# FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/

On Monday, Oct. 26, KrebsOnSecurity began following up on a tip from a reliable source that an aggressive Russian cybercriminal gang known for deploying ransomware was preparing to disrupt information technology systems at hundreds of hospitals, clinics and medical care facilities across the United States. Today, officials from the **FBI** and the **U.S. Department of Homeland Security** hastily assembled a conference call with healthcare industry executives warning about an “imminent cybercrime threat to U.S. hospitals and healthcare providers.”

The agencies on the conference call, which included the **U.S. Department of Health and Human Services** (HHS), warned participants about "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers."

The agencies said they were sharing the information "to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

The warning came less than two days after this author received a tip from **Alex Holden**, founder of Milwaukee-based cyber intelligence firm Hold Security. Holden said he saw online communications this week between cybercriminals affiliated with a Russian-speaking ransomware group known as Ryuk in which group members discussed plans to deploy ransomware at more than 400 healthcare facilities in the U.S.

One participant on the government conference call today said the agencies offered few concrete details of how healthcare organizations might better protect themselves against this threat actor or purported malware campaign.

"They didn't share any IoCs [indicators of compromise], so it's just been 'patch your systems and report anything suspicious'," said a healthcare industry veteran who sat in on the discussion.

However, others on the call said IoCs may be of little help for hospitals that have already been infiltrated by Ryuk. That's because the malware infrastructure used by the Ryuk gang is often unique to each victim, including everything from the Microsoft Windows executable files that get dropped on the infected hosts to the so-called "command and control" servers used to transmit data between and among compromised systems.

Nevertheless, cybersecurity incident response firm **Mandiant** today released a list of domains and Internet addresses used by Ryuk in previous attacks throughout 2020 and up to the present day. Mandiant refers to the group by the threat actor classification "UNC1878," and aired a webcast today detailing some of Ryuk's latest exploitation tactics.

**Charles Carmakal**, senior vice president for Mandiant, told Reuters that UNC1878 is one of most brazen, heartless, and disruptive threat actors he's observed over the course of his career.

"Multiple hospitals have already been significantly impacted by Ryuk ransomware and their networks have been taken offline," Carmakal said.

One health industry veteran who participated in the call today and who spoke with KrebsOnSecurity on condition of anonymity said if there truly are hundreds of medical facilities at imminent risk here, that would seem to go beyond the scope of any one hospital group and may implicate some kind of electronic health record provider that integrates with many care facilities.

So far, however, nothing like hundreds of facilities have publicly reported ransomware incidents. But there have been a handful of hospitals dealing with ransomware attacks in the past few days.

–*Becker's Hospital Review* reported today that a ransomware attack hit Klamath Falls, Ore.-based Sky Lakes Medical Center's computer systems.

–*WWNY's Channel 7 News* in New York reported yesterday that a Ryuk ransomware attack on St. Lawrence Health System led to computer infections at Caton-Potsdam, Messena and Gouverneur hospitals.

–*SWNewsMedia.com* on Monday reported on "unidentified network activity" that caused disruption to certain operations at Ridgeview Medical Center in Waconia, Minn. SWNews says Ridgeview's system includes Chaska's Two Twelve Medical Center, three hospitals, clinics and other emergency and long-term care sites around the metro area.

–*NBC5* reports The University of Vermont Health Network is dealing with a "significant and ongoing system-wide network issue" that could be a malicious cyber attack.

-A story at *BleepingComputer.com* says Wyckoff Hospital in New York suffered a Ryuk ransomware attack on Oct. 28.

This is a developing story. Stay tuned for further updates.

**Update, 10:11 p.m. ET:** The FBI, DHS and HHS just jointly issued an alert about this, available here.

**Update, Oct. 30, 11:14 a.m. ET:** Added mention of Wyckoff hospital Ryuk compromise.