# Crytek confirms Egregor ransomware attack, customer data theft

bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/

Sergiu Gatlan

By
Sergiu Gatlan

- August 10, 2021
- 03:45 PM
- 0


Game developer and publisher Crytek has confirmed that the Egregor ransomware gang breached its network in October 2020, encrypting systems and stealing files containing customers' personal info later leaked on the gang's dark web leak site.

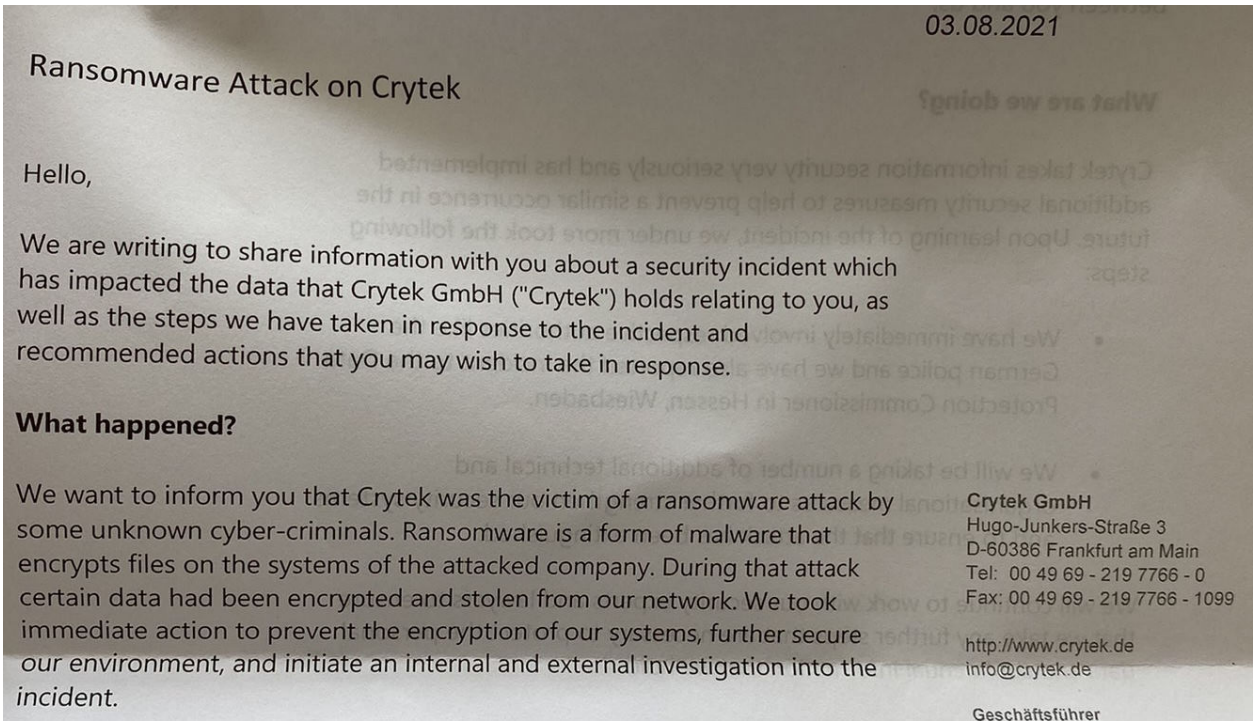
The company acknowledged the attack in breach notification letters sent to impacted individuals earlier this month and shared by one of the victims with BleepingComputer today.

"We want to inform you that Crytek was the victim of a ransomware attack by some unknown cyber-criminals," Crytek said in a letter mailed to one of their customers impacted in the incident.

"During that attack certain data had been encrypted and stolen from our network. We took immediate action to prevent the encrypton of our systems, further secure our environment, and initiate an internal and external investigation into the incident.

Crytek confirmed that Egregor operators later leaked documents stolen during the incident on their data leak site.

"Based on our investigation, the information in some case included individuals' first and last name, job title, company name, email, business address, phone number and country," Crytek revealed.



03.08.2021

Ransomware Attack on Crytek

Hello,

We are writing to share information with you about a security incident which has impacted the data that Crytek GmbH ("Crytek") holds relating to you, as well as the steps we have taken in response to the incident and recommended actions that you may wish to take in response.

**What happened?**

We want to inform you that Crytek was the victim of a ransomware attack by some unknown cyber-criminals. Ransomware is a form of malware that encrypts files on the systems of the attacked company. During that attack certain data had been encrypted and stolen from our network. We took immediate action to prevent the encryption of our systems, further secure our environment, and initiate an internal and external investigation into the incident.

