LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Analyst Note

August 6, 2021 TLP: White Report: 202108061430

Ransomware Attack on COVID-19 Vaccination Registration Portal in Italy's Lazio Region Possibly Involved Two Ransomware Variants (RansomEXX and LockBit2.0)

Executive Summary

On August 1, 2021, the Lazio region in Italy suffered a ransomware attack which impacted the region's COVID-19 vaccination registration portal, thereby halting new vaccination appointments for days. A new, temporary website came online on August 5, 2021 with the original site expected to relaunch on Monday, August 9, 2021. While most media outlets are reporting that RansomEXX ransomware was responsible for the attack, an Italian security researcher claimed to have evidence that LockBit2.0 was also involved. A terrorism investigation in Italy has been opened as a result of the attack.

Report

Between Saturday night, July 31, 2021, and Sunday morning, August 1, 2021, the Lazio region in Italy suffered a RansomEXX ransomware attack that disabled the region's IT systems, including the COVID-19 vaccination registration portal. Furthermore, an Italian security researcher claimed to have evidence that the attack may have also involved LockBit 2.0 ransomware. While the Tweet has since been deleted, a screenshot was obtained (see below). The system was shut down during incident response to allow for internal verification following the attack and to avoid further infection. The LockBit 2.0 ransomware gang is actively recruiting corporate insiders to help them breach and encrypt networks, according to BleepingComputer.

The Lazio region of Italy is the second most populated region of Italy and includes the country's capital, Rome. President of the Lazio Region, Nicola Zingaretti, said that a terrorism investigation had been opened as a result of the attack, stating that, while the perpetrators were still unidentified, the attack likely came from abroad.

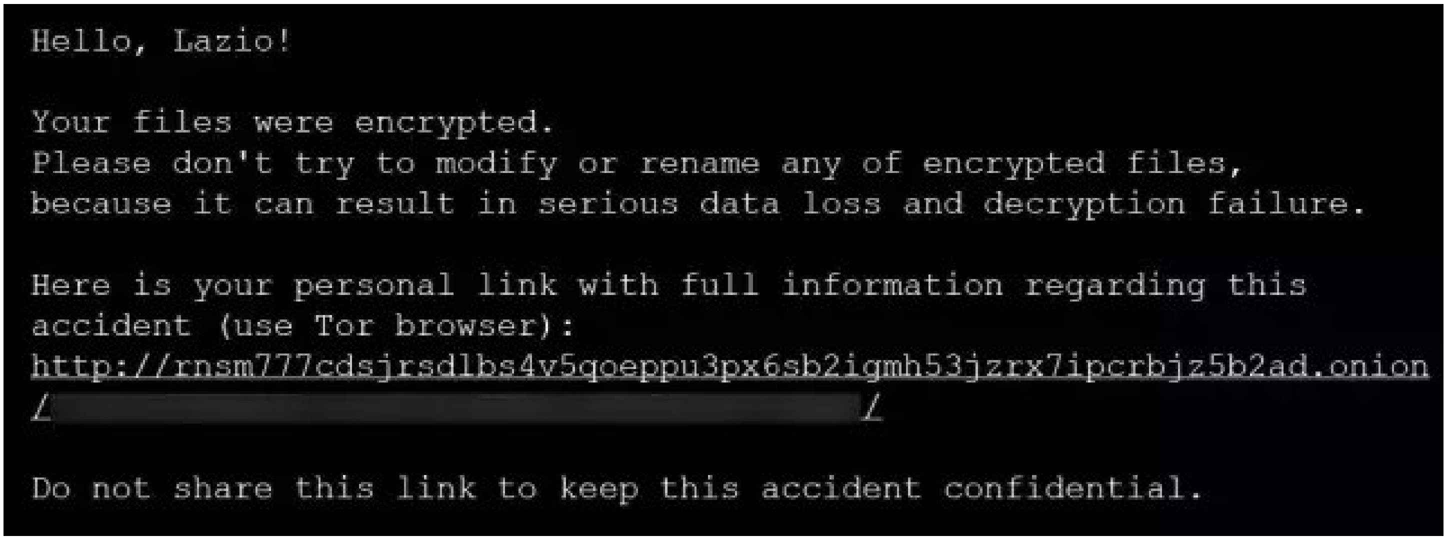
According to the Councilor for Health of Lazio, Alessio D'Amato, the attack likely began after administrator credentials of an employee of LazioCrea (the company that manages the computer network of the region) were compromised and obtained by the threat actors, thereby allowing the attackers to log on to the LazioCrea VPN and deploy ransomware on the regional CED network.

Chuck Everette, director of cybersecurity advocacy at cybersecurity company Deep Instinct Ltd., stated that "the attack on Lazio's vaccine portal appears to be part of a supply chain attack and is therefore not an isolated incident. As this attack is part of a wider campaign, it should be the cause of further concern for other government agencies and healthcare organizations across the world."

While the ransomware attack reportedly encrypted almost every file in the datacenter, officials stated that vaccinations would continue as normal for those who had already booked an appointment with new vaccine bookings to be suspended for the next few days following the incident. On August 3, 2021, the Lazio Region stated on Twitter that the services for booking vaccination appointments would be restored within 72 hours, by Friday, August 6, 2021. On August 5, 2021, the president of the Lazio region stated that the vaccination appointments had resumed with a new website at prenotavaccino-covid.regione.lazio.it, while a temporary version of the original site for vaccine appointments would reportedly launch on Monday, August 9, 2021.

The RansomEXX ransomware-as-a-service (RaaS) operation, previously known as Defray777, has been active since 2018 but came to fame in 2020 after attacks on major organizations, including the Texas Department of Transportation. RansomEXX started as a Windows variant, but a Linux variant was discovered in January 2021. The ransomware is usually delivered as a secondary in-memory payload without ever touching the disk, which makes it harder to detect and highly evasive. In February 2021, RansomEXX ransomware hit the French health insurance company Mutuelle Nationale des Hospitaliers (MNH), severely disrupting the company's operations.

Screenshot 1 – Ransom Note for Lazio



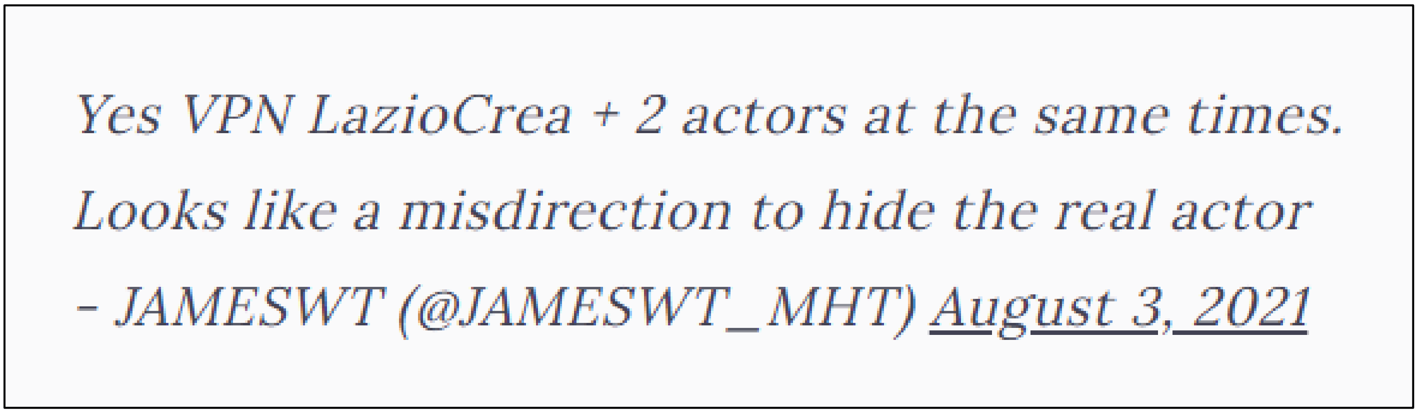
```
Hello, Lazio!

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.
```

Screenshot 2 – Tweet by Italian Security Researcher JAMESWT (@JAMESWT_MHT) on 3 August 2021



Yes VPN LazioCrea + 2 actors at the same times.

