Why The Real Number Of Ransomware Attacks Is Higher Than You Think

The number of ransomware attacks is higher than you think. Recently, a University of Vermont network found that even more ransomware attacks have infected their hospitals.

The same cybercrime gang that infected at least three other hospitals recently has also attacked University of Vermont Health Network, according to two sources from the investigation.

Last week Wednesday, federal agencies warned US healthcare providers of an “increased and imminent cybercrime threat” by a gang that uses ransomware called Ryuk.

On Thursday, the FBI and Cybersecurity and Infrastructure Security Agency (part of the Department of Homeland security) sent an update with new technical information regarding the attacks.

It’s rumored that 20 medical facilities have been hit by the recent wave of ransomware, although the investigation is ongoing and nothin has been officially confirmed. Many of these facilities are within the same hospital chain.

The FBI and the Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security, sent an updated alert Thursday night with new technical information, adding that they have “credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.”

Ryuk has been confirmed to have hit the following: the Sky Lakes Medical Center, with 21 locations in Oregon; Dickinson

County Healthcare System in Michigan and Wisconsin; and the St. Lawrence Health System in northern New York..

The infections of Ryuk made Sky Lakes Medical Center inaccessible, which halted radiation treatments for cancer patients, according to the Center's spokesperson, Tom Hottman.

"We're still able to meet the care needs for most patients using work-around procedures, i.e. paper rather than computerized records. It's slower but seems to work," he wrote, in an email.

A major wave of ransomware attacks began at the end of September when Universal Health Services, one of the biggest hospital chains in the U.S., was hit, forcing doctors and nurses to use pen and paper to file patient information. Ransomware typically gains access to secure systems and encrypts their files, demanding money to decrypt the files.

Trickbot is the notorious cybercrime botnet that transmits Ryuk. Both Microsoft and reportedly U.S. Cyber Command have undertaken efforts recently to disrupt Trickbot, but not with success.

Attacks on theU.S.'s healthcare systems have risen this year, said Allan Liska, an analyst at the cybersecurity firm Recorded Future, who monitors known infections.

"We've tracked 62 reported healthcare ransomware infections this year. Compared to 50 all of last year," Liska said.

"Keep in mind that unless an incident becomes public, there is a couple-of-month lag between the incident and reporting. So the real number is much higher," Liska said.

A Department of Health and Human Services security memo produced for health care providers this year, which was reviewed by NBC News, shows that private security companies and the U.S. government attribute Ryuk ransomware to Russian

cybercriminal groups.

The private security firm CrowdStrike assessed with “medium confidence” that Russian threat actors use Ryuk, and the cybersecurity company FireEye said the “most likely hypothesis” is that Ryuk operators are Russian cybercriminals, according to the memo.

Russian cybercriminal groups sometimes work with the Russian government, but in other instances they can work on their own.

Read these simple things you can do to help avoid a ransomware/malware attack