Registry Key Change Alert Investigation Runbook

Registry key changes can indicate both legitimate system or application updates and malicious activity, such as persistence mechanisms, privilege escalation, or configuration tampering by attackers. Prompt investigation of registry key change alerts is essential to distinguish between benign and suspicious modifications and to prevent potential compromise.

This runbook provides a step-by-step approach for investigating registry key change alerts using Microsoft Defender for Endpoint, Tanium, and Splunk, with recommendations for OSINT enrichment.

1. Initial Alert Review

Steps:

- Review the alert in Microsoft Defender for Endpoint, Tanium, or Splunk.
- Record key details:
    - Registry key path and value before/after change
    - Device name and user account involved
    - Timestamp of the change
    - Source of detection (e.g., real-time monitoring, scheduled scan)

2. Validate the Alert

Checks:

- Determine if the change is expected:
    - Was there a recent software installation, update, or configuration change?
    - Is the registry key associated with known system or application behavior?
- Review the detection method (signature, heuristic, behavioral) for context.

3. OSINT Enrichment

Steps:

- Research the registry key and value using OSINT sources:
    - **Google Search:** Search for the registry key path and value to find documentation or threat reports.
    - **Malware Analysis Sites:** Check VirusTotal Intelligence, Hybrid Analysis, or Any.run for references to the key in malware samples.
    - **Security Forums/Threat Feeds:** Look up the key on sites like BleepingComputer, Malwarebytes Labs, or MITRE ATTCCK for known malicious registry modifications.
- Document findings, including whether the key is linked to malware, persistence, or legitimate software.

4. Investigate Device and User Impact

Checks:

- **Microsoft Defender for Endpoint:**
    - Review device timeline for related suspicious activity (process launches, file changes, network connections).
    - Check for additional alerts or correlated threats on the device.
- **Tanium:**
    - Query for the registry key/value across other endpoints to determine scope.
    - Check for similar changes on other devices or by the same user.
    - Gather system information (running processes, autoruns, scheduled tasks).
- **Splunk:**
    - Search logs for events preceding and following the registry change (e.g., process creation, user logon, file modifications).
    - Correlate with authentication and privilege escalation events.

5. Containment and Remediation

Actions:

- If the change is determined to be malicious or suspicious:
    - Revert the registry key to its previous value (if possible and safe).
    - Isolate the affected device using Microsoft Defender for Endpoint if compromise is suspected.
    - Remove or disable any persistence mechanisms (e.g., autoruns, scheduled tasks) linked to the registry change.
    - Run a full malware scan on the affected device.
    - Reset credentials for affected users if credential theft or privilege escalation is suspected.

6. Communication and Documentation

Steps:

- Notify affected user(s) and relevant IT/security teams.
- Document all investigative steps, findings, and actions in your incident management system.
- Escalate to management or compliance if sensitive systems or data are involved.

7. Post-Incident Activities

Recommendations:

- Review and tune detection rules for registry changes in all security tools.
- Update threat intelligence feeds and blocklists as needed.
- Conduct a post-incident review to identify gaps and improve processes.
- Provide user awareness training if the change was user-driven or due to risky behavior.

Malicious File Alert Investigation Runbook

Malicious file alerts indicate that a potentially harmful file has been detected within the environment. Such files can be used to deliver malware, exfiltrate data, or provide unauthorized access to attackers. Prompt and thorough investigation is essential to contain threats and prevent further compromise.

This runbook outlines a step-by-step approach for investigating malicious file alerts using Microsoft Defender for Endpoint, Tanium, and Splunk, and includes recommended OSINT checks to validate and enrich findings.

1. Initial Alert Review

Steps:

- Review the alert in Microsoft Defender for Endpoint, Tanium, or Splunk.
- Record key details:
    - File name and hash (MD5/SHA1/SHA256)
    - File path and device name
    - User associated with the alert
    - Timestamp of detection
- Note the detection source (e.g., real-time protection, scheduled scan, behavioral detection).

2. Validate the Alert

Checks:

- Confirm the alert is not a false positive by:
    - Reviewing file reputation in Microsoft Defender for Endpoint.
    - Checking if the file is signed or associated with legitimate software.
    - Reviewing detection method (heuristic, signature-based, behavioral).

