Security Incident Management Runbook

Gmail, Tumblr, Salesforce, Twitter as C2

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 runbook provides a systematic approach to detecting, analyzing, containing, eradicating, and recovering from incidents involving the use of third-party services for Command and Control (C2) operations. These incidents leverage legitimate services, such as Gmail, Salesforce, or Twitter, making them difficult to monitor. This guide outlines the necessary steps for responding to such threats efficiently.

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.	• Access Tokens • Configuration Files
Internal	Data that is owned by the organization that may result in financial loss if compromised.	• System Log Files • Internal procedures
Public	Data that is made available to the public consumption.	• Public websites • Advertisements and Promotions

Technologies, Systems, Services, Process

Name	Definition	Capabilities
Threat Hunting	Proactive search for threats within the network.	• Identifies potential C2 activities via third-party services.
Network Analysis	Examination of network traffic for suspicious activity.	• Detects unusual patterns and possible C2 channels.
Gcat	A command and control tool using Gmail for communication.	• Helps identify C2 channels using Gmail.

Response Procedures

Detection Phase

Role/Team/System	Description	Objectives	Action
Firewall Analyst	Review firewall logs to detect suspicious traffic.	Identify unauthorized C2 communication.	Regularly analyze firewall logs and alert on anomalous behavior.
Incident Responder	Monitor and validate network threats.	Confirm presence of C2 channels.	Correlate findings with threat intelligence.
Network Administrator	Monitor network traffic for anomalies.	Detect unauthorized access patterns.	Implement threat hunting tools and set up alerts.

Analysis Phase

Role/Team/System	Description	Objectives	Action
Security Analyst	Analyze detected traffic to confirm C2 activity.	Confirm and assess the scope of the attack.	Examine network logs and identify involved systems.
Incident Responder	Coordinate analysis efforts and validate threats.	Ensure a comprehensive threat assessment.	Collaborate with analysts and validate with forensic data.
Forensic Analyst	Investigate compromised systems.	Understand the attack method and impact.	Perform forensic analysis and assess data exfiltration.

Containment Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Disable compromised accounts and services.	Stop C2 communication.	Disable affected accounts and remove compromised services.
Network Administrator	Block C2 communication channels.	Prevent further unauthorized access.	Block suspicious Ips and domains and implement network segmentation.
Security Administrator	Ensure containment strategies are applied.	Secure the environment against further threats.	Oversee containment actions and verify effectiveness of blockades.

Eradication Phase

Role/Team/System	Description	Objectives	Action
Security Administrator	Remove malicious tools and software.	Ensure complete removal of threats.	Conduct thorough scans and patch vulnerabilities.
Database Administrator	Secure and review database access.	Protect database integrity.	Revoke compromised access and monitor database activities.
Endpoint Analyst	Clean up infected endpoints.	Ensure endpoints are secure.	Scan and clean endpoints and update security policies.

Recovery Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Restore normal operations.	Resume secure operations.	Re-enable secure configurations.
Incident Responder	Confirm full recovery.	Validate that systems are secure.	Perform a final assessment.
Operations Manager	Ensure ongoing secure operation.	Restore full functionality.	Validate system performance.

Post-Incident Phase

Role/Team/System	Description (optional)	Objectives	Action
CISO	Communicate with senior leadership.	Inform stakeholders of the incident and resolution.	Brief the leadership team.
Security Analyst	Review the incident for lessons learned.	Improve future response efforts.	Conduct a post-incident review.
Awareness Team	Update training materials.	Improve user preparedness.	Integrate lessons into training.