Incident Response for Token Theft

Overview

This document provides a generalized incident response procedure for addressing token theft incidents, applicable to any organizational security environment. It covers detection, triage, investigation, containment, post-containment actions, documentation, and monitoring to ensure a rapid and effective response to unauthorized token access.

1 Alert Acknowledgment

- Acknowledge alerts received via Security Information and Event Management (SIEM), Identity and Access Management (IAM), or endpoint detection tools.
- Alert types include:
  - User-reported issues: Suspicious or malicious behavior, inability to access accounts, or unauthorized activity.
  - IAM Alerts: Unfamiliar sign-in properties, impossible travel, or sign-ins from new devices or locations.
  - Endpoint Alerts: Suspicious rule creation, high outbound activity, malicious link clicks, or malware detection.

2 Initial Triage

- Identify affected user(s) and determine their role (e.g., privileged or standard).
- Review alert details: timestamp, IP address, application involved, and token type.
- Confirm suspicious activity by analyzing IAM sign-in logs for unusual patterns.

3 Investigation

- **Check for Other Users from Same IP**: Use sign-in logs and query tools to identify other users signing in from the same suspicious IP.
- **Phishing Analysis**: Review security alerts for indicators like malicious URLs, attachments, or email-based threats. Remove identified malicious emails from mailboxes following established procedures.
- **Audit Log Review**: Analyze audit logs to identify unauthorized application consents, newly created or updated authentication methods, or newly registered devices.
- **Log Correlation**: Search for lateral movement, privilege escalations, or other suspicious activity patterns across the environment using SIEM or related tools.

4 Containment

- Upon confirmation of token theft, follow the below actions:
  - Revoke all active sessions and refresh tokens for the affected user.
  - Force an immediate password reset.
  - Enforce re-registration of multi-factor authentication (MFA).
  - Remove suspicious applications, newly created or updated authentication methods, and new registered devices (if identified).
  - Notify the affected user.
  - Escalate to relevant teams if needed.
- Provide all relevant user and incident details to the operations team for swift action.

5 Post-Containment Actions

- **Identify and Remove Malicious Artifacts**: Check outbound activity (e.g., emails) from the user to identify and remove potentially malicious content.
- **Investigate Logs**: Review endpoint and SIEM logs for suspicious activities, such as rule creation, moved messages, file downloads, or unauthorized permission changes.

6 Documentation

- Complete a thorough root cause analysis (RCA) in the incident ticket.
- Document every step clearly for auditing and knowledge sharing to improve future incident response.

7 Monitoring and Recovery

- Monitor the affected account for 48–72 hours for new suspicious sign-ins or token-related activity.
- Revalidate access control policies to ensure risky sign-ins are blocked.
- Confirm MFA policies are correctly enforced for the user and environment.
- Remove any legacy authentication methods if identified.

Conclusion

This procedure provides a universal framework for responding to token theft incidents, ensuring rapid containment and recovery while maintaining security best practices.