Arizona Beverages knocked offline by ransomware attack

By Zack Whittaker

Published: 2019-04-02 · Archived: 2026-04-06 03:17:50 UTC

Arizona Beverages, one of the largest beverage suppliers in the U.S., is recovering after a massive ransomware attack last month, TechCrunch has learned.

The company, famous for its iced tea beverages, is still rebuilding its network almost two weeks after the attack hit, wiping hundreds of Windows computers and servers and effectively shutting down sales operations for days until incident response was called in, according to a person familiar with the matter.

More than 200 servers and networked computers displayed the same message: “Your network was hacked and encrypted.” The company’s name was in the ransom note, indicating a targeted attack.

Notices posted around the office told staff to hand in their laptops to IT staff. “Do not power on, copy files, or connect to any network,” read the posters. “Your laptop may be compromised.”

It took the company another five days before the company brought in incident responders to handle the outbreak, the source said. Many of the back-end servers were running old and outdated Windows operating systems that are no longer supported. Most hadn’t received security patches in years.

The source said they were “surprised” an attack hadn’t come sooner given the age of their systems.

A day after the attack hit, staff found the backup system wasn’t configured properly and were unable to retrieve the data for days until the company signed an expensive contract to bring in Cisco incident responders. A spokesperson for Cisco did not immediately comment. The company’s IT staff had to effectively rebuild the entire network from scratch. Since the outbreak, the company has spent “hundreds of thousands” on new hardware, software and recovery costs.

“Once the backups didn’t work, they started throwing money at the problem,” the person said.

The ransomware infection, understood to be iEncrypt (related to BitPaymer) per a screenshot seen by TechCrunch, was triggered overnight on March 21, weeks after the FBI contacted Arizona to warn of an apparent Dridex malware infection. The FBI declined to comment, but the source said incident responders believed Arizona’s systems had been compromised for at least a couple of months.

The ransom note asked to email the attacker “to get the ransom amount.” There’s no known decryption tool for iEncrypt.

Dridex is delivered through a malicious email attachment. Once the implant installs, the attacker can gain near-unfettered access to the entire network and can steal passwords, monitor network traffic and deliver additional malware. With help from international partners, the FBI took down the password-stealing botnet in 2015, but the malware continues to pose a threat. More recently, Dridex has been used to deliver ransomware to victims.

Kaspersky said two years after the takedown that the malware is "still armed and dangerous."

Incident responders seem to believe Arizona's earlier Dridex compromise may have led to the subsequent ransomware infection.

"Initially, Dridex was used to steal credentials to enable wire fraud, but since 2017 it is more commonly observed running more targeted and higher value operations," said Adam Meyers, vice president of intelligence at security firm CrowdStrike. He said the company has "observed this malware being used to deploy enterprise ransomware, which we call 'Big Game Hunting.' "

The ransomware also infected the company's Windows-powered Exchange server, knocking out email across the entire company. Although its Unix systems were unaffected, the ransomware outbreak left the company without any computers able to process customer orders for almost a week. Staff began processing orders manually several days into the outage.

"We were losing millions of dollars a day in sales," the source said. "It was a complete shitshow."

The company still has a ways to recover from the ransomware attack. The source put the figure at "about 60 percent up-and-running," but the company's security awareness has improved.

A spokesperson for Arizona Beverages did not respond to an email requesting comment. Phone lines to the company did not appear to be functioning. We sent several messages to senior executives via LinkedIn prior to publication but did not hear back.

It's the latest in an uptick in high-profile ransomware events in recent weeks.

Last year, German manufacturer KrausMaffei was also said to be hit on November 21 by the same iEncrypt ransomware, based off a leaked screenshot of the ransom note. Similar initial ransomware infections have been connected to later ransomware attacks. Trend Micro said in December that Dridex and other malware families like Emotet were linked. Weeks before Arizona's outbreak, a local Georgia county was hit by a similar ransomware attack.

> Aluminum manufacturing giant Norsk Hydro shut down by ransomware

---