Bristol airport still recovering from 'ransomware' attack

NEWS by Mark Mayne

An attack 'similar to' ransomware forced airport staff to take key information screens offline at Bristol Airport, and four days later full service has not yet been resumed.

An attack ‘similar to’ ransomware forced airport staff to take key information screens offline at Bristol Airport, and four days later full service has not yet been resumed.

In a series of tweets on Saturday, the Airport staff thanked passengers for their patience, but conceded that while "digital screens are now live in arrivals and departures", further work is ongoing to "restore complete site-wide coverage as soon as possible."

https://www.scmagazineuk.com/bristol-airport-recovering-ransomware-attack/article/1493225

Site-wide coverage was still pending on Tuesday morning, according to a Twitter post:

oli@olicourt

Replying to @BristolAirport
It's now Tuesday and the screens aren't working....

Bristol Airport
✔ @BristolAirport

Hi Oli, Digital screens have been restored in key areas of the terminal and the team are working hard to restore site wide coverage as soon as possible ~ Kirsty

No flights have been disrupted by the attack, according to the Airport. In comments to the BBC, the Airport spokesman said it had taken "longer than people might have expected" to rectify "an online attempt to target part of our administrative systems" due to a "cautious approach".

Although ransomware has been enjoying a quieter profile in recent months, the global incidents created by WannaCry and Petya/Non-Petya malware based on the Eternal Blue exploit affected thousands, and caused millions of pounds in damages - not least to one victim of Petya, shipping firm Maersk, which lost between US$ 250 million (£201 million) and US$ 300 million (£241 million) as a result of the attack.

David Emm, Principal Security Researcher, Kaspersky Lab told SC Media UK that good security policies were key in containing the incident. "While Bristol Airport has indicated that this was the result of a ransomware attack, there's not yet any information available on how its systems became infected. It does seem, however, that the airport took the computers, which control the flight information screen, offline; this is a positive and smart move to contain the problem."

https://www.scmagazineuk.com/bristol-airport-recovering-ransomware-attack/article/1493225

"It is good practice to apply inhouse policies to reduce the spread of any infection. These include ensuring that not all staff automatically have admin rights to computers, not giving write-access to data and systems unless this is required, segmenting the network, and also applying a default-deny approach so that only apps that are approved can run, are all simple steps which can be taken to help make networks more secure", he summarised.

Javvad Malik, security advocate AlienVault echoed the value of fallback processes to SC Media UK: "Ransomware remains a common attack method and is typically indiscriminate against its targets. Which is why all industry verticals, even those which have traditionally not been targeted should invest in security controls that can provide protection from ransomware, or have the ability to quickly detect and recover from such attacks. As this airport incident showed, having manual processes to fall back on allowed customers to continue being serviced, albeit at a much slower rate."

Andy Miles, CEO, ThinkMarble was also upbeat about the strategy followed by the airport, which deals with eight million passengers a year (contrasting with Heathrow's 75 million).

"The key lesson to learn from the Bristol airport attack is that everyone is open for attack, and to be prepared and vigilant. It is best practice to follow the National Cyber Security Centre’s incident management guidance, which is to have incident response plans in place that protect assets, systems and essential services. No flights are believed to have been affected and the ransomware was contained. Therefore with the information we have it sounds like the right action was taken. Any organisation that can be vulnerable to cyber-attack (and that really applies to all organisations in this day and age) needs to conduct regular penetration testing and reviews of systems to formulate and update incident response plans as cyber threats evolve."