[CS-TR-24-1002] Living off the Land, But in Your Systems

Malware-free attacks, a hallmark of Living Off the Land (LoTL) strategies, underscore the importance of user and entity behavior analytics (UEBA) for timely detection. Cyber threat actors frequently exploit remote access and administration tools, scripting tools, and penetration testing tools in LoTL attacks. CriticalStart's Cyber Threat Intelligence (CTI) analysts have tracked several categories of LoTL tools detected and contained by CriticalStart's Risk & Security Operations Center (RSOC) analysts from January 2024 to date. These tools, while legitimate for IT operations, can be misused by attackers in compromised environments to execute hands-on-keyboard attacks and evade detection. Addressing the challenges posed by LoTL attacks is essential for organizations to bolster their cybersecurity defenses against threat actors who leverage legitimate tools and processes.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.
