Case Study

UncommonX Crushes Ransomware Attack for The City of Gary

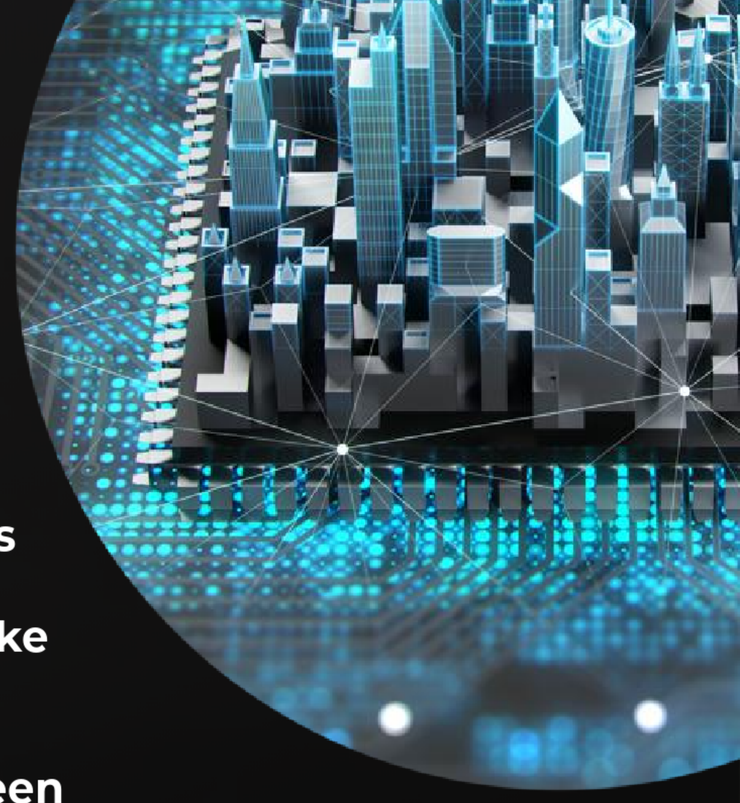
The Incident

In April 2021, the city of Gary, Indiana was the victim of a ransomware attack that infected several servers. The IT department was suddenly locked out of critical systems supporting essential city services. A message left by the attackers said they had encrypted files and demanded a ransom to unlock them. They also threatened to release stolen data on the dark web. If not recovered quickly, the loss of services and data would impact thousands of residents and businesses.

The IT team, led by chief innovation officer Lloyd Keith, immediately took action to cut off any further damage. They then provided basic network functionality to city staff managing the most crucial services. At that point, faced with limited resources, Keith decided to seek outside help. One of his vendors, Network Solutions Inc., recommended UncommonX to assist with the investigation, containment, and recovery process.

> "UncommonX was the only MDR vendor able to provide us with such a detailed, comprehensive view of our entire network. They uncovered and delivered the critical insight needed to help our city improve its cyber security posture in days."
>
> **— Lloyd Keith, CIO, City of Gary, Ind.**

UncommonX



The Response

We immediately engaged with Keith's team through our Security Operations Center (SOC). Our specialists quickly deployed our patented UxP™ MDR platform. After UxP™ (UncommonX Platform) mapped Gary's entire digital environment, the discovery phase provided insight to the overall impact of the ransomware incident. The SOC also checked to make sure the attackers weren't still in the system.

The discovery phase confirmed that a conti strain of ransomware had been released through a spear phishing email in one of the city's departments. Working with the Gary IT department, our team contained the ransomware and helped eradicate it from their need environment.

They then began recovering servers and computers. Lloyd's team had backed up files on a regular basis and re-imaged new computers the year before, which helped speed up the process.

Throughout every phase, we provided regular reports to Keith that he could share with the mayor's office.

The Results

The City of Gary was back online within 24 hours. Full recovery took a week and a half. We also helped reduce the city's vulnerabilities by patching gaps in their network with a suite of security tools. Finally, we monitored threat intelligence sources, as well as the dark web, to make sure the attackers hadn't released any of the data they had stolen.

Lloyd Keith realized that maintaining effective full-time security would be difficult alone. So, Gary signed a long-term contract with UncommonX for their MDR solution. Keith and city officials decided it was more cost effective to add increased security measures now than pay the considerable costs to recover from another cyber attack later.

Solutions Provided

+ Managed Detection and Response (MDR)
+ Incident Response
+ Managed Security
+ 24/7 Monitoring
+ Asset Discovery & Inventory
+ Threat Detection

Contact Us Today:

Nils Lindokken
nlindokken@uncommonx.com
708-557-6457
www.uncommonx.com

UNCOMMONX