Take down: Hackers looking to shut down factories for pay

August 9 2017, by Emery P. Dalesio

This undated photo provided by AW North Carolina shows production operations inside the company's Durham, N.C., factory. Online thieves are increasingly hitting today's just-in-time manufacturing sector with cyberattacks that demand ransom to make computer malware go away. Malware entered the North Carolina transmission plant's computer network via email last August, spreading like a virus and threatening to lock up the production line until the company paid a ransom. (AW North Carolina via AP)

The malware entered the North Carolina transmission plant's computer

network via email last August, just as the criminals wanted, spreading like a virus and threatening to lock up the production line until the company paid a ransom.

AW North Carolina stood to lose $270,000 in revenue, plus wages for idled employees, for every hour the factory wasn't shipping its crucial auto parts to nine Toyota car and truck plants across North America, said John Peterson, the plant's information technology manager.

The company is just one of a growing number being hit by cyber-criminals looking for a payday.

While online thieves have long targeted banks for digital holdups, today's just-in-time manufacturing sector is climbing toward the top of hackers' hit lists.

Production lines that integrate computer-imaging, barcode scanners and measuring tolerances to a hair's width at multiple points are more vulnerable to malevolent outsiders.

"These people who try to hack into your network know you have a set schedule. And they know hours are meaningful to what you're doing," Peterson said in an interview. "There's only a day and a half of inventory in the entire supply chain. And so if we don't make our product in time, that means Toyota doesn't make their product in time, which means they don't have a car to sell on the lot that next day. It's that tight."

This undated photo provided by AW North Carolina shows production operations inside the company's Durham, N.C., factory. Online thieves are increasingly hitting today's just-in-time manufacturing sector with cyberattacks that demand ransom to make computer malware go away. Malware entered the North Carolina transmission plant's computer network via email last August, spreading like a virus and threatening to lock up the production line until the company paid a ransom. (AW North Carolina via AP)

He said that creates pressure on manufacturers to make the criminals go away by paying the sums demanded.

"They may not know what that number is, but they know it's not zero. So what is that number? Where do you flinch?"

Last August at the 2,200-worker Durham transmission factory, the computer virus coursed through the plant's network, flooding machines

with data and stopping production for about four hours, Peterson said.

Data on some laptops was lost, but the malware was blocked by a firewall when it tried to exit the plant's network and put the hackers' lock on the plant's computer network.

The plant was hit again in April, this time by different crooks using new malware designed to hold data or devices hostage to force a ransom payment, Peterson said. The virus was contained before affecting production, and no ransom was paid to either group, he said.

Manufacturers, government and financial firms are now the top targets globally for illicit intrusions by criminals, foreign espionage agencies and others up to no good, according to a report this spring by NTT Security.

This undated photo provided by AW North Carolina shows production

operations inside the company's Durham, N.C., factory. Online thieves are increasingly hitting today's just-in-time manufacturing sector with cyberattacks that demand ransom to make computer malware go away. Malware entered the North Carolina transmission plant's computer network via email last August, spreading like a virus and threatening to lock up the production line until the company paid a ransom. (AW North Carolina via AP)

A survey of nearly 3,000 corporate cybersecurity executives in 13 countries last year by Cisco Systems Inc. found about one out of four manufacturing organizations reported cyberattacks that cost them money in the previous 12 months.

Since 2015, U.S. manufacturers considered "critical" to the economy and to normal modern life, like makers of autos and aviation parts, have been the main targets of cyberattacks—outstripping energy, communications and other critical infrastructure, according to Department of Homeland Security incident response data. The numbers may be imprecise because companies in key industries often don't report attacks for fear of diminished public perception.

But attacks demanding ransom against all U.S. institutions are spiraling higher. The FBI's Internet Crime Complaint Center received 2,673 ransomware reports in the year ending last September—nearly double from 2014.

While manufacturers are increasingly prey to these cyber-stickups, it may just be because criminals are playing the odds and striking as many enterprises of all types as they can across a targeted region, said John Miller, who heads a team at cybersecurity firm FireEye that tracks money-driven online threats.

Attackers "aren't necessarily going after manufacturing to the exclusion of other sectors or with a preference above other sectors. It's more that, 'OK, we're going to try to infect everybody in this country that we can,'" Miller said.

One high-profile example came in May and June, when auto manufacturers including Renault shut down production after they were swept up in the worldwide onslaught of the WannaCry ransomware virus.

This undated photo provided by AW North Carolina shows the outside of the company's Durham, N.C., factory. Online thieves are increasingly hitting today's just-in-time manufacturing sector with cyberattacks that demand ransom to make computer malware go away. Malware entered the North Carolina transmission plant's computer network via email last August, spreading like a virus and threatening to lock up the production line until the company paid a ransom. (AW North Carolina via AP)

But attackers also are increasingly injecting ways to remotely control the robots and other automated systems that control production inside targeted factories.

The threat of computer code tailored to hit specific targets has been around since researchers in 2010 discovered Stuxnet, malware apparently designed to sabotage Iran's nuclear program by causing centrifuge machines to spin out of control. Stuxnet is widely believed to be a covert American and Israeli creation, but neither country has officially acknowledged a role in the attack.

Malicious software that attacked Ukraine's electricity grid last December was built to remotely sabotage circuit breakers, switches and protection relays, researchers said.

Cyberattacks that reach into industrial control systems have doubled in the past two years in the U.S. to nearly four dozen so far in the federal fiscal year that ends in September, outstripping last year's total, according to DHS data.

"I think the emerging threat you're going to see in the future now is really custom ransomware that's going to be targeted more toward individual companies," said Neil Hershfield, the acting director of the DHS team that handles emergency response to cyberattacks on industrial control systems.