Published on *The National Law Review* https://natlawreview.com

Joint Advisory Outlines Attacks by Daixin Team

Article By:

Linn F. Freedman

The Cybersecurity & Infrastructure Security Agency, the FBI and the U.S. Department of Health & Human Services released a Joint Advisory last week warning organizations, particularly those in the health care and public health (HPH) sectors, of the ransomware and data extortion operations by the Daixin Team.

The Advisory is designed to provide information to organizations to help prevent ransomware attacks. According to the Advisory:

The Daixin Team is a ransomware and data extortion group that has targeted the HPH Sector with ransomware and data extortion operations since at least June 2022. Since then, Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations where they have:

- Deployed ransomware to encrypt servers responsible for healthcare services—including electronic health records services, diagnostics services, imaging services, and intranet services, and/or
- Exfiltrated personal identifiable information (PII) and patient health information (PHI) and threatened to release the information if a ransom is not paid.

The criminals gain access to victim's systems through virtual private network servers by exploiting unpatched vulnerabilities or using previously-compromised credentials (obtained with phishing emails) to access VPN servers that do not have multifactor authentication enabled. The Advisory lists the indicators of compromise and mitigation steps that organizations can take to protect against Daixin. If your organization is included in the HPH sectors, prompt attention to the Advisory is warranted.

National Law Review, Volumess XII, Number 307