# Sodinokibi Ransomware Hits Travelex, Demands $3 Million

bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/

Ionut Ilascu

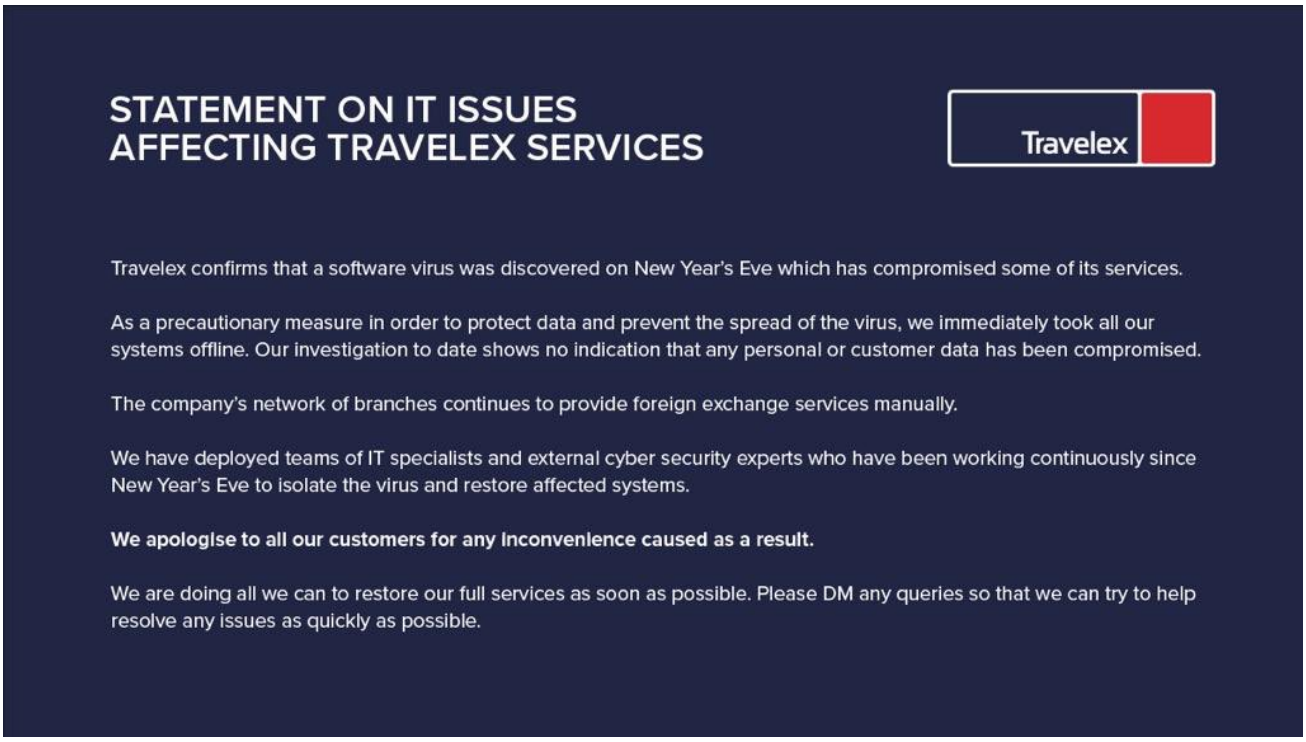
By
Ionut Ilascu

- January 6, 2020
- 01:48 PM
- 0


It's been more than six days since a cyber attack took down the services of the international foreign currency exchange company Travelex and BleepingComputer was able to confirm that the company systems were infected with Sodinokibi ransomware.

The attack occurred on December 31 and affected some Travelex services. This prompted the company to take offline all its computer systems, a precaution meant "to protect data and prevent the spread of the virus."

As a result, customers could no longer use the website or the app for transactions or make payments using credit or debit cards at its more than 1,500 stores across the world. Hundreds of customer complaints came pouring in via social media since the outage began.




In replies to customers today, Travelex was unable to provide updates about progress on restoring its services. In the meantime, the company shows a cyber incident notification on the main page of its website and "planned maintenance" on other pages.

## All network locked, files stolen

On January 3, ComputerWeekly magazine received inside information that the London-based foreign currency exchange company fell victim to a ransomware attack, albeit the malware family remained unknown.

The same news outlet today reported that the ransomware used in the Travelex attack is Sodinokibi.

BleepingComputer was able to independently confirm that Travelex systems were indeed infected by REvil ransomware. We were told that the extension added to some of the encrypted files was a string of more than five random characters, similar to .u3i7y74. This malware typically adds different extensions to files locked on other computer systems.


In addition to the ransom note, the Sodinokibi crew told BleepingComputer that they encrypted the entire Travelex network and copied more than 5GB of personal data, which includes dates of birth, social security numbers, card information and other details.

We were told that they deleted the backup files and that the ransom demanded was $3 million; if not paid in seven days (countdown likely started on December 31), the attackers said they will publish the data they stole.

## Travelex left the door open

Details about how the intrusion occurred are not available at the moment but Travelex was running insecure services before the incident, which could explain how the attacker may have breached the network.

The company is using the Pulse Secure VPN enterprise solution for secure communication, which was patched last year against an "incredibly bad" vulnerability (CVE-2019-11510), as security researcher Kevin Beaumont describes it in a recent blog post.

On unpatched systems, the flaw "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)," Beaumont explains.

A public exploit for this has been available since August 21, 2019. Soon after, someone started scanning the internet for vulnerable endpoints.

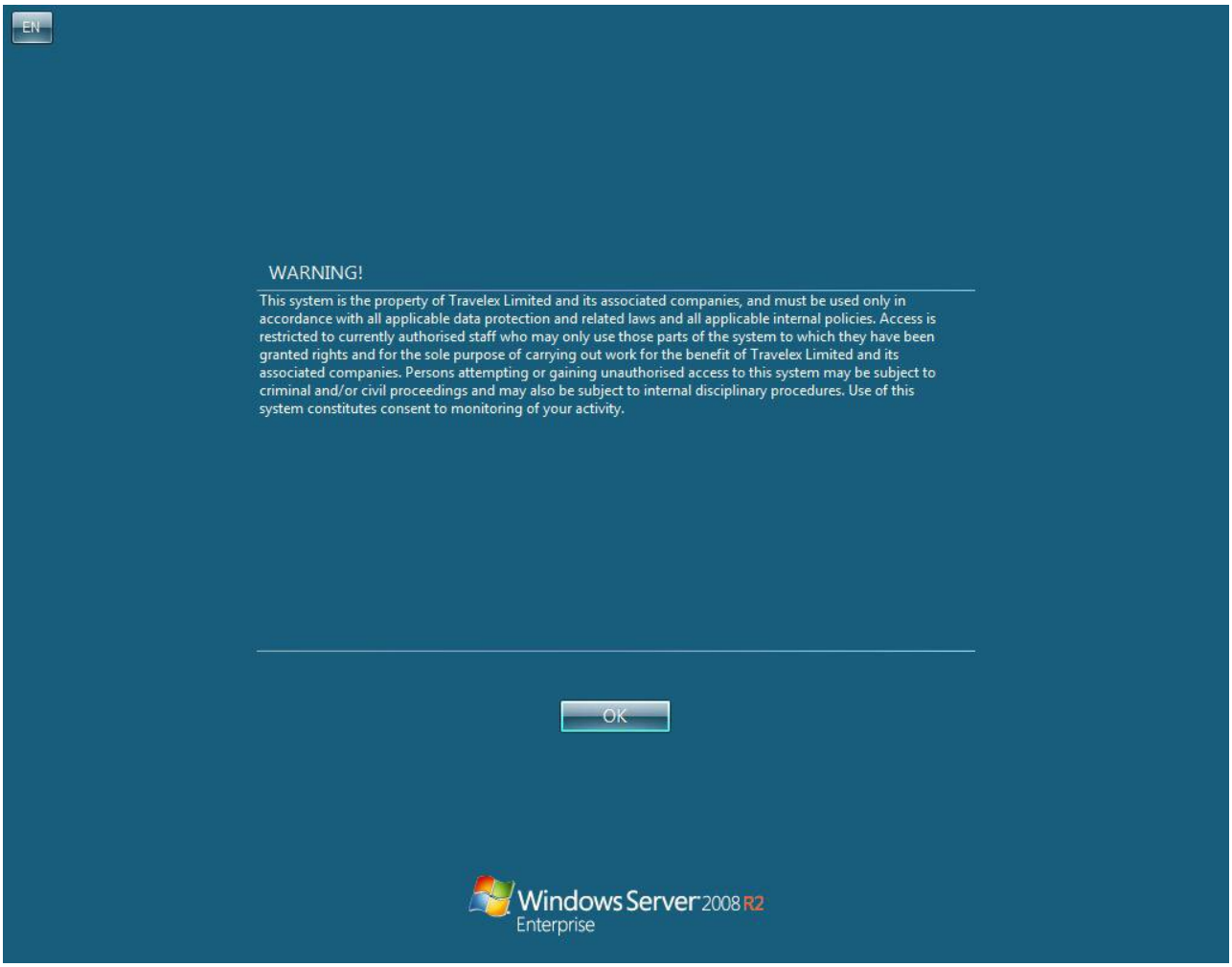
Troy Mursch, chief research officer at Bad Packets, found about 15,000 systems that were directly exploitable via this security issue. Mursch then started to contact organizations at risk, warning them about the danger of leaving their systems unpatched.

Travelex was one of the companies Mursch alerted of the issue but he did not get a reply:


source: Bad Packets Report

Attackers typically spend significant time on the network before deploying the ransomware and encrypting files. This is to get familiar with the network and find systems with important data and backups, to increase their chances of getting paid.

Furthermore, Kevin Beaumont discovered that Travelex had on its Amazon cloud platform Windows servers that were exposed to the internet and did not have the Network Level Authentication feature enables. This means that anyone could connect to the server before authenticating.



source: Kevin Beaumont

**Update [06/01/2020, 18:26 EST]**: Pulse Secure issued a statement today about ransomware actors exploiting unpatched VPN servers. The company is not validating any recent findings as it does not have any data about the attacks.

"As of now, we are unaware of receiving reports directly from customers about this derivative exploit – no firsthand evidence," Pulse Secure told BleepingComputer.

The current communication underlines that a patch for the software is available since April 24, 2019, and that customers were informed multiple times about the fix, via emails, in-product and support website notifications.

"Actors will take advantage of the vulnerability that was reported on Pulse Secure, Fortinet and Palo Alto VPN products – and in this case, exploit unpatched VPN servers to propagate malware, REvil (Sodinokibi), by distributing and activating the Ransomware through interactive prompts of the VPN interface to the users attempting to access resources through unpatched, vulnerable Pulse VPN servers." Scott Gordon (CISSP), Pulse Secure Chief Marketing Officer.

Since the release of the patch, support engineers have been available 24x7 for customers needing help to solve the problem, including those not under an active maintenance contract.

## Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Extortion
- Ransomware
- Sodinokibi
- Travelex

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article



## You may also like: