Understanding Corporate Ransomware – A Case Study in the Nordics

Emil Larsson[1,2][0009−0008−2442−4058] and Meiko Jensen[1][0009−0003−2397−9813]

[1] Karlstad University, Universitetsgatan 2, 65188 Karlstad, Sweden
[2] Swedish Defence University, Drottning Kristinas väg 37, 11428 Stockholm, Sweden
{emil.larsson|meiko.jensen}@kau.se

Abstract. Ransomware is continuously evolving and has recently seen record-breaking payouts. This paper describes developments in corporate ransomware which have contributed to this continued rise. It provides an interdisciplinary case study of a ransomware campaign conducted in northern Europe during 2023 and 2024. We argue that underlying factors, including the broad rollout of personal cloud backups, have caused modern ransomware groups to shift towards expending more effort per attack in order to attack bigger targets. We perform an analysis of such an attack using a combination of internal and open sources, as well as using forensic techniques. The analysis shows how the attackers approach high-value targets, use both traditional crypto-ransomware tools and hacking, and utilize multiple avenues of extortion to negotiate the highest possible ransom.

Keywords: ransomware · double extortion · case study · Akira · malware.