AIRLOCK DIGITAL

airlockdigital.com

Stop Living off the Land Attacks

With Airlock Digital Application Control (Allowlisting)

Prevent LOTL Attacks with Application Allowlisting

Living off the land (LOTL) attack techniques, or fileless malware, present a formidable challenge to modern organizations' cybersecurity tech stacks and enterprise strategies. So much so that the 'Five Eyes' alliance (the United States, United Kingdom, Canada, Australia and New Zealand) warned of their active use by state sponsored actors and acknowledged their emergence in the broader cyber threat environment.

How do living off the land attacks occur?

Attackers often gain initial access to an environment using techniques such as exploit kits, hijacked native tools, memory-only malware or stolen credentials. They commonly use fileless malware or LOLBin techniques (that leverage legitimate system components to hide malicious activity) to perpetrate their attacks.

These techniques are preferred because they rely on native system tools and legitimate software, and do not execute code on disk. As a result, they are hard to detect, including by traditional anti-malware products.

Why are LOTL attacks so successful?

Distinguishing malicious LOTL activity from legitimate behavior can challenge organizations in a range of ways. These include:

- Attacks look like normal system behavior and can be 'lost in the noise'
- LOLBin attacks are often novel and change rapidly to avoid identification
- Verbose and highly tuned logging is required to capture behaviors in order to identify living off the land attacks

Preventing LOTL attacks with Airlock Digital

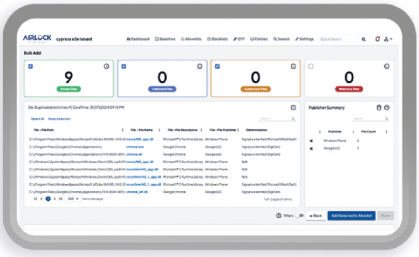
Fortifying an organization's defenses against living off the land attacks is a key priority for cybersecurity professionals. Application control (allowlisting) is a pivotal strategy in this battle, a fact acknowledged by the Five Eyes alliance in its joint guidance on identifying and mitigating these attacks.

Because living off the land attacks leverage legitimate functionality that exists within organizations to achieve nefarious objectives, Airlock Digital is ideally positioned to help minimize the threat posed by these types of attacks.

Our application control (allowlisting) solution makes it easy for an organization to determine whether that functionality is in use in its environment and if so, block the supporting program from executing. With that functionality unable to execute, malicious actors cannot abuse it with living off the land techniques. This greatly reduces a significant risk to people, data and operations.

Airlock Digital application control (allowlisting) is a critical addition to your cybersecurity stack

Incorporating Airlock Digital's application control (allowlisting) solution into your endpoint cybersecurity stack can help your organization prevent the threat presented by LOTL techniques. Our allowlisting solution, can help you proactively stay ahead of advanced and traditional digital threats. Book a demo today to find out how Airlock Digital can improve the security posture of your organization.



AIRLOCK DIGITAL

AVAILABLE FOR

Windows™ | Linux® | macOS™