Understanding the Discrepancy in Login Count Tracking for Microsoft Accounts in Windows Systems

Author : Hun13r

Date : February 2025

Introduction

An investigation into missing login counts for Microsoft cloud accounts in the Windows registry revealed a significant discrepancy. Specifically, I observed that the Windows registry does not document login counts for cloud-based Microsoft accounts in the same manner as it does for local user accounts. This anomaly raises important questions about how Windows handles Microsoft account authentication and the tracking of user login activity.

This article explores the root cause of this discrepancy, the underlying mechanisms involved, and the forensic techniques investigators can employ to track login activities for Microsoft accounts when the registry fails to capture this data.

The Issue: Missing Login Count for Microsoft Accounts in the Registry

During a forensic analysis of a Windows 10 system, I discovered that login counts for local user accounts were accurately recorded in the system's registry, specifically within the Security Accounts Manager (SAM) file, located at:

C:\Windows\System32\config\SAM

However, upon investigating the registry for cloud-based Microsoft accounts, I noted that login counts for these accounts were absent. This discrepancy led me to explore the reasons behind the differential handling of local and Microsoft account login data, particularly in the context of forensic analysis.

Why the Discrepancy Exists

Local accounts are managed by the SAM database, whereas Microsoft accounts authenticate via Microsoft's cloud services. As a result, login data such as login counts or timestamps are not stored in the local SAM database.

Where to Find Login Data for Microsoft Accounts

1. **Event Logs**
   - Event ID 4624 in Windows Event Viewer records successful logons for both local and Microsoft accounts.

2. **Microsoft Account Activity Page**
- Accessible via https://account.microsoft.com/security, it provides a history of account logins.

3. **Registry Keys**
- HKEYLOCALMACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI contains some authentication data.

Conclusion

The absence of login count data for Microsoft accounts in the SAM file is due to the cloud-based nature of authentication. Forensic investigators should rely on Event Logs and the Microsoft Account Activity Page to track login data effectively. Understanding these discrepancies is crucial for forensic professionals conducting Windows system investigations.

Author Information

Name: Hun13r
Company: Greaton Forensics
Email: admin@greaton.co.uk