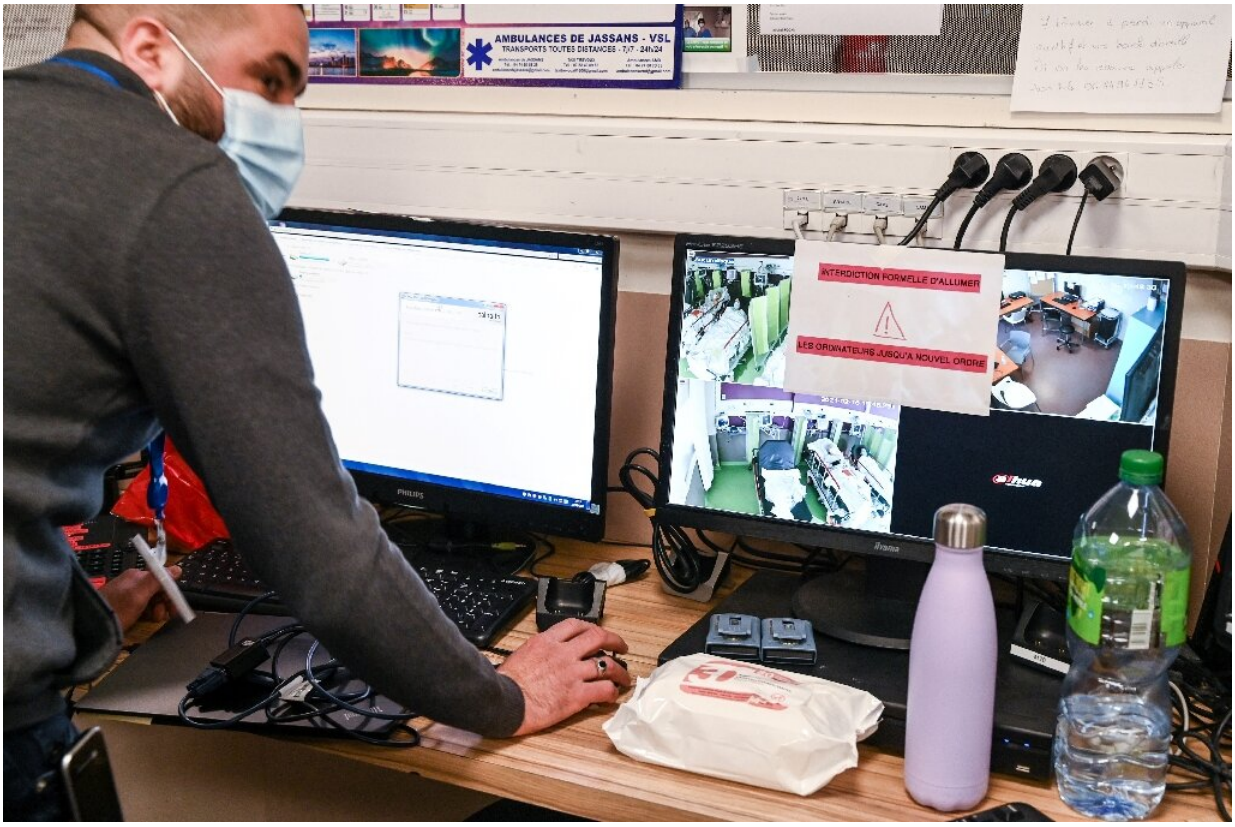
As COVID cases rose, so did hospital hacks in France

May 26 2021



Separate ransomware attacks have knocked out computer systems in more than half a dozen French hospitals, forcing them to return to using pen and paper.

At 2:00 a.m. on a day in early February, the deputy director of the main hospital in the southwestern French town of Dax took an urgent call

from a normally unflappable colleague in the IT department.

"He's usually very calm, but I could tell in his voice that there was something very unusual," Aline Gilet-Caubere told AFP from her office.

The technician reported how personnel working overnight were suddenly unable to use their computers, which were flashing up a ransom note saying the hospital's systems had been hacked and encrypted.

The attackers made a classic demand: they would provide a key to reverse the damage upon payment in Bitcoin, and they supplied email addresses to arrange the transfer.

"We imagined we were a sanctuary as a hospital, with our role, that no-one would dare (target us)," Gilet-Caubere said. "But not at all, in fact. That's part of the psychological shock."

Unwilling and unable to pay, hospital managers had no choice but to order a return to the pre-internet, pre-computer era.

In the middle of the COVID-19 pandemic, paper records reappeared. Doctors took up pencils again and scribbled notes.

A manual system using stickers and flowcharts kept track of patients as they moved around.

There was no telephone system or email.

Payroll and supplier data were lost. All of the roughly 110-120 different software platforms run in the hospital were out-of-order.

And more than three months later, after weeks of chaos and frustration for medics, as well as months of work by specialised cybercrime

technicians, the hospital is still not back to normal.

"We can't say when everything will be finished. We keep discovering problems," Gilet-Caubere said.

French President Emmanuel Macron pledged an extra billion euros for cybersecurity in the health sector in February.

'Crisis in a crisis'

But the 2,200 staff at the Dax hospital were not the only ones to find themselves battling a public health emergency over the last 18 months and the worst technology outages of their careers.

Elsewhere in France, at least half a dozen other public hospitals have had their operations severely disrupted after being targeted by ransomware hackers since the start of the COVID outbreak in Europe in early 2020.

Cyrille Politi, chief technology advisor at the Hospital Federation of France, has no doubt that hackers have stepped up attacks—and have stepped over a moral line that made public hospitals mostly off-limits.

"It's a real paradigm shift," he told AFP.

According to French Digital Affairs Minister Cedric O, 27 hospitals experienced some form of cyberattack last year, including ransomware, while there was one per week on average in the first two months of the year.

In February, as alarm grew about the vulnerability of the health system, President Emmanuel Macron asked to be briefed personally by staff from Dax and Villefranche-sur-Saone.

He announced an extra billion euros for cybersecurity in the health sector, calling the spate of attacks at the height of the pandemic a "crisis within a crisis".

Impunity

Though uncommon in France, attacks on hospitals have been a regular feature of global cybercrime for years, particularly in the United States.

"What these actors (hackers) are looking for across the board are targets that have an operational imperative," says Adam Meyers from US-based cybersecurity firm CrowdStrike.

"They target things like healthcare because healthcare is one of the

unfortunate sectors where it's not a money decision, it's a life-or-death decision."

The Dax hospital in southwest France employs 2,200 people.

And in the US too, the pandemic was seen as a business opportunity by some hackers.

After dozens of attacks in late 2020, the FBI and US authorities warned about "credible information of an increased and imminent cybercrime threat" to hospitals and healthcare providers.

The bad news for hospitals, and other potential targets, is that ransomware attacks are becoming more sophisticated and more numerous.

Everything from information about the IT vulnerabilities of individual organisations to hacking and encryption technology is for sale online in closed criminal forums.

Gangs with names such as Evil Corp or DarkSide operate beyond the reach of Western law enforcement in Russia, or former Soviet republics, cybersecurity firms say.

The attack on the Dax hospital used a well-known malware called Ryak, and IT director Gilbert Martin said the hackers left "Russian traces".

But with the risks low, profits high, and the potential targets almost limitless, ransomware hacking is growing exponentially globally.

Victims made an estimated $350 million in payments in cryptocurrencies in 2020, an increase of 311 percent from 2019, according to specialised analysis company Chainalysis.

Earlier this month, DarkSide created fuel shortages in the US and extracted more than four million dollars from Colonial Pipeline, a company carrying gasoline and diesel from the US Gulf coast to the northeast.

"Those who ply their trade in this multi-billion dollar sector are operating with almost complete impunity," Brett Callow from cybercrime firm Emsisoft told AFP.

For radiologist Nicolas Pontier at the Dax hospital, the experience of being unable to treat his cancer patients was a wake-up call that he hopes

will be heeded by others.

"I never imagined I'd have to stop for two months," he said. "I thought in a week or two it would be sorted out. We still don't have a fully functional system."