# Understanding Inactive Subdomains Results

The Subdomains - Inactive Results section highlights subdomains that are either currently unresolved or offline. Monitoring these inactive subdomains is crucial for understanding potential risks and managing your organization's attack surface. Even though these subdomains may not be actively in use, they can still pose security risks if reactivated without proper security measures in place.

## Unresolved Subdomains:

Unresolved subdomains are those that could not be resolved during the scan, meaning they do not currently point to an active IP address. However, based on historical data, these subdomains existed in the past. ReConfirm continues to monitor these subdomains to detect any changes that might make them active again.

1. **Total Unresolved Subdomains:**
   The total count of unresolved subdomains detected during the scan. For example, if ReConfirm identified a total of **589** unresolved subdomains, these are now flagged for monitoring.
2. **Subdomains List:**
   A detailed list of unresolved subdomains, such as `expiredjs.demodata.com` and `backupserver.demodata.com`. Although these subdomains are inactive, they may be unintentionally reactivated in the future. When an inactive subdomain becomes resolvable again, ReConfirm will detect the change and add it back to the active attack surface. Monitoring unresolved subdomains is essential to prevent unauthorized reactivation and potential exploitation by attackers.
   Example Subdomains:
   - `expiredjs.demodata.com`
   - `legacyservice.demodata.com`
   - `archive.demodata.com`
3. **Potential Risks:**
   These subdomains, if reactivated without proper security measures, can become an entry point for attackers. It is essential to periodically review and assess the need for these subdomains to avoid accidental exposure of outdated or vulnerable services.

## Offline Subdomains:

Offline subdomains are those that could be resolved to an IP address but were not reachable during the scan. This could be due to several reasons, such as being behind a firewall, the server being offline, or network configuration issues.

1. **Total Offline Subdomains:**
   The total count of offline subdomains detected during the scan. For instance, if ReConfirm found **13** offline subdomains, these are now flagged for further review.
2. **Subdomains List:**
   A list of offline subdomains with their resolved IP addresses. These subdomains were detected but could not be probed, meaning ReConfirm could not scan them for vulnerabilities. This can occur if the subdomain is protected by a firewall or if the server is not responding.
   Example Offline Subdomains:
   - **Subdomain:** `mail.demodata.com`
     - **Resolved IP:** 192.168.1.1
   - **Subdomain:** `archive.demodata.com`
     - **Resolved IP:** 10.0.0.1
   - **Subdomain:** `api.demo2.demodata.com`
     - **Resolved IP:** 172.16.0.2
3. **Potential Risks and Recommendations:**
   - **Behind a Firewall:** If a subdomain is behind a firewall, evaluate whether it needs to be externally resolvable and reachable. If not, consider removing it from external DNS to minimize exposure.
   - **Offline or Non-Responsive:** If a subdomain is offline or not responding, assess whether it is still needed. If it is obsolete, consider removing it from the external DNS to prevent it from becoming a potential security risk in the future.

# Example Analysis:

- **Unresolved Subdomain:** `legacyservice.demodata.com`
  - **Status:** Unresolved
  - **Action:** Monitor for reactivation. If this subdomain becomes resolvable again, ensure that it is properly secured or decommissioned if it is no longer needed.
- **Offline Subdomain:** `api.demo2.demodata.com`
  - **Resolved IP:** 172.16.0.2
  - **Status:** Offline (could not be probed)
  - **Analysis:** This subdomain resolves to an IP address but is not reachable, possibly due to firewall protection or server downtime. Review the necessity of this subdomain being externally resolvable. If it is not required for external use, consider removing it from DNS to reduce the attack surface.

# Importance of Monitoring Inactive Subdomains:

Inactive subdomains, whether unresolved or offline, can pose a hidden threat. Attackers may exploit these subdomains if they become active again without proper security controls. Regular monitoring and periodic review of inactive subdomains help ensure that they do not inadvertently become vulnerabilities within your organization's digital infrastructure.

---

Revision #3
Created 16 September 2024 12:00:17 by Raphael
Updated 16 September 2024 12:38:32 by Raphael