Prejudicando mais do que o balanço final: um panorama sobre fraudes e a segurança cibernética.

Ao analisar as fraudes e ataques cibernéticos que ocorrem em todo o mundo, é possível identificar todos os custos e prejuízos que estes trazem as empresas e economias afetadas. As estimativas informadas calculam que o custo gerado por esse tipo de crime em todo o mundo foi de USD 445 bilhoes[1]. Quando esses crimes acabam tendo sucesso, os prejuízos financeiros são muito relevantes, no entanto os danos à reputação e o impacto no negócio que surgem em consequência dos ataques, acabam sendo mais prejudiciais.

A proteção contra ameaças de fraude e a segurança cibernética são uma preocupação crescente para as empresas hoje em dia. Para muitos, tornou-se imperativo proteger suas organizações de tais perigos, especialmente considerando que as ameaças e os ataques continuam sem ser combatidos. Além disso, os métodos dos fraudadores evoluem e se modificam constantemente, aumentando a preocupação das empresas.

Algumas informações indicam que os incidentes de fraude e ataques à segurança cibernética estão aumentando, não somente em frequência, mas também em severidade e impacto. As companhias que não conseguirem garantir que seus funcionários estejam bem capacitados para reconhecer e agir contra essas ameaças utilizando processos, procedimentos e protocolos de segurança adequados, não somente correm um maior risco de perdas financeiras, as quais incluem perda de ativos, como também um maior risco de dano à reputação e interrupção do negócio.

Como se alterou o cenário de fraude?

As ameaças de fraude e segurança cibernética continuam evoluindo à medida que surgem indivíduos e organizações criminosas mais bem preparadas e organizadas.

Conforme ilustrado no diagrama 1, os estelionatários e indivíduos que cometem crimes cibernéticos se tornaram mais sofisticados nos últimos anos. Houve uma notável mudança no perfil dos indivíduos por trás dos ataques.

[1] De Perdas Líquidas de McAfee: Estimando o Custo Global do Crime Cibernético, arquivo mais recente de www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf de 4 de abril de 2016.

Diagram 1. Do passado ao presente: as principais mudanças nas ameaças de segurança da informação

O cenário da ameaça cibernética continua evoluindo à medida que surgem indivíduos e organizações melhores organizados e mais sofisticados.

No passado, os invasores eram basicamente indivíduos, operando de modo oportunista, casual ou eventual, em sua maioria motivada pelo desejo de provar que podiam ter sucesso realizando um ataque de fraude.

Agindo sozinhos ou em conjunto para cometer fraudes interna ou externa, os fraudadores realizam, cada vez mais, ações que buscam ocasionar transtornos e destruição.

Hoje, quem realiza os ataques são sindicatos e grupos criminosos que são controlados de maneira similar às empresas. Estas empresas criminosas estão normalmente bem organizadas e, em sua maioria, bem financiadas. Estão motivadas basicamente por ganhos financeiros; porém, em alguns casos, por benefícios geopolíticos. Esses estelionatários estão cada vez mais focados em ocasionar transtornos e destruição. Existe também o risco de fraude interna e, da mesma maneira, a fraude interna pode ser realizada por indivíduos oportunistas ou por um funcionário que opera em conjunto com um grupo que pertence a essas organizações criminosas.

O Diagrama 2 mostra a natureza da transformação dos múltiplos aspectos da fraude ou do ataque à segurança cibernética. Algo que se destaca, é o fato de os ataques terem objetivos cada vez mais específicos, com fraudadores que realizam uma grande quantidade de pesquisa e planejamento prévios à tentativa de ataque. Essas tentativas também mudaram de padrão, deixando de ser ataques oportunistas realizados uma única vez para ataques dirigidos, planejados e contínuos. Os envolvidos continuarão suas tentativas a um determinado alvo, caso exista a possibilidade de sucesso.

Os métodos dos ataques estão evoluindo de modo constante e, também, se adaptando para superar as defesas que as organizações desenvolvem. Não é de surpreender que tenha ocorrido um crescimento no uso de tecnologia por parte dos estelionatários. Os métodos de ataque tendem a ter como alvo as fraquezas na tecnologia e na natureza humana e, em alguns casos, em ambos. É por essa razão que é muito importante revisar, com frequência, os procedimentos e processos internos, para garantir que todos os funcionários estejam capacitados e conscientes de suas responsabilidades no caso de uma tentativa de ataque.

Qual é o perfil de um fraudador?

