



Sodinokibi/REvil ransomware hits Argentinian ISP

TLP Amber :

Date Updated: 2021-06-15 - 20:01

Start Date: 2020-07-18

Actors: gold southfield

Description:

On Saturday 18, 2020, Telecom Argentina, one of the largest Internet Services Providers (ISPs) in the country, suffered a ransomware attack that disrupted its customer service systems and the company's official websites. After the initial compromise, the threat actors managed to gain control over an internal Domain Admin, which they used to deliver the ransomware payload to the final targets. As a result, over 18,000 workstations were affected. According to researchers, the ransomware that caused this incident was [Sodinokibi](#), also known as [REvil](#). The threat actors demanded US\$7.5 million in Monero cryptocurrency as a ransom to decrypt the affected files. However, the company claimed that it didn't agree to pay the ransom and it was able to restore access to its systems.

Motivations : Personal GainRevenge

Targeted Industries : [telecommunications](#)

Quick Links : [Tools](#) [Sources](#)

Tools

NAME ↕	DESCRIPTION
sodinokibi	Sodinokibi is a ransomware that uses AES to encrypt session keys and data that is sent to the control server, and Salsa20 to encrypt user files, which are renamed with a random personal extension. The trojan exploits an Oracle WebLogic vulnerability (CVE-2019-2725) to gain access to the victim's machine. Then, it tries to execute itself with elevated user rights in order to access all files and resources on the system without any restriction. Sodinokibi tries to avoid infecting computers from Iran, Russia, and other countries that were formerly part of the USSR.

↑ [Back to Top](#)

Sources

- 1. <https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/>
- 2. <https://www.welivesecurity.com/2020/07/21/telecom-argentina-hit-major-ransomware-attack/>
- 3. <https://www.lanacion.com.ar/tecnologia/reportan-ataque-ransomware-telecom-piden-us75-millones-nid2399977/>

↑ [Back to Top](#)

CLASSIFICATION: DELOITTE CONFIDENTIAL: This report and its attachments (if any) are intended solely for the use of the recipient hereof. If you are not the intended recipient of this message, you are prohibited from reading, disclosing, reproducing, distributing, disseminating, or otherwise using this transmission. Delivery message to any person other than the intended recipient is not intended to waive any right or privilege. If you have received this message in error, please promptly notify the sender by reply e-mail and immediately delete this message from your system. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. This report and its attachments (if any) are provided by the Deloitte entity within the Deloitte network that Your Company has entered into an agreement with, and such agreement governs the provision and use of this report and its attachments (if any). "Your Company" means the company, organization, or other legal entity that you work for as a partner, principal, director, employee, or contractor and any affiliates thereof. This report and its attachments (if any) contain general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this report and its attachments (if any), rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this report and its attachments. © 2020