14/03/2016 - Symantec identifica milhões de e-mails de spam diários contaminados com o Trojan financeiro Dridex

Construído para captar dados bancários das vítimas, o Dridex é um dos malwares mais perigosos em circulação atualmente

O Trojan Dridex surgiu como uma das ameaças mais perigosas às instituições financeiras em 2015. O número de infecções detectadas pela Symantec subiu de maneira significativa ao longo do ano. Entre janeiro e abril, havia menos de 2 mil infecções por mês, número que atingiu quase 16 mil em junho, antes de cair e se estabilizar entre 3 mil e 5 mil por mês no último
trimestre.

As campanhas de spams espalhando Dridex (detectado pela Symantec como W32.Cridex) às vezes pode sobrecarregar as organizações atingidas por elas. Em análises recentes dessas campanhas, a Symantec descobriu que a operação do malware continua se dando em grande escala, com milhões de novos e-mails enviados diariamente. Os hackers por trás do Dridex são disciplinados e arrojados: operam em uma semana de trabalho normal, aperfeiçoando continuamente o malware, e fazem um esforço significativo para camuflar suas campanhas de spam como se fossem e-mails legítimos.

Pelo menos 145 campanhas de spam Dridex foram observadas durante um período de 10 semanas. O número de e-mails bloqueados pela Symantec por campanha foi de mais de 270 mil, o que indica que o número total de malwares espalhados a cada dia atinja a casa dos milhões. Cerca de 75% dessas campanhas usaram □□ nomes de empresas reais no endereço do remetente e, frequentemente, no texto de e-mail. A grande maioria estava disfarçada de e-mails financeiros, como faturas, recibos e ordens de pagamento.

O Dridex está focado, principalmente, em clientes de instituições financeiras de países ricos que falam inglês, como os Estados Unidos, Reino Unido e Austrália. Mas já foram detectados ataques também em países de língua não inglesa na Europa e na região da Ásia-Pacífico. O malware é configurado para atingir clientes de cerca de 300 diferentes organizações em mais de 40 regiões.

Você encontra mais detalhes sobre esses ataques no Blog Post e também no Whitepaper da Symantec. Caso queira falar com um especialista em segurança da Symantec, por favor, entre em contato com a Market21 Comunicação.