

FUJIFILM shuts down network after suspected ransomware attack

bleepingcomputer.com/news/security/fujifilm-shuts-down-network-after-suspected-ransomware-attack/

Lawrence Abrams

By

[Lawrence Abrams](#)

- June 2, 2021
- 03:03 PM
- 0



FujiFilm is investigating a ransomware attack and has shut down portions of its network to prevent the attack's spread.

FujiFilm, also known as just Fuji, is a Japanese multinational conglomerate headquartered in Tokyo, Japan, which initially started in optical film and cameras. It has grown to include pharmaceuticals, storage devices, photocopiers and printers (XEROX), and digital cameras.

FUJIFILM earned \$20.1 billion in 2020 and has 37,151 employees worldwide.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at [+16469613731](https://www.signal.me/+16469613731) or on Wire at [@lawrenceabrams-bc](https://www.wire.com/@lawrenceabrams-bc).

Likely ransomware attack

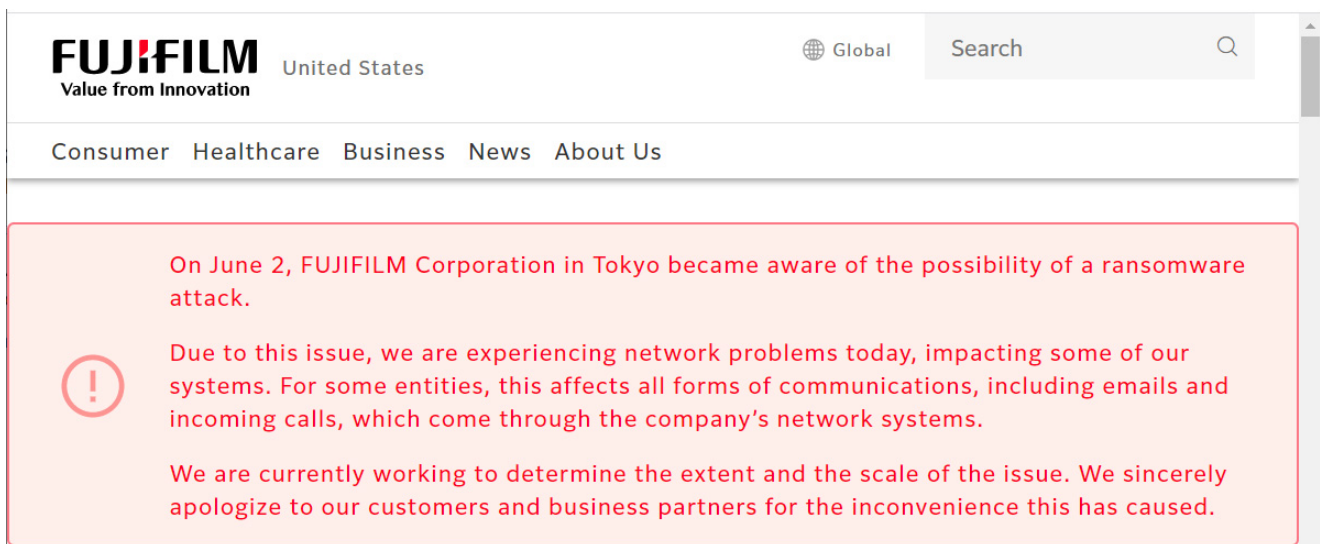
Today, FUJIFILM announced that their Tokyo headquarters suffered a cyberattack Tuesday night that they indicate is a ransomware attack.

"FUJIFILM Corporation is currently carrying out an investigation into possible unauthorized access to its server from outside of the company. As part of this investigation, the network is partially shut down and disconnected from external correspondence," FUJIFILM said in a statement.

"We want to state what we understand as of now and the measures that the company has taken. In the late evening of June 1, 2021, we became aware of the possibility of a ransomware attack. As a result, we have taken measures to suspend all affected systems in coordination with our various global entities."

"We are currently working to determine the extent and the scale of the issue. We sincerely apologize to our customers and business partners for the inconvenience this has caused."

Due to the partial network outage, FUJIFILM USA has added an alert to the top of their website stating that they are experiencing network problems that are impacting their email and phone systems.



The screenshot shows the top of the FUJIFILM USA website. The header includes the FUJIFILM logo with the tagline "Value from Innovation", the text "United States", a "Global" link with a globe icon, and a search bar. Below the header is a navigation menu with links for "Consumer", "Healthcare", "Business", "News", and "About Us". A prominent red alert banner is displayed in the main content area. The banner contains the following text:

On June 2, FUJIFILM Corporation in Tokyo became aware of the possibility of a ransomware attack.

Due to this issue, we are experiencing network problems today, impacting some of our systems. For some entities, this affects all forms of communications, including emails and incoming calls, which come through the company's network systems.

We are currently working to determine the extent and the scale of the issue. We sincerely apologize to our customers and business partners for the inconvenience this has caused.

Alert about cyberattack on FUJIFILM USA website

While FUJIFILM has not stated what ransomware group is responsible for the attack, Advanced Intel CEO [Vitali Kremez](#) has told BleepingComputer that FUJIFILM was infected with the Qbot trojan last month.

"Based on our unique threat prevention platform Andariel, FUJIFILM Corporate appeared to be infected with Qbot malware based on May 15, 2021," Kremez told BleepingComputer.

"Since the underground ransomware turmoil, the Qbot malware group currently works with the REvil ransomware group."

"A network infection attributed to QBot automatically results in risks associated with future ransomware attacks."

The operators of the Qbot trojan have a long history of working with ransomware operations to provide remote access to compromised networks.

In the past, the [ProLock](#) and [Egregor](#) ransomware gangs partnered with Qbot, but with the shutdown of those operations, the REvil ransomware operation has been utilizing the botnet.

While ransomware has been active since 2012, it has recently gained worldwide attention after the [attacks on Colonial Pipeline](#), the US's largest fuel pipeline, and the world's largest beef producer, [JBS](#).

The US government has [created a ransomware task force](#) to recommend new policies and guidelines for battling the growing threat.

Related Articles:

[Costa Rica declares national emergency after Conti ransomware attacks](#)

[The Week in Ransomware - May 6th 2022 - An evolving landscape](#)

[Conti, REvil, LockBit ransomware bugs exploited to block encryption](#)

[REvil ransomware returns: New malware sample confirms gang is back](#)

[New Black Basta ransomware springs into action with a dozen breaches](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.