# Incident Response Playbook
# Canadian Tire Corporation
# Malware Attack

**Created by Victor Onukwu**
**For Lighthouse Labs & Canadian Tire Corporation**
**October 27, 2023**

# Table Of Content

# Introduction

The Incident Response Playbook for Canadian Tire Corporation is presented as a vital tool for dealing with the constantly evolving landscape of malware incidents. The playbook aims to provide a structured and coordinated approach to help the organization respond effectively to malware threats. It focuses on three main objectives: prompt and efficient incident response, compliance and transparency, and continuous improvement through learning.

The document emphasizes the importance of minimizing potential damage and restoring normal operations quickly by reducing the time between identifying malware incidents and mitigating their impact. It also highlights the significance of complying with regulatory standards and maintaining transparent communication with stakeholders, considering the company's publicly traded status. Additionally, the playbook prioritizes learning and adaptation by including a post-incident review process to gain valuable insights from each incident and enhance the organization's cybersecurity defenses.

In the following pages, the playbook outlines a step-by-step workflow that involves a diverse incident response team, including cybersecurity experts, IT professionals, legal and compliance representatives, and communication specialists. This collaborative approach ensures that all stakeholders work together effectively to address and mitigate malware threats. The document emphasizes the company's commitment to remaining vigilant in the face of an ever-changing cybersecurity landscape and evolving the playbook to meet new challenges and threats as they arise.

# Overview

This playbook provides a comprehensive strategy and workflow for responding to malware incidents within the Canadian Tire Corporation. Its goal is to facilitate a coordinated and effective response to minimize damage, disruptions, and reputational harm while complying with legal standards. The key objectives include swift incident identification, isolation and containment of affected systems, mitigation and recovery efforts, transparent communication with stakeholders, investigation and attribution of malware, compliance with legal requirements, and continuous improvement of cybersecurity policies and procedures. The playbook follows a structured workflow with different stages, such as initial incident identification, technical analysis, stakeholder involvement, and post-incident review. Each phase outlines the responsibilities of relevant teams and stakeholders, including IT and Security, Legal, Compliance, CISO, and Communications. Finally, the playbook emphasizes the importance of conducting

a post-incident review to learn from the incident and improve cybersecurity measures and legal compliance.

# Scope

The scope of the Malware Incident Response Playbook and Workflow for Canadian Tire Corporation outlines the objectives and essential elements of this extensive plan for responding to malware incidents. The main goals include implementing a structured approach to handle malware incidents, minimizing their impact on the organization's operations and reputation, establishing clear responsibilities and procedures, ensuring compliance with legal and regulatory requirements, and continuously improving through post-incident reviews. It encompasses various types of malware incidents, such as ransomware, trojans, and spyware, across all Canadian Tire Corporation locations. The playbook covers the legal and regulatory framework, emphasizes transparent communication, the importance of employee training, documentation, and regular testing. It also highlights the significance of confidentiality and compliance, with defined responsibilities for key stakeholders at each phase of incident response.
Furthermore, the scope acknowledges the potential for collaborating with external entities like law enforcement and regulatory authorities and allows for customization to address specific incident characteristics and emerging threats. Appendices may include reference materials and contact information. Overall, this scope establishes the groundwork for a comprehensive and adaptable response plan, ensuring that Canadian Tire Corporation is well-prepared to effectively manage malware incidents while adhering to legal and regulatory standards.

# Roles and Responsibilities

**CSIRT Structure**
The CSIRT is structured as follows:

CSIRT Director: John Baker!
Incident Handlers: Charles Taylor!
Forensic Analysts: Thomas Cook!
Communication and PR Specialists: Susan O’Brien*
Legal and Regulatory Compliance Experts: Maxwell O’niel
IT and Security Teams: Rex Lee*

**CSIRT Leadership**
CSIRT Director:

Overall leadership and coordination of the CSIRT.
Incident prioritization and resource allocation.
Liaison with executive management, legal counsel, and external stakeholders.

**Incident Handlers**
Incident Handlers:
Initial detection, classification, and containment of security incidents.
Isolation of affected systems.
Notification of relevant stakeholders:
Engage internal stakeholders (CIO, CISO, legal, HR, PR).
Communicate with external stakeholders (regulatory bodies, affected customers).

**Coordination with Forensic Analysts for in-depth analysis.**

**Forensic Analysts**
Forensic Analysts:
In-depth analysis of security incidents to understand their origin and behavior.
Preservation and analysis of digital evidence.
Collaboration with legal and regulatory compliance experts for evidence handling.

**Communication and PR Specialists**
Communication and PR Specialists:
Internal and external communication during and after security incidents.
Messaging to employees, customers, regulatory bodies, and the public.
Media management and reputation preservation.

**Legal and Regulatory Compliance Experts**
Legal and Regulatory Compliance Experts:
Ensuring compliance with applicable laws and regulations (e.g., PIPEDA).
Collaboration with law enforcement, if required.
Legal counsel on data breach notification requirements.

**IT and Security Teams**
IT and Security Teams:
Collaboration with CSIRT in incident containment, eradication, and recovery efforts.
Implementation of security measures and patches to prevent re-infection.
Vulnerability assessments and system integrity checks.

# Playbook Steps

## Preparation Phase

**Preparation and Planning:**
Effective preparation and planning are fundamental for a swift and organized response to a malware incident. This phase ensures that all relevant stakeholders understand their roles, the procedures to be followed, and the resources available. Below is a detailed preparation and planning step for the malware incident response playbook:

**Establish an Incident Response Team (IRT):**
Designate an IRT comprising individuals with expertise in cybersecurity, forensics, legal, communications, and executive leadership.
Assign specific roles and responsibilities to team members.
Ensure the team is aware of its responsibilities and maintains updated contact information.

**Develop an Incident Response Plan:**
Create a comprehensive incident response plan tailored to the organization's specific needs, focusing on malware incidents.
Document procedures for identifying, classifying, containing, eradicating, and recovering from malware incidents.
Specify communication protocols, legal and regulatory requirements, and stakeholder engagement procedures.

**Inventory Critical Assets:**
Identify and maintain an up-to-date inventory of critical systems, applications, and data.
Prioritize assets based on their criticality to the organization's operations.
Establish backup and recovery procedures for critical assets.

**Network and System Monitoring:**
Implement continuous network and system monitoring tools to detect unusual activity or anomalies.
Configure alerts and triggers to identify potential malware-related behaviour.
Ensure that logs are collected and retained for analysis.

**Security Awareness and Training:**
Conduct regular cybersecurity awareness and training programs for employees at all levels.

Train employees on recognizing phishing attempts and suspicious links, the most common malware entry points.
Promote a culture of vigilance and immediate reporting of security concerns.

Legal and Regulatory Compliance:
Appoint legal counsel well-versed in data protection laws and incident response.
Ensure understanding of the legal obligations related to data breaches, including breach notification requirements under applicable laws (e.g., PIPEDA in Canada).
Establish a framework for engaging with law enforcement agencies in the event of cybercrimes.

Vendor and Supply Chain Security:
Assess the cybersecurity practices of third-party vendors and supply chain partners.
Implement contractual agreements that outline security requirements and incident response expectations from vendors.
Collaborate with key vendors for information sharing and security improvements.

**Backup and Recovery Strategy:**
Develop a robust backup and recovery strategy that includes regular data backups.
Ensure backups are isolated from the primary network to prevent malware infections from affecting them.
Test the restoration process to verify the integrity of backups.

**Communication and Notification Plans:**
Establish clear communication channels for internal and external stakeholders, including employees, customers, shareholders, and regulatory authorities.
Create templates for incident notifications and messages to maintain consistency and clarity during communication.
Designate a spokesperson or communications lead responsible for external messaging.

**Incident Simulation and Testing:**
Conduct regular tabletop exercises and incident simulations to ensure the effectiveness of the incident response plan.
Evaluate the coordination and response of the IRT and the organization as a whole.
Identify areas for improvement and update the plan accordingly.

**Resources and Budget Allocation:**
Allocate necessary resources and budget to support incident response activities, including Cybersecurity tools, personnel, and legal support.
Ensure that the IRT has access to the required resources for a swift and effective response.

**Documentation and Record-Keeping:**
Develop a system for documenting incident details, actions taken, and outcomes. Maintain a central repository for incident-related records, logs, and reports. Ensure that all records are retained in accordance with legal and regulatory requirements.

By meticulously preparing and planning for malware incident response, Canadian Tire Corporation can enhance its readiness to mitigate and recover from such incidents, safeguard critical assets, and minimize the impact on its operations, reputation, and stakeholders. This phase serves as the foundation for a well-coordinated response to future malware incidents.

