Preparing Against and Responding to Ransomware Attacks

Presented by:

Louisiana Secretary of State Kyle Ardoin

July 23, 2019 Cybersecurity Incident 1

- On July 23 2019 at 5 AM, the Information Security Team received a report from the Louisiana Department of Education that the Sabine Parish School District was the victim of a ransomware attack.
- IST responded to the incident by gathering additional details and discovered two additional school districts (City of Monroe in Ouachita and Morehouse Parish) affected by the same strand of ransomware.
- The nature of the attacks prompted the governor to declare a state of emergency, activating Louisiana's cybersecurity commission. The commission is chaired by the President of the Cyber Innovation Center and co-chaired by the Adjutant General of the Louisiana National Guard. The Louisiana Secretary of State is a commissioner.
- In response to the attack, the Department of State shut off internet access and email access as a precautionary measure. This being the first such attack on local government entities since our new cybersecurity policies were in place, we were very cautious and treated the incident as a "test run" in the event of a major attack on our systems.

November 10, 2019 Cybersecurity Incident 2

- Incident 2 occurred on November 10, 2019 and affected many clients of a Managed Service Provider (MSP), 7 of which were Clerk of Court offices.
- The MSP was compromised by an attacker, who then pushed ransomware out to many of the MSP's clients. By the time this event occurred, we learned from past events and other ongoing events that it is not necessary to "pull the plug" as a first resort.
- We have learned to trust our layered defense mechanisms that are in place and stay in contact with our Managed Security Service Provider (MSSP) to help monitor the situation.
- While our MSSP was monitoring the situation, we were constantly reviewing logs to verify that no unusual behavior was occurring on our network.
- We also were in contact with affected offices and incident responders to keep up with the incident as it played out.

November 17, 2019
Cybersecurity Incident 3

- On November 17, 2019, another ransomware attack hit Louisiana, this time on larger-scale impacting multiple state agencies.
- Officials suspect the virus was able to affect state agencies due to a state employee's opening of a suspicious link.
- The state's Office of Technology Services shut down network traffic and were able to prevent a larger spread. The attackers infiltrated 200 of the state's 5,000 servers and about 2,000 computers were damaged.
- The largest disruption, in terms of impact to public services, came through the Office of Motor Vehicles, which took weeks to become fully operational. OMV uses a computer system which is approximately 40 years old, forcing the department to reimage OMV computers.
- The Louisiana Department of State's network is separate from the state's OTS network. Our department insisted on not consolidating our department's IT with a statewide IT department due to the sensitive nature of elections.

Importance of Intergovernmental Information Sharing

- The November 17 ransomware attack occurred one day after the Louisiana General Election (Sunday), although our department was not notified of the attack until Monday.
- Using lessons we learned from the July attack, we did not shut down all internet and email access on our servers, but were more strategic in what we isolated to prevent any potential infestation.
- It is vital that all levels of government share information right away to prevent a larger or more devastating breach of data.
- Our federal and state partners must notify us of any potential or ongoing attacks immediately. Any delay in information sharing only increases the potential danger to our computers and sensitive data, in addition to extension of the outage to public services.
- Local governments must also know that we are available to help in the event of an attack on their systems (such as the one that occurred in July). Local governments should not feel ashamed or scared to come to their state partners to assist in preventing and stopping attacks. Further delays in notifying state agencies of hits only exacerbates the problem.

Unintended Consequences of Cyber Incidents

- Louisiana's gubernatorial election was contentions and hotly contested. The Democrat Governor was re-elected by a nearly 40,000 margin, but the race for Secretary of State nearly 40,000 less votes cast. Undervotes are common as citizens are not required to vote on every race, which caused many individuals to perpetuate conspiracy theories that the elections were hacked.
- Due to the November attack occurring the day after the general election, conspiracy theories, misinformation and disinformation became a more serious problem.
- Our office had to directly respond to numerous inquiries and social media posts purporting to tie the cyberattack to the general election results.
- Cyberattacks are a prime opportunity for some to cast doubt on our elections. Election officials must be ready to respond to citizens and media outlets that tie cybersecurity news to election infrastructure, even when no tie exists.
- Luckily, we were able to quickly provide accurate information to our partners in the media who helped broadcast the truth about the cyber attack and undervote, thus maintaining voter confidence in the election.

