RANSOMWARE AND MUNICIPAL WEBSITES

A PREVENTION AND PROTECTION STRATEGY

360

Ransomware and Municipal Websites:
A Prevention and Protection Strategy

presented by: 360Civic

Audience
Public officials, communication officers, online security personnel and managers responsible for public sector and municipal websites.

INTRODUCTION

This whitepaper will focus on the recent municipality-targeted ransomware attacks, their respective payloads, local government specific mitigation methodologies and remediation strategies. It is not intended as legal advisement, but as a core reference document to defer to for tools and holistic guidance in safeguarding against ransomware attacks, including specific attack vectors.

WHAT IS RANSOMWARE?

Ransomware is computer code, or malware, that is deployed into a network with the intent of disabling systems. Methods of deployment vary, but it usually gains access when someone connected to the network clicks on a malicious link or opens a file in a phishing email. Once inside, ransomware self-proliferates and hides or encrypts data inside the environment, rendering it inaccessible.

After a system has been crippled, the attacker will make contact and offer a key that will unlock any blocked data – for a price. Payment is requested in cryptocurrency such as Bitcoin, as this makes the transfer of funds harder to trace.

The first ransomware attack dates back to 1989, the era of the floppy disk. But it wasn't until about ten years ago that attacks became more commonplace, and began utilizing more sophisticated encryption algorithms such as RSA encryption.

THE REALITY OF RANSOMWARE IN THE PUBLIC SECTOR

In June 2018, per current trends, the Wall Street Journal foresaw that 38% of all public sector organizations in the United States would experience a ransomware attack in 2018. That's up from 31% the previous year, and just 13% in 2016. In actuality, as of November 2018, 42% of all public sector organizations in the Unites States have been victimized by ransomware. Per Christopher Mitchell, Houston's Chief Information Security Official, "Compromise is inevitable."

There is currently no greater security challenge to municipal websites, school district sites and public utility sites than ransomware. The rapid increase in successful attacks can be attributed to cybercriminals' accurate knowledge base of the inherent vulnerabilities within municipality networks, and their strategic exploitation.

The most common ransomware variants today have names like CryptoLocker, SamSam and WannaCry. New variants will continue to emerge, but right now the options available to thieves are already so abundant that further innovation is not yet required.

Perhaps the most disturbing sign of how ransomware has become mainstream is the emergence of Ransomware-as-a-Service (RaaS). Now, those without programming skills or hacking experience can get in on the extortion racket by purchasing malicious code online. If they are successful in pulling off a ransomware attack, they provide the author of the code with a cut of the ransom.

The breadth and seriousness of the problem can be illustrated by a closer look at some of the specific attacks that have occurred in just the previous 12 months:

Atlanta, Georgia
The city's municipal computer systems were attacked, resulting in postponed court dates and a temporary switch to typewriters for conducting city business. The attackers demanded a $51,000 ransom to restore system access. Local officials urged any residents who have done business with the city to make sure their bank accounts have not been compromised.

Riverside County, Ohio
The Riverside Fire and Police Department fell victim to not one, but two ransomware attacks. The first infection occurred in April, effectively encrypting ten months of investigative work specific to active investigations.

The second attack in May was much less effective due to precautionary measures put in place, including a newly installed backup system, by The Riverside Fire and Police after the first infection. Officials said the second ransomware infection only locked up data for the last eight hours of work, and the department fully recovered.

This isn't the first incident of ransomware undermining police servers; police in Cockrell Hill, Texas suffered a similar breach in which they lost eight years of evidence.

Baltimore, Maryland
The city's 911 dispatch system was breached, shutting down computer-aided dispatches for potentially life-saving situations for 36 hours. Six days of data were permanently lost. The cost of recovery: $20,000.

San Diego, California
Computers and IT systems at the Port of San Diego had to be taken offline

for weeks after a ransomware attack. Payment in Bitcoin was demanded for a key to decrypt files that were being held hostage. Both the FBI and the Department of Homeland Security joined the investigation.

Spring Hill, Tennessee

It's not just major cities that are targeted for ransomware: Spring Hill, Tennessee, population 38,000, had its servers locked by a group demanding $250,000 – five times the amount requested in the Atlanta attack. All online credit or debit card payments were temporarily suspended for several days during the recovery. The ransom was not paid, and restoration efforts to the city's servers may cost more than $100,000.

Madison County, Indiana

Six hundred county computers and 75 servers were infected with ransomware. The county, following the advice of its insurance carrier, paid a $21,000 ransom to restore services.

Matanuska-Susitna, Alaska

Government officials declared a state of emergency after a ransomware attack infected nearly all of the borough's 500 workstations and 120 of its 150 servers, including its domain, email (Exchange), and even its backup and disaster recovery servers. Mat-Su Borough IT Director Eric Wyatt estimated recovery costs from the infection would not exceed $750,000.

Rockport, Maine

After a backup server was compromised, city officials discovered they could not open files on their computers. The hacker requested a surprisingly modest sum of $1,200 in Bitcoin for the codes to unlock files, and even provided a "customer service" chat window with tips on how to acquire cryptocurrency. Rockport officials rejected the offer. It cost this city of 3,400 about $10,000 for restoration of its systems, as well as $25,000 to install security improvements.

Onslow, North Carolina

Targeted by the Ryuk ransomware variant, Onslow Water and Sewer Authority (ONWASA) was the victim of a highly targeted cyber crime scheme that was executed after the county's infrastructure had been significantly damaged by Hurricane Florence. As ONWASA's entire internal computer system, including servers and personal computers, were infected by ransomware, all activities requiring computers (service orders, account creation and payments) had to be performed manually. Although ONWASA did not disclose the ransom amount demanded or the costs involved in rebuilding IT assets, the Ryuk variant has been highly profitable with ransoms in the six-figure range, the highest seen being $320,000.

While these and countless other occurrences suggest that cities are losing the war against ransomware, it is also true that the overwhelming majority of attempted breaches are successfully thwarted.

Billions of instances of malicious traffic are blocked every year by city and state IT agencies. The problem is they just keep coming. The city of Fort Worth, Texas has reported about 15,000 intrusion attempts every day. Just one has to get through to do damage.

As one network security expert commented, "We're outgunned."

PUBLIC SECTOR SITES: THE MOST APPEALING TARGETS

Almost all ransomware attacks are not premeditated. Hackers search for vulnerabilities wherever they can be found, whether it's a small village in Alaska or a major metropolitan city. While private sector businesses have also faced ransomware attacks, the public sector has proved a much more inviting target for obvious reasons:

All That Lovely Data

Local governments are attractive targets for cybercriminals for the valuable data they store, and the fact that many are connected to state systems and big networks, where the quantity and quality of data is likely to be greater. And in a few cases with small jurisdictions, local governments are attractive targets because some are willing to pay the extortion fee to regain access to their records.

The Stakes are Higher

An attack on a retailer can stop customers from buying items online, and perhaps obtain data on credit cards used to make purchases. But when a city's systems are compromised, it can disrupt police departments, transportation systems, courts, libraries, tax collection and emergency services. Such incidents can erode public trust, impact the reputation of elected officials and lower a municipality's credit rating. That brings a sense of urgency to the crisis that is more likely to result in a ransom being paid.

Vulnerability

Budget cuts in local governments have resulted in reductions in staff and resources, including those assigned to maintain IT safety. An internal study in the state of Texas found that just 200 out of 1,100 cities had even one staff member dedicated to cybersecurity. Personnel and system upgrades cost money, and those that don't pay now may find the price much higher after an attack.

The Attacks Have Worked

One of the most disturbing reasons hackers target municipalities is that often, too often, they are successful. The FBI has warned against dealing with a hacker, since "some individuals or organizations are never provided with decryption keys after paying a ransom." But the city of Leeds, Alabama paid $12,000 to regain access to their systems, and a school district in Leominster, Massachusetts paid $10,000 to get their computers unlocked.

HOW CAN PUBLIC SECTOR ENTITIES PROTECT THEMSELVES?

As one public official in Spring Hill commented after the attack there, "paper and pencil seem to work pretty well against those kinds of things."

However, as that solution is no longer practical, some plan of action is essential.

