Internet 171

Mitigando Estelionatos na Rede

Danton Nunes (*danton.nunes@inexo.com.br*)

GTS 39 – Semana da Infraestrutura da Internet no Brasil

Quem nunca recebeu?

- Mensagens fraudulentas por e-mail, *Whatsapp* ou telefone celular.
- Você conhece quem tenha caído nessas arapucas? (Eu conheço mais de uma!)
- Esse é o pior problema de segurança na Internet hoje, mas pode ser mitigado com boas práticas em cada passo do processo.

Exemplos reais (de minha caixa postal de refugos)

Olá, **danton@inexo.com.br**.

Você está **recebendo a sua conta Vivo** para pagamento.
Para pagar, **basta utilizar o código de barras abaixo.**

Data de vencimento: 18/11/2024
Valor: R$ 359,92
Código de barras: 42297.11504 00064.897317 05991.008623 1 99060000035992

Parabéns, você foi selecionado para se tornar um cliente Bradesco Prime Digital!

Nº DE PROTOCOLO	3130226/2024
EMAIL CADASTRADO	danton.nunes@inexo.com.br
DATA DO CONVITE	14/11/2024
VALIDADE DO CONVITE	30 DIAS

Prezado(a) danton.nunes@inexo.com.br , devido ao seu bom relacionamento com o banco **Bradesco**, sua conta foi selecionada para fazer parte do seleto grupo de clientes do segmento **Prime Digital**.

Confira alguns dos benefícios:

1. Acesso a agências exclusivas **Bradesco Prime**.
2. Acesso a cartão de créditos Black e Infinity sem anuidades.
3. Acumule 1 ponto por cada real gasto no programa **Livelo**.
4. Gerente disponível 24 horas por dia através do Whatsapp.

Atenção: Renovação do Seu Domínio

Estimado **danton.nunes@inexo.com.br**,

Estamos aqui para alertá-lo sobre a urgência da renovação do seu domínio. Este registro anual é fundamental para garantir sua visibilidade online e deve ser atualizado antes da data de expiração para evitar que e-mails e hospedagem, sejem interrompidos, afetando a continuidade do seu negócio.

A fatura da renovação do seu domínio já está disponível. Você pode efetuar o pagamento através do boleto anexo ou utilizando o código de pagamento indicado abaixo. Não deixe para a última hora pois não é possível prorrogar o prazo de pagamento pelo nosso sistema.!

03399.54349 20377.318850 63217.901014 4 99180000499990

e o vigarista capricha!

A conta bancária para receber o valor existe e tem cara de ser verossímil.

O banco nem deveria aceitar abrir uma conta assim!

mensagem que mandei para os contatos dos envolvidos.

Note que nenhum dos dois seguem a RFC-2142!

From: Danton Nunes <danton.nunes@inexo.com.br> danton@inexo.com.br (IMAP)

To: suporteinternet@santander.com.br registro.admin@kinghost.com.br

Subject: mail-abuse@cert.br

```
Caros responsáveis por santander.com.br e kinghost.com.br

A mensagem anexa é uma fraude, se passando por alguém da locaweb, cobrando uma
suposta renovação de seu domínio, no absurdo valor de R$4.999,90 (cinco mil
reais menos dez centavos).

A mensagem foi enviada originalmente por apoio@poliedrometalica.com.br que
acredito seja uma conta com senha comprometida. O endereço de retorno é
1apoio@poliedrometalica.com.br, que pode ser outra conta comprometida. De acordo
com o 'whois', o contato desse domínio é registro.admin@kinghost.com.br

O boleto contido na mensagem é do banco Santander (código 033) de uma conta que
parece ser de alguma coisa relacionada ao Facebook. No anexo é possível ver o
código de barras completo e dele extrair os números de agência e conta.

Por favor, façam o que for necessário para que esta mensagem pare de circular
pela Internet. Uma pessoa menos informada que tivesse negócios com a locaweb
poderia cair nessa armadilha e perder dinheiro para o meliante.

Atenciosamente,
--
Danton Nunes      |Informática, Consultoria e Serviços pela Internet
InterNexo Ltda.   |http://inexo.com.br/ e-mail:danton.nunes@inexo.com.br
S.J.Campos,BRASIL |fone:(12)3797-6865 móvel:(12)99144-7458 INOC:28262*DAN
```

