

DAIXIN TEAM HITS HEALTHCARE

- Threat actors potentially based in the far East, English fluent, professional negotiators
- Extortion for ransom with significantly higher victim pay rate
- Actively targeting U.S. Healthcare (e.g., [Fitzgibbon](#), [Oakbend](#), and others)
- Tor blog, HTTPS Exfil, 'Daxin' backdoor malware? (ref: [CISA released Broadcom report](#))

```

READ-ME_DaixinRansomNote.txt ▼
1 Welcome to the ransomware world!
2 We have exfiltrated critical documents and information from your network.
3 Your systems are encrypted.
4
5 Do not try to solve this by yourself (or contact the recovery company)-
6 you will only lose time and money.
7
8 To contact us:
9 1.) Install official Tor Browser (https://www.torproject.org/download/)
10 2.) Open [redacted] in Tor Browser
11 3.) Input your personal PIN
12 Your personal PIN is: [redacted]
13 Do not share this PIN!
14 If you do not contact us, the data will be published within 5 days.
15
16 $$$ Daxin Team $$$

```

DAIXIN Team

Here you can get links to:

Information compromised in the Data Breach includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, 'PII'), and medical and treatment information ('PHI'), The PII and PHI that collected and maintained - the 'Private Information.' Private Information can commit a variety of crimes including, e.g., opening new financial accounts, taking out loans in, using to obtain medical services, using health information to target other phishing and hacking intrusions based on their individual health needs, using information to obtain government benefits, filing fraudulent tax returns using information, obtaining driver's licenses in names but with another person's photograph, and giving false information to police during an arrest.

```

Fitzgibbon Hospital - Missouri - https://www.fitzgibbon.org/
- Tree
http://[redacted].onion/fileslist.zip
- Meditech table LabRequisitionDetails.csv.zip
http://[redacted].onion/LabRequisitionDetails.csv.zip
- Meditech table BarInsurances.csv.zip
http://[redacted].onion/BarInsurances.csv.zip
- Table MmStockReqs.csv.zip
http://[redacted].onion/MmStockReqs.csv.zip
- "Converted to PDF" directory
http://[redacted].onion/Converted_to_PDF/
- Directory "Cancer Center Forms / SCANNED DOCUMENTS /" (PII PHI)
http://[redacted].onion/SCANNED_DOCUMENTS.zip
- Full leak
http://[redacted].onion/ffiles/fitz/

```