A logical place to start is by identifying the vulnerabilities in the public sector site that make ransomware attacks possible. The first line of defense should not require a large investment in technology or personnel – all it takes is vigilance on the part of anyone with access to the municipal online network.

How often do employees have to be told to not click on a suspicious email? Since most phishing emails are now ransomware, a cybersecurity awareness and education program is one of the most effective steps a public sector entity can take. Make sure all personnel (employees, contractors, elected officials) understand how to spot phishing, and how to maintain the habit of smart password management. And if someone slips and does click on something hazardous, stress the importance of reporting it immediately, which can help to limit the damage.

The next key to combating a ransomware attack is to make sure all of the data on a municipal website is backed up. Such backups are only effective if they are continuous (some cloud services run 15-minute interval backups) and if the data is saved on a system that is either not always online or requires authentication. Test those backups regularly.

Many cities have adopted the 3-2-1 rule, which means three copies of your data, in two forms of media, with one of them offsite. The offsite backup must be in a system that is not connected to the main network. If the backups are in a different building but still on the same network, they are also at risk.

With the 3-2-1 rule, in the event of a ransomware attack, a municipality can be back in business in a matter of hours, by wiping its servers and refreshing from the backup.

While email is the most common method of entry for ransomware, this malicious code can also enter a system when a hacker scans the internet for systems with open ports that are exposing Remote Desktop Protocol (RDP), virtual network computing (VNC), or other remote administration services, and hijacking those services to get access to victim servers. Scanning tools such as Nmap, masscan, and Shodan can detect any exposure. Some systems have also added port switches as an extra precaution. When a port detects abnormal traffic, the switch shuts it down at the port level and alerts IT personnel, so they can determine if there is a problem.

Additional steps that can be taken include:

- Review all firewalls for vulnerabilities
- Install anti-virus software (it won't always work but it can help)
- Periodic penetration and vulnerability assessments
- Disabling macro scripts from office files transmitted over email
- Cybersecurity insurance (it won't prevent attacks, but it can mitigate the financial burden of recovery if the worst happens)

WHO IS IN CHARGE?

It is imperative to know who will be responsible for guarding against ransomware attacks. There is often confusion over this, especially at a time when smaller budgets have resulted in smaller staffs. If the internal IT department consists of one person, it's asking a lot of that person to implement every ransomware precaution while still fulfilling his or her other daily obligations in places with multiple servers and hundreds of terminals.

For this reason, many public sector entities are turning to outside security firms with the experience and resources to combat the ransomware threat. These companies will assess a city's security status, and take appropriate steps to implement additional precautions as part of a multilayered security program. They will also schedule regular assessments and audits of the network's security posture, to make sure best practices are being maintained.

CONCLUSION

The risk of ransomware has grown exponentially in recent years, and shows no sign of receding. But by building secure defenses, educating employees about the guises of ransomware, and leveraging the expertise of companies experienced in data protection, it is possible to significantly reduce the risk of infestation.

Prepared by 360Civic

Since the arms race is still raging between public sector websites trying to protect confidential information and hackers trying to steal it, 360Civic is proud to announce a ransomware protection service, available to any entity that uses our servers for hosting. Through our decades of experience in web design, technology development and hosting services, we understand where vulnerabilities exist, and we integrate security features into every product we build.

SOURCES

http://www.etcentric.org/municipalities-increasingly-targeted-for-ransomware-attacks/

http://www.govtech.com/security/Phishing-Malware-Ransomware-Among-Top-Public-Sector-Threats-Reports-Find.html

http://www.govtech.com/security/Riverside-Ohio-Just-the-Latest-in-a-Spate-of-Government-Focused-Ransomware-Attacks.html

https://paymentweek.com/2018-6-27-local-government-workers-brace-ransomware-attack/

https://www.wsj.com/articles/ransom-demands-and-frozen-computers-hackers-hit-towns-across-the-u-s-1529838001

https://www.orrick.com/Insights/2018/04/Ransomware-Attacks-for-Local-Governments-and--Public-Agencies-A-Primer

http://knowledgecenter.csg.org/kc/content/atlantas-ransomware-attack-evidence-threat-state-and-local-governments

https://statescoop.com/public-sector-outgunned-on-ransomware-experts-say

https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#1932c3724123