Quick Action and Safe Storage Help New Orleans Recover from Ransomware Attack and Build a Strong Defense Against Future Threats

THE SECURITY ALERTS ARRIVED early on Friday, Dec. 13, 2019: suspicious remote logins were occurring on the City of New Orleans' servers.

"The logins were coming from accounts I knew weren't being used at 5 a.m. That keyed us in that something bad was happening," says Bill Healy, the city's director of operations for information technology and innovation.

Aware of increasing ransomware attacks on cities across the country, the city's IT department wasted no time in responding.

"We took the most immediate and drastic actions we could to mitigate damage from the attack," says Kimberly LaGrue, the city's chief information officer.

At 11 a.m., the city began shutting off its Internet access. By 11:30 a.m., Internet connections for all of the data center's 470 servers and the thousands of virtual machines they contained had been completely shut down.

By isolating machines on a virtual network, investigators soon discovered the culprit: a variant of Ryuk malware, which has been used since 2018 to launch ransomware attacks on businesses, governments and hospitals. Researchers estimate the cost of Ryuk attacks in 2019 reached $7.5 billion.

With Ryuk, as with other ransomware attacks, hackers break into an organization's network, usually by stealing an email account's login credentials in a phishing scam. They then use the compromised account to install and spread malware on the network. The malware encrypts data, making it impossible for workers to access systems and information they need. Attackers then demand payment, usually in Bitcoin, to release the data.

Thanks to the city's quick action, the New Orleans attackers didn't get far enough to make a ransom demand. Forensic analysis later revealed only one server had been completely encrypted. Several others had been partially encrypted when the city disrupted the attack by shutting off Internet access.

In the beginning, however, there was no way of knowing the extent of the damage. The city had to test and sanitize all of its data and find a safer place to store it. This served two purposes: to remove the current infection and to keep the hackers from later reinfecting the system — a growing trend in ransomware attacks. In the meantime, the city's more than 4,000 workers could no longer access mission-critical online tools and information.

MOVING TO SAFE STORAGE

New Orleans was faced with 50 terabytes of SQL data that it needed to analyze, sanitize and store. It set up a virtual local area network (VLAN) where it could isolate all servers. A monitoring service was used to determine which virtual machines on the servers — or files within those machines — were infected and had to be scrubbed. The scrubbed data then had to be moved to new, safe storage and backup systems while existing servers were still being patched and upgraded.

"We basically had to double our storage needs in order to recover," Healy says.

The city selected Pure Storage to supply the hardware and software for both primary and disaster recovery (DR) storage. Pure's storage system deduplicates all data stored on it, saving precious space for the city and allowing additional copies to be easily made and stored. The city had previously run only its most important applications on its fastest storage, but with Pure Storage they could run far more – and faster. This helps city workers do their jobs more efficiently during normal operation and speed recovery time in the event of another attack.

"We have a platform that gives us a better and faster storage option. It makes us more comfortable with the response we are able to provide for our organization should there be another attack," LaGrue says.

Cyberattacks on municipalities have been on the rise for several years, a trend that has accelerated during the pandemic.

"Everything we hear in the industry tells us there has been an uptick in phishing attempts and malware attacks since COVID-19. The hacker community is exploiting vulnerabilities and preying on pandemic-related fears, and we have to be ready for them," says LaGrue.

Pure Storage's data snapshots are immutable, meaning hackers can't modify or delete them, and they even have an option that prevents these snapshots from being tampered with by a seemingly authorized administrator without first contacting Pure Storage. The city also worked with disaster recovery and data management firm Veeam, which provides additional protections to make backup data immutable.

"That means even if an attacker gets in and finds our backups, he or she can't do anything to them," Healy says.

Restoring data and moving it to a secure storage system quickly was the key to a swift recovery. With help from Pure Storage, the city's IT department set up the new storage platforms quickly and began data migration. Recovery and

backup systems can take a long time for IT administrators to learn and deploy, but city administrators found Pure Storage and Veeam simple to use.

"We needed the new system to be easy to learn and implement so that we could manage other parts of the recovery while building out the new storage," LaGrue says. "The Pure Storage team provided a simple solution and gave us a wealth of cross-training and knowledge that helped us get it up and running quickly."

RECOVERING AMID A PANDEMIC

In the midst of the city's recovery efforts, the COVID-19 pandemic hit. While recovery efforts never stopped, the IT department had to shift its focus to providing a remote working environment for the city's 4,000 workers.

"It delayed our recovery plan by about two months," LaGrue says.

In addition, before going back online, the city added multiple new layers of network security.

"We could have had the network restored much quicker, but it wouldn't have been nearly as secure," Healy says.

Healy and LaGrue learned some important lessons while managing the attack, and have suggestions to help other governments avoid ransomware attacks or mitigate their damage:

> "We were in a time crunch. We were very fortunate to have a solution that was simple and straightforward, so our engineers could start using it very quickly."
>
> **Kimberly LaGrue, CIO, New Orleans**

✓ **Know your organization's disaster recovery plan** so that you can move quickly to stop an attack. "Our IT team has been working on disaster recovery for years, and we knew what to do as soon as we detected the threat. It's like knowing which exit to use during a fire drill," LaGrue says.

✓ **Isolate traffic between nodes on the network**. "Granular management gives you a bit more control over traffic from bad actors," Healy says.

✓ **Use a layered, multi-vendor approach to network security** to uncover more vulnerabilities and decrease the chances of another attack.

✓ **Use a secure, easy-to-deploy storage and backup system.** "It helps me sleep at night to know if our data is compromised, we can quickly retrieve it from a safe storage system," LaGrue says.

Today, New Orleans has completed 80 percent of the work needed for recovery. It is bringing the last of its legacy operations back online, and has distributed nearly all of the 500 new computers and laptops it needed to order when its old hardware couldn't be configured to meet new security requirements. The city expects to achieve a full recovery by the first anniversary of the attack.

By providing efficient, secure and economical storage and backup systems, Pure Storage and Veeam speeded New Orleans' recovery and provided a stronger defense against future attacks. As a result, the city can now focus on achieving its other important objectives.

"Serving our community is our bottom line. By making efficient investments in storage and security, we can direct more funding to initiatives that help our citizens," LaGrue says.

This paper was created by the Government Technology Content Studio, with input from Pure Storage and Veeam.