Attacks/Breaches | 1 MIN READ QUICK HITS

Ransomware Barrage Aimed at US Healthcare Sector, Feds Warn

A CISA advisory warns that the Daixin Team ransomware group has put the US healthcare system in its crosshairs for data extortion, and provides tools to fight back.

Dark Reading Staff
Dark Reading

October 24, 2022

Source: JAM via Alamy

Daixin Team has actively targeted the US Healthcare and Public Health (HPH) sector since last June, according to a joint advisory issued by the FBI, Cybersecurity and Infrastructure Agency (CISA), and the Department of Health and Human Services (HHS), which provides indicators of compromise (IoCs) and tactics techniques and procedures (TTPs).

Third-party investigations revealed that the Daixin Team ransomware is based on Babuk Locker source code, targets VMware EXSi servers and encrypts files, the advisory said.

Officials believe the Daixin Team uses phishing campaigns to steal VPN credentials, and exploits.

"Daixin actors gain initial access to victims through virtual private network (VPN) servers. In one confirmed compromise, the actors likely exploited an unpatched vulnerability in the organization's VPN server," the advisory explained. "In another confirmed compromise, the actors used previously compromised credentials to access a legacy VPN server that did not have multifactor authentication (MFA) enabled."

The FBI reported that as of October, the HPH sector makes up a full 25% of ransomware complaints filed to its Internet Crime Complaint Center, and accounted for the most overall ransomware reports during 2021.

Vulnerabilities/Threats Threat Intelligence