## Detection Phase

**Incident Identification and Classification**
**Early Warning Systems:**

- Continuous Monitoring: Implement robust monitoring systems to track network and system activities in real-time.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) should be actively scanning for suspicious behaviour.
- Endpoint Detection and Response (EDR) tools should be deployed to identify unusual activities on individual devices.
- Network traffic should be continuously analyzed for signs of malware communication.

**Anomaly Detection:**

- Establish a baseline of normal network and system behaviour to detect deviations.
- Define critical thresholds for system resource utilization, network traffic, and user activities.
- Use Security Information and Event Management (SIEM) tools to analyze logs for unusual patterns.
- Regularly monitoring for Indication of Compromises (IoCs) and responding swiftly when detected. Examples are;

  ☐ Unusual Network Traffic Patterns:
  Frequent connections to suspicious IP addresses or domains.
  Abnormal network traffic volume, such as spikes in outbound data.

  ☐ Malicious File Signatures:
  Detection of known malware file signatures in system logs or antivirus scans.

  ☐ Unexplained System Behaviour:

Frequent system crashes or slowdowns without an obvious cause.
Unauthorized changes in system configurations.

☐ New or Unrecognized Files:
Discovery of unknown files or executables in critical system directories.

☐ Anomalous User Account Activity:
Multiple failed login attempts.
Unusual account privileges changes or escalations.

☐ Suspicious Registry Changes:
Unauthorized modifications to the Windows Registry.
Changes to autostart entries, which may indicate malware persistence.

☐ Unauthorized Access or Login Activity:
Logs showing logins from unusual or unauthorized IP addresses or locations.

☐ Email and Web-Based IoCs:
Suspicious email attachments or links.
Clicking on malicious URLs or downloading files from untrusted sources.

☐ Endpoint IoCs:
Unexpected system and application crashes.
Changes in system memory or CPU usage.

☐ Phishing Attempts:
Receipt of phishing emails by employees, possibly containing malicious links or attachments.
Reports of suspicious or unsolicited communication.

**User and Employee Reporting**:
Promote a culture of security awareness among employees.
Encourage users to report any unusual system behaviour, phishing attempts, or suspicious emails.
Implement a user-friendly reporting mechanism for employees to alert the IT and Security teams.

**Incident Triage:**
Designate a Computer Security Incident Response Team (CSIRT) or an Incident Response Team (IRT) responsible for triaging potential incidents.
When an incident is reported or detected, assess its severity and scope. Is it a possible malware incident or a false positive?
Prioritize incidents based on impact and urgency.

**Malware Identification and Classification:**
If the incident is determined to be potentially malware-related, the IRT should conduct a preliminary analysis.
Collect and analyze relevant data, including system logs, network traffic, and any suspicious files.
Utilize antivirus and threat intelligence databases to identify known malware strains.
Classify the malware based on its characteristics, behaviour, and threat level (e.g., ransomware, trojan, spyware).
Collaborate with threat intelligence sources and vendors to gather information on emerging threats.

**Documentation:**
Maintain detailed records of the incident identification and classification process.
Document the incident's initial description, date and time of detection, severity, and the classification of the malware.
Ensure that all findings are documented and accessible for the incident response team.

**Stakeholder Notification:**
If a potential malware incident is confirmed, notify the relevant stakeholders.
This may include the CIO, CISO, IT team, and executive management.
Legal counsel should be engaged for potential regulatory requirements.

**Escalation:**
If a significant malware incident is confirmed, escalate the issue to the senior management team and involve external incident response experts if necessary.
Activate pre-defined communication channels and incident response plans

## Analyze Phase

**Malware Analysis:**
Malware Sandbox: If the nature of the malware is uncertain, employ a malware sandbox environment to safely analyze its behaviour without exposing the organization's systems to risk.

Behavioural Analysis: Investigate the malware's behaviour, including its communication with external servers, file modifications, and persistence mechanisms.

Infection Source: Identify the likely entry point of the malware, such as a malicious email attachment, compromised website, or vulnerable application.

**Notification and Escalation:**
Incident Response Team: Ensure immediate communication with the IRT, which should consist of the CIO, CISO, and other relevant security personnel. The team should meet to discuss the incident.

Stakeholder Notification: Depending on the classification and initial assessment, determine which stakeholders need to be informed. In the case of a confirmed malware incident, this may include executive management, legal counsel, and relevant departments.

**Evidence Preservation:**
Preserve Evidence: As the incident is investigated, make sure to preserve evidence that may be required for legal or regulatory purposes. This includes logs, network traffic data, and malware samples.
Chain of Custody: Maintain a clear chain of custody for all collected evidence to ensure its integrity and admissibility.

**Documentation:**
Incident Report: Start documenting the details of the incident, including the initial detection, alerts, actions taken, and findings from malware analysis.
Case Number: Assign a unique case number to the incident for reference.

**Post-Initial Assessment Actions:**
Communicate Findings: Brief executive management on the initial findings and potential impact of the malware incident. Discuss the immediate steps required for containment and mitigation.
Continuation: Depending on the initial assessment, the incident may move on to the containment phase or further analysis by the forensics team.

## Containment Phase

**Isolate Affected Systems:**
The Incident Response Team (IRT) in coordination with IT and Security teams should promptly identify all systems and devices infected by malware.
Affected systems should be immediately isolated from the network. This can be achieved through the use of firewall rules, network segmentation, or physically disconnecting the compromised devices.

**Disable Affected User Accounts:**

It's essential to disable or lock user accounts that are compromised or associated with infected systems. This helps prevent the malware from accessing shared resources and spreading via user credentials.
User accounts should only be re-enabled once systems are verified as clean and secure.

**Block Command and Control (C2) Communication:**
Identify the communication channels and domains used by the malware to establish connections with command and control servers.
Utilize firewall rules, DNS sinkholes, or intrusion detection/prevention systems to block outbound and inbound traffic to known C2 servers.
Continuously monitor and update the list of C2 servers as more information becomes available during the incident.

**Deploy Network and Host-Based Security Controls:**
Enhance security controls such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and endpoint detection and response (EDR) solutions to detect and prevent the malware from propagating.
Implement email and web filtering to block malicious email attachments and links that may deliver malware.

**Monitor Network Traffic:**
Continuously monitor network traffic to identify any unusual or suspicious patterns that may indicate further infections or lateral movement.
Analyze network logs, IDS/IPS alerts, and firewall logs to gain insights into the malware's behavior.

**Establish a Containment Team:**
Appoint a specific team or personnel responsible for overseeing the containment efforts.
The containment team should work closely with the IRT, IT, and security teams to ensure effective implementation.

**Document Containment Actions:**
Maintain detailed records of all containment actions, including isolation of systems, disabling user accounts, and any network or security control changes made.
This documentation is crucial for analysis, reporting, and post-incident review.

**Communication and Coordination:**
The IRT should maintain clear and open communication with all stakeholders, informing them of the containment measures being taken.
Collaborate with the Legal and Public Relations teams to ensure compliance with legal requirements and to manage external communication.

**Regularly Assess the Efficacy of Containment:**
Continuously monitor the effectiveness of containment measures to ensure that the malware is not spreading further or regenerating.
Modify or strengthen containment measures as necessary based on the evoving threat landscape.

## Eradication Phase

**Malware Identification and Analysis:**
Malware Identification:
Identify the specific malware variant, including its name, characteristics, and potential payload.
Ascertain if it is a known malware with available removal tools or if it's a new, custom malware that requires specific actions.

Malware Behavior Analysis:
Analyze the malware's behaviour to understand its impact on infected systems.
Determine if it possesses self-propagation capabilities or if it communicates with external servers (C2 servers).

**Malware Persistence Mechanisms:**
Identify how the malware maintains persistence on infected systems, such as registry entries, startup services, or scheduled tasks.
Develop a plan to remove these persistence mechanisms.

**Infected System Isolation:**
Network Isolation:
Disconnect infected systems from the network to prevent further malware spread.
Block outgoing communication to known malicious IP addresses or domains related to the malware.

**User Account Isolation:**
Disable or isolate user accounts associated with infected systems.
Reset passwords for affected accounts to prevent unauthorized access.

**Malware Removal:**
Anti-Malware Tools:

Use reputable anti-malware software to scan and remove the malware.
Ensure that the anti-malware definitions are up to date.

Manual Removal:
If the malware is highly customized or evades automated tools, perform manual removal.
Follow best practices to avoid collateral damage while deleting infected files or registry entries.

System Rollback:
Restore affected systems from clean backups taken before the malware infection.
Ensure that backup data is free from malware contamination.

Patch and Update:
Identify and patch vulnerabilities that the malware exploited to prevent re-infection.
Ensure all systems have the latest security updates and patches applied.

