the redsense advantage

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)