Transforming Weakness into Strength: Improving Unreliable Malware Detection Methods

Pavel Novák, MSc.
Department of Computer Systems and Communications
Faculty of Informatics of the Masaryk University
Brno, Czech Republic

Malware, particularly ransomware, has been a persistent threat for many years, despite ongoing efforts by researchers to develop effective detection methods. One common defense against ransomware is data backup—not only of raw data but also of entire virtual systems. However, backup strategies face their own challenges, with the primary concern being the durability and retention of backups. Many companies do not maintain a large number of backups, making them vulnerable to patient and skilled attackers who can remain undetected long enough to compromise all backup copies. During this period, various suspicious activities initiated by the malware may occur, which, when analyzed in context, could indicate an ongoing infection. The solution me and my colleagues are working on is to identify such suspicious events, gather them, and compare them against known malware patterns, adding another layer of defense against threat actors.