FUJIFILM shuts down network after suspected ransomware attack

By
Lawrence Abrams (https://www.bleepingcomputer.com/author/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 (tel:+16469613731) or on Wire at @lawrenceabrams-bc.

Likely ransomware attack

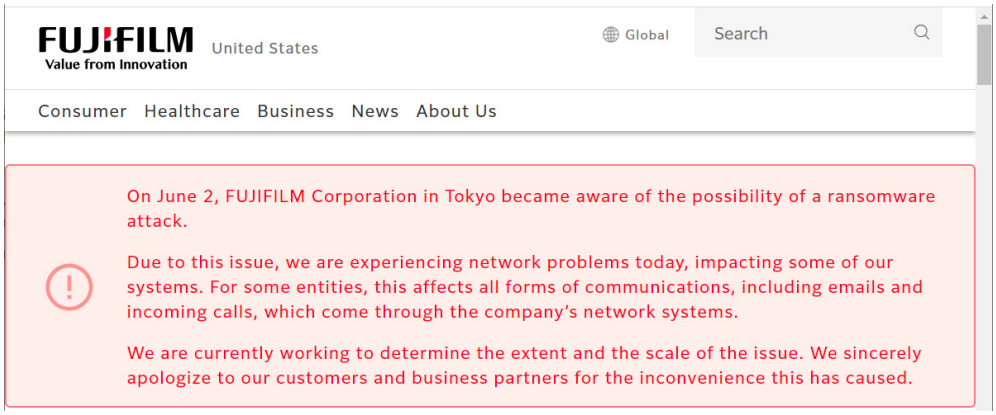
Today, FUJIFILM announced that their Tokyo headquarters suffered a cyberattack Tuesday night that they indicate is a ransomware attack.

"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.



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 (https://twitter.com/VK_Intel) 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 (https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/) and Egregor (https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/) 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 (https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/), the US's largest fuel pipeline, and the world's largest beef producer, JBS (https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/).

The US government has created a ransomware task force (https://www.bleepingcomputer.com/news/security/security-expert-coalition-shares-actions-to-disrupt-ransomware/) to recommend new policies and guidelines for battling the growing threat.

Related Articles:

Integris Health patients get extortion emails after cyberattack (https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/)

Nissan Australia cyberattack claimed by Akira ransomware gang (https://www.bleepingcomputer.com/news/security/nissan-australia-cyberattack-claimed-by-akira-ransomware-gang/)

The Rise of Ransomware in Healthcare: What IT Leaders Need to Know (https://www.bleepingcomputer.com/news/security/the-rise-of-ransomware-in-healthcare-what-it-leaders-need-to-know/)

Boeing confirms cyberattack amid LockBit ransomware claims (https://www.bleepingcomputer.com/news/security/boeing-confirms-cyberattack-amid-lockbit-ransomware-claims/)

The biggest cybersecurity and cyberattack stories of 2023 (https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2023/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

FUJIFILM (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FUJIFILM/)

QBOT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/QBOT/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)

REVIL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/REVIL/)

TOKYO (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/TOKYO/)