# Policy Document
# Prepared for Canadian Tire Corporation Malware Incident Response Plan/Playbook

**Prepared by: Victor Onukwu**

**Purpose: Lighthouse Labs Project**

**Date: October 27, 2023**

# Table of Content

# 1. Documentation Policy:

Assumption: All incident-related documentation is stored securely and backed up.

Policy: Effective documentation is critical for both incident management and regulatory compliance. This policy outlines the specific details related to documentation, storage, and retention of information associated with a malware incident.

1.1. Incident Documentation:
Incident Details: All relevant incident details must be documented, including the date and time of detection, incident classification, affected systems, initial analysis, and the nature of the malware involved.

Actions Taken: Document every action taken during the incident response process, from isolation and containment to eradication and recovery. This includes any system changes, patching, malware removal, and communications.

Communication Records: Keep records of all internal and external communications related to the incident, including emails, phone calls, and meeting notes.

Forensic Analysis: Documentation of forensic analysis, including findings, evidence collected, and methods used, is crucial for legal and regulatory purposes.

1.2. Storage and Retention:
Secure Storage: Ensure that all incident-related documentation is stored securely on encrypted, password-protected, and access-controlled systems. Access to this information should be restricted to authorized incident response team members and legal personnel.

Redundant Backups: Maintain redundant backups of all incident-related documentation. Backup copies should be stored off-site or on cloud-based platforms to prevent data loss in case of physical system compromise.

Document Classification: Categorize documents as per their sensitivity. Ensure that any highly confidential information is further protected and restricted to only necessary personnel.

Retention Period: Incident-related documentation should be retained for a minimum of seven years, as per legal requirements. After this period,

documents should be securely destroyed, ensuring that no sensitive data remains.

1.3. Record Integrity and Authenticity:
Timestamps: Ensure that all documents and records are timestamped to track when they were created, modified, or accessed.

Chain of Custody: Maintain a documented chain of custody for any physical evidence collected during the incident response, as this may be crucial in legal proceedings.

1.4. Access Control:
Access Authorization: Only authorized personnel, such as incident response team members, legal counsel, and management, should have access to incident-related documentation.

Access Logs: Maintain access logs to track who accessed incident documentation, when, and for what purpose. Regularly review access logs for any unauthorized or suspicious access.

1.5. Legal Considerations:
Legal Privilege: Understand that some incident documentation may be covered by attorney-client privilege. Ensure that legal counsel is involved in defining what documentation falls under this privilege.

Regulatory Compliance: Ensure that all incident documentation is retained in accordance with applicable data protection and privacy laws and regulatory requirements, such as PIPEDA.

# 2. Initial Response Policy:

Assumption: Unusual network behaviour or system anomalies have been detected, indicating a potential malware incident.

Policy: The Initial Response phase is critical to contain and manage a malware incident effectively. This phase sets the tone for the entire incident response process, and a swift and well-coordinated response is essential.

2.1 Isolation of Affected Systems:
Objective: To prevent the malware from spreading further and causing additional damage.

Responsibilities: The Incident Response Team (IRT) will take immediate action to isolate affected systems.
Procedure:

- Identify and document the affected systems.
- Disconnect affected systems from the network to limit their communication with other devices.
- Disable all affected user accounts to prevent unauthorized access.
- Ensure that isolated systems are powered down, if necessary, to prevent malware persistence.

Timeline: All affected systems should be isolated within one hour of detection.

Documentation: Maintain detailed records of the systems that were isolated and actions taken.

2.2 Notification of the Incident Response Team:
Objective: To ensure that the IRT is alerted promptly and can initiate the response process.

Responsibilities: Any team member or employee who detects unusual behavior or suspects a malware incident should immediately notify the IRT.
Procedure:

- Establish a designated incident notification channel (e.g., a hotline or dedicated email address) for reporting potential incidents.
- Ensure that all team members are aware of the notification process and are reachable.
- If the incident is reported outside of regular working hours, an on-call member of the IRT should be promptly alerted.

