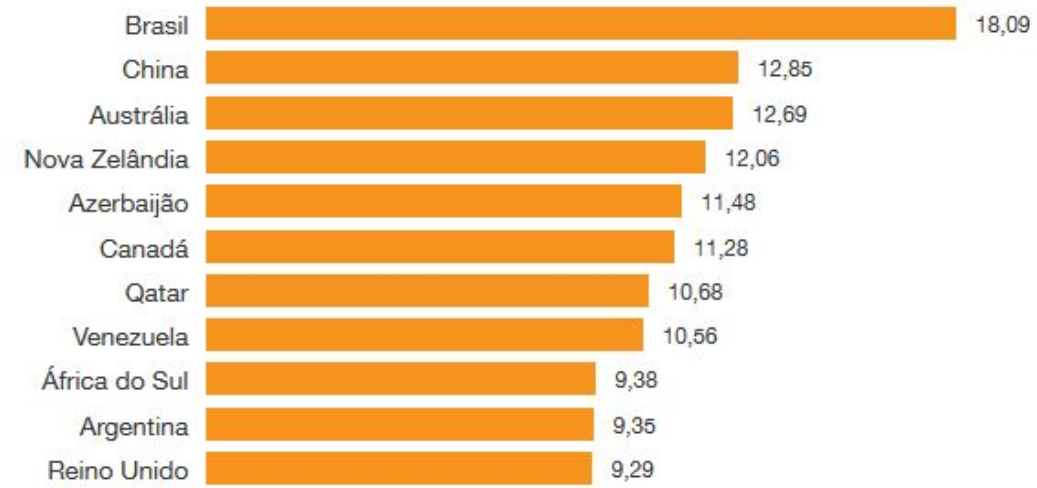
Crimes Virtuais

Brasileiro é quem mais sofre fraudes na internet



Fonte: Kaspersky Lab

O Brasil foi considerado o ambiente virtual mais perigoso para bancos em 2014 pela Kaspersky. Em 2015, bancos brasileiros perderam R$ 1,8 bilhão com ataques virtuais, segundo a Febraban (Federação Brasileira de Bancos).

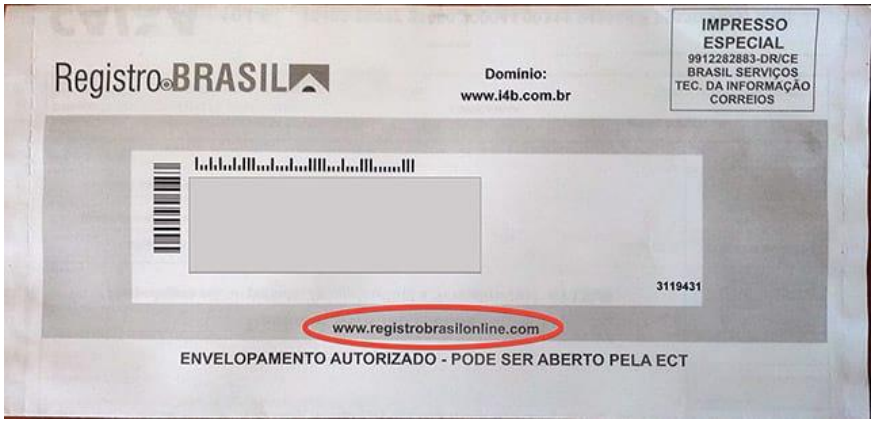
Bases de dados de outros antivírus apontam o Brasil como fonte de ataques. A Symantec concluiu que, em 2016, a maior parte de ameaças on-line veio dos Estados Unidos (24%), seguidos da China (9,6%) e do Brasil (5,8%).

Tipos mais Comuns

- Boleto de registro de domínio
- Faturas de registro de marcas
- Falsos e-mails de instituições financeiras
- Oportunidades de emprego falsas
- Furto de identidade
- Pishing
- Sites maliciosos
- Romances pela internet
- Spam
- Malwares
- Golpes por Smartphones
- Fraude de controle de conta
- Botnets
- Teste de cartão
- Fraude “Limpa”
- Fraude “Amigável”
- Lavagem de Dinheiro
- Esquemas de Triangulação
- Etc.

Boleto de registro de domínio

O Registro.br cuida do registro de nomes de domínios, da administração e da publicação do DNS (Sistema de Nome de Domínios) para o domínio ".br", além dos serviços de distribuição e manutenção de endereços Internet.



Oportunidades de emprego falsas

Golpes que prometem emprego online, com vagas de trabalho a partir de casa. No golpe de trabalhar em casa, as vítimas são atraídas por conta de uma variedade de oportunidades. Esses sites podem ser tão convincentes que as vítimas frequentemente são levadas a descontar cheques e ordens de pagamento enviados pelo correio, para depois reenviar uma parte do dinheiro por meio de seus cheques pessoais, dinheiro e ordens de pagamento para uma terceira parte, agindo como laranjas. As vítimas são levadas a fornecer ao fraudador suas informações pessoais, com a promessa de salários-hora acima da média ou do pagamento de centenas de dólares por semana. Para algumas vítimas, o golpista chega a prometer o envio do hardware e do software necessários para efetuar o "trabalho".

Furto de identidade

Furto de identidade é o ato pelo qual uma pessoa tenta se passar por outra com o objetivo de obter vantagens indevidas. Alguns destes casos podem ser tipificados como falsa identidade, assim sendo considerados crimes. No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de e-mail e envie mensagens se passando por você ou falsifique os campos de e-mail, fazendo parecer que ele foi enviado por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser.

Phishing e Sites maliciosos

Em computação, phishing é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir informações sigilosas, tais como senhas e números de cartão de crédito, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, como um correio ou uma mensagem instantânea.

Outras formas de phishing são os sites que duplicam o site original se passando por este, assim que a pessoa faz o login, as informações são guardadas no banco de dados e direcionado para o site original, na primeira vista você sequer reconheceu o que aconteceu, como depois de redirecionado pensa que esta no site original faz o login novamente, mas os hackers já estão com suas informações guardadas. Portanto, tome cuidado em sempre ver se a URL onde estão fazendo a identificação de usuário seja a URL válida que sempre acessa, lembre-se também de que sites de instituições financeiras sempre usam SSL, o famoso cadeado nos navegadores, geralmente identificados pela cor verde.

Ex.: Orkut

Pishing

Crescimento de 52% em 2012 em todo o mundo

Prejuízos atingiram cerca de US$ 1,5 bi em 2012

Brasil está entre os 5 países com maior frequência de ataques de pishing

Romances pela internet

Romance scammer é mais uma das muitas armadilhas que proliferaram nas redes sociais. Golpistas criam falsos perfis no Facebook para seduzir mentes e corações de homens ou mulheres com o intuito de lhes arrancar boas quantias de dinheiro. Muitos internautas que morderam o “anzol” scammer acumulam decepções, traumas e, em alguns casos consumados, prejuízos financeiros. Existem até casos de suicídio. Para combater a prática, na web até já existem grupos organizados de “caça-scammers”.

Spam e Malware

Spam: Mensagens eletrônicas com links maliciosos enviados sem o consentimento do usuário e que, geralmente, são despachadas para um grande número de pessoas.

Usado para disseminar conteúdos mais agressivos (Malware) e obter informações pessoais

Malware: Software malicioso, instalado sem consentimento.

Vírus, worms e cavalos de tróia

Golpes por smartphones

Golpes aplicados por meio de smartphones já representam **15%** das fraudes na internet.

Ocupam a segunda posição do total de fraudes na internet, só perdem para os e-mails falsos que ao serem abertos, espalham vírus pelos computadores.

Invasão de celulares em todo o país aumentaram 55% só no último trimestre.

Fraude de controle de conta
Botnets

Fraudador obtém acesso às contas bancárias ou ao cartão de crédito da vítima - por meio de violação de dados ou malware - utilizando as informações para realizar transações não autorizadas

Rede privada infectada com um software malicioso. Essa rede é utilizada, por exemplo, para roubar dados, enviar spam e permitir que criminosos acessem os dispositivos.

Teste de cartão

Fraudadores usam as lojas online para testar informações do cartão de crédito que estão em seu poder, com o objetivo de descobrir se eles foram bloqueados/cancelados, e se os limites de crédito foram atingidos.

Fraude “Limpa”
Fraude “Amigável”

Utilizam das informações roubadas do cartão de crédito, e com grande quantidade de dados pessoais, os criminosos efetuam compras fazendo-se passar pelos verdadeiros portadores do cartão sem levantar suspeita.

Quando um consumidor faz uma compra online usando seu próprio cartão de crédito e, após receber a o produto ou serviço, solicita o estorno ao banco emissor. Uma vez aprovado, o estorno cancela a transação financeira e o consumidor recebe de volta o montante gasto.

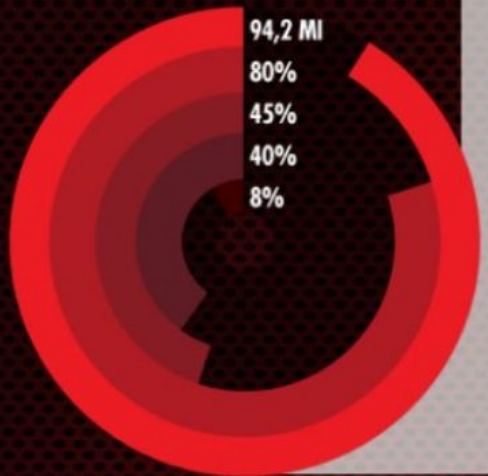
Lavagem de Dinheiro
Esquemas de Triangulação

Processo que oculta as origens de fundo obtidos ilegalmente, por transferências de recursos envolvendo bancos estrangeiros ou empresas legítimas.

Criminosos usam cartões de crédito roubados para comprar mercadorias arrematadas em leilões online ou adquiridas em sites de e-commerce. Em seguida, revendem essas mercadorias a clientes legítimos, que não estão envolvidos na fraude.

OS PERIGOS QUE RONDAM AS REDES SOCIAIS

PORQUE AS REDES SOCIAIS SÃO OS PRINCIPAIS ALVOS DE USUÁRIOS MAL INTENCIONADOS?



94,2 MILHÕES DE BRASILEIROS USAM A INTERNET

80% DAS ATIVIDADES DOS USUÁRIOS SÃO FEITAS EM REDES SOCIAIS E BLOGERS

45% DOS INTERNAUTAS BRASILEIROS USAM REDES SOCIAIS

40% DAS CONTAS E 8% DAS MENSAGENS NAS REDES SOCIAIS SÃO SPAMS


A CADA MINUTO DO DIA
100.000 TWITTES SÃO ENVIADOS
APROXIMADAMENTE 690.500 CONTEÚDOS SÃO EXPOSTOS NO FACEBOOK
48 HORAS DE VÍDEO SÃO VISTOS NO YOUTUBE
3.600 FOTOS SÃO COMPARTILHADAS NO INSTAGRAM
571 WEBSITES SÃO CRIADOS

CONSEQUÊNCIAS

ROUBO DE INFORMAÇÕES

- A cada **15 segundos**, um brasileiro é vítima de tentativa de fraude com documentos roubados ou informações furtadas da internet
- Mais de **28 milhões** de brasileiros já foram vítimas de golpes na internet
- Ameaças virtuais e cibercrimes custam **R$16 bi** anualmente ao país

DANOS AO COMPUTADOR

- Quando a máquina é infectada, os criminosos conseguem ter acesso a tudo o que é guardado e digitado: senhas de banco e de cartões, número de CPF, identidade, endereço, fotos e vídeos
- Espalhar malwares
- Apagar todas as informações do sistema
- Abrir e fechar navegadores à toa e sem comandos
- Lentidão
- Bloqueio de softwares
- Pane total do sistema

OS GOLPES MAIS FAMOSOS NAS REDES SOCIAIS

FACEBOOK

- **1,1 BILHÃO** DE USUÁRIOS ATIVOS POR DIA
- **996 MIL** VÍDEOS CARREGADOS POR MÊS
- **460 MILHÕES** DE FOTOS POSTADAS POR MÊS
- **715 MILHÕES** DE MENSAGENS ENVIADAS POR MÊS
- **160 MILHÕES** DE POSTAGENS NO MURAL POR MÊS
- **1,6 BILHÕES** DE COMENTÁRIOS POR MÊS
- **1,6 BILHÕES** DE LIKES POR MÊS
- **125 BILHÕES** DE IMAGENS COMPARTILHADAS POR ANO

PRINCIPAIS GOLPES

- Notícias sobre morte de celebridades
- Fotos polêmicas ou escandalosas
- "Você viu o que falaram sobre você?"
- Descubra quem te visitou/te deletou/te bloqueou
- Mude a cor do seu Facebook

TWITTER

500 MILHÕES DE USUÁRIOS REGISTRADOS

200 MILHÕES DE USUÁRIOS ATIVOS EM 2013

300 MIL NOVOS VISITANTES POR DIA

175 MILHÕES DE TWITTES POR DIA

750 TWITTES POR SEGUNDO

PRINCIPAL GOLPE

- Links maliciosos enviados por DM: Assista seu vídeo no Facebook

YOUTUBE

1 BILHÃO DE USUÁRIOS ATIVOS POR MÊS

72 HORAS DE VÍDEOS CARREGADOS POR MINUTO

4 BILHÕES DE HORAS DE VIDEOS ASSISTIDOS POR MÊS

PRINCIPAL GOLPE

- Vírus enviado por email: "Um(a) amigo(a) lhe enviou um vídeo do YouTube" com link duvidoso

INSTAGRAM

100 MILHÕES DE USUÁRIOS ATIVOS POR MÊS

40 MILHÕES DE FOTOS POSTADAS POR DIA

8500 LIKES POR SEGUNDO

1000 COMENTÁRIOS POR SEGUNDO

PRINCIPAL Ggolpe

Perfis falsos que atraem para fraudes virtuais (com links suspeitos nos perfis ou em sites)

tumblr.

TUMBLR

400 MILHÕES DE USUÁRIOS ATIVOS POR MÊS

38.000 POSTS POR MINUTO

MAIS DE 30 MILHÕES DE TUMBLRS EXISTENTES

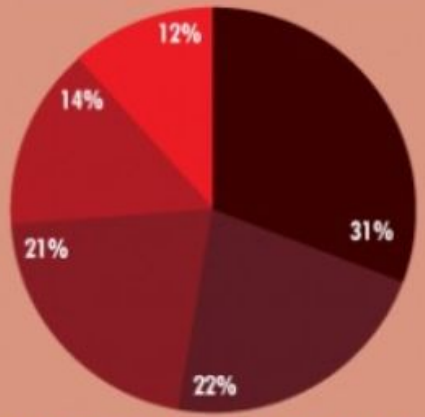
CERCA DE 12 BILHÕES DE POSTS EXISTENTES

PRINCIPAL GOLPE

- Mensagem publicada no tumblr pela falsa organização GNAA afeta mais de 8 mil contas contra a vontade dos usuários (ameaçando deletar a conta daqueles que não a repassarem)


LINKEDIN
225 MILHÕES DE USUÁRIOS CADASTRADOS
170 MIL NOVAS CONTAS POR DIA
5,7 BILHÕES DE BUSCAS EM 2012
MAIS DE 2 MILHÕES DE GRUPOS ATIVOS NA REDE
PRINCIPAL GOLPE
• Pishing com solicitações falsas, fazendo com que o usuário acesse um link malicioso

LINKS MALICIOSOS NA WEB



31% ENTRETENIMENTO
22% BUSCADORES
21% MÍDIAS SOCIAIS
14% PORNOGRAFIA
12% BANNERS E ANÚNCIOS PUBLICITÁRIOS

DICAS DE SEGURANÇA

Bitdefender®

- √ CUIDADO AO CLICAR EM LINKS
- √ NÃO ACREDITE QUE UMA MENSAGEM SEJA REALMENTE DE QUEM ELA DIZ SER
- √ PARA EVITAR QUE VOCÊ ENTREGUE ENDEREÇOS DE E-MAIL DE SEUS AMIGOS, NÃO PERMITA QUE SERVIÇOS DE REDES SOCIAIS EXAMINEM O SEU CATÁLOGO DE ENDEREÇOS DE E-MAIL
- √ DIGITE O ENDEREÇO DE SEU SITE DE REDE SOCIAL DIRETAMENTE NO SEU NAVEGADOR OU USE SEUS MARCADORES PESSOAIS
- √ SEJA SELETIVO PARA ACEITAR AMIGOS EM REDES SOCIAIS
- √ ESCOLHA SUA REDE SOCIAL COM CUIDADO
- √ TENHA SEMPRE EM MENTE QUE TUDO O QUE VOCÊ COLOCAR NA REDE SOCIAL SERÁ PERMANENTE
- √ TENHA CUIDADO AO INSTALAR APLICATIVOS ADICIONAIS NO SEU SITE

Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos

Em **11** anos, a Central de Denúncias recebeu e processou **3.861.707** denúncias anônimas envolvendo **668.288** páginas (URLs) distintas (das quais **232.577** foram removidas) escritas em **9** idiomas e hospedadas em **86.143** hosts diferentes, conectados à Internet através de **50.405** números IPs distintos, atribuídos para **98** países em **5** continentes. As denúncias foram registradas pela população através dos **7** hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.

http://indicadores.safernet.org.br/