# Ransomware extortion affecting local administrations

Reference: Memo [190604-2] Date: 04/06/2019 - Version: 1.0
Keywords: extortion, disruption, ransomware, government, public services
Sources: publicly available information

## Key Points

- In the US, the city of Baltimore's IT infrastructure suffered a ransomware attack that created disruption in public services.
- The attack was most likely executed with the use of a ransomware dubbed Robbinhood.
- Similar ransomware attacks against local administrations or public services have taken place across the US and globally.

## Summary

On May 7, hackers infected about 10 000 of Baltimore city government's computers with an aggressive form of ransomware. The criminals responsible demanded 13 Bitcoin (approximately 102.420,94 Euro) to unlock all data or 3 Bitcoin to release specific systems ahead of a deadline, which has passed. The authorities refused to pay the ransom, which resulted in service disruption. Baltimore mayor also said "[they are] going to get [the threat actors] and punish them to the fullest extent of the law." Consequently, local residents have been unable to pay utility bills, parking tickets and some taxes online. In addition, public servants have been unable to send or receive emails from their normal accounts.

The situation became more complex when public servants, in the absence of email service from the city systems, tried to open personal Gmail accounts. Due to a security procedure, Google blocked the creation of these accounts since they were considered as automatically created mailboxes that may be used for advertising or other malicious purposes. In an emailed statement to the US media outlet Fox News Google's spokesman said: "We have restored access to the Gmail accounts for the Baltimore city officials. Our automated security systems disabled the accounts due to the bulk creation of multiple consumer Gmail accounts from the same network." Gmail distinguishes between individual users and users in businesses and other organisations, requiring the latter to pay for the service. Another news outlet comment based on an announcement from the mayor's office that Google's systems deemed the city officials to be part of an organisation, and shut down the temporary accounts. Emails to the city health department, city council aides, and the mayor's office bounced on Thursday 23th of May.

An article in the New York Times claimed that the US National Security Authority's (NSA) leaked EternalBlue exploit was used to spread the ransomware infection in the network. This led to a Maryland congressman asking questions about the NSA's responsibility in making the ransomware attack possible. The NSA declined to comment the matter.

## Analysis

In Baltimore, the ransomware used by attackers is dubbed RobbinHood, a recent player in the ransomware scene. This ransomware is not being distributed through spam but rather through other methods, which could include hacked remote desktop services or other trojans that provide access to the attackers. RobbinHood disconnects all network shares from the infected computer. This could be the cause of service disruption in the incident of the city of Baltimore.

Similar extortion / ransomware attacks against local administration or public services have taken place across the US. For example, in September 2018, hackers targeted the port of San Diego in a ransomware attack that disrupted the agency's IT systems. In March 2019, a ransomware attack hit the computers of Jackson County, Georgia, reducing government activity to a crawl until officials decided to pay cybercriminals $400,000 in exchange for the file decryption key. In April 2019, the Robbinhood ransomware attack hit government computers in Greenville, North Carolina. A spokesperson for Greenville told the Wall Street Journal that the city never wound up paying, and that while its systems aren't entirely restored, "all of our major technology needs are now being met."

Historically, local governments and public services were among the first organisations to be hit with ransomware. The first known case was in November 2013, when the Swansea Police Department in Massachusetts was infected with CryptoLocker.

Globally, other public services were also deeply affected by ransomware, such as the WannaCry assault that disrupted the UK's national health service in 2017.

Although local administrations do not pay ransoms nearly as frequently as other targets, they generate outsized media coverage because of the effect these attacks have on the functioning of essential infrastructure and processes. This possibly creates a perception among attackers that these are potentially profitable targets. Statistics show that although government agencies are less likely to pay the ransom than other victims, there is still an almost one in five chance that an attacker will get paid.