Ransomware attack hits Italy's Lazio region, affects COVID-19 site

Lawrence Abrams

By
Lawrence Abrams

- August 3, 2021
- 02:13 PM
- 1

The Lazio region in Italy has suffered a reported ransomware attack that has disabled the region's IT systems, including the COVID-19 vaccination registration portal.

Early Sunday morning, the Lazio region suffered a ransomware attack that encrypted every file in its data center and disrupted its IT network.

"On the night between Saturday and Sunday the Regione Lazio suffered a first cyber attack of criminal matrix. We don't know who is responsible and their goals," Nicola Zingaretti, the President of the Lazio region, said in a statement on Facebook.

"The attack blocked almost every file in the data center. The vaccination campaign continues as normal for all those who have booked. Vaccine bookings will open for now suspended in the next few days. The system is currently shut down to allow internal verification and to avoid the spread of the virus introduced with the attack."

While ransomware gangs are known to steal data during an attack as leverage in extortion attempts, the region states that health, financial, and budget data are safe.

The outage has also affected the Salute Lazio health portal used to register for COVID-19 vaccines.

"There is a powerful hacking attack on regional ced. The systems are all disabled including all of the Salute Lazio portal and the vaccine network. All defense and verification operations are under way to avoid the misappropriation. Vaccination operations may experience delays," the region said in a statement.

In June, Italy instituted a new 'Green Pass' certificate system that allows people to prove that they have been vaccinated, tested negative, or previously had COVID-19.

This green pass will be required for indoor dining at restaurants and bars and be required to access fitness centers, amusements parks, museums, and other locations with a large crowd starting on August 6th.

With over 70% of the Lazio population vaccinated and a massive surge in registrations since the announcement of the Green Pass policy, there is concern that the disruption to the online COVID-19 vaccination

However, the region states that there has been no disruption to existing appointments for vaccinations and that the online registration system should be back online in a few days.

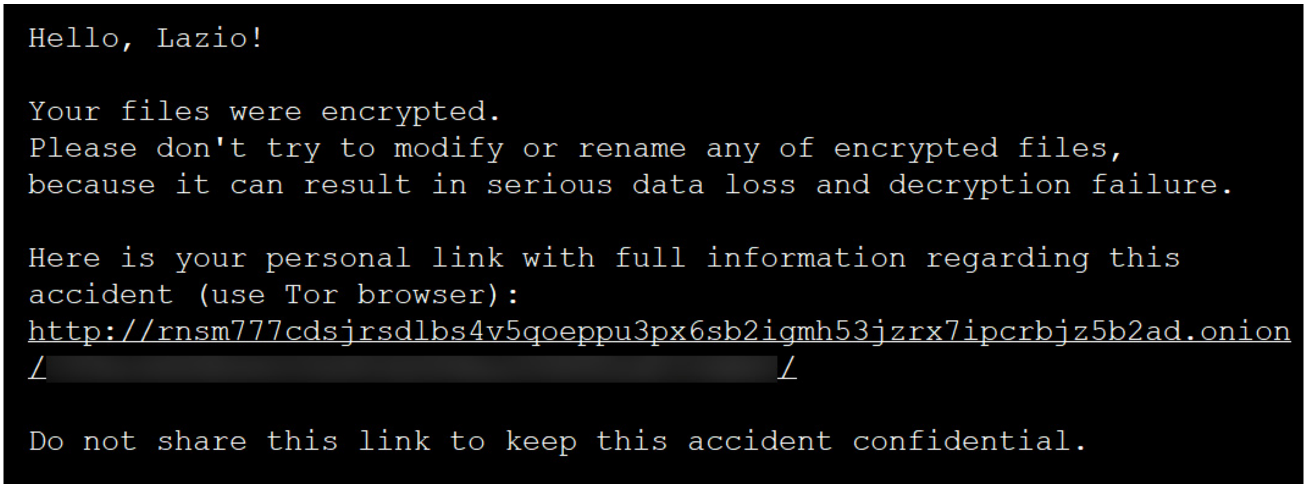
"The vaccination campaign won't stop! In yesterday's day, 50 thousand vaccines were administered, despite the biggest cyber attack suffered," the region stated on Facebook.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Possible RansomEXX ransomware attack

Today, sources have told BleepingComputer that the cyber attack on Lazio was conducted by a ransomware operation known as RansomEXX.

In a redacted ransom note shared from the attack on Lazio, the threat actors state, "Hello, Lazio!" and warn the region that their files were encrypted. The ransom note also includes a link to a private dark web page that Lazio can use to negotiate with the ransomware gang.



```
Hello, Lazio!

Your files were encrypted.
Please don't try to modify or rename any of encrypted files,
because it can result in serious data loss and decryption failure.

Here is your personal link with full information regarding this
accident (use Tor browser):
http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion
/[redacted]/

Do not share this link to keep this accident confidential.
```

Alleged Lazio ransom note

The ransom note does not state what operation conducted the attack but the ONION URL listed is a known Tor site for the RansomEXX operation.

BleepingComputer also received a screenshot of the negotiation page warning that the region must pay a ransom to decrypt their files. The threat actors gave no ransom demand.

RansomEXX negotiation pages are unique per victim, and if the threat actors stole data during the attack, the threat actors provide details on the page, including the amount of data stolen and screenshots of files.

In this case, the negotiation page showed no indications that RansomEXX stole any data.

Update: After posting our article, Italian security researcher JAMESWT stated that there is evidence in Italy that the attack was conducted by LockBit 2.0 but could not share further information.

BleepingComputer will update this article when more information becomes available.

Who is RansomEXX

The RansomEXX gang launched their operation originally under the name Defray in 2018. However, in June 2020, the operation rebranded as RansomEXX where it began to target large corporate entities more actively.

Similar to other ransomware operations, RansomEXX will breach a network using vulnerabilities or stolen credentials.

Once the threat actors gain access to a network, they quietly spread through the network while stealing unencrypted files for extortion attempts.

After gaining access to the Windows domain controller, they deploy the ransomware on the network to encrypt all devices.

The RansomEXX gang has a history of high-profile attacks, including Brazil's government networks, the Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Ecuador's CNT.

Update 8/3/21: Added information about it possibly being LockBit 2.0.

Related Articles:

Luxury fashion house Zegna confirms August ransomware attack

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

- COVID-19
- Cyberattack
- Italy
- Lazio
- RansomEXX
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

rawatnimisha - 9 months ago

Nice! This information is very useful. Thanks for sharing this , keep sharing such information...

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: