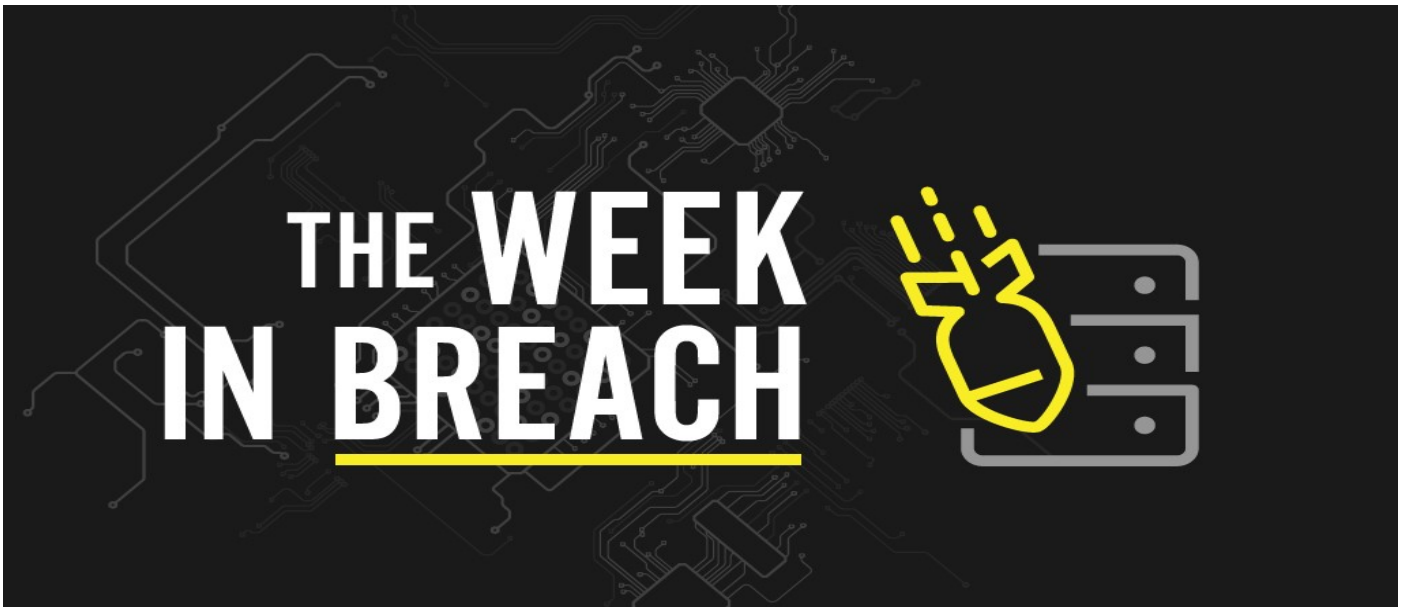
THE WEEK IN BREACH NEWS: 02/24/21 – 03/02/21

DenBe Computer Consulting
Connecting Business

March 3, 2021 by Dennis Jock

This Week in Breach News:

Steris gets caught up in a third-party data breach.



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within

Steris

https://www.infosecurity-magazine.com/news/steris-touted-as-latest-accellion/

Exploit: Third Party Data Breach

Steris: Medical Equipment Sales

Risk to Business: 1.919 = Severe

The ransomware gang Clop is claiming to have snatched an unspecified amount of information belonging to the Steris Corporation during a ransomware attack at third party cloud solutions provider Accellion. A small amount of internal data including studies and communications was identified as Steris data.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Third party threats are growing more serious as cybercriminals collect information used in past breaches to fuel future attacks.

Gab

https://www.hackread.com/gab-hacked-ddosecrets-leak-profiles-posts-dms-passwords-online/

Exploit: Hacking

Gab: Social Media Platform

Risk to Business: 1.479 = Extreme

Right wing social media platform Gab was hacked by hacktivist group DDoSecrets. The platform is notorious for lax censorship of hate speech and is a haven for extremists including white supremacists, neo-Nazis, white nationalists, the alt-right, and QAnon conspiracy theorists. DDosSecrets has posted 70 GB of Gab content to its website including public posts, private posts, user profiles, hashed passwords for users, DMs, and plaintext passwords for groups in SQL format, along with over 70,000 messages in more than 19,000 chats with over 15,000 users in plaintext format.

Individual Risk: 1.447 = Extreme

It is unclear how many individuals may have been impacted. Gab users should be wary of spear phishing attempts, as well as potential legal consequences for nationalist or hate group activity.

Customers Impacted: Unknown

How it Could Affect Your Business: Hacktivists are growing bolder in their quest to expose hate in public and private spaces. Information like this will haunt users for years on the dark web.

Covenant Healthcare

https://www.wnem.com/news/covenant-healthcare-reports-data-breach-through-employee-emails/article_eaf988fc-76c8-11eb-99f1-cbedd3811c29.html

Exploit: Phishing

Covenant Healthcare: Medical System

Risk to Business: 2.212 = Severe

Bad actors obtained access to two employee email accounts at Covenant Healthcare, leading to the exposure of personal information for an estimated 45K patients. The Michigan-based health system is undertaking an investigation with outside cybersecurity professionals.

Individual Risk: 1.712 = Severe

Potentially stolen patient information includes includes names, addresses, dates of birth, Social Security numbers, driver's license numbers, medical diagnosis and clinical information, medical treatment, prescription information, doctors' names, medical record numbers, patient account numbers, and medical insurance information. The hospital is offering identity theft protection to impacted patients.

Customers Impacted: 45k

How it Could Affect Your Business: Phishing is the gateway to dangerous cybercrime, and regular phishing resistance training helps keep that gate closed.