Incident Response Plan
Malware Threat

Scenario

User called in worried that their host system is compromised by a virus or a form a malware.

- Inspired by a real event and combined with skills/tools learned from studies.

Executive Summary

This document describes the plan for responding to a Cyber Security Incident involving potential malware. Here we will outline the approach to respond, contain, identify, eradicate, recover, and review for lessons learned when dealing with potential malware threats.

Tools Used

- Splunk: Security Information and Event Management
- CrowdStrike: Enterprise Security Console for Endpoint Detection and Response (EDR)
- Wireshark: Network Protocol analyzer
- VirusTotal: OSINT tool used to provide antivirus scanning and results for suspicious files and URL links.

Step 1: Identify and Isolate the Device

- Determine if the device is managed by your organization
- Disable the endpoint device from accessing your network
    - Log into CrowdStrike Console
    - Navigate to Host Setup and Management
    - Search for user's endpoint device Hostname and isolate device from network
        - This will prevent potential spread of malware infection and any potential lateral movement within the internal network
- Ensure another Incident Response team member contacts user to gather any information from the end user to assist in the investigation
- Create a live document to keep any notes, screenshots, tools used, and process followed

Step 2: Identify Type, Scope, and Timeline of Malware Threat

- Review Firewall logs for any suspicious outbound traffic
- Check device history for any anomalies
    - Windows Event Log
        - Identify any suspicious activity
            - Any Data Exfiltration (IOC – Large amounts of COPY operation)
            - Time of Access (IOC – Unusual login times/dates, example: after hours)
    - Check EDR for any system detections
        - Determine if any malicious files were downloaded to device
            - If **NO** malicious files were downloaded proceed to Step 3
            - If **YES** and a malicious file was downloaded:
                - Create an image of infected system
                - Capture device information by following the Order of Volatility
                    - Capture most volatile (can spontaneously change) to least
                - Create Hash files of all information copied for Data Integrity
                - Escalate to Incident Response Team Lead

- Document Chain of Custody
- Restore Device from Backup (if possible)
  - Determine earliest time/date of non compromised endpoint device
- Hand off incident and relevant documentation to Digital Forensics and Malware Analysis Team for further investigation.

Step 3: Assess Damage and Remediation of Malware Threat

- Log into SIEM (Splunk) console
  - Search indexes and review web traffic logs
    - Example Index Searches using Splunk:
      - index=wireshark user="username" url="URL AND url!=*.js*" | stats count by user url
        - Aggregates events by user/URL and excludes any .js links
  - Change Date and Time of search to Date/Time in question
- After aggregating URL Links, run links through VirusTotal (OSINT Tool)
- Determine if any other malicious links are involved
  - Create a sandbox environment
  - Navigate to malicious link
  - Check connections and possible IOC's
    - IOC's will indicate if there are any other potential IP Addresses, Domains, or URL's associated with original URL link
- Block all Malicious URL links
- Scan device using an Anti-Virus/Anti-Malware scanner to ensure no malicious files are on endpoint device
- Restore Device from Backup (if needed/possible)
  - Determine earliest time/date of non compromised endpoint device

Step 5: Understanding Root Cause, Conclusion, and Lessons Learned

- Root cause of Incident is from the user clicking on a Malicious link from a browser search.
  - Searched in google using keywords or phrases
  - Clicked on first link
  - User redirected to Malicious URL CAPTCHA page
  - User clicked on CAPTCHA and was redirected to second Malicious URL
  - User then clicked "ALLOW Notification" pop up
    - This caused the endpoint device to receive spam notifications
- Confirmed no Data Exfiltration occurred
- Confirmed no Virus was downloaded to endpoint device
- Blocking all notifications and Blacklisting URL links remediated incident
- Ensure live document has all information captured to discuss any Lessons Learned for improvement of process

Resourses Used

- Developing your Incident Response Plan (ITSAP.40.003):
  - https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003
- Annex- 3A (Security Control Catalogue):
  - https://www.cyber.gc.ca/en/guidance/annex-3a-security-control-catalogue-itsg-33
- Backing up your Information (ITSAP.40.002):
  - https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002