German Ransomware Attack Against Hospital Claims a Life

September 18, 2020 - We've been warning about this for years and now it has actually happened. A ransomware attack in Germany is the first known instance where the criminals behind it are now actually responsible for what can only be described as a murder.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The attack took place against University Hospital in Dusseldorf, Germany. It was so severe that the hospital had to shut down all surgical procedures and divert all emergency care to other hospitals in the area. This included ambulance traffic.

Nevertheless, an ambulance carrying a patient in critical condition and in need of immediate surgery arrived at the hospital while the attack was going on. Unable to provide care, the hospital sent the patient to another facility, but the patient died in route. Any way you look at it, the patient involved in this incident is a murder victim.

While this is the first known incident where a death can be directly attributed to a malware attack, it certainly won't be the last. And the problem isn't isolated to hospital systems alone. Medical identity theft is also of grave concern because victims may find that inaccurate health information is included in their medical records once someone has stolen their identity. This could easily lead to incorrect treatments which could be life threatening. The is especially true when patients are incapacitated.

It has been known for several years now that cybersecurity in medical settings is lacking. That situation has only gotten worse as patients have flocked to telemedicine services because of cost and convenience issues. Many providers have rapidly expanded these services but haven't forced the medical professionals working in their systems to adopt strong cybersecurity protocols.

While we are not fans of overregulation, it is becoming more and more clear that some cybersecurity standards need to be adopted at all levels of medicine, from large companies all the way down to individual practitioners. The incident in Germany shines a light on this issue and it's something that should be addressed with some sense of urgency. If it isn't, we can all expect to see more incidents like this one, and any one of us could become the next victim.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS