Campari hit by Ragnar Locker Ransomware, $15 million demanded

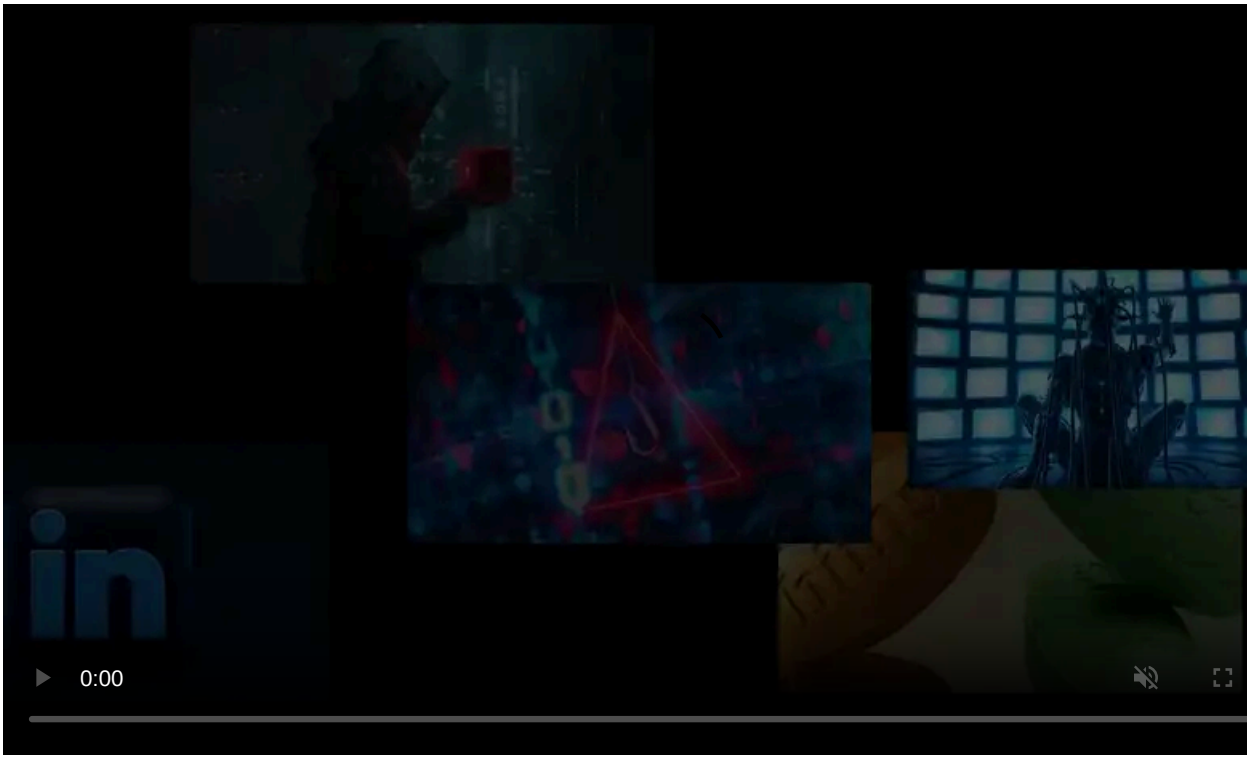
By Lawrence Abrams

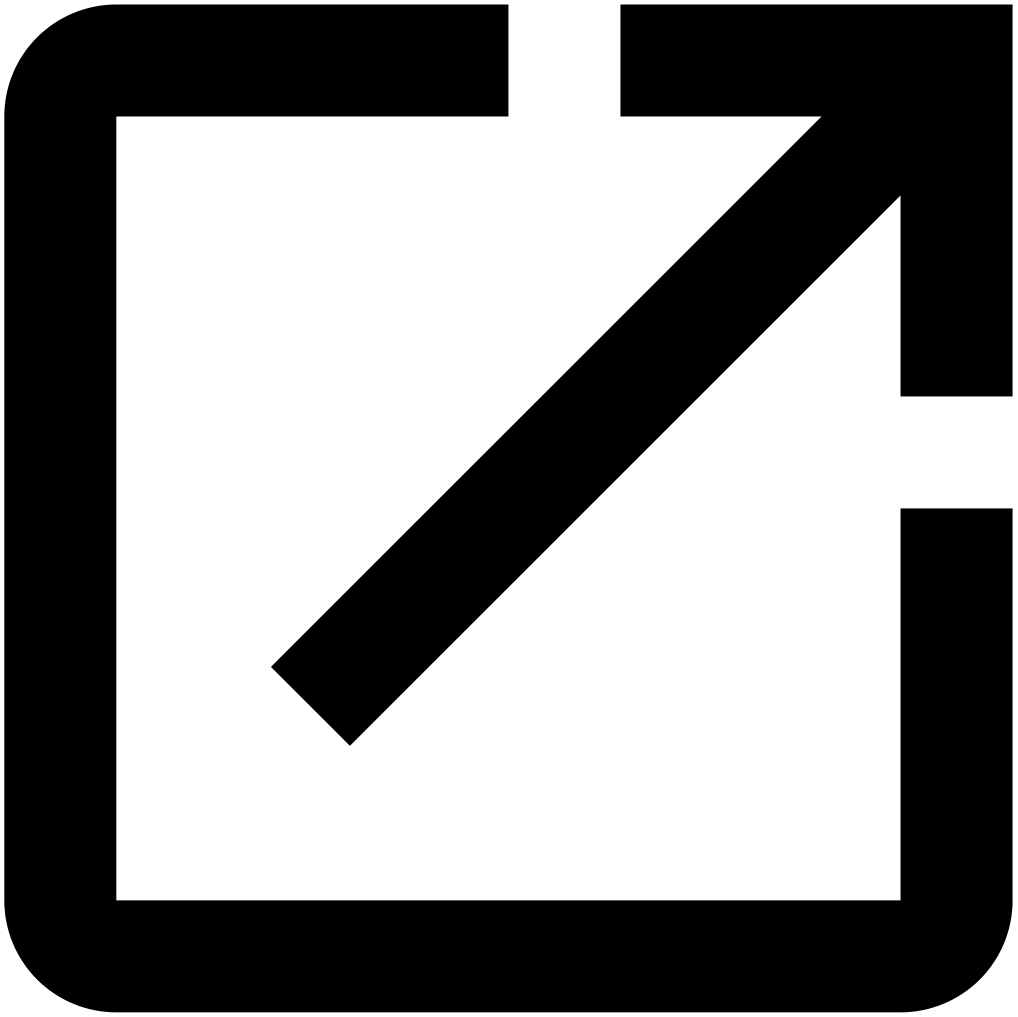
Published: 2020-11-05 · Archived: 2026-04-05 15:48:59 UTC

Italian liquor company Campari Group was hit by a Ragnar Locker ransomware attack, where 2 TB of unencrypted files was allegedly stolen. To recover their files, Ragnar Locker is demanding $15 million.

Campari Group is an Italian beverage company known for its popular liquor brands, including Campari, Frangelico, SKYY vodka, Epsolon, Wild Turkey, and Grand Marnier.

As first reported by ZDNet, Campari released a press statement on Monday where they stated they suffered a cyberattack over the weekend, which caused them to shut down their IT services and network.


0:00



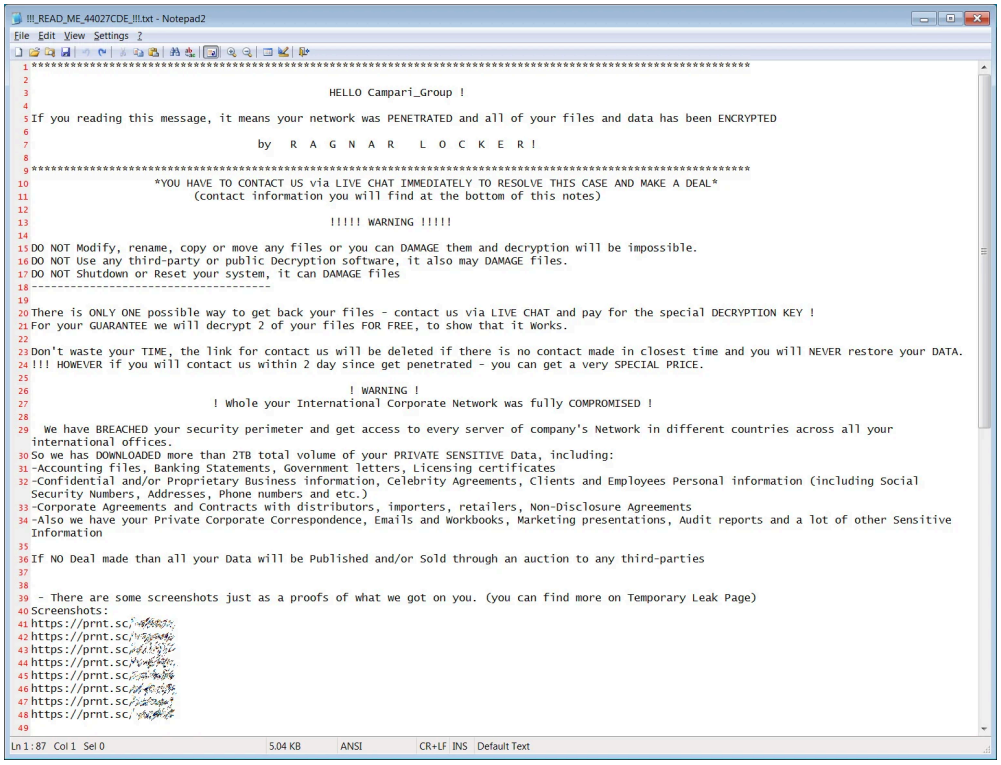
"Campari Group informs that, presumably on 1 November 2020, it was the subject of a malware attack (computer virus), which was promptly identified. The Group's IT department, with the support of IT security experts, immediately took action to limit the spread of malware in data and systems. Therefore, the company has implemented a temporary suspension of IT services, as some systems have been isolated in order to allow their sanitization and progressive restart in safety conditions for a timely restoration of ordinary operations," Campari said in a statement.

Due to this attack, the web sites for Campari and Campari Group are currently down.

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.

Ragnar Locker claims to have stolen 2 TB of data

In a Ragnar Locker sample discovered today by security researcher Pancak3 and installed by BleepingComputer, the ransom note clearly shows that it was used in the attack against Campari Group.



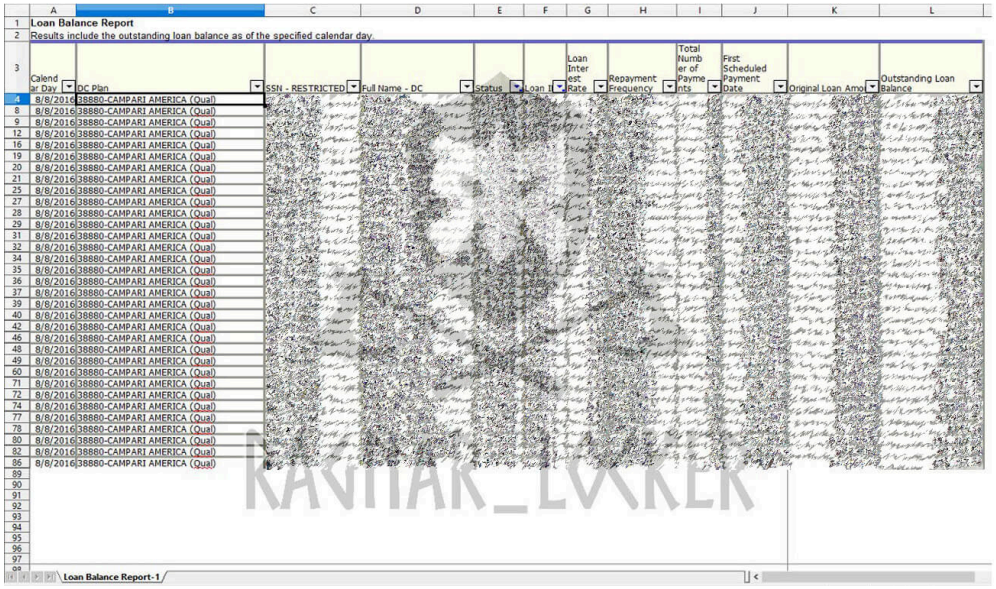
Ragnar Locker ransom note for Campari

Source: BleepingComputer

In the ransom note, the Ragnar Locker group claims to have stolen 2 TB of unencrypted files during the attack, including banking statements, documents, contractual agreements, emails, and more.

> We have BREACHED your security perimeter and get access to every server of company's Network in different countries across all your international offices.
> So we has DOWNLOADED more than 2TB total volume of your PRIVATE SENSITIVE Data, including:
> -Accounting files, Banking Statements, Government letters, Licensing certificates
> -Confidential and/or Proprietary Business information, Celebrity Agreements, Clients and Employees Personal information (including Social Security Numbers, Addresses, Phone numbers and etc.)
> -Corporate Agreements and Contracts with distributors, importers, retailers, Non-Disclosure Agreements
> -Also we have your Private Corporate Correspondence, Emails and Workbooks, Marketing presentations, Audit reports and a lot of other Sensitive Information

As proof that they stole data, the ransom note contains eight URLs to screenshots of some of the stolen data. These screenshots are for sensitive documents, such as bank statements, a UK passport, employee U.S. W-4 tax forms, a spreadsheet containing SSNs, and a confidentiality agreement.



A spreadsheet containing employee's SSN numbers
Redacted by BleepingComputer

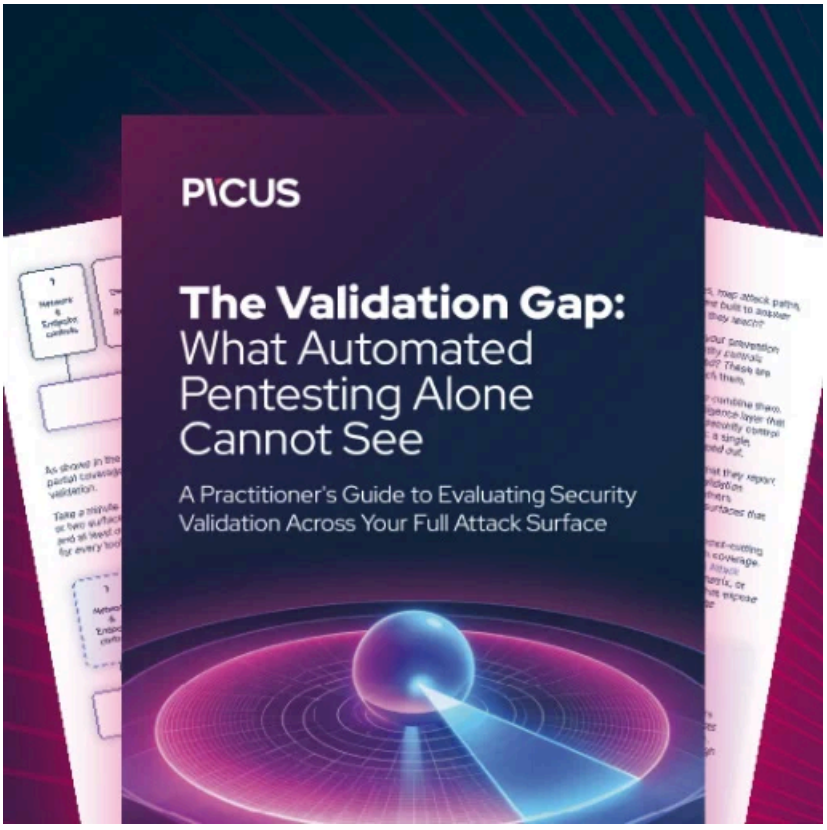
Pancak3 told BleepingComputer that Ragnar Locker claims to have encrypted most of Campari Group's servers from twenty-four countries and are demanding $15,000,000 in bitcoins for a decryptor.

This price also includes a promise to delete data from their file servers and not publish or share the data, as well as a network penetration report and recommendations to improve security.

It should be noted that ransomware negotiation service Coveware has found that ransomware operations are increasingly not keeping their promise to delete stolen data after a ransom is paid.

Ragnar Locker has been involved in other large attacks this year, including ones on Portuguese multinational energy giant Energias de Portugal (EDP) and French maritime transport and logistics company CMA CGM.

Bleeping Computer has contacted Campari Group with questions related to this attack but has not heard back.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

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.
