Brazil's court system under massive RansomExx ransomware attack

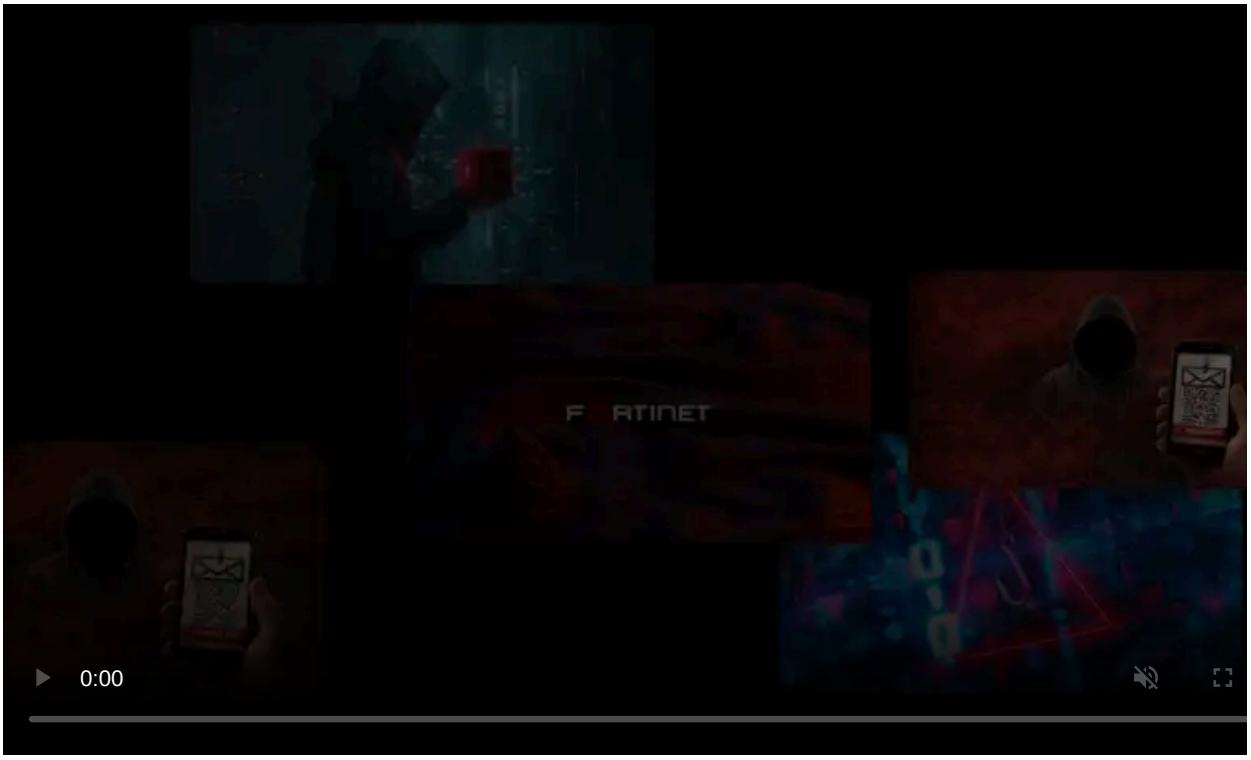
By Sergiu Gatlan

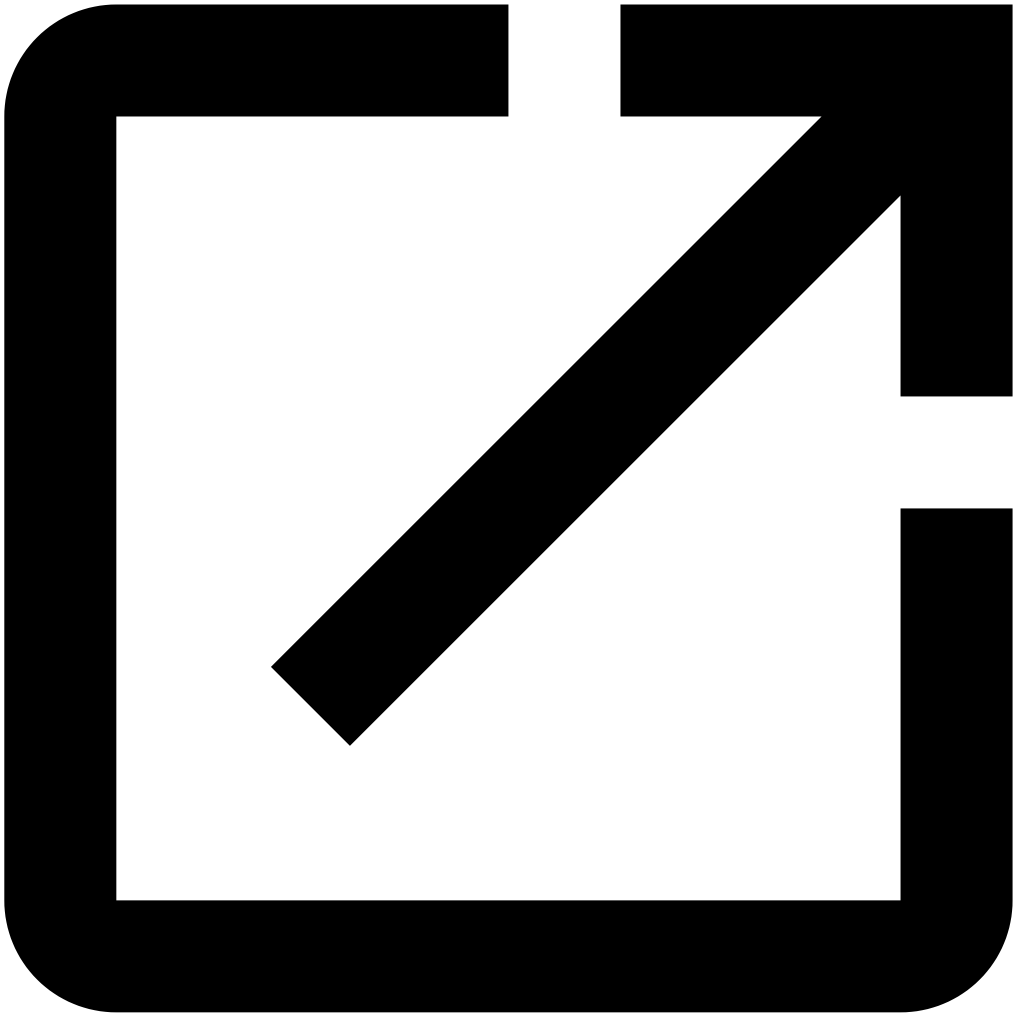
Published: 2020-11-05 · Archived: 2026-04-05 22:03:44 UTC

Brazil's Superior Court of Justice was hit by a ransomware attack on Tuesday during judgment sessions that were taking place over video conference.

"The Superior Court of Justice (STJ) announces that the court's information technology network suffered a hacker attack on Tuesday (3), during the afternoon, when the six group classes' judgment sessions took place," STJ President Humberto Martins said in an official statement on the Supreme Federal Court's website.

"The Secretariat for Information and Communication Technology (STI) is working on systems recovery to restore all court services as quickly as possible."


F RTINET
0:00



Brazilian journalist Mateus Nunes has told BleepingComputer that the websites of multiple other Brazilian federal government agencies are also currently offline.

However, it is not yet known if they were attacked by the same threat actors or if they are hosted on the same site as the courts.

Systems offline two days later

The systems of the Superior Tribunal de Justiça (aka STJ) were shut down to stop the spread throughout the court's network but not before all case files and backups were encrypted according to STJ IT specialists.

Two days after the ransomware attack took place, the Superior Court of Justice website and systems are still offline until all systems will be fully restored.

"A Domain Admin account was exploited which allowed the hacker to have access to our servers, to enter into administration groups of the virtual environment and, finally, encrypt a good part of our virtual machines," as one of the IT technicians told O Bastidor.

STJ "will operate on duty until next Monday," November 9, and all judgment sessions, virtual and / or by video conference will be either suspended or canceled until the court network's security will be restored.

The court's IT department also advised all users including judges, interns, and outsourced workers not to use any computers (personal ones included) if they were or are still connected to the court's network.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

"According to the resolution, administrative, civil and criminal procedural deadlines are suspended from the 3rd to the 9th of November (inclusive), returning to flow on the 10th," a statement on the court's website said.

"For the purpose of counting the term in criminal proceedings, the suspension period will be considered a reason of force majeure, according to the provision of paragraph 4 of article 798 of the Code of Criminal Procedure (CPP). Also according to the resolution, the measures can be reviewed at any time, depending on the result of efforts to normalize the systems."

RansomExx behind the attack

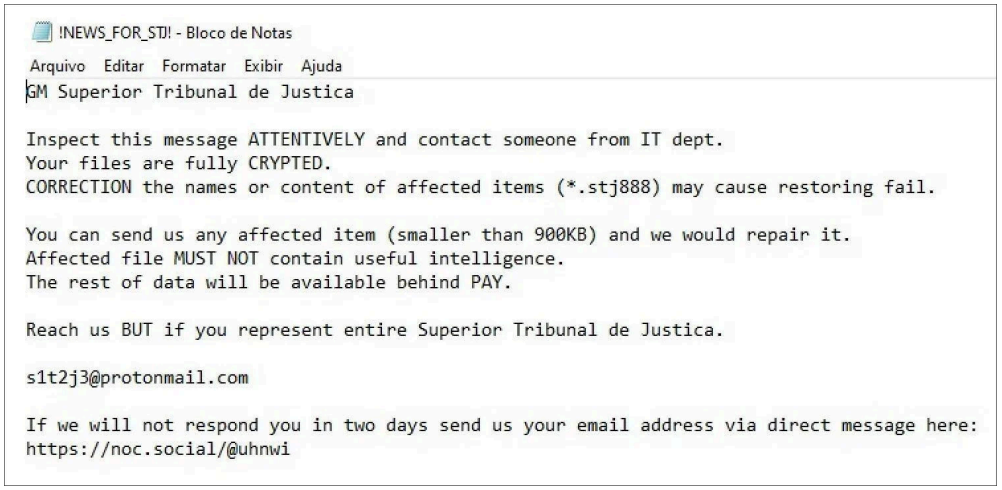
While the official STJ statements do not mention the ransomware gang responsible for this attack, a ransom note recovered from one of the encrypted computers shows that the RansomExx gang was behind it.

RansomExx sent BleepingComputer the following message when contacted for more details regarding the attack:

```
 Hello,
Ignore this message if you aren't officially represent whole affected company.
Send us any encrypted file (not greater than 1MB) for test decryption.
Then we will send you detailed instructions.
This step is necessary because we don't share such information for anyone except authorized persons.
Speak english.
```

According to an anonymous source, Pernambuco State Court of Justice (Tribunal de Justiça do Estado de Pernambuco — TJPE) systems were also hit by RansomExx on October 27, with their files being encrypted using the .tjpe911 extension.

RansomExx is a rebranded Defray777 ransomware version that became a lot more active during June 2020 and known for attacking high-profile organizations.



STJ ransom note

The Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies are among the gang's previous victims.

During their attacks, RansomExx's operators compromise the victims' networks and steal unencrypted sensitive documents while spreading laterally to other systems.

Once the RansomExx operators successfully compromise the victims' Windows domain controller, they deploy the ransomware payloads on all available network devices.

This is a developing story ...

H/T Altieres

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
