Cybersecurity firm Mimecast confirmed that SolarWinds hackers who breached its network stole some of its source code.Implemented additional static and security analysis across the source code tree."Using this entry point, the threat actor accessed certain Mimecast–issued certificates and related customer server connection information. The threat actor also accessed a subset of email addresses and other contact information, as well as encrypted and/or hashed and salted credentials. In addition, the threat actor accessed and downloaded a limited number of our source code repositories, but we found no evidence of any modifications to our source code nor do we believe there was any impact on our products."Back in December, the SolarWinds supply chain attack made the headlines when a Russian cyber espionage group tampered with updates for SolarWinds' Orion Network Management products that the IT company provides to government agencies, military, and intelligence offices.Mimecast was one of SolarWinds customers that were impacted by the attack, its systems were infected with the Sunburst backdoor distributed through tainted Orion software updates.The company urged customers hosted in the United States and United Kingdom to reset any server connection credentials in use on the Mimecast platform as a precautionary measure.Implemented enhanced monitoring of all stored certificates and encryption keys.