NYC CYBER SECURITY LESSONS LEARNED

Increasing Cybersecurity Threats to Critical Infrastructure

WHAT GUIDED OUR CYBER EFFORTS

Iranian Hackers Exploit PLCs in Attack on Water Authority in U.S.

Nov 29, 2023 Newsroom

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) revealed that it's responding to a cyber attack that involved the active exploitation of Unitronics programmable logic controllers (PLCs) to target the Municipal Water Authority of Aliquippa in western Pennsylvania.

The attack has been attributed to an Iranian-backed hacktivist collective known as Cyber Av3ngers.

"Cyber threat actors are targeting PLCs associated with [Water and Wastewater

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

CISA is responding to active exploitation of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) Sector. Cyber threat actors are targeting PLCs associated with WWS facilities, including an identified Unitronics PLC, at a U.S. water facility. In response, the affected municipality's water authority immediately took the system offline and switched to manual operations—there is no known risk to the municipality's drinking water or water supply.

cisa.gov

Cyber-Attack Closes Hospital Emergency Rooms in Three US States

Ardent Health, which oversees hospitals in states including Texas, New Mexico and Oklahoma said it was targeted over Thanksgiving

By **Homeland Security Today**

November 28, 2023

Facebook | Twitter

A cyber-attack has shut down emergency rooms in at least three states, a hospital operator warned on Monday, forcing the organization to divert patients to other facilities.

hstoday.us

Long Beach declares state of emergency after cyber attack

BY **STAFF REPORT** · NOVEMBER 19, 2023 · 2 MINUTE READ · NO COMMENTS

In a special meeting Friday, the Long Beach City Council unanimously approved the proclamation of a local emergency in response to the recent cyber-security attack targeting the City's online systems.

According to a public statement from the City, the emergency measure aims to streamline and bolster the City's response efforts as it investigates and resolves the incident.

"We are committed to safeguarding our City systems and public services," said Mayor Rex Richardson in a public statement. "Our team is working around the clock to rectify this issue and the goal is always to provide quality public service to our community and make Long Beach a great place to live, work and play."

In line with the Long Beach Municipal Code, the City Manager recommended the adoption of the emergency proclamation due to the threat to the City. The emergency will remain in effect until Dec. 5, 2023, providing emergency powers through the Thanksgiving holiday weekend. Any

Cyberattack hits 2 New York hospitals, forces ambulance diversions

Officials say two hospitals in New York have been hit with a cyberattack and are diverting patients to other facilities

By **The Associated Press**
October 20, 2023, 12:19 PM ET • 2 min read

KINGSTON, N.Y. -- Two hospitals in New York were hit with a cyberattack and are diverting patients to other facilities, hospital officials said Friday.

The cyberattack affected computer systems at HealthAlliance Hospital in Kingston along with Margaretville Hospital and Mountainside Residential Care Center — all part of the Westchester Medical Center Health Network.

RIVERHEAD NEWS-REVIEW

09.29.2022 FEATURED STORY

Ransomware attack on Suffolk County heightens importance of cybersecurity for local municipalities

By Brianne Ledda, Melissa Azofeifa and Tim Gannon

The Register®

that the continued state of emergency was necessary "because certain functions, including remote public document searches, remain offline and require a complete overhaul due to the fact that the former clerk IT administrator failed to update these systems in decades."

Schlusser disagrees, and claims he alerted Bellone's IT team to potential intrusions months before the ransomware attack, as well as an FBI warning that there was an active ransomware campaign being waged against the county shortly before the attack was discovered.

Despite claims that the county's state of emergency is long past expired, a post-breach report found 600 instances of malware on county systems that had gone undetected for years. So far, the ransomware incident has cost Suffolk County $5.4 million for investigation and restoration, and $12 million for new hardware and software.

The New York Times

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

By Alan Blinder and Nicole Perlroth

March 27, 2018

244

ATLANTA — The City of Atlanta's 8,000 employees got the word on Tuesday that they had been waiting for: It was O.K. to turn their computers on.

But as the city government's desktops, hard drives and printers flickered back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi.

Atlanta's municipal government has been brought to its knees since Thursday morning by a ransomware attack — one of the most sustained and consequential cyberattacks ever mounted against a major American city.

The digital extortion aimed at Atlanta, which security experts have linked to a shadowy hacking crew known for its careful selection of targets, laid bare once again the vulnerabilities of governments as they rely on computer networks for day-to-day operations. In a ransomware attack, malicious software cripples a victim's computer or network and blocks access to important data until a ransom is paid to unlock it.

"We are dealing with a hostage situation," Mayor Keisha Lance Bottoms said this week.

The assault on Atlanta, the core of a metropolitan area of about six million people, represented a serious escalation from other recent cyberattacks on American cities, like one last year in Dallas where hackers gained the ability to set off tornado sirens in the middle of the night.

