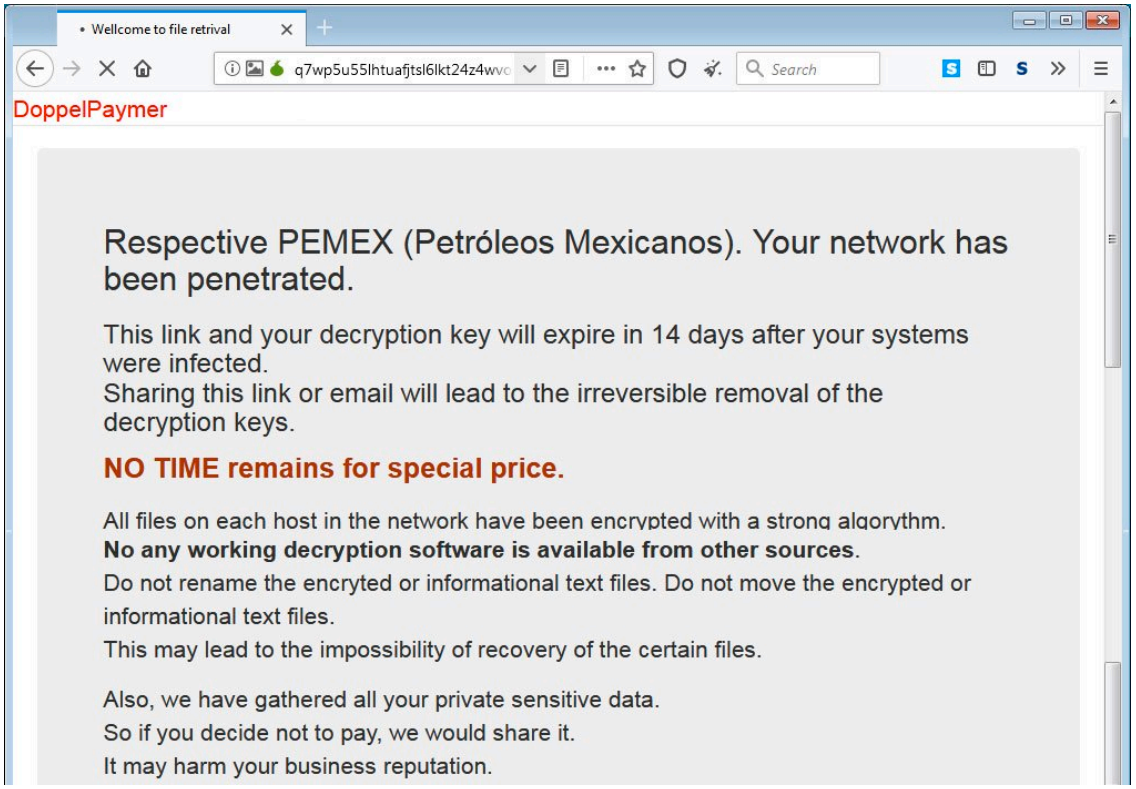
Louisiana was hit by Ryuk, triggering another cyber-emergency

By Sean Gallagher

Published: 2019-11-21 · Archived: 2026-04-05 21:24:22 UTC

On November 15, the Charles-Nicolle University (CHU) Hospital in Rouen, France, was hit by ransomware that spread across five sites. The hospital was forced to shut down its networks to prevent the malware from spreading, according to a report from Le Monde, and staff were forced to use paper and pencil for tracking patients. While there were reports of a demand of a ransom payment of 1,500 euros for each of the more than 6,000 computers affected at the hospital, a hospital spokesperson denied that a ransom demand had been made and said none would be paid. As of November 18, about 25% of the hospital's applications had been restored.

Also on November 15, the government of the Canadian territory of Nunavut suffered a ransomware outbreak that affected about 5,000 computers territory-wide. That attack, according to Nunavut government spokesperson Chris Puglia, used a variant of DoppelPaymer ransomware; the same malware hit Mexico's state-owned oil company PEMEX on November 12.



The PEMEX Tor payment site was widely posted on social media.

The PEMEX Tor payment site was widely posted on social media.

Despite documentation of the Pemex attack, company executives have continued to deny the company was affected.

> 📌 #Pemex🇲🇽reitera hacer caso omiso a boletines apócrifos que circulan en medios de información y redes sociales. Toda la información referente a la empresa productiva del Estado es publicada únicamente por vías institucionales y las redes oficiales.
>
> — Petróleos Mexicanos (@Pemex) November 17, 2019

According to security researcher Vitali Kremez, both the Nunavut and PEMEX ransomware attacks used the same Tor "hidden service" Web portal. Within the portal, the actors behind the ransomware left the note rationalizing their attack: "We don't care who you are and why this happens. No one died. That's all."

While they may or may not use the same type of communications with victims as opportunistic attacks—DoppelPaymer uses a Web portal similar to those used by opportunistic attacks, while Ryuk keeps its communications over email—both of these attacks were targeted rather than opportunistic. While they may use similar initial compromise methods as opportunistic attacks (phishing, automated vulnerability scanning and exploitation, or attacks using Remote Desktop Protocol), targeted attacks are the product of researching a compromised network and releasing the ransomware only after determining who the target is (and how likely they will be to pay). As a result, they require less work for attackers because they reduce the number of victims they need to communicate with.
