Economic Aspects of Ransomware

Lukas Vaclavik[a,*]

[a] *Brno University of Technology, Faculty of Business and Management, Kolejní 2906/4, 612 00 Brno, Czech Republic*

Abstract

Purpose of the article The aim of this article is to conduct a search of current scientific knowledge in the field of extortion software ransomware and its economic aspects.

Methodology/methods The paper will explain the principle of ransomware, the motivation of the use of this kind of malicious software by attackers and other aspects on the basis of scientific articles and professional literature on this issue. Emphasis will be placed on the economic nature of ransomware from the perspective of both the attacker and the victim. Based on relevant publicly available data from around the world, an evaluation of the current situation and further developments will be made.

Scientific aim Explanation the principle of ransomware with emphasis on its economic aspects from the perspective of the attacker and the victim and their evaluation.

Findings Ransomware causes huge tens of billions of dollars in damage around the world every year, and the trend is growing. Due to the large percentage of victims who pay the required ransom, the attackers receive financial flows, which further motivate them to continue their activities. However, from the point of view of the affected individuals or organizations, decision-making is not easy, as re-access to its important data is usually crucial. The situation is often made even more complicated by the absence of key data backups or the fear of damaging a business name or honor.

Conclusions Ransomware has become one of the biggest threats to cyberspace in recent years. Due to the expansion of the Internet and cloud computing, this model of crime is widely used. It creates an ideal and comfortable environment for the spread of this type of malware. Data is an increasingly important and valuable commodity for potential end-user, business or government victims. Their loss or theft carries certain risks and damages, which usually outweigh the required payment for their re-opening. From the point of view of the victims, there are two components of economic impacts: the consequences of the attack (business recovery) and the costs of building a defence. Among other things, the attackers are favoured by the abundant spread of cryptocurrencies, which provides them with the necessary anonymity and fundamentally limits the possibilities of security forces to catch them.

Keywords: Ransomware, Economics of ransomware, Cybercrime, Malware, Cybersecurity

JEL Classification: K42, L86, M21

[*] Corresponding author. Tel.: +420 54114 2601
E-mail address: xvacla21@vutbr.cz