NAPADI Z IZSILJEVALSKIMI VIRUSI NA INFORMACIJSKE SISTEME DRŽAVNE UPRAVE

Boštjan Tavčar[1]
[1] Ministrstvo za obrambo, Uprava RS za zaščito in reševanje, 1000 Ljubljana
bostjan.tavcar@urszr.si

Referat opisuje širšo problematiko napadov z izsiljevalskimi virusi na omrežja državne uprave in državnih podjetij, specifičnost teh napadov, ekonomski model in motive, dejanske možnosti zgodnje zaznave napadov ter ukrepanje ob napadih. Predstavljeni bodo trendi v razvoju orodij, ki se jih poslužujejo napadalci s poudarkom na uporabi umetne inteligence. Na kratko bo predstavljena študija primera nekaj tovrstnih napadov. Ena od študij primera, napad na Upravo RS za zaščito in reševanje, je bila širše predstavljena na konferenci HEK.SI, https://www.youtube.com/watch?v=cAo-VFWPG7I.

Ključne besede: Kibernetski napad, izsiljevalski virusi, QILIN, hekerska skupina, varnostna dokumentacija, URSIV

ATTACKS WITH EXTORTION VIRUSES ON STATE ADMINISTRATION INFORMATION SYSTEMS

The paper describes the broader issue of attacks with ransomware on the networks of the state administration and state-owned companies, the specificity of these attacks, the economic model and motives, the actual possibilities of early detection of attacks, and action in the event of attacks. Trends in the development of tools used by attackers will be presented, emphasising the use of artificial intelligence. A case study of some such attacks will be briefly presented. One of the case studies, the attack on the Administration for Civil Protection and Disaster Relief, was widely presented at the HEK.SI conference, https://www.youtube.com/watch?v=cAo-VFWPG7I.

Keywords: Cyber-attack, ransomware, QILIN, hacker group, security documentation, URSIV