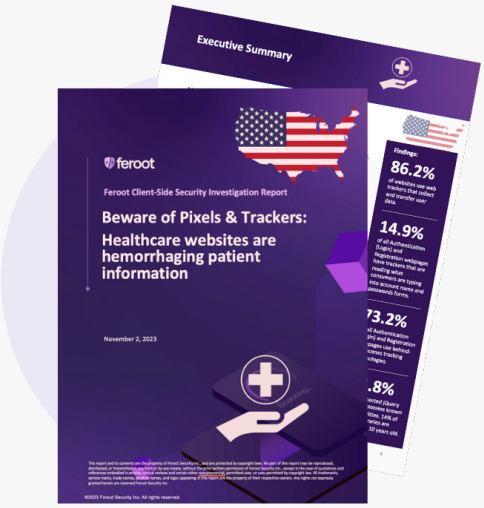
Feroot Security Investigation Reveals Wide-spread Patient Data Exposures on U.S. Healthcare Websites

Feroot Security Investigation Finds 86% of Healthcare Websites Share Data with Web Tracking and Surveillance Tools Without Explicit and Informed Consent.



Feroot Investigation Report of Healthcare Websites Hemorrhaging Patient Information

TORONTO, ON, CANADA, November 1, 2023 /EINPresswire.com/ -- Feroot Security, a cyber security company for the client-side of business websites and web applications, released today a report titled "Beware of Pixels & Trackers: Healthcare websites are hemorrhaging patient information." This report details how numerous medical-related websites might be sharing patient information with major tech corporations, potentially violating patients' privacy rights.

Key findings in this report offer insights for cybersecurity, compliance and privacy executives at healthcare organizations as well as for policymakers, and auditors:

-- 86% of the healthcare and telehealth websites analyzed were found collecting data without user consent.
-- 73% of all authentication (Login) and Registration web pages expose private authentication and health information to web trackers and pixels.
-- 14.9% of all authentication (Login) and Registration web pages have trackers that are reading what consumers are typing into account name, password and other other forms that collect information such as Social Security Numbers, names, addresses, appointment schedules, billing information, and medical diagnoses.

Feroot's investigation found the use of third-party surveillance tools and technologies owned by companies controlled by the jurisdiction of China and Russia, on over 4% of healthcare websites, which highlights serious security, privacy and confidentiality concerns.

The research assessed 33,408 unique healthcare web pages across 1,515 distinct healthcare websites and portals, involving 530 different healthcare providers.

210 unique web tracking tools were discovered by the research. These tools are linked to 155 unique tech corporations including Alphabet Inc.'s Google, Microsoft, Meta's Facebook, and ByteDance, the parent company of TikTok. Web trackers and pixels are a form of visitor surveillance tools on websites to monitor user behaviors and relay collected data back to their parent tech companies for website analytics and ad campaigns. Collected data can also be sent internationally; the research identified this happening in a number of cases with data sent to locations in 26 countries.

Tracking tools on user-authenticated and unauthenticated web pages can access personal health information (PHI) such as IP addresses, medical record numbers, home or email addresses, appointment dates, or other info provided by users on pages and thus can violate HIPAA Rules that govern the Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates.

Healthcare organizations must adhere to guidelines set by bodies like the HHS and the FTC, which focus on the importance of patient data in the digital realm or run the risk of serious fines or potentially more stringent punishment.

For more information about the 2023 Feroot Client-Side Security Report - Beware of Pixels & Trackers on U.S. Healthcare Websites and its findings, download it here.

About Feroot Security:
Feroot Security believes customers should be able to do business securely with any company online, without risk or compromise. Feroot secures client-side web applications so businesses can deliver flawless digital user experiences to their customers. Leading brands trust Feroot to protect their client-side attack surface. To learn more, visit www.feroot.com.

For additional details or inquiries, please reach out to:
Feroot Security Inc.
press@feroot.com

Ivan Tsarynny
Feroot Security Inc
+1 647-299-0956
email us here
Visit us on social media:

Twitter
LinkedIn
