Shutterfly discloses data breach after Conti ransomware attack

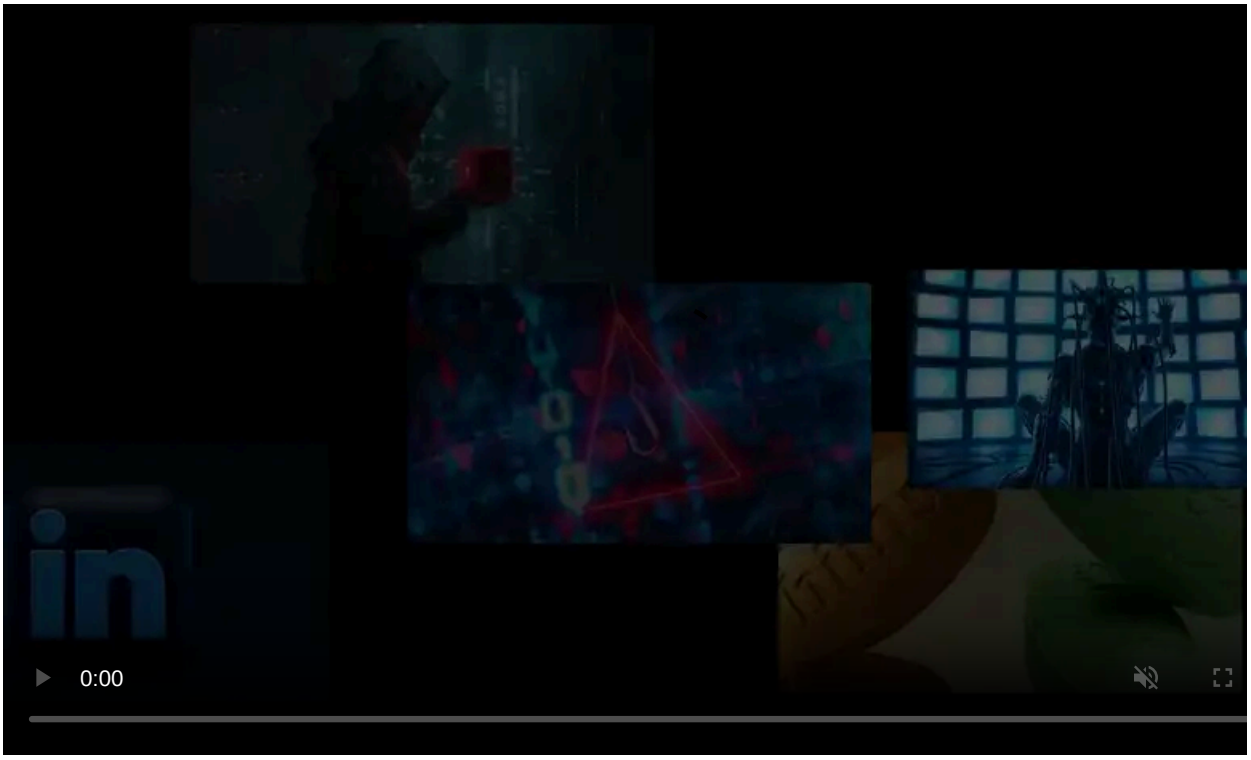
By Lawrence Abrams

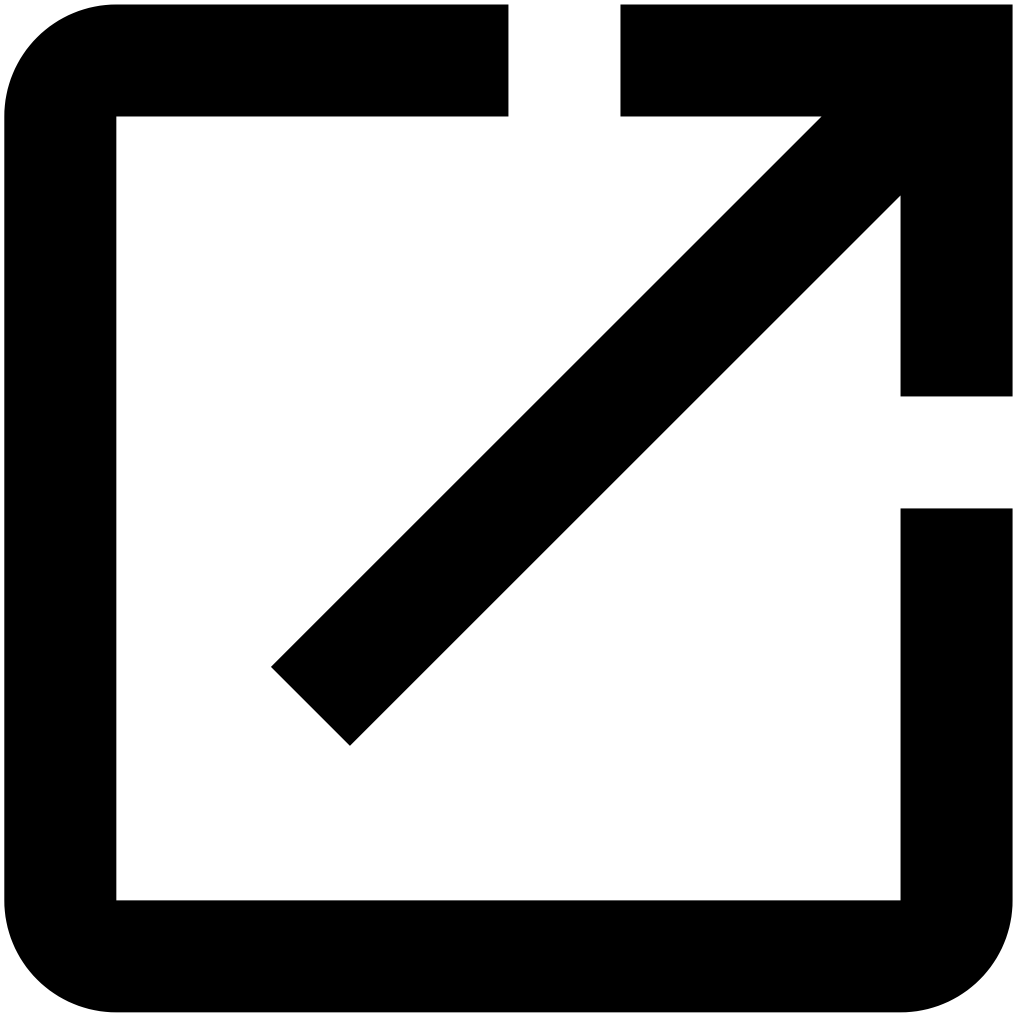
Published: 2022-03-29 · Archived: 2026-04-05 19:04:22 UTC

Online retail and photography manufacturing platform Shutterfly has disclosed a data breach that exposed employee information after threat actors stole data during a Conti ransomware attack.

Shutterfly offers photography-related services to consumers, the enterprise, and education through various brands, including Shutterfly.com, BorrowLenses, GrooveBook, Snapfish, and Lifetouch.

Today, Shutterfly disclosed that its network was breached on December 3rd, 2021, due to a ransomware attack.


0:00



Visit Advertiser websiteGO TO PAGE

During ransomware attacks, threat actors will gain access to a corporate network and steal data and files as they spread throughout the system. Once they gain access to a Windows domain controller, and after harvesting all valuable data, they deploy their ransomware to encrypt all network devices.

According to Shutterfly's data breach notification, the Conti threat actor deployed the ransomware on December 13th, 2021, when the company first became aware that they were compromised.

"The attacker both locked up some of our systems and accessed some of the data on those systems. This included access to personal information of certain people, including you," reads Shutterfly's data breach notification filed with the California Attorney General's Office.

"We believe the access occurred on or about December 3, 2021. We discovered the incident on December 13, 2021.

Shutterfly states that the documents stolen during the attack may have contained employees' personal information, including names, salary and compensation information, and FMLA leave or workers' compensation claims.

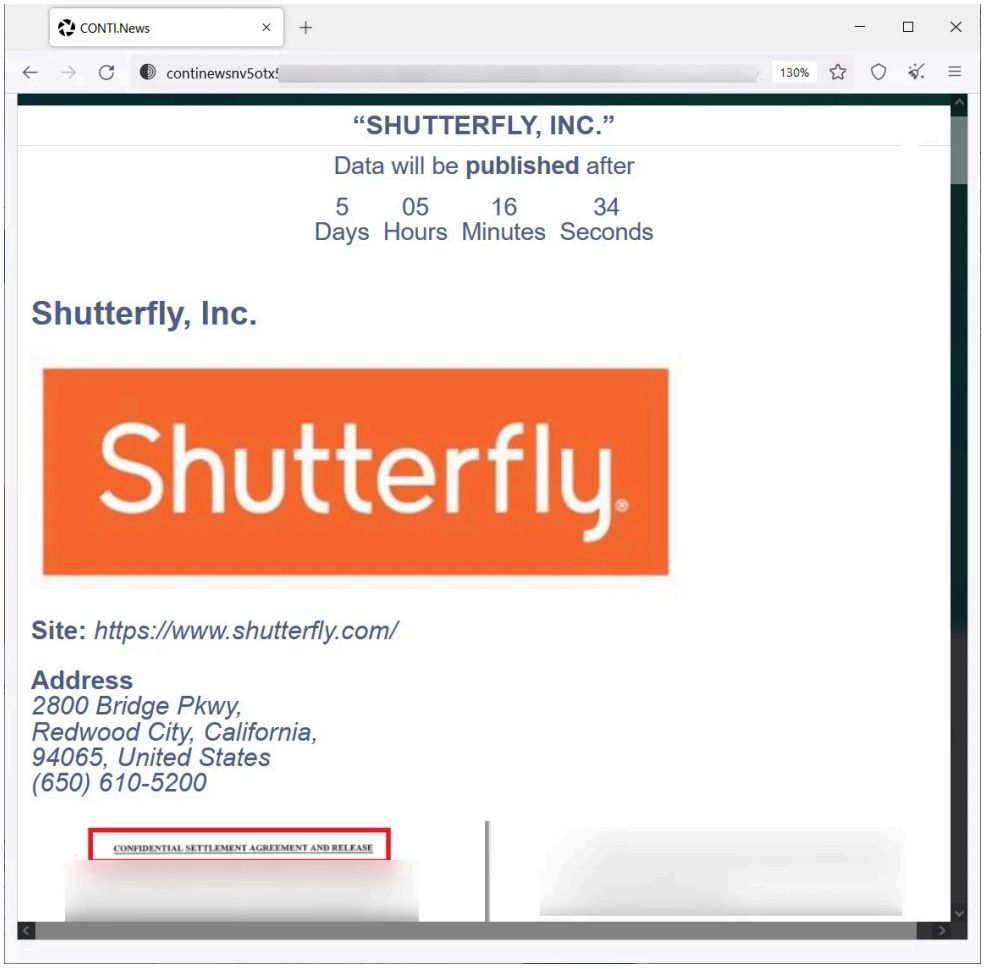
Shutterfly is offering two years of free credit monitoring from Equifax for those affected.

Shutterfly hit by Conti Ransomware

While Shutterfly's data breach notification did not shed much light on their attack, BleepingComputer broke the news in December that the company had suffered a Conti ransomware attack.

At the time of the attack, a source told BleepingComputer that Conti had encrypted over 4,000 devices and 120 VMware ESXi servers belonging to Shutterfly.

A private data leak page also showed samples of the data stolen from Shutterfly, which we are told included 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.

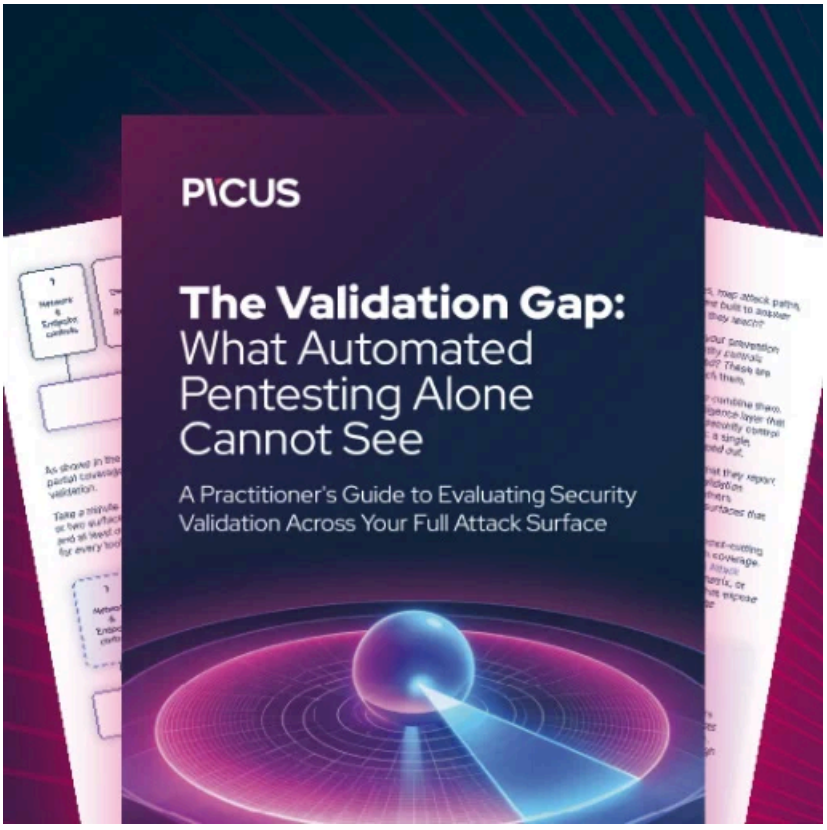


Conti ransomware data leak page for Shutterfly

Since then, the Conti ransomware operation has released 7.02 GB of data they claim was stolen during the attack, including archives named for finance, legal, customer service, and payroll data.

Shutterfly states that they are working with outside cybersecurity experts to continue investigating the attack.

However, Shutterfly warns employees to continue monitoring their credit reports and accounts for suspicious activity and to remain vigilant.



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/shutterfly-discloses-data-breach-after-conti-ransomware-attack/