FBI warns ransomware assault threatens US health care system

October 30 2020, by Frank Bajak

This Thursday, June 14, 2018, file photo, shows the FBI seal at a news conference at FBI headquarters in Washington. In an alert Wednesday, Oct. 28, 2020, the FBI and other federal agencies warned that cybercriminals are unleashing a wave of data-scrambling extortion attempts against the U.S. healthcare system that could lock up their information systems just as nationwide cases of COVID-19 are spiking. (AP Photo/Jose Luis Magana, File)

Federal agencies warned that cybercriminals could hobbled all 250 U.S. facilities of the hospital chain Universal Health Services, forcing doctors and nurses to rely on paper and pencil for record-keeping and slowing lab work. Employees described chaotic conditions impeding patient care, including mounting emergency room waits and the failure of wireless vital-signs monitoring equipment.

Also in September, the first known fatality related to ransomware occurred in Duesseldorf, Germany, when an IT system failure forced a critically ill patient to be routed to a hospital in another city.

Holden said the Russian-speaking group behind recent attacks was demanding ransoms well above $10 million per target and that criminals involved on the dark web were discussing plans to try to infect more than 400 hospitals, clinics and other medical facilities.

While no one has proven suspected ties between the Russian government and gangs that use the Trickbot platform that distributes Ryuk and other malware, Holden said he has "no doubt that the Russian government is aware of this operation." Microsoft has been engaged since early October in trying to knock Trickbot offline.

Dmitri Alperovitch, co-founder and former chief technical officer of the cybersecurity firm Crowdstrike, said there are "certainly lot of connections between Russian cyber criminals and the state," with Kremlin-employed hackers sometimes moonlighting as cyber criminals.

In this Nov. 1, 2017, file photo, traffic along Pennsylvania Avenue in Washington streaks past the Federal Bureau of Investigation headquarters building. In an alert Wednesday, Oct. 28, 2020, the FBI and other federal agencies warned that cybercriminals are unleashing a wave of data-scrambling extortion attempts against the U.S. healthcare system that could lock up their information systems just as nationwide cases of COVID-19 are spiking. (AP Photo/J. David Ake, File)

Increasingly, ransomware criminals are stealing data from their targets before encrypting networks, using it for extortion. They often sow the malware weeks before activating it, waiting for moments when they believe they can extract the highest payments, said Brett Callow, an analyst at the cybersecurity firm Emsisoft.

A total of 59 U.S. health care providers or systems have been impacted by ransomware in 2020, disrupting patient care at up to 510 facilities, Callow said.

Hospitals and clinics have been rapidly expanding data collection and adding internet-enabled medical devices, many of which are poorly secured. Hospital administrators, meanwhile, have been slow to update software, encrypt data, train staff in cyber hygiene and recruit security specialists, leaving them vulnerable to cyber-attacks.

And as hospitals respond to the coronavirus crisis, privacy and security protocols fall by the wayside, leaving patients open to identity theft, said Larry Ponemon, a data security expert. "The bad guys smell the problem."