GRUPO NEW SPACE
A Visão do Futuro

NS PREVENTION

/ Monetização /

Programas de Fidelização de Cliente

/ Índice /

Este relatório é o primeiro de uma série que aborda as táticas de monetização utilizadas especialmente por cyber criminosos no intuito de detalhar seus modos de agir atuais, em relação a táticas, técnicas, procedimentos e possíveis tendências.

Nesse sentido, é notório como os programas de fidelidade de empresas em diversos segmentos são frequentemente atacados. Para tanto, os cyber criminosos despendem tempo considerável na criação de novas táticas de ataque para rápida monetização desse produto. Neste documento, iremos discorrer sobre nossas pesquisas nessa temática, focando em observações analíticas acerca das novidades empenhadas por esses engenhosos atacantes para, por fim, fomentar ações de prevenção.

1. HISTÓRICO

Buscando compreender os fundamentos dos programas de fidelidade, nos deparamos com uma afirmação que contempla explicação clara e definida da temática abordada. Programa de fidelidade é um "programa de incentivo contínuo oferecido por um varejista para recompensar clientes e encorajar repetição de negócios"[1].

Aprofundando-se em perímetro nacional, uma das empresas pioneiras na implementação de programa de fidelidade no mercado das companhias aéreas, sob o título específico de "programa de milhagens", foi a TAM. Criado em meados de 1993, o TAM Fidelidade veio com a missão de fidelizar os clientes a partir da oferta de vantagens promocionais na compra de passagens aéreas.

[1] Matilda Dorotic, Tammo H. A. Bijmolt, e Peter Verhoef no artigo C. Loyalty Programmes: Current Knowledge and Research Directions. International Journal of Management Reviews, 2012, Vol. 14, pp.217-237. DOI: 10.1111/j.1468-2370.2011.00314.x

Em janeiro de 1994, a companhia aérea Varig também iniciou seu programa de fidelidade, denominado Smiles. Porém, cabe ressaltar que em 2002 a companhia de linhas aéreas GOL adquiriu a Varig e absorveu seus produtos, incluindo também o programa de fidelização.

Até o ano de 2009, o mercado nacional de recompensa por programas de fidelização, aqui tratados até então como programas de milhagens, era restrito ao mercado de companhias aéreas. Deste período em diante, outras companhias em diferentes segmentos aderiram também aos programas.

A prática de fidelização foi ganhando força no mercado, o que ampliou a diversidade dos programas existentes. Dessa forma, cresceram também os ataques cibernéticos, pois a visibilidade do programa e a possibilidade de rápida monetização de baixos valores despertaram a curiosidade e a atração de muitos protagonistas das fraudes digitais. Por meio de pesquisa, identificamos que no período de 2009 a 2012 ocorreu um alto volume de fraudes nos programas de fidelização por milhagem aérea.

A maioria desses ataques cibernéticos foi realizada pelo envio de e-mails com provável propósito de capturar dados legítimos a serem empregados de maneira ilícita, ou seja, para obtenção de vantagens financeiras. Esta técnica é denominada Phishing Scam.

1.1 Phishing Scam

Phishing, também conhecido como phishing scam ou phishing/scam, foi um termo originalmente criado para descrever o tipo de ataque que se dá por meio do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco ou site popular. O e-mail busca induzir a ação do usuário, trazendo um conteúdo similar a um texto corporativo e um link que o direciona para uma página fraudulenta (falsificada), projetada na maioria das vezes para furtar dados pessoais e financeiros.

A palavra phishing (de "fishing") vem de uma analogia criada pelos fraudadores, na qual "iscas" (e-mails) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, estes termos vêm sendo utilizados também para se referir aos seguintes casos:
• Mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
• Mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A partir de 2012, medidas de segurança cibernéticas foram aplicadas nos sites das companhias aéreas, o que mitigou parcialmente os riscos de novos ataques. Adicionalmente, foram realizadas campanhas de conscientização direcionadas para os clientes, ações muito importantes e necessárias na frente de educação contínua. O volume de fraudes em programas de fidelização por intermédio de milhas aéreas reportadamente diminuiu e, com isso, os cyber criminosos direcionaram os ataques para outros modelos e programas de fidelidade, elencados a seguir neste relatório.

2. ANÁLISE SITUACIONAL

Com os obstáculos encontrados para realizar as monetizações em milhas aéreas, os fraudadores cibernéticos começaram a migrar os ataques para outros programas de fidelidade, tais como Multiplus, Dotz e Km de Vantagens. Vamos entender a proposta de cada um:

Multiplus: trata-se de um concentrador de plano de fidelização. Segundo encontrado no site da instituição: "O que é Multiplus? Na Multiplus, você junta em uma única conta os pontos que ganha nos cartões de crédito, com passagens aéreas e em várias empresas e troca por mais passagens aéreas, diárias em hotel, combustível, aparelhos eletrônicos, produtos esportivos e outros milhares de opções e prêmios". Ou seja, suporta a gestão de planos de milhagens, pontuações de cartões de crédito e mais de 300 empresas associadas.

Dotz: tem por objetivo criar uma moeda virtual que poderá ser utilizada em compras em vasta rede de parceiros. Permite também a troca por produtos pré-selecionados, pagamentos de contas de consumo e recarga de telefones pré-pagos. Conforme pode ser conferido no site da empresa: "O que é Dotz? Dotz é mais que um programa de fidelidade. É uma poderosa moeda de troca que você ganha nas compras feitas em estabelecimentos parceiros. E como Dotz tem uma das maiores redes de parceiros do país, você ganha mais e troca seus dotz mais rápido por milhares de produtos e viagens. É fácil. E é grátis!".

Km de Vantagens: programa de premiação destinado aos consumidores de combustível e demais serviços automobilísticos da rede de postos Ipiranga. Como pode ser visto em seu próprio site: "O que é o Programa Km de Vantagens? O programa Km de Vantagens é o 1º programa de fidelidade no segmento de postos de serviço. Nele, sempre que o consumidor adquirir produtos e serviços na rede credenciada de postos Ipiranga – Pista de abastecimento, Jet Oil, Jet Oil Motos e ampm – ou nos sites Shoptime, PneuStore e posto Ipiranga, acumulará pontos, chamados de Km, que darão acesso a benefícios e promoções exclusivas".

A variedade de produtos e serviços oferecidos por essas empresas é visivelmente maior que a das companhias aéreas. Por isso, os atores litigiosos estão dispostos a explorar qualquer fragilidade existente em sistemas, processos e tecnologias para alcançar a possibilidade de monetização rápida.

Está claro que a farta gama de opções de intercâmbio é cenário fértil para ações mercantilistas, inclusive por aqueles que estão à margem da lei.

Nota-se também o maior poder de angariação de vítimas pelos protagonistas dessa modalidade de fraude eletrônica.

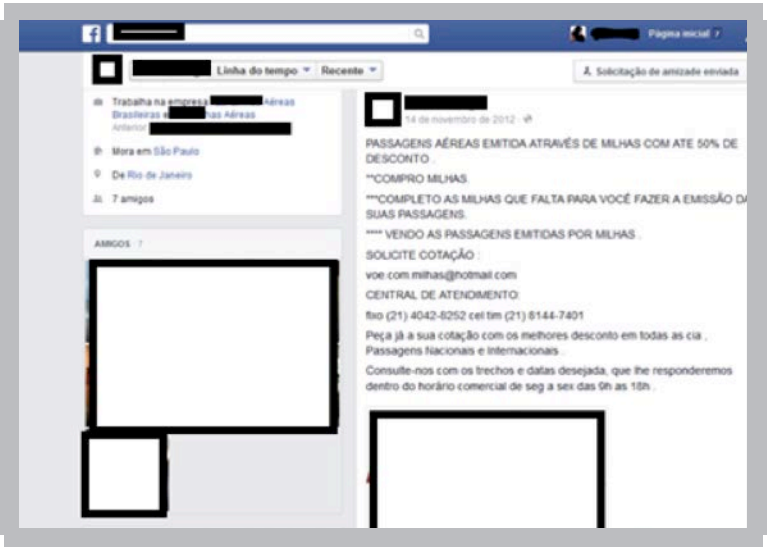
2.1. Modus Operandi de táticas correntes de monetização

O método aplicado nos ataques contra os sistemas de fidelização de clientes baseia-se no clássico phishing scam, entretanto, as tecnologias utilizadas pelos fraudadores cibernéticos foram sofisticadas, passando a utilizar técnicas e textos rebuscados que nos fazem crer estar em ambiente seguro e legítimo das instituições alvo.

As informações e imagens dispostas nas falsas páginas foram construídas para que fiquem idênticas ao site real, proporcionando maior sensação de autenticidade ao golpe aplicado, com o claro intuito de alavancar a monetização por meio da coleta de credenciais de forma ilícita.

A cadeia de comunicação litigiosa utiliza tecnologias blindadoras, ou seja, criptografadas, o que dificulta o trabalho de polícias especializadas e equipes técnicas na busca pelos agentes maliciosos.

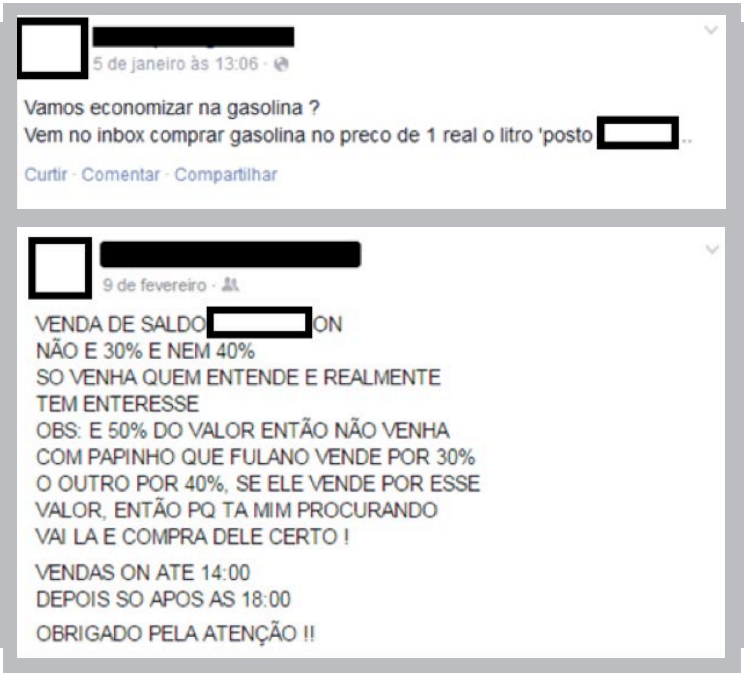
a) Procedimento de monetização em companhias aéreas:
Os autores da fraude compram bilhetes aéreos com o uso de pontos subtraídos de forma ilegal de contas legítimas e os vendem por preço exponencialmente inferior aos praticados no mercado legal. Estes bilhetes são normalmente comercializados de 40% a 70% abaixo de seu valor de mercado. Confira a seguir um exemplo.



b) Procedimento de monetização em distribuidora de combustíveis:

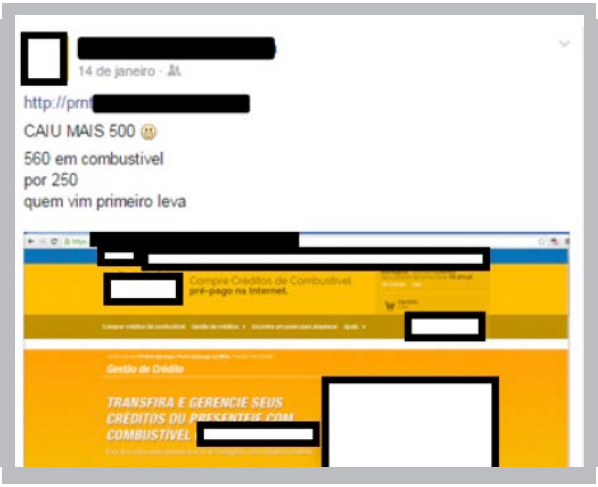
No programa de acúmulo de pontuação e benefícios das distribuidoras de combustíveis, o cliente tem a possibilidade de comprar combustível com descontos para abastecer, bem como adquirir produtos em empresas parceiras.

