THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR

City of Columbus Cyber Incident Response Fact Sheet
August 13, 2024

Timeline

- 7/18/2024 – Department of Technology analyst detected suspicious activity. Experts were engaged to analyze activity and identified threat actor involvement. Mayor Andrew J. Ginther was advised, and the decision was made to take city offline at 11:31 p.m.
- 7/19/2024 – FBI and Homeland Security engaged.
- 7/20/2024 through 7/21/2024 – Ongoing forensic investigation continued. Decision was made to advise city leadership and then public that the incident was not CrowdStrike related.
- 7/22/2024 – City leadership was briefed. Employees were made aware. Press release was issued alerting public to the cyber attack, and that forensic investigation would take time.
- 7/29/2024 – Press release was issued communicating that threat actor's attempted ransomware event and was thwarted, but some data was accessed and the investigation continues.
- 7/30/2024 – Forensic investigation revealed threat actor had access to employee personal information. Experian was engaged for credit monitoring.
- 7/31/2024 – Threat actor auction commenced.
- 8/1/2024 – Press release about employee credit monitoring was issued.
- 8/6/2024 – Letters to employees with credit monitoring information were sent.
- 8/7/2024 – Second attempt by threat actor at auction.
- 8/8/2024 – Threat actor release of data occurred.
- 8/9/2024 – City confirms 1) data encrypted/corrupted and 2) threat actor access to copied data eliminated.

Summary of Key Events

- Over the weeks since this cyber attack occurred, the city has been working around the clock with all available resources.
- **The investigation continues, but the city can now share that the stolen data backups published by the threat actor, Rhysida, were either encrypted or corrupted.**
- On July 29, 2024, the city communicated it had successfully thwarted the threat actor's attempt to encrypt its systems.
- On July 30, 2024, forensic investigation revealed the threat actor had access to employee personal information and Experian was engaged for credit monitoring.
- On Wednesday, July 31, 2024, the threat actor posted an auction for what it claimed to be city data on the dark web. This consisted of a claim of 6.5TB of data with associated "screen shots" of various city systems. No live data or sample data was posted.
- The city continues to conduct forensic analysis to determine the nature of the data the threat actor claimed to possess, particularly whether it included personally identifiable information or other data required to be protected under federal and/or state law.
- While our investigation has confirmed that some city data was either temporarily accessed or copied, the city has also determined, in collaboration with federal and state law enforcement, counsel, cybersecurity experts, and city IT staff, that the majority of the data obtained by the

threat actor is unusable. This is because the stolen copies which purported to include city backup files were either encrypted or corrupted.

- The city did not receive a ransom request.
- The re-auction posted by the threat actor on August 7, 2024 suggests that no one purchased the city's data, so a final attempt was made to sell by advertising a partial download, but the link was broken.
- On August 8, 2024, the threat actor released data on the dark web.
- The city has now confirmed there was not 6.5 terabytes of data released by the threat actor. Rather, the amount was far smaller. The city is still confirming, but it was a fraction of the amount claimed by the threat actor to have been released.
- The data purported to be released was city backups which were determined to be corrupted or encrypted, along with miscellaneous other files that are currently undergoing continued data mining analysis.
- While the city continues to evaluate the data impacted, as of Friday August 9, 2024, our data mining efforts have not revealed that any of the dark web-posted data includes personally identifiable information.
- Our decision to provide notice to employees and offer of credit monitoring was made on July 31, 2024, before the city was made aware of the threat actor's auction.
- The city's decision to offer credit monitoring to employees was precautionary.
- The city does have some evidence that the city's payroll system was accessed long enough to view certain files within it. There is currently no evidence to support that the payroll documents within that system were downloaded by the threat actor or posted to the dark web.
- The city has now made the call that in a further precautionary move, it will be expanding credit monitoring to former employees in the days to come.
- The city remains confident that the actions taken to prevent the encryption of the city's systems and protect our data were the best possible course of action.