# Whitepaper

# O custo real dos códigos maliciosos: Um olhar nos servicos Anti-fraude da S21sec's para Bancos e Instituições Financeiras

Daniel Brett

S21sec

Whitepaper

# O Custo real dos códigos maliciosos: Um olhar sobre os Serviços Anti-fraude combinados com os serviços de Inteligência e de Resposta para Bancos e Instituições Financeiras

**A indústria bancária internacional sofre atualmente de uma lacuna no que diz respeito a softwares mal-intencionados ou códigos maliciosos, em termos de inteligência, de análise, de resposta a incidentes e de recuperação de dados. S21sec fornece um serviço completo Anti- Fraude que reduzirá drasticamente as perdas financeiras diretas e mitigará os riscos financeiros e os riscos de reputação para o banco.**

## Conteúdo

## Exame sobre os Riscos e os Custos de um Código Malicioso

Quais são os riscos e os custos de um incidente de códigos maliciosos para um banco e de que maneira eles são diferentes para o fenômeno atual de Phishing? Neste guia de solução vamos examinar os riscos e os custos financeiros que este tipo relativamente novo de ataque representa para o setor de serviços financeiros e para os bancos em particular. Nós mostraremos a redução de perdas com fraudes ao utilizar os serviços Anti Código Malicioso da S21sec e, então, indicar como ele funciona.

**O que é um ataque de Código Malicioso?** Programas de códigos maliciosos são automáticamente transferidos a partir de falsas páginas web ou de "log keystrokes" secretamente, quando um cliente visita um site de home banking. O Código malicioso se esconde nos diretórios do sistema e dos monitores quando o consumidor abre uma "conexão HTTPS" criptografada (Hypertext Transfer Protocol over Secure Sockets Layer) a sites bancários em particular. Uma vez que uma "conexão HTTPS" foi estabelecida, o código malicioso "logs keystrokes" tira fotos da tela do processo de login para obter a informação do consumidor. O Código Malicioso captura os detalhes e os envia para os criminosos.[1]

**Qual é a diferença do Phishing?** Neste tipo de ataque não é utilizado nenhum site externo que se passa pelo site oficial do Banco. O cliente estará usando o verdadeiro site do banco, enquanto o roubo de identidade ocorre. O outro problema é o vetor de ataque. O Código Malicioso geralmente não é detectado por produtos antivírus e a infecção geralmente ocorre em visitas reais, a sites informativos, que foram modificados por hackers, ilegalmente, para conter códigos maliciosos, ou links para o código malicioso. Em vários casos, tem sido o próprio Banco, cujo site foi usado para infectar seus próprios usuários.[2] Isto tem implicações importantes para os Bancos que podem ser submetidos a processos e a multas, se forem encontrados, ainda que inadvertidamente, hospedando códigos maliciosos em seus próprios sites. [3]

**Bank of India – Hosted Malicious Code Attack**

The Bank of India suffered an attack, in August 2007, originating in Russia which introduced malicious software in the front page of the bank's website, infecting any clients that connected to it.

The attackers introduced malicious code into the web server via an IFRAME located in Russia. The malicious code used a kit known as MPACK that, by means of an exploit, was able to infect visitors to the front page of the Bank of India website.

This attack, as well as infecting millions of users obliged the Bank IT department to take down the website for 24 hours. Damage estimation: 24hrs without service and incalculable damage to the bank's corporate image.

O resultado para os clientes é muito negativo. Ao contrário dos ataques de phishing, onde os clientes podem muitas vezes vir a perceber que a sua falta de conhecimento os levou a confiar na credibilidade de um site de terceiros imitando o de seu banco, em ataques de código malicioso, os clientes estão usando o site do próprio banco quando o roubo acontece. Isto tem

[1] As defined by The Financial Services Authority, UK.
[2] Bank of India, August 2007.
[3] FSA, UK, fines Norwich Union Life GBP 1.26 million for information security lapses, 17 Dec 2007.

consequências graves para a credibilidade do banco on-line, da marca do banco e da sua imagem para esse cliente.

Para os Bancos o resultado também é negativo. Os riscos são, em primeiro lugar, em matéria de processos e de ações de órgãos reguladores sobre a hospedagem de códigos maliciosos em sites do banco. Outros são os riscos de danos à imagem da marca do banco, e o atrito na base de usuários on-line com clientes migrando para a concorrência ou deixando de utilizar serviços bancários on-line. Finalmente, há o risco de que criminosos podem derrotar os atuais procedimentos do banco, os modelos de segurança e os mecanismos de autenticação. Todos os itens acima implicam um risco de atenção da mídia.

*Os números do UK Bank mostram perdas por fraude na Internet de £ 21.4M a partir de janeiro a junho de 2008. Um crescimento de até 185% sobre o mesmo período de 2.007.* [4]

*Os relatórios da S21sec mostram que Código Malicioso representam 30% das fraudes na Internet em 2008; o resto é phishing. Mas o código malicioso está*

**Riscos**

- Perda financeira para a fraude
- Multas e processos por hospedagem de códigos maliciosos.
- Perda de confiança e dano à imagem de marca
- Migração para a concorrência
- Derrota dos modelos atuais de segurança bancária e dos mecanismos de autenticação
- Aumento da atenção da mídia nos incidentes de segurança do banco

**Custos dos Riscos**

Temos que separá-los em Custos Tangíveis ou fáceis de atribuir valor e Custos Intangíveis, cuja valoração monetária é mais difícil.

- Custos tangíveis de
    - Contabilizando o investimento nos modelos atuais de segurança nos mecanismos de autenticação.
    - O aumento de investimento em medidas defensivas.
    - As perdas diretas com as fraudes por transferência de dinheiro para contas de terceiros.
    - As perdas diretas decorrentes da gestão de casos, de aconselhamento de clientes e de investigações internas.
    - Multas por infrações de perda de dados, no caso da falta de procedimentos de segurança necessários para lidar com os ataques de códigos maliciosos. Nós vemos isso como um problema se o banco hospeda códigos maliciosos em seus próprios sites.
- Custos intangíveis de
    - Experiências negativas dos clientes.
    - Redução na confiança dos clientes
    - Aconselhamento complexo para o cliente.
    - Aumento da atenção da mídia.
    - Dano à imagem da marca.

Examinaremos os Custos tangíveis na próxima seção em um Estudo de caso.

## Estudo de Caso – Impacto de um ataque de Código Malicioso

É muito difícil fornecer dados sobre fraude. Os Bancos não os divulgam. Este estudo de caso é construído com base nos valores obtidos a partir de nossas próprias informações com mais de 90 bancos que utilizam os nossos serviços e as tendências que eles expressam são corroborados com os dados fornecidos pela APACS, a organização dos serviços de pagamentos do Reino Unido.

### Escopo de um Ataque

Se tomarmos um típico banco grande com operações internacionais, teremos 4 a 5 novos exemplos de códigos maliciosos atacando este banco todos os dias: pelo menos 120 ataques por mês. Nós não sabemos da eficácia desses ataques. Os bancos não divulgam esta informação. Podemos fazer uma estimativa conservadora de que o banco perderia dinheiro em pelo menos 20% desses ataques, de nossa experiência com os clientes. Muitos bancos centrais acompanham de perto as transferências acima de 3000 Euros. Então, vamos supor que durante cada ataque "bem sucedido" cada cliente pode perder no máximo de 3000 Euros. Não sabemos exatamente quantos usuários estão comprometidos por ataque. Mas, a partir das credenciais que recuperamos de cada site comprometido por Código Malicioso, normalmente encontramos blocos de pelo menos quinze usuários comprometidos, indicando pelo menos 15 casos "bem sucedidos" de roubo de identidade por entidade bancária, durante um ciclo de infecção. Em todos esses casos de fraude haverá gestão pelo pessoal do banco. Vamos assumir, pelo menos 10 horas-homem de gerenciamento de casos para cada incidente. O custo interno das investigações da fraude pode chegar facilmente a 1000 €. Assim, supondo alguns números muito conservadores, podemos fazer o seguinte caso:

- 5 ataques bem-sucedidos por mês (menos de 10% de "sucesso")
- 10 usuários comprometidos por ataque "bem sucedido" (menos do que os blocos de 15 credenciais que encontramos)
- Assim, 50 usuários comprometidos por mês.
- € 1500 perdas diretas por usuário. (Um palpite informado: metade da perda máxima possível sem alertar o banco central)
- Perdas totais por mês: 5 x 10 x 1500 = 75,000 €
- € 0,9 milhões por ano perdidos para a fraude direta (75,000 x 12)
- 600 clientes afetados por ano (5x10x12)
- € 0,6 milhões por ano perdidos para gerir os casos de fraude (€ 1000 por caso x 600 casos)
- Perdas Diretas: € 0,9 milhões
- Perdas indirectas: € 0,6 milhões
- Total de € 1,5 milhões

As estatísticas que temos do Reino Unido apoiam nossos cálculos. As estatísticas mostram uma perda direta de 40 milhões de libras (€ 52 milhões) dos bancos de 12 Estados por ano. Isso é uma perda média da indústria de £ 3.3 milhões de libras (€ 4,3 milhões) por banco, valor que reflete tanto os casos de phishing e de código malicioso. A S21sec encontrou código malicioso entre os nossos clientes em cerca de 30% de todos os ataques. Se aplicarmos essa relação com os valores do Reino Unido, chegamos a 1 milhão de libras (€ 1,3 milhões) por banco. Todas as taxas de câmbio a partir de outubro de 2008.

Existem outros custos identificáveis, além dos custos diretos e indiretos de fraude. Na primeira seção, "riscos e custos de Código Malicioso", identificam-se os seguintes custos tangíveis:

- Desperdiçar o investimento em modelos atuais de segurança bancária e em mecanismos de autenticação.
- Aumento do investimento em medidas defensivas.
- Perdas diretas com fraudes pela transferência de dinheiro para contas de terceiros.
- Perdas indiretas por gestão de casos, aconselhamento de clientes e investigação internas.
- Coimas por infrações perda de dados, no caso em que o banco encontra-se à falta de procedimentos de segurança necessários para lidar com os ataques de códigos maliciosos. Nós vemos isso como um problema se o banco encontra-se a hospedar códigos maliciosos em seus próprios sites.

Se assumirmos um cenário de pior caso para o nosso estudo de caso, podemos acrescentar os seguintes conceitos para os custos: o desperdício de investimento em segurança na Internet, um aumento do investimento em correções para o combate, e multa por hospedar em seu próprio website um código malicioso.

**Desperdício do investimento na solução atual**: O ataque nega o modelo de segurança do banco e o mecanismo atual de autenticação em aplicações web. Estas funcionalidades de segurança custam 500.000 euros para aplicar, por isso estamos somando o desperdício desse investimento.

**Aumento do investimento em correções**: Medidas futuras - mudanças no aplicativo da Web necessárias para combater novos ataques usando as mesmas táticas. 300.000 EUR

**Multas**: Multa de 100.000 de euros pela garantia dada pelos Bancos que seus que os sites e a sua infra-estrutura web estavam livres de Código Malicioso.

Então, vamos rever o Melhor e o Pior cenário de risco para um banco. O melhor caso inclui apenas os custos diretos e indiretos de fraude por Código Malicioso e, na pior das hipóteses, incluem os custos tangíveis de riscos mais abrangentes.

| | Melhor Cenário | Pior cenário |
|---|---|---|
| Desperdício do investimento na solução atual | - | €500.000 |
| Investimento em novas Contramedidas | - | €300.000 |
| Custos diretos com fraude | €900.000 | €900.000 |
| Custos indiretos com fraude | €600.000 | €600.000 |
| Multas por perda de dados | - | €100.000 |
| Total | €1.500.000 | €2.400.000 |

**Tabela 1 Custos tangíveis de um incidente de código malicioso**

Como os serviços da S21Sec podem ajudar a reduzir as perdas e a mitigar os riscos?

Reavaliação do atual modelo de segurança do banco: Gostaríamos de avaliar a aplicação web e aconselhar para minimizar o risco de este evento acontecer para proteger o investimento nesta área por um longo período de tempo. Gostaríamos de fazer uma varredura de vulnerabilidade diária nas páginas web do Banco. Gostaríamos também de fazer uma busca

contínua por evidências de códigos maliciosos hospedados em sites do próprio Banco. Esperamos reduzir a negação do modelo de segurança atual em 50%.

Futuras Contramedidas: O custo das contramedidas futuras não pode ser desprezado. Contudo, podemos fornecer inteligência que garanta ao banco investir a quantidade mínima de dinheiro para o máximo benefício. Prevemos uma redução notável (cerca de 50%) neste item.

Os custos diretos e indiretos de Perdas por Fraude: Ao detectar a fraude baseado no código malicioso e agir o mais rapidamente possível, podemos reduzir a janela de atividade dos atacantes de 60 para 20 horas (na verdade, bloqueamos um web site em menos de 5 horas em média). Isso dá ao banco a capacidade de detectar os clientes infectados em tempo real, permitindo assim que o banco impeça as transferências fraudulentas antes que eles ocorram. Como reduzimos a janela de tempo em dois terços, reduzem-se os clientes afetados por incidente de 10 para 3. Esta é uma redução de dois terços do número de casos afetados. Haverá um efeito semelhante em perdas indiretas.

Multas regulatórias: Ao assegurar que o banco não é responsável por hospedar códigos maliciosos, praticamente elimina-se a possibilidade destes tipos de multas.

| | Pior cenário | Com Serviço Anti-fraude |
|---|---|---|
| Desperdício do investimento na solução atual | €500.000 | €250.000 |
| Investimento em novas Contramedidas | €300.000 | €150.000 |
| Custos diretos com fraude | €900.000 | €300.000 |
| Custos indiretos com fraude | €600.000 | €200.000 |
| Fines for Data Loss Breaches | €100.000 | €0 |
| Totals | €2.400.000 | €800.000 |

**Tabela 1 Comparação com Serviços Anti-fraude contratados**

Conclui-se deste caso de Códigos Maliciosos que os bancos serão capazes de reduzir drasticamente as perdas diretas e indiretas com este tipo de ataque através da contratação de Serviços Anti-fraude. Haverá também uma notável redução do risco de desperdício de investimento em segurança, do aumento do investimento em nova contra-medidas e multas por perda de dados.

Não podemos quantificar os riscos intangíveis, no entanto, os riscos da experiência negativa do cliente, redução da confiança do cliente, aconselhamento complexo ao cliente, exposição negativa na mídia e de dano à imagem da marca a partir de valores de fraude será significativamente reduzido.

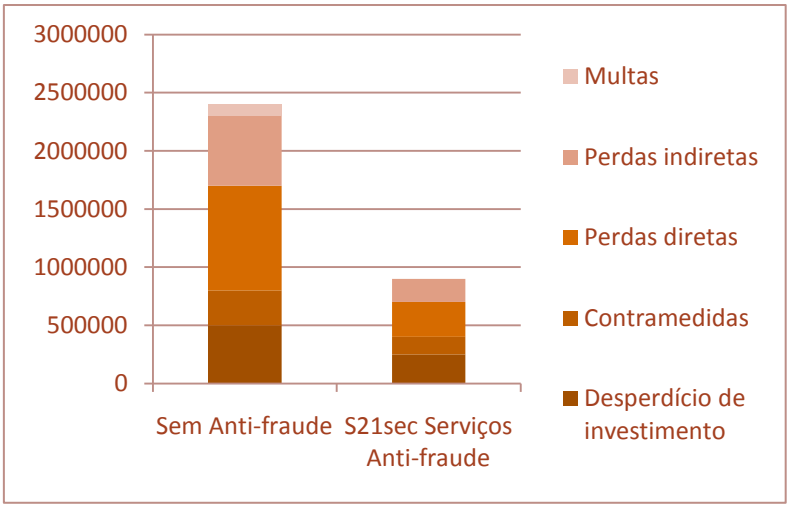


**Diagrama 1 Redução nas perdas com os Serviços contratados**

O custo dos serviços de luta contra códigos maliciosos pode variar em função das quantidades de páginas vigiadas, de sites escaneados e do pacote de serviços encomendados. Mas vamos estimar € **150.000** por ano, neste exemplo. A justificativa para este custo pode ser feita contra a economia da perda direta. A mitigação de riscos torna-se um benefício adicional sem custos para o banco.

## Descrição dos Serviços e-crime Anti-fraude da S21Sec

S21sec propõe uma solução para cobater Códigos Maliciosos baseada em concretos componentes que podem ser distribuídos em cinco áreas ou regras: Prevenção, Detecção, Informes de Inteligência, Reação e Gerenciamento.

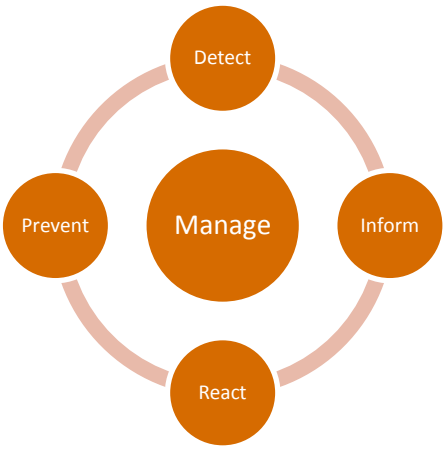


Diagram 2 Five Roles

**Prevenção**: Em primeiro lugar, nós garantimos o total controle do Banco sobre a sua infra-estrutura de Internet. Estamos falando sobre o domínio principal do Banco (www.a-bank.com), sites e aplicações web. Nós garantimos que essas áreas estão livres de Código Malicioso livre e sem risco para hospedar códigos maliciosos no futuro. Esta é uma situação lamentável quando o próprio website Banco é a fonte de infecção para os seus clientes. Os exemplos são do Banco do Índia e a Embaixada da Síria em Londres , ambos em 2007.

**Detecção**: Nós detectamos códigos maliciosos de várias maneiras. Em primeiro lugar, procuramos detectar em tempo-real os usuários do homebanking que estão usando os computadores infectados ou comprometidos. O banco poderá avisá-los, enviando-os para uma página específica, ou chamá-los. Em segundo lugar, nós executamos um software robô de crawling em toda a infra-estrutura que vai à caça de códigos maliciosos na web e tenta encontrar amostras assim que elas são criadas para que os bancos possam atuar e minimizar os danos que estes ataques poderiam causar.

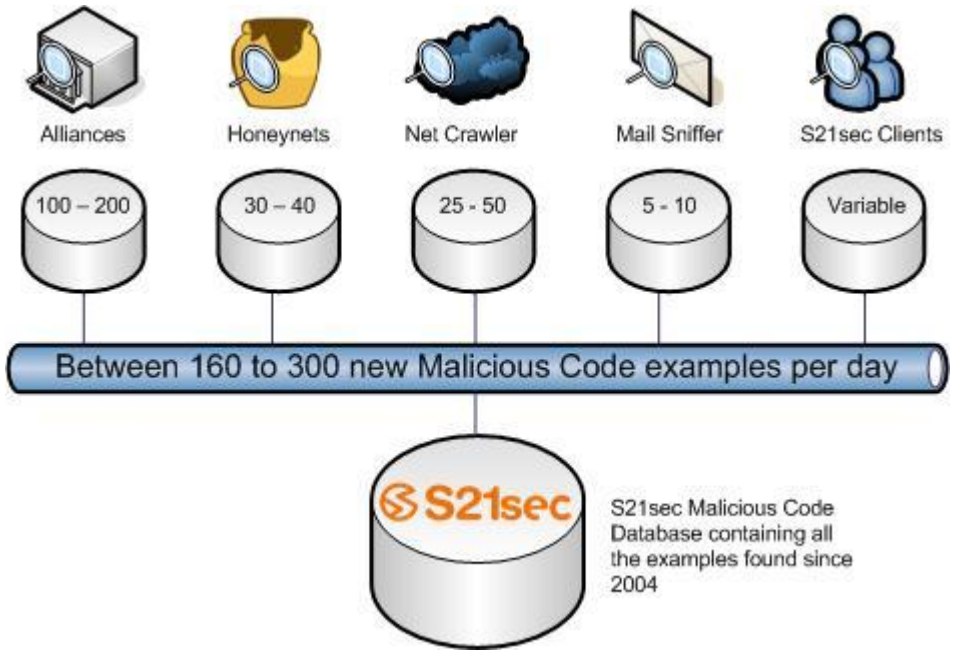


Diagrama 3: Infra-estrutura de Web Crawling

**Informes**: Realizamos análise e inteligência em três áreas diferentes. Em primeiro lugar, analisamos o Código Malicioso recolhido no estágio anterior. Estes relatórios são muito úteis para minimizar o risco de o Código Malicioso especialmente criado para o Banco em particular.

Em segundo lugar, criamos relatórios periódicos de inteligência, onde falamos sobre as tendências mais gerais dentro da comunidade de código malicioso penal: vetores de infecção, sites e canais de controle, e sites de informação. Nós olhamos como o Código Malicioso interage através da criação de usuários de testes de home banking, incluindo atividades incomuns que pode ser descobertas e recomendações sobre as medidas defensivas que podem ser implantadas.

Em terceiro lugar, procedemos com investigações sob medida para os bancos. Estas investigações poderão ser de cerca de cepas específicas de códigos maliciosos, ou pode ser relativo a sistemas de autenticação e de que maneira códigos maliciosos interage e as formas de subvertê-los.

**Reação**: Há quatro áreas de reação ativa às ameaças de códigos maliciosos detectados. Em primeiro lugar, interromper o funcionamento das redes de códigos maliciosos por meio do bloqueio da infra-estrutura que os autores de códigos maliciosos estão utilizando para a distribuição de códigos maliciosos e coleção de dados e de informações. Nós fechamos os sites que atuam como vetores de infecção ou de estruturas de controle e de comando para o código malicioso. Nós também encerramos os endereços de e-mail e os nomes de domínio que fazem parte desta estrutura.

Em segundo lugar, enviamos informações para os provedores de antivírus (A/V), fornecedores de navegador da Web e distribuidores para incluir o novo código malicioso nos sites que fazem parte dos vetores de distribuição. Isso garante a rápida adoção de proteção seja com A/V através de navegadores web (por exemplo IE8 Anti-Phishing e barra de ferramentas anti código malicioso) para proteger a base de usuários de clientes do banco que usam seus sites. .

A terceira reação é a de recuperação de dados. Estamos ativamente atentos à infra-estrutura dos autores de código malicioso com o objetivo de obter as credenciais roubadas dos usuários. Ao mesmo tempo, excluímos estas informações da infra-estrutura criminosa. Isso reduz o risco de que as credenciais roubadas sejam utilizadas de forma fraudulenta e permite ao banco tomar medidas para encerrar ou observar de perto as contas afetadas. O sucesso da recuperação dos dados depende dos autores de códigos maliciosos serem negligente em seus protocolos de segurança. Experimentamos uma taxa de sucesso de 1 em cada 5 casos, ou cerca de 20%.

A quarta maneira como reagimos é de ativar uma isca. Estas iscas são contas especiais ou as credenciais de um usuário fictício que o banco sabe que vai ser explorada por criminosos. Nós ajudamos o banco a carregar as credenciais para a infra-estrutura de controle do código malicioso. Isso resulta em evidência para as Agências de Aplicação da Lei enquanto os bancos observam o fluxo de dinheiro para fora destas contas para a infra-estrutura criminosa.

A forma final para responder a incidentes é via remota forense. A S21sec envia por e-mail um arquivo executável em um computador suspeito do banco. Isso pode estar dentro da própria

rede do banco (por exemplo, um laptop do diretor) ou o de um cliente. O executável instala um módulo do programa Bitácora Horizon, com capacidades para analisar o sistema e recuperar códigos maliciosos na máquina e enviar os binários para S21sec para análise. Esta análise forense remota não pode substituir uma verdadeira análise física, mas continua a ser uma técnica muito útil, que pode ser implantada rapidamente em qualquer local para resultados rápidos.

**Gerenciamento**: Nós fornecemos um portal web como interface para o Banco – chamado de Unified Management of Security Services (UMSS). Este portal fornece um ponto único de contato com S21sec e o Banco que contratou os serviços. Ele fornece relatórios, fluxo de trabalho e um painel. Isso melhora a visibilidade do serviço que está sendo fornecido pela S21sec e torna mais fácil a demonstração de seus benefícios para justificá-lo aos níveis superiores de Gerência. Ele reduz o tempo que a equipe de segurança precisa empregar em gestão e treinamento de como utilizar o serviço.


**Diagrama 5: Código Malicioso: Visão Geral dos Serviços**

## Sumário de benefícios dos Serviços Anti-fraude da S21sec

Podemos controlar o risco que Código Malicioso impõe ao seu banco. Podemos prover inteligência, análise e resposta a incidentes além da recuperação de dados. Os benefícios são:

- Perder menos dinheiro para as fraudes
- Gastar menos dinheiro gerenciando casos de fraude
- Reduzir o risco de multas regulatórias
- Reduzir o risco de insatisfação do cliente e da migração para a concorrência
- Reduzir o risco de exposição negativa na mídia
- Reduzir o risco com a imagem da marca
- Aumentar a inteligência e a compreensão das operações criminosas
- Gastar dinheiro apenas nas contramedidas eficazes e eficientes para lidar com a ameaça de Código Malicioso

Quais as nossas diferenças para as demais soluções do mercado?

- **INTEGRIDADE** - Nós colocamos ênfase na verificação de integridade e na garantia de que seus sites estão livres de códigos maliciosos, para eliminar os riscos de multas por auto-hospedar códigos maliciosos.
- **REAL-TIME -** Oferecemos detecção em tempo real dos clientes suspeitos com base no comportamento.
- **QUALIDADE -** A qualidade da nossa informação é World Class assim como os benefícios que você ganha com isso.
- **RESPOSTA** - Não somos apenas capazes de estudar o código malicioso e fornecer informações. Nós fornecemos os serviços de resposta mais abrangente disponível: Bloqueio da infra-estrutura Criminal, Estreita colaboração com provedores de A/V e de Browser, Serviços de recuperação de dados, Ativação de isca e Forense remota.
- **SOLUÇÃO PERSONALIZADA -** Nós podemos personalizar a nossa oferta às suas necessidades para que você não pague por um serviço que você não precisa.
- **SEM INSTALAÇÃO** – Nada para instalar no cliente: serviço prestado a partir do SOC da S21sec.
- **TARIFÁVEL -** Relatórios completos mensais e painel de instrumentos para gerenciar e justificar os serviços.
- **ROI –** Investimentos justificáveis: os nossos serviços se justificam após dois meses de serviço.

Por favor, entre em contato para coordenar um piloto de 2 meses de prestação de servicos para avaliação, sem custo e sem compromisso.

David Oliveira e Eraldo Schiola

david.oliveira@tec10.com.br e eraldo.schiola@tec10.com.br

www.tec10.com.br

+55.11.3813.7266