# Playbook: Ransomware

**Investigate, remediate (contain, eradicate), and communicate in parallel! Containment is critical in ransomware incidents, prioritize accordingly.**

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

## Investigate

`TODO: Expand investigation steps, including key questions and strategies, for ransomware.`

1. **Determine the type** of ransomware (*i.e.,* what is the family, variant, or flavor?)[1]
    1. Find any related messages. Check:
        - graphical user interfaces (GUIs) for the malware itself
        - text or html files, sometimes opened automatically after encryption
        - image files, often as wallpaper on infected systems
        - contact emails in encrypted file extensions
        - pop-ups after trying to open an encrypted file
        - voice messages
    2. Analyze the messages looking for clues to the ransomware type:
        - ransomware name
        - language, structure, phrases, artwork
        - contact email
        - format of the user id
        - ransom demand specifics (*e.g.*, digital currency, gift cards)
        - payment address in case of digital currency
        - support chat or support page
    3. Analyze affected and/or new files. Check:
        - file renaming scheme of encrypted files including extension (*e.g.*, `.crypt`, `.cry`, `.locked`) and base name
        - file corruption vs encryption
        - targeted file types and locations
        - owning user/group of affected files
        - icon for encrypted files
        - file markers
        - existence of file listings, key files or other data files
    4. Analyze affected software or system types. Some ransomware variants only affect certain tools (*e.g.*, databases (https://www.bleepingcomputer.com/news/security/mongodb-apocalypse-professional-ransomware-group-gets-involved-infections-reach-28k-servers/)) or platforms (*e.g.*, NAS products (https://forum.synology.com/enu/viewtopic.php?f=3&t=88716))
    5. Upload indicators to automated categorization services like Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php), ID Ransomware (https://id-

ransomware.malwarehunterteam.com/), or similar.

2. **Determine the scope:**
    1. Which systems are affected? `TODO: Specify tool(s) and procedure`
        - Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc. Use endpoint protection/EDR, endpoint telemetry, system logs, etc.
        - Check similar systems for infection (*e.g.*, similar users, groups, data, tools, department,configuration, patch status): check IAM tools, permissions management tools, directory services, *etc.*
        - Find external command and control (C2), if present, and find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, netflow or router logs, *etc.*
    2. What data is affected? (*e.g.*, file types, department or group, affected software) `TODO: Specify tool(s) and procedure`
        - Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools
        - Find changes to normally-stable or critical data files. Check file integrity monitoring tools
3. **Assess the impact** to prioritize and motivate resources
    1. Assess functional impact: impact to business or mission.
        - How much money is lost or at risk?
        - How many (and which) missions are degraded or at risk?
    2. Assess information impact: impact to confidentiality, integrity, and availability of data.
        - How critical is the data to the business/mission?
        - How sensitive is the data? (*e.g.*, trade secrets)
        - What is the regulatory status of data (*e.g.*, PII, PHI)
4. **Find the infection vector.** Check the tactics captured in the Initial Access tactic (https://attack.mitre.org/tactics/TA0001/) of MITRE ATT&CK[4]. Common specifics and data sources include:
    - email attachment: check email logs, email security appliances and services, e-discovery tools, *etc.*
    - insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, *etc.*
    - self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, *etc.*)
    - infection via removable drives (worm or virus)
    - delivered by other malware or attacker tool: expand investigation to include additional attacker tools or malware

# Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

## Contain

`TODO: Customize containment steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

**In ransomware situations, containment is critical. Inform containment measures with facts from the investigation. Prioritize quarantines and other containment measures higher than during a typical response.**

Quarantines (logical, physical, or both) prevent spread *from* infected systems and prevent spread *to* critical systems and data. Quarantines should be comprehensive: include cloud/SaaS access, single-sign-on, system access such as to ERP or other business tools, *etc.*

- Quarantine infected systems
- Quarantine affected users and groups.
- Quarantine file shares (not just known-infected shares; protect uninfected shares too)
- Quarantine shared databases (not just known-infected servers; protect uninfected databases too)
- Quarantine backups, if not already secured
- Block command and control domains and addresses
- Remove vector emails from inboxes
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs

`TODO: Consider automating containment measures using orchestration tools.`

## Eradicate

`TODO: Customize eradication steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

- Rebuild infected systems from known-good media
- Restore from known-clean backups
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs
- **Watch for re-infection:** consider increased priority for alarms/alerts related to this incident.

## Reference: Remediation Resources

`TODO: Specify financial, personnel, and logistical resources to accomplish remediation.`

# Communicate

`TODO: Customize communication steps for ransomware`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure

3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?"), which can be more intrusive/disruptive during ransomware incidents
    3. Communicate requirements: "what should users do and not do?" See "Reference: User Actions for Suspected Ransomware," below
5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider ransomware a data breach or otherwise requires notifications (*e.g.*, HHS/HIPAA (https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf))) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Communicate with regulators, including a discussion of what resources they can make available (not just boilerplate notification: many can actively assist)
8. Consider notifying and involving law enforcement (https://www.nomoreransom.org/en/report-a-crime.html)
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
9. Communicate with security and IT vendors
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

# Recover

`TODO: Customize recovery steps for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

> ***We do not recommend paying the ransom:*** *it does not guarantee a solution to the problem. It can go wrong (e.g., bugs could make data unrecoverable even with the key). Also, paying proves ransomware works and could increase attacks against you or other groups.*[2, paraphrased]

1. Launch business continuity/disaster recovery plan(s): *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Recover data from known-clean backups to known-clean, patched, monitored systems (post-eradication), in accordance with our well-tested backup strategy.

- Check backups for indicators of compromise
- Consider partial recovery and backup integrity testing

3. Find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page (https://www.nomoreransom.org/en/decryption-tools.html).
4. Consider paying the ransom for irrecoverable critical assets/data, in accordance with policy `TODO: Expand and socialize this decision matrix`
    - Consider ramifications with appropriate stakeholders
    - Understand finance implications and budget
    - Understand legal, regulatory, and insurance implications
    - Understand mechanisms (*e.g.*, technologies, platforms, intermediate vendors/go-betweens)

# Resources

## Reference: User Actions for Suspected Ransomware

`TODO: Customize steps for users dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Disconnect your system from the network `TODO: include detailed steps with screenshots, a pre-installed tool or script to make this easy ("break in case of emergency"), consider hardware network cut-off switches`
3. Take pictures of your screen using your smartphone showing the things you noticed: ransom messages, encrypted files, system error messages, *etc.*
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. Where were you when it happened, and on what network? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are you using? (operating system, hostname, *etc.*)
    7. What account were you using?
    8. What data do you typically access?
    9. Who else have you contacted about this incident, and what did you tell them?
5. Contact the help desk and be as helpful as possible
6. Be patient: the response may be disruptive, but you are protecting your team and the organization! **Thank you.**

## Reference: Help Desk Actions for Suspected Ransomware

`TODO: Customize steps for help desk personnel dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure `TODO: Customize template with key questions (see below) and follow-on workflow`

3. Ask the user to take pictures of their screen using their smartphone showing the things they noticed: ransom messages, encrypted files, system error messages, *etc.* If this is something you noticed directly, do the same yourself.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. What networks are involved? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are involved? (operating system, hostname, *etc.*)
    7. What data is involved? (paths, file types, file shares, databases, software, *etc.*)
    8. What users and accounts are involved? (active directory, SaaS, SSO, service accounts, *etc.*)
    9. What data do the involved users typically access?
    10. Who else have you contacted about this incident, and what did you tell them?
5. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
6. Get detailed contact information from the user (home, office, mobile), if applicable
7. Record all information in the ticket, including hand-written and voice notes
8. Quarantine affected users and systems `TODO: Customize containment steps, automate as much as possible`
9. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery

## Additional Information

1. "Ransomware Identification for the Judicious Analyst" (https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst), Hahn (12 Jun 2019)
2. No More Ransom! (https://www.nomoreransom.org) Project, including their Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php?lang=en) service and their Q&A (https://www.nomoreransom.org/en/ransomware-qa.html)
3. ID Ransomware (https://id-ransomware.malwarehunterteam.com/) service
4. MITRE ATT&CK Matrix (https://attack.mitre.org), including the Initial Access (https://attack.mitre.org/tactics/TA0001/) and Impact (https://attack.mitre.org/tactics/TA0040/) tactics