Timeline: Notification of the IRT should occur within 15 minutes of detecting the incident.

Documentation: Maintain a log of incident notifications, including the time and source of the report.

2.3 Initial Triage:
Objective: To conduct a preliminary assessment of the incident to determine its severity and potential impact.

Responsibilities: A designated IRT member, often the incident lead, should conduct the initial triage.
Procedure:

- Assess the information provided in the incident report to understand the nature of the incident.
- Consider whether it is a confirmed or suspected malware incident.

- Determine the potential impact on critical systems and data.

Timeline: The initial triage should be completed within 30 minutes of the incident report.

Documentation: Maintain records of the initial assessment, including the classification of the incident.

2.4 Escalation and Coordination:
Objective: To ensure that the incident response process is coordinated effectively and escalated as necessary.

Responsibilities: The incident lead will coordinate and escalate the response efforts.
Procedure:

- If the incident is confirmed as a malware incident, escalate it to the relevant members of the IRT.
- Notify executive management, including the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- If the incident's severity is beyond the capacity of the internal team, initiate external incident response support (e.g., third-party security consultants).

Timeline: Escalation should occur promptly, ensuring all relevant parties are informed within 60 minutes of the incident's confirmation.

Documentation: Maintain records of all escalations and notifications, specifying the parties involved and the time of notification.

# 3. Containment Policy:

Assumption: The organization uses network segmentation to isolate affected systems.

Policy: Implementing Effective Containment

The containment phase is a crucial step to prevent the spread of malware and limit the damage it can cause. It is essential to isolate affected systems, disable compromised accounts, and block command and control (C2) traffic promptly. Here are the specific policies and procedures to be followed during the containment phase:

3.1 Extent Assessment:

Assumption: The incident response team (IRT) has identified the malware infection and its impact.

Policy: IRT will assess the extent of the malware infection to determine the number of affected systems, the pathways of infection, and the type of malware involved. This assessment will guide the scope of the containment efforts and remediation activities.

Procedure:

- IRT will initiate a comprehensive system scan to identify all affected endpoints and servers.
- IRT will document the findings, including the number of infected systems and the malware types detected.

3.2 Isolation:
Assumption: The organization uses network segmentation to isolate affected systems.

Policy: IRT will isolate affected systems to prevent the malware from spreading further within the organization's network. This will minimize the potential damage caused by the malware and provide a controlled environment for eradication efforts.

Procedure:

- IRT will work with the network security team to isolate infected systems from the rest of the network. This may involve configuring firewalls, isolating VLANs, or implementing network access controls.
- IRT will ensure that the isolated systems are unable to communicate with other network segments or the internet to prevent further infection.
- IRT will create documentation detailing the isolation process, including dates, times, and affected systems.

3.3 Account Disablement:
Assumption: Compromised user accounts have been identified.

Policy: IRT will disable affected user accounts to prevent unauthorized access and further damage. This will include disabling accounts that may have been used to facilitate the malware infection or propagation.

Procedure:

- IRT will work closely with the IT department to disable compromised user accounts based on the findings of the incident assessment.

- IRT will communicate with affected users to inform them of the account disablement and provide instructions on the remediation process.
- IRT will document the list of disabled user accounts and maintain a record of the actions taken.

3.4 Firewall Rules:
Assumption: The organization has configured firewalls to block C2 traffic.

Policy: IRT will implement firewall rules to block command and control (C2) traffic originating from infected systems. This will disrupt the malware's ability to communicate with external malicious servers and limit its ability to exfiltrate data or receive commands.

Procedure:

- IRT, in collaboration with the network security team, will create specific firewall rules to block outgoing and incoming C2 traffic.
- IRT will continuously monitor the firewall logs to ensure the effectiveness of the rules and to identify any attempts to bypass them.
- IRT will maintain a record of the firewall rules and regularly review and update them as needed.

# 4. Eradication Policy:

Assumption: Frequent system backups are maintained and easily accessible.

Policy:

4.1. Backup Strategy:
Maintain a robust backup strategy that encompasses critical systems, databases, and data. This strategy should include frequent incremental backups and regular full backups to ensure the availability of clean data.

4.2. Backup Access:
Ensure that backups are securely stored, both on-site and off-site. Access to backup data should be restricted and require multi-factor authentication for restoration purposes.

4.3. Restoration Priority:
In the event of a malware incident, prioritize the restoration of critical systems and data. The restoration process should be initiated immediately upon malware removal.

4.4. Verification and Testing:
Prior to restoration, perform verification and testing of backup data to ensure its integrity and that it is free from malware. This includes confirming that backups are free from vulnerabilities and that the malware has not infected backup copies.

4.5. Malware Removal:
The removal of malware should be performed systematically on each affected system. Ensure that all instances of the malware are identified and removed, and that any persistence mechanisms are neutralized.

4.6. Patch Management:
Identify and address the vulnerabilities that allowed the malware to infiltrate the network. Update systems with security patches and ensure all software and applications are up-to-date to prevent future infections.

4.7. System Integrity Checks:
Conduct thorough system integrity checks on all affected systems to verify that malware remnants have been eradicated. These checks should include validating system files, registries, and key system components.

4.8. Documentation:
Maintain detailed records of all actions taken during the eradication process. This includes documenting the malware removal process, system restoration, vulnerability patching, and the results of system integrity checks.

4.9. User Awareness:
Inform users and administrators of the changes made during the eradication process and advise them on best practices to avoid malware infection in the future.

4.10. Continuous Monitoring:
Implement continuous monitoring to ensure that malware does not reappear on the network or that any persistent malware is detected promptly.

4.11. Regular Updates:
Regularly update and refine the eradication procedures based on lessons learned from each incident. Ensure that the process is streamlined and efficient for future incidents.

# 5. Recovery Policy:

Assumption: Vulnerability assessments are conducted monthly, and a variety of systems are in place to ensure data recovery.

Policy: In the event of a malware incident, the Recovery phase is a critical step to restore impacted systems and resume normal operations while ensuring the highest level of security. This policy outlines the steps, processes, and guidelines to facilitate a swift and secure recovery process.

Policy Details:

1. System Restoration:
Backup Management: Ensure that regular backups of critical systems and data are maintained and accessible. Backup processes should be consistent, reliable, and include both on-site and off-site storage.
Restoration Plan: Develop a restoration plan that clearly outlines the sequence in which systems will be restored. Prioritize critical systems, and create a timeline for restoration, which should be based on the criticality of the system.

2. Reconfiguration:
System Hardening: Before systems are restored, ensure that they undergo a hardening process to eliminate vulnerabilities that may have been exploited by the malware. This includes applying security patches, disabling unnecessary services, and implementing security best practices.
Network Reconfiguration: Review and reconfigure the network to prevent re-infection. Implement stricter firewall rules and access controls, as well as traffic monitoring for anomalies.

3. Vulnerability Assessments:
Post-Incident Assessment: Conduct a comprehensive vulnerability assessment post-incident to identify any potential weaknesses that could have led to the malware infection.
Security Patch Management: Ensure that all security patches are promptly applied to mitigate known vulnerabilities.

4. Monitoring:
Continuous Monitoring: Continuously monitor restored systems for any signs of re-infection or unusual behaviour. Implement intrusion detection systems and log analysis tools to promptly detect any threats.
Event Logging: Enable and maintain detailed event logging on all systems to facilitate rapid incident detection and investigation in the future.

5. Recovery Timeframe:

Time-Frame Definition: Establish specific recovery timeframes for different systems based on their criticality. For critical systems, aim for a minimal recovery time, while less critical systems can have a longer recovery window.
Benchmarking and Improvement: Continually benchmark and assess recovery timeframes to improve efficiency in future incidents.

6. Communication:
Status Updates: Provide regular status updates to the Incident Response Team (IRT) and executive management regarding the recovery progress. Clear communication is crucial to maintain confidence in the recovery process.
Completion Notification: Notify all stakeholders, including relevant regulatory bodies, once the recovery process is complete and normal operations are fully restored.

7. Lessons Learned:
Post-Incident Review: Conduct a post-incident review to identify areas of improvement in the recovery process. Lessons learned from the recovery phase should be integrated into future recovery plans and training programs.

8. Documentation:
Recovery Documentation: Maintain comprehensive records of the recovery process, including timelines, actions taken, and any issues encountered. Documentation should be securely stored and easily accessible.

9. Follow-Up Actions:
Regular Security Assessments: Ensure that regular security assessments, including vulnerability scans and penetration tests, are conducted every six months. Address any vulnerabilities discovered in a timely manner.
Recovery Process Enhancements: Continually evaluate and enhance the recovery process based on lessons learned and technological advancements.

# 6. Communication Policy:

Assumption: The Public Relations (PR) team is readily available for crisis communication.

Policy:
The communication policy for a malware incident is a critical aspect of incident response. Effective and timely communication is essential for managing the incident, mitigating potential damage, and maintaining the trust of stakeholders.

1. Internal Communication:

Internal Notification: Once a malware incident is confirmed, the Incident Response Team (IRT) should immediately notify all relevant internal stakeholders. This includes the IRT members, IT teams, legal, HR, and senior management.
Regular Updates: Regular updates regarding the incident's status, progress, and any actions taken should be shared with all internal stakeholders, including executives, to ensure everyone is informed and aligned.

2. External Communication:
Stakeholder Notification: As soon as it is determined that the malware incident has the potential to impact external stakeholders, including customers and regulatory bodies, external communication should be initiated.
Initial Communication (Within 4 Hours): The PR team should draft an initial communication within four hours of confirming the incident. This communication should acknowledge the incident, reassure stakeholders that it is being addressed, and provide a general outline of the steps being taken to resolve it.
Detailed External Communication Plan (Within 24 Hours): Within 24 hours, a comprehensive external communication plan should be prepared. This plan should outline the specific messaging for affected parties, a timeline for communication, and designate the responsible individuals for each communication task.

3. Coordination with PR:
PR Team Activation: The PR team should be activated as soon as the malware incident is confirmed, and they should remain on standby 24/7 for the duration of the incident.
Message Consistency: The PR team will work in coordination with the IRT and senior management to ensure that all messages are consistent, accurate, and aligned with the incident response strategy.

4. Communication Channels:
Diverse Channels: Communication should utilize diverse channels, including press releases, emails, website updates, and social media platforms, to ensure that stakeholders receive information through their preferred channels.
Clear and Accessible Information: All communication should be clear, concise, and easily accessible. The website should include a dedicated section with updates on the incident and mitigation efforts.
Customer Support Center: The customer support center should be staffed and well-prepared to handle inquiries and concerns from affected customers.

5. Regulatory Reporting:
Legal Compliance: Ensure compliance with all legal requirements regarding incident reporting. In case of legal or regulatory obligations, reports should be prepared and submitted within the required timeframes.

Data Protection Laws: In cases involving the compromise of customer data, full compliance with data protection laws (e.g., PIPEDA) should be ensured, and reports should be submitted to regulatory authorities and affected customers as mandated by law.

6. Post-Incident Communication:
Incident Summary: Once the malware incident is fully resolved, provide an incident summary to all stakeholders. This should include a detailed account of what occurred, the steps taken to address it, and measures implemented to prevent future incidents.
Lessons Learned: Include insights gained from the incident and how the organization plans to enhance security and incident response procedures moving forward.