Shutterfly services disrupted by Conti ransomware attack

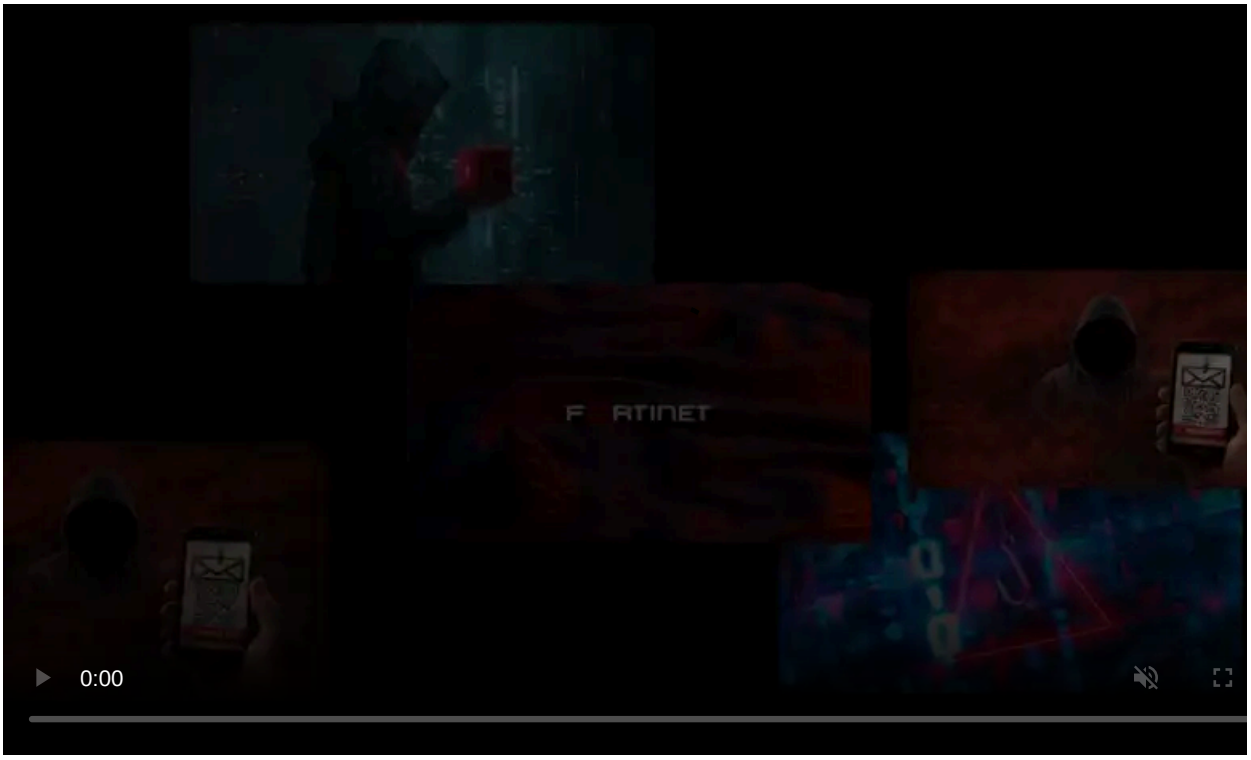
By Lawrence Abrams

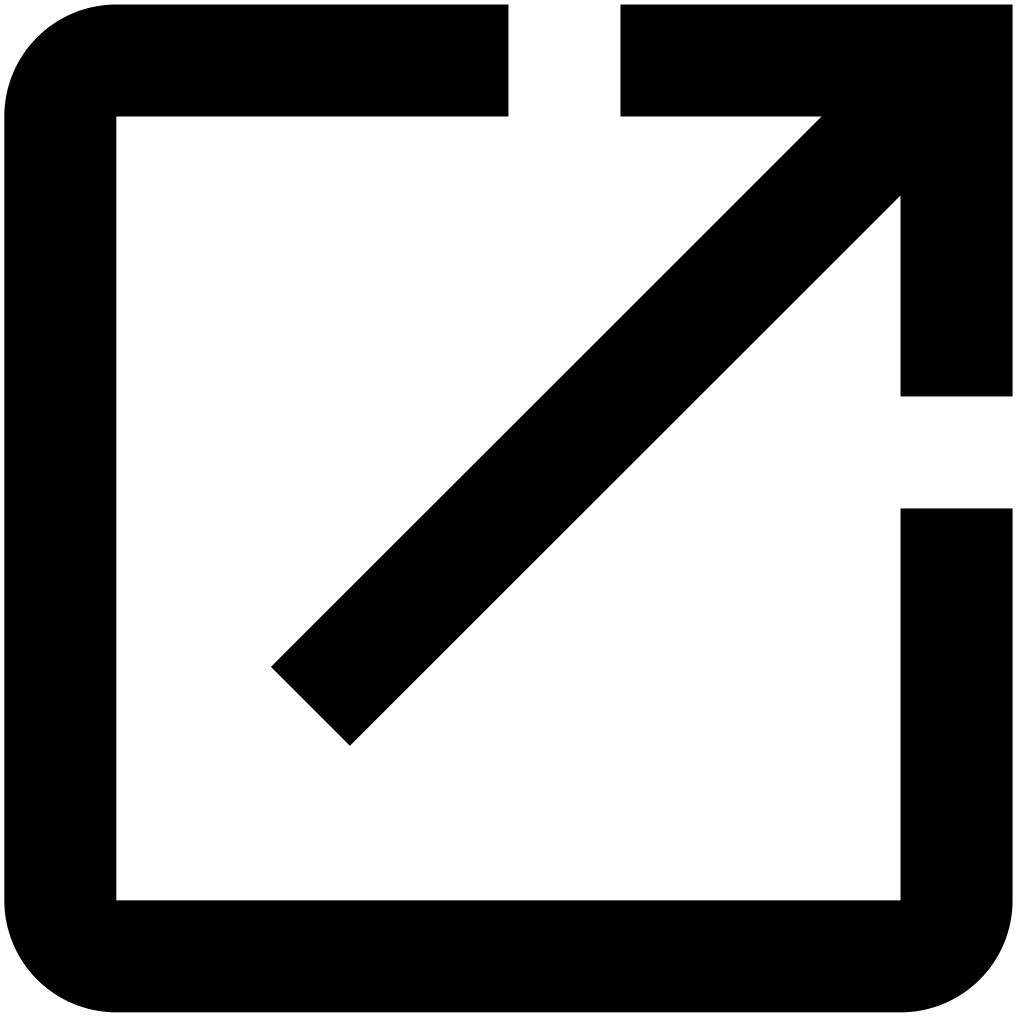
Published: 2021-12-27 · Archived: 2026-04-05 20:44:50 UTC

Photography and personalized photo giant Shutterfly has suffered a Conti ransomware attack that allegedly encrypted thousands of devices and stole corporate data.

Although many associate Shutterfly with their website, the company's photography-related services are aimed at consumer, enterprise, and education customers through various brands such as GrooveBook, BorrowLenses, Shutterfly.com, Snapfish, and Lifetouch.

The main website can be used to upload photos to create photo books, personalized stationary, greeting cards, post cards, and more.


F RTINET
0:00



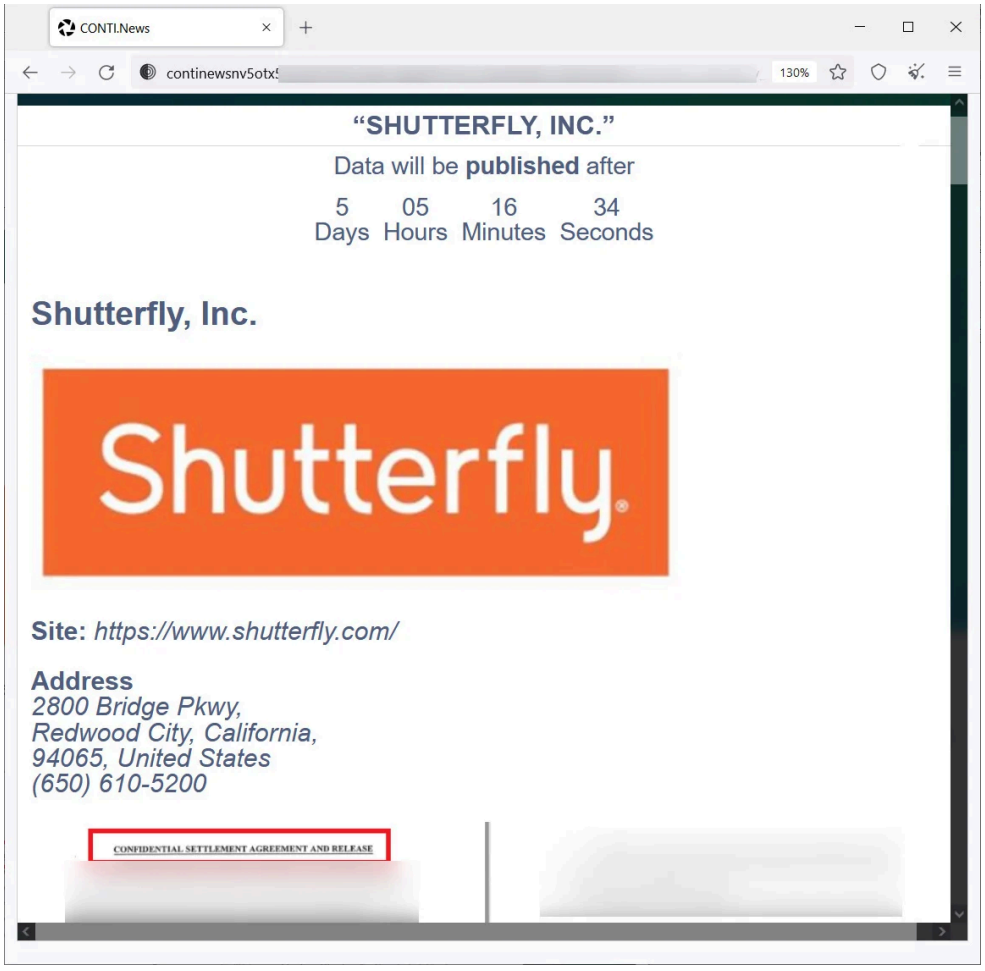
Shutterfly suffers a Conti ransomware attack

On Friday, a source told BleepingComputer that Shutterfly suffered a ransomware attack approximately two weeks ago by the Conti gang, who claims to have encrypted over 4,000 devices and 120 VMware ESXi servers.

While BleepingComputer has not seen the negotiations for the attack, we are told that they are in progress and that the ransomware gang is demanding millions of dollars as a ransom.

Before ransomware gangs encrypt devices on corporate networks, they commonly lurk inside for days, if not weeks, stealing corporate data and documents. These documents are then used as leverage to force a victim to pay a ransom under the threat that they will be publicly released or sold to other hackers.

Conti has created a private Shutterfly data leak page containing screenshots of files allegedly stolen during the ransomware attack, as part of this " double-extortion" tactic. The attackers threaten to make this page public if a ransom is not paid.



Private data leak page on Conti dark web site

BleepingComputer has been told that these screenshots include legal agreements, bank and merchant account info, login credentials for corporate services, spreadsheets, and what appears to be customer information, including the last four digits of credit cards.

Conti also claims to have the source code for Shutterfly's store, but it is unclear if the ransomware gang means Shutterfly.com or another website.

After contacting Shutterfly on Friday about the attack, BleepingCompuer was sent a statement confirming the ransomware attack late Sunday night.

This statement, shown in its entirety below, says that the Shutterfly.com, Snapfish, TinyPrints, or Spoonflower sites were not affected by the attack. However, their corporate network, Lifetouch, BorrowLeneses, and Groovebook had disrupted services.

> "Shutterfly, LLC recently experienced a ransomware attack on parts of our network. This incident has not impacted our Shutterfly.com, Snapfish, TinyPrints or Spoonflower sites. However, portions of our Lifetouch and BorrowLenses business, Groovebook, manufacturing and some corporate systems have been experiencing interruptions. We engaged third-party cybersecurity experts, informed law enforcement, and have been working around the clock to address the incident."
>
> "As part of our ongoing investigation, we are also assessing the full scope of any data that may have been affected. We do not store credit card, financial account information or the Social Security numbers of our Shutterfly.com, Snapfish, Lifetouch, TinyPrints, BorrowLenses, or Spoonflower customers, and so none of that information was impacted in this incident. However, understanding the nature of the data that may have been affected is a key priority and that investigation is ongoing. We will continue to provide updates as appropriate." - Shutterfly.

While Shutterfly states that no financial information was disclosed, BleepingComputer was told that one of the screenshots contains the last four digits of credit cards, so it is unclear if there is further, and more concerning, information stolen during the attack.

When BleepingComputer reached out to Shutterfly about the screenshot they referred us back to the original statement.

The Conti ransomware gang

Conti is a ransomware operation believed to be operated by a Russian hacking group known for other notorious malware infections, such as Ryuk, TrickBot, and BazarLoader.

This operation runs as a Ransomware-as-a-Service, where the core team develops the ransomware, maintains payment and data leak sites, and negotiates with victims. They then recruit "affiliates" who breach the corporate network, steal data, and encrypt devices.

As part of this arrangement, ransom payments are split between the core group and the affiliate, with the affiliate usually receiving 70-80% of the total amount.

Conti commonly breaches a network after a corporate device becomes infected with the BazarLoader or TrickBot malware infections, which provide remote access to the hacking group.

Once they gain access to an internal system, they spread through the network, harvest data, and deploy the ransomware.

Conti is known for attacks on other high-profile organizations in the past, including Ireland's Health Service Executive (HSE) and Department of Health (DoH), the City of Tulsa, Broward County Public Schools, and Advantech.

Due to the increased activity by the cybercrime gang, the US government recently issued an advisory on Conti ransomware attacks.

Update 12/27/21: Updated with response about financial information in stolen data.

Source: https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomware-attack/