Fujifilm confirms ransomware attack disrupted business operations

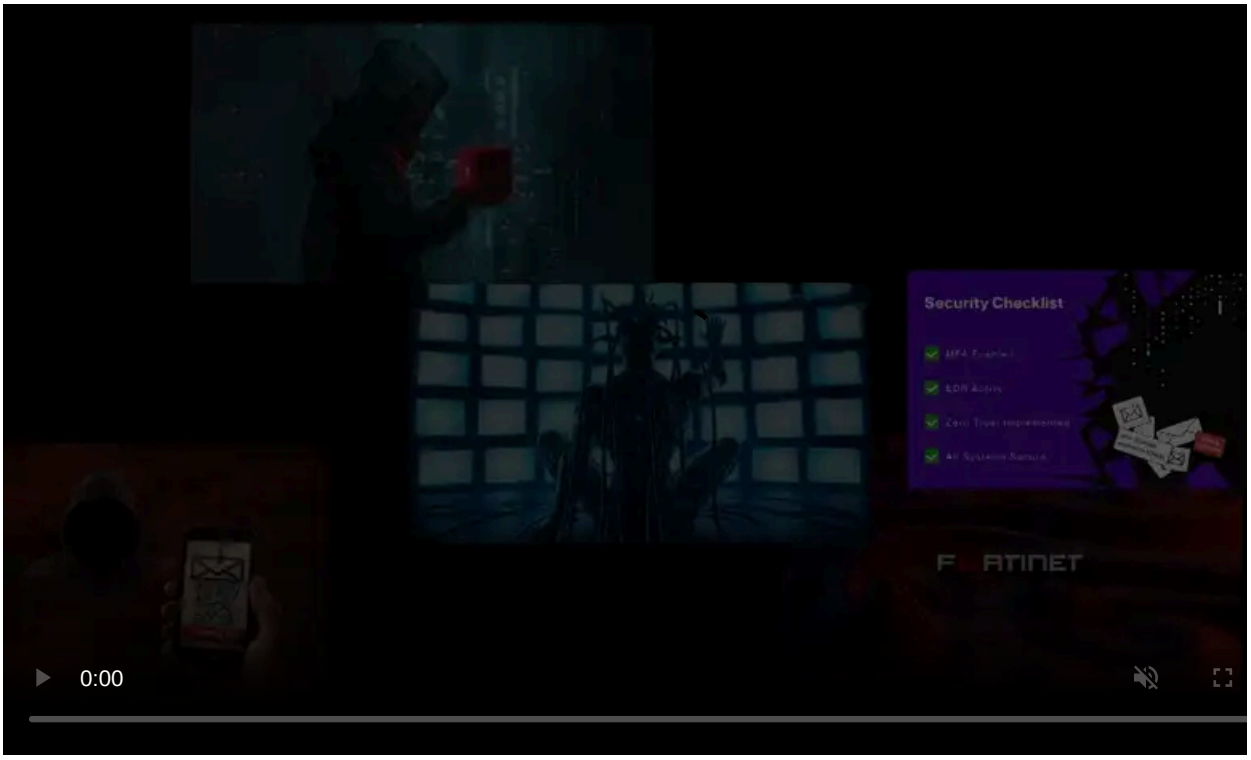
By Lawrence Abrams

Published: 2021-06-04 · Archived: 2026-04-06 15:38:33 UTC

Today, Japanese multinational conglomerate Fujifilm officially confirmed that they had suffered a ransomware attack earlier this week that disrupted business operations.

On June 2, Fujifilm disclosed that they suffered a cyberattack but would not confirm if the attack was caused by ransomware.

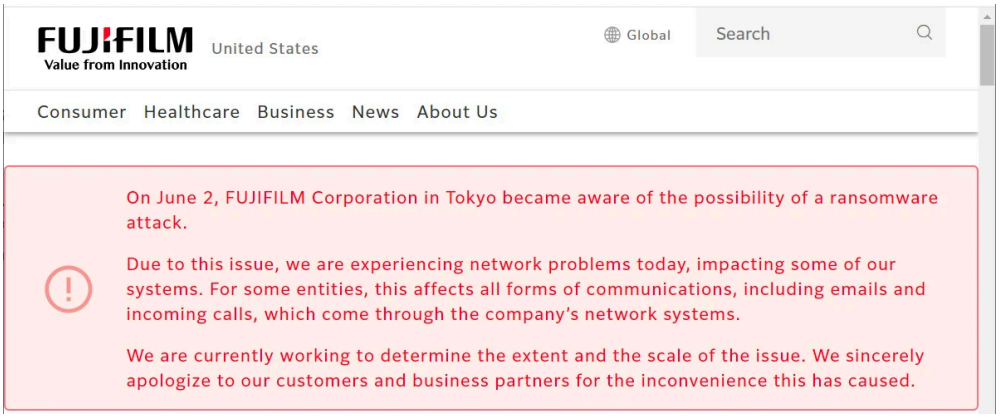
However, in multiple conversations with Fujifilm employees, BleepingComputer learned that it was internally known that the attack was caused by ransomware and that the company was forced to take down portions of its network worldwide.