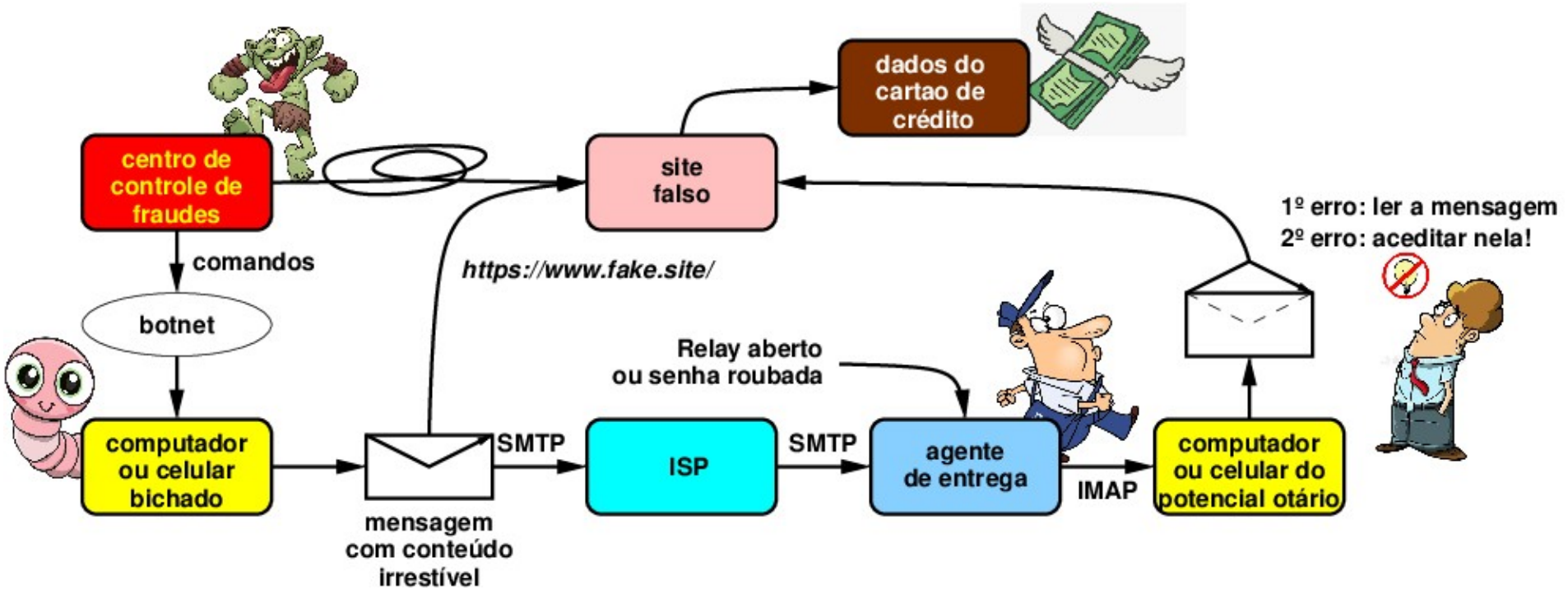
1 Attachment 641 kB

Notícia • Estadão / São Paulo

Fraude na conta de idosos: polícia fecha falsa central bancária especializada em golpes

Coforme o governo de SP, investigações tiveram início após denúncia de uma vítima que perdeu R$ 56 mil

Um processo complicado...



Atores: 1 o criminoso

- Comanda o disparo de mensagens fraudulentas, usando computadores tomados (botnet)
- Mantém site falsificado (physhing) para coleta de informações sensíveis da vítima, geralmente dados de cartão de crédito.

Suponho que não possamos contar com sua ajuda!

Atores: 2. Computador tomado

- Normalmente o proprietário não sabe que seu computador está sendo abusado.
- Software desatualizado, com bugs conhecidos e custa caro atualizar!.
- Alguém clicou onde não devia e baixou executáveis clandestinos!

Atores: 3. Provedor de Serviços IP

- Não pode intervir no tráfego passante por sua rede.
- Pode (e deve!) fechar a porta 25/tcp exceto para endereços de servidores de e-mail conhecidos (bloqueia para todo o mundo e vai criando exceções. iptables, ipset, … ajudam)

Atores: 4. Provedor de serviços de e-mail

- Usuários com senhas fracas e abusáveis.
- Termos de uso complicados, que fazem o usuário clicar no aceito sem ler (e sem obedecer depois)
- Podem ser vítimas de *password harvesting*.
- *Message-ID* (RFC-5322) ausente ou sem sentido.

Atores: 5. Agente de Entrega

- Normalmente usa IMAP para entregar mensagens
- Também pode ser vítima de password harvesting, pois dificilmente alguém usa senhas diferentes para receber e enviar

Atores 6: O otá^H^H^Husuário

- Não tem malícia ou conhecimento para distinguir uma mensagem falsa de uma verdadeira (e há mensagens falsas muito bem feitas!)
- Entrega seus dados de bandeja.

Como mitigar o problema

- Dado o caráter de múltiplos atores, cada um deve fazer sua parte para evitar golpes de falsificação e estelionato.
- As melhores práticas correntes (série BCP do IETF) são de grande ajuda no lado técnico da coisa toda

Mitigação: 1a. ISP e usuário final

- O usuário final geralmente tem pouco conhecimento de TI, então a ajuda do ISP é fundamental.
- O ISP pode suspeitar da presença de *botware* em uma máquina de cliente, analisando os fluxos de dados (aqui há espaço para aprendizado de máquina e inteligência artificial)

Mitigação: 1b. ISP e usuário final

- ISP deve ter o e-mail *abuse@meu.domínio* e o mais importante: jamais tenha `/var/mail/abuse → /dev/null` (veja RFC-2142)
- Recebida uma mensagem por esse meio deve encontrar o usuário, através dos logs do NAT (se for o caso) e informá-lo da reclamação.

Mitigação: 1c. ISP e usuário final

- O ISP pode ser proativo e analisar fluxos de dados passantes por sua rede (mas não os dados em si!) para observar comportamentos anômalos. De novo, inteligência artificial pode ser uma mão na roda para isto.

Mitigação: 2. provedor de hospedagem

- Também precisa manter endereços de contato abuse@... e security@... para receber reclamações sobre conteúdo falsificado.
- Depois de conferir a veracidade da reclamação (com o dono aparente do site), tirá-lo da vista, mas não removê-lo pois pode ser usado como prova

  OK, eu não sou advogado, mas isso me parece bom senso.

Mitigação 3a. Provedor de e-mail

- Como nos outros atores manter endereços de security@ e abuse@ e não descartar simplesmente o que chegar neles.
- Gerenciamento de senhas, recomendar senhas de alta entropia e fazer varreduras periódicas para encontrar senhas fracas (John the Ripper?).

Mitigação: 3b. provedor de e-mail

- Inserir nas mensagens autenticadas um cabeçalho identificando o remetente real, isto é, aquele que se autenticou no *Submission*. Isso permite identificar contas comprometidas.
- Também cabe aqui ser proativo e procurar comportamentos anômalos.

Mitigação: 4a. o usuário

- Seguir as recomendações de segurança do provedor de e-mail e de entidades públicas de segurança, como o cert.br
- Não ignorar os termos e condições (por vezer um documento longo e maçante), clicando no botão “Aceito”, sem lê-los e muito menos obedecê-los.

Mitigação: 4b. usuário

- Também é importante que o usuário leia as dicas de segurança dos bancos, como usar cartões virtuais de uso único, preferir cartão de crédito a débito ou PIX pois cartão de crédito permite glosar a transação e é mais fácil de estornar.
- Sempre que vir uma oferta irresistível, desconfie. Telefone, mande e-mail, ou mensagem de texto para a loja com a tal “promoção”.
- Não deixar barato: reclame!

Mitigação 5: anti colheita de senhas

- Há mecanismos para reduzir a probabilidade de se acertar uma senha, o mais simples é analisar as mensagens de senha recusada no log e no caso de várias negações repetidas colocar o endereço IP ou o ASN da origem de castigo por um longo período.
- Os logs também são úteis para fundamentar reclamações aos ISPs dos *harvesters*.

Conclusões

- Embora este trabalho tenha focado e-mail, qualquer processo de envio de mensagens que possam conter um link, possui riscos similares.
- O processo se parece com uma *supply-chain*, e o que queremos reforçar é a rastreabilidade.
- Automatizar a comunicação entre os participantes (exceto o meliante, claro) facilitaria muito o processo.
- Há muito espaço para Inteligência Artificial aí.

Conclusões

- Este trabalho é um apelo aos atores que participam desta comunidade a seguir à risca as boas práticas correntes (BCPs, RFCs, BCOP) pois elas ajudam muito na prevenção desses crimes.
- Houve um tempo em que RFC era *Request for Comments*, agora é *Read and Follow Carefuly*.

Referências

1. D.Crocker, **RFC-2142**, 1997, Mailbox Names for Common Services, Roles and Functions, *https://datatracker.ietf.org/doc/html/rfc2142*
2. G. Lindberg, **RFC-2505/BCP-30**, 1999, Anti-Spam Recommendations for SMTP MTAs, *https://datatracker.ietf.org/doc/html/rfc2505*
3. CERT.br, Cartilha de Segurança para Internet, vários fascículos, *https://cartilha.cert.br*

Referências

4. Encryption Consulting, 2024,Top 10 Supply Chain Attacks that Shook the World, *https://www.encryptionconsulting.com/top-10-supply-chain-attacks-that-shook-the-world/*

Agradecimentos

1. Adriano Cansian, pela revisão e dicas,
2. CERT.br pelo excelente trabalho com a cartilha de segurança

Obrigado!