Part of what makes the attack on Atlanta so pernicious are the criminals behind it: A group that locks up its victims' files with encryption, temporarily changes their file names to "I'm sorry" and gives the victims a week to pay up before the files are made permanently inaccessible.

Threat researchers at Dell SecureWorks, the Atlanta-based security firm helping the city respond to the ransomware attack, identified the assailants as the SamSam hacking crew, one of the more prevalent and meticulous of the dozens of active ransomware attack groups. The SamSam group is known for choosing targets that are the most likely to accede to its high ransom demands — typically the Bitcoin equivalent of about $50,000 — and for finding and locking up the victims' most valuable data.

In Atlanta, where officials said the ransom demand amounted to about $51,000, the group left parts of the city's network tied in knots. Some major systems were not affected, including those for 911 calls and control of wastewater treatment. But other arms of city government have been scrambled for days.

The Atlanta Municipal Court has been unable to validate warrants. Police officers have been writing reports by hand. The city has stopped taking employment applications.

NEWS

Baltimore's 911 emergency system hit by cyberattack

The disruption was the second cyber attack on a major U.S. city within the past week.

March 28, 2018, 3:35 PM EDT / Updated March 28, 2018, 3:35 PM EDT / Source: Reuters

WASHINGTON – Baltimore's computer network that supports emergency calls was hacked this past weekend and suffered temporary disruption that forced city officials to resort to manual operations to handle calls, the city mayor's office said.

A "limited breach" affecting Baltimore's computer-assisted dispatch system, which is used to support and direct 911 and other emergency calls, was identified Sunday morning, according to Frank Johnson, Baltimore's chief information officer.

The disruption was the second cyber attack on a major U.S. city within the past week, coming just days after Atlanta was struck by a widespread ransomware attack that interrupted bill collection services, downed the airport's wireless internet and impeded other city services. A senior U.S. cyber security official said there were no indications the two attacks were related.

During the Baltimore outage, details of incoming callers seeking emergency support were unable to be relayed to dispatchers electronically and instead had to be manually managed by call center support staff, Johnson said.

He said the impacted computer server was isolated and taken offline to mitigate the threat and the computer-assisted dispatch system was fully restored by early Monday morning, about 17 hours after the issue was identified.

"These critical services were not impacted nor disrupted at any time, as they were temporarily transitioned to manual mode," Johnson said in a statement.

A spokesman for the mayor's office said the 911 dispatch system itself was not hacked. He declined to say if the city had identified any suspects behind the breach, whether any information was stolen from its systems or if other city services had been recently targeted by cyber attacks.

He added: "This is an active investigation. Getting into further details could compromise the investigation."

An FBI spokesman told the Baltimore Sun that the bureau was aware of the breach and providing technical assistance. The regional FBI office in Baltimore could not be immediately reached for comment.

The New York Times

Ransomware Attack Hits 22 Texas Towns, Authorities Say

By Manny Fernandez, Mihir Zaveri and Emily S. Rueb

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.

HOUSTON — Computer systems in 22 small Texas towns have been hacked, seized and held for ransom in a widespread, coordinated cyberattack that has sent state emergency-management officials scrambling and prompted a federal investigation, the authorities said.

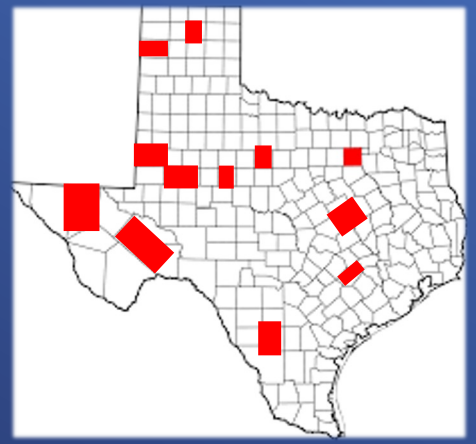
The Texas Department of Information Resources said Monday that it was racing to bring systems back online after the "ransomware attack," in which hackers remotely block access to important data until a ransom is paid. Such attacks are a growing problem for city, county and state governments, court systems and school districts nationwide.

By Tuesday afternoon, Texas officials had lowered the number of towns affected to 22 from 23 and said several government agencies whose systems were attacked were back to "operations as usual."

The ransomware virus appeared to affect certain agencies in the 22 towns, not entire government computer systems. Officials said that there were common threads among the 22 entities and that the attacks appeared not to be random, but they declined to elaborate, citing a federal investigation.

It was unclear who was responsible. The state described the attacker only as "one single threat actor."

Elliott Sprehe, a spokesman for the information resources department, declined to provide further specifics or release the names of the towns affected because of the "potential for further attacks."



WHAT'S AT STAKE FOR ALL LOCAL MUNICIPALITIES, NYC BY THE NUMBERS

- 25,000 911 CALLS
- 11.6 MILLION ANNUALLY
- 1 BILLION GALLONS OF WATER
- 13,000 TRAFFIC LIGHTS
- 8.5 MILLION NYC RESIDENTS
- 120 AGENCIES
- 52,000 NYPD EMPLOYEES
- 320,000 NYC EMPLOYEES
- 3200 POWER COMPANIES NATION WIDE
- 52,000 DRINKING WATER AND 16,000 WASTEWATER SYSTEMS NATIONWIDE
- 17 SECTORS USG CRITICAL INFRASTRUCTURE
- 90% OF CRITICAL INFRASTRUCTURE IN THE U.S. IS OPERATED AND OWNED BY THE PRIVATE SECTOR

NEW YORK CITY'S RESPONSE

CYBER STRATEGIES: 2013 TO PRESENT

- **NOVEMBER 2013** – NYPD IB DETAILED TO FBI CYBER DIVISION
- **JANUARY 2015** – NYPD INTRODUCES NYC CYBER COMMAND (NYC3) CONCEPT
- **NOVEMBER 2015** – NYPD IB JOINS FBI NY CYBER TASK FORCE
- **FEBRUARY 2017**-NYPD/FBI NY CYBER TF-DEP VULNERABILITY ASSESSMENT
- **JULY 2017** – NYC CYBER CRITICAL SERVICES AND INFRASTRUCTURE (CCSI) WORKING GROUP
- **JULY 11, 2017** – CREATION OF NYC3 BY EXECUTIVE ORDER TO LEAD THE CITY'S CYBER DEFENSE EFFORTS
- **DECEMBER 2018/2019**-IBM CYBER RANGE
- **JANUARY 2022**-NEW YORK CITY OFFICE OF TECHNOLOGY AND INNOVATION

- “ INTELLIGENCE IS BEING ABLE TO UNDERSTAND PROBLEMS, AND REALLY GOOD INTELLIGENCE IS BEING ABLE TO DO SOMETHING ABOUT THOSE PROBLEMS WE UNDERSTAND”

NYC CYBER COMMAND

JANUARY 23, 2015

NYC Participants

282 Members

80 Organizations

12 Sectors

NYC Participating Sectors

GOVERNMENT

HEALTHCARE

FINANCE

ENERGY

TRANSPORTATION

LAW ENFORCEMENT

TECHNOLOGY

MEDIA

HOSPITALITY

EMERGENCY SERVICES

TELECOMMUNICATIONS

WATER

NYC Mission

Mission – To better protect New York City's critical services and infrastructure by:

1. **Sharing real-time threat information and other relevant data (e.g. Indicators of Compromise)**
2. **Training jointly**
3. **Deploying volunteers should an entity or sector require assistance**

Action 1: Sharing Real-Time Threat Information

123 Cyber Threat Intelligence notifications were made in 2020 including:

- CISA Alerts
- FBI Flash
- FBI PINs
- JRIC Alerts
- NYPD-IB Cyber BOLOs
- NYPD SOC
- Open Source
- Victim notifications

The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

By David E. Sanger, Clifford Krauss and Nicole Perlroth

Published May 8, 2021 Updated May 13, 2021

One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks.

The operator of the system, Colonial Pipeline, said in a vaguely worded statement late Friday that it had shut down its 5,500 miles of pipeline, which it says carries 45 percent of the East Coast's fuel supplies, in an effort to contain the breach. Earlier Friday, there were disruptions along the pipeline, but it was not clear at the time whether that was a direct result of the attack or of the company's moves to proactively halt it.

On Saturday, as the F.B.I., the Energy Department and the White House delved into the details, Colonial Pipeline acknowledged that its corporate computer networks had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom. The company said it had shut the pipeline itself, a precautionary act, apparently for fear that the hackers might have obtained information that would enable them to attack susceptible parts of the pipeline.

Administration officials said they believed the attack was the act of a criminal group, rather than a nation seeking to disrupt critical infrastructure in the United States. But at times, such groups have had loose affiliations with foreign intelligence agencies and have operated on their behalf.

