*[S21sec]

A segurança digital do futuro, hoje no BRASIL

*[Serviço Anti-Fraude]

Dezembro 2009

tec10
CyberIntelligence

Quem somos e onde estamos

Quem somos

Empresa especializada em serviços de segurança da informação:

- Líder e referência no setor da segurança digital.
- Fundada no ano 2000 para prevenir e gerenciar o risco das organizações e das pessoas na vida digital.
- Contribui para a criação de uma verdadeira cultura de segurança nas organizações.

S21sec está dedicada exclusivamente à Segurança da Informação

Onde estamos: âmbito de atuação internacional e estratégia de expansão

- 6 escritórios na Espanha
- 3 escritórios internacionais
- 1 parceiro internacional (Brasil – Tec10)

FATORES QUE PERMITEM NOSSA INTERNACIONALIZAÇÃO

• Conhecimento do mercado : Os ataques são globais e se utilizam mundialmente das mesmas técnicas

•Modelo de serviços e gerenciamento 24x7

• Uma das melhores equipes de segurança digital do mundo

: alianças e colaborações

Internacionais

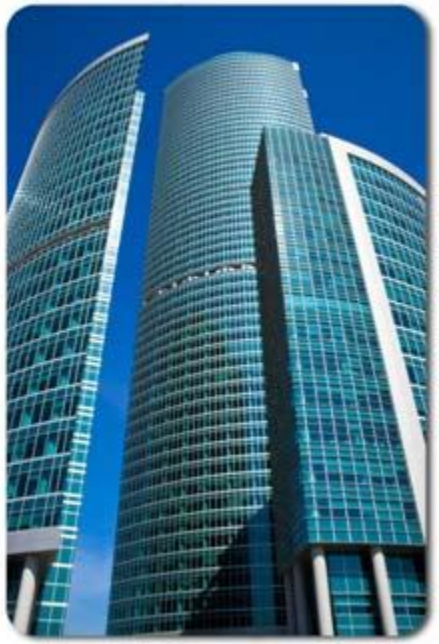
- OTAN
- Interpol
- Europol
- Carnegie Mellon
- Microsoft (BTF)
- Digital Phisnet
- FIRST
- APWG
- ENISA
- VeriSign
- Principais companhias privadas (Team Cymru, iDefense, CSIS)

Na Espanha

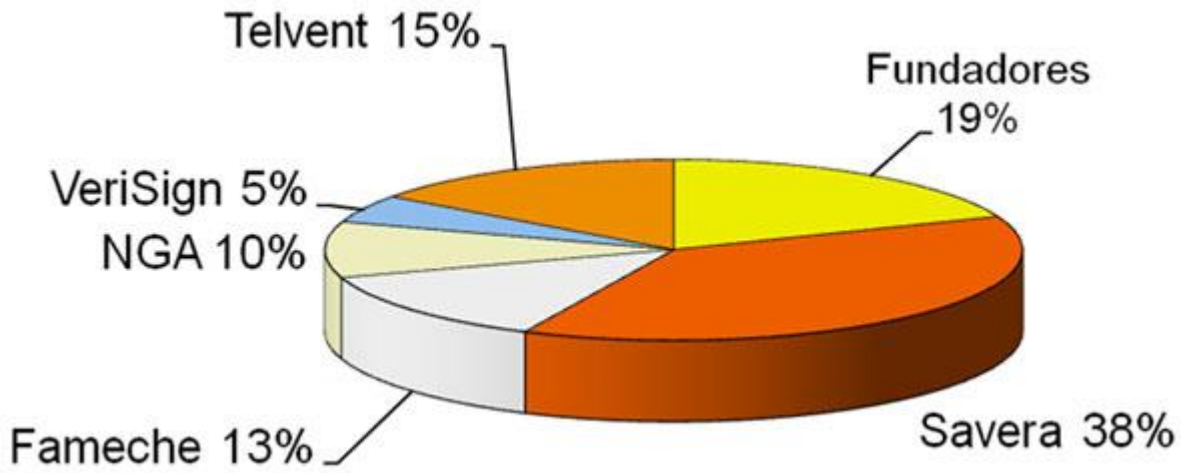
- Ministério da Defesa
- CCN-CERT
- Guarda Civil
- Polícia Nacional
- Mossos
- Ertzaintza
- Cátedra Serviços de Inteligência e Sistemas Democráticos
- RedIris
- INTECO

Confiança de grandes clientes

- 26 das 35 companhias do IBEX
- 20% das companhias do índice Eurostoxx
- 90% do setor financeiro Espanhol
- Organismos e instituições das administrações públicas
- As principais companhias de telecomunicações entre elas Telefônica e Movistar
- Companhias de comércio eletrônico, *utilities* e construção
- As maiores linhas aéreas nacionais e companhias de transporte e logística
- Defesa e Forças de Segurança do Estado
- Setor Médico (Sanofi, Grifols, etc..)



Confiança dos nossos acionistas



Composição acionária em março de 2008

S21sec labs : colaboramos com especialistas

Centros de conhecimento:
Universidades e centros tecnológicos

tec10 S21sec

S21sec labs : colaboramos com especialistas

Sócios de alto nível

VeriSign

Microsoft

McAfee

TippingPoint

cisco

TELVENT

MELBOURNE IT

S21sec labs : colaboramos com especialistas

Em grandes projetos de P+D+i

segur@

identica

SEGURIDAD 2020

CDTI
Centro para el Desarrollo Tecnológico Industrial

SEVENTH FRAMEWORK PROGRAMME

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

tec10 S21sec

Nossa força

tec10
CyberIntelligence

O que nos diferencia:
Uma equipe especializada em segurança

- 100% dos nossos profissionais dedicados exclusivamente a segurança
- 250 pessoas com o único objetivo de zelar pela segurança dos sistemas de Informação e Comunicação.
- Profissionais reconhecidos internacionalmente e certificados dentro da área de segurança digital.

SEI Partner

Microsoft

CISA
Certified Information Systems Auditor

Certified Information Systems Security Professional
CISSP

GIAC

CISCO

CISM
Certified Information Security Manager

tec10

S21sec

O que nos diferencia: INOVAÇÃO
O primeiro centro europeu de P+D+i em Segurança

- Investimentos desde o princípio de mais de 25% dos recursos ao P+D+i

- Criação do primeiro centro europeu em P+D+i especializado em segurança digital

- Um passo adiante: A inovação como motor do negócio
  - Desenvolvimento de tecnologias de ponta em segurança para a melhoria contínua de nossos serviços e fazer frente as novas necessidades.

S21sec labs

tec10 S21sec

O que nos diferencia: qualidade e certificações

- 4 certificações da AENOR como reconhecimento à gestão da qualidade, à gestão da segurança da informação, à gestão do P+D+i e aos processos do ciclo de vida do software.

- Primeira empresa espanhola certificada para prestação de serviços de cumprimento às normas PCI-DSS como ASV y QSA.

- Homologados para suportar o programa de certificação de prestadores de serviço ASIMELEC

- Certificados e homologados pela Microsoft como provedores de serviços de diferentes instituições.

APPROVED SCANNING VENDOR

QUALIFIED SECURITY ASSESSOR

Unidades de negócios

tec10
CyberIntelligence

Unidades de negócios

Todos nossos serviços englobam o ciclo completo da segurança

S21sec UMSS
Unidad de Servicios Globales de Seguridad

- Consultoría estratégica
- Serviços 24x7: Compliance, gestão de dispositivos, avaliação de segurança, formação e conscientização

S21sec e-crime
Unidad de Inteligencia

- Fraude
- Vigilância Digital
- Inteligência

S21sec tech
Unidad de Productos

bitacora

S21sec university
Unidad de Formación

- Formação especializada
- Planos de carreira
- Cursos Online

S21sec labs
Unidad de I+D+i

- Avaliação de produtos
- Observatório tecnológico
- Pesquisa e desenvolvimento

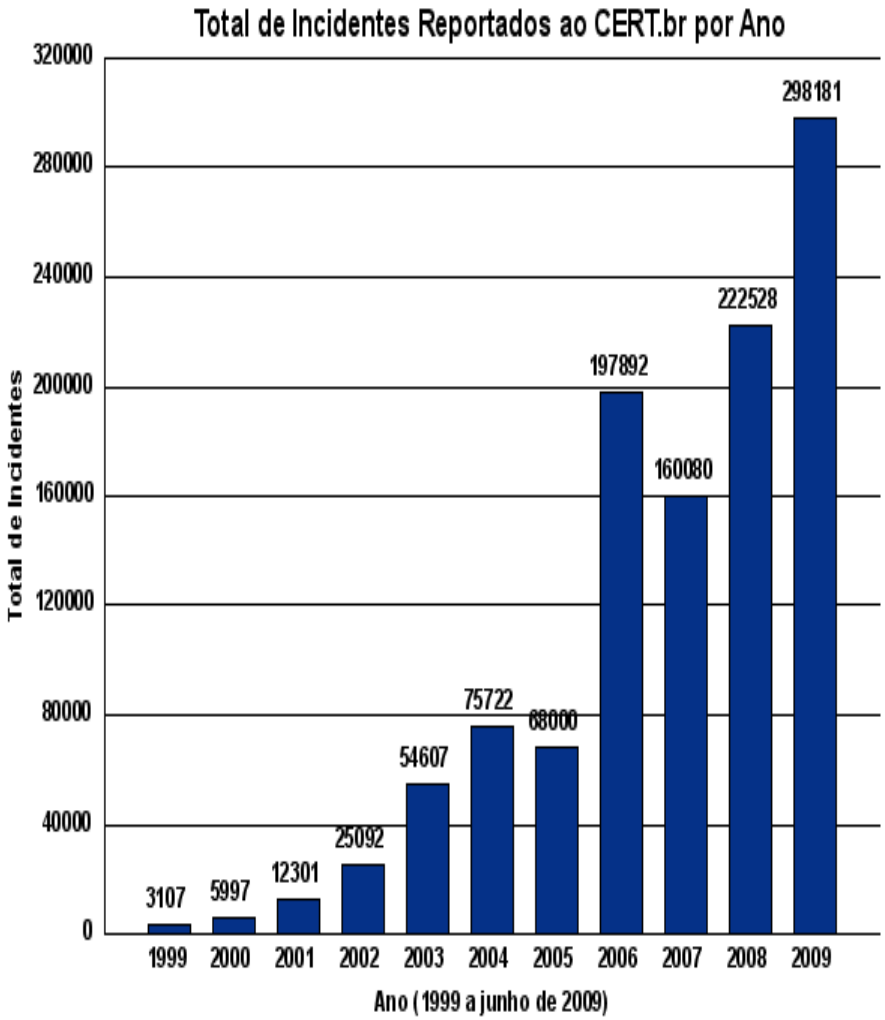
S21sec e-Crime

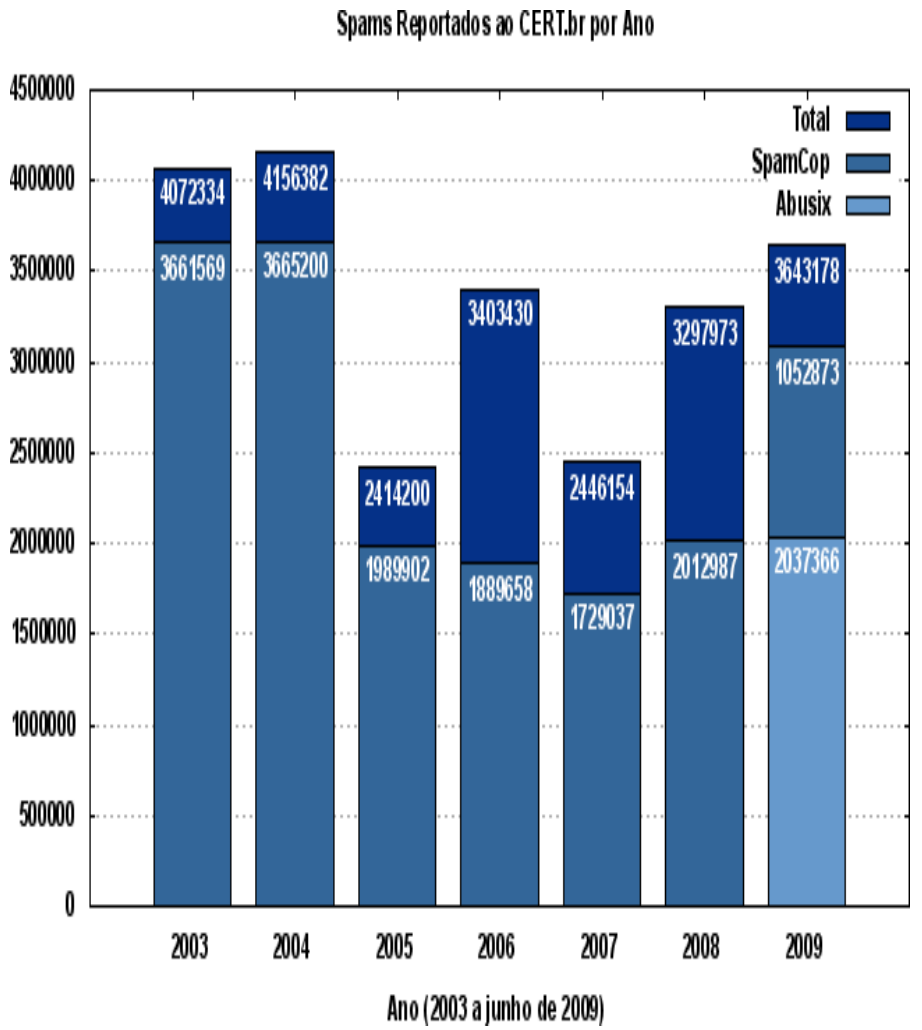
Serviços Anti-Fraude

O que enfrentamos ?

tec10
CyberIntelligence

Incidentes no Brasil (Fonte: cert.br)





Quais os riscos e os custos de um Código Malicioso?

tec10
CyberIntelligence

Riscos e Custos do Código Malicioso

- Perdas diretas com as fraudes por transferência de dinheiro
- Perdas indiretas da gestão de casos, de aconselhamento de clientes e de investigação interna
- Multas, processos e penalidades dos órgãos competentes por hospedagem de códigos maliciosos e perdas de dados
- Desperdício do investimento na solução atual de segurança bancária e dos mecanismos de autenticação
- O aumento de investimento em contramedidas
- Experiências negativas e redução na confiança dos clientes
- Migração dos clientes para a concorrência
- Aumento da atenção da mídia nos incidentes de segurança do banco
- Perda de confiança, dano à imagem corporativa e à marca
- Custos diretos com campanhas de marketing para reabilitação e recuperação da credibilidade.

Estudo de Caso

O impacto de um ataque de Código Malicioso

tec10
CyberIntelligence

Estudo de Caso – Melhor cenário

- Identificamos de 4 a 5 novos Malwares por dia = 120 ataques por mês
- Recuperamos em média 15 credenciais roubadas por ataque

- Consideraremos 5 ataques bem-sucedidos por mês
- Consideraremos 10 usuários comprometidos por ataque
  - 50 clientes afetados por mês.
  - 600 clientes por ano
- € 1500 perdas diretas por usuário.
- 10 horas-homem para cuidar de cada caso: € 1000

	Mês	Ano
Perda Direta (€)	75.000	900.000
Perda Indireta(€)	50.000	600.000
TOTAL(€)	**125.000**	**1.500.000**

Estudo de Caso – Pior cenário

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

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

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

Estudo de Caso – A amplitude do ataque

	Melhor Cenário	Pior Cenário
Desperdício na solução atual		500.000
Investimento em novas contramedidas		300.000
Custos diretos	900.000	900.000
Custos indiretos	600.000	600.000
Multas		100.000
TOTAL	**€1.500.000**	**€2.400.000**

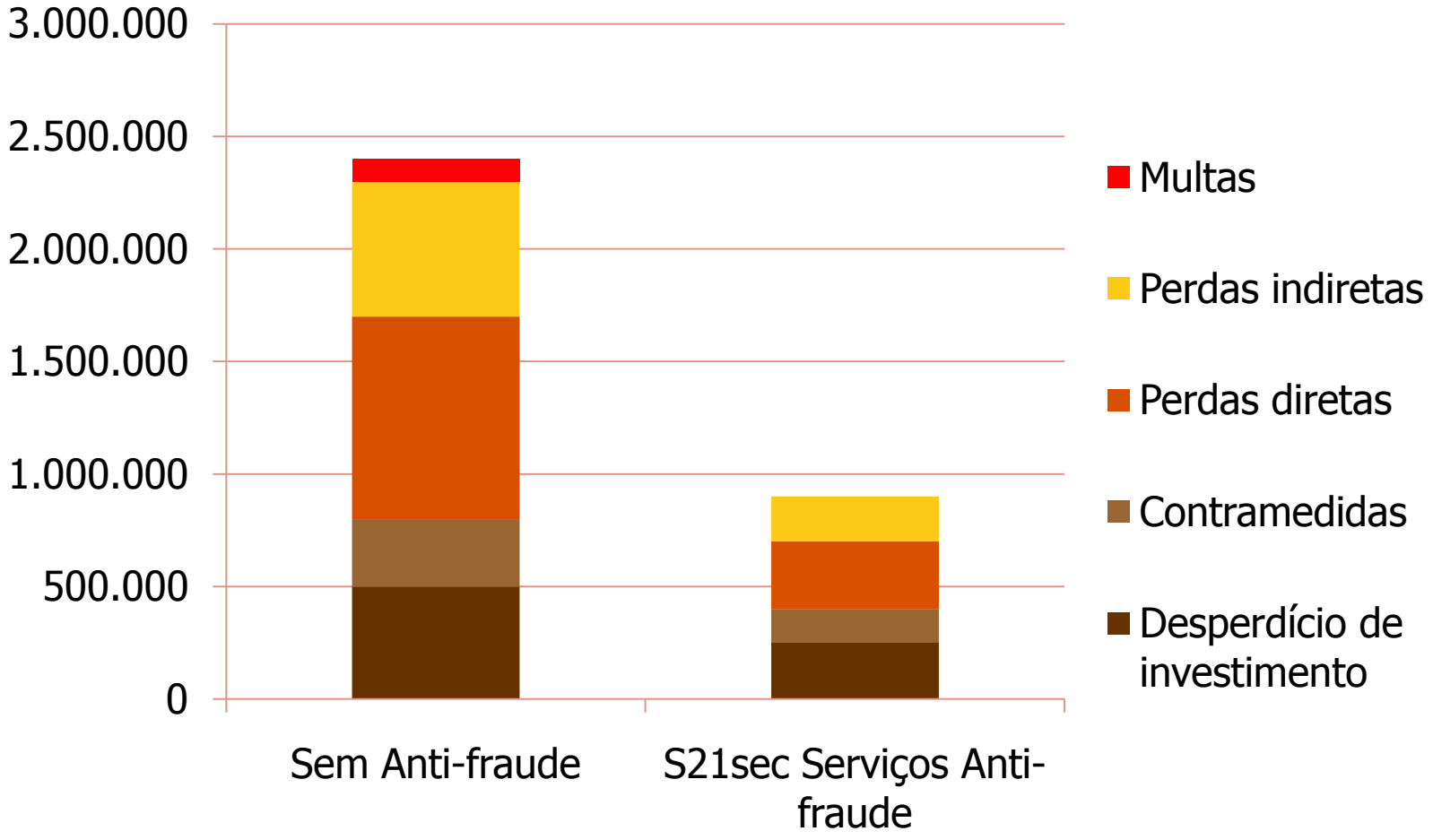
Como a S21Sec muda este cenário?

- Salvar investimento em segurança (50%)
  - Varredura diária dos Websites para identificar vulnerabilidades e códigos maliciosos
- Contramedidas (50%)
  - Inteligência
  - Eficácia e eficiência
- Custos diretos e indiretos (66%)
  - Reduzimos período de atuação: de 60 para 20h
  - Detectamos os clientes para evitar transferências
- Sem multas

Quadro comparativo com S21Sec

	Pior Cenário	Com Anti-fraude
Desperdício na solução atual	500.000	250.000
Investimento em novas contramedidas	300.000	150.000
Custos diretos	900.000	300.000
Custos indiretos	600.000	200.000
Multas	100.000	
TOTAL	**€ 2.400.000**	**€ 800.000**

Quadro comparativo – Custo Annual (€)



Descrição dos Serviços Anti-Fraude

tec10
CyberIntelligence

Características do serviço

Características do serviço

Prevenção

- Lista negra de URL's
- Prevenção de Web Malware Testes de Integridade
- Difusão de URL's maliciosas

Detecção

- Detecção em tempo real de código malicioso nos clientes.
- Detecção de "Phishing"
- Monitoramento de registro de domínios
- Monitoramento de Envenenamento de DNS (*Pharming*)
- Monitoramento de reabertura de casos de url maliciosas.
- Lista de IP's infectados

Informes de Inteligência

- Informativos do Serviço de Inteligência
- Rede de clientes dos serviços antifraude.
- Análise manual de código malicioso
- Análise remota de código malicioso
- Informativos sob demanda

Reação

- Recuperação de informação e Credenciais
- Colocação de Iscas
- Fechamento de Sites
- Serviços de solução de infecções sob medida

Gerenciamento

- UMSS

tec10 S21sec

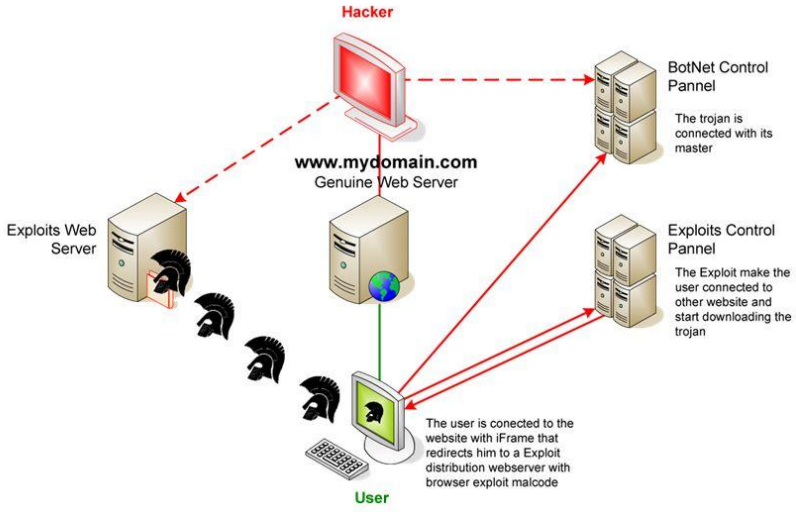
Prevenção de Fraude – Webmalware*

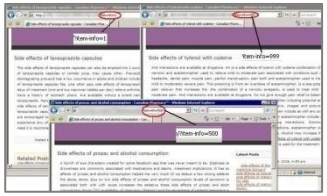
Prevent

- URL Blacklist
- WebMalware* Prevention Service
- Dissemination of Malicious URLs
- Vulnera

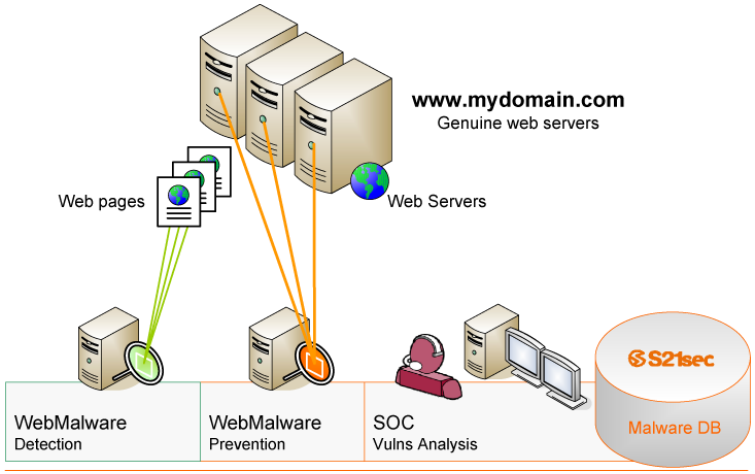
Uma análise diária dos sites web para comprovar que não tem nenhum tipo de vulnerabilidade que possa permitir aos criminosos enviar arquivos diretamente aos sites dos nossos clientes.

