Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen

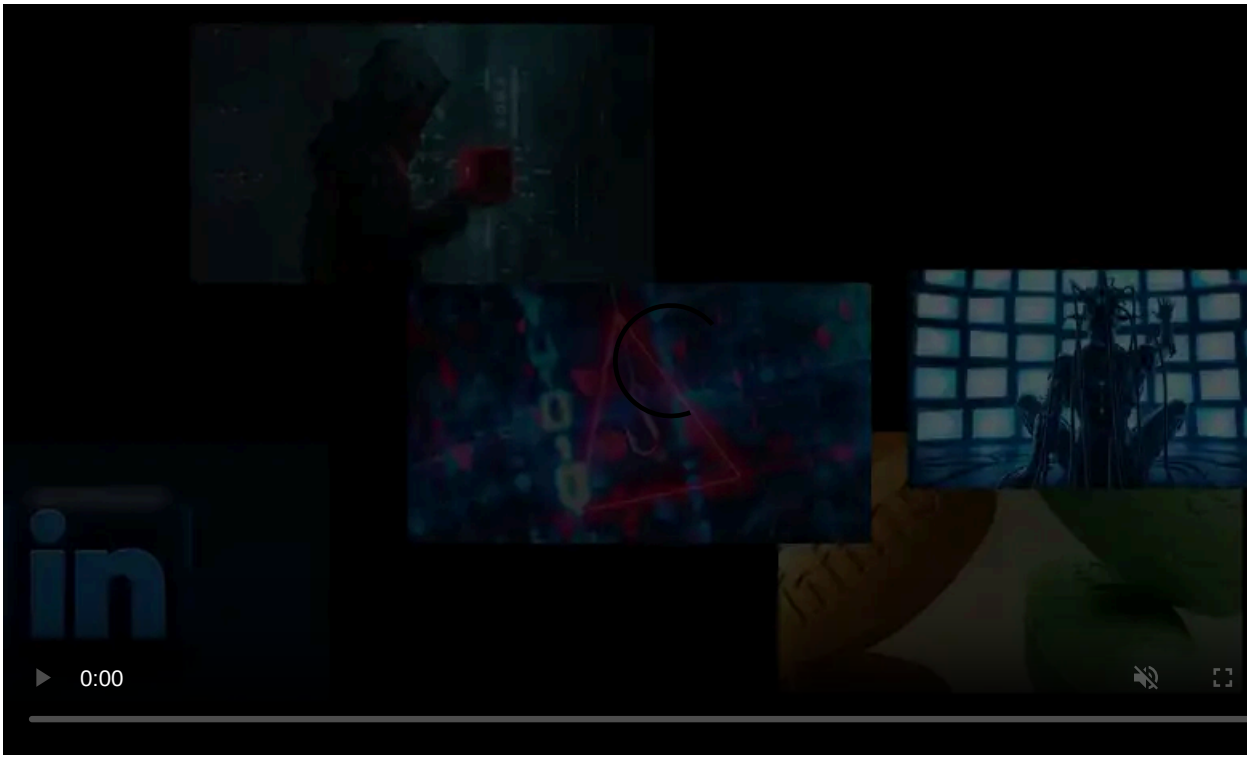
By Lawrence Abrams

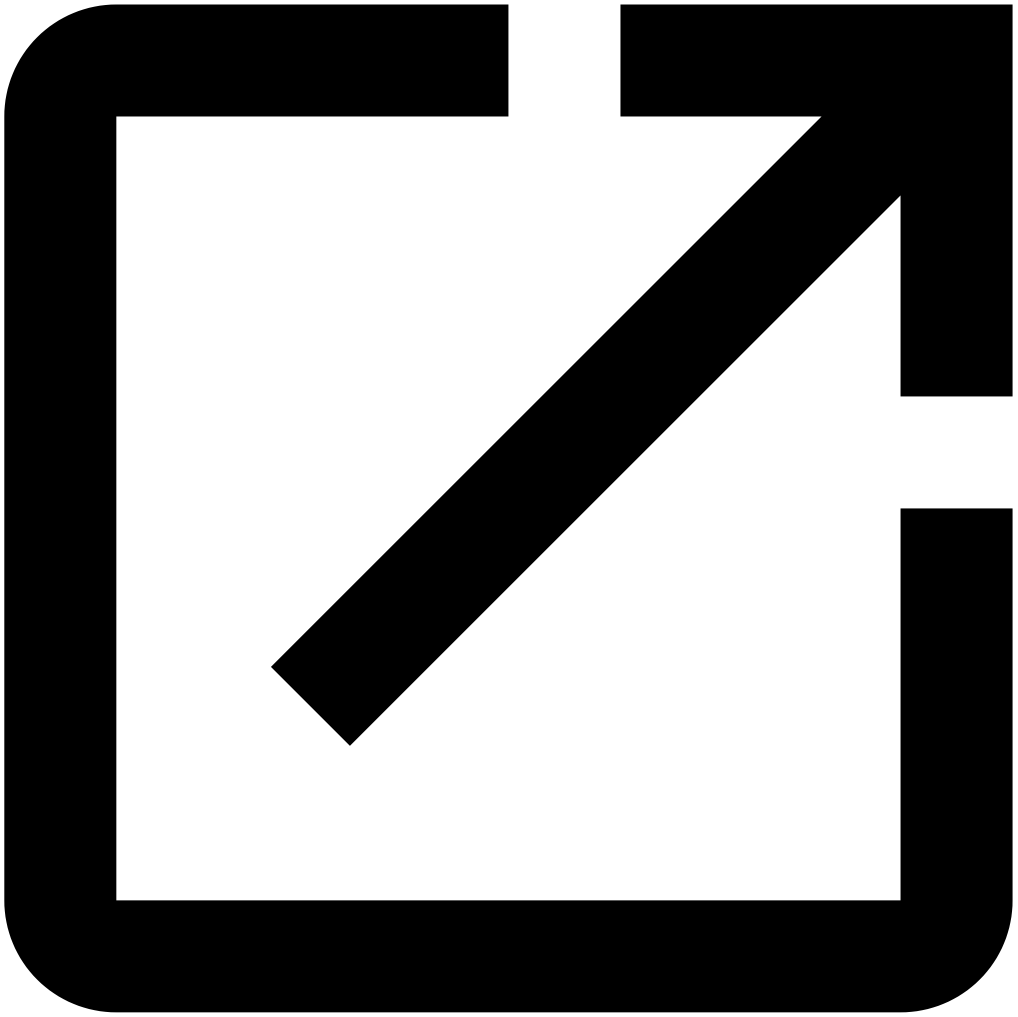
Published: 2020-11-05 · Archived: 2026-04-05 16:54:24 UTC

Japanese game developer Capcom has suffered a ransomware attack where threat actors claim to have stolen 1TB of sensitive data from their corporate networks in the US, Japan, and Canada.

Capcom is well-known for its iconic game franchises, including Street Fighter, Resident Evil, Devil May Cry, Monster Hunter, and Mega Man.

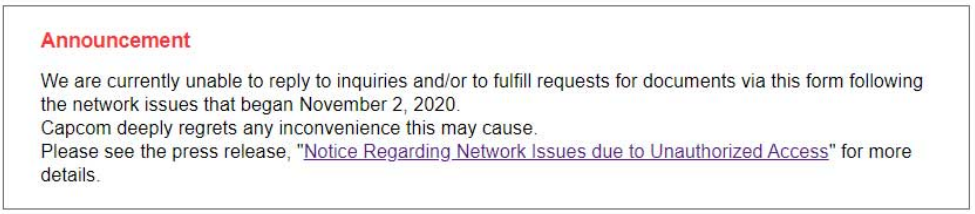
Yesterday, Capcom announced that they had been hit with a cyberattack on November 2nd, 2020, that led to the halting of portions of their corporate network to prevent the attack's spread.


0:00



"Beginning in the early morning hours of November 2, 2020 some of the Capcom Group networks experienced issues that affected access to certain systems, including email and file servers. The company has confirmed that this was due to unauthorized access carried out by a third party, and that it has halted some operations of its internal networks as of November 2."

Since the attack, Capcom has been displaying notices on its site warning visitors that emails and document requests will not be answered due to the attack impacting email systems.



Notice about email being down

At the time, Capcom did not disclose the details of the cyberattack, but in a ransomware sample found by security researcher Pancak3 we see that the Ragnar Locker ransomware gang attacked them.

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.

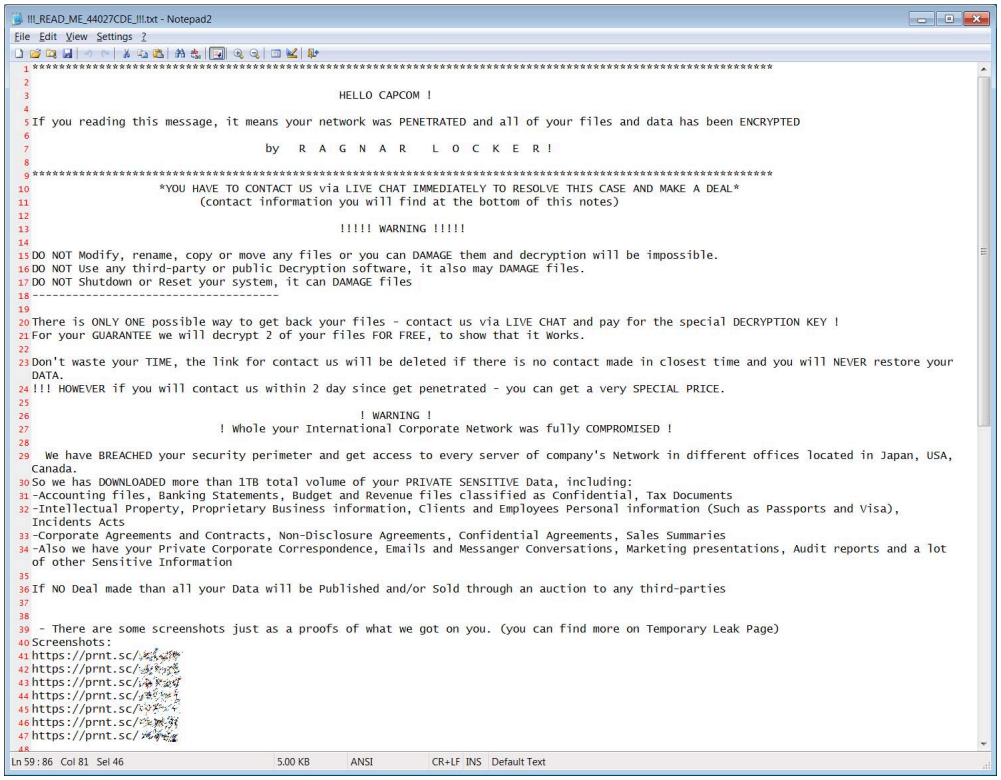
Ransomware gang claims to have stolen 1 TB of files

After running the Ragnar Locker sample, we get access to the ransom note created on Capcom's computers during the attack. This ransom note provides a huge amount of visibility into the Ragnar Locker attack.

In the ransom note created during the attack, the Ragnar Locker operators state that they have stolen 1 TB of unencrypted files from the corporate networks in Japan, the USA, and Canada.

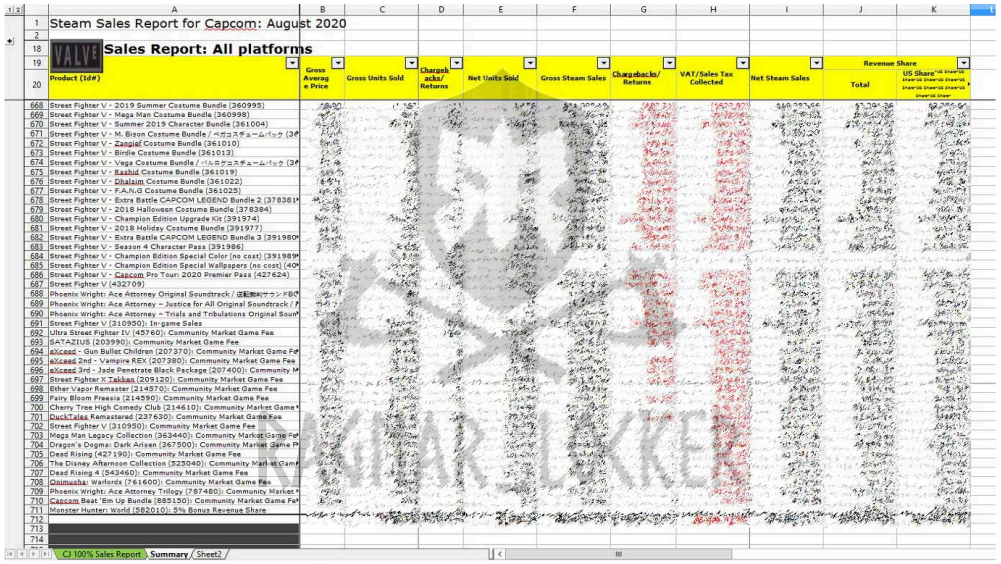
We have BREACHED your security perimeter and get access to every server of company's Network in different offices located in Japan, USA, Canada.
So we has DOWNLOADED more than 1TB total volume of your PRIVATE SENSITIVE Data, including:
-Accounting files, Banking Statements, Budget and Revenue files classified as Confidential, Tax Documents
-Intellectual Property, Proprietary Business information, Clients and Employees Personal information (Such as Passports and Visa), Incidents Acts
-Corporate Agreements and Contracts, Non-Disclosure Agreements, Confidential Agreements, Sales Summaries
-Also we have your Private Corporate Correspondence, Emails and Messanger Conversations, Marketing presentations, Audit reports and a lot of other Sensitive Information

If NO Deal made than all your Data will be Published and/or Sold through an auction to any third-parties



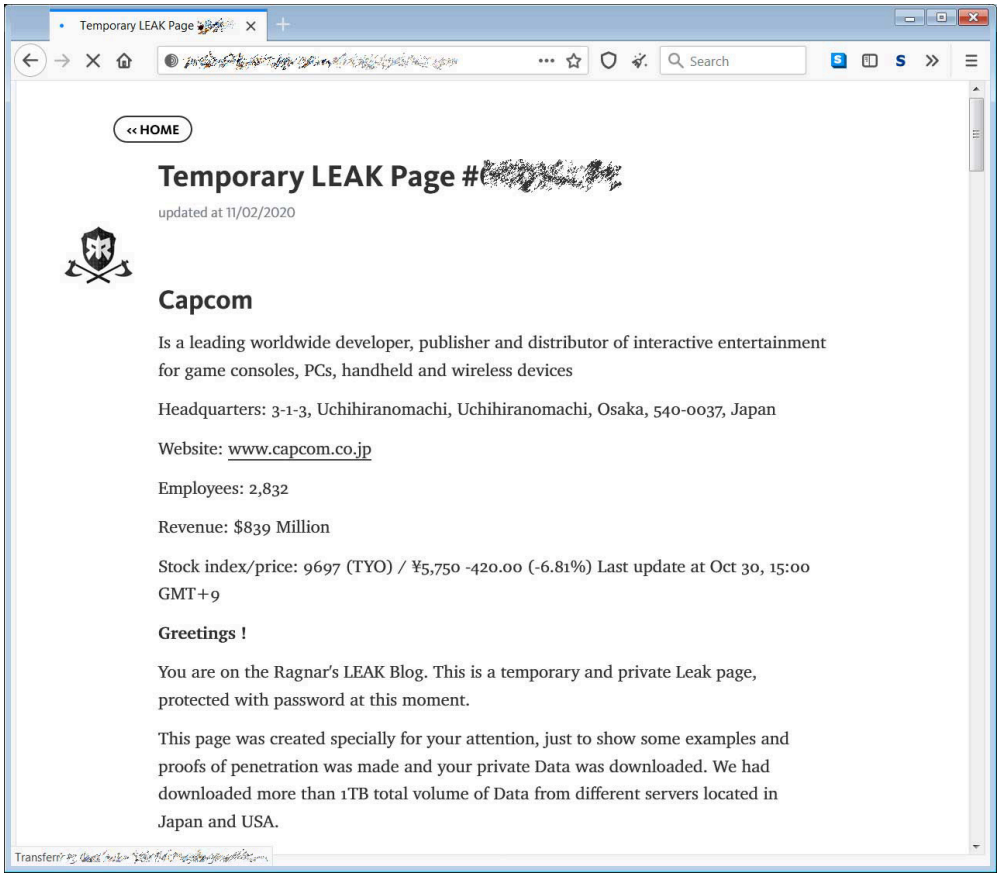
Capcom ransom note

Enclosed in the ransom note are seven print.sc URLs that display screenshots of stolen files, including employee termination agreements, Japanese passports, Steam sales reports from August, Bank statements, contractor agreements, and a screenshot of Active Directory Users and Computers MMC for the Capcom Windows domain.



