Malware attack disrupts delivery of L.A. Times and Tribune papers across the U.S.

latimes.com/local/lanow/la-me-ln-times-delivery-disruption-20181229-story.html

Emily Alpert Reyes

Dec. 29, 2018 8:10 PM PT

The Los Angeles Times and other newspapers were hit by a malware attack.

(Los Angeles Times)

By Tony Barboza, Meg James, Emily Alpert Reyes

What first arose as a server outage was identified Saturday as a malware attack, which appears to have originated from outside the United States and hobbled computer systems and delayed weekend deliveries of the Los Angeles Times and other newspapers across the country.

Technology teams worked feverishly to quarantine the computer virus, but it spread through Tribune Publishing's network and reinfected systems crucial to the news production and printing process. Multiple newspapers around the country were affected because they share a production platform.

The attack delayed distribution of Saturday editions of the Los Angeles Times and San Diego Union Tribune. It also stymied distribution of the West Coast editions of the Wall Street Journal and New York Times, which are printed at the Los Angeles Times' Olympic printing plant in downtown Los Angeles.

By Saturday afternoon, the company suspected the cyberattack originated from outside the United States, but officials said it was too soon to say whether it was carried out by a foreign state or some other entity, said a source with knowledge of the situation.

“We believe the intention of the attack was to disable infrastructure, more specifically servers, as opposed to looking to steal information,” said the source, who spoke on condition of anonymity because he was not authorized to comment publicly. The source would not detail what evidence led the company to believe the breach came from overseas.

Foreign cyberattack hits newspapers: Here is what we know »

Tribune Publishing said in a statement Saturday that “the personal data of our subscribers, online users, and advertising clients has not been compromised. We apologize for any inconvenience and thank our readers and advertising partners for their patience as we investigate the situation.”

“Every market across the company was impacted,” said Marisa Kollias, spokeswoman for Tribune Publishing. She declined to provide specifics on the disruptions, but the company’s properties include the Chicago Tribune; Baltimore Sun; Capital Gazette in Annapolis, Md.; Hartford Courant; New York Daily News; South Florida Sun Sentinel and Orlando Sentinel.

No other details about the origin of the attack were immediately available and the motive remained unclear.

Tribune Publishing sold The Times and the San Diego Union-Tribune to Los Angeles biotech entrepreneur Dr. Patrick Soon-Shiong in June, but the two companies continue to share various systems, including software.

It’s unclear how many Times subscribers were impacted by late deliveries and the paper could not provide firm numbers, but a source said that a majority received their papers Saturday morning, albeit several hours late. The Times said that print subscribers who did not get their papers Saturday would receive them with their regularly scheduled delivery of the Sunday edition.

“We apologize to our customers for this inconvenience,” The Times said in a statement. “Thank you for your patience and support as we respond to this ongoing matter.”

The Times and the San Diego paper became aware of the problem near midnight on Thursday. Programmers worked to isolate the bug, which Tribune Publishing identified as a malware attack, but at every turn the programmers ran into additional issues trying to access a myriad of files, including advertisements that needed to be added to the pages or paid obituaries.

After identifying the server outage as a virus, technology teams made progress Friday quarantining it and bringing back servers, but some of their security patches didn't hold and the virus began to reinfect the network, impacting a series of servers used for news production and manufacturing processes.

By late Friday, the attack was hindering the transmission of pages from offices across Southern California to printing presses as publication deadlines approached.

At one point, Times staffers were making contingency plans to hand-deliver pages from the editorial offices in El Segundo to its Olympic printing plant in downtown Los Angeles. Working through the problems created a logjam at the plant, and the resulting cascade of delays pushed back printing and delivery.

San Diego was particularly hard hit by the problem, in large part because of the paper's position in the press run. Between 85% and 90% of the Saturday edition of the Union-Tribune did not reach subscribers on Saturday morning, said Jeff Light, publisher and editor of the San Diego Union-Tribune.

"Papers that should have arrived in San Diego around 3 a.m. to 4 a.m. instead arrived at 7 a.m. and 8 a.m." Light said. Because the newspaper relies on independent contractors to deliver the paper to neighborhoods, many of those people were not available later in the day to do the deliveries.

The first signs of trouble at the Union-Tribune came late Thursday night when sports editors tried to send information, via digital files, to the plate-making facility. But those digital files which contain information that ultimately becomes the pages of the newspaper would not transmit to the plate-making process. Editors seemed to be locked out of the system, having to perform work-arounds.

The transmission of community editions, including the Glendale News Press and Burbank Leader, also appeared in doubt Friday night. Ultimately, a page designer in Orange County figured out he could send all the community papers' news pages from his unaffected computer, said John Canalis, executive editor of Times Community News.

The problem caused widespread issues in South Florida, one of Tribune Publishing's major markets. The South Florida Sun Sentinel told readers that it had been "crippled this weekend by a computer virus that shut down production and hampered phone lines," according to a story on its website.

Malware attacks are extremely common, affecting millions of computers in homes, offices and other organizations every day, said Salim Neino, chief executive of the company Kryptos Logic.

In some cases, dubbed "ransomware," the attackers disable the system and demand money, said Neino, whose company tackled a major ransomware attack called WannaCry last year.

In other instances, the goal is simply to disrupt or “break stuff” by wiping systems, Neino said. Malware has also been used to quietly infect computers and then sell access to other cybercriminals, who can steal banking credentials or exploit other valuable information, Neino said.

Several individuals with knowledge of the Tribune situation said the attack appeared to be in the form of “Ryuk” ransomware. One company insider, who was not authorized to comment publicly, said the corrupted Tribune Publishing computer files contained the extension “.ryk.”

“Ryuk” attacks are “highly targeted, well-resourced and planned,” according to an August advisory by the U.S. Department of Health and Human Services’ cybersecurity program. Victims are deliberately targeted and “only crucial assets and resources are infected in each targeted network.”

It was unclear whether company officials have been in contact with law enforcement regarding the suspected attack. But Katie Waldman, a spokeswoman for the Department of Homeland Security, said “we are aware of reports of a potential cyber incident effecting several news outlets, and are working with our government and industry partners to better understand the situation.”

Tribune declined to comment on the specifics of the malware attack.

Neino also said that tracking the identity of attackers can be difficult since malware code is often freely distributed online.

For instance, even if an attack appears to be Russian because of the “malware family traits,” Neino said, “code still could have been sourced, weaponized and deployed by an actor who downloaded it from an underground forum anywhere in the world.”

Pam Dixon, executive director of the World Privacy Forum, a nonprofit public interest research group, said that “usually when someone tries to disrupt a significant digital resource like a newspaper, you’re looking at an experienced and sophisticated hacker.”

Dixon added that the holidays are “a well known time for mischief” by digital troublemakers, because organizations are more thinly staffed.

“It’s an optimal time to attack a major target,” she said.

The highest-profile cyberattack of a media company was in late 2014 at Sony Pictures Entertainment in Culver City. Hackers, which the FBI later determined were affiliated with the North Korean government, broke into Sony Pictures’ computer system and copied huge chunks of data, which they later posted online for the world to see.

tony.barboza@latimes.com

meg.james@latimes.com

emily.alpert@latimes.com