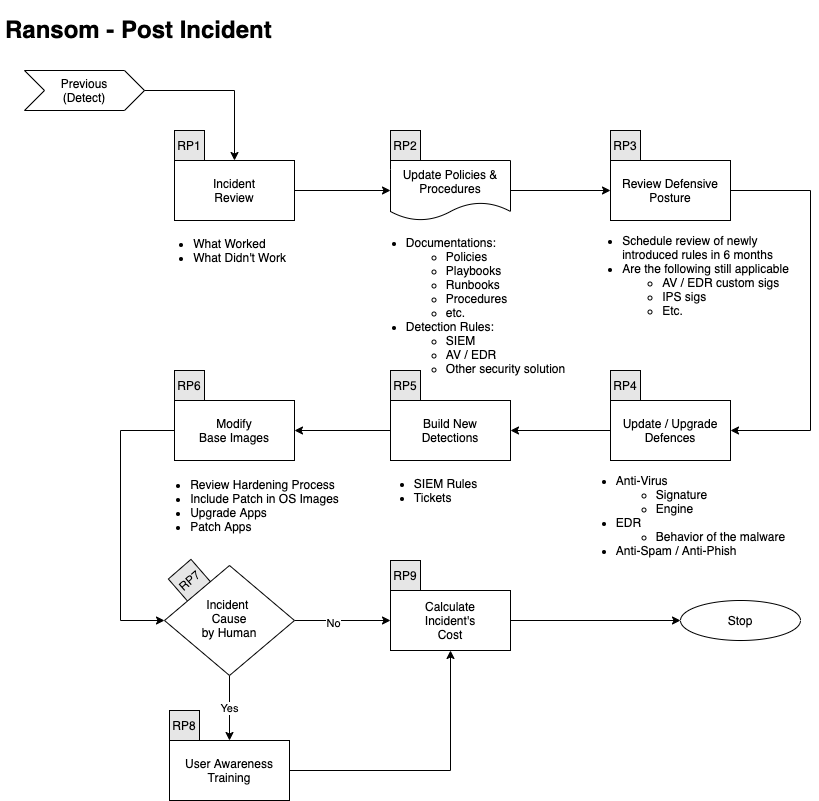
- Can we upgrade OS?

**Restore Data**

- Use a clean backup

**6. Post Incident**

**Workflow**



**Incident Review**

- What worked

- What didn't work

**Update Mode of Operations**

**Update the following documents as required:**

- Policies

- Processes

- Procedures

- Playbooks

- Runbooks

**Update Detection Rules in:**

- SIEM

- Anti-Spam

- Malware Gateway

- EDR

- Other security solution

**Review Defensive Posture**

- Schedule review of newly introduced rules in6 months

- Are the following still applicable

- Firewall Rules

- Proxy Rules for C2

- AV / EDR custom Signatures

- IPS Signatures

**Update & Upgrade Defences**

Various security solutions might need to be updated or upgraded to prevent a similar incident from occurring again. Here are a few items to consider:

- Anti-Virus

- Signatures

- Engine

- EDR

- Behaviour (TTP)

- Custom Detection

- Anti-Spam

- Filter

- Anti-Phishing

**Build New Detection**

If the incident was detected late in the Kill Chain, we need to try to improve our detection to catch a similar incident earlier.

We could for instance:

- Create SIEM rules

- Generate SNOW tickets

- Create Miro Plays

- etc.

Modify Base Images

If the Ransom was caused by a lack of hardening or sufficient patch level:

- Review hardening processes

- Include critical patches in base Images

- etc.

**User Awareness Training**

If the incident was caused by a human error

- Create / Select new mandatory training

- From Security Education Vendor

- From YouTube video

- Built by internal teams

**Calculate Incident's Cost**

**Calculate the incident's Cost**

- Time Spent

- Ransom paid

- Downtime

- Fines / Penalties

- etc.

**References**

This Playbook was built using the following references:

https://www.dfir.training/index.php?option=com\_jreviews&format=ajax&url=media/download&m=14tt1&1600804844570

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf