

Security weaknesses analysis



Malwarebytes Scan Report 2025-07-01 135546.txt
Document



Malwarebytes Scan Report 2025-07-17 192255.txt
Document

Break down these scan reports from employee host machines and tell me where the organization appears to be lacking in security.

I reviewed both Malwarebytes scan reports, and here's a breakdown of what they show, plus what they suggest about weaknesses in your organization's security posture.

Report 1 (7/1/2025 – User: [REDACTED], Windows 11) 📄

- **Threats Detected:** 13 (all quarantined)
- **Notable Detections:**
 - **Infatica P2B Agent (PUP.Optional.Infatica)** – a proxyware program that can turn the machine into part of a proxy/VPN network, often monetized by selling bandwidth. This can introduce **data leakage and abuse risk**.
 - **MediaArena, OneLaunch, OneStart** – adware and potentially unwanted applications, bundled with free software downloads.
- **Observations:**
 - User had multiple **suspicious installers** in their **Downloads folder** (e.g., Just_Convert, SmartViewPDF, Easy PDF). This strongly suggests **unsafe software installation practices**.
 - Malwarebytes is running in **Free mode**, meaning **no real-time protection**—threats are only caught during manual scans, not prevented.

Report 2 (7/17/2025 – User: [REDACTED], Windows 10) 📄

- **Threats Detected:** 86 (none quarantined)
- **Notable Detections:**
 - **Chrome browser hijackers & adware extensions** (SearchEncrypt, Spigot, Conduit, Trovi, DefaultSearch). These modify browser settings, track browsing, and redirect searches.
 - Malware found across **multiple Chrome profiles** (Default, Profile 15, Profile 17, Profile 18). This indicates **persistent and repeated reinfections**.
- **Observations:**

- No threats were quarantined → user likely dismissed detections or lacked admin action.
- Heavy browser PUP presence shows **lack of browser extension control**.
- Like Report 1, Malwarebytes is in **Free mode**, so infections persist unchecked until manually scanned.

Key Security Gaps Identified

1. No Real-Time Protection

- Both reports show Malwarebytes Free → manual detection only. Malware can persist between scans.

2. Unsafe User Practices

- Employees are downloading/installing adware-laden apps ([REDACTED] host).
- Chrome hijackers spreading across multiple profiles ([REDACTED] host).
- Suggests lack of **application whitelisting** or **download restrictions**.

3. Weak Browser Security Controls

- No policy restricting Chrome extensions, allowing adware/hijackers to install and sync across profiles.

4. Poor Endpoint Governance

- Users are running manual scans themselves rather than centrally managed security tools.
- Threats not quarantined on one system, leaving them active.

5. Lack of Centralized IT/Security Oversight

- No indication of centralized monitoring, patching, or endpoint protection.
- Users likely have **local admin rights**, enabling them to install whatever they want.

Recommendations

- **Deploy centrally managed endpoint protection (EDR/antivirus)** with real-time protection.
- **Restrict user privileges** (limit local admin rights).
- **Application whitelisting** to prevent unauthorized software installations.
- **Browser extension management policies** (block risky Chrome add-ons).
- **Security awareness training** to address unsafe download and installation habits.
- **Regular automated scans & patching** controlled by IT, not reliant on employees.

Would you like me to draft this into a **formal incident report** (executive-style summary + technical findings + recommendations), or would you prefer a **shorter risk assessment memo** for management?

Sources