Already in the midst of a crisis, a Houston hospital was attacked by ransomware

https://www.databreaches.net/already-in-the-midst-of-a-crisis-a-houston-hospital-was-attacked-by-ransomware/

August 30, 2020

It's been a rough year for the U.S. in terms of COVID-19. And some areas have been hit worse than others. On August 1, CNN tweeted about how rough things were at Houston's United Memorial Medical Center.

Yesterday was Dr. Joseph Varon's 134th day leading the coronavirus unit at Houston's United Memorial Medical Center.

Last week, he signed more death certificates than he has at any point in his career.

But that wasn't the only added stress United Memorial Medical Center (UMMC) was dealing with. Although details are still sketchy, it appears that the Houston medical center also got hit with ransomware at the end of July.

On or about August 3, Maze Team — who had briefly sworn off attacking medical facilities because of the pandemic, added UMMC to their leak site. The threat actors use the site to name victims who have not paid their ransom demands. They generally dump some of the data that they claim to have hacked, presumably to motivate their victims more to pay up before more data is dumped. Maze Team's approach has been adopted by a number of other ransomware threat actors or teams, but it is not clear to me that the naming and data dumping actually brings most victims around to paying ransom. There have only been a few cases that this blogger can recall where names were subsequently removed from a site. For the post part, it seems that if victims do not agree to pay, they continue to stand firm, even when the threat actors add their name to a leak site, dump data, attempt to auction it, or otherwise try to sell it.

As is Maze Team's pattern, they did not indicate how much ransom they were demanding. Nor did they indicate whether this particular attack involved collaboration or partnership with any other ransomware threat group. The fact that the listing was never removed, however, strongly suggests that the center did not pay the ransom demand.

Most of the files Maze posted as proof of the claimed UMMC hack were just general files from the center, but one folder did contain some identifiable patient records. DataBreaches.net was able to confirm that there were real people with those names living in the Houston area.

But if the files Maze posted constitute %5 of what was exfiltrated, then Maze didn't get many files from the center, it seems. But what did they get, and how did UMMC respond to the attack? Were any vital systems or servers encrypted? Was patient care impacted at all? Was the medical center able to restore from backup? Hopefully, the attack had minimal impact. There has been no notice on the center's site about any service interruptions or delays and no local media coverage to alert residents to any issues, so this may be a very minor incident in terms of the center's ability to care for patients.

DataBreaches.net reached out to UMMC via email to inquire about the ransomware incident but with everything they have had going on there and their current challenges like dangerously high heat and some impending storms, I won't even try to guess when a response might be forthcoming. This post will be updated when one is received, though.