FBI CYBER DIVISION

Private Industry Notification

8 April 2014

PIN #: 140408-009

(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain

(U) Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.

(U) The deadline to transition to EHR is January 2015, which will create an influx of new EHR coupled with more medical devices being connected to the Internet, generating a rich new environment for cyber criminals to exploit. According to open source reporting from SANS, Ponemon, and EMC²/RSA, the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.

- (U) A SANS report dated February 2014, indicates health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property. Data analysis revealed multiple devices (e.g., radiology imaging software, digital video systems, faxes, printers) and security application systems (e.g., Virtual Private Networks (VPN), firewalls, and routers) were compromised. Once medical devices are compromised, malicious traffic is transmitted through VPNs and firewalls. The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

- (U) According to a Ponemon Institute report dated March 2013, 63% of the health care organizations surveyed reported a data breach in the past two years with an average monetary loss of $2.4 million per data breach. The majority of each data breach resulted in the theft of information assets. Lastly, 45% reported that their organizations have not implemented security measures to protect patient information.

- (U) An EMC²/RSA White Paper published in 2013 indicated that in the first half of 2013, over two million health care records were compromised, which was 31% of all reported data breaches. Cyber criminals are selling the information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

(U) Reporting Notice

(U) The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI field office. The FBI's 24/7 Strategic Information and Operations Center can be reached by telephone at 202-323-3300 or by e-mail at SIOC@ic.fbi.gov. FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Notes: Law Enforcement Response

(U) Information contained in this product is UNCLASSIFIED. There is no additional information available on this topic.

(U) For comments or questions related to the content or dissemination of this document, please reference CYD-CC-1674.