Is there an end in sight for Oakland's ransomware crisis?

March 9 2023, by Shomik Mukherjee

Credit: Unsplash/CC0 Public Domain

A ransomware attack against Oakland that has affected city services and exposed reams of sensitive personnel data is creating a nightmare for city officials who aren't sure what it will take to resolve the crisis.

While there is much still unknown about the full extent of the attack that has unfolded over the last month, experts in cybercrime say the resolution is not likely to be a happy one for those affected.

"This is a really devastating cyberattack for sure," said Sarah Powazek, the director of a cybersecurity academic program at the University of California-Berkeley. "It's a big deal, and it's really unfortunate how poorly prepared folks are for dealing with this. And I'm not blaming the city at all—it's sad that cities are supposed to be prepared and know what to do with what is an international cyber attack."

The attack was carried out by hackers associated with the ransomware group Play, also known as PlayCrypt, that has targeted municipalities around the globe, including the small city Cordoba in Argentina, as well as hotels in Brazil and other private businesses.

The city has released few details about the attack, and has not revealed how its data was compromised or the dollar amount sought by the hackers.

As the frequency of ransomware attacks has increased, public entities like Oakland have found themselves more vulnerable, and with fewer resources to defend themselves. Other victims of such attacks in the Bay Area include Bay Area Rapid Transit and Contra Costa County.

Over the past weekend, the Play hackers released about 11 gigabytes of data from the Oakland attack to the dark web, including home addresses and social security numbers of numerous city employees—including the current mayor, and her predecessor—as well as police files and other city data, according to multiple city sources who reviewed the data.

The city has offered one year of free credit protection to employees whose data may have been compromised.

Ransomware attacks in recent years have become more frequent, reaching what some experts call epidemic levels since 2019. Earlier this month, President Joe Biden declared ransomware attacks a national security threat, and a report on national security warned that they could "undermine public trust in the foundation" of democracy.

Information stolen in previous ransomware attacks has been trafficked in countries like Russia and North Korea, where crackdowns on such information is less common.

That has included medical reports involving abused children, sensitive photos of breast-cancer patients, PTSD studies that name specific veterans, and even the schematics for a missile stolen from a defense contractor.

"These things can have devastating, potentially life-threatening consequences," said Brett Callow, a cybersecurity analyst at New Zealand-based cybersecurity firm Emsisoft, which has logged every ransomware attack on a U.S. public agency in the past decade.

Oakland officials have offered few details of last month's attack, but the city temporarily shut down its 311 call line that coordinates requests for city services; the internal system for contracting and funding external vendors; the permit center for local developments; and the systems that handle business tax and parking fee payments.

That means far more could have been stolen from Oakland than what's already been exposed. In addition to current and former city employees, even those who paid for parking tickets in recent years may have had vehicle information or even financial details exposed.

Daniel Aranki, an assistant professor in information at UC Berkeley, said it is very likely, based on previous ransomware attacks, that the information published on the dark web is just a portion of the overall data that was compromised.

"Most typically, a tactic that these groups take is to release some of the information, to let the victims know that they're serious about the ransom," Aranki said. "If you release all the data you have, you lose leverage."

If it's true that the hackers are holding more information hostage, does that mean the city will pay up?

Quincy, a city in Massachusetts, last year paid $500,000 to restore its data, though experts say hackers often aren't done extorting money after receiving an initial payment. The highest dollar amount demanded in recent memory, according to one expert, is $5 million last fall from Wheat Ridge, Colorado, which didn't cough up the money after being forced to close city hall.

Since the data breach, many looking to place the blame have zeroed in on Mayor Sheng Thao and her predecessor, Libby Schaaf. A city audit last year, first reported by the Oakland Observer, found that "staffing and resource constraints" had left the city vulnerable to "ransomware attacks, cyberattacks, and other threats."

But several experts said these attacks are too sophisticated for most public agencies and even cities to currently be able to handle. Even sophisticated technology systems often fail, they say—leaving agencies like Los Angeles public schools, the city of Baltimore and now Oakland vulnerable.

IT systems need to be quite mature "to not ever be susceptible to them," Powazek said.

2023 MediaNews Group, Inc.
Distributed by Tribune Content Agency, LLC.

Citation: Is there an end in sight for Oakland's ransomware crisis? (2023, March 9) retrieved 26 April 2024 from https://techxplore.com/news/2023-03-sight-oakland-ransomware-crisis.html