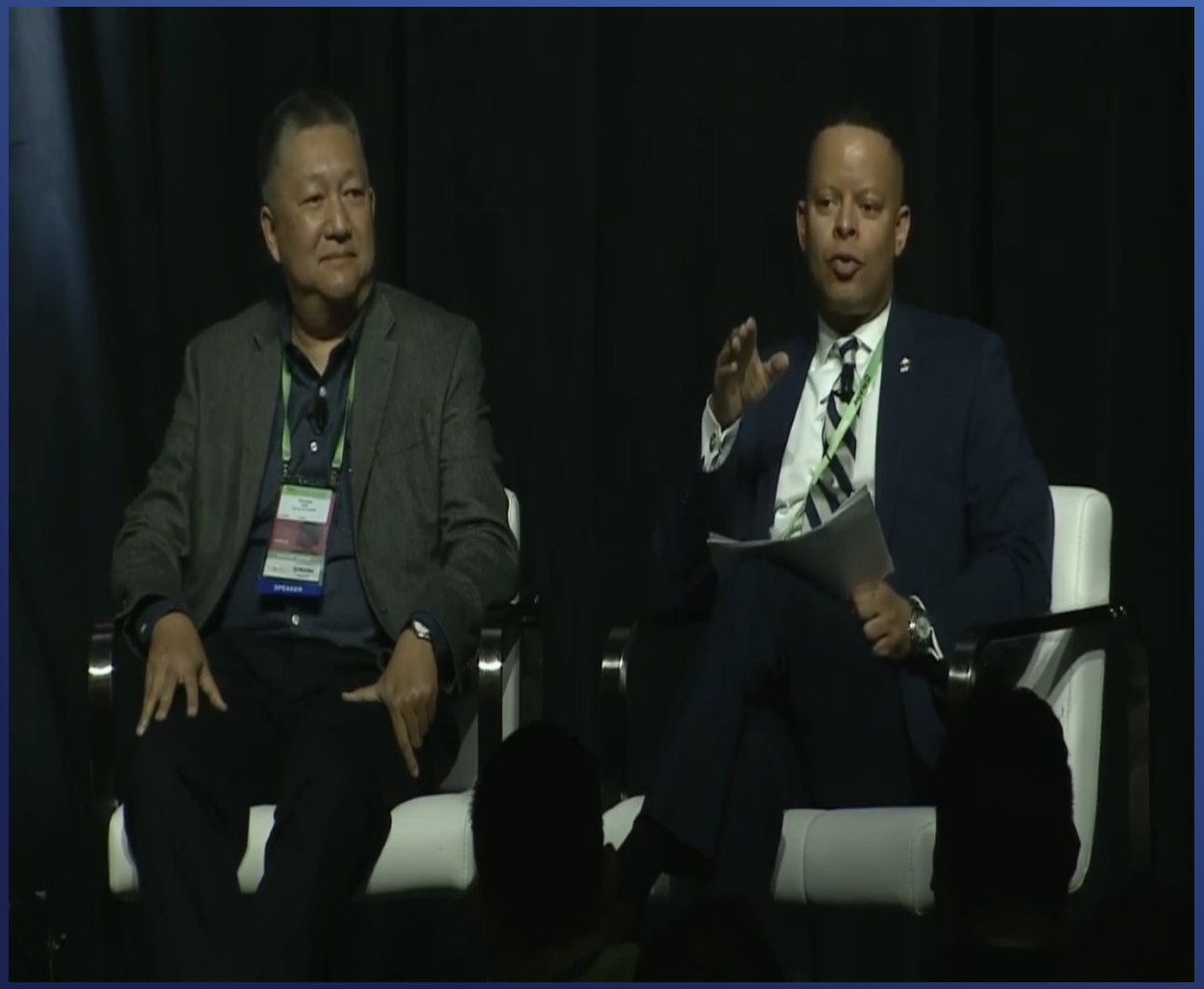
Action 2b: Training Jointly - IBM Cyber Range 07-26-2019

Action 2c: Training Jointly - IBM Cyber Range 12-06-2019

CYBER VULNERABILITY ASSESSMENTS AGAINST CRITICAL INFRASTRUCTURE

RSA CYBER CONFERENCE 2020

"LESSONS FROM AMERICA'S TWO LARGEST CITIES ON PREPARING FOR CYBERATTACKS" THE NYPD'S ROLE IN PROTECTING NYC FROM CYBERATTACKS AND THE IMPORTANCE OF SHARING INFORMATION BETWEEN SECTORS TO INCREASE RESILIENCE/CYBER PREPAREDNESS (*PANEL INCLUDED TIM LEE, CHIEF INFORMATION SECURITY OFFICER FOR THE CITY OF LOS ANGELES*) .



APRIL 2023, RSA CYBER CONFERENCE, SAN FRANCISCO-UNDER PRESSURE: WHAT CYBER CAN LEARN FROM FIRST RESPONDERS

WHAT GUIDED OUR CYBER EFFORTS

For more information on how to enhance your local cyber strategies:

Gustavo A. Rodriguez

(ret) Lieutenant Special Assignment NYPD

Founding member-NYC Cyber Command

Linkedin @Gustavo Rodriguez MA, MPA