Mercado Digital

folhainfo@folhadelondrina.com.br

Credenciais são principais alvos de cibercriminosos

Mie Francine Chiba
Reportagem Local

De junho de 2018 a maio de 2019, 85% dos vazamentos detectados por empresa de inteligência cibernética oram dados como CPF, e-mail e senha de acesso a serviços

Cerca de 85% dos vazamentos detectados em um monitoramento realizado pela empresa NS Prevention, do Grupo New Space, de junho de 2018 a maio de 2019 eram dados de credenciais – CPF e e-mail ou e-mail e senha. Outros 15% eram dados de cartões de crédito. No total, o monitoramento chegou a mais de 2 bilhões de credenciais e 370 milhões de dados de cartões vazados e comercializados em canais da internet como IRC (Internet Relay Chat), sites de compartilhamento, Skype e Telegram. Os dados estão no 4º Relatório Anual de Riscos e Fraudes no Cenário Cibernético.

Os segmentos mais afetados são o de turismo e hotelaria (51%) e redes sociais (40%). No monitoramento feito em uma única empresa, a empresa identificou quase 2,5 mil tentativas de ataque no período da pesquisa.

Credenciais são o principal alvo dos cibercriminosos porque apresentam um grande potencial. Com dados como e-mail, CPF e senha, os criminosos podem ter acesso a uma série de serviços, como meios de pagamento, plataformas onde já ficam cadastrados dados de cartões de crédito do usuário. Com o acesso a esse tipo de serviço, os criminosos podem realizar compras facilmente.

Além disso, 70% da população mundial usa a mesma senha para mais de um serviço, afirma Bordini. Um prato cheio para o cibercriminoso. "Com uma senha ele consegue ter acesso a outros sites." Mesmo se o usuário não guarda os dados do cartão de crédito nos sites e serviços, seus dados pessoais podem ser comercializados pelos cibercriminosos.

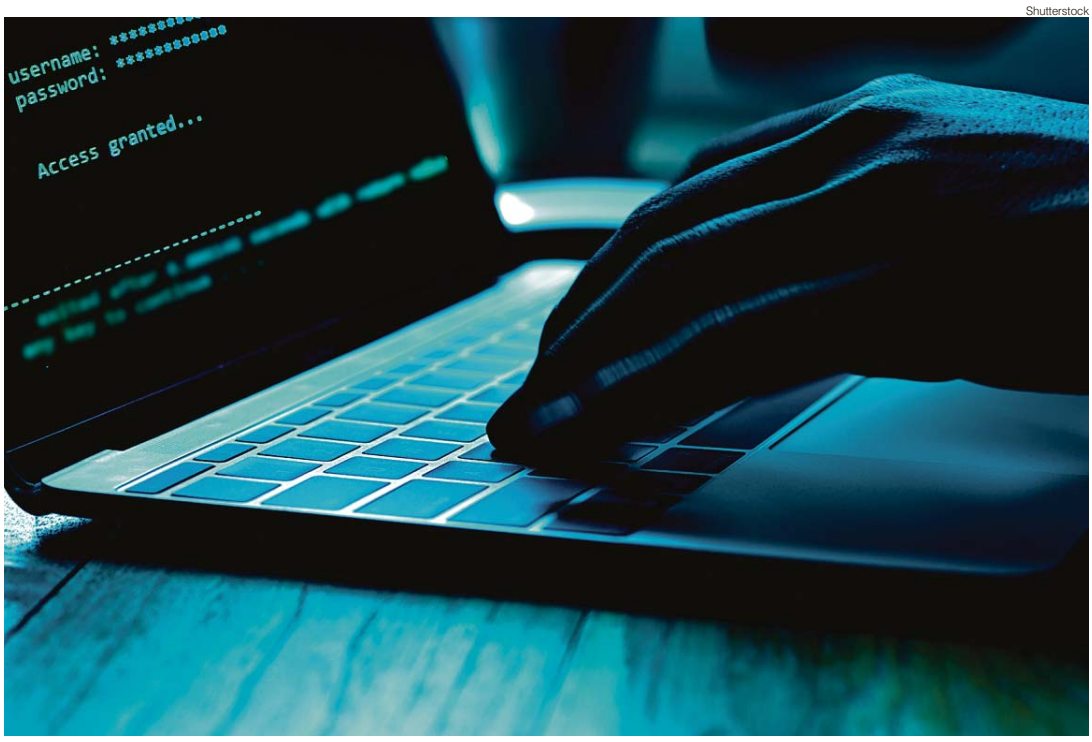
Na visão de Thiago Bordini, diretor de inteligência cibernética do Grupo New Space, o grande volume de credenciais vazados reflete a falta de investimento das empresas em monitoramento de incidentes e medidas preventivas e a falta de mão de obra especializada para atuar nas organizações. Mas também mostra o descuido dos usuários em relação aos seus próprios dados.

