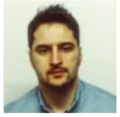
Ubisoft, Crytek data posted on ransomware gang's site

zdnet.com/article/ubisoft-crytek-data-posted-on-ransomware-gangs-site/

Home Innovation Security

Details about hackers obtained the files remain unclear. Ransomware gang also threatened to leak the source code of Watch Dogs: Legion, an upcoming Ubisoft game.



Written by Catalin Cimpanu, Contributor on Oct. 15, 2020

A ransomware gang going by the of Egregor has leaked data it claims to have obtained from the internal networks of two of today's largest gaming companies — Ubisoft and Crytek.

Data allegedly taken from each company has been published on the ransomware gang's dark web portal on Tuesday.

egregor-leak.png

Image: ZDNet
Details about how the Egregor gang obtained the data remain unclear.

Ransomware gangs like Egregor regularly breach companies, steal their data, encrypt files, and ask for a ransom to decrypt the locked data.

However, in many incidents, ransomware gangs are also get caught and kicked out of networks during the data exfiltration process, and files are never encrypted. Nevertheless, they still extort companies, asking victims for money to not leak sensitive files.

Usually, when negotiations break down, ransomware gangs post a partial leak of the stolen files on so-called leak sites.

On Tuesday, leaks for both Crytek and Ubisoft were posted on the Egregor portal at the same time, with threats from the ransomware crew to leak more files in the coming days.

For the Ubisoft leak, the Egregor group shared files to suggest they were in possession of source code from one of the company's Watch Dogs games. On its web portal, the group touted they were in possession of the source code for the Watch Dogs: Legion game, scheduled to be released later this month. It was, however, impossible to verify that these files came from the new game, rather than an existing release.

ubisoft-leaked-folder.png

Image: ZDNet

For the past year, security researchers have tried to reach out and notify Ubisoft about several of its employees getting phished, with no results, which may provide a clue of how the hackers might have got it.

But while hackers leaked only 20 MB from Ubisoft, they leaked 300 MB from Crytek, and this data contained a lot more information.

The Crytek files included documents that appeared to have been stolen from the company's game development division. These documents contained resources and information about the development process of games like Arena of Fate and Warface, but also Crytek's old Gface social gaming network.

crytek-leak-folders.png

Image: ZDNet

crytek-leak.png

Image: ZDNet

crytek-leak-minutes.png

Image: ZDNet

Neither Ubisoft nor Crytek responded to emails seeking comment on the leaks. None of the companies reported major security incidents weeks, nor any abnormal and prolonged downtimes, suggesting the Egregor intrusion didn't likely impact cloud and gaming system, but merely backend office and work networks, where most ransomware incidents usually incur damages.

However, in an email interview with ZDNet, the Egregor gang provided more details about the two incidents. The ransomware operators said they breached the Ubisoft network, but only stole data, and did not encrypt any of the company's files.

On the other hand, "Crytek has been encrypted fully," the Egregor crew told ZDNet.

The Egregor group said that neither company engaged in discussions, despite their intrusions, and no ransom has been officially requested yet.

"In case Ubisoft will not contact us we will begin posting the source code of upcoming Watch Dogs and their engine," the group threatened, promising to publish more data in a press release tomorrow.