Incident Handler's Journal

Date: April 28, 2023	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	Webroot MS Malicious Software Removal Tool
The 5 W's	• **Who**: Unknown • **What**: Mimikatz attacks • **Where**: At a fertility center company • **When**: Friday 7:00 a.m. • **Why**: The company doesn't have proper security defense. Endpoints are currently using outdated signature-based antivirus, Sophos. Alternative antivirus is Webroot from the MSP but is not properly managed. I checked the Webroot console after a long period, then noticed few computers were infected with Mimikatz attacks.
Additional notes	1. The infected computers are old devices (never upgraded the storage) and still running a very old version of SentinelOne agent previously installed by our MSP. 2. The attacks happened a few days ago but Webroot had no email notification. 3. We disconnected/isolated some infected computers but not all because we had not enough spare ones to replace them. 4. We did a factory reset or swap the SSD with a new one for all infected devices. 5. Ran the MS MRT in an attempt to remove the malware, but it comes back daily. 6. We reset all employees' passwords in case the Mimikatz has compromised some active accounts. 7. Replaced both Sophos and Webroot with a new purchase of SentinelOne XDR, managed by us. 8. Unfortunately, we couldn't identify the root cause of this attack because we lacked security tools, expertise, and a security monitoring system.