

A informação da sua ficha médica vale 10 vezes mais no mercado negro do que o número do seu cartão de crédito.

É isso mesmo!

O alarme soou no mês passado em um alerta enviado pelo FBI para que todos os prestadores de serviço de assistência médica nos EUA se protegessem contra ataques cibernéticos.

O alerta veio depois de um dos maiores hospitais no país – o Community Health Systems Inc. – ter informado à polícia que hackers Chineses haviam invadido sua rede de computadores e roubado informações pessoais de 4,5 milhões de pacientes.

A indústria de saúde nos EUA, um gigante de R\$ 7,2 trilhões, virou alvo dos crimes cibernéticos porque muitas empresas ainda dependem de sistemas de computador ultrapassados, dizem os especialistas em segurança da informação.

“Os hospitais possuem sistema de TI com pouca proteção, de modo que fica relativamente fácil para os hackers conseguirem acessar grande quantidade de dados individuais para cometer fraudes médicas”, comentou Dave Kennedy, especialista em segurança de sistemas de saúde e CEO da TrustedSEC L.L.C..

Através de entrevistas com executivos do setor, investigadores de crimes cibernéticos e especialistas em fraude foram capazes de mapear em detalhes um verdadeiro mercado que funciona no submundo dos dados roubados de pacientes.

Os dados a venda incluem nomes de pacientes, datas de nascimento, números de apólice de seguro saúde, códigos de diagnóstico e informações sobre faturamento.

Os fraudadores usam esses dados para criar identidades falsas através das quais compram equipamentos médicos ou remédios que possam ser revendidos. Ou então, combinam um nº de paciente verdadeiro com um nº falso de prestador de serviços e inventam pedidos de reembolso que submetem às operadoras de seguro-saúde.

O uso de dados médicos roubados dos prontuários não é imediatamente identificado pelos pacientes ou por seus prestadores de serviço, rendem aos criminosos anos de uso dessas informações em suas fraudes.

Isso torna os dados médicos roubados mais valiosos do que o furto de números de cartões de crédito, já que estes tendem a ser rapidamente cancelados pelos bancos que detectam a fraude logo nas primeiras compras irregulares.

Don Jackson, Director de Inteligência na PhishLabs, uma companhia de proteção contra crimes cibernéticos, monitorou o submundo no qual os hackers vendem esse tipo de informação. Descobriu que os dados médicos roubados podem valer R\$ 24 cada um, cerca de 10 a 20 vezes mais do que o nº de um cartão de crédito americano.

Aumentam os ataques

A quantidade de organizações do setor de assistência médica que reportou ter sido vítima de um ataque cibernético aumentou nada menos do que 40% em 2013, comparado a um crescimento de 20% em 2009, informa a pesquisa anual do Ponemon Institute um instituto formador de opinião em políticas de proteção aos dados.

O fundador do instituto, Larry Ponemon possui vasto conhecimento dos casos de ataque a operadoras de assistência médica que nunca vieram a público. Segundo ele, em 2014 aumentou não apenas a quantidade de ataques cibernéticos, mas também o número de dados roubados.

O aumento desses crimes tem sido alimentado pela digitalização cada vez maior dos prontuários médicos, um movimento que vem sendo adotado pela maioria dos prestadores de serviços nos EUA.

Os prestadores de serviço de assistência médica e as operadoras de seguro saúde são obrigados por lei a divulgar publicamente as violações de seus bancos de dados quando essas tenham afetado mais de 500 pessoas, mas não há leis que as obriguem a processar os criminosos.

Por isso é difícil saber qual o custo total dos crimes cibernéticos no sistema de saúde.

Especialistas do setor de seguros dizem que essa é mais uma das diversas despesas repassadas aos consumidores como parte do aumento exponencial dos prêmios de seguro saúde.

Algumas vezes os consumidores só descobrem que seus dados foram roubados após os fraudadores usarem o nº de seu plano de saúde, se passando por eles para obter cobertura de saúde. Quando as contas vencidas e não pagas são enviadas para as empresas de cobrança, essas vão tentar obter o pagamento das vítimas das fraudes.

Um paciente descobriu, no ano passado, que seu prontuário médico mantido por uma grande rede de hospitais havia sido violado, quando começou a receber avisos de cobrança por um procedimento cardíaco ao qual ele nunca havia se submetido.

Os dados desse paciente também haviam sido usados para comprar uma scooter e diversos equipamentos médicos, um roubo que totalizou dezenas de milhares de reais.

Fraude Médica

Hospitais e prestadores de serviço privados são apenas alguns dos alvos fáceis para as fraudes. O próprio governo vem desenvolvendo esforços para combater as fraudes no sistema público de saúde, focando os esquemas tradicionais de superfaturamento.

Em 2012 e 2013 as fraudes envolvendo o sistema público de saúde chegaram a R\$ 14,4 bilhões, conforme mostra o banco de dados mantido pela Medical Identity Fraud Alliance.

“Conversando com alguns hospitais e com pessoas do setor, constatei que eles estão usando velhos sistemas de informação — Plataformas Windows com mais de 10 anos de idade, sem terem recebido nem mesmo um remendo”, comentou Jeff Horne, Vice Presidente da firma de segurança cibernética Accuvant.

Nas palavras do Sócio da KPMG, Michael Ebert, segurança cibernética não tem disso contemplada no orçamento de muitos prestadores de serviços de saúde, não é prioridade criptografar os dados eletrônicos dos prontuários médicos dos pacientes.

Sendo Diretor de um hospital, “você vai investir em um novíssimo equipamento de Imagem de Ressonância Magnética – MRI ou vai colocar dinheiro em um novo sistema de firewall?” disse ele.

Há alguns meses comecei a chamar a atenção para os imensos danos que os crimes cibernéticos estão causando nos EUA.

Precisamos colocar esse assunto em discussão para proteger clientes de planos de saúde e claro, de planos de previdência complementar aqui no Brasil.

Grande abraço.

Eder.

Adaptado do artigo “Your medical record is worth more to hackers than your credit card”, escrito por Caroline Humer e Jim Finkle.

Fonte: [Blog do Eder](#), em 09.10.2014.