

The background is an abstract, textured image with shades of blue and teal. A prominent diagonal line runs from the top right towards the bottom left, separating the image into two main sections. The texture appears like water or a rough surface.

Modelo de ameaças dirigidas a cenários de ataques

Aplicação prática

Venda de informações vazadas

Empresa de SP vende informações sigilosas em site comentários

03 de julho de 2009 • 20h47 • atualizado às 21h10

NOTÍCIA

APinformação
Informações para crédito e cobrança

Sobre nós Assine Agora Esqueci minha senha

Retorno	End/Tel	Cheque	Pendência
Últimas consultas	✓	✓	✓
Síntese Cadastral	✓	✓	✓
Endereço	✓	✓	✓
Telefones (fixos e/ou celular)	✓	✓	✓
Telefones próximos (vizinhos)	✓	✓	✓
Possíveis familiares (mãe e irmãos)	✓	✓	✓
Renda presumida			✓
Cheques sem fundos		✓	✓
Pendências financeiras			✓
Protestos, Ações e Falências			✓
Dados do Veículo			
Preço da consulta - R\$⁽²⁾	0,08	0,20	1,55
Veja modelo do consulta			

(2) Mensalidade: R\$ 25,00 + consultas

- O que aconteceria com sistemas que usam informações cadastrais para valiar o risco de **liberação de crédito** para uma pessoa? Será que isso facilita a fraude no sistema financeiro?
- No caso ao lado, milhares de dados sobre **situação de crédito** de muitos brasileiros estavam a disposição de fraudadores.

Venda de informações vazadas

Venda de informações sigilosas na rua em SP preocupa autoridades

Deputado estadual teve seus dados entre os vendidos na Santa Efigênia. Para polícia, venda de informações pessoais ajuda em ações criminosas.

Do G1, em São Paulo, com informações do Jornal Hoje

Tamanho da
letra
A- A+



A venda de informações sigilosas em CDs na Rua Santa Efigênia, no Centro de São Paulo, **revelada nessa terça-feira (24) pelo Jornal Hoje**, preocupa as autoridades. De acordo com a polícia, os dados podem servir para ações criminosas que vão de seqüestros a golpes bancários. Nos CDs aos quais a reportagem teve acesso, estavam informações que vão de registros do Imposto de Renda até dados cadastrais do Detran. A venda de informações sigilosas é crime previsto por lei.

- Não é qualquer tipo de informação que tem apelo de venda, portanto, não há estímulo ao seu vazamento. Mas o que aconteceria com sistemas que usam informações pessoais para efetuar algum tipo de PID (processo de identificação de uma pessoa baseado em dados que apenas aquela pessoa saberia sobre ela mesma - **personally identifiable information (PII) data**).
- No caso ao lado, milhares de dados sobre os cidadãos brasileiros como IRPF, dados do DETRAN etc. a venda.

Venda de informações vazadas

26/01/2011 18h21 - Atualizado em 26/01/2011 18h21

LG expõe dados pessoais de mais de 71 mil clientes brasileiros na rede

Arquivo com nome e endereço de clientes estava junto com manual on-line. Empresa culpa ataque hacker e diz que já tomou providências sobre o caso.

Do G1, em São Paulo imprimir



O site da LG expôs dados pessoais de mais de 71 mil clientes brasileiros na internet. As pessoas tiveram disponibilizados, no link que daria acesso ao manual on-line do telefone celular LG GT540, seus nomes completos, endereços, CPF, datas de nascimento e números de telefone.

Segundo reportagem publicada no site do jornal "Folha de S.Paulo", as informações ficaram disponíveis até domingo (23).

A LG afirmou que entre sábado (22) e domingo (23) seu site foi invadido e que "já tomou as providências para que isso não ocorra novamente". Na segunda-feira (24), a lista não estava mais disponível.


Manual on-line do smartphone LG GT540 (foto), apresentou dados de clientes. (Foto: Divulgação)

- Muitos ambientes que operam ações críticas como o sistema bancário lançam mão de processos de autenticação forte, sendo o envio de mensagens para um dispositivo móvel, um desses métodos. O que aconteceria se todos os dados de um proprietário de celular vazassem, esse método ainda seria confiável?
- No caso ao lado, os dados cadastrais de 71 mil clientes vazaram. Colocando esses 71 mil em um potencial de risco muito maior.

Phishing – explorando a confiança do atacado

Phishing personalizado: Nome completo + número no programa de milhas

>>> Dados da TAM vazam e são usados em golpe virtual



É normal que golpes na web utilizem o nome de empresas conhecidas para atrair as vítimas. No entanto, circularam nas últimas semanas e-mails maliciosos que usam não apenas o nome, mas dados da companhia aérea TAM. As mensagens acompanham o nome completo da vítima e também o número do cartão de fidelidade.

Em nota à imprensa, a TAM admitiu que golpes com o nome da empresa e dados do cliente estão em circulação desde o dia 14 de dezembro. Nenhuma explicação a respeito de como os criminosos obtiveram os dados foi fornecida.

O golpe informa à vítima que a TAM estaria oferecendo uma viagem nacional gratuitamente. Para obter mais informações, é preciso abrir um arquivo. O link termina em ".doc", porém o internauta é imediatamente redirecionado a um arquivo executável (".exe"). Se executado, o software malicioso instala ladrões de senhas bancárias.

TAM Linhas Aéreas S/A - Av. Jaramir, 550 - Lote 4/OP - CEP: 82.913-002/0091-40
Central de Reservas 4062-5700 ou 0800-570-5700 (gratuito não cobradas)
Serviço Fale com o Presidente (atendimento ao consumidor) 0800-123 295.

- Qual a chance de você não interagir com um sistema que te contacta confirmando todos os seus dados “sigilosos”, ids que só esse sistema possui, oferecendo vantagens ou tratamentos proativos de problemas (fraudes).
- No caso ao lado, os dados cadastrais da TAM vazaram, proporcionando aos atacantes criar uma comunicação extremamente dirigida e muito “verossímil” fazendo com que muitos usuários legítimos fossem ludibriados a agirem contra os próprios interesses.

A busca por uma causa - Hacktivismo



- A título de “proteger os cidadãos”, algumas pessoas (eventualmente até com boa intenção), expõe ainda mais os dados pessoais passíveis de vazamento (provenientes de sistemas com brechas).
- No caso ao lado, os dados cadastrais da Tefefônica foram vazados para atrair atenção para uma causa – proteger esses dados contra um vazamento “criminoso”. O que só agravou o caso, acelerando o vazamento e potencializando ainda mais grupos fraudadores que dependem de dados cadastrais.

Crimes comuns com uso de inteligência

Pelo número da placa do carro obtinham informações da vítima

Tópico: banco de dados do Detran SP

16-01-11 16:25 PM

banco de dados do Detran SP

BANCO DE DADOS DO DETRAN ESTADO DE SÃO PAULO
PLACA, CPF, MODELO, ENDEREÇO....

Somente Usuário Registrados podem Ver o Link. Registre-se

Banco de dados do DETRAN oferecido para download

Bando usava site e CDs para roubar mansões

Ladrões faziam lista de placas de carros que encontravam na rua e cruzavam dados para [br]encontrar endereços
10 de fevereiro de 2011 | 0h 00

Quatro integrantes de uma quadrilha que usava informações confidenciais de donos de veículos para invadir residências na cidade de São Paulo foram presos, no início da noite de anteontem, na Avenida Senador Queiroz, no centro da capital paulista.

Durante uma patrulha, policiais militares das Rondas Ostensivas Tobias de Aguiar (Rota) suspeitaram do grupo, que demonstrou nervosismo com a chegada da viatura. Um dos rapazes suspeitos, ao perceber a abordagem, tentou se desfazer de um papel. Os policiais encontraram a folha, que trazia uma lista com nomes, endereços, telefones e placas de veículos, a maioria importada.

Segundo a Polícia Militar, durante o dia, os criminosos faziam uma pesquisa de placas de veículos parados nas ruas e em estacionamentos da região central. A maioria dos carros era de propriedade de chineses, japoneses e coreanos.

Os integrantes do grupo entravam então em um site na internet com essas informações e dados compilados em CDs - comprados, segundo um dos rapazes, na Rua Santa Ifigênia. Por meio do endereço eletrônico, conseguiam levantar dados pessoais dos donos dos veículos, como endereço e telefone.

A quadrilha então telefonava para as residências e, se não houvesse ninguém no local, os ladrões invadiam as casas e furtavam todo tipo de objeto. Mesmo se os moradores estivessem em casa, o bando não desistia do roubo; quando invadiam as residências, aliás, chegavam a agredir algumas vítimas.

Detran na luta contra fraude

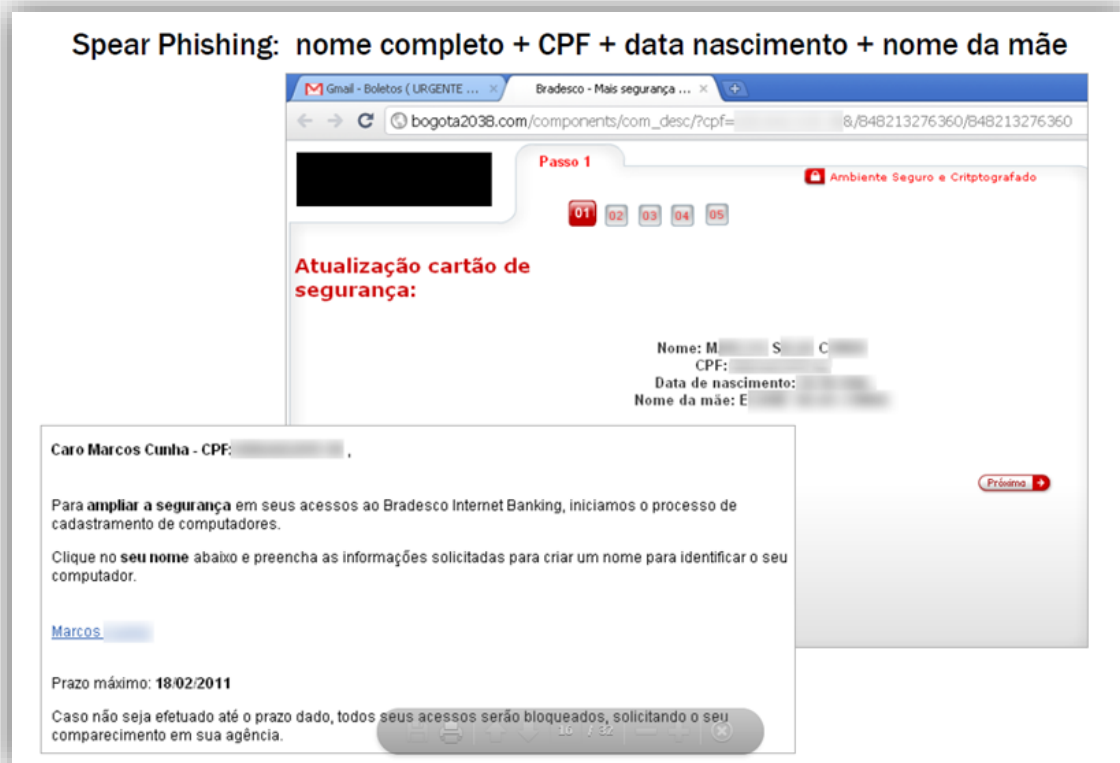
Estado adotou novo sistema eletrônico que capta os números do motor e placa, bem como transmite dados codificados

Publicado em 29/04/2011, às 10h00

Um equipamento para vistoria eletrônica de veículos promete facilitar a vida dos usuários, diminuindo em até 50% o tempo do procedimento. A máquina possui um cabo com uma câmera que consegue captar os números de chassi, motor e placa traseira e transmite dados codificados. O equipamento também armazena a imagem completa do carro. O investimento total foi de R\$ 2,7 milhões.

- Imagine o uso de seus dados e preferências para estimular o comércio eletrônico. O que impede o mesmo tipo de análise de direcionar assaltantes para sua casa para roubarem aqueles obras de arte que você declarou no seu imposto de renda?
- No caso ao lado, o cruzamento de vários dados cadastrais (IRPF, DETRAN, etc.) orientavam o crime organizado como e onde atacar minimizando risco deles e garantindo ao máximo o lucro.

Uso do pânico combinado com dados vazados



- Imagine ser abordado pelo seu “banco” te informando dados legítimos seus e avisando que você tem que tomar ações tempestivas para evitar que todo seu dinheiro seja furtado? Chama-se spear phishing e acontece o tempo todo. Há grupos de fraude criando verdadeiras centrais telefônicas com URAs para dar mais veracidade ao golpe.
- No caso ao lado, o phishing visava a informação obter as informações bancárias da vítima.

Quebra de controle de acesso

Um integração mal feita entre a receita federal e o site do ministério do trabalho permitiu que o atacante construísse uma chamada a uma URL do ministério do trabalho que por sua vez buscava dados sigilosos da Receita Federal (que os entregava, pois confiava em uma origem legítima da requisição – site do ministério do trabalho). Isso permitia acesso irrestrito os dados atualizados da receita federal.

No caso ao lado, o atacante ainda copiou toda a base exposta localmente para consulta, caso a folha fosse corrigida.

A falha

Através de um script PHP copiaram a base de dados completa

```
1. <pre>
2. <?php
3.   if (empty($_GET['cpf'])) {
4.     die("Digite o Cpf");
5.   }
6.   $cpf = $_GET['cpf'];
7.
8.   $f = @file_get_contents
9.
10.  ("http://www.mte.gov.br/validarcpf.asp?nrCPF=" . $cpf);
11.
12.  if (preg_match("/NRCPF/i", $f)) {
13.    preg_match_all("/(.*)"/i', $f, $dados);
```

Sarcastica »» Faça sua Consulta: <http://www.alexgo.org/...> É inteiramente grátis para você. Isso você só tem aqui na CYBERSKYNET.

Vazamentos quebrando controle de acesso

- Esses dados da Receita Federal são muito visados pois são usados em esquemas de grupos fraudadores, tanto para obtenção de crédito, quanto para abrir contas em nomes de laranjas quando eles sabem que seus crimes podem ser rastreados.

Mesmo depois dos sites removidos, para conforto e comodidade do ladrão, criaram um bot local nos canais IRC.
Resultado da consulta em PVT

```
lost100 lcpf [REDACTED]
by_ChUcK lcpf [REDACTED]
by_ChUcK lcpf [REDACTED]
<- by_ChUcK has disconnected (Connection reset by peer)
asteriX lcpf 77416945887
```

```
A!3xG0 Mãe: INEDIALY [REDACTED] MATTOS
A!3xG0 Pai: OLIR [REDACTED]
A!3xG0 Nascimento: 15/12/1981
A!3xG0 Endereço 1 [REDACTED]
A!3xG0 Telefone: (067) 9[REDACTED]
A!3xG0 Nome: ANDREZA [REDACTED]
A!3xG0 Endereço: [REDACTED] COXIM - MS - 79400-000
A!3xG0 Data: 29/09/2010
A!3xG0 Endereço 2 [REDACTED]
A!3xG0 Telefone: (000)
A!3xG0 Nome: ANDREZA [REDACTED]
A!3xG0 Endereço: [REDACTED] - CENTRO COXIM - MS - 79400-000
A!3xG0 Data: 29/09/2010
A!3xG0 Erro: Nenhum usuário encontrado.
A!3xG0 Erro: Nenhum usuário encontrado.
```

Não demorou para criarem uma aplicação de consulta



depois disso alguns bancos passaram a pedir o NOME DO PAI nas transações...

Roubo de identidade

Presos em São Paulo hackers que fraudavam Nota Fiscal Paulista

Dupla possuía senha mestra para acessar valores e desviá-los para conta de terceiro fraudador
21 de outubro de 2010 | 21h 10

SÃO PAULO- Dois hackers foram presos em uma lan house tarde desta quinta-feira, 21, por fraude na Nota Fiscal Paulista. O terceiro membro do grupo, que recebia o dinheiro desviado, não foi preso.

De acordo com o Tenente José Filho, do 48º Batalhão da Polícia Militar, a denúncia anônima a PM foi até a lan house e surpreendeu os dois hackers, que estavam praticando o crime no bairro Jardim Aurora. Eles possuíam acesso ao sistema da receita, que fornecia o número do CPF de diversos contribuintes, então quem tinha dinheiro a receber pela Nota Fiscal Paulista desviavam para a conta bancária de um terceiro membro do grupo.

A polícia estimou que, em uma semana, o golpe causou prejuízo de R\$ 1 milhão. Está sendo procurado o homem conhecido como T3, cujo valor era remetido. O caso foi encaminhado ao 68º DP.

SP muda programa Nota Fiscal Paulista para combater golpes online

Por Redação do IDG Now!
Publicada em 02 de fevereiro de 2011 às 09h56
Atualizada em 02 de fevereiro de 2011 às 17h54

Cibercriminosos desviavam créditos obtidos com o programa por pessoas que ainda não estavam cadastradas; transferências foram limitadas.

O governo do Estado de São Paulo mudou as regras de cadastro e resgate de créditos do programa Nota Fiscal Paulista após descobrir uma onda de golpes online, informou nesta quarta-feira (2/2) o jornal O Estado de S.Paulo.

A partir de agora, transferências de créditos só poderão ser feitas para uma conta corrente com o mesmo CPF informado no cadastro do programa.

- Nesse caso, a quebra do controle de acesso foi usada literalmente para aquisição de recursos financeiros (dinheiro) – apropriar-se de créditos do programa Nota Fiscal Paulista por ter um modelo de negócio frágil que permitia a fraude. O programa permitia que os créditos fossem acumulados em CPFs de pessoas ainda não cadastradas no programa. Os atacantes “criavam” esses cadastros e se apropriavam dos créditos.

Roubo de identidade

Nesse caso, a vítima percebeu o delito quando identificou um montante muito grande de créditos em seu cadastro no programa Nota Fiscal Paulista. Esses créditos eram provenientes de dezenas de dívidas feitas em seu nome, com seus dados legítimos, por estelionatários.

Mecânico tem dados roubados e fica com dívida de R\$ 685 mil

As dívidas são de uma suposta boate, na qual o mecânico Zeferino mora. Na papelada, o trabalhador aparece no lugar.



dívidas de mais de R\$ 685 mil.

Vítima descobre golpe pelo site da Nota Fiscal

Ao conferir seus créditos, jovem encontrou compra de carro por R\$ 24 mil. Ela avisou a polícia e três suspeitos foram detidos.

28 de abril de 2011 | 0h 00

Rejane Lima / SANTOS - O Estado de S. Paulo

O acesso ao site da Nota Fiscal Paulista, da Secretaria da Fazenda de São Paulo, fez com que a analista de sistemas Camila Elena Muza Cruz, de 28 anos, percebesse que estava sendo vítima de um golpe, evitasse o prejuízo e ajudasse a Polícia Civil do Guarujá, na Baixada Santista, a esclarecer três casos de estelionato.

O golpe foi descoberto quando Camila consultou no site do governo quantos créditos do Imposto sobre Circulação de Mercadorias e Serviços (ICMS) tinha a receber e percebeu que, entre as compras com seu CPF, havia um Fiat Palio zero quilômetro no valor de R\$ 24 mil.

"Vi a compra, descobri a concessionária pelo CNPJ e liguei lá. Fui informada que o carro seria entregue naquele dia", diz Camila, que mora em São Paulo e registrou a ocorrência no 28.º DP, na Freguesia do Ó, zona norte, que avisou a polícia do Guarujá.

Investigadores ficaram na concessionária aguardando o comprador e, assim, detiveram a comerciante Erineide Holanda de Araujo, de 29, com documentos falsos em nome de Camila. Ela estava acompanhada por seu companheiro e um amigo. Os três foram encaminhados à Delegacia Sede do Guarujá, onde foram ouvidos e dispensados. "Na abordagem, Erineide não se identificou como Camila e a compra já havia sido feita. Ela não pode ser presa em flagrante e está respondendo por estelionato em liberdade", disse o investigador chefe, Paulo Sergio Carvalhal de Lima.

Roubo de identidade

- Identidades e dados cadastrais são extremamente úteis para dar legitimidade a golpes, bem como, “comprar” de forma “legítima” e pouco rastreável, os ativos usados em crimes. Por exemplo a compra de um domínio que será usado em um golpe usando a identidade de um cidadão de bem, como você. Caso o golpe fosse rastreado, as autoridades chegariam no leitor e não no criminoso.

```
domínio:      gruposantandersa.com.br
entidade:     ██████████ Caseiro Vicente
documento:    ██████████ 098-26
país:         BR
ID entidade:  JACVI10
ID admin:     JACVI10
ID técnico:   JACVI10
ID cobrança:  JACVI10
servidor DNS: ns1.dominios.uol.com.br
status DNS:   06/02/2011 AA
último AA:    06/02/2011
servidor DNS: ns2.dominios.uol.com.br
status DNS:   06/02/2011 AA
último AA:    06/02/2011
servidor DNS: ns3.dominios.uol.com.br
status DNS:   06/02/2011 AA
último AA:    06/02/2011
saci:         sim
criado:        02/02/2011 #7853937
expiração:     02/02/2012
alterado:      02/02/2011
provedor:      UOLHOST (22)
status:        publicado

ID:           JACVI10
nome:         Jos? Antonio Caseiro Vicente
e-mail:        caseirovicente@bol.com.br
criado:        02/02/2011
alterado:      02/02/2011
provedor:      UOLHOST (22)
```



Ministério da Fazenda
Secretaria da Receita Federal do Brasil

Comprovante de Situação Cadastral no CPF

Nº do CPF: ██████████ 098-26

Nome da Pessoa Física: ██████████ CASEIRO VICENTE

Situação Cadastral: REGULAR

Digito Verificador: 00

Cyber Espionagem

- A busca por dados é constante. Os vazamentos ocorrem muito mais frequentemente do que a mídia anuncia. Uma vez que seus dados, i. e. endereço, telefone etc. se tornam de conhecimento público, tornar-se um alvo de espionagem depende apenas do interesse que sua exposição pública atrai.
- Algumas vezes, os sistemas de uma empresa serão alvos de ataques simplesmente pelo tipo de “clientes” que eles atendem. Neste caso, usaram uma falha do WhatsApp para implantar spywares em dispositivos de pessoas publicamente expostas.

WhatsApp detecta vulnerabilidade que permite o acesso de hackers

Empresa pediu aos 1,5 bilhão de usuários em todo o mundo que "atualizem o aplicativo para sua versão mais recente"

Por EFE

© 14 maio 2019, 06h04 - Publicado em 14 maio 2019, 06h03

A vulnerabilidade no sistema, para a qual a empresa lançou um patch na segunda-feira, foi detectada há apenas alguns dias e, por enquanto, não se sabe quanto tempo duram as atividades de espionagem.

Os hackers faziam uma ligação através do WhatsApp para o telefone cujos dados queriam acessar e, mesmo que o destinatário não respondesse à chamada, um programa de spyware era instalado nos dispositivos.

Em muitos casos, a chamada desaparecia mais tarde do histórico do aparelho, de modo que, se ele não tivesse visto a chamada entrar naquele momento, o usuário afetado não suspeitaria de nada.

O WhatsApp assegurou que logo após tomar conhecimento dos ataques, alertou a organizações de direitos humanos (que estavam entre as vítimas da espionagem), empresas de segurança cibernética e o Departamento de Justiça dos EUA.

Hacktivismo

- Explorar ambientes com alta visibilidade – sites de eventos, copas do mundo – grandes eventos de qualquer natureza, trazem a visibilidade para uma causa que o Hacktivista busca. Vulnerabilidades de infraestrutura e com exploração automatizada costumam ser os mecanismos favoritos de exploração desses grupos.
- Neste caso, invadiram o site do PSOL e “pixaram” a página.

Hackers de um grupo chamado 'Pryzraky' invadiram o site do PSOL do RJ nesta semana.

O grupo colocou uma foto de Jair Bolsonaro com a frase “Tem que se fu*** e acabo!(sic) Talkei?”.



Após isso, o grupo modificou a mensagem deixada na página para: “Seu site foi ocupado pacificamente pela Pryzraky, tanto que nenhum dado foi deletado, somos apenas vítimas dessa sociedade opressora e não sabemos o que fazemos”.

Ransomware e variantes

- O ransomware clássico bloqueia seu acesso aos seus dados e sistemas. Mas há variantes, como no caso ao lado. Tráfego gerado para propositalmente sobrecarregar o servidores Web carregando as mensagens de extorsão.
- Esse tipo de ataque torna-se viável quando o grupo criminoso encontra ambientes de empresas vulneráveis e usa esses ambientes (o custo do ataque em termos de banda e servidores fica para empresa) para deflagrar o ataque.

MENU

G1

SEGURANÇA DIGITAL

Segunda-feira, 05/03/2018, às 18:47, por Altieres Rohr

Hackers colocam ameaça de extorsão em tráfego de ataque

Criminosos estão utilizando uma **nova técnica para amplificar ataques de negação de serviços** -- os ataques cuja finalidade é derrubar sites na web. Mas, além de terem quebrado o recorde de tráfego em ataques desse tipo, a nova onda de atividade maliciosa trouxe mais uma novidade, segundo a empresa especializada Akamai: o tráfego de ataque traz em si uma mensagem de extorsão, solicitando o pagamento de 50 criptomoedas Monero para que o ataque seja supostamente interrompido.

Ataques de negação de serviço distribuída (DDoS, na sigla em inglês) inundam um site alvo com tráfego ilegítimo para congestionar a rede e impedir que internautas acessem a página. Nesses novos ataques, os alvos estão recebendo uma enxurrada de mensagens pedindo o pagamento --

10:11:08.223268 IP x.x.x.x.11211 > x.x.x.x.46093: UDP, length 1400
E....@.9...ux2...{...+.....ZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmj
tCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786L
g57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZ
GpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJo
Xi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JF
dwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32
BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR
To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YV
Q7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD
1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtC
KQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg5
7D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGp
oPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi
2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdw
gtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_To_456786Lg57D45CRj5v32BF
BwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghXJoXi2mamQtJd1YVQ7SwXUGDimZGpoPay_50_XMR_T
o_456786Lg57D45CRj5v32BFbBwMzKEmjtCKQfms1nU7JFdwgtEgcwmReMD1HaHGPghX

ataques de
ma empresa,
moedas
\$ 53 mil.

Quadro com tráfego do ataque de negação de serviço. Trecho destacado se repete várias vezes dizendo "Pay 50 XMR to" ('pague 50 Monero para') e o endereço da carteira da moeda virtual. (Foto: Reprodução/Akamai)

Cyberwarfare

- O espaço cibernético é um domínio de guerra. A informação (inteligência), sempre fez parte da guerra, bem como, a desinformação.
- No caso ao lado um possível espião governamental usou de uma invasão para espionar e divulgar informações a público. Se são fakenews ou não, não é relevante. Estabelece-se nesse momento uma guerra de informação que compele cada uma das partes a explorar e detalhar cada vez mais aquela informação. Iniciando a guerra de informação.

Sauditas hackearam CEO da Amazon, diz consultor de segurança

Além de CEO da Amazon, Jeff Bezos também é o dono do jornal The Washington Post, em que escrevia Jamal Khashoggi

Por: **Estadão Conteúdo**
© 31 mar 2019, 09h21 - Publicado em 31 mar 2019, 09h19

Além de CEO da Amazon, Jeff Bezos também é o dono do jornal "The Washington Post", em que escrevia Jamal Khashoggi, um dissidente saudita que foi morto no consulado da Arábia Saudita em Istambul, na Turquia.

O consultor de Bezos afirma que o governo da Arábia Saudita tinha a intenção de prejudicar o empresário desde outubro, quando o jornal passou a cobrir o assassinato de Khashoggi.

Ele disse também que David Pecker, presidente da AMI – a empresa que controla o tabloide "The National Enquirer", que publicou a história da relação de Bezos com a ex-apresentadora de TV Lauren Sanchez – era aliado do príncipe herdeiro da Arábia Saudita, Mohammed bin Salman (conhecido como MBS).

Quem é seu atacante?

Seus atacante mimetizam ao máximo seus ambiente, seus clientes. Antecipe-se a eles ou nunca vai achá-los.

Quais são seus atacantes? O que os motiva? Eles estão preocupados com o desafio técnico? Com a exploração de novidades tecnológicas? Atacar empresas com muitos recursos?

99% das vezes eles buscando o caminho mais simples para viabilizar ganhos financeiros da maneira mais prática possível. O modelado de ameaças deve identificar o que motiva o atacante e porque ele investiria em um ataque A ou B. Só assim desenharemos cenários realmente plausíveis.



Quem é seu atacante?

Seus atacante mimetizam ao máximo seus ambiente, seus clientes. Antecipe-se a eles ou nunca vai achá-los.

Eis porquê perfil “Hacker” é tão ruim quando usado em modelagens, porque o mero conhecimento e skill técnico não são a motivação, mas o meio para chegar em um objetivo.

Os fraudadores, por exemplo, se valem de pouquíssimo skill técnico, mas são altamente motivados por possibilidades de ganhos rápidos e fáceis, desistindo de ambientes que oferecem muita resistência aos ataques.



Grupos fraudadores e suas motivações



Fraudadores Profissionais

Fraudes, começam pequenas, mas logo escalam e o fraudadores se multiplicam a medida que a informação se espalha.



Comemorações dos lucros do grupo

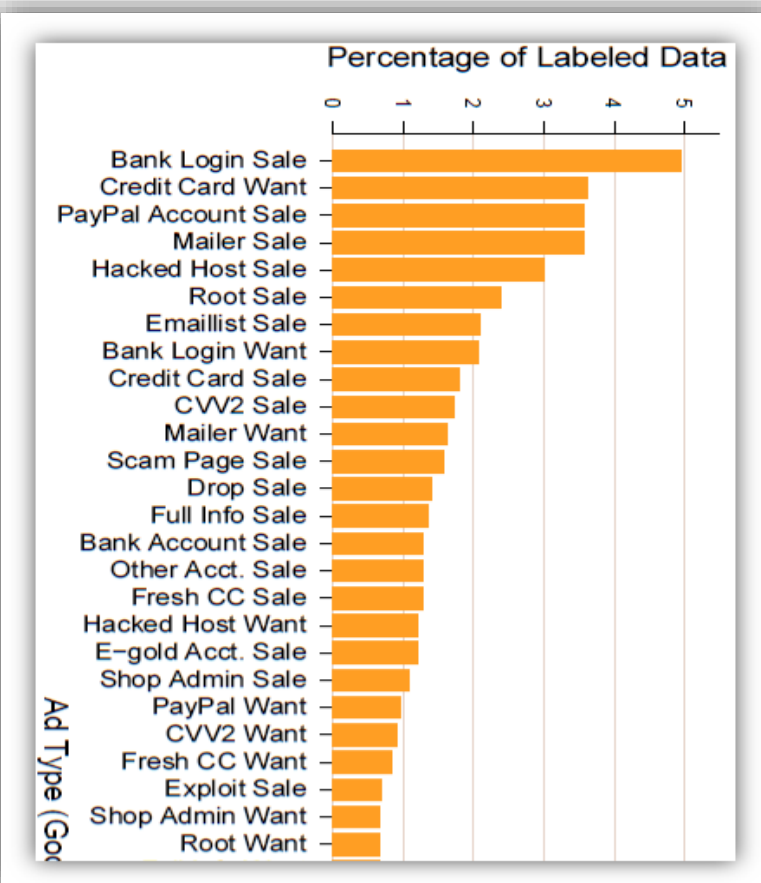
Um grupo organizado de fraudadores com uma meta, atingir um objetivo financeiro (como qualquer projeto tradicional de uma companhia) e curtir o resultado desse projeto.

Grupos fraudadores e suas motivações

Análise dos tipos de informação que mais são vendidas no mercado negro de informações

- Segundo o estudo “*An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants* - Carnegie Mello/Berkeley. CCS’07, October 29–November 2, 2007, Alexandria, Virginia, USA.” dados de acesso bancário são o produto mais ofertado (portanto são os mais vazados).
- Em Segundo lugar temos os anúncios de pessoas comprando informações de cartões de crédito.
- Em terceiro, anuncios de acessos a carteiras virtuais (Paypal) vazados.

Estudo do mercado negro de informações

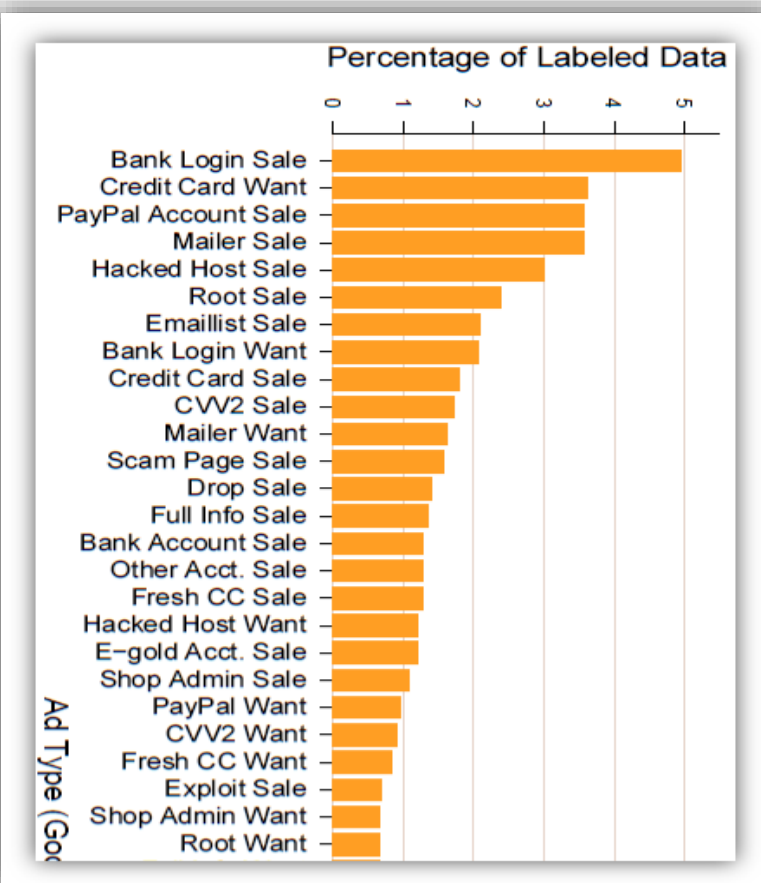


Grupos fraudadores e suas motivações

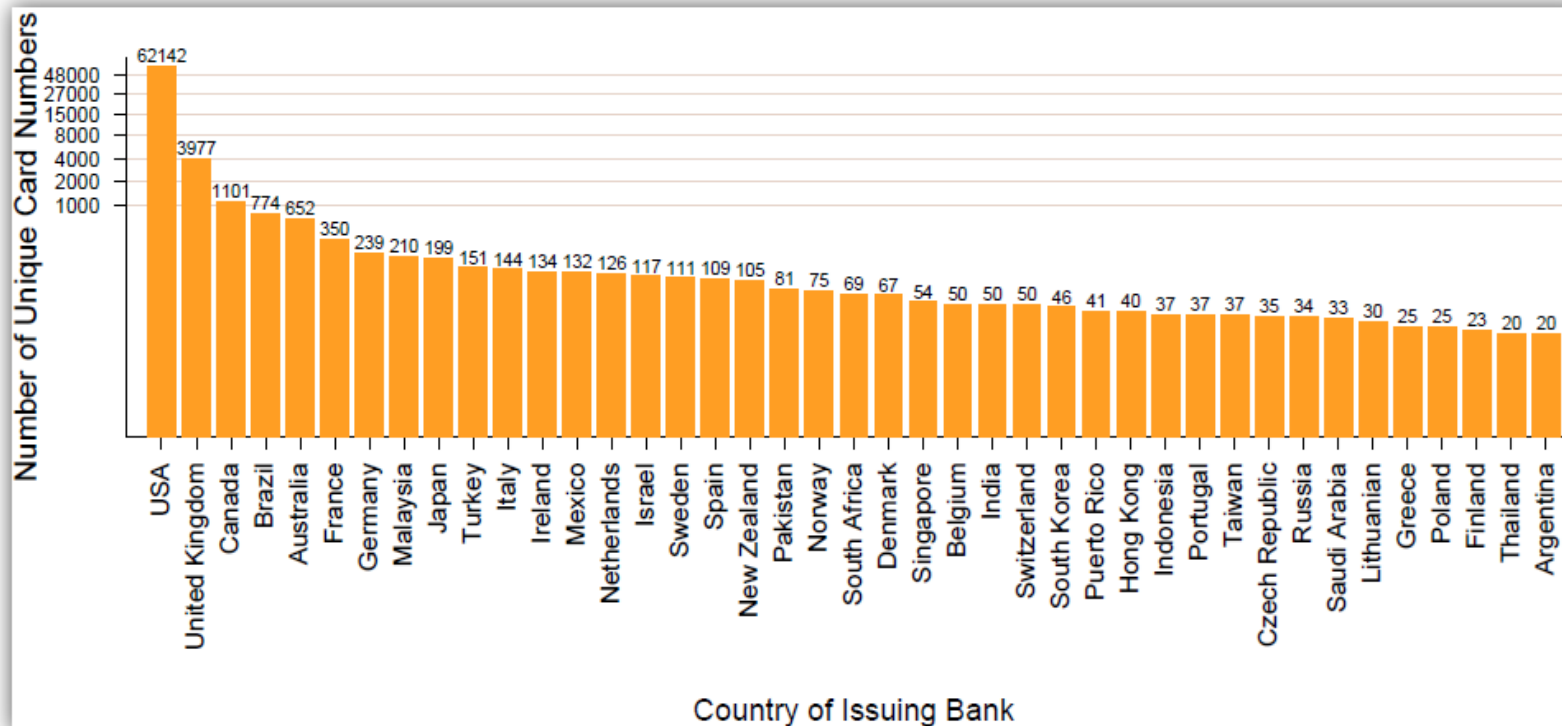
Análise dos tipos de informação que mais são vendidas no mercado negro de informações

- Em quarto, temos sistemas de e-mail sendo oferecidos – lembrando que os milhares de milhares de e-mails enviados em SPAM, estelionato etc. tem que partir de um sistema de emails legítimo, ou dificilmente chegaram ao destinatário e, não menos importante, não podem ser rastreado de volta ao atacante.
- O estudo é antigo, mas os dados não mudaram muito, pois os processos do mercado financeiro não mudaram muito ao longo dos anos.

Estudo do mercado negro de informações



Grupos fraudadores e suas motivações



- Segundo o estudo, cartões emitidos nos EUA, UK, Canda e Brasil estão entre os mais procurados.

Fonte: "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants - Carnegie Mello/Berkeley. CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA." dados de acesso bancário são o produto mais ofertado (portanto são os mais vazados).

Blackmarket exchange

- Alguns desses ativos (CC) são transacionados em fóruns que são instalados em servidores de companhias idôneas vulneráveis, recebem todo o tráfego das negociações e, ao final delas, simplesmente desaparecem.



Blackmarket exchange

- Furto de acessos (contas), controles de ambientes operacionais (admin) que são ativos mais “técnicos” mesmo que somados não se comparam ao bom e velho mercado de ativos financeiros (dinheiro, cartões, acessos bancários, meios alternativos de pagamento).



Blackmarket exchange

- Os atacantes buscam acessos a recursos financeiros (commodities - compra de um computador por exemplo) para vendê-lo no mercado (venda da commodity).
- Esse ataque clássico é extremamente difícil de ser investigado pelos forças policiais, logo, extremamente atrativo para os atacantes.



Olhando o panorama geral

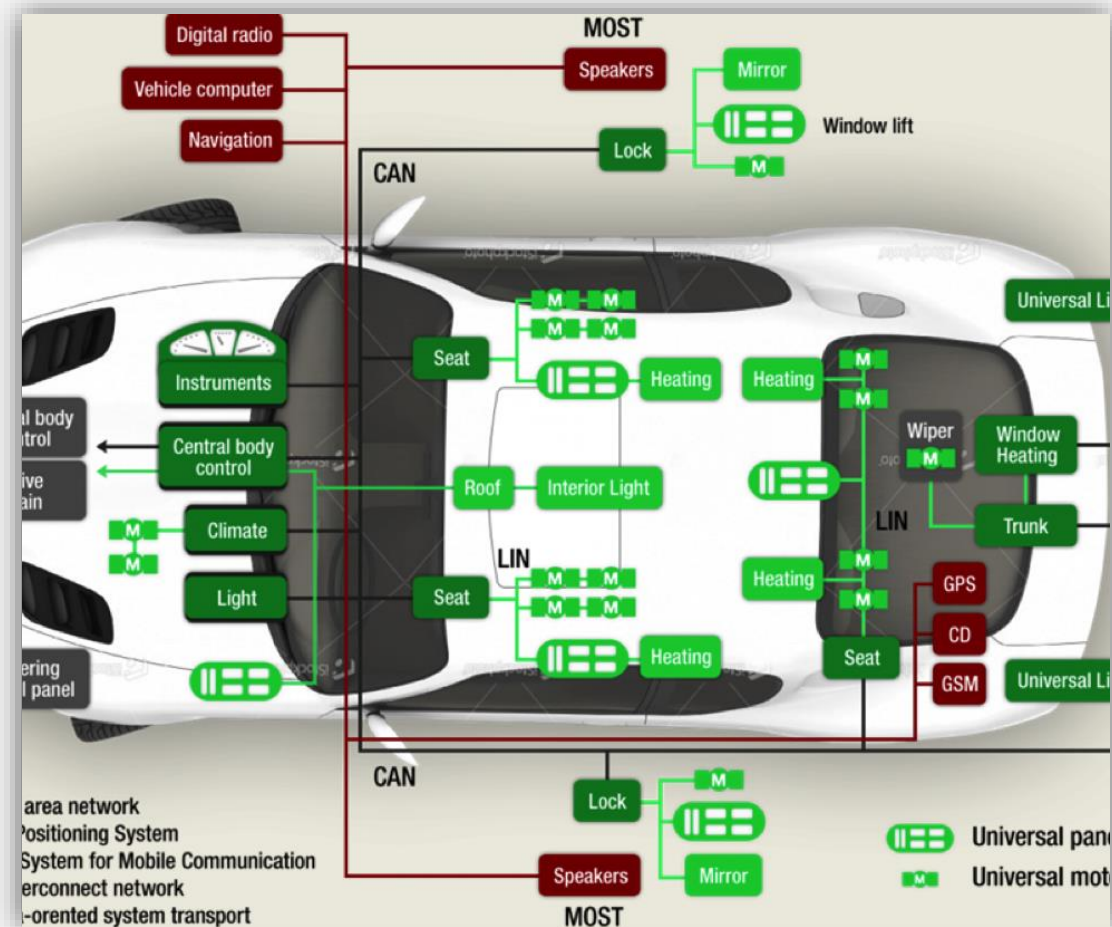


Nova tecnologia, novo espaço de guerra, novas possibilidades de fraude.

Transportar drogas é um delito muito corriqueiro – há series de TV que abordam por várias temporadas esse mesmo tema. Mas imagine o potencial que teria um carro “autônomo” na mão de criminoso cujo intento é transportar armas e drogas. Ou a quantidade de informações médicas disponíveis afetando diretamente mercados como o do tráfico internacional de órgãos. Toda nova tecnologia, se não for bem projetada, servirá para “automatizar”, não só os processos benéficos para sociedade, como também, todos os demais processos.

A tecnologia nasce...

- Não resta dúvida que o futuro é automação e conforto. Mas sem o devido modelo de ameaças orientando a mudança de controles de processos...



A tecnologia nasce... E as ameaças também

- Não resta dúvida que o futuro é automação e conforto. Mas sem o devido modelo de ameaças orientando a mudança de controles de processos... As ameaças se tornaram riscos reais e sérios para sociedade.



The screenshot shows the Black Hat USA 2017 website. The main header features the 'black hat USA 2017' logo and a 'REGISTER NOW' button. Below the header is a navigation bar with links: ATTEND, TRAININGS, BRIEFINGS, ARSENAL, FEATURES, SCHEDULE, SPECIAL EVENTS, SPONSORS, and PROPOSALS. The main content area is titled 'CAR HACKING - HANDS ON' by CANBUSHACK, INC. for July 22-23 & July 24-25. A 'BACK TO TRAINING' button is visible. On the left, a sidebar lists links: PRICING, OVERVIEW, WHO SHOULD TAKE THIS COURSE, STUDENT REQUIREMENTS, and WHAT STUDENTS SHOULD BRING. The pricing table shows four options: EARLY (\$3,200), REGULAR (\$3,500), LATE (\$3,700), and ON-SITE (\$3,800). The ON-SITE option is highlighted with a white background.

EARLY	REGULAR	LATE	ON-SITE
\$3,200	\$3,500	\$3,700	\$3,800
ENDS MAY 19 2359 PT	ENDS JULY 7 2359 PT	ENDS JULY 21 2359 PT	ENDS JULY 24

OVERVIEW
Overview

Conhecer os processos e algoritmos

O QUE PODE SER HACKEADO NUM CARRO?

programadores invadiram os sistemas do Toyota Prius e do Ford Escape. Eis o que eles conseguiram controlar pelo notebook:



Giraram o volante do Escape para qualquer direção, após modificar o sistema do assistente de estacionamento. Mas só conseguiram fazer isso a até 8 km por hora.



Frearam o Prius quantas vezes quiseram quando conseguiram hackear o programa de pré-colisão — que ajuda a parar o carro ao notar que o veículo da frente está perto demais.



Depois de invadir o assistente de curvas, responsável por deixar a direção suave, bloquearam o giro do volante do carro da Ford, restringindo seus movimentos a 45 graus.



Pisaram fundo por segundos com o Prius quando o motorista tirava o pé do acelerador. Nessa hora, o movimento do pedal envia dados para o velocímetro, que pode ser hackeado.

O QUE PODE SER HACKEADO NUM CARRO? (FOTO: ALEXANDRE AFFONSO)

- Engane alguns sensores e o algoritmo vai tomar as “ações” que um atacante quer.
- Com todos os demais processos de negócios a regra é a mesma. Se você domina o processo e consegue antecipar as “regras” que serão aplicadas baseadas em uma “entrada de dados”, você controla o resultado da operação como um todo.

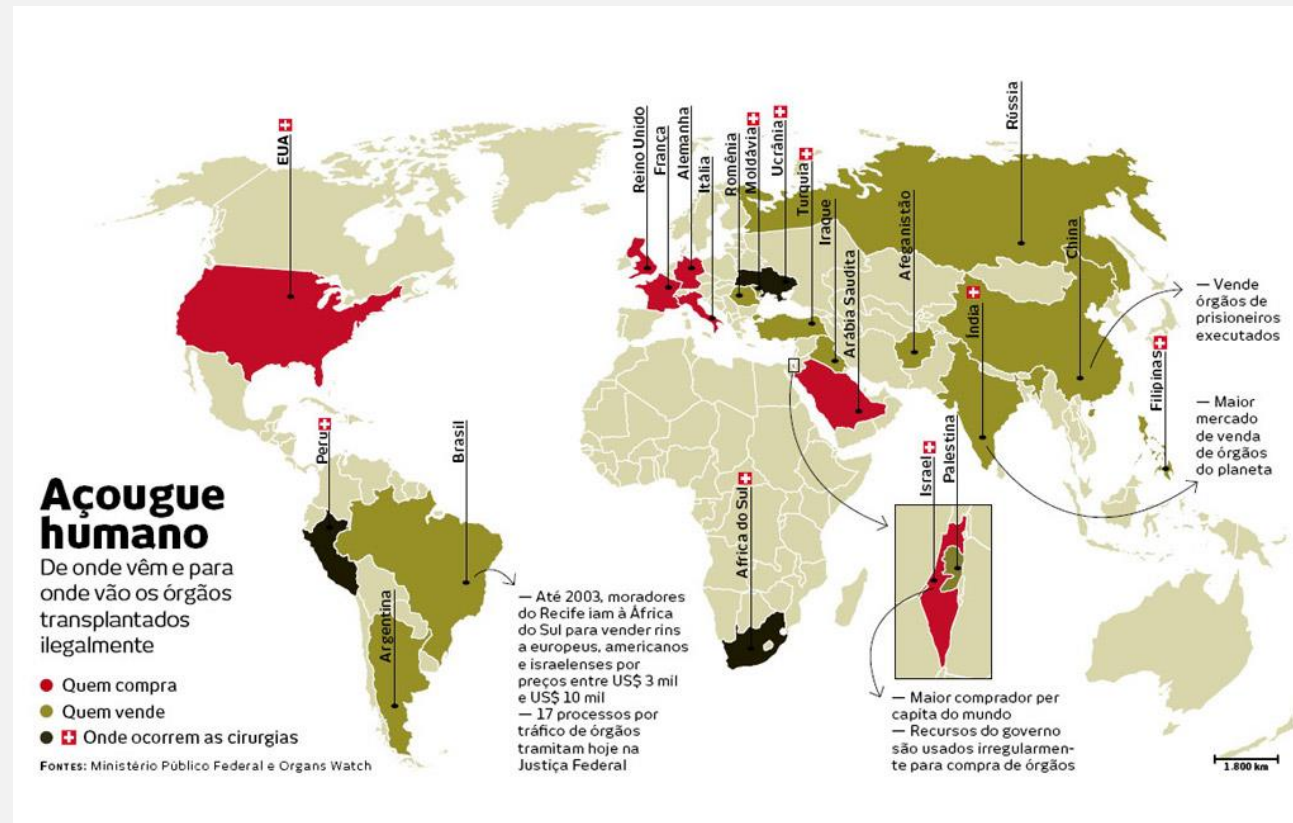
Conhecer os processos e algoritmos

- Por que correr o risco de ser pego traficando drogas, quando se pode “transportá-las de forma automática”?



Dados médicos

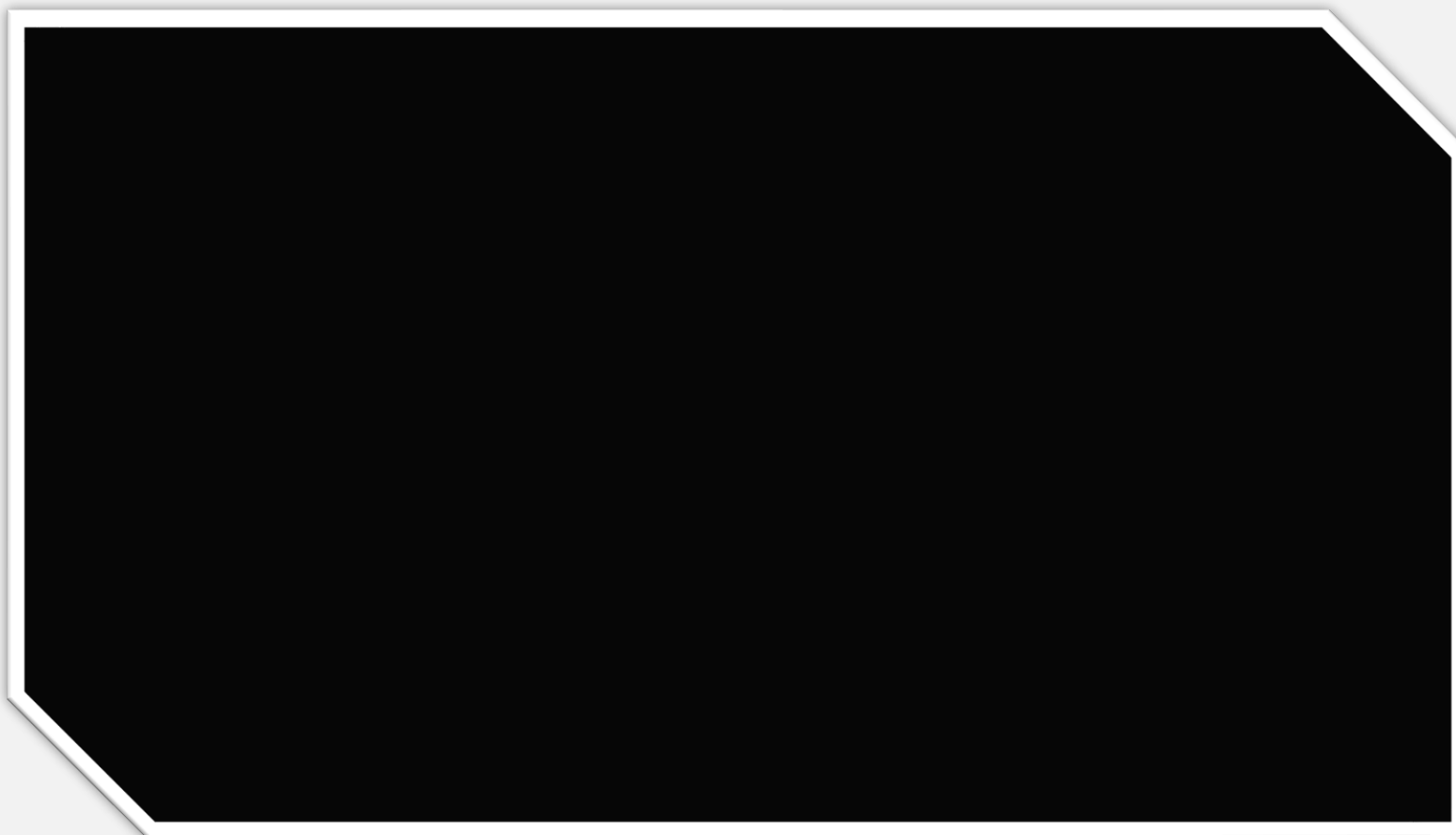
Em um cenário em que um transplante pode salvar a vida de uma pessoa rica, surgem grupos especializados em “prover” acesso a órgão “a tempo” de salvar essa pessoa. Basta coletar todos os dados médicos e biométricos de toda população, escolher um “doador” compatível e resolver a transação.



Adulteração de controles – Furto e venda de veículos

Como um policial fiscaliza um veículo – Chassis e placas? E se um grupo organizado pudesse furtar veículos e revende-los com chassis e placas que nunca cairiam em uma fiscalização?

Assista o vídeo de como operacionaliza-se esse golpe.



Furtos usando processos bancários mal desenhados

O pagamento por boleto bancário é um sistema muito simples. Ele é apenas uma “casca” para uma ordem de pagamento. Como muitas vezes o pagador não tem certeza dos dados do pagamento (em uma transação de e-commerce, por exemplo) os atacantes manipulam as informações e uma vez efetuada a ordem de pagamento, não há como desfazê-la.



Furtos usando processos bancários mal desenhados

Por não conhecer de antemão todos os dados do destinatário de um pagamento, o pagador tem que depositar a confiança na “fonte da informação”. Eis a grande falha. O atacante precisa apenas “ganhar a confiança do atacado” para efetuar essa parte do Golpe, que movimentava bilhões de reais anualmente.



Processos bancários mal desenhados e o crime organizado

O crime organizado é conhecido por articular atividades compondo golpes em várias etapas. Dentre elas, aliciamento de terceiros que facilitam golpes visando lucro fácil.

No caso ao lado, temos o um esquema que usava cartões clonados, boletos falsos, vírus para adulteração de boletos, mas nada disso adianta sem um elaborado esquema para circular e resgatar esses ativos.



Processos que se valem da “relação de confiança”.

Processos (modalidades) de pagamentos

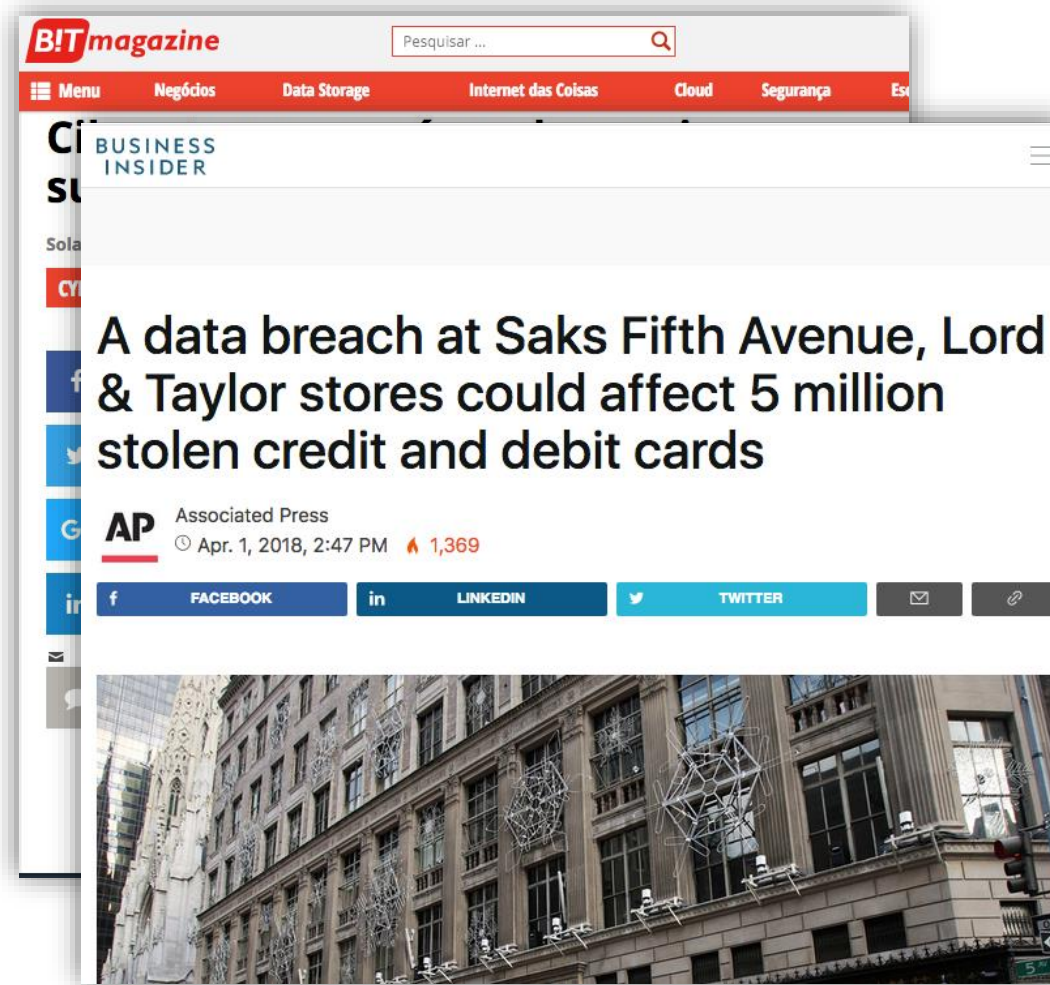
Artifícios técnicos são empregados apenas pelo fato de muitos desses processos serem automatizados, hoje em dia. Mas o ataque, em si, é feito ao processo e as premissas de que esses processos se valem, dentre eles, da relação de confiança entre um comprador e um vendedor, por exemplo.



Processos que se valem da “relação de confiança”.

