BitPaymer Ransomware Paralyzes IT Systems of the Alaskan Town | SOC Prime

By Eugene Tkachenko

Published: 2018-08-01 · Archived: 2026-04-05 14:50:04 UTC

Delaware, USA – August 1, 2018 – Another Ransomware attack practically froze the Matanuska-Susitna borough. The incident occurred on Tuesday, July 24, and the network did not fully recover so far. Attackers used BitPaymer Ransomware to encrypt 500 computers and 120 servers connected to government networks. According to official representatives of the Borough, no sensitive data was stolen, and the attempt to encrypt all the backup copies failed. In spite of this, the infrastructure restoration is still ongoing, the phone server was launched only this Monday, and the mail server is still being restored. IT security staff of Matanuska-Susitna reported that malware infected the network on May 3, and on July 17 it was first detected by an antivirus solution. However, the antivirus was able to clean the systems only from the Trojan module of BitPaymer, and when IT staff attempted to remove ransomware components manually, BitPaymer encrypted all systems. This ransomware appeared a year ago and security researchers suggest that its creators are the same who operate the Necurs botnet and spread Dridex banking trojan.

Furthermore, researchers from Sophos published a report on SamSam Ransomware activity. Experts assume that the development of malware and all attacks are conducted by a lone cybercriminal, who managed to get almost $6 million in ransom payments from 233 victims. According to Sophos, this cybercriminal infects one organization per day, and one in four pays a ransom. To detect the attack at early stages, you can use SIEM with Ransomware Hunter use case, which helps to discover suspicious connections and attempts to communicate with Ransomware C&C servers.
