Universidade Federal de Pernambuco
Centro de Informática

Graduação em Sistemas de Informação

Panorama Atual de Smishing no Brasil

José Durval Carneiro Campello Neto

Trabalho de Graduação

Recife
12 de Dezembro de 2018

Universidade Federal de Pernambuco
Centro de Informática

José Durval Carneiro Campello Neto

Panorama Atual de Smishing no Brasil

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: *Vinicius Cardoso Garcia*

Recife
12 de Dezembro de 2018

Este trabalho é dedicado aos familiares e professores,
que mesmo nas piores horas não me deixaram desistir.

Agradecimentos

Agradeço a todos os meu familiares, pelo apoio e carinho em todos esses anos. Agradeço especialmente a minha mãe, Martha Nusia, minha irmã, Raphaella e ao meu tio, Joaquim Pedro, pois vocês me proporcionaram o direcionamento necessário para que eu soubesse o que fazer. Agradeço a todos os meus professores, em especial ao meu orientador Vinícius Garcia, pela dedicação e paciência para me orientar nesse trabalho de graduação.

Existem mil formas de prisão,mas só uma de liberdade
—EMICIDA (2018)

Resumo

Com o avanço da tecnologia e redução dos preços dos aparelhos móveis, ocorreu uma quebra de paradigma na sociedade brasileira. Sociedade esta que antes utilizava de maneira predominante o computador pessoal para acessar a Internet, agora se utiliza de seus dispositivos móveis para tal acesso. Percebendo essa mudança de paradigma, os atacantes começaram a alterar o seu modo de atuação, saindo do Phishing, que é um golpe com intuito de roubar dados sensíveis através de e-mail, e migrando para o Smishing, ou SMS Phishing, que é um golpe direcionado para os usuários de dispositivos móveis. Este trabalho de graduação se propõe a definir um panorama atual do cenário de Smishing no Brasil, e identificar quais fatores tornam esse tipo abordagem possivelmente mais efetiva do que os Phishings tradicionais, os Phishings enviados via e-mail.

Palavras-chave: Segurança, Phishing, Smishing, Mobile

Abstract

With the advance of technology and the reduction of the prices of mobile devices, there has been a break in Brazilian's society paradigm. This society that once used to predominantly use their personal computer to access the internet, now uses its mobile devices to such access. Realizing this paradigm shift, the attackers began to change their mode of operation, moving away from traditional phishing and migrating to smishing, or sms phishing, which is a targeted blow to mobile device users. This graduation work proposes to define the current perspective of the scenario of smishing in Brazil, and to identify which factors make this type of approach possibly more effective than traditional phishings.

Keywords: Security, Phishing, Smishing, Mobile

Sumário

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

Introdução

1.1 Motivação

Todos os anos, ataques de Phishing, que é um golpe com o intuito de roubar dados sensíveis, são responsáveis por perdas milionárias, em particular para o setor financeiro, pelo fato de ser um ataque de simples execução e com capacidade de atingir um alto número de indivíduos. Uma única campanha de Phishing pode alcançar centenas de milhares de usuários de um banco, ou de serviços populares como Netflix ou Uber. Independente de ser uma parcela pequena de pessoas caindo no Phishing, o dano ainda pode ser milionário, visto que o atacante poderá ter acesso a dados sensíveis como, por exemplo, informações de cartão de crédito, dados pessoais, e até credenciais de acesso. Essas informações podem ser utilizadas para realizar compras online fraudulentas ou, inclusive, para realizar um ataque mais direcionado no futuro, conhecido como Spear Phishing visando um dano financeiro maior. Spear Phishing, são ataques onde o fraudador estuda profundamente às vítimas para construir uma campanha mais efetiva. Geralmente são golpes mais bem elaborados, e com foco em poucas pessoas de renda mais elevada.

Ultimamente uma nova modalidade de Phishing vem ganhando fama entre os atacantes, o Smishing (ou sms phishing). Segundo Assolini (ASSOLINI, 2016), a popularidade do Smishing entre os invasores provavelmente se deve ao fato de cada vez mais pessoas estarem utilizando o internet banking nos seus celulares, cuja segurança é considerada inferior ao do desktop, em conjunto com o baixo custo de envio de SMS em massa.

A desvantagem do Phishing tradicional, Phishing enviado através de e-mail, sobre o Smishing encontra-se no fato de que muitas pessoas não leem seus e-mails diariamente, ou as mensagens suspeitas são automaticamente direcionadas para a caixa de spam. No caso do Smishing, além de não existir uma caixa de spam, existe a notificação do celular, a qual fica constantemente alertando que há um sms novo. Esses fatores contribuem para que uma campanha de Smishing seja mais bem sucedida que a de um Phishing tradicional.

Sendo este o contexto, se torna válida a realização de um levantamento do panorama atual do Smishing no Brasil, visto que apenas conhecendo a ameaça será possível mitigá-la.

1.2 Objetivo

O objetivo principal deste trabalho de graduação é traçar o panorama atual do Smishing, elencando as principais características desse tipo de ataque no Brasil. Será levado em conta a sua infraestrutura, a instituição alvo, técnicas de engenharia social e se o atacante utiliza-se de alguma técnica para prolongar a vida útil da página falsa. Para atingir esse objetivo, será

realizada uma avaliação de URLs coletada' através do PhishTank[1], a qual será armazenada posteriormente numa planilha online.

1.3 Estrutura do Trabalho

Este trabalho está dividido em 5 capítulos,sendo este o primeiro capítulo,cuja estrutura será descrita a seguir:

- Capítulo 2: Capítulo onde é abordado o referencial teórico.
- Capítulo 3: Capítulo onde é descrita a metodologia utilizada.
- Capítulo 4: Capítulo onde é exposto os resultados obtidos através da avaliação.
- Capítulo 5: Capítulo com as considerações finais e possíveis trabalhos futuros.

[1]PhishTank é uma comunidade livre que qualquer um pode submeter, verificar e acompanhar informações de Phishing (PHISHTANK, 2018)

CAPÍTULO 2

Fundamentação Teórica

Neste capítulo, serão apresentados os principais conceitos e pressupostos que estão teoricamente presentes neste trabalho.

2.1 Engenharia Social

Segundo Mitnick (2002 apud ALENCAR; LIMA; FIRMO, 2013) e Soni, Firake e Meshram (2011 apud ALENCAR; LIMA; FIRMO, 2013) "Engenharia social pode ser entendida como uma arte para manipular pessoas, fazendo-as tomar ações que normalmente não fariam para um estranho, normalmente cedendo algum tipo de informação.". Podemos citar também como definições de engenharia social: "A arte e ciência de fazer pessoas realizaram os seus desejos."Bernz (1996 apud GRANGER, 2001), "Engenharia social geralmente é uma manipulação inteligente da tendencia humana em confiar."(GRANGER, 2001) e "Conseguir informações necessárias (por exemplo, uma senha) de uma pessoa sem precisar invadir o sistema."Berg (1995 apud GRANGER, 2001).

Todas as definições citadas acima sobre o significado de engenharia social estão corretas, sendo umas mais específicas que outras. É possível verificar, inclusive, que todas convergem para uma mesma pessoa, o atacante, manipulando outra pessoa, a vítima, a realizar suas vontades de livre escolha, ou seja, sem haver coerção da mesma. Frequentemente a vitima não percebe que sofreu, ou está sofrendo, um ataque de engenharia social.

Segundo Granger (2001), ataques de engenharia social podem ser divididos em dois aspectos, sendo eles: Físico e Psicológico. O Aspecto físico é o ambiente, roupas ou objetos que aumentem o nível de confiança da vítima no atacante. Por exemplo, um atacante usando crachá e farda de uma determinada empresa seria capaz de obter acesso ao escritório e conseguir, de maneira mais fácil, informações privilegiadas, além de poder observar a rotina interna dos funcionários. Já o aspecto psicológico se trata da manipulação da natureza humana, explorando nosso desejo de confiar no outro e nossa aversão a conflitos. Desta forma, como evidenciado por Orgill et al. (2004), a combinação dos dois aspectos frequentemente resulta em um ataque bem sucedido de engenharia social, alcançando a informação desejada pelo atacante.

2.2 Ataque Semântico

Segundo Schneier (2000), um ataque semântico é um ataque computacional que explora as vulnerabilidades humanas. Ao invés de explorar as vulnerabilidades do sistema, os ataques semânticos se aproveitam da maneira como os humanos interagem com os computadores ou

interpretam mensagens. Schneier (2000) prevê que ataques semânticos serão mais sérios do que ataques físicos ou mesmo sintáticos. Pois os ataques semânticos visam diretamente a interface homem/computador, a qual considera ser a interface de maior insegurança da Internet.

Por se tratar de um ataque não técnico, qualquer pessoa, independente do seu nível de conhecimento, seria capaz de realizar um ataque semântico utilizando apenas técnicas de engenharia social, sem a necessidade de exploração de vulnerabilidades ou conhecimento avançado em computação. Além disso, os ataques semânticos são de difícil detecção e prevenção, visto que agem apenas sobre o fator humano. Desta forma, não possuem uma assinatura ou padrão definido para que haja a possibilidade de identificação e bloqueio, destes tipos de ataque, pelas equipes responsáveis.

Esses fatores são os que fazem os ataques semânticos terem um potencial tão perigoso, e serem amplamente utilizados ainda hoje. Pois, ao contrário de outros tipos de ataques os quais deixaram de ser utilizados no decorrer dos anos, sejam por correção de vulnerabilidades, surgimentos de novos protocolos ou padrões já conhecidos, um ataque semântico não possui mitigação fácil, ou efetiva, por ter foco no ser humano e não no computador.

2.3 Crime Cibernético

Para Carvalho (2013) crimes cibernéticos são qualquer tipo de delito cometido, ou sofrido, com a utilização de um computador, uma rede de computadores ou um de dispositivo eletrônico. Ou seja, qualquer crime no qual o computador seja o objeto, sujeito ou instrumento, é considerado um crime cibernético. HERMAN (2013) dá exemplos claros nos quais os computadores assumem cada um desses papéis. O computador assume um papel de objeto de um crime quando há um roubo de software, ou código confidencial, da maquina. Já quando assume um papel de sujeito, o mesmo é utilizado para ataques e tentativas de invasão. Por último o computador assume o papel de instrumento quando é utilizado para enviar mensagens falsas, criação de site fraudulento e propagação de código malicioso.

Partindo dessa definição, é possível concluir que um ataque de Phishing, e suas derivações, pode ser considerado um crime cibernético.

2.4 Phishing

Enquanto que Hong (2012) define phishing como um tipo de ataque de engenharia social, no qual criminosos enviam mensagens eletrônicas se passando por empresas legítimas, Kumaraguru et al. (2009), bem como Zhang et al. (2006), definem phishing como um ataque semântico que se aproveita da falta de conhecimento do usuário de distinguir sites falsos de sites legítimos, em que as vitimas recebem e-mails falsos para capturar suas informações sensíveis. Geralmente esses e-mails se utilizam de engenharia social para causar uma certa urgência na vitima, como, por exemplo, uma multa ou taxa adicional caso ela não realize a atualização cadastral.

"Esses e-mails levam a sites falsos que são semelhantes ou virtualmente idênticos a sites legítimos e atraem as pessoas a divulgar informações confidenciais."(KUMARAGURU et al., 2009). Informações as quais podem ser: credenciais de acesso, dados pessoais, dados bancá-

rios, e de cartão de crédito, ou até mesmo uma *selfie* [1], visto que vários serviços digitais, como bancos e corretoras de investimentos, exigem uma imagem do portador da conta para criação, ou recuperação do acesso, de cadastros.

É possível subdividir o phishing em categorias baseadas no público alvo, no meio de propagação e na técnica empregada. Para este trabalho, serão citados o Spear Phishing, Phishing com Operador, Atendente Impostor, Pharming, Smishing e Vhishing, os quais serão devidamente apresentados neste capítulo.

2.4.1 Spear Phishing

Ao contrário do Phishing tradicional, onde o foco é mais genérico e com o intuito de pegar o máximo possível de vítimas, o Spear Phishing é um tipo de ataque com um público alvo bem definido, onde o atacante tem bastante conhecimento sobre o tipo de pessoa que vai receber a mensagem, o alvo.

Phishing enviado para funcionários de uma organização específica para conseguir credenciais de acesso de um sistema interno, ou um atacante se passando pelo presidente da empresa, solicitando um pagamento urgente e secreto a sua secretaria ou funcionário do financeiro [2], são exemplos genéricos de um ataque de Spear Phishing. Abrangendo para o cotidiano do CIn[3], um exemplo claro de Spear Phishing seria um atacante em posse dos e-mails dos alunos que são, ou foram, monitores, enviar um e-mail se passando pelo Gmon[4]. Esse e-mail informaria que o sistema está prestes a passar por uma mudança de arquitetura, e que todos os comprovantes de monitoria não salvos na máquina do aluno seriam perdidos. No corpo do e-mail teria um link para um site falso do Gmon, que além de pegar as credenciais dos alunos, seria distribuído, também, um software malicioso.

2.4.2 Phishing com Operador

Nessa categoria de Phishing o atacante é notificado, muitas vezes por um painel web, quando uma possível vitima acessa seu site malicioso. O operador, no caso o atacante, verifica algumas características da conexão antes de liberar o acesso da vítima ao servidor. Características essas tais como o provedor de acesso à Internet, user-agent[5] e o referer[6].

