McAfee Labs: Liquidity Trumps Longevity in Market for Stolen Medical Records
Wednesday, October 26, 2016 04:01:00 AM (GMT)

Report Reveals Consequences of Failing to Appreciate "Second Economy" Dynamics of Cybersecurity; Medical Records Fail to Eclipse Market Value of Stolen Financial Data and Pharmaceutical, Biotech Data

NEWS HIGHLIGHTS

- McAfee Labs finds stolen medical records available for sale from $0.03 to $2.42 per record
- Comparable stolen financial account records available for $14.00 to $25.00
- Credit and debit card account data available for $4.00 to $5.00 per account record
- Most lucrative cybercrime targeting health care industry data is pharmaceutical, biotech intellectual property
- Cybercrime-as-a-service economy is developing specifically around health care industry data
- Concerted effort by cybercriminals to recruit health care industry insiders as accomplices

Intel® Security today released its ***McAfee Labs Health Warning*** report, which assesses the marketplace for stolen medical records; compares it with the marketplace for stolen financial services data; identifies health care focused cybercrime-as-a-service trends; and profiles cybercrime targeting intellectual property in the pharmaceutical and biotechnology industries. The Intel Security research asserts that the development of the market for stolen data and related hacking skills indicate that the "business of cybercrime" in the health care sector is growing.

"In an industry in which the personal is paramount, the loss of trust could be catastrophic to its progress and prospects for success," said Raj Samani, Intel Security's CTO for Europe, the Middle East, and Africa. "Given the growing threat to the industry, breach costs ought to be evaluated in the Second Economy terms of time, money, and trust—where lost trust can inflict as much damage upon individuals and organizations as lost funds."

The Value of Stolen Data

Intel Security found that the price per record for stolen patient medical records remains lower than financial account records and retail payment account information, despite the increasingly time-sensitive, or perishable, nature of data such as credit and debit card numbers.

In recent years, Intel Security has observed the cybercriminal community extend its data theft efforts beyond financial account data to medical records. Although credit and debit card numbers can be canceled and replaced quickly, this is not the case for protected health information (PHI) that does not change. This "nonperishable" PHI could include family names, mothers' maiden names, social security or pension numbers, payment card and insurance data, and patient address histories. But, though this dynamic has led to industry speculation that the price per medical record could soon rise to rival or even eclipse that of financial account or payment card data, Intel Security's 2016 research did not illustrate such price-point movement.

Intel Security's research found the average health record price point to be greater than that of basic personally identifiable information, but still less than that of personal financial account data. The per record value of financial account data ranged from $14.00 to $25.00 per record, credit and debit cards drew around $4.00 to $5.00, but medical account data earned only from $0.03 to $2.42. The findings suggest financial account data continues to be easier to monetize than personal medical data, which could require an investment that financial payment data does not require. Upon stealing a cache of medical records, it is likely cybercriminals must analyze the data, and perhaps cross-reference it with data from other sources before lucrative fraud, theft, extortion, or blackmail opportunities can be identified. Financial data, therefore, still presents a faster, more attractive return-on-investment (ROI) opportunity for cybercriminals.

“Liquidity trumps longevity in the race to monetize stolen data,” said Raj Samani, Intel Security’s CTO for Europe, the Middle East, and Africa. “If I steal a million credit or debit card numbers, I can quickly sell this digital merchandise before banks and retailers discover the theft and cancel these numbers. Alternatively, a million medical records contain a rich cache of permanent PHI and personal histories, but such data requires a greater investment of time and resources to exploit and monetize it.”

Theft of Intellectual Property and Business Confidential Data

Intel Security’s research also investigated the targeting of biotechnology and pharmaceutical firms for their intellectual property and business confidential information. The researchers suggest that the economic value of such information is considerably higher than the cents-per-record data Intel Security’s researchers identified within patients’ health care accounts.

Intel Security researchers found evidence that formulas for next-generation drugs, drug trial results, and other business confidential information constitutes significant value. The stores of such data at biopharmaceutical companies, their partners, and even government regulators who are involved in bringing new drugs to market have become a premium target of cybercriminals.

“Corporate espionage has gone digital along with so many other things in our world,” Samani said. “When you consider that research and development is a tremendous expense for these industries, it should be no surprise that cybercriminals are attracted to the ROI of this category of health care data theft.”

The Economics of Cybercrime-as-a-Service

Intel Security also identified cybercriminals leveraging the cybercrime-as-a-service market to execute their attacks on health care organizations. Researchers found evidence of the purchase and rental of exploits and exploit kits to enable the system compromises behind health care data breaches. In one case, a relatively non–technically proficient cyber thief purchased tools to exploit a vulnerable organization, leveraged free technical support to orchestrate his attack, and then extracted more than 1,000 medical records that the service provider said could net him about $15,564.

The researchers also observed brazen efforts by cybercriminals, through online ads and social media, to recruit into their ranks health care industry insiders with access to valuable information.

“When a well-developed community of cybercriminals targets a less prepared industry such as health care, organizations within that industry tend to play catch-up to protect against yesterday’s threats, and not those of today or tomorrow,” Samani continued. “Gaining the upper hand in cybersecurity requires a rejection of conventional paradigms in favor of radical new thinking. Where health care organizations have relied on old playbooks, they must be newly unpredictable. Where they have hoarded information, industry players must become more collaborative. Where they have undervalued cyber defense overall, they must prioritize it. In the Second Economy, if you win the ‘time’ contest with attackers, you are in a position to preserve money and trust.”

For more information, read the full report: *Health Warning*.

For information on how stolen medical records might be exploited by cybercriminals, please see the “*The Weaponization of Political Candidates’ Medical Records*” blog.

For guidance on how organizations can refocus their security strategies to better protect their enterprise from the threats detailed in this report, please see: *A Second Economy Prognosis for Health Care Cybersecurity*.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique McAfee Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. The mission of Intel Security is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

No computer system can be absolutely secure.

View source version on businesswire.com: http://www.businesswire.com/news/home/20161025006879/en/

--30-- JPE/SF

Contact:

For Intel Security
RH Strategic
Sarah Horowitz, 202-379-0546
shorowitz@rhstrategic.com

Industries: Technology, Data Management, Software, Security, Health, Biotechnology, Pharmaceutical
Languages: English
Primary Identifiers: INTC-US
Related Identifiers: INTC-US, US458140100
Source: Intel Security
Subjects: Survey, Product/Service