East Tennessee Children’s Hospital updates information on ransomware incident

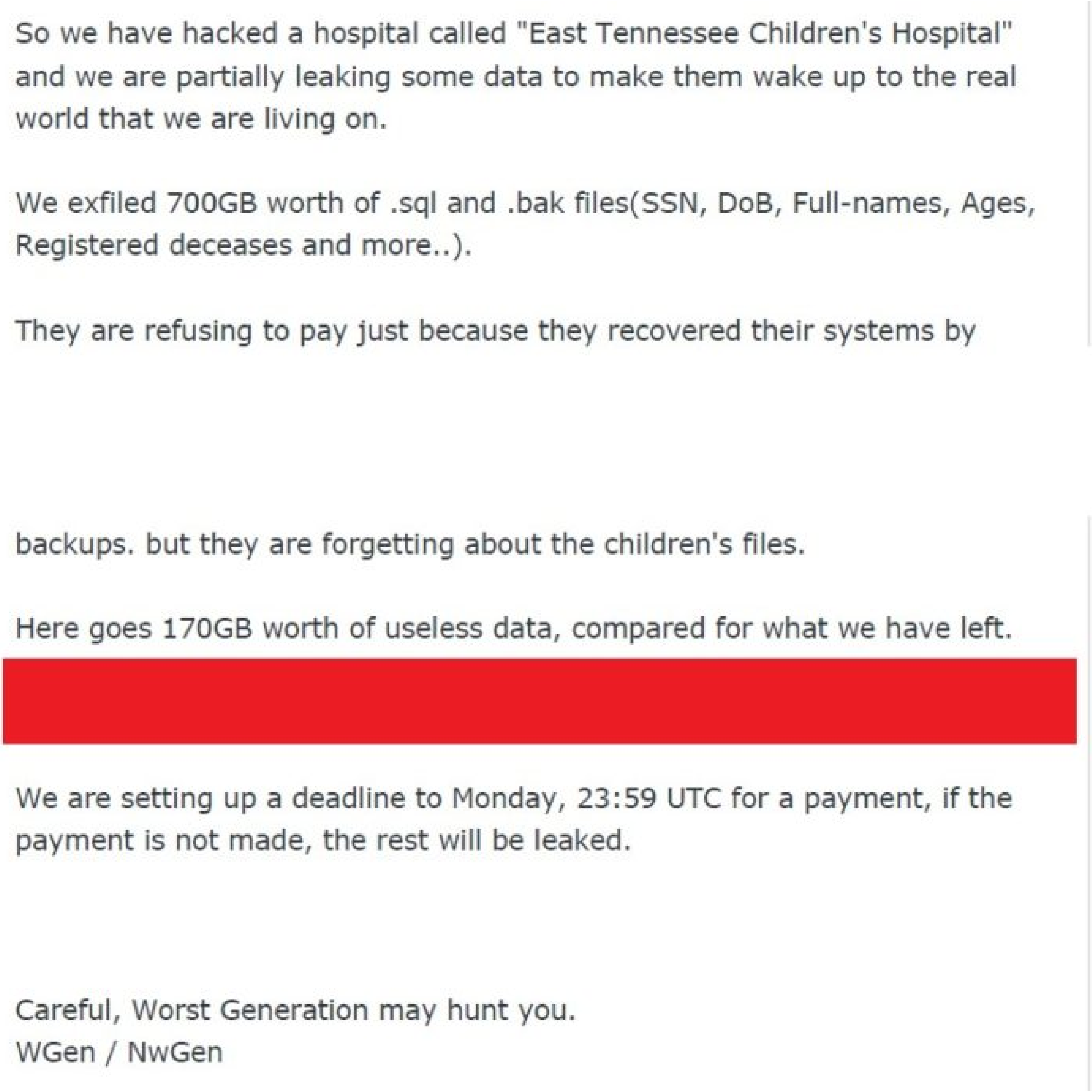
databreaches.net/east-tennessee-childrens-hospital-updates-information-on-ransomware-incident/

Dissent

April 8, 2022

On March 15, this site noted that the East Tennessee Children’s Hospital had posted a notice about an IT security incident. At the time, they did not identify the incident as a ransomware incident.

DataBreaches.net subsequently found some explanation for that notice — a listing on a Russian-language forum offering data from ETCH with numerous screencaps and a compressed archive of files. The listing was posted by a user affiliating with a group they called “NWGEN” and stated that although ETCH had been able to recover from backup, they were “forgetting about the children’s files.” The threat actor claimed that they had “exfiled 700GB worth of .sql and .bak files(SSN, DoB, Full-names, Ages, Registered deceases and more..)” and were dumping 170GB of “useless” data at that point.