Crytek GmbH
Hugo-Junkers-Straße 3
D-60386 Frankfurt am Main
Tel: 00 49 69 - 219 7766 - 0
Fax: 00 49 69 - 219 7766 - 1099

http://www.crytek.de
info@crytek.de

Geschäftsführer

*Crytek ransomware letter (BleepingComputer)*

## Data breach impact downplayed

The game developer tried to reassure affected customers by saying "the website itself was difficult to identify [..], so that in our estimation, only very few people will have taken note of it."

Crytek added downloading the leaked data would've also taken too long, which would have also likely represented a significant hurdle that stopped people from trying to grab it.

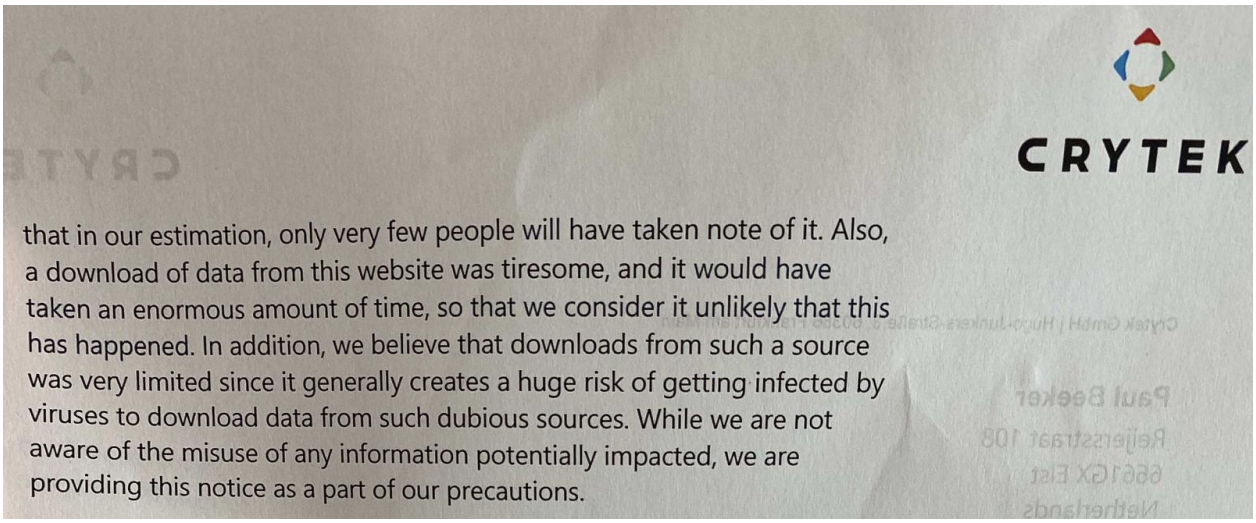
Crytek also believes that those who attempted downloading the stolen data were discouraged by the "huge risk" of compromising their systems with malware embedded in the leaked documents.

While these points would make sense for individuals with little to no experience in using computers, most people who would want and know how to get their hands on this type of data would likely use downloaders and open the leaked files in a virtual machine.

Furthermore, threat actors commonly download files leaked on ransomware data leaks to sell or share with other cybercriminals.

Considering this, Crytek's attempts to downplay the seriousness of the data breach resulting from the October 2020 ransomware attack don't hold water.

"While we are not aware of misues of any information potentially impacted, we are providing this notice as part of our precautions," Crytek added.




