The malware that shut down MedStar Health’s computer systems and locked up patient records now appears to be a ransomware attack.

MedStar employees encountered a pop-up message demanding payment of 45 Bitcoin, approximately $19,000 in exchange for a digital key that would unlock the data, according to several reports.

The malware has blocked MedStar employees from accessing patient data and, in some cases, having to turn patients away.

Although MedStar Health has yet to publicly state that the attack is ransomware, the Washington Post reported that MedStar employees encountered a pop-up message demanding payment of 45 Bitcoin, approximately $19,000 in exchange for a digital key that would unlock the data, and the Baltimore Sun quoted a doctor saying that the criminals also gave MedStar employees the option of paying 3 Bitcoins ($1,250) for a key to access one of the locked computers.

“You just have 10 days to send us the Bitcoin,” a note obtained by the Post said. “After 10 days we will remove your private key and it’s impossible to recover your files."

MedStar said at the end of last week that the majority of its systems are now working.

"As of Friday morning, we were approaching 90 percent functionality of our systems," the provider said in a statement.

MedStar explained that its inpatient and outpatient EHRs are functioning, as are its registration and scheduling system.

"Numerous other systems are also back online, and we are working on the remaining clinical and administrative systems that connect to our network and are resolving unique, site-specific issues on a real-time basis."

The FBI continues to investigate the MedStar attacks and a series of other recent ransomware attacks at health organizations.

U.S. hospitals have been attacked in California, Kentucky, Maryland and the District of Columbia.

Like Healthcare IT News on Facebook and LinkedIn Share71