Processos (modalidades) de pagamentos

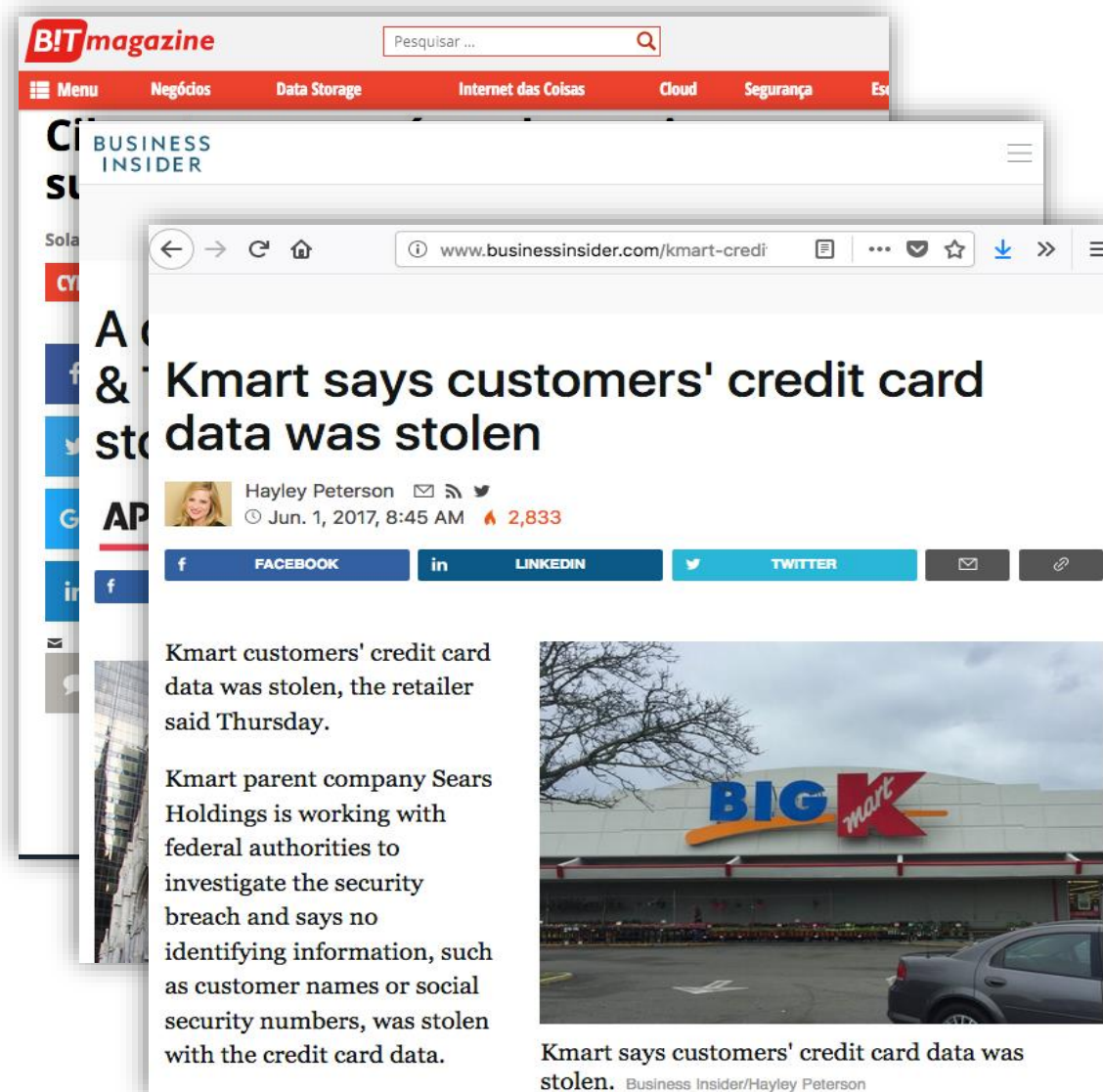
Artifícios técnicos são empregados apenas pelo fato de muitos desses processos serem automatizados, hoje em dia. Mas o ataque, em si, é feito ao processo e as premissas de que esses processos se valem, dentre eles, da relação de confiança entre um comprador e um vendedor, por exemplo.



Processos que se valem da “relação de confiança”.

Processos (modalidades) de pagamentos

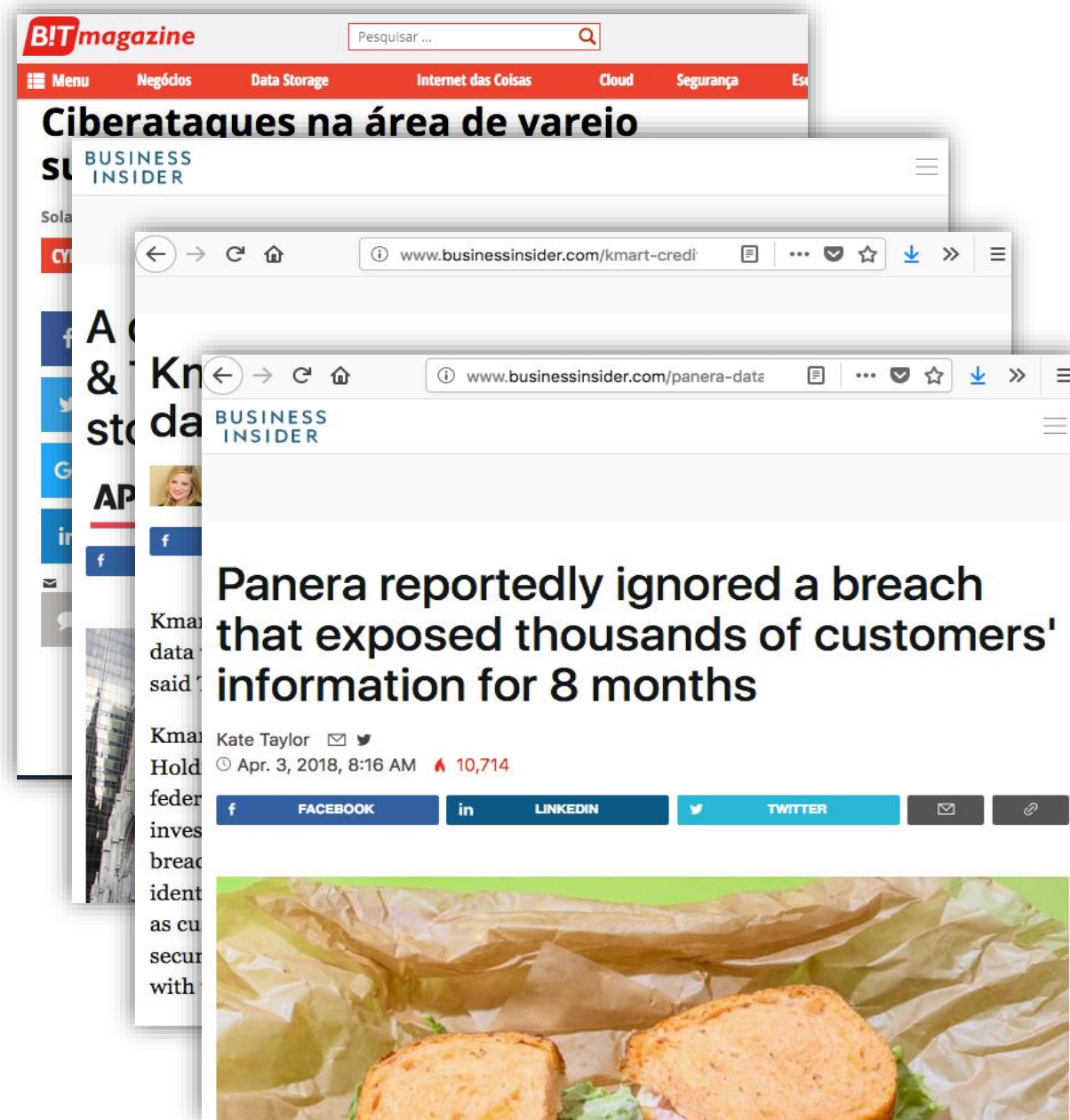
Artifícios técnicos são empregados apenas pelo fato de muitos desses processos serem automatizados, hoje em dia. Mas o ataque, em sí, é feito ao processo e as premissas de que esses processos se valem, dentre eles, da relação de confiança entre um comprador e um vendedor, por exemplo.



Processos que se valem da “relação de confiança”.

Processos (modalidades) de pagamentos

Artifícios técnicos são empregados apenas pelo fato de muitos desses processos serem automatizados, hoje em dia. Mas o ataque, em si, é feito ao processo e as premissas de que esses processos se valem, dentre eles, da relação de confiança entre um comprador e um vendedor, por exemplo.



A close-up, low-angle shot of a shark swimming underwater. The shark's body is dark and sleek, with its fins visible. The water is a deep blue, and sunlight filters through from above, creating a shimmering effect on the shark's skin and the water's surface. The overall mood is mysterious and powerful.

“

Conheces teu inimigo e conhece-te a ti mesmo; se tiveres cem combates a travar, cem vezes serás vitorioso. Se ignoras teu inimigo e conheces a ti mesmo, tuas chances de perder e de ganhar serão idênticas. Se ignoras ao mesmo tempo teu inimigo e a ti mesmo, só contarás teus combates por tuas derrotas. - **Sun Tzu**.

Resumindo

Conhecer a si mesmo

Dominar os processos de negócio que se pretende modelar e como eles se relacionam com clientes, consumidores, parceiros, sistema financeiro, ou seja, dominar o conteúdo que define quem você é em termos de empresa.

Conhecer teu inimigo

O que move teu perfil de atacante, quem ele almeja atacar de fato e como ele pode explorar teus processos e tecnologias para alcançar seus objetivos.

Nota: Exatamente por todas as considerações e dados apresentados até aqui, nosso método se baseia primariamente nos processos, avaliando a tecnologia quando necessário para desenhar controles automatizados.