Stolen Capcom August 2020 Steam sales report
Redacted by BleepingComputer

Also enclosed in the ransom note is a link to a private data leak page on Ragnar Locker's website containing a 24MB archive containing additional stolen documents, including revenue forecasts, salary spreadsheets, NDAs, immigration forms, corporate communications, and royalty reports.



Capcom temporary data leak page

The ransom note contains a link to the Ragnar Locker Tor negotiation site, where Capcom can discuss the ransom demand with the attackers. At this time, the chat page has not been used by Capcom, so there is no indication as to the ransom amount Ragnar Locker is demanding.

Pancak3 told BleepingComputer tonight that Ragnar Locker claims to have encrypted 2,000 devices on Capcom's networks and are demanding $11,000,000 in bitcoins for a decryptor.

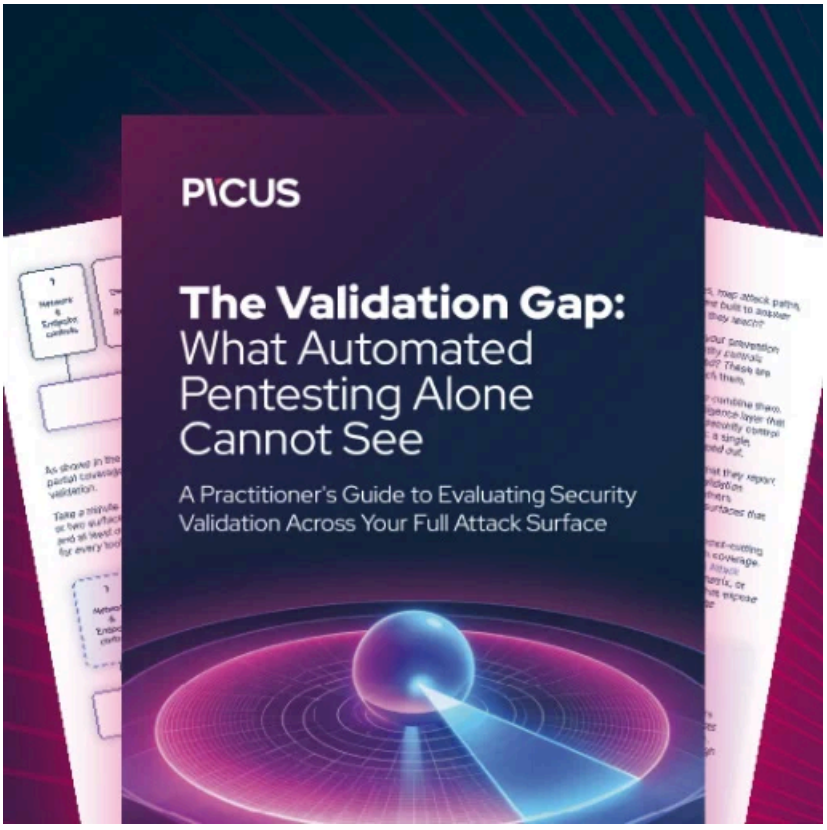
This ransom also includes a promise to delete any stolen data and a network penetration security report.

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

Ragnar Locker has been involved in other massive attacks this year, including ones on Portuguese multinational energy giant Energias de Portugal (EDP), where a $10.9M ransom was demanded. In September, they hit French maritime transport and logistics company CMA CGM, which led to significant downtime for the network and operations.

BleepingComputer has attempted to contact Capcom but has not received a response due to their email issues.

Update 11/5/20 7:00 PM EST: Added information on ransom amount.



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.

Source: https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/