PATIENT DIES AFTER CYBERATTACK ON GERMAN HOSPITAL

Executive Summary

A German citizen has died as a result of to a ransomware attack on a German hospital. Duesseldorf University Clinic has been under a ransomware attack for approximately one week which has limited its ability to provide medical care. The patient was not able to get care at the clinic and had to be re-routed to another clinic but passed away before she could receive proper treatment. The attackers are thought to have gained network access through a vulnerable VPN device. Similar VPN devices are common among healthcare and other industry verticals.

Analysis

Düsseldorf University Clinic was targeted by a ransomware attack that occurred on September 10, 2020, the attack encrypted 30 of the clinic's servers, the clinic began to triage and relocate patients to other healthcare facilities. The attack locked clinicians out of critical data necessitating operations be postponed and emergency patients be relocated to other sites. The clinic claims that the attack exploited a vulnerability in "widely used commercial add-on software." One German news source (Heise Online) reported that the hackers likely exploited an arbitrary code execution vulnerability in a Citrix VPN device (CVE-2019-19781) and claims the attackers had access for months prior to the attack. Reports state that no data was permanently destroyed, as some ransomware operators will do to increase the pressure on the victim organization to pay the ransom. The ransomware operators neglected to specify the ransom payment amount for the encryption key, which is standard practice. It's unknown if the attackers targeted the clinic specifically, or were targeting the University. The ransomware may have been self-propagating and spread on its own to the clinic. Once the attackers were notified that the ransomware impacted an operational healthcare organization, the attackers provided the decryption key for free and there was no further communication. German prosecutors are considering negligent manslaughter charges.

Assessment

Due to the failure to communicate payment instructions and their actions after being notified that their ransomware impacted a hospital, HC3 assesses that the ransomware operators are likely amateurs and the clinic was not attacked by any major threat actors. The vulnerability in the Citrix VPN was initially made public On December 17, 2019 along with mitigation actions as well as a permanent patch on January 24, 2020. HC3 issued a white paper on this vulnerability.

References

Police launch homicide inquiry after German hospital hack
https://www.bbc.com/news/technology-54204356

Cyber attack on Düsseldorf University Hospital (German language)
https://www.heise.de/news/Cyber-Angriff-auf-Uniklinik-Duesseldorf-Shitrix-schlug-zu-4904979.html

HC3 White Paper: APT41 Citrix and Zoho Attacks on Healthcare
https://www.hhs.gov/sites/default/files/apt41-citrix-and-zoho-attacks-on-healthcare.pdf