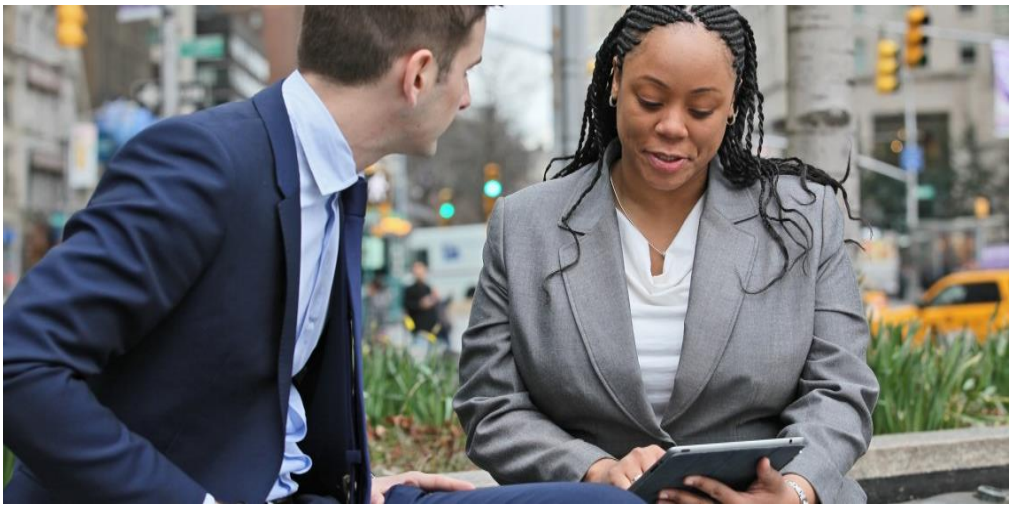
Vazamento de dados expõe 56 milhões de cartões de crédito

Cyber Essentials

3ª edição
Setembro 2014



Uma empresa norte-americana do ramo de produtos para casa e construção confirmou recentemente uma suspeita de fraude que levou ao vazamento de 56 milhões de cartões de crédito e débito de seus clientes dos Estados Unidos e Canadá. A quantidade é superior à de outro caso de ampla repercussão que envolveu uma grande empresa de varejo e no qual 40 milhões de números de cartões foram expostos.

Segundo as investigações, uma grande quantidade de dados de cartões bancários foi colocada à venda por meio do mesmo site que ofereceu informações sobre cartões de crédito no caso anterior.

O vazamento causou prejuízo de US$ 62 milhões, e essa cifra pode aumentar no quarto

As análises sugerem que a técnica utilizada na fraude mais recente é uma possível variante do *malware* empregado no ataque anterior, reforçando a possível ligação entre os casos.

A empresa vai intensificar a implementação de *chips* e tecnologia PIN em suas lojas nos Estados Unidos até o fim deste ano. Atualmente, *chips* em cartões de crédito não são amplamente usados nos EUA , ao contrário do que ocorre no Canadá.

pwc

Incidência do *malware* do tipo *"backoff"*

Os recentes casos de fraudes direcionados para esse setor elevam a preocupação com o *malware* conhecido como *"backoff"*, que infecta sistemas em pontos de venda (PDV). De acordo com as autoridades norte-americanas, essa ameaça já afetou mais de mil empresas nos Estados Unidos.

As organizações precisam se preparar para combater ataques direcionados

Ameaças avançadas (APT)

Casos como esses e o vazamento de informações em bancos norte-americanos de grande porte revelam que as organizações têm dificuldade de se preparar para lidar com ameaças avançadas (APTs) e de detectar e responder aos incidentes de maneira tempestiva. As investigações apontam que as ações realizadas pelos criminosos duraram meses até serem descobertas.

Como se proteger?

A prevenção exige um conjunto de ações, que inclui a conscientização das pessoas, a adoção de controles tecnológicos, um modelo de resposta a incidentes que contemple a prevenção a APTs e uma estratégia de segurança cibernética para garantir mais resiliência em caso de ataques.

Nossos contatos

Cyber & Information Security
PwC Brasil

Edgar D´Andrea
Sócio líder
edgar.dandrea@br.pwc.com

Eduardo Batista
Diretor
eduardo.batista@br.pwc.com

Fernando Mitre
Gerente sênior
fernando.mitre@br.pwc.com

Magnus Santos
Gerente
magnus.santos@br.pwc.com

Maressa Juricic
Gerente
maressa.juricic@br.pwc.com

PwC Brasil @PwCBrasil youtube.com/PwC PwC Brasil