Preventative Measures Taken

- Replaced Windows 7 and ensured Clerks of Court had no administrative access to prevent installation of unauthorized applications; behavior-based antivirus with central control and logging
- Behavior-based protection against malware, phishing and data loss
- Mandatory cybersecurity awareness training
- Multi-Factor Authentication starting with all external access and any access to the Voter Registration Database
- Network Segregation: Physically separated the network wiring of the clerks of court and registrars of voters from the parish network
- Albert sensors scanning all network traffic entering and leaving the network
- DNS security
- Limit vendor access to our network

Engage With Trusted Partners

- Louisiana Cybersecurity Commission: Goal of advancing the State's cyber ecosystem and position Louisiana as a national leader and preferred location for cyber business, education, and research — there is a specific committee on Election Security.
- National Guard: During the 2019 Gubernatorial election, members of the National guard shadowed our elections and IT staff to get a detailed understanding of what we do and the specific needs of our office.
- ISACs and CISA: We review the information and update our defenses accordingly, and the Homeland Security Information Network (HSIN) portal
- State Fusion Center: We receive local indicators of compromise and act on them; unique HSIN portal.
- Managed Security Service Provider: Hands on inspection of logs; Incident Response provider; hands on (not automated) internal and external penetration tests; expert recommendations for architecture and products

The State of Managed Service Providers (MSPs)

- Many local government agencies are not capable of maintaining a full-time IT staff sufficient enough to handle system maintenance, therefore outsourcing the work to MSPs.
- In the past, firewalls, system patching and anti-virus software was sufficient. However, in recent years, attacks have become much more sophisticated-yet many MSPs (mostly “mom and pops” with very limited experience) are still operating under what worked several years ago.
- As attacks grew more sophisticated, many MSPs have not been upfront with their clients about the need to invest more into their security. This leads to serious problems for their clients-and the MSPs themselves.

Many MSPs Are Behind The Times

- Many MSPs use remote monitoring and management (RMM), a web-based automation tool, allowing them to deliver their services to as many clients as possible. Anyone with internet access can log-in to an RMM with a username and password.
- This presents a problem because many RMMs do not utilize multi-factor authentication (MFA) and MSPs are often given full or high levels of access to local government systems.
- Nation-states or criminal enterprises have very little trouble accessing RMMs with no MFA.
- Russia, China, and Iran can identify MSP vendors through public records, target them through phishing, and deploy devastating viruses.
- Too many MSPs are using outdated techniques, exposing themselves and their clients to dangerous ransomware attacks from bad actors. If MSPs aren't protecting themselves, how can they protect their clients?

What MSPs and Local Officials Can Do

- I'm a free enterprise supporter; if MSPs do not change, then the market will correct itself. Just as the answer to Bush v. Gore was DRE, the answer to 2016 concerns is DRE with a paper component.
- MSPs must be more upfront with their clients. Too often, MSPs are worried about asking for a client to invest more for their security, which is more difficult to protect in the age of sophisticated attacks.
- Local officials must turn to those who provide security to fit today's challenges, including behavior-based protections against potential attacks.
- Local officials should consider using managed security service providers (MSSPs). While MSPs attempt to protect systems on a very basic level to ensure operability, MSSPs are focused on keeping those same systems safe and secure by preventing and detecting, rather than simply responding to, attacks.
- State officials should check with their local partners to ensure their safety at the cyber-level. State officials have no safety net.

Cybersecurity Guidance for Local Election Authorities

In the next thirty days, Louisiana is embarking on a program to help our local election authorities manage cybersecurity risk. With our partners in the FBI, CISA, and our MSSP, we will ensure that local election authorities understand the level of service provided by their MSP vendors. We are promoting a standard that includes the following minimum security controls that all MSPs supporting Louisiana's local election authorities should achieve well in advance of the 2020 presidential election:

- Advanced endpoint protection
- Threat detection (network and endpoint)
- Multi-factor authentication for remote login credentials (such as RRM tools)
- Incident response planning
- Log aggregation, analysis, and review