**Verification and Testing:**
Verification of Eradication:
Conduct follow-up scans with anti-malware tools to confirm that the malware is no longer present.
Verify the absence of persistence mechanisms and traces in the system.

Functionality Testing:
Verify that the systems are operational after malware removal.
Test critical applications to ensure they are functioning as expected.

**Preventive Measures:**
Security Policy Review:
Review and update security policies and procedures to prevent future malware incidents.
Consider implementing application whitelisting, restricting user privileges, and enhancing employee training.

**User Awareness Training:**
Conduct security awareness training for employees to recognize and avoid malware.
Educate users on safe browsing habits and email best practices.

**Vulnerability Management:**

Implement a robust vulnerability management program to identify and remediate vulnerabilities promptly.
Regularly scan systems for potential weaknesses and apply patches as needed.

**Documentation and Reporting:**
Documentation:
Document the entire eradication process, including actions taken, tools used, and outcomes.
Maintain a record of systems and accounts affected.

Incident Report:
Create an incident report summarizing the malware, eradication process, and lessons learned.
This report will serve as a reference for future incidents and potential legal or regulatory requirements.

**Post-Eradication Monitoring:**
Continuous Monitoring:
Continuously monitor the systems to detect any signs of re-infection or persistence.
Implement real-time intrusion detection and monitoring tools.

**Incident Recovery Assessment:**
Assess the effectiveness of the eradication process in the weeks following the incident.
Adjust security measures as needed to prevent future incidents.

**Feedback and Improvement:**
Lessons Learned:
Conduct a post-incident review with the Incident Response Team to identify lessons learned and areas for improvement.
Update the incident response playbook and workflows based on these findings.

## Recovery Phase

**Document Impact Assessment:**
Conduct a detailed assessment to determine the scope of the malware's impact, identifying affected systems, data, and any potential data breaches.
Collaborate with the Forensics and IT teams to ensure an accurate assessment.

**Restore Systems from Clean Backups:**
Identify unaffected and clean backups for all impacted systems.
Prioritize the restoration of critical systems that support business operations.

Ensure that backups are secure and free from malware.

**Reconfigure Systems to Prevent Reinfection:**
Assess and address vulnerabilities that allowed malware entry (e.g., unpatched software).
Implement necessary security updates and patches.
Review and strengthen security policies and configurations.
Implement a host-based intrusion detection system (HIDS) to monitor system integrity.

**Conduct Vulnerability Assessments:**
Perform thorough vulnerability assessments across the network to identify weaknesses.
Prioritize vulnerabilities based on potential impact and exploitability.
Establish a remediation plan for addressing identified vulnerabilities.

**Continuously Monitor Systems:**
Implement continuous system monitoring and intrusion detection.
Set up alerts for suspicious activity and potential re-infections.
Ensure that security tools are regularly updated and functioning properly.

**Post-Incident Verification:**
Confirm that all malware has been successfully removed from affected systems.
Conduct comprehensive testing to verify the restoration of normal system functionality.
Ensure that security configurations are correctly applied and effective.
Verify the effectiveness of implemented security updates.

**User Training and Awareness:**
Provide security awareness training to employees and system users.
Educate users about recognizing phishing attempts, social engineering, and best security practices.
Encourage strong password management and multi-factor authentication.

**Document Recovery and Security Enhancements:**
Document all actions taken during the recovery process, including system changes and security updates.
Maintain a recovery log, detailing timelines and the responsible parties for each action.
Ensure that lessons learned from the incident are incorporated into future security strategies.

**Review and Improve Incident Response Plan:**
Conduct a post-incident review of the recovery phase, seeking input from all involved parties.

Analyze the effectiveness of the recovery process and identify areas for improvement.
Update the incident response plan and workflows to reflect any lessons learned and new security measures.

**Communication with Stakeholders:**
Keep stakeholders, especially executive management and customers, informed of the progress of the recovery efforts.
Assure stakeholders that the company is taking measures to prevent future incidents.

**Legal Compliance:**
Ensure that all actions taken during the recovery process align with legal and regulatory compliance requirements, such as data breach notification laws

**Final Approval and Closure:**
Obtain final approval from the Incident Response Team and executive management to close the recovery phase.
Confirm with stakeholders that all goals and objectives have been met.
Issue a formal incident closure report to all relevant parties.

**Note:**
The recovery phase is a critical step in the incident response process, ensuring that affected systems are not only cleaned of malware but also made resilient against future attacks. It's essential to maintain a strong focus on security enhancements, employee training, and documentation to continually strengthen the organization's security posture.

## Post-Incident Activities

**Objectives:**
To assess the effectiveness of the incident response efforts.
To identify lessons learned and areas for improvement.
To create a comprehensive incident report for documentation and potential legal or regulatory requirements.

**Key Participants:**
Incident Response Team (IRT)
Forensics Team
Legal Counsel
CISO (Chief Information Security Officer)
CIO (Chief Information Officer)
Security Analysts

Public Relations (PR) Team
External Consultants (if required)

**Review Meeting:**
Schedule a post-incident review meeting with all relevant stakeholders within two weeks of the incident resolution.

**Data Gathering and Analysis:**
Collect and review all available incident data, including:
Incident timeline.
Actions taken during the incident.
Forensic analysis findings.
Communication records.
Lessons learned from team members.
Analyze the incident from start to finish to understand the malware's behavior and the organization's response.

**Identify Successes and Areas for Improvement:**
Recognize actions that were effective in containing and mitigating the incident.
Identify areas where the response could have been more efficient or effective.
Evaluate the adequacy of existing security controls and policies.

**Lessons Learned:**
Document key lessons learned from the incident, including:
What worked well.
What did not work as expected.
What unforeseen challenges arose.
Opportunities for enhancing response procedures.
Training and awareness gaps.

**Incident Report Creation:**
Compile all the collected data and insights into a comprehensive incident report.
The report should include:
Executive summary.
Incident details and timeline.
Actions taken during the incident.
Forensic findings.
Impact assessment (financial, operational, reputational).
Regulatory compliance assessment.
Lessons learned and recommendations.

**Recommendations:**
Provide a set of actionable recommendations based on lessons learned to improve the organization's security posture. These may include:
Changes to incident response procedures.

Updates to security policies and controls.
Enhancements to employee training and awareness programs.
Adjustments to system configurations.
Consideration of technology and tools that may enhance security.

**Documentation:**
Ensure that the incident report and all supporting documents are comprehensively documented and stored securely for future reference. This documentation is crucial for regulatory compliance and potential legal proceedings.

**Communication:**
Share the incident report with executive management and the Board of Directors. Discuss the findings, recommendations, and the organization's commitment to improving security.

**Follow-Up Actions:**
Develop a timeline for implementing the recommendations and improvements identified in the report.
Monitor the progress of these actions and provide regular updates to the executive team.

**Training and Awareness:**
Conduct training sessions and awareness campaigns to ensure that all employees are informed about the lessons learned and the organization's response improvements.

**Continuous Improvement:**
Integrate the lessons learned into the organization's incident response playbook and workflows.
Review and update the playbook as necessary to reflect the improvements made.

# Workflow Steps

Workflow for Responding to a Malware Incident:

**Detection and Identification:**
Immediately report any unusual system behavior to the Incident Response Team.
The CIO and CISO should lead the identification and classification process.

**Containment:**
The IRT, along with the security team, should work to isolate affected systems and limit the malware's spread.
User accounts identified as compromised should be disabled.

**Eradication and Recovery:**
A joint effort of the IRT and IT team is essential to remove malware, restore clean backups, and reconfigure systems.
A security assessment should be conducted to identify and address vulnerabilities.

**Communication and Stakeholder Involvement:**
The Public Relations team should work alongside the IRT to communicate internally and externally.
Legal counsel should be consulted to ensure regulatory compliance.

**Investigation and Analysis:**
The Forensics team, supported by the IRT, conducts a thorough analysis to understand the malware's behavior and origin.

**Legal and Regulatory Compliance:**
Legal counsel and regulatory compliance experts should ensure adherence to applicable laws.
Interaction with law enforcement, if required, should be coordinated.

**Post-Incident Review and Documentation:**
The IRT should lead the post-incident review and ensure comprehensive documentation.

**Follow-Up Actions:**
The CISO, CIO, and security team should ensure that systems are monitored and potential re-infection is addressed.

# Incidents of Compromise

Data Breach: Malware can exfiltrate sensitive data, such as customer information, intellectual property, or financial records, and transmit it to unauthorized parties.

Ransomware: The malware can encrypt critical data or systems, rendering them inaccessible until a ransom is paid to the attackers.

System Disruption: Malware can disrupt critical systems or services, causing operational downtime, affecting customer service, and causing financial losses.