Security Checklist
0:00

Visit Advertiser websiteGO TO PAGE

At approximately 10:0 AM EST on Tuesday, Fujifilm told employees to shut off their computers and all servers immediately. Furthermore, the network outage prevented access to email, the billing system, and a reporting system.

To alert their customers, Fujifilm also added notifications to their websites warning customers about the disruption to their business.



Notification about cyberattack on Fujifilm website

Fujifilm confirms a ransomware attack

Today, Fujifilm has released an updated statement that officially confirms that the attack was caused by ransomware deployed on the night of June 1st, 2021.

> - We confirmed that the unauthorized access we recognized on the night of June 1, 2021 was ransomware.
> - We have confirmed that the scope of impact is limited to specific networks in the country.
> - Since the range has been identified, from today, we are proceeding with the operation of servers and personal computers that have been confirmed to be safe, and the networks that were blocked are also starting communication in sequence.

While it has not been disclosed what ransomware gang was behind the attack, it is believed to be the REvil ransomware operation.

Advanced Intel's Vitali Kremez told BleepingComputer that Fujifilm had recently been infected by the Qbot trojan, which is currently partnering with the REvil ransomware operation to provide remote access to compromised networks.

Using the remote access provided by the trojan, the REvil ransomware gang will infiltrate a network and spread slowly to other devices while stealing unencrypted data.

Once they gain access to a Windows domain administrator account and have harvested any data of value, they deploy the ransomware throughout the system to encrypt devices.

If Fujifilm did not pay the ransom, we will know soon enough who was responsible, as the data will likely be released on a ransomware data leak site as a further method to leverage a ransom payment.

Ransomware attacks see increased scrutiny

While ransomware attacks have been a problem since 2012 and a target of numerous law enforcement operations in the past, they have seen increased scrutiny recently after gangs targeted critical infrastructure, healthcare, and the food supply.

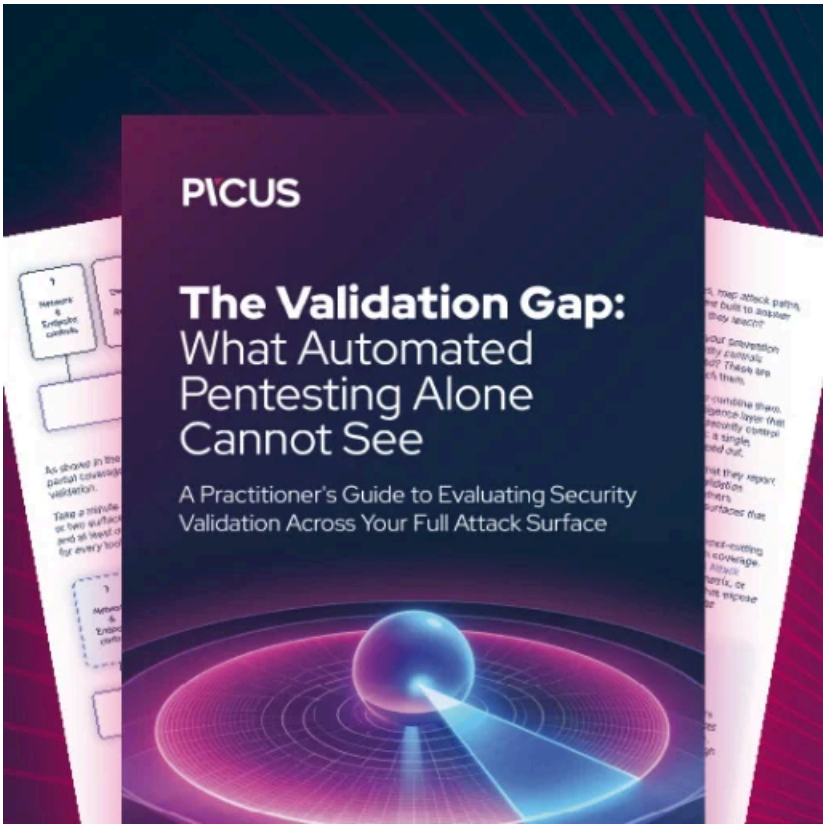
Last month, the DarkSide ransomware operation attacked Colonial Pipeline, the largest US fuel pipeline. It led to a shutdown of the pipeline and a temporary shortage of gas in some states.

Also, last month, Ireland's HSE, the country's publicly funded healthcare system, and the Department of Health were attacked by the Conti ransomware gang, leading to significant disruption in healthcare services.

More recently, JBS, the world's largest meat producer, was attacked by the REvil ransomware operation, which led to the temporary shut down of production sites. Today, JBS announced that they are back online and fully operational after restoring from backups.

As most of the large ransomware operations are believed to be operated out of Russia, White House Press Secretary Jen Psaki said that President Biden would be discussing these attacks with Russian President Vladimir Putin at the June 16th Geneva summit.

"It will be a topic of discussion in direct, one-on-one discussions — or direct discussions with President Putin and President Biden happening in just a couple of weeks," Psaki said at the press briefing.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/fujifilm-confirms-ransomware-attack-disrupted-business-operations/