So we have hacked a hospital called "East Tennessee Children's Hospital" and we are partially leaking some data to make them wake up to the real world that we are living on.

We exfiled 700GB worth of .sql and .bak files(SSN, DoB, Full-names, Ages, Registered deceases and more..).

They are refusing to pay just because they recovered their systems by backups. but they are forgetting about the children's files.

Here goes 170GB worth of useless data, compared for what we have left.

[redacted]

We are setting up a deadline to Monday, 23:59 UTC for a payment, if the payment is not made, the rest will be leaked.

Careful, Worst Generation may hunt you.
WGen / NwGen

A forum listing with data from ETCH seen on a Russian-language forum in March.

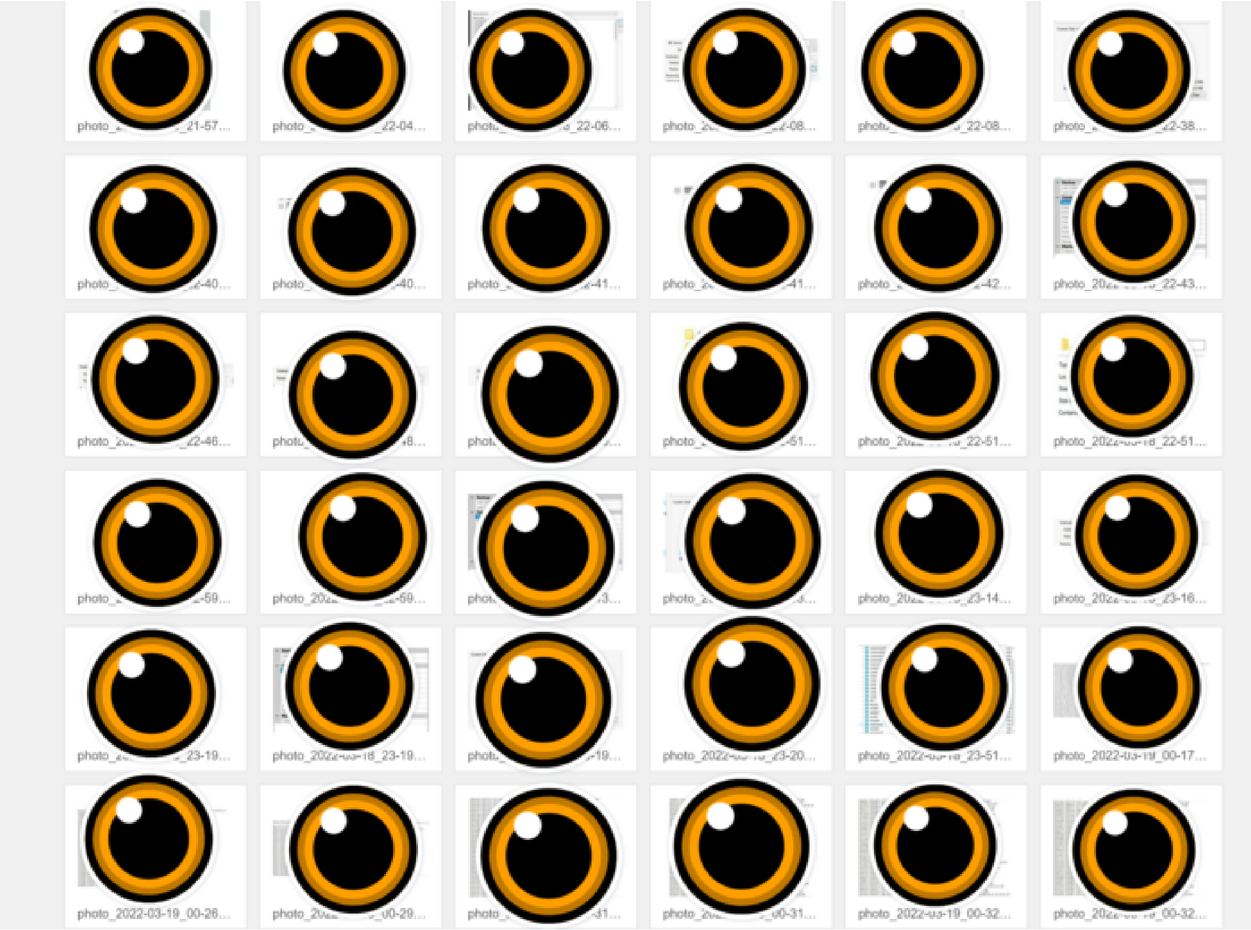
The listing did not get much response other than from one individual who noted that the original torrent link did not work. Perhaps the attacker misgauged how much people might detest them for trying to capitalize on children’s sensitive information. In any event, there is no indication of how many people may have downloaded the data, and there was no further leak of ETCH data posted on that forum by that user. A quick check of other sites did not find the data from ETCH on two other popular forums where hacked data are often leaked (but of course, there are more than three places on the internet where such data might be shared).

