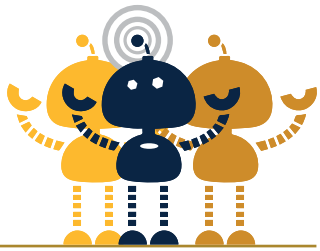
Ransomware Attacks Targeting Municipalities



By Devin Chwastyk, Esq. & Chase J. Wright, Esq., McNees Wallace & Nurick LLC

On May 7, 2019, the city of Baltimore discovered that its integral systems were the subject of a ransomware attack, breaching the City's phone systems, emails, documents and critical operational databases, affecting roughly 10,000 City computers.

The City notified the F.B.I. and took offline as many other systems as possible to prevent the spread of the cyberattack, but not before the malicious software locked and encrypted many of the City's systems.

The hackers responsible for the attack demanded 13 bitcoins – valued at approximately $100,000 – as ransom, to release the City's inaccessible databases and operational tools. Bitcoin is a cryptocurrency, without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

In a move intended to disincentive future attacks, Baltimore rejected hackers' demands and did not pay the ransom.

Shortly after the Baltimore attack, officials announced that they were the victim of a RobinHood ransomware attack. Ransomware is a type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems.

A ransomware attack involves malicious software infecting a computer, which then encrypts a victim's data and demands a ransom to restore access (usually within a short timeframe). RobinHood is a new variant of ransomware that uses a sophisticated attack method and has mainly targeted municipalities.

Lasting Damage

Since the discovery of the attack in Baltimore, the City has still not fully recovered, and central data remains inaccessible, seemingly in perpetuity. The lasting damage that the ransomware attack will have on the City is already one for the history books, as the mounting costs continue to multiply.

The City's budget office estimates that the attack will cost over $18.2 million in costs and lost revenue, with an even larger impact on the local economy due to the City's lack of communication and operation in many departments. City Finance Director Henry Raymond estimates that the City has already spent $10 million in recovery and forensic expenses, and it is expected to lose over $8 million more in lost revenue.

In the weeks following the Baltimore attack, the City's head of information security acknowledged and apologized for the City's slow response. In Baltimore, out-of-date computer systems and lack of experience and resources helped create a more susceptible environment to this type of attack.

Although newer to the public eye, ransomware attacks on municipalities are no longer an outlier. Recent studies show that over 170 ransomware attacks have hit U.S. cities and local governments in the past six years. In 2018 alone, over 50 ransomware attacks have targeted local governments, and at least 21 similar incidents have already occurred this year.

One of the most recent attacks hit the Palm Beach, Fla., a suburb of Riviera Beach, which resulted in City agreeing to pay 65 bitcoins (approximately $600,000) in ransom to retrieve the city's encrypted records.

Counter to the approach taken in the cities of Baltimore and Atlanta, the Riviera Beach City Council decided to pay the ransom outright, as opposed to ignoring the hackers and attempting to retrieve the records themselves. Following the attack, the city council has already approved spending approximately $1 million on new computers and hardware.

The recent increase in these attacks can be attributed to multiple factors.

For one, unlike large corporations that have deep pockets to invest in comprehensive cyber protection programs, local governments often lack those fiscal resources to devote to proactive measures. This lack of financial resources limits municipalities' ability to obtain and retain high-talent information technology (IT) professionals and invest in the latest technology. And with the rise of cryptocurrencies like Bitcoin, payment of cyber-ransom is virtually impossible to track.

Proactive steps

Municipalities around the U.S. can learn from the events in Baltimore, Atlanta, and Riviera Beach and should take proactive steps to patch similar vulnerabilities. Such measures include increasing IT budgets; consulting with data security professionals; investing in cybersecurity programs; properly training staff to detect malicious content; updating computer systems; and implementing policies and procedures to prevent slow responses in the event of such an attack.

Additionally, all municipalities should consider whether they have adequate cyber insurance policies to cover for direct and indirect costs in the event of such an incident.

These are just some of the latest examples of the threat facing municipalities around the country. Preparation is the key to building safeguards to fend off a similar attack in your local government.

About the authors: *Devin Chwastyk, Esq., is the chair of the Privacy & Data Security Group at McNees Wallace & Nurick. He can be reached at dchwastyk@mwn.com. Chase J. Wright, Esq., is an associate at the firm and is a member of the Security and Data Privacy Group. He can be reached at chasewright@mcneeslaw.com. Learn more about McNees Wallace & Nurick at www.mcneeslaw.com.*