Was sind Living-off-the-Land-(LotL)-Angriffe, und warum versagt Anwendungs-Whitelisting gegen sie?

Kurze Antwort: Living-off-the-Land-Angriffe nutzen Software, die bereits installiert und bereits vertrauenswürdig ist – Systemhilfsprogramme, Administrationstools, Browser – anstatt neue schädliche Dateien einzuschleusen. Anwendungs-Whitelisting versagt, weil der Angreifer innerhalb von Programmen agiert, die die Whitelist ausdrücklich zulässt.

Die Whitelist wird zur Zielliste

Anwendungs-Whitelisting beantwortet eine einzige Frage: „Darf diese Datei ausgeführt werden?“ Moderne Angriffstechniken machen diese Frage bedeutungslos. Wenn Angreifer schädlichen Code im Arbeitsspeicher eines zugelassenen Prozesses verstecken, hat die Whitelist bereits zugestimmt. In der Praxis verrät eine Whitelist einem Angreifer genau, in welchen Prozessen er sich am sichersten verstecken kann.

Die bessere Frage

Wirksame Verteidigung muss sich von *„Ist diese Datei erlaubt?“* zu *„Was tut dieser Code gerade tatsächlich?“* weiterentwickeln. Das erfordert die Untersuchung von Verhalten und Arbeitsspeicher auf Kernel-Ebene, wo die tatsächliche Aktivität sichtbar ist – nicht auf Dateiebene, die der Angreifer bereits umgangen hat.

Revision #1
Created 2026-07-24 04:26:51 UTC by Dennis Underwood
Updated 2026-07-24 04:26:51 UTC by Dennis Underwood