Phishing and Social Engineering: Malware can be used to launch phishing attacks, tricking users into revealing sensitive information, such as login credentials or financial data.

Botnet Formation: Malware can turn compromised devices into a part of a botnet, which can be used for various malicious activities, including DDoS attacks, sending spam, or further malware distribution.

Keylogging: Malware can record keystrokes on an infected system, capturing sensitive information like passwords and credit card numbers.

Backdoor Creation: Malware can create a hidden entry point (backdoor) into the system, allowing attackers to maintain unauthorized access for future attacks.

Each of these compromises can have varying levels of impact, from data loss to financial costs and damage to an organization's reputation. Developing robust incident response plans and cybersecurity measures is essential to mitigate the risks associated with these malware attack compromises.

# Communication Tree for Malware Incident Response

**Incident Response Team (IRT):**
Team Leader: Victor Onukwu
Responsibilities: Overall coordination of the incident response plan, decision-maker.
IT Security Specialist: [Name]
Responsibilities: Technical expertise for malware identification and eradication.
Forensics Analyst: [Name]
Responsibilities: Investigating the incident and collecting forensic evidence.
Legal Counsel: [Name]
Responsibilities: Ensuring legal and regulatory compliance.
Communications Coordinator: [Name]
Responsibilities: Handling internal and external communications.

**IT and Security Teams:**
Chief Information Officer (CIO): Rex Lee
Responsibilities: Oversight of the IT and security teams, decision-making authority regarding IT infrastructure.
Chief Information Security Officer (CISO):
Responsibilities: Leading security initiatives and managing cybersecurity resources.
IT Personnel: [Names]
Responsibilities: Technical support in identifying and containing the incident.
Security Personnel: [Names]
Responsibilities: Assisting with malware removal and system security.

**Public Relations and Communications Team:**
Public Relations Manager: [Name]
Responsibilities: Crafting and delivering internal and external communications.
Media Relations Specialist: [Name]
Responsibilities: Handling media inquiries and press releases.
Customer Relations Specialist: [Name]
Responsibilities: Communicating with affected customers and addressing concerns.

**Legal and Regulatory Compliance:**
General Counsel: [Name]
Responsibilities: Overseeing legal compliance and liaising with regulatory bodies.
Privacy Officer: [Name]
Responsibilities: Ensuring compliance with data protection laws, such as PIPEDA.

**Executive Management:**
Chief Executive Officer (CEO): Greg Hicks*
Responsibilities: Briefing the CEO on the incident's severity and impact.
Chief Financial Officer (CFO): Gregory Craig*
Responsibilities: Reporting financial implications and budgetary needs.
Chief Operating Officer (COO): TJ Flood*
Responsibilities: Ensuring operational continuity.

**Human Resources:**
HR Manager: [Name]
Responsibilities: Supporting HR-related actions, including employee notifications and support.

**External Stakeholders:**
Regulatory Authorities: PIPEDA
Responsibilities: Reporting the incident to relevant regulatory bodies as required.
Supply Chain Partners: [Names]
Responsibilities: Communicating the incident's impact on the supply chain.

Affected Customers: [Names]
Responsibilities: Reaching out to affected customers and addressing their concerns.

# Citation


Cybersecurity and Infrastructure Security Agency. (2020). Federal government cybersecurity incident and vulnerability response playbooks. U.S. Department of Homeland Security1

Treasury Board of Canada Secretariat. (2020). Playbook for cloud security control implementation. Government of Canada. https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-services/playbook-cloud-security-control-implementation.html

Exabeam. (2020). Incident Response Plan: Best Practices, Templates and Tools. Exabeam. https://www.exabeam.com/information-security/incident-response-plan-best-practices-templates-and-tools/

IncidentResponse.org. (2023). Malware Outbreak Incident Response Playbook. IncidentResponse.org. https://www.incidentresponse.org/playbooks/malware-outbreak

Canadian Tire Corporation. (2023). Président, Services Financiers Canadian Tire et Président et chef de la direction, Banque Canadian Tire. Canadian Tire Corporation. https://corp.canadiantire.ca/French/leadership-team/default.aspx

Joint Task Force Working Group. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. National Institute of Standards and Technology1

SweetProcess. (2023). How to Write a Policy: The Ultimate Guide. SweetProcess.https://www.sweetprocess.com/how-to-write-a-policy/

Compass. (2023). Cyber Security Immersive. Compass. https://compass.com/cyber-security-immersive