How France's TV5 was almost destroyed by 'Russian hackers'

bbc.com/news/technology-37590375

By Gordon Corera

By Gordon Corera
Security correspondent, BBC News

Published
10 October 2016

Image source, Getty Images

Image caption,
TV5Monde's TV station, website and social media accounts were all hit in April 2015

A powerful cyber-attack came close to destroying a French TV network, its director-general has told the BBC.

TV5Monde was taken off air in April 2015. A group calling itself the Cyber Caliphate, linked to so-called Islamic State, first claimed responsibility.

But an investigation now suggests the attack was in fact carried out by a group of Russian hackers.

The attack used highly targeted malicious software to destroy the TV network's systems.

Image source, Getty Images

Image caption,
Yves Bigot is the director-general of TV5Monde

Corrupted data

Wednesday 8 April was a big day for Yves Bigot, the director-general of TV5Monde.

His network, which broadcasts around the world, had just launched its latest channel. French ministers had been in attendance at the Paris headquarters.

That evening Mr Bigot went for dinner to celebrate with a counterpart from Radio Canada.

Just as they were being served their appetisers at 20:40 local time, a flood of texts and calls informed him that all 12 channels had gone off air.

"It's the worst thing that can happen to you in television," Mr Bigot told me in his Paris office.

It quickly became clear that the network had been subject to a serious cyber-attack.

"We were a couple of hours from having the whole station gone for good."

Image source, Tv5monde

Image caption,
Screens went blank in the foyer of TV5Monde

It was a race against time - more systems were corrupted with every passing minute. Any substantial delay would have led satellite distribution channels to cancel their contracts, placing the entire company in jeopardy.

"We were saved from total destruction by the fact we had launched the channel that day and the technicians were there," said Mr Bigot.

"One of them was able to locate the very machine where the attack was taking place and he was able to cut out this machine from the internet and it stopped the attack."

At 05:25 local time, one channel was restored. Others followed later that morning.

"We owe a lot to the engineer who unplugged that particular machine. He is a hero here," Mr Bigot said.

Bespoke attack

The attack was far more sophisticated and targeted than reported at the time. The perpetrators had first penetrated the network on 23 January.

They carried out reconnaissance of TV5Monde to understand the way in which it broadcast its signals. They then fabricated bespoke malicious software to corrupt and destroy the internet-connected hardware that controlled the TV station's operations - such as the encoder systems used to transmit programmes.

Image source, Getty Images

Image caption,
Twelve TV5Monde channels were taken off air

The attackers used seven different points of entry. Not all of them were part of TV5Monde or in France. In one case, a company based in the Netherlands was targeted because it supplied the remote controlled cameras used in TV5's studios.

Who was responsible?

At 20:40 local time - when the first calls were made - the people in charge of digital content at the broadcaster told Mr Bigot that messages had been posted on the channel's Twitter and Facebook pages.

The hackers said they were from a group calling themselves the Cyber Caliphate, and made threats against France. It was only a few months since the Charlie Hebdo attacks and it seemed this could have been a follow-up strike by so-called Islamic State (IS).

Image source, Tv5monde

Image caption,
The TV5Monde website was defaced

But as the investigation by French authorities began, a different picture began to emerge.

France's cyber-agency told Mr Bigot to be careful about linking the incident directly to IS - instead he was advised to say only that the messages claimed to be from IS.

The investigators had come to believe that the attackers had used the jihadist posts to try to cover their tracks.

Mr Bigot was later told evidence had been found that his network had been attacked by a group of Russian hackers, who are known as APT 28.

Mysterious motive

"I have absolutely no idea," said Mr Bigot, when I asked why TV5Monde had been targeted.

He explained that the investigators had only been able to prove two things.

Firstly, that the attack was designed to destroy the channel, and secondly, that it was linked to APT 28.

"There are two things that the investigation won't probably be able to achieve," he added.

"The first one is why us - why TV5Monde?

"And the second one is: Who gave the order and the money to that Russian group of hackers to actually do it?"

Destructive intent

It's not uncommon for cyber-attackers to enter a target's network to look for information.

But what happened to TV5 was not espionage - the aim was destruction. And that is indicative of a new trend: attacks with physical-world consequences.

Arguably, the pioneering state-backed attack of this type was Stuxnet.

This was carried out - it is widely believed - by the US and Israel against Iran's nuclear programme and involved damaging the centrifuge programme at Natanz.

More recently, a power station in Ukraine was switched off by cyber-attackers.

The TV5 attack fits into this pattern of highly-targeted attacks, rather than the kind of general criminal activity typically seen on the web.

The issue as to why Russian hackers targeted the company is one that has occupied intelligence analysts in the UK and US, as well as France.

In London, the conclusion was that it was most likely an attempt to test forms of cyber-weaponry as part of an increasingly aggressive posture.

Dangerous precedent

The impact on TV5 was enormous.

In the immediate aftermath, staff had to return to using fax machines as they could not send emails.

"We had to wait for months and months before we reconnected to the internet," recalled Mr Bigot.

The financial cost was €5m ($5.6m; £4.5m) in the first year, followed by over €3m ($3.4m; £2.7m) every following year for new protection.

But the biggest challenge has been to the way the company works. Every employee has had to change their behaviour.

Special authentication procedures are needed to check email from abroad, flash drives have to be tested before being inserted.

For a media company that exists by moving material in and out of its systems, the costs in efficiency have been real.

"We never will be as we were before," said Mr Bigot. "It is too dangerous."

More on this story

Russia's 'cyber war' against the West

8 October 2016

Related Internet Links

TVMonde5

The BBC is not responsible for the content of external sites.