3. OSINT Enrichment

Steps:

- Gather file hashes (MD5, SHA1, SHA256) and perform the following checks:
    - **VirusTotal:** Submit the hash or file to VirusTotal to check for known malware signatures and community comments.
    - **Hybrid Analysis:** Use Hybrid Analysis to review sandbox analysis reports.
    - **Any.run:** Search Any.run for interactive malware analysis if available.
    - **Malshare/MISP:** Check repositories like Malshare or your organization's MISP instance for related threat intelligence.
    - **ReversingLabs, Joe Sandbox, or other OSINT sources** as available.

- Document findings, including detection rates, behavioral indicators, and threat intelligence context.

4. Investigate Device and User Impact

Checks:

- **Microsoft Defender for Endpoint:**
    - Review device timeline for related suspicious activity (file creation, process launches, network connections).
    - Check for additional alerts or correlated threats on the device.
    - Run a full scan if not already performed.
- **Tanium:**
    - Query for presence of the file across other endpoints.
    - Check for similar files, processes, or registry changes.
    - Gather system information (running processes, network connections, autoruns).
- **Splunk:**
    - Search logs for file execution events, lateral movement, or unusual user activity.
    - Correlate with authentication logs for signs of account compromise.

5. Containment and Remediation

Actions:

- Use Microsoft Defender for Endpoint to isolate the affected device if compromise is suspected.
- Quarantine or delete the malicious file using Defender or Tanium.
- Reset credentials for affected users if credential theft is suspected.
- Block the file hash via endpoint protection policies.
- Remove persistence mechanisms (e.g., scheduled tasks, autoruns) if identified.

6. Communication and Documentation

Steps:

- Notify the affected user(s) and relevant IT/security teams.
- Document all investigative steps, findings, and actions in your incident management system.
- Escalate to management or compliance if sensitive data or critical systems are involved.

7. Post-Incident Activities

Recommendations:

- Review and tune detection rules in Microsoft Defender for Endpoint, Tanium, and Splunk.
- Update threat intelligence feeds and blocklists.
- Conduct a post-incident review to identify gaps and improve response processes.
- Provide user awareness training if the infection vector was user-driven (e.g., email attachment).

Vendor List of Organization

Microsoft microsoft.com

Amazon amazon.com

Apple apple.com

Facebook (Meta) facebook.com IBM ibm.com

Deloitte deloitte.com

Accenture accenture.com

Cisco cisco.com

Oracle oracle.com

Malicious URL Click Alert Runbook

The increasing sophistication of cyber threats has made malicious URLs a common vector for attacks such as phishing, malware delivery, and credential theft. When a user clicks on a malicious link, it can put sensitive data, user accounts, and the broader organization at risk. Timely and effective response to such incidents is critical to minimizing potential damage and preventing further compromise.

This runbook provides a comprehensive, step-by-step guide for investigating and responding to alerts triggered by malicious URL clicks. It is specifically designed for environments utilizing Splunk, Microsoft Defender for Endpoint, and Azure Active Directory (Azure AD).

1. Initial Alert Review

When an alert for a malicious URL click is received, it is crucial to quickly assess the situation and gather relevant information.

Steps:

- Review the alert details in the tool where it was triggered (Splunk, Microsoft Defender for Endpoint, or Azure AD).
- Identify the user, device, and timestamp associated with the alert.
- Note the URL in question and any associated threat intelligence (e.g., known phishing or malware domains).
- Check if the alert is part of a larger campaign or if multiple users are affected.

2. Validate the Alert

Before taking action, confirm the alert is genuine and not a false positive.

Required Checks:

- Cross-reference the URL with threat intelligence feeds (e.g., Microsoft Threat Intelligence, open-source feeds).
- Check if the URL is known to be associated with phishing, malware, or other threats.
- Review user activity logs in Splunk for evidence of suspicious behavior following the URL click (e.g., file downloads, credential entry).
- Use Microsoft Defender for Endpoint to check for any correlated alerts on the user's device (e.g., malware detection, unusual processes).
- In Azure AD, review sign-in logs for the user for any suspicious activity (e.g., impossible travel, risky sign-ins).

3. Investigate User and Device Impact

Determine the scope of the incident and whether the user or device has been compromised.

Steps:

- In Splunk, search for additional activity from the user or device around the time of the alert, such as:
    - Access to other suspicious URLs
    - Unusual network connections
    - File downloads or process launches
- In Microsoft Defender for Endpoint:
    - Run a quick or full scan on the affected device.
    - Check for new or unknown processes, registry changes, or file modifications.
    - Review automated investigation results, if available.
- In Azure AD:
    - Review recent sign-ins for the user for anomalies.
    - Check for changes to user account settings or MFA status.