Today, The Daily Times in Tennessee has an update on the incident and reports that a new press release was issued by the hospital yesterday. The following is part of that press release:

> **What Happened?** On March 13, 2022, ETCH identified unusual activity on its network. We promptly began taking steps to secure our systems and commenced a comprehensive investigation into the incident. Through the investigation to date, we have determined that ETCH experienced a cyber incident. While our investigation is ongoing, on March 18, 2022, we determined that certain documents stored within ETCH's environment may have been copied from or viewed on the system as part of the cyber incident between March 11, 2022 – March 14, 2022. Based on the investigation, ETCH is currently working to determine the scope of potentially affected information and conducting a detailed review of the potentially impacted data to determine the type of information present and to whom it relates. This effort is currently ongoing.
>
> **What Information Was Involved?** While the investigation to determine the full scope of potentially affected information is ongoing and may vary by individual, the relevant ETCH systems may contain the following types of information at the time of the event: names, date of birth, Social Security number, driver's license or state identification number, non-resident identification number, other demographic information, medical information, health insurance information, credit or debit card information, financial information, billing information, other personal health information, and usernames and passwords.

The full press release can be found on ETCH's website, here.

But "may have been copied or viewed?" ETCH had direct knowledge and proof as to some of what had happened, as they actually negotiated with the threat actors and were given multiple examples of proof. Then, too, some data were actually dumped and made freely available to the public.


photo_[redacted]21-57...
photo_[redacted]22-04...
photo[redacted]_22-06...
photo_2[redacted]22-08...
photo[redacted]_22-08...
photo_[redacted]22-38...
photo_[redacted]2-40...
photo_[redacted]-40...
photo_[redacted]2-41...
photo_2[redacted]41...
photo_[redacted]-42...
photo_202[redacted]_22-43...
photo_202[redacted]_22-46...
photo[redacted]8...
phot[redacted]...
photo_[redacted]51...
photo_202[redacted]_22-51...
photo_2022-03-18_22-51...
photo_[redacted]2-59...
photo_202[redacted]2-59...
phot[redacted]3...
photo_2[redacted]3...
photo_202[redacted]_23-14...
photo_202[redacted]_23-16...
photo_2[redacted]_23-19...
photo_2022-03-18_23-19...
photo[redacted]-19...
photo_2022-03-18_23-20...
photo_2022-03-18_23-51...
photo_2022-03-19_00-17...
photo_2022-03-19_00-26...
photo_202[redacted]_00-29...
photo[redacted]31...
photo_202[redacted]00-31...
photo_2022-03-19_00-32...
photo_202[redacted]_00-32...

The threat actors showed a negotiator for ETCH numerous files that they had exfiltrated during negotiations. These are just some. Redacted by DataBreaches.net.

The threat actors also uploaded some of the negotiations between them and "Todd," someone who claimed to be an IT employee for ETCH, but used a Yahoo.com address. At one point, the negotiator indicated that they would reduce their demand to $300,000.00.

The deadline given to ETCH to pay came and went, and it appears the initial data dump was reuploaded by the original poster to another file-sharing site on April 1. Yet no additional data has been leaked. Does that mean that there is still some negotiation going on?

ETCH's press release is totally silent on the issue of ransom or any negotiations.

But should ETCH have told people that they know some data has already been dumped on the internet? How much personnel information does that 3.8 GB compressed archive contain?

And what, if anything, have the attackers done with any patient data?

Update May 23, 2022: ETCH reported this incident to the Maryland AG's Office on May 19 as impacting **422,531 people.**

Related Posts:

- East Tennessee Children's Hospital Statement on…
- Methodist Family Health discloses breach potentially…
- Tennessee Orthopaedic Clinics notifies HHS of…
- Ransomware group starts leaking data allegedly from…
- Updates on three class action lawsuits involving…