O valor do combustível comprado fica disponível na conta do programa de pontuação do cliente. Para abastecer utilizando este crédito, basta informar ao frentista sobre o benefício no ato do abastecimento, juntamente com o número do CPF. A operação será realizada por meio da máquina POS (Point of Sale). No momento do pagamento, o cliente digita a senha do programa de pontuação e o número de seu CPF. Estes mesmos dados são utilizados pelo cliente para acessar sua conta no site. O valor pago é descontado do crédito disponível no programa de pontuação.



Os supostos criminosos beneficiam-se desse processo por meio da venda irrestrita do crédito que foi comprado muito provavelmente de forma ilegal.

Utilizando-se da técnica de phishing scam, o fraudador cibernético consegue acesso não autorizado aos dados dos clientes e, posteriormente, ao site do programa. Com isso, é possível comprar os produtos oferecidos em parceria e utilizar o combustível disponível nos postos da rede.



c) Procedimento de monetização para a moeda virtual

Destacamos no segmento de programas de fidelização o programa de benefícios de acúmulo de pontos que se transformam em moeda virtual. Por se tratar de uma moeda que permite a aquisição de diversos produtos e serviços, esse programa está exposto a uma forte tendência de monetização pelos cyber criminosos.

O cliente acumula pontos ao realizar compras nos estabelecimentos parceiros físicos ou online por meio do seu cartão ou do código do programa e, posteriormente, pode trocá-los por prêmios ou serviços oferecidos.

Para conferir o saldo e trocar pontos, o cliente pode acessar o site da empresa ou o aplicativo de celular com o CPF ou com o cartão do programa.

Ao realizar uma troca, o cliente já pode retirar seu produto no estabelecimento parceiro. Caso a troca tenha sido feita pelo site, o produto será recebido no endereço cadastrado.

É possível também realizar o pagamento de contas de consumo até um limite de R$ 300,00 uma vez por semana com o mesmo CPF e fazer a recarga de celular pré-pago.

Para realizar as fraudes nesse programa de fidelização, os cyber criminosos capturam as credenciais de acesso dos clientes por meio da técnica phishing scam. Com isso, conseguem pleno acesso ao programa e podem usufruir dos recursos disponíveis.

Para realizar as fraudes nesse programa de fidelização, os cyber criminosos capturam as credenciais de acesso dos clientes por meio da técnica phishing scam.

Dentre as possibilidades para realização de ataques neste produto e consequente monetização, destaca-se a recarga de celulares pré-pagos. De posse das credenciais de acesso ao programa de fidelização, o agente malicioso ingressa no site da instituição utilizando os dados legítimos de vítimas do possível golpe para usufruir da premiação que foi acumulada pelo usuário.

De posse dos pontos, o fraudador promove o seu livre comércio, criando anúncios em grupos de redes sociais e demais canais de comunicação, como fóruns. Os créditos para recarga de celulares pré-pagos são, muitas vezes, oferecidos por valor 50% abaixo do mercado. Esta prática emprega alta atividade no mercado ilícito cibernético, gerando recursos financeiros para os cyber criminosos.

O pagamento de contas de consumo também é um serviço largamente utilizado para monetizar os agentes fraudadores. De posse das credenciais de acesso e uso, os agentes maliciosos pagam contas de terceiros, ou seja, beneficiam outros de forma ilegal, uma vez que promovem livre pagamento de quantias até ínfimas, contudo, de forma indiscriminada, o que dinamiza e amplia o ato destas operações.

Posteriormente, conferimos algumas capturas de telas em chats que os supostos fraudadores utilizam para comunicação e troca de informações, também conhecidos como internet relay chat (IRC).

d) Monetização baseada em vulnerabilidade sistêmica – Caso rede distribuição de combustível

Um estudo aplicado ao modo de operação do programa de fidelização da rede distribuidora de combustíveis demonstrou comportamentos que colidem com as suas regras.

O modelo proposto restringe o crédito de bônus uma vez ao dia. Porém, em testes laboratoriais foi possível notar uma fragilidade sistêmica que ultrapassa essa regra.

Existem duas formas de aquisição: a primeira é feita online em equipamento eletrônico conhecido como POS (Point of Sale), um dispositivo eletrônico portátil que permite o pagamento de quantias para as instituições financeiras e/ou adquirentes; o segundo método é a aquisição offline, ou seja, por fila de processamento, que teoricamente deveria ser processado no outro dia. Entretanto, por falha sistêmica, foi constatado por teste em campo que era possível realizá-lo no mesmo dia.

O pagamento de contas de consumo também é um serviço largamente utilizado para monetizar os agentes fraudadores.

3. IMPACTO ECONÔMICO

Visando apresentar os impactos econômicos causados pelos crimes cibernéticos, fizemos algumas simulações do volume financeiro perdido pelas companhias aéreas com os constantes ataques realizados por cyber criminosos brasileiros no período de julho de 2015 a abril de 2016.

Uma das táticas mais utilizadas pelo criminosos é obter as credenciais dos usuários e usá-las para a comercialização de milhas. As informações foram coletadas por meio das atividades de monitoramento da NS Prevention.

Os prejuízos das companhias aéreas não ficam restritos somente ao furto, mas também englobam o montante que deverá ser ressarcido aos seus clientes.

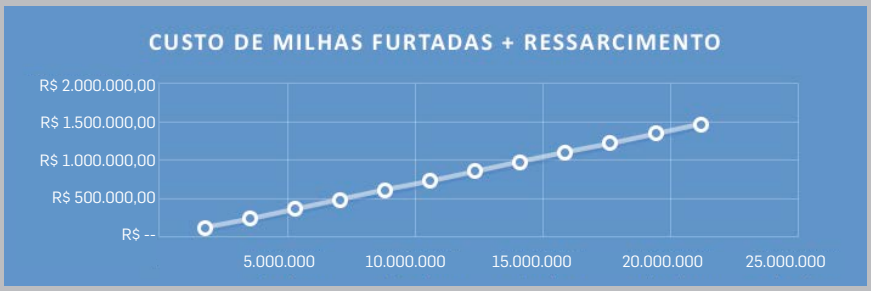
Para demonstrar este impacto sob as credenciais que monitoramos, apresentaremos o montante obtido nas atividades da NS Prevention no primeiro trimestre de 2016, no qual foram levantados 972.156 pontos dentre 436 credenciais coletadas de uma determinada companhia aérea.

Sendo esses 972.156 pontos furtados e não tomadas as devidas ações em tempo hábil, o prejuízo representa o dobro, uma vez que as companhias aéreas devem assumir as milhas furtadas e o seu ressarcimento para os clientes.

Portanto, neste caso, o prejuízo é de 1.944.312 pontos, o que representa a soma do que foi furtado e do que deverá ser ressarcido aos clientes lesados.

Levando em consideração que no site da empresa o pacote de pontos é vendido por aproximadamente R$ 14,28, podemos dimensionar um prejuízo sobre os 1.944.312 furtados e ressarcidos de R$ 136.101,84.

Fizemos também uma simulação do impacto entre as milhas furtadas e o custo gerado ao longo de 12 meses no caso deste cenário se perpetuar. O resultado encontrado foi que no final de um ano, se mantido um volume de 1.944.312 pontos por mês, o custo gerado seria de R$ 1.620.499,02.



O prejuízo direto estimado em uma companhia aérea com fraudes envolvendo seu programa de fidelização chega a aproximadamente R$ 1 milhão ao ano.

Segundo Cenário: Passagem Aérea com Milhas Furtadas

Em simulação realizada no site de uma companhia aérea, fizemos algumas cotações de passagens utilizando pontos para dimensionar o prejuízo que o furto dos 972.156 pontos poderia causar. O resultado mostrou que o prejuízo acumulado pode chegar a R$ 440.930,80 ao longo de 12 meses.

Pontos Furtados	Origem	Trechos	Valor Passagem	Qtd. Milhas	Qtd. Passagem	Custo	Custo Anual
972.156	CHG	SP X BRZ	R$ 1.183,00	14.000	69	R$ 82.147,18	R$ 985.766,18
972.156	GRU	SP X BH	R$ 651,00	10.000	97	R$ 63.287,36	R$ 759.448,27
972.156	GRU	SP X BRZ	R$ 650,00	10.000	97	R$ 63.190,14	R$ 758.281,68
972.156	VCP	SP X RJ	R$ 670,00	12.000	81	R$ 54.278,71	R$ 651.344,52
972.156	VCP	SP X BSB	R$ 720,00	14.000	69	R$ 49.996,59	R$ 599.959,13

Dados Extraídos do site no dia 03/05/2016

Evidência da data da cotação de passagem

Terceiro Cenário: Dano à Imagem da Cia Aérea

Um dos danos causados com o furto e comercialização de credenciais e, consequentemente, com a subtração de pontos dos clientes é o dano à imagem da companhia.

Não iremos mencionar neste relatório o dano à imagem, que por muitas vezes se torna algo imensurável e intangível. Mas, é possível citar a quantidade de reclamações de clientes com a perda dos pontos e a possibilidade de escândalo caso ocorra fraude ou furto e isso seja divulgado na mídia, prejudicando diretamente os negócios da empresa.

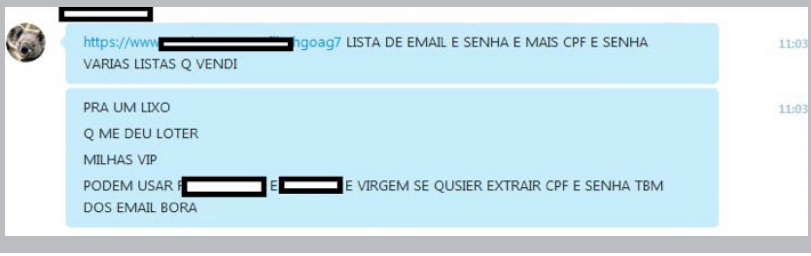
4. PERFIL DOS CYBER CRIMINOSOS

Durante o período de monitoramento realizado pela NS Prevention, notou-se que vem aumentando o número de hackers que comercializam credenciais de companhias aéreas com o objetivo de se monetizar. Tais criminosos já portam ferramentas automatizadas para realizar testes em credenciais, quebrando senhas e validando a quantia de pontos adquiridos por cada cliente.

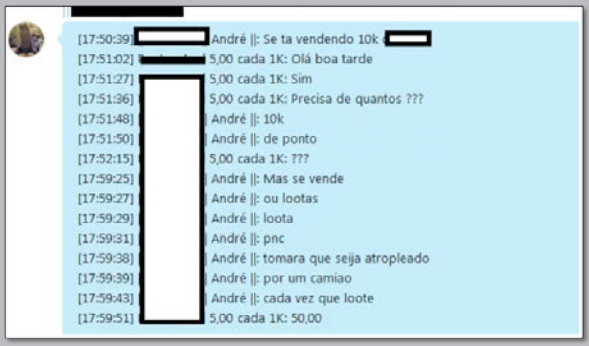
Nesse primeiro momento, detectamos cerca de 21 perfis que comercializam credenciais e facilitam a venda ilegal de milhas e passagens aéreas.

O perfil de idade varia entre 15 e 27 anos e são atuantes tanto em São Paulo como em outros estados brasileiros. Os fraudadores chegam a comercializar milhas por diversos valores, conforme evidenciado a seguir nas imagens coletadas em 19/04/2016.

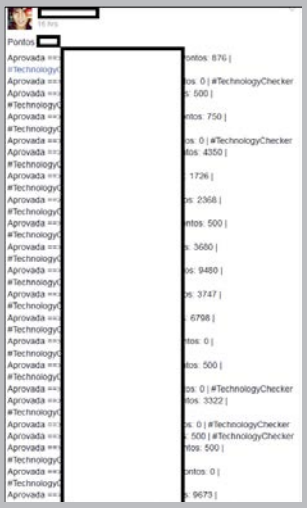
O perfil do fraudador está em uma faixa etária que vai de 15 a 27 anos e sua atuação ocorre tanto em São Paulo como em outros estados brasileiros.

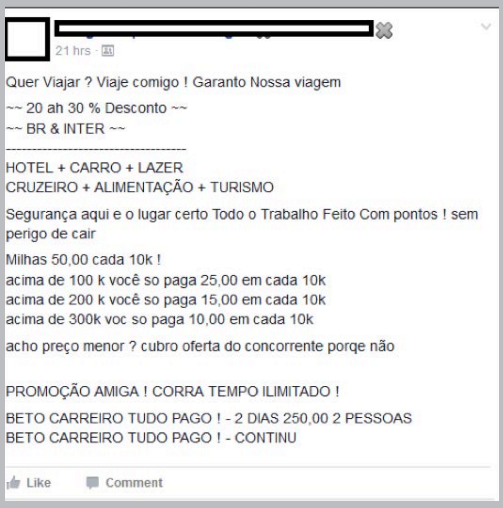


Evidência de venda de milhas em redes sociais



Evidências de venda de milhas em redes sociais





5. TENDÊNCIA

Os programas de fidelização adotados em um passado recente tornaram-se verdadeiros sistemas robustos de resgate de produtos e serviços. Cabe mencionar que sob a ótica contemporânea no meio digital, estes programas fornecem verdadeiras moedas eletrônicas.

Com isso, nota-se que os atores das fraudes eletrônicas atuais dispensam atores intermediários para acesso à moeda real. Estes acabam por comprar e trocar mercadorias em sites de comércio eletrônico, o que de certa forma provê alguma autonomia na execução de suas práticas ilícitas.

A contração no processo da fraude, ou seja, o menor número de passos torna a fraude mais acessível aos protagonistas da mesma, uma vez que estes têm maior autonomia em suas atividades, menor dependência de terceiros e melhor campo de intercâmbio dentro do mercado virtual.

6. ANÁLISE NEW SPACE PREVENTION

Conforme demonstrado neste relatório, os programas de fidelização travam disputa acirrada entre si, disponibilizando diversas opções para intercâmbio dos pontos conquistados pelos clientes.

Como consequência, nota-se um aumento expressivo de fraudes nesse segmento. Contudo, nem mesmo todos os investimentos aplicados em segurança da informação são suficientes para conter totalmente o crescimento dessa modalidade criminosa aplicada atualmente.

A expansão de operações hoje existentes nesse específico mercado de premiação e recompensas demonstra maior interesse e poder de atividade por parte de possíveis fraudadores, uma vez que sua gama de práticas está mais ampla que no início de suas operações em um passado recente.

Dentre as táticas utilizadas pelos cyber criminosos com o propósito de perpetrar fraudes contra sites que promovem programas de pontuação e recompensas, percebe-se a clara utilização de um conjunto de técnicas que contemplam:

1. Telas falsas: buscam se assemelhar ao máximo de suas páginas originais, no entanto, têm claro objetivo de coletar dados e credenciais de acesso para efetuar práticas criminosas.

2. E-mails: possuem nomes e características que buscam se passar por mensagens eletrônicas verdadeiras enviadas pelas instituições, porém, remetem a sites falsos que tem por objetivo coletar dados legítimos para serem usados em possíveis ataques cibernéticos.

3. Programas espiões: são aplicativos maliciosos que alteram arquivos de configuração cruciais para navegação na Internet, direcionando o usuário para uma página falsa de forma a acreditar que está em ambiente seguro e legítimo, embora esteja em site criado com o propósito de capturar credenciais de acesso para posterior uso.

Nota-se que os atores das fraudes eletrônicas atuais dispensam atores intermediários para acesso à moeda real. Estes acabam por comprar e trocar mercadorias em sites de comércio eletrônico, o que de certa forma provê alguma autonomia na execução de suas práticas ilícitas.

Do acesso à rastreabilidade gerada no processo já descrito, constata-se extrema dificuldade em registrar as atividades praticadas entre os criminosos, uma vez que estes se valem de canais de comunicações fechados e até exclusivos para troca de informações e práticas utilizadas.

De modo geral, nota-se uma expansão nas atividades ilícito-cibernéticas para vertentes que não estão restritas ao mercado financeiro. Conclui-se que, com o emprego de programas de fidelização, extensão e uso dos serviços citados, o protagonista da fraude eletrônica tem amplo campo de atividade, desbravando novas linhas de atuação e gerando pontos de atenção e necessidades de investimentos em recursos para proteções e medidas de contenção.