*Crytek data leak (BleepingComputer)*

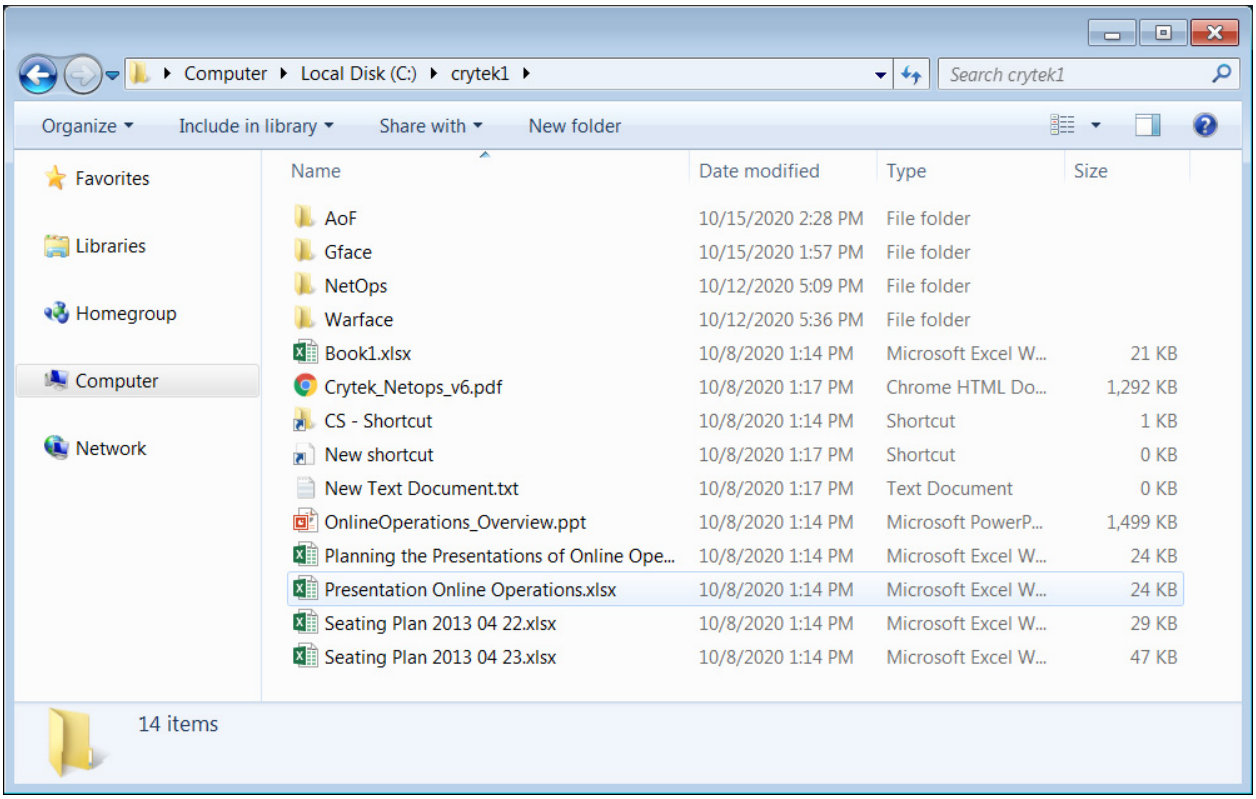
As BleepingComputer reported in October, Crytek's systems were hit by Egregor ransomware in an attack confirmed by sources familiar with the incident.

While we were not told how many Crytek systems were encrypted in the attack, we were told that files were encrypted and renamed to include the '.CRYTEK' extension.

The stolen data leaked by Egregor on their data leak site included:

- Files related to WarFace
- Crytek's canceled Arena of Fate MOBA game
- Documents with information on their network operations

Other well-known companies and organizations worldwide attacked by Egregor in the past include Barnes and Noble, Kmart, Cencosud, Randstad, and Vancouver's TransLink metro system.



*Stolen Crytek data (BleepingComputer)*

## Egregor affiliates arrested in Ukraine

In February 2021, several members of the Egregor ransomware operation were arrested in Ukraine following a joint operation between French and Ukrainian law enforcement.

Law enforcement officers made the arrests after French authorities could trace ransom payments to individuals located in Ukraine.

The arrested individuals are believed to be Egregor affiliates whose job was to hack into corporate networks and deploy the ransomware.

Egregor launched in September 2020, right after the Maze ransomware gang began shutting down its operation.

At the time, BleepingComputer was told by threat actors that Maze's affiliates switched to Egregor's RaaS, allowing the new RaaS to launch with experienced and skilled hackers.

Egregor operates as a ransomware-as-a-service (RaaS) where the ransomware developers partner with affiliates who conduct the attacks, splitting the ransom payments.

As part of this arrangement, the core team earns between 20-30% of all paid ransoms, while affiliates pocketed the other 70-80%.

Cybersecurity firm Kivu said in a February report that Egregor has 10-12 core members and 20-25 semi-exclusively vetted members, and it amassed over 200 victims since its September launch.

*A Crytek spokesperson was not available for comment when contacted by BleepingComputer earlier today or after our initial report from October 2020.*

## Related Articles:

Ransomware attack exposes data of 500,000 Chicago students

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Crytek
- Data Breach
- Egregor
- Ransomware

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article



## You may also like: