MasterChef, Big Brother producer hit by DoppelPaymer ransomware

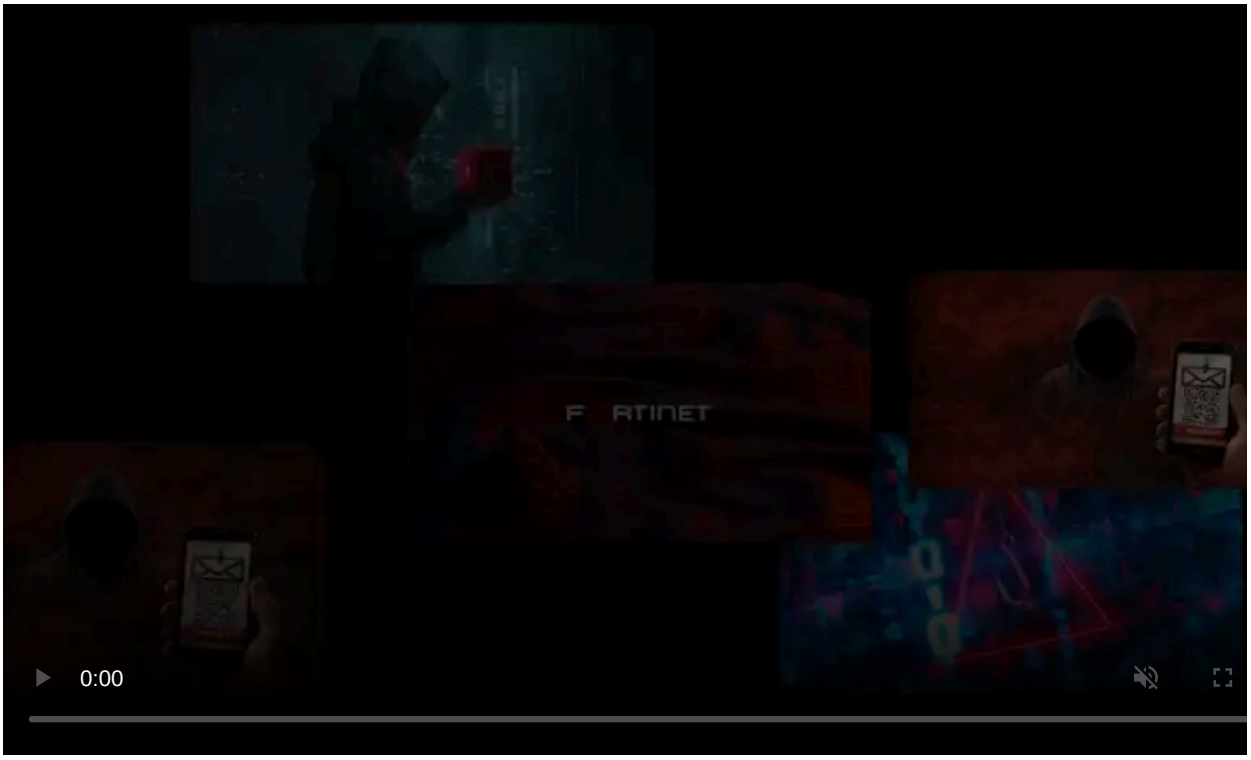
By Sergiu Gatlan

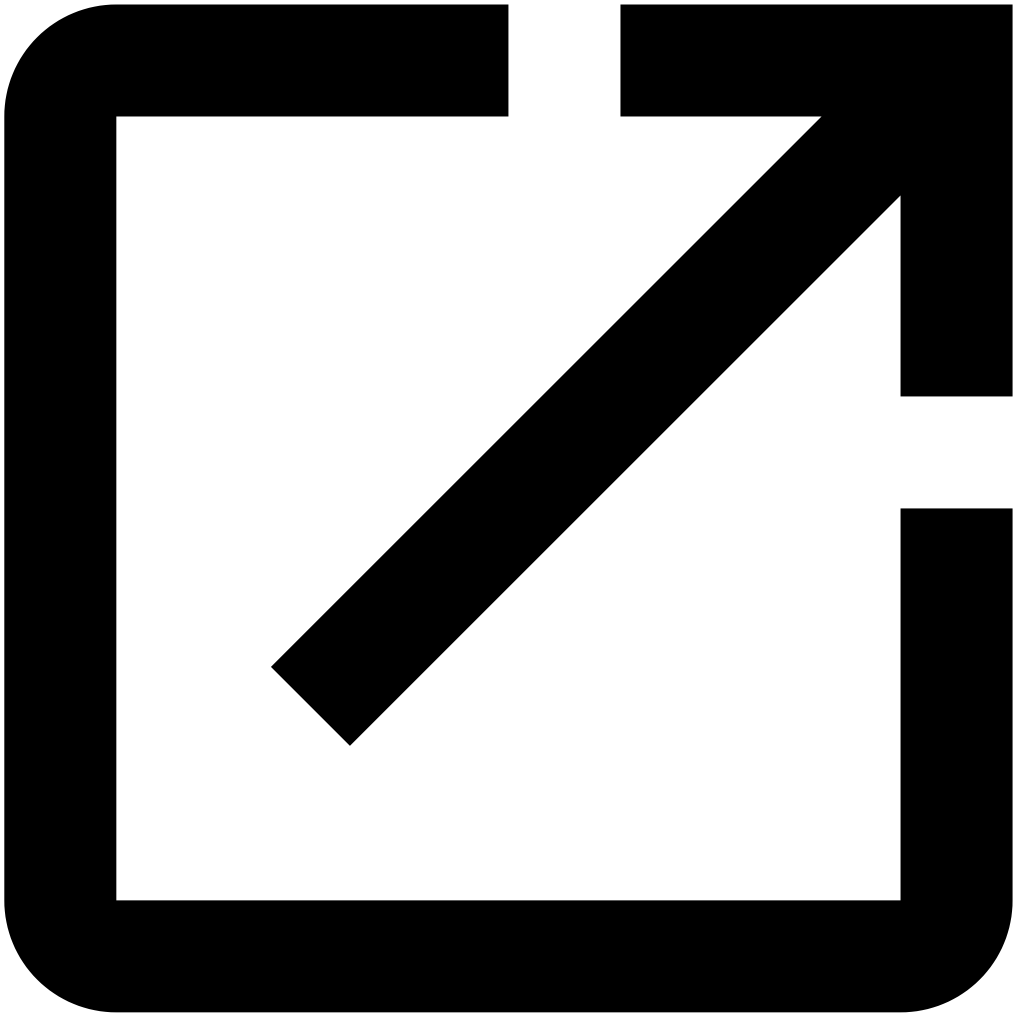
Published: 2020-11-27 · Archived: 2026-04-05 23:45:47 UTC

French multinational production and distribution firm Banijay Group SAS was hit earlier this month by a DoppelPaymer ransomware attack and had sensitive information stolen by the ransomware operators during the incident.

Yesterday, Banijay publicly confirmed a cyber incident that led to employee and commercially sensitive data potentially being compromised.

Banijay became one of the largest if no the largest international groups in the audiovisual content production and distribution market after acquiring Endemol Shine Group for $2.2 billion in July 2020.


F RTINET
0:00



The group is now home to more than 120 production companies across 22 territories and it is behind some of the biggest global entertainment brands including scripted and non-scripted content.

Banijay's brand list includes MasterChef, Survivor, Big Brother, The Kardashians, Mr. Bean, Black Mirror, Extreme Makeover: Home Edition, and Deal or No Deal among many others.

Only Endemol networks affected in the attack

"Banijay is currently managing a cyber incident involving the pre-existing Endemol Shine Group and Endemol Shine International networks," the group said.

"The business has reason to believe certain personal data of current and ex-employees may have been compromised, as well as commercially sensitive information."

Banijay reported the incident to local authorities in the United Kingdom and the Netherlands, where the assets affected in the attack are located.

The French-based audiovisual production group has also hired third-party security experts to help with the attack investigation.

"The global group is currently investigating the situation with independent specialists, and to date, has reported the issue to the relevant local authorities in both the Netherlands and the UK – the territories affected by the incident," Banijay added.

"We are continuing to take the appropriate steps and remain committed to protecting our employees, past and present, so if we do identify any cases of data being taken or misused, we will contact the affected individuals directly."

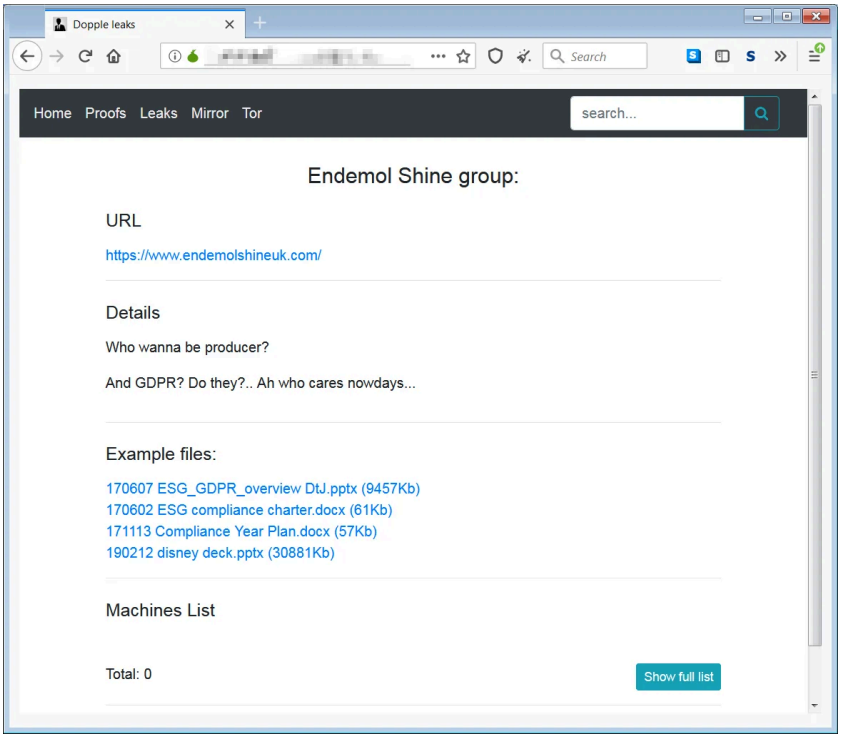
DoppelPaymer claiming to be behind attack

While Banijay has only shared that they have suffered a cyber-attack and that some of their data might have been compromised, the DoppelPaymer ransomware gang is claiming to be responsible.

As proof of the their involvement in the attack, the DoppelPaymer operators have shared several documents presumably stolen from Banijay's systems, a tactic adopted from Maze Ransomware starting with February 2020.

DoppelPaymer is also taunting the French production group by referencing GDPR compliance issues and leaking an internal GDPR compliance document, among others.

DoppelPaymer is a ransomware operation known for hitting enterprise targets since at least mid-June 2019 by gaining access to admin credentials and using them to deploy the ransomware payloads to all devices after compromising the entire network.



This ransomware gang is also known for asking large ransoms since they have been known to encrypt hundreds and even thousands of devices on their victims' networks.

For instance, in November 2019, Mexico's state-owned oil company PEMEX was hit by DoppelPaymer and was asked to pay $4.9 million worth of bitcoins as a ransom.

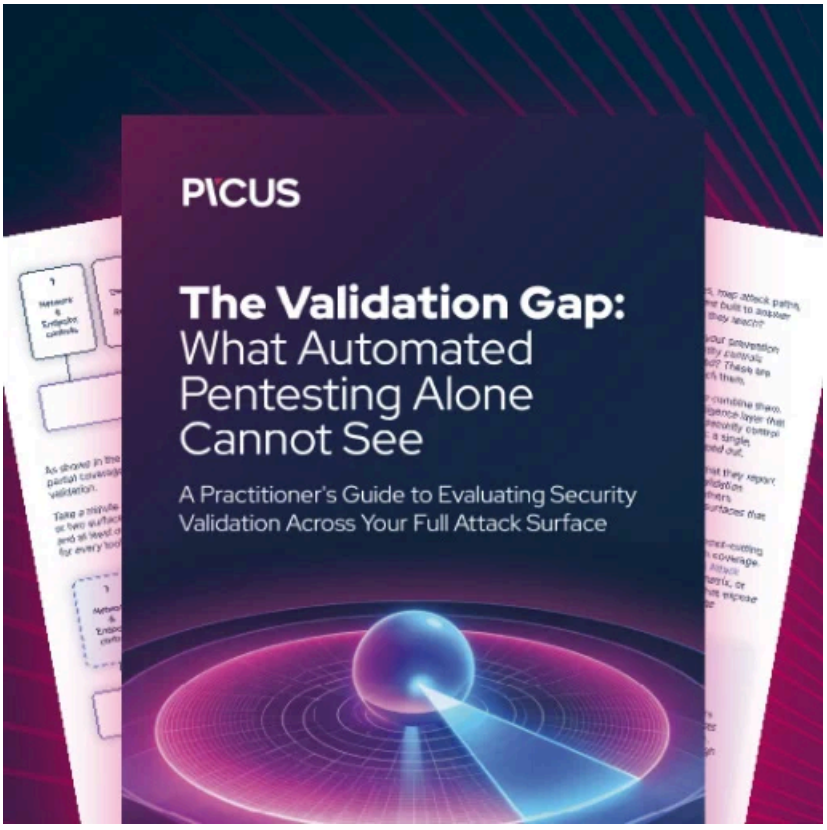
DoppelPaymer got its name from BitPaymer (with which it's sharing large portions of code) but the gang has also added numerous upgrades including a threaded encryption process for faster operation.

A Banijay spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today.

Update 1: Added DoppelPaymer ransomware info and updated title.

Update 2: A Banijay spokesperson said that the incident is still under investigation.

> The pre-existing Endemol Shine Group network, which also comprises Endemol Shine International, has been targeted in a cyber-attack. We are currently investigating the matter and at this stage have no further comment.



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/masterchef-big-brother-producer-hit-by-doppelpaymer-ransomware/