

Ransomware Struck Another Pipeline Firm—and 70GB of Data Leaked

 [wired.com/story/linestar-pipeline-ransomware-leak](https://www.wired.com/story/linestar-pipeline-ransomware-leak)

Andy Greenberg

June 7, 2021



When ransomware hackers hit Colonial Pipeline last month and shut off the distribution of gas along much of the East Coast of the United States, the world woke up to the danger of digital disruption of the petrochemical pipeline industry. Now it appears another pipeline-focused business was also hit by a ransomware crew around the same time, but kept its breach quiet—even as 70 gigabytes of its internal files were stolen and dumped onto the dark web.

A group identifying itself as Xing Team last month posted to its dark web site a collection of files stolen from LineStar Integrity Services, a Houston-based company that sells auditing, compliance, maintenance, and technology services to pipeline customers. The data, first spotted online by the WikiLeaks-style transparency group Distributed Denial of Secrets, or DDoSecrets, includes 73,500 emails, accounting files, contracts, and other business documents, around 19 GB of software code and data, and 10 GB of human resources files that includes scans of employee driver's licenses and Social Security cards. And while the breach doesn't appear to have caused any disruption to infrastructure like the Colonial Pipeline incident, security researchers warn the spilled data could provide hackers a roadmap to more pipeline targeting.

DDoSecrets, which makes a practice of trawling data leaked by ransomware groups as part of its mission to expose data it deems worthy of public scrutiny, published 37 gigabytes of the company's data to its leak site on Monday. The group says it was careful to redact potentially sensitive software data and code—which DDoSecrets says could enable follow-on hackers to find or exploit vulnerabilities in pipeline software—as well as the leaked human resources material, in an effort to leave out LineStar employees' sensitive, personally identifiable information.

But the unredacted files, which WIRED has reviewed, remain online. And they may include information that could enable follow-on targeting of other pipelines, argues Joe Slowik, a threat intelligence researcher for security firm Gigamon who has focused on critical infrastructure security for years as the former head of incident response at Los Alamos National Labs. While Slowik notes that it's still not clear what sensitive information might be included in the leak's 70 GB, he worries that it could include information about the software architecture or physical equipment used by LineStar's customers, given that LineStar provides information technology and industrial control system software to pipeline customers.

"You can use that to fill in lots of targeting data, depending on what's in there," says Slowik. "It's very concerning, given the potential that it's not just about people's driver's license information or other HR related items, but potentially data that relates to the operation of these networks and their more critical functionality."

Xing Team is a relatively new entrant to the ransomware ecosystem. But while the group writes its name with a Chinese character on its dark web site—and comes from the Mandarin word for “star”—there's little reason to believe the group is Chinese based on that name alone, says Brett Callow, a ransomware-focused researcher with antivirus firm Emsisoft. Callow says he's seen Xing Team use the rebranded version of Mount Locker malware to encrypt victims' files, as well as threaten to leak the unencrypted data as a way to extort targets into paying. In the case of LineStar, Xing Team appears to have followed through on that threat.

That leak could in turn serve as a stepping stone for other ransomware hackers, who frequently comb dark web data dumps for information that can be used to impersonate companies and target their customers. "If you were to steal data from a pipeline company, that could possibly enable you to construct a fairly conventional spearphishing email to another pipeline company," says Callow. "We absolutely know that groups do that."

LineStar did not respond to multiple requests for comment prior to publication, but sent an emailed statement several hours after this story went live. "LineStar is a small, private company and we were the victim of a ransomware attack in late April that targeted corporate data. There was no impact to either internal or customer operations," said LineStar CFO Chris Boston in the statement. "Immediately following the attack, we notified our employees of a potential breach involving employee personal information, engaged third-party IT experts and notified the FBI. We have been taking every reasonable measure to protect our

employees while responding to an internal data breach and subsequent theft." Boston further claimed that "comparisons made" in this story were "completely inaccurate and provably untrue," but did not provide any specific objections.

DDoSecrets' practice of republishing the leaked data of ransomware victims—even in a redacted form—has been criticized for amplifying ransomware groups' coercive techniques. But the group's cofounder Emma Best, who uses the pronoun "they," argues that doing so for the LineStar leak in particular helps to shine a spotlight on an industry with a long record of environmental scandals. The Colonial Pipeline itself leaked 1.2 million gallons of gasoline into a nature preserve in North Carolina less than a year prior to being targeted by ransomware, Best points out. "To torture a metaphor, fuel is the fuel of our economy, but it's also a poison when they frequently leak or the pipeline's construction, operation, or maintenance infringe on communities, typically already marginalized ones," Best told WIRED in a text interview.

Best notes that even the shutdown of the pipeline following Colonial's ransomware incident in May, which triggered gas shortages across the East Coast, wasn't primarily due to safety concerns, but business and billing issues. "This isn't an industry that has the public interest at heart," Best writes. They didn't confirm if they had found any evidence of wrongdoing in the leaked LineStar files, but argue that it's noteworthy either way. "With some industries, you have to stop and study them regardless of individual wrongdoing because the industry itself is either so inherently harmful or fraught with danger that to not study it would be reckless."


The breach of a second pipeline firm by ransomware operators after Colonial's shutdown may seem to signal a trend of cybercriminal hackers specifically targeting critical infrastructure. But Emsisoft's Brett Callow points out that ransomware groups like Xing Team are targeting companies mostly indiscriminately, casting a wide net as they seek to maximize their ransom payments.

"There has been a lot of talk about critical infrastructure being targeted in this war-like situation, but that is really bullshit," Callow says. "They are just going after everybody. It's a feeding frenzy."

That hacking epidemic, however, now extends to the industrial backbone of the American economy. And with the breach of a company that serves as a hub of one such industry, the stakes are only getting higher.

Updated 6/8/21 4:00pm EST with a comment from LineStar.

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- Freedom, mayhem, and the [uncertain future of Revel mopeds](#)
- The hostile takeover of a [Microsoft Flight Simulator server](#)

- Goodbye Internet Explorer—and good riddance
- How to take a slick, professional headshot with your phone
- Online dating apps are actually kind of a disaster
- 👁 Explore AI like never before with our new database
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- ✨ Optimize your home life with our Gear team's best picks, from robot vacuums to affordable mattresses to smart speakers