KASPERSKY FRAUD PREVENTION - CLIENTLESS ENGINE

Segurança mais inteligente – melhor serviço bancário digital

Enquanto as instituições financeiras estão correndo para fornecer aos clientes a mais intuitiva e satisfatória experiência em Banco On-line, os criminosos virtuais profissionais estão correndo para desenvolver malwares ainda mais sofisticados para tirar total proveito de cada nova oportunidade de fraude on-line.

Novas e poderosas técnicas de ataque que você talvez já tenha visto em ação incluem:

- **Infiltração de página da Web** - campos adicionais "injetados" em sua página de login, capturando dados confidenciais do cliente, como o número do cartão CVS para uso em ataques de "cartão ausente".
- **Pop-ups falsos (phishing)** - adicionando uma solicitação "pop-up" de dados adicionais própria do hacker, talvez um número de celular para que verificações de dois fatores possam ser interceptadas.
- **Adulteração de transações** - os exemplos incluem instruir os clientes a "reembolsar" o dinheiro falsamente registrado como uma entrada por engano na conta deles, ou para fazer uma transação de "teste" para ajudar o banco.

Todas essas técnicas começam carregando o malware, geralmente na forma de Cavalos de Troia de serviços bancários, em seu sistema de Banco On-line e esse malware normalmente é introduzido através do ponto mais vulnerável de seu sistema: seus clientes. Os invasores começam infectando o próprio dispositivo de seu cliente e, então, usam a conexão on-line do cliente como o ponto de entrada deles.

Como você se protege contra ataques de fraude complexos iniciados a partir de dispositivos infectados de usuários, sem comprometer a experiência de Banco On-line descontraída e simplificada que cria clientes leais e felizes?

O Clientless Engine do Kaspersky Fraud Prevention impede que criminosos virtuais iniciem ataques bem-sucedidos utilizando:

Detecção de malware financeiro:
Busca e identificação proativas de malwares que tentam infectar suas páginas da Web através dos dispositivos de seus clientes.

Detecção de qualquer computador ou celular infectado que tente iniciar atividades mal-intencionadas através de sua conexão com o site, sem causar impacto a clientes não infectados ou à sua experiência em serviços bancários digitais.

Relatórios abrangentes:
Alertam-no para que seu banco possa tomar medidas, que poderiam incluir:

- Bloquear a transação
- Encerrar a sessão do usuário
- Cuidar do caso do cliente para garantir que o incidente não se repita.

Gerenciamento de endpoints:
Fornece dados de incidentes através do console do Kaspersky Fraud Prevention, e transmite esses dados para sistemas internos ou de terceiros para uma análise e pesquisa mais detalhadas, se necessário.

Feeds de inteligência:
Fornecem a suas equipes de gerenciamento de Banco On-line as informações de que elas precisam para tomar decisões complexas sobre segurança.

Quando você tem a visibilidade de cada incidente em potencial, o processo não possui atritos para os usuários, a menos que o dispositivo deles tenha sido comprometido pelo malware de serviço bancário. Nesse caso, você estará lá para tranquilizá-los, e para aconselhá-los sobre como permanecer seguros no futuro.

O resultado é um ambiente de Banco On-line mais seguro para todos, proporcionando a você a liberdade para angariar e manter mais clientes através do desenvolvimento posterior da funcionalidade de seu portal de serviços bancários digitais, sem aumentar o risco de tentativas de fraude não detectadas.

Entre em contato conosco para saber mais: KFP@kaspersky.com
http://www.kaspersky.com/business-security/fraud-prevention

Folheto informativo do Clientless Engine do Kaspersky Fraud Prevention - agosto de 2015 GL