4. Containment and Remediation

Take immediate action to contain the threat and prevent further impact.

Actions:

- Isolate the affected device using Microsoft Defender for Endpoint's device isolation feature, if compromise is suspected.
- Reset the user's password in Azure AD and require re-authentication.
- Revoke active sessions for the user in Azure AD.
- Remove or quarantine any malicious files detected on the device.
- Block the malicious URL at the proxy, firewall, or email gateway to prevent further access.
- If phishing is suspected, warn other users who may have received the same message or link.

5. Communication and Documentation

Ensure proper communication and documentation throughout the incident.

Steps:

- Notify the affected user about the incident and instruct them not to interact with suspicious emails or links.
- Inform IT security or incident response teams as per escalation procedures.
- Document all findings, actions taken, and evidence collected in your incident management system.

- If sensitive data may have been exposed, escalate to compliance or legal teams as required.

6. Post-Incident Activities

After the incident is contained, take steps to prevent recurrence and strengthen defenses.

Recommendations:

- Conduct a post-incident review to identify gaps in detection or response.
- Update security awareness training for users, emphasizing the risks of clicking unknown links.
- Tune detection rules in Splunk, Microsoft Defender for Endpoint, and Azure AD to improve alerting.
- Review and update email and web filtering policies.
- Share threat intelligence with relevant teams to improve organizational awareness.

Password Spray Attack Alert Runbook

A password spray attack is a type of brute-force attack where an attacker attempts to gain unauthorized access to user accounts by trying a few commonly used passwords against many usernames. Unlike traditional brute-force attacks, which try many passwords against one account, password spray attacks are designed to avoid account lockouts and detection. This runbook provides a comprehensive guide for responding to password spray attack alerts, including what to check and how to handle the situation.

1. Initial Alert Review

When a password spray attack alert is received, it is important to act quickly and methodically. Begin by reviewing the details of the alert in your security platform, such as Microsoft Defender for Endpoint, Azure AD Identity Protection, or your SIEM tool.

Steps:

- Open the alert in your security dashboard.
- Review the alert summary, including the time of detection, affected accounts, and source IP addresses.
- Note any patterns, such as the number of accounts targeted or the frequency of login attempts.

2. Validate the Alert

Before proceeding with remediation, confirm that the alert is legitimate and not a false positive.

Required Checks:

- Examine the login attempts for consistency with known password spray techniques (e.g., multiple accounts targeted with the same password).
- Check if the source IP addresses are external or from known malicious ranges.
- Review the geolocation of the login attempts for anomalies (e.g., logins from unexpected countries).
- Cross-reference the alert with other recent security events or user reports.

3. Investigate Affected Accounts

Identify which user accounts were targeted and whether any were successfully compromised.

Steps:

- List all accounts that experienced failed login attempts during the attack window.
- Check for any successful logins immediately following failed attempts.
- Review account activity logs for unusual behavior, such as changes to account settings, mailbox rules, or data access.
- Contact users whose accounts were targeted to verify if they experienced any issues.

4. **Containment and Remediation**

Take immediate steps to contain the attack and remediate any compromised accounts.

Actions:

- For accounts with suspicious or successful logins, force a password reset and require multi-factor authentication (MFA) if not already enabled.
- Temporarily block or restrict access from suspicious IP addresses using firewall rules or conditional access policies.
- Disable accounts that show signs of compromise until they can be fully investigated and secured.
- Remove any unauthorized changes or malicious rules from compromised accounts.

5. **Communication and Documentation**

Proper communication and documentation are essential for effective incident response.

Steps:

- Notify affected users about the attack and any actions they need to take, such as resetting their passwords or reporting suspicious activity.
- Document all findings, actions taken, and evidence collected during the investigation.
- Escalate the incident to your security operations or IT leadership if the attack is widespread or if sensitive data may have been accessed.

6. **Post-Incident Activities**

After containing the attack, take steps to prevent future incidents and improve your security posture.

Recommendations:

- Review and update password policies to require strong, unique passwords.
- Enforce MFA for all user accounts, especially those with elevated privileges.
- Monitor for recurring attack patterns and tune alert thresholds as needed.
- Provide user awareness training on password security and phishing risks.
- Conduct a post-incident review to identify lessons learned and update this runbook if necessary.