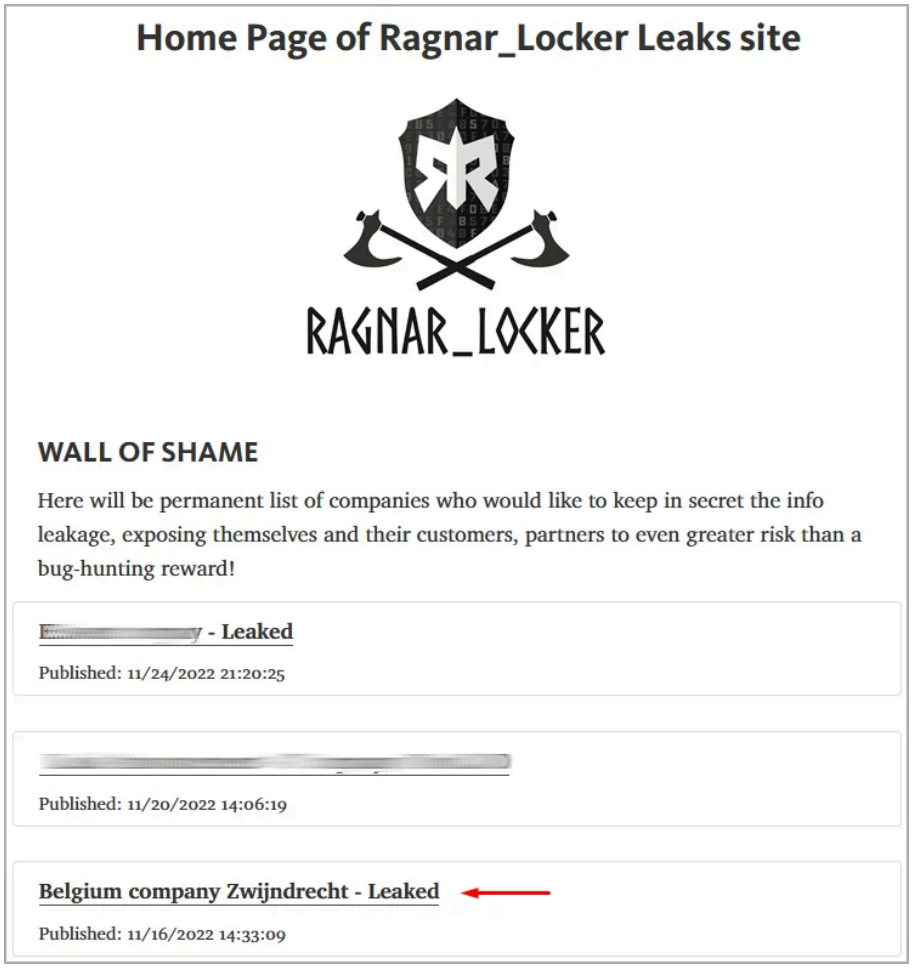
Ransomware gang targets Belgian municipality, hits police instead

By Bill Toulas

Published: 2022-11-26 · Archived: 2026-04-06 03:26:45 UTC

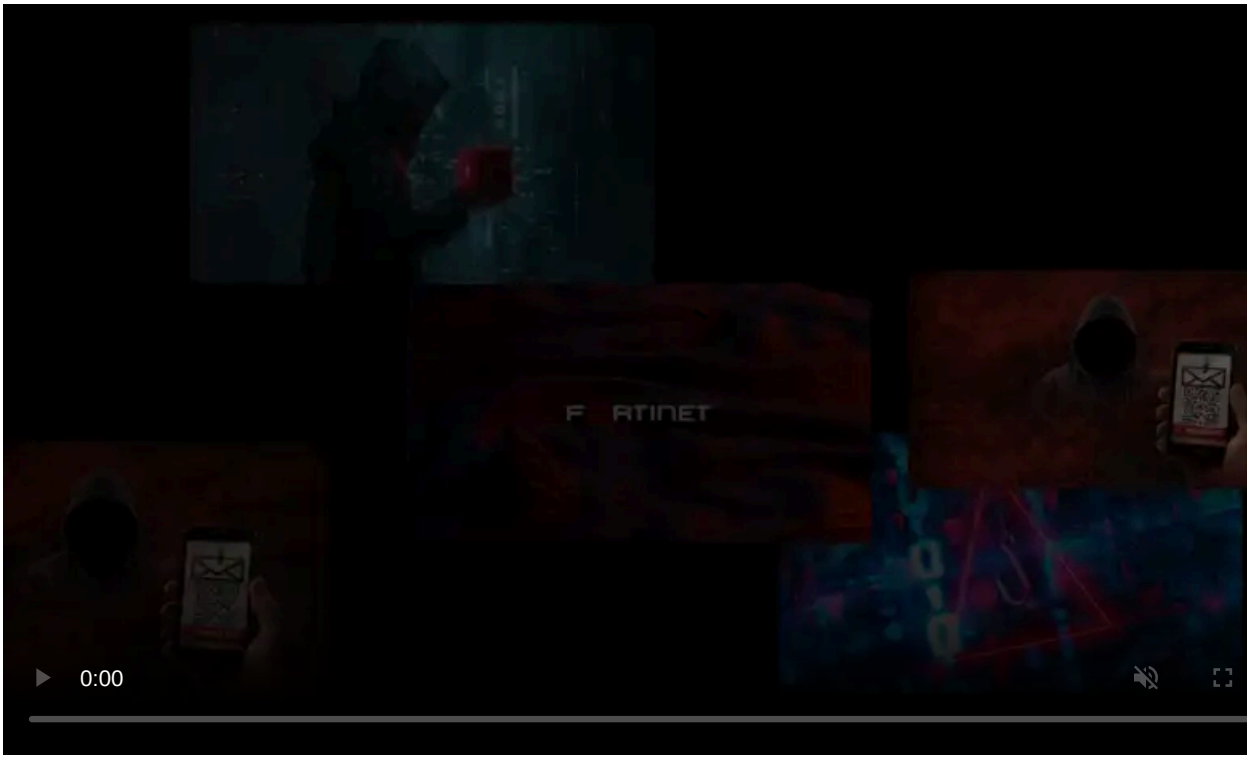
The Ragnar Locker ransomware gang has published stolen data from what they thought was the municipality of Zwijndrecht, but turned out to be stolen from Zwijndrecht police, a local police unit in Antwerp, Belgium.

The leaked data reportedly exposed thousands of car number plates, fines, crime report files, personnel details, investigation reports, and more.



Ragnar Locker listing the wrong victim *(BleepingComputer)*

This type of data can potentially expose people who reported crimes or abuse and could compromise ongoing law enforcement operations and investigations.


F RTINET
0:00

Belgian media outlets call this data leak one of the biggest of this kind that has impacted a public service in the country, exposing all data kept by Zwijndrecht police from 2006 until September 2022.

Police confirm attack

Zwijndrecht police responded to the local media coverage via a post on Facebook, downplaying the impact of the incident and saying that the hackers only accessed a part of the network where the police held administrative data.

The police say that the threat actors could only access data on the administrative network, therefore primarily affecting personnel.

Zwijndrecht police statement on Facebook

Chief of police at Zwijndrecht, Marc Snels, told the VRT news network that the data leak resulted from human error, and they are now contacting all exposed individuals to inform them about the incident.

"It is not the case that all data has been leaked. This network mainly contains personal information from our staff, such as personnel lists and photos from personnel parties," commented Snels to local media.

"But it is true that there is sometimes sensitive information on that network, even though we always try to put it only on the professional network. Those are human errors. For example, fines and PVs have also been leaked. Also, photos of child abuse. That is very painful, of course." - Chief of Zwijndrecht Police.

Wider impact than claimed

Although this incident has not impacted the national police network in Belgium, the breach on the local Zwijndrecht network is still significant for thousands of people.

Belgian journalist Kenneth Dée broke the news of the attack on Het Laatste Nieuws, sharing that the threat actors allegedly attacked a poorly protected Citrix endpoint to breach the police's network.

Dée's investigation of the data revealed telecom service subscriber metadata and SMS of people under covert police investigation.

Moreover, the leaked files contain footage from traffic cameras, exposing the whereabouts of individuals at specific dates and times.

"This is the largest law-enforcement leak in the history of Belgium and probably the most impactful leak we have ever seen in our country," Dée told Bleeping Computer.

"It should be a wakeup call for local police and the way they handle citizens' data, and hopefully, it will set things in motion towards changes on that front."

The country's data protection office has not yet announced an investigation on the case, but the prosecutor opened a criminal proceeding that focuses on the hacking incident itself.

Belgian lawyer and privacy activist Matthias Dobbelaere-Welvaert told BleepingComputer that exposed individuals should change everything they can, including license plates, identity cards, passports, etc.

"You can't easily change where you live, but even if you change all documents, the repercussions of this security incident could be for a lifetime, and theft identity is no joke," says Dobbelaere-Welvaert.

"It’s my opinion that as long as not all police network systems are adequately protected, no smart camera should be allowed to turn on."

Source: https://www.bleepingcomputer.com/news/security/ransomware-gang-targets-belgian-municipality-hits-police-instead/