Looks like a misdirection to hide the real actor

- JAMESWT (@JAMESWT_MHT) August 3, 2021

Analyst Comment

HC3 CTI has observed recent, similar cyber-attacks impacting the Lazio region in Italy since June 2021. On June 12, 2021, the English-speaking actor 'Mastiff' advertised COVID-19 vaccination data of 7.4 million Italian citizens on RaidForums. The actor claimed they had exfiltrated this data in the past month and that some of the vulnerability are still open and undisclosed but not for sale. On June 13, 2021, the actor stated the data had been sold to an undisclosed party and removed the advertisement. A large majority of the database samples shared by the actor 'Mastiff' were for individuals in the Lazio region, the same region that suffered a RansomEXX attack on its COVID-19 vaccine registration portal on July 31, 2021. Furthermore, on June 2, 2021, the actor 'LulzSecITA' claimed to have breached the governmental web portal of the Lazio Region in Italy at regione.lazio.it. The actor shared screenshots as proof showing 52 databases related to the mortal. The actor likely carried out the attack to raise awareness of the poor security that the Italian institutions have, according to Mandiant Threat Intelligence.

References

COVID-19 vaccine portal for Italy's Lazio region hit with cyberattack (2 August 2021)
https://www.zdnet.com/article/covid-19-vaccine-booking-website-for-italys-lazio-region-hit-with-cyberattack/

Hackers block Italian Covid-19 vaccination booking system in 'most serious cyberattack ever' (2 August 2021)
https://www.cnn.com/2021/08/02/business/italy-hackers-covid-vaccine-intl/index.html

Italian website for vaccination appointments targeted by hackers (2 August 2021)
https://www.euronews.com/2021/08/02/italian-website-for-vaccination-appointments-targeted-by-hackers

Regione Lazio on Facebook (1 August 2021)
https://www.facebook.com/plugins/post.php?href=https%3A%2F%2Fwww.facebook.com%2FRegioneLazio%2Fposts%2F4165073446894549

Italian vaccine booking site taken offline in ransomware attack
https://siliconangle.com/2021/08/03/italian-vaccine-booking-site-taken-offline-ransomware-attack/

French MNH health insurance company hit by RansomExx ransomware (10 February 2021)
https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by-ransomexx-ransomware/

Regione Lazio: attacco con RansomEXX e LockBit 2.0
https://www.punto-informatico.it/regione-lazio-attacco-ransomexx-lockbit-2-0/

Lazio Region on Twitter (3 August 2021)
https://twitter.com/RegioneLazio/status/1422558361845964802

JAMESWT on Twitter (3 August 2021)
https://twitter.com/JAMESWT_MHT/status/1422652277467328517

Italy's Lazio region resumes Covid vaccine bookings after hack (5 August 2021)
https://www.thelocal.it/20210805/italys-lazio-region-resumes-covid-vaccine-bookings-after-hack/

LulzSec_ITA on Twitter (2 June 2021)
https://twitter.com/LulzSec_ITA/status/1267796345382985728

Cyberattack shuts down Italian region's COVID-19 vaccine scheduling app (3 August 2021)
https://www.scmagazine.com/analysis/application-security/cyberattack-shuts-down-italian-regions-covid-19-vaccine-scheduling-app

Prosecutors probe terrorism among reasons behind Italy region hacking - sources (3 August 2021)
https://www.reuters.com/article/italy-hack/prosecutors-probe-terrorism-among-reasons-behind-italy-region-hacking-sources-idINL8N2PA5N7

Cybereason vs. RansomEXX Ransomware (21 January 2021)
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback