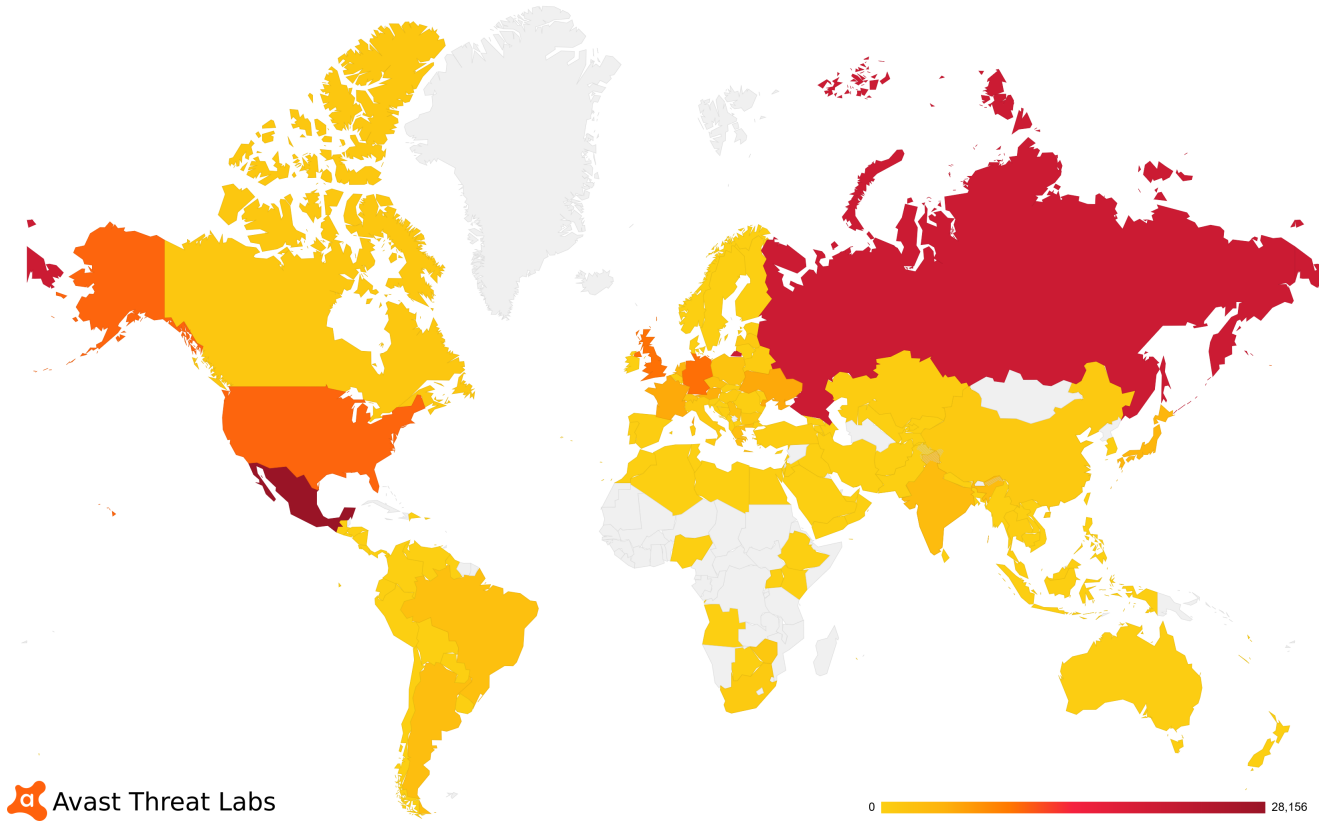
Ransomware Strain Troldesh Spikes Again – Avast

blog.avast.com/ransomware-strain-troldesh-spikes

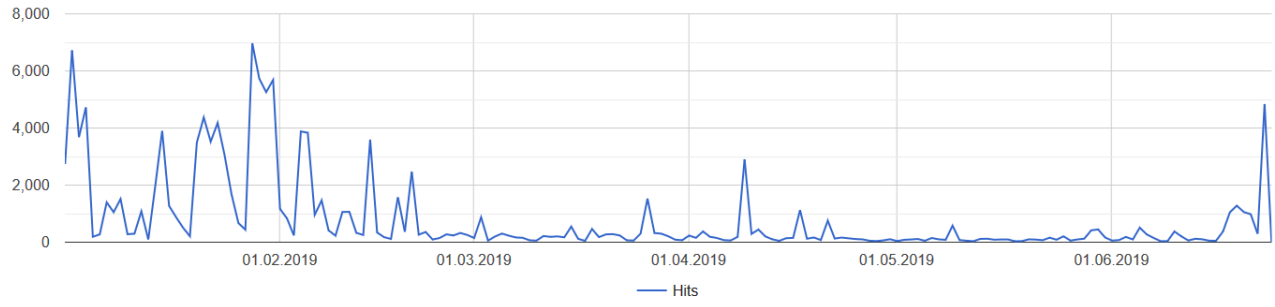


Jeff Elder 25 Jun 2019

Avast software has blocked more than 100,000 attacks by the ransomware strain this year, and recently shows the highest prevalence of it since January

This week the ransomware known as Troldesh, which made headlines early this year, spiked again in Russia, Mexico, and the U.S.

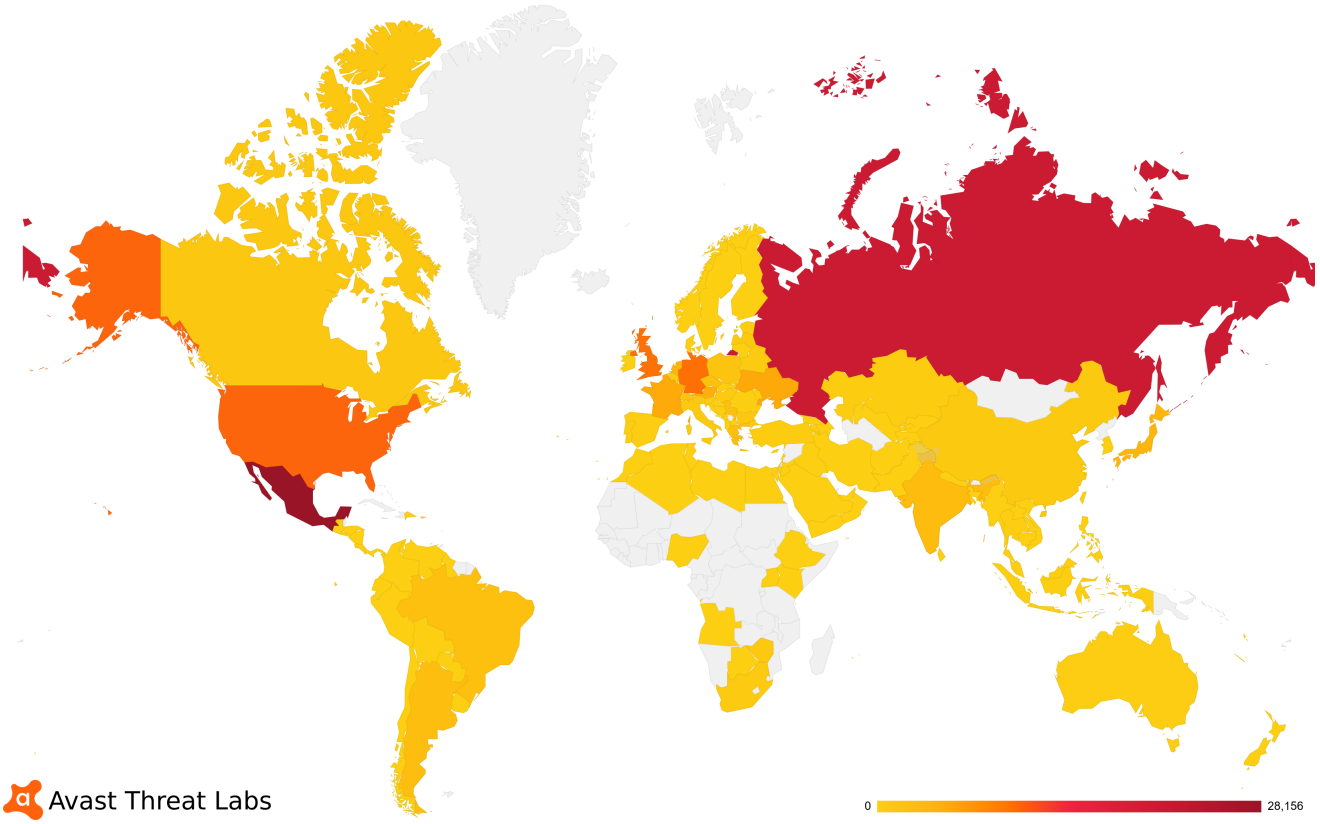
Avast software has blocked more than 100,000 attacks by the ransomware strain this year, and recently shows the highest prevalence of it since January.



Graph shows attacks of Troldesh blocked by Avast. Last spike on right is from June 24.

Troldesh (aka Shade) was spread by phishing emails last winter, and is reportedly now being spread via social networks and other messaging platforms, where posts point to malicious links.

Avast researcher Jakub Křoustek was able to track a spike Monday (June 24) predominantly in Russia and Mexico, but with smaller spikes in the U.K. and Germany.



"We see a spike in the number of its attacks that is probably more to do with Troldesh operators trying to push this strain harder and more effectively than any kind of significant code update," Křoustek said. "Troldesh has been spreading in the wild for years with thousands of victims with ransomed files and it will probably stay prevalent for some time."

Ransomware caused global disruption in 2017's WannaCry outbreak. Last spring a ransomware attack locked up many of the files of the city of Baltimore, and other attacks hit Atlanta, San Antonio, and other cities. It is a type of malicious software (aka malware) that is designed to take your computer files – and sometimes even your entire computer – hostage.

The malware encrypts your files so that they cannot be opened, or it locks you out of your computer completely to prevent access to all of those important photos, videos, accounting files, work documents, and other files. Many security experts advise against paying ransom to hackers because it empowers them, and encrypted files are often not released, anyway. Find out more about protecting yourself from ransomware here.