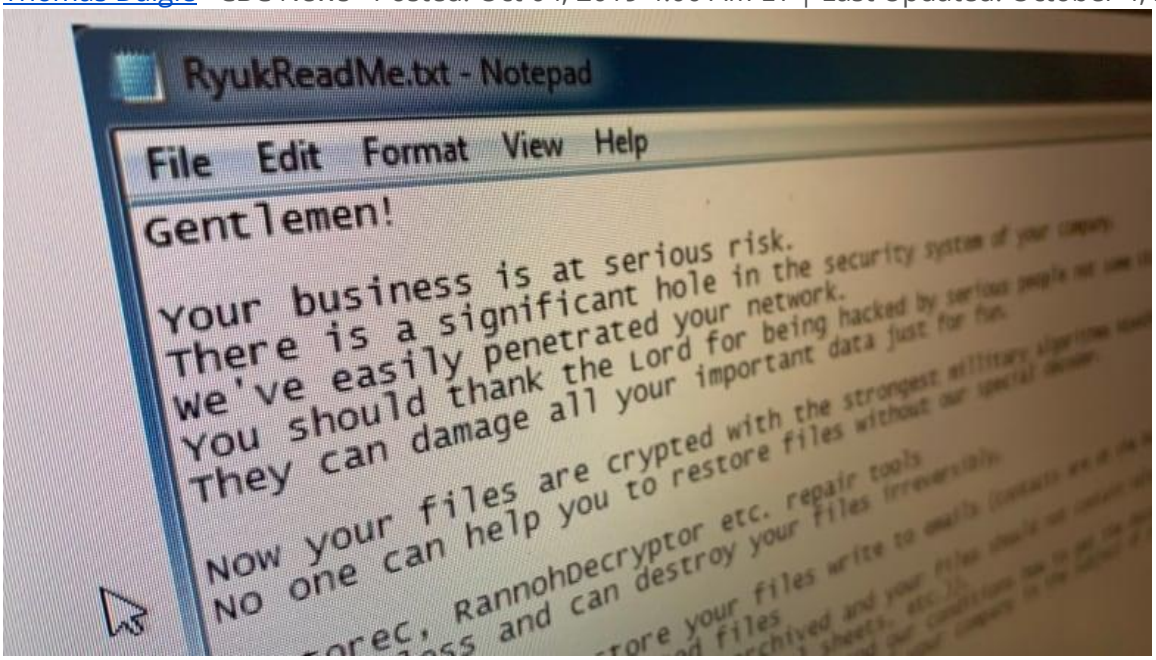
Here's what we know about the ransomware that hit 3 Ontario hospitals

Malicious software can remain dormant for months

Thomas Daigle · CBC News · Posted: Oct 04, 2019 4:00 AM ET | Last Updated: October 4, 2019



The Ryuk malware is known to store a ransom note in infected computers. (Thomas Daigle/CBC)

120 comments

Hackers have crippled the computer systems of three Ontario hospitals in recent weeks, prompting concern about the type of malicious software used and whether more facilities may be at risk.

The malware, known as "Ryuk," attacks computer networks but remains invisible to average users for weeks or months. During that time, it collects information about the organization and its perceived ability to pay a ransom.

Ryuk then locks files, demanding the network owner pay a sum of money to make them accessible again.

The criminals behind the attack "will learn how you operate from A to Z... then they'll hit you," Zohar Pinhasi, a Florida-based cyber counterterrorism expert told CBC News. He said it's likely other Canadian hospitals are affected and haven't yet detected it.

"If you get hit by them, it would be devastating."

Delays for patients, headaches for staff

The impact of the malware attack has been wide-ranging for the three affected hospitals, located in Toronto and southwestern Ontario. Email systems were taken offline, health-care records became harder to access and patients were warned of longer wait times.

Employees had to transcribe patient information onto paper by hand. Hospital officials stressed, though, no data had been accessible to the hackers.

Sarah Downey, president and CEO of Toronto's Michael Garron Hospital, said the Ryuk malware first struck a laptop before it spread to the network. (Ed Middleton/CBC)

The malware "came into our system, but no data left our hospital," said Sarah Downey, CEO of Toronto's Michael Garron Hospital. "It was picked up by a firewall before [the data] could leave."

Michael Garron Hospital, formerly known as the Toronto East General, posted a message on its website on Sep. 26, alerting the public that it had "discovered a virus on one of the IT systems."

The same day, the Listowel Wingham Hospitals Alliance said on Facebook its two hospitals in rural southwestern Ontario were suffering an "information technology system disruption, which means our clinical applications are affected."

All three hospitals said they paid no money to retrieve their files and no specific amount was demanded. Systems at all three facilities are in the process of being restored, the hospitals said.

The RCMP urges malware victims not to pay any ransom because there's no guarantee the files will be unlocked. Cyber criminals may even demand more money or identify the victim as a target for further attacks.

First identified in Aug. 2018, cybersecurity experts estimate Ryuk netted hackers the Bitcoin equivalent of $3.7 million US within five months.

Pinhasi, the U.S.-based expert, said the hackers "are sitting on a goldmine."

Michael Garron Hospital, formerly known as Toronto East General Hospital. (Ed Middleton/CBC)

In an advisory last June, the U.K.'s National Cyber Security Centre warned the malicious code associated with Ryuk will block anti-malware software, allow hackers to monitor a victim's computer activity and spread to other machines on the same network.

Access to the computers can even be sold to "other criminal operators," the British report said.

It's unclear how the Ontario hospitals became targets, but the malware often penetrates systems using a Trojan horse: a user opens an infected email attachment and the malicious code spreads. (Police advise users not to click on emails from people they don't know.)

Hospitals often targeted

The Ontario health-care facilities aren't the only ones that have fallen victim to Ryuk attacks in recent days.

This week, three Alabama hospitals said a similar infection shut down computer systems and blocked access to patient lists. Several hospitals in Australia were paralyzed by a ransomware attack, also reported to involve Ryuk.

The episode, however, barely compares to the massive proportions of the global WannaCry ransomware pandemic in 2017, then described by European police as reaching an "unprecedented level" of infection.

In this 2017 file photo, employees watch electronic boards to monitor possible ransomware cyberattacks at the Korea Internet and Security Agency in Seoul, South Korea during the WannaCry pandemic. (Yun Dong-jin/Yonhap via The Associated Press)

At the time, many of the victims were found to have been running out-of-date Windows software that wasn't protected from such infections.

Adam Mansour, a cybersecurity expert with IntelliGO Networks in Toronto, said health-care facilities are particularly vulnerable to malware attacks because of their reliance on specialized software that only rarely gets updated.

"Hospitals, unfortunately have software that is hard to upgrade," he said.

Hard to beat

It's unclear who's responsible for the recent string of Ryuk attacks. Cybercrime analysts and specialized bloggers have suggested several criminal groups have been mounting such attacks and that the malware itself may originate from Russia.

The name "Ryuk" itself is taken from a Japanese comic book character who "cannot be harmed by conventional human weapons," according to a description on the industry website Comic Vine.

It seems the malware can't easily be beaten, either. Mansour said system administrators usually have to "reimage" computers to reset them to their previous configurations from before the ransomware attack to restore full functionality.

He warns, though, it doesn't always work. "We've seen a lot of cases where just reimaging... is really just delaying the inevitable, which is that (the malware) will come right back."