Problema





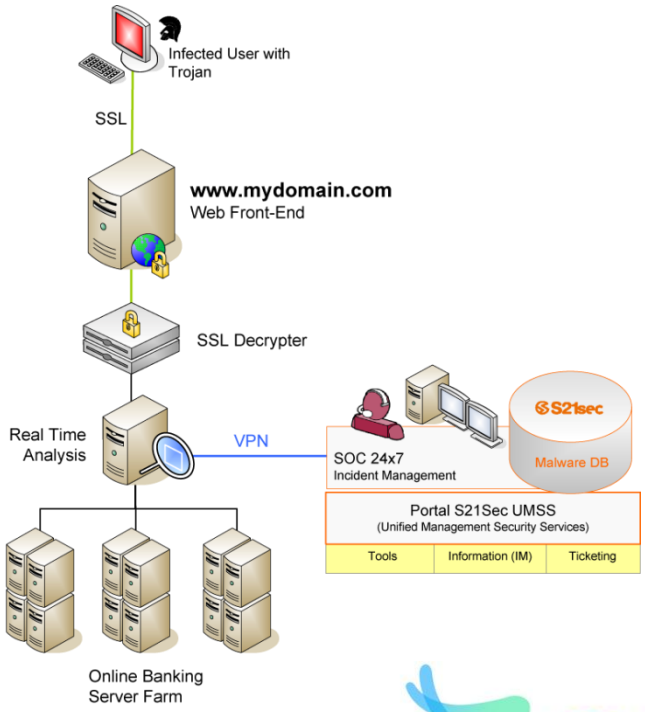
Solução



tec10 S21sec

Detecção de Fraude em Tempo Real

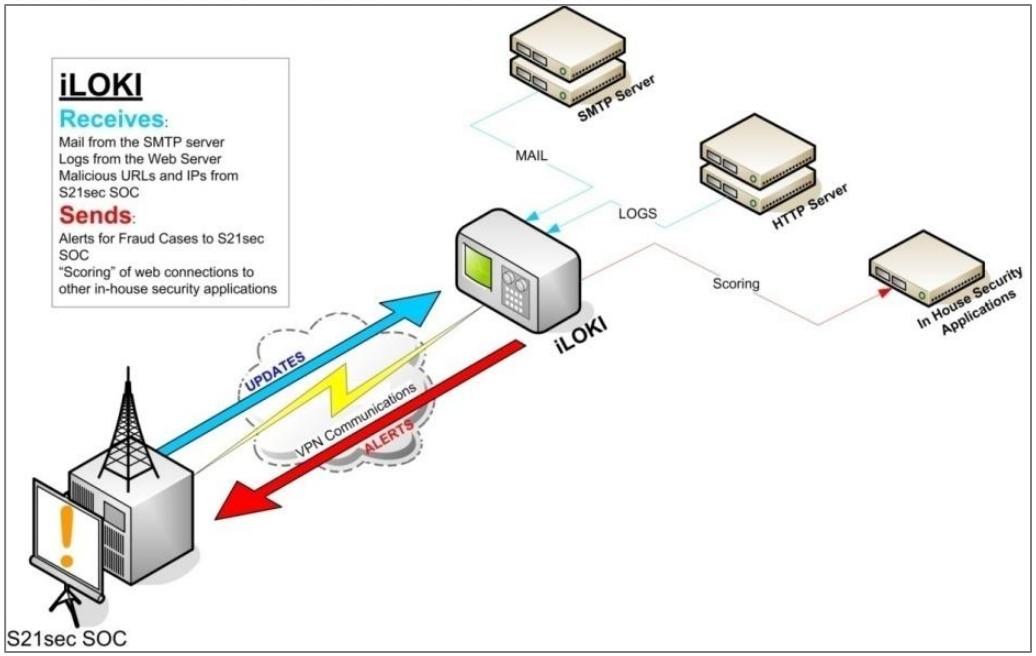
Mediante estudos do comportamento dos exemplos de códigos maliciosos que dispomos, somos capazes de detectar clientes infectados a partir da análise do lado do servidor. Isto permite a detecção de clientes infectados em **TEMPO REAL,** e realizar ações diretas, como limitar as transações econômicas ou redirecioná-los a uma área segura da web para receber conselhos de como reparar o incidente.



tec10 S21sec

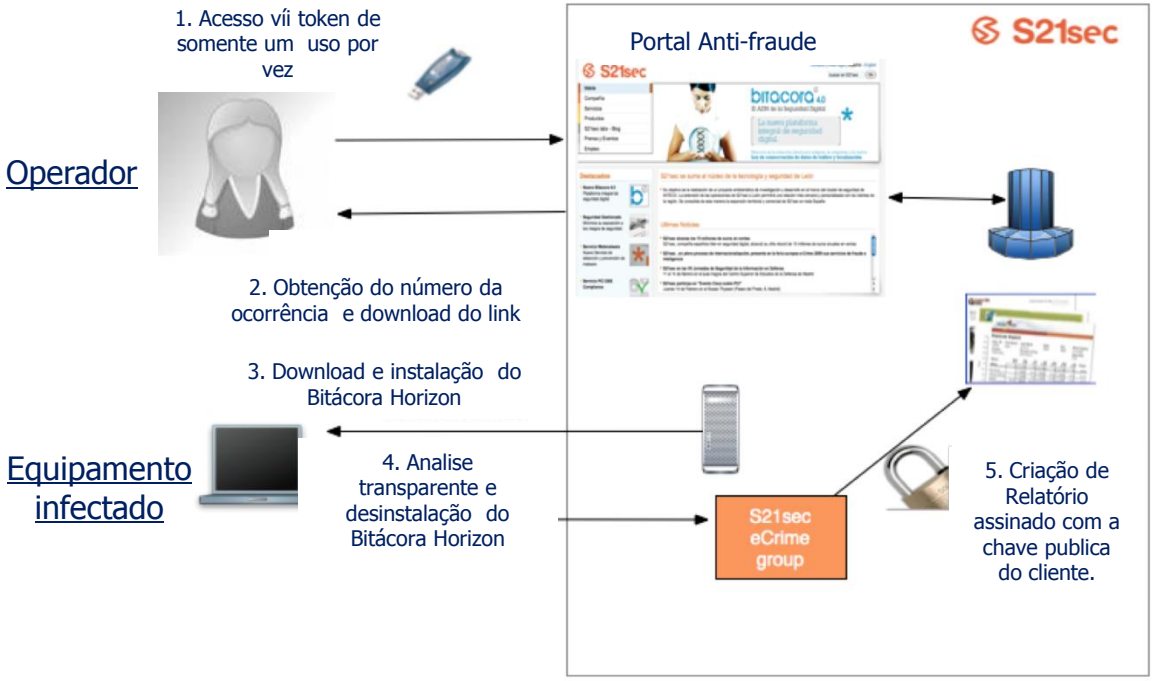
Detecção de Fraude – Detector de Abuso

Um dos melhores lugares para recolher informações sobre ataques antes que eles ocorram, é a partir da web e dos servidores de e-mail dos clientes. Para isso, instalamos uma caixa de detecção de Phishing dentro da rede do cliente que busca sinais de atividade fraudulenta, sem comprometer nenhum sistema de segurança ou configuração da rede.



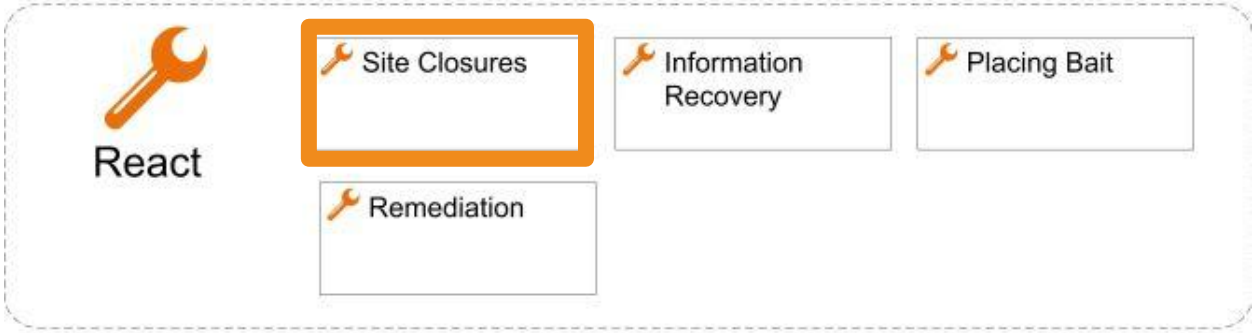
tec10 S21sec

Inteligência – Análise Remota



6. O cliente é alertado via e-mail da disponibilidade dos informes que são criptografados e assinados digitalmente e são acessíveis através do portal .

Resposta a Fraude – Fechamento de sites



Fechamos sites fraudulentos e infra-estruturas criminosas em tempos recordes. 5 horas em média após a detecção da fraude. Este serviço é totalmente gerenciado a partir do nosso SOC Europeu em Madrid.

tec10 S21sec

Gestão do serviço

Manage

- SOC 24*7
- eCrime Portal – Key Metrics Dashboard
- Reporting: Monthly Service Reports
- Outsourcing: Fraud Specialists in your team

Os clientes dispõe de um portal dedicado para gerenciar e utilizar os serviços de e-crime que foram contratados.

As grandes diferenças da S21sec

tec10
CyberIntelligence

As grandes diferenças da S21Sec

- **INTEGRIDADE** – Ênfase na verificação de integridade e na garantia de que seus sites estão livres de 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 dos SOC´s da S21sec em Madrid e em Pamplona
- **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.

Casos & Referências

Companhias que depositam sua confiança nos serviços da S21sec.

tec10
CyberIntelligence

Referências do Setor Financeiro

- Santander
- La Caixa
- Bancaja
- Caja Ahorros Mediterráneo
- Banesto
- Banco Sabadell
- Banco Pastor
- Caja Madrid
- Sermepa
- 4B
- Red6000.....etc……..

- 90% destes bancos são clientes do nosso serviço anti-fraude.
- 70% deles tem o serviço de auditoria da S21sec.
- 30% utilizam o Bitácora, nossa ferramenta SIEM
- 10% contrataram nosso serviço de Vigilância Digital.

BBVA (Contrato Mundial)

- Serviço gerenciado de segurança perimetral. Gestão dos dispositivos de segurança.
- Serviço de detecção de fraude (FDS)
- Serviço de auditoria de segurança lógica da infra-estrutura e aplicativos.
- Serviço antiphishing, antipharming, antimalware e análise remota.
- Gestão de logs e correlação de eventos através do Bitácora (ferramenta SIEM desenvolvida pela S21sec)
- Auditorias de conformidades às políticas de segurança.
- Especialistas em segurança S21sec na equipe do BBVA.

SEPA – Single Euro Payment Area

- Desconto nos serviços para os bancos associados.

*[Muito Obrigado]

Eraldo Schiola
eraldo.schiola@tec10.com.br
+55-11-3813.7266
+55-11-9656.4022

David Oliveira
david.oliveira@tec10.com.br
+55-11-3813.7266
+55-11-9185.1383

www.tec10.com.br

tec10
CyberIntelligence