Sodinokibi Ransomware Behind Travelex Fiasco: Report

By Tara Seals

Published: 2020-01-07 · Archived: 2026-04-05 18:46:24 UTC

Researchers suspect the cybercriminals attacked using an unpatched critical vulnerability in the company's seven Pulse Secure VPN servers.

The Sodinokibi ransomware strain is apparently behind the New Year's Eve attack on foreign currency-exchange giant Travelex, which has left its customers and banking partners stranded without its services.

The criminals behind the attack are demanding a six-figure sum in return for the decryption key, according to reports, and are directing the company to a payment website hosted in Colorado.

"It is just business. We absolutely do not care about you or your details, except getting benefits. If we do not do our work and liabilities – nobody will not co-operate with us. It is not in our interests," the readme file for the ransomware, obtained by Computer Weekly, said. "If you do not cooperate with our service – for us it does not matter. But you will lose your time and your data, cause just we have the private key. In practice time is much more valuable than money."

Sodinokibi, also known as REvil, appeared in April 2019. It has been responsible for a string of high-profile hits, including attacks on 22 Texas municipalities and various dentist offices around the country. Researchers from Secureworks Counter Threat Unit (CTU) believe that the group behind the infamous GandCrab ransomware, which earlier this year claimed to have retired, is actually responsible for Sodinokibi, given that the string decoding functions and other code aspects employed by Sodinokibi and GandCrab are nearly identical.

Travelex, a ubiquitous fixture at airports, provides foreign-exchange services in 70 countries across more than 1,200 retail branches. The attack resulted in Travelex websites in at least 20 countries going offline, left its retail locations to carry out tasks manually, and many customers remain stranded without travel money. Its global banking partners, including Barclays, First Direct, HSBC, Sainsbury's Bank, Tesco and Virgin Money, have also been left adrift with no way to buy or sell foreign currency.

It's unclear whether the company plans to pay the ransom, and it has offered no timeline on cleanup. While the company has admitted the attack, many of its websites merely are showing a warning screen saying that they're down for "planned maintenance."

It has not returned Threatpost's requests for comment.

Unpatched Pulse Secure Servers

The attack could have been successful in part because Travelex took several months to patch critical vulnerabilities in its Pulse Secure VPN servers, according to Bad Packets.

Pulse Secure offers a popular enterprise remote access family of products. The company issued an urgent patch for two critical vulnerabilities in its Zero Trust VPN product in April. CVE-2019-11510 is an arbitrary file reading vulnerability allows sensitive information disclosure enabling unauthenticated attackers to access private keys and user passwords, according to the advisory; further exploitation using the leaked credentials can lead to remote command injection (CVE-2019-11539) and allow attackers to gain access inside private VPN networks.

"That vulnerability is incredibly bad — it allows people without valid usernames and passwords to remotely connect to the corporate network the device is supposed to protect, turn off multi-factor authentication controls, remotely view logs and cached passwords in plain text (including Active Directory account passwords)," explained researcher Kevin Beaumont (a.k.a. Gossi the Dog), in a posting this week.

He said that in August, he became aware that public exploits had been made available and that cybercriminals including APTs were actively scanning the internet for the issue (using public tools like the Shodan search engine). A corresponding report from Bad Packets that month indicated that major cyberattacks could be imminent.

"On August 25th 2019, Bad Packets scanned the internet and found almost 15,000 endpoints across the world had the issue directly exploitable," Beaumont noted. "Those results included networks at governments across the world — many incredibly sensitive organizations included — and basically a list of the world's largest companies. It was clear organizations were simply not patching."

One of these organizations was Travelex, which had seven unsecured Pulse Secure servers, according to Bad Packets; it also said that the company waited until November – eight months after the vulnerability disclosure – to patch the issues.

https://twitter.com/bad_packets/status/1213536922825420800?ref_src=twsrc%5Etfw

Bad Packets indicated that this lag time could have provided the window in which the cybergang infiltrated the Travelex network – a speculation that is somewhat supported by Pulse Secure itself, which issued a statement this week that it has indeed seen the Sodinokibi ransomware being delivered via exploits for the vulnerabilities.

"The ransomware situation at Travelex shines a harsh spotlight on the potential devastation of a cybersecurity incident," Jonathan Knudsen, senior security strategist at Synopsys, said in an emailed statement. "The lost business and negative publicity from a scenario such as this can be crushing. Ransomware continues to be a popular tool for cybercriminals…If you fall victim to a ransomware attack, you must have a plan ready to execute. The plan should include removing infected systems from your network, wiping them and reinstalling the operating system and applications, then restoring data from your backups."

Source: https://threatpost.com/sodinokibi-ransomware-travelex-fiasco/151600/