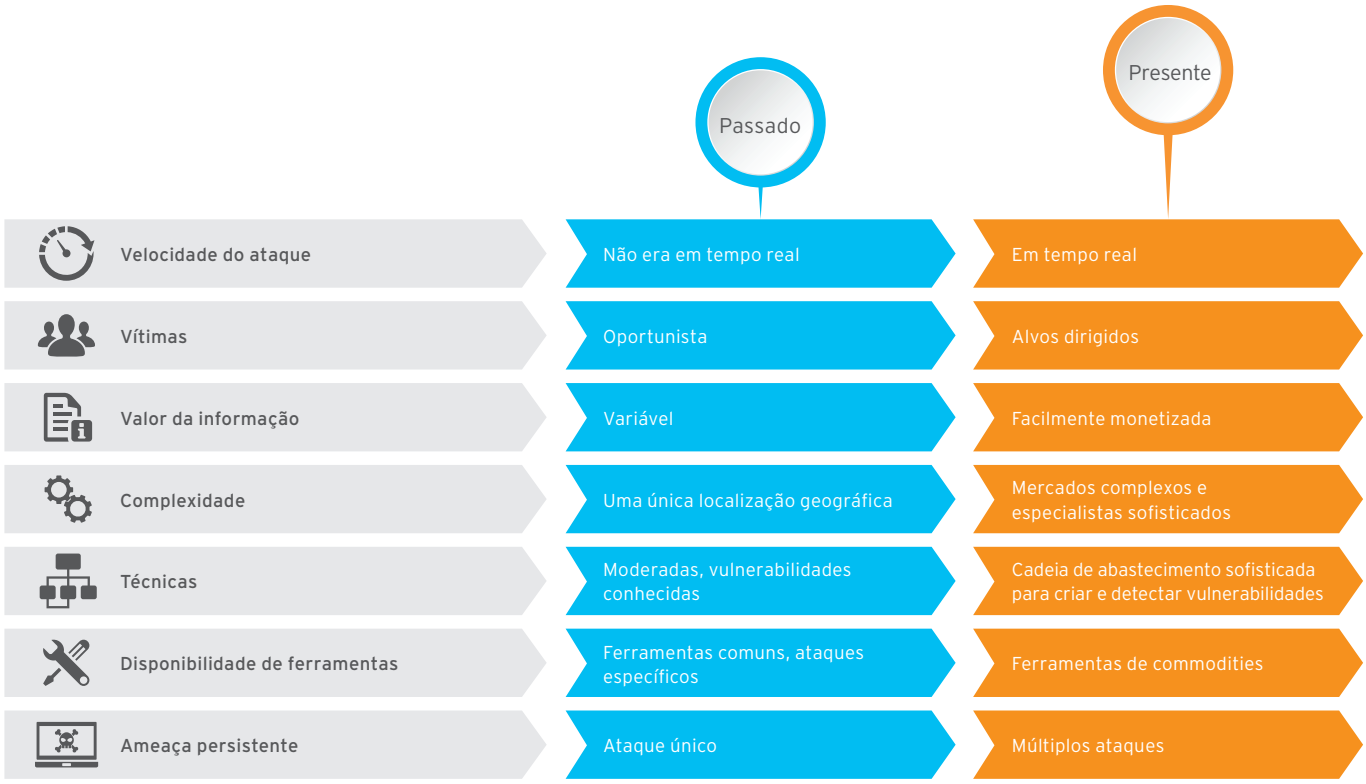
A KPMG traçou o perfil de um fraudador tendo como base a análise de 596 casos de crimes realizados por funcionários administrativos, entre os anos de 2011 e 2013, com algumas estatísticas reveladoras.

O alvo são seus empregadores

O fraudador típico é do sexo masculino, e estão entre os 36 e os 55 anos, e tende a cometer fraude contra seu próprio empregador.

- 61% dos fraudadores são empregados da companhia a qual atacam.
- 41% estão empregados por um período maior a 6 anos.

Diagram 2. Ameaças em evolução: uma ilustração sobre os desafios da segurança da informação.



Costumam trabalhar em conjunto

Tendem a trabalhar em uma posição de finanças ou relacionado a ela, incluindo o departamento de operações, ou têm posições de gerência sênior. Além disso, costumam ser funcionários da empresa por mais de 6 anos. Durante esse tempo, realizaram fraudes por mais de 1 a 5 anos em 72% dos casos, nos quais em 70% das vezes trabalharam em conjunto com outros empregados, causando danos por dezenas de milhares, centenas de milhares e, ainda, milhões de dólares.

- 18% estão entre USD 50.000 e USD 200.000.
- 43% excedem os USD 500.000, 16% dos quais excedem os USD 5.000.000.

Também agem por conta própria

Quando este fraudador trabalha sozinho, a grande maioria das fraudes que comete ocorrem entre 1 e 5 anos, também causando dano econômico significativo.

- 21% estão entre USD 50.000 e USD 200.000.
- 32% excedem os USD 500.000, 9% dos quais excedem os USD 5.000.000.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

1461583 08/16