Com dados como e-mail, CPF e senha, os criminosos podem ter acesso a uma série de serviços

Um dos métodos de ataque mais utilizados pelos cibercriminosos, segundo a NS Prevention, é o spoofing, um tipo de ataque no qual um hacker se passa por outro aparelho ou usuário de uma rede com o objetivo de roubar dados, disseminar malware ou contornar controles de acesso. O bom e velho phishing, e-mails ou mensagens falsos que induzem o usuário a revelar informações pessoais, é outro método de ataque mais utilizado pelos criminosos. Mas invasões cibernéticas também são comuns, explorando falhas nos sites e aplicativos das empresas, afirma o diretor do Grupo New Space.

As invasões atingem empresas que detêm um grande volume de informações. O segmento de turismo e hotelaria, que detinha 51% dos dados coletados pela NS Prevention, é conhecido por práticas inseguras, como pedido de envio de dados do cartão de crédito por e-mail para reservas, afirma Bordini. As redes sociais, responsáveis por 40% dos dados vazados, são um alvo importante porque suas credenciais podem ser utilizadas para acesso a outros tipos de serviços.

Na sua visão, com a entrada em vigor da LGPD (Lei Geral de Proteção de Dados), em 2020, deverá fazer com que as empresas intensifiquem as medidas para evitar vazamentos de dados, já que a Lei obrigará as companhias a reportarem vazamentos e a pagarem multas. Do lado do usuário, algumas das recomendações do diretor é usar senhas fortes ou usar serviços de gerenciamento de senhas.



Shutterstock

Monitoramento chegou a mais de 2 bilhões de credenciais e 370 milhões de dados de cartões vazados e comercializados em canais da internet

SEGURANÇA

Veja os dados do 4º Relatório Anual de Riscos e Fraudes no Cenário Cibernético

Perda da credibilidade é maior temor das empresas

Para Jeferson D´Addario, CEO do Grupo Daryus, o maior medo das empresas é a perda da credibilidade diante de um vazamento de dados. "O maior medo das empresas grandes não são nem as multas, mas a vergonha, a perda da credibilidade por um acesso e/ou vazamento (de dados)."

O temor pode ser visto na Pesquisa Nacional de Segurança da Informação, realizada pelo Grupo Daryus em parceria com o Grupo New Space. Questionados sobre as principais preocupações das empresas frente a incidentes, 75% indicaram perda ou vazamento de dados. Na sequência, vêm perda financeira e interrupção operacional (65%); e ciberataque (61,4%).

Mesmo assim, cerca de 40% das empresas entrevistadas responderam que ainda não estão preparadas para a LGPD, que entra em vigor em 2020. Apenas 15% responderam que sim e outros 44% informaram ter um planejamento em desenvolvimento. "A lei se aplica a todos que têm dados pessoais armazenados de alguma forma, seja em um caderno ou num banco de dados top de mercado", alerta D´Addario.

Segundo o CEO, a preparação para a Lei deve começar já. "A grande dica é: comece ontem." A preparação, conforme ele, é um trabalho de gestão empresarial, que deve ser feito com suporte de consultoria especializada tanto na área jurídica como de segurança da informação e cibersegurança, que devem fazer uma análise de gap para saber o que a empresa já possui implementado em relação ao que a lei exige e o que não. A partir daí, pode-se traçar o plano de ação e executá-lo. **(M.F.C.)**