A Raytheon|Websense anunciou a divulgação do Relatório e Análise de Saúde em 2015, desenvolvido pelo Websense Security Labs™ e que avalia o cenário atual das ciberameaças e dos ataques direcionados contra o setor de saúde para roubo de dados médicos. O relatório mostra que o setor de saúde sofre muitos ataques e está cada vez mais vulnerável, especialmente com a próxima onda de dispositivos conectados chegando a um ambiente tecnológico que já apresenta um alto nível de complexidade.

"A rápida digitalização no setor de saúde, em conjunto com o valor das informações médicas, motivou um grande aumento no número de ataques direcionados contra o setor", disse Carl Leonard, principal analista de segurança da Raytheon|Websense. "Os setores financeiro e de varejo já aprimoraram suas defesas virtuais, mas nossas pesquisas revelam que as organizações de saúde precisam rapidamente adaptar seus sistemas de segurança para enfrentar os desafios inerentes da economia digital – antes de se tornarem a principal fonte para o roubo de informações pessoais".

Em 2014, a Raytheon|Websense descobriu que o número de ataques virtuais contra hospitais aumentou 600% em um período de 10 meses. Em seguimento a tal descoberta, o Websense Security Labs recentemente reexaminou a telemetria de ataques contra o setor de saúde, descobrindo uma nova inteligência nas ferramentas de ciberataques mais produtivas e eficazes, além das técnicas e tendências de segurança que impactam o setor.

Os destaques do Relatório de Análise do Setor de Saúde 2015 do Websense Security Labs incluem:

- O número de ataques e incidentes de segurança na a indústria de saúde é 340% maior que a média e, por esse motivo, é o alvo mais provável para o roubo de dados pessoais; as informações médicas são 10 vezes mais valiosas no mercado negro, aumentando a possibilidade do setor ser alvo dos hackers. A proliferação de registros médicos eletrônicos criou um ambiente de dados pesado, enquanto as redes criadas pelos milhares de prestadores de serviços de saúde representam uma enorme superfície para ataques.

- Um em cada 600 ataques no setor de saúde envolve malware avançado. A probabilidade da indústria de saúde ser atingida por malware avançado é quatro vezes maior que qualquer outro setor. Muitas empresas do setor não possuem a capacidade de investimento ou as habilidades administrativas, técnicas ou organizacionais necessárias para detectar, mitigar e prevenir ataques virtuais, e o malware avançado representa uma ameaça significativa para a infraestrutura de saúde.

- A probabilidade do setor de saúde enfrentar esquemas de phishing é 74% maior. A falta de treinamentos e programas de conscientização relativos à segurança de TI aos funcionários agrava o perigo dos ataques de phishing, resultando em mais incidentes de segurança.

- O setor de saúde é 4,5 vezes mais propenso a sofrer ataques do ransomware Cryptowall e três vezes mais do malware Dyre. Inicialmente usado para atacar o setor financeiro e roubar centenas de milhões de dólares, novas capacidades de exploração tornam o malware Dyre uma grande ameaça para o roubo de dados de organizações de saúde do mundo inteiro, enquanto o Cryptowall encripta e armazena como reféns dados críticos de saúde com o objetivo de resgate.

O relatório também examina os desafios envolvidos na criação de uma estratégia global de TI para o setor de saúde, com considerações regionais, bem como o possível impacto de segurança com os dispositivos conectados aos sistemas de pacientes.

Fonte: Risk Report, em 15.10.2015.