Case study

City shakedown

A targeted extortion attack leaves a local government in a predicament

Public entities tend to have tighter budgets than organizations operating in the private sector, and this can have an impact on their ability to invest in IT security. As a result, they are becoming an increasingly attractive target for cybercriminals.

For example, in 2018, Atlanta's municipal government was hit by an outbreak of SamSam ransomware that brought down their computer systems for a number of days, resulting in numerous municipal services being impaired and a bill in the region of $2.7 million to recover from the incident. More recently, in May 2019, Baltimore's government fell victim to a ransomware attack, causing widespread disruption.

Whether these were targeted or merely opportunistic attacks remains unclear, but what is undoubtedly true is that the nature of cyber extortion events has changed over recent years. In the past, ransomware was often distributed widely through mass-email campaigns without a specific target in mind, in the hope that a small number of individuals and organizations would be caught out. Actual ransom amounts demanded were fairly modest – typically sitting around $300.

However, as ransomware has become an established method of attack, end point protection systems have become increasingly effective at blocking the ransomware and there is greater awareness about the dangers of clicking on suspicious links. To make up for this, many cybercriminals are changing their methods and instead of adopting a scatter-gun approach, they are now handpicking vulnerable organizations and encrypting their data. And because they have a better understanding of their victims, these cybercriminals are also raising their demands accordingly, with many requesting amounts in excess of $50,000.

One of our policyholders affected by this type of incident was a local government for a small city with a population below 100,000. The city's responsibilities include public transportation, parking, social housing, parks and recreation facilities, and recycling and waste disposal, to name just a few.

Brute force attack uncovers easy-to-guess passwords

The incident began when a hacker was able to gain access to the city's computer systems via the Remote Desktop Protocol (RDP). RDP allows remote users to connect to the desktop of another computer through a network connection and is **typically used by organizations to allow employees to access their networks while they are away from the office.** Unfortunately, the port that the city used for RDP access was open to the internet.

A brute force attack is where a hacker uses a computer program to crack passwords by trying every possible password combination in quick succession.

Having identified this open port as a way of gaining access to the city's computer systems, the hacker initiated a brute force attack against the local administrator account by running a computer program to crack passwords by trying every possible password combination in quick succession. Unfortunately, the password for this local administrator account was commonly used and had been set up as a default for new accounts but had never been changed. With the password lacking complexity, the hacker's brute force program had cracked the password within six days.

Upon logging into the local administrator account, the hacker made use of a password-scraping tool, which **allowed them to obtain login credentials for other accounts on the network with greater access privileges.** From here, they used a scanning tool to gain information about what was on the insured's network. In particular, the hacker appeared to be attempting to find the location of any back-ups in the knowledge that if they could encrypt the city's back-ups, they would have more leverage when extracting the ransom payment. In this case, **the city had failed to save their back-ups externally,** allowing the hacker to locate them while searching the network.

The hacker now went on to the next stage of the attack. Using a strain of ransomware, the hacker began to encrypt the city's data, applications and back-ups, leaving them with a ransom note demanding 15 bitcoins (equivalent to over $60,000 at the time of the attack) in exchange for the decryption key.

Ransomware research leads to breakthrough

Upon discovering the ransom note, the city's IT staff initially tried to deal with the incident themselves, but with the back-ups encrypted, **they soon realized that any attempt to decrypt the affected servers without the decryption key would be unsuccessful.**

Fortunately for the city, the attack happened over a weekend, but they were well aware that if they didn't regain access to their data and applications quickly, their ability to provide services would be severely impacted. Without access to their computers, **employees would be unable to respond to email queries and complaints from city residents** and certain processes, such as applications for social housing or building permits, would all have to be carried out manually. Furthermore, with online payment systems rendered inaccessible, city residents would be unable to pay things like water bills or parking tickets.

It was therefore essential to act quickly and it was at this point that the incident was notified to CFC. With the back-ups unavailable, our claims team explored the other options available to the policyholder. Utilizing the information contained on the ransom note, our threat intelligence team figured out which ransomware variant had been used to carry out the attack. It transpired that an ethical hacker had found flaws in this variant's encryption algorithms and had managed to create a tool that could successfully decrypt affected files. With this tool, our team managed to decrypt the servers without having to pay the ransom demand or cause major disruption to public services.

Questions emerge over hacker's access of sensitive data

The city had now regained access to their computer systems, but there was still a question mark over whether there had been a data breach. **The city stored sensitive information on their computer systems relating not only to employees but to a large number of city residents too,** and if this had been accessed or exfiltrated during the course of the attack, a large-scale notification process would have to be carried out. In most cases involving automated ransomware, sensitive data isn't accessed. But as this incident did not involve automated ransomware and appeared to have been a targeted attack, it was initially unclear whether the hacker had accessed the city's sensitive data or not.

In order to address this issue, **we engaged one of our forensic partners** to determine the root cause of the attack and discover what exactly the hacker had done while they had access to the insured's computer systems. This was a significant undertaking as the city's network was made up of over 700 connected devices, with nearly 500 users across 20 sites. After several weeks of investigations, it was determined that the hacker had not accessed any sensitive information, and this was based on three factors: there was no evidence of large zip files being created, which are typically seen in cases of data exfiltration; the artifacts on the system relating to the attack appeared to be limited to harvesting password credentials, locating back-ups and encrypting files; and **the amount of time the hacker spent on the system was not deemed to be long enough to carry out meaningful data exfiltration.**

Nevertheless, the forensic investigation did uncover a number of pre-existing malware infections that were unrelated to the attack. Our forensics partner conducted an analysis of these malware strains and confirmed that they were not known to be capable of accessing or stealing data and later utilized threat hunting software to remove the malware from the network.

The city may not have had to carry out notifications, but the cost of the attack was still significant. The cost of the forensic investigation and security assessment alone came to $180,541. This came on top of the $15,000 in legal fees and $5,000 to engage a crisis communications consultancy to deal with a media inquiry about the attack, bringing the total claim cost to $200,541.

Large networks and sensitive data put public entities at risk

This claim highlights a few key points. Firstly, it demonstrates how important it is to work with an experienced cyber insurer with a dedicated incident response team in place. **When you buy a cyber policy, you are not just buying a promise to pay valid claims.** You are also paying for a service to help and advise you when things go wrong. This includes gaining access to threat intelligence that many organizations may be unaware of.

> Malicious actors are constantly seeking out vulnerabilities to exploit, and an open port used for RDP is one of the most common that they look out for.

In this case, our incident response team identified the ransomware variant used in the attack, researched it and found a decryption tool to counter the attack, enabling the insured to regain access to their computer systems without giving in to the hacker's demand or impairing vital public services.

Secondly, if businesses are using the Remote Desktop Protocol, then they should make sure that it is not exposed directly to the internet and make use of a virtual private network (VPN) instead. Malicious actors are constantly seeking out vulnerabilities to exploit, and an open port used for RDP is one of the most common that they look out for. In addition, businesses should ensure that they have good password hygiene in place and enable two-factor authentication to reduce the risk of attacks like this from happening.

Finally, it reveals how vulnerable public entities are to sizeable losses like this. Because public entities are primarily financed by taxation or central government funding, they do not have the business interruption risk that most private organizations face. However, due to the fact **public entities will typically operate large networks with significant amounts of sensitive data,** they can incur substantial system damage, forensic investigation and notification costs in the event of a cyber attack, illustrating the importance of cyber insurance for this industry sector. ●