SUPPLY CHAIN ATTACKS: DEVELOPING COUNTERING CAPACITY BY EVALUATING SYSTEM VULNERABILITIES FROM A HACKING PERSPECTIVE

Taha TOKGÖZ, Dilara Berrak TARHAN, Olcay OKUN

Abstract: As technology advances rapidly, cyber threats are also becoming increasingly sophisticated. In particular, the complex techniques employed by threat actors in malware can overwhelm existing static malware analysis tools and complicate the analysis process. This paper proposes the use of the Model Context Protocol (MCP) as a novel approach to static malware analysis. MCP aims to enhance analysis accuracy and efficiency by evaluating the code obtained through malware reverse engineering not only syntactically but also functionally and contextually. It leverages Large Language Models (LLMs) to automatically analyze the relationships between different code components and identify potential malicious behavior patterns. To provide a concrete example, a case study was conducted on a ransomware sample. The results demonstrated that the MCP approach can detect obfuscated or hidden functionalities, such as file encryption methods, more quickly and accurately compared to manual inspections. The findings reveal that using MCP can significantly enhance manual review capabilities with existing static analysis tools and significantly shorten the overall analysis process.

Keywords: Cyber Security, Malware Analysis, MCP (Model Context Protocol), LLM (Large Language Model), Ransomware

TEDARİK ZİNCİRİ SALDIRILARI: SİSTEM AÇIKLARININ HACKLEME PERPEKTİFİNDE DEĞERLENDİRLEREK KARŞI KOYMA KAPASİTESİ GELİŞTİRİLMESİ

Özet: Dijitalleşmenin hız kazanmasıyla birlikte kurumsal ekosistemler giderek daha karmaşık hâle gelmekte ve bu durum siber tehditlerin ölçeğini, etkisini ve karmaşıklığını artırmaktadır. Özellikle tedarik zincirlerine yönelik siber saldırılar, yalnızca hedef organizasyonları değil, ekosistem içinde yer alan yüzlerce kurumu etkileyerek sistematik riskler oluşturmaktadır. Bu çalışmada, son beş yıl içinde gerçekleşmiş tedarik zinciri saldırıları detaylı olarak incelenmiş, bu saldırılarda kullanılan yöntemler sınıflandırılmış ve kurumların saldırılara karşı koyma kapasitelerini geliştirebilmeleri için yönetim bilişim sistemleri (YBS) tabanlı çözümler önerilmiştir. Ayrıca, zararlı yazılım analizine yönelik olarak Model Context Protocol (MCP) yaklaşımı önerilmiş ve LLM tabanlı analizlerin, manuel analiz yöntemlerine kıyasla hız ve doğruluk açısından önemli avantajlar sağladığı ortaya konmuştur.