Security Incident Management Runbook

Malicious Driver

Revision: ***1***
Date: ***August 14th, 2024***

Group: ***3***

Ananthu Krishna Vadakkeppatt
Ramachandra Muralidhara
Syed Mujahid Hamid Ali
Yannish Kumar Ballachander Sreedevi

Table of Contents

Introduction

This playbook offers an efficient way to handle incidents where a malicious driver is involved. A malicious driver is a piece of software that works with an operating system to carry out illegal operations, like obtaining system privileges, disabling security, or opening the door for other attacks. Since these drivers function at a low level inside a system, they are very difficult to identify. The steps for identifying the existence of a malicious driver, assessing its impact, containing the threat, getting rid of the driver, and recovering the system are all covered in this playbook.

Data Classification

The Organization's Data Classification Standard is used to determine the overall impact.

Classification	Definition	Example
Confidential	Data that may cause harm to the company and/or public if compromised.	• Configuration Files • Driver keys
Internal	Data that is owned by the organization that may result in financial loss if compromised.	• Log files • Private company reports
Public	Data that is made available to the public consumption.	• Open-source code • Driver documentation

Technologies, Systems, Services, Process

Name	Definition	Capabilities
Endpoint Analysis	An examination technique of activities on endpoints	• Identifies unusual behavior • Finds unauthorized processes
Memory Analysis	A technique to analyze computer memory to detect anomalous behavior.	• Identifies if code injection took place • Identifies anomalous behavior
SeaDuke	A tool for analyzing and monitoring drivers	• Monitors driver activities • Detects anomalous behavior
Wingbird	A tool to detect connection to unauthorized drivers	• Detects if any unauthorized connection is made to an external driver • Scans drivers to check presence of malicious code.

Response Procedures

Detection Phase

Role/Team/System	Description	Objectives	Action
Security Analyst	Monitor systems for suspicious activities and potential security incidents.	Identify and report anomalies that may indicate the presence of a threat.	Set up real-time alerts for unusual login attempts, file changes, or unauthorized access.
Memory Analyst	Analyze system memory for signs of malicious activity.	Detect code injections, unauthorized processes, and other memory-based threats.	Use memory forensics tools to scan for suspicious processes or injected code.
Network Administrator	Monitor network traffic for unusual patterns or unauthorized access attempts.	Identify network-based indicators of compromise.	Implement IDS/IPS to detect unusual traffic patterns or communication with known malicious IPs.

Analysis Phase

Role/Team/System	Description	Objectives	Action
Security Analyst	Perform a detailed analysis of logs and alerts to confirm the presence of a threat.	Confirm the nature of the threat and its impact on the system.	Correlate logs and alerts with known indicators of compromise.
Incident Responder	Assess the situation and develop a response strategy.	Determine the extent of the compromise and plan for containment.	Gather information from various sources to build a timeline of the attack.
Lawyer	Review the legal implications of the incident.	Ensure compliance with legal and regulatory requirements.	Assess the need for data breach notification and prepare necessary legal documentation.

Containment Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Isolate compromised systems and disable the threat.	Prevent further spread and damage.	Disconnect affected systems from the network and disable malicious processes.
Network Administrator	Block malicious traffic and secure the network perimeter.	Stop the attack from propagating across the network.	Implement firewall rules to block traffic from known malicious IPs and isolate affected network segments.
Security Administrator	Ensure all security controls are properly configured and updated.	Harden systems against further compromise.	Apply necessary security patches and updates, reconfigure security settings, and ensure all endpoint protection tools are active and up-to-date.

Eradication Phase

Role/Team/System	Description	Objectives	Action
Security Administrator	Completely remove all traces of the threat from the environment.	Ensure systems are clean and secure.	Scan all systems for residual malware or compromised files and remove them.
Database Administrator	Secure database systems and remove any unauthorized access points.	Protect sensitive data and restore database integrity.	Review database access logs, revoke compromised credentials, and apply patches to any exploited vulnerabilities.
Endpoint Analyst	Verify that all endpoints are secure and free of threats.	Ensure endpoint security and compliance.	Perform a comprehensive scan of all endpoints, reconfigure security settings, and confirm the removal of any malicious software.

Recovery Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Restore normal system operations and ensure systems are secure.	Resume secure and normal operations.	Re-enable systems, verify security configurations, and ensure all updates and patches are applied.
Incident Responder	Confirm the effectiveness of the recovery process and ensure no residual threats.	Validate that all threat vectors have been neutralized and systems are fully operational.	Conduct a final review of the incident response and recovery process, ensuring all systems are secure and operational.
Operations Manager	Oversee the return to normal operations across the organization.	Ensure full operational capability and prevent future incidents.	Coordinate with all departments to confirm normal operations are restored and document any operational changes required to prevent reoccurrence.

Post-Incident Phase

Role/Team/System	Description (optional)	Objectives	Action
CISO	Oversee the post-incident review and update security strategies.	Improve organizational security posture and prevent future incidents.	Conduct a post-incident review, identify lessons learned, and update security policies and procedures accordingly.
Security Analyst	Analyze the incident for root causes and potential gaps in security.	Ensure that similar incidents are prevented in the future.	Perform a root cause analysis and recommend improvements to detection and prevention measures.
Awareness Team	Educate staff on the incident and update security awareness training.	Improve organizational awareness and readiness for future incidents.	Develop and deliver updated security awareness training based on the lessons learned from the incident.