Após ter liberado o acesso, o operador interage com a vítima para conseguir dados sensíveis, e até mesmo corrigir informações incorretas que a vítima possa ter digitado. Na prática, enquanto a vitima insere os dados no site falso, o operador preenche os mesmos dados no site legítimo e interage com a vitima de acordo com o que for solicitado no site legítimo. Essa categoria de phishing é muito utilizada em sites que solicitam um segundo fator de autenticação[7],

[1] Auto-retrato

[2] Golpe conhecido como CEO Fraud

[3] Centro de informática da Universidade Federal de Pernambuco

[4] Sistema on-line para gerenciamento das monitorias do centro de informática da UFPE

[5] user-agent é um componente do protocolo http que indica o dispositivo que está efetuando aquela conexão

[6] Refer é um componente do protocolo http que indica o site que o levou para o site atual

[7] O segundo fator de autenticação é uma segurança adicional que ajuda a proteger os usuários que tiverem suas senhas roubadas tanto por phishing ou por vazamento de banco de dados (PETSAS et al., 2015)

ou seja, além da senha é necessário um código único para só então ter acesso ao sistema.

2.4.3 Atendente Impostor

O atendente impostor é um golpe cujo atacante cria um perfil falso em uma rede social, se passando por uma empresa legítima. Esse perfil falso observa os canais oficiais da empresa, a qual ele está imitando, a procura de um cliente insatisfeito ou com alguma dúvida. Quando encontra essa possível vítima, o perfil falso entra em contato reproduzindo um canal oficial de comunicação e solicita alguns dados, geralmente sensíveis, para que o problema da vítima seja solucionado.

Um exemplo prático desse golpe é um cliente reclamando na página oficial de um cartão de crédito sobre seu limite de crédito muito baixo. Nessa hora, o atendente impostor entra em contato com a vítima, através de um chat privado, se apresentando como um canal oficial e se oferecendo para ajudá-la. Durante a conversa, o atacante solicita os dados do cartão de crédito para que o limite seja alterado com sucesso.

2.4.4 Pharming

É uma categoria de phishing no qual é utilizado em conjunto com um servidor DNS[8] malicioso, ou comprometido. Esse servidor DNS resolve o domínio da organização alvo de forma errada, fazendo com que mesmo a vítima digitando o domínio correto da organização, ela seja redirecionada para um site falso, tornando difícil a detecção pela vítima. Normalmente, esse DNS malicioso é configurado na rede da vítima devido à vulnerabilidade no roteador, JavaScript[9] maliciosos ou engenharia social.

Outra característica que diferencia o pharming do phishing tradicional é a infraestrutura na qual ele se encontra. Geralmente são servidores web configurados com virtual hosts[10] com várias páginas de phishing. O servidor redireciona a vítima para o phishing de acordo com o domínio o qual ela está tentando acessar. Ao tentar acessar só o IP do servidor, geralmente é mostrado a página padrão de configuração do servidor.

2.4.5 Smishing

Smishing, ou SMS[11] Phishing, é uma categoria de phishing na qual o atacante utiliza-se de SMS ou aplicativos de mensagens instantâneas[12] para enviar a URL maliciosa, ao contrário do phishing tradicional que se utiliza de e-mail como meio de divulgação do site malicioso.

Visto que smishing foca em usuários com dispositivos móveis, é perceptivo algumas características únicas como as telas elaboradas para dispositivos móveis e restrições de user-agent

[8] Sistema de resolução de nomes

[9] É uma linguagem de programação muita utilizada em sites

[10] "Refere-se a uma prática de servir mais de um site no mesmo servidor. Um Virtual Host pode ser baseado em IP, ou seja, diferentes IPs servindo vários sites no mesmo server, ou ainda baseado em nome de domínio, ou seja, vários domínios servindo no mesmo server."(ROSA, 2016)

[11] Short Message Service, ou serviço de mensagens curtas

[12] O aplicativo mais utilizado, atualmente, nesse segmento é o WhatsApp

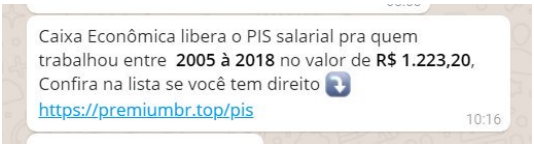
móveis. Como pode ser observado na imagem 2.3, ao acessar a mesma URL[13] tem-se comportamentos distintos de acordo com seu user-agent.

Esse categoria de phishing será o foco principal deste trabalho de graduação no qual, no capítulo 3, será descrito a metodologia utilizada para coletar e avaliar casos de Smishing focado no público brasileiro.

Figura 2.1: Exemplo de Smishing

Fonte: O Autor

Figura 2.2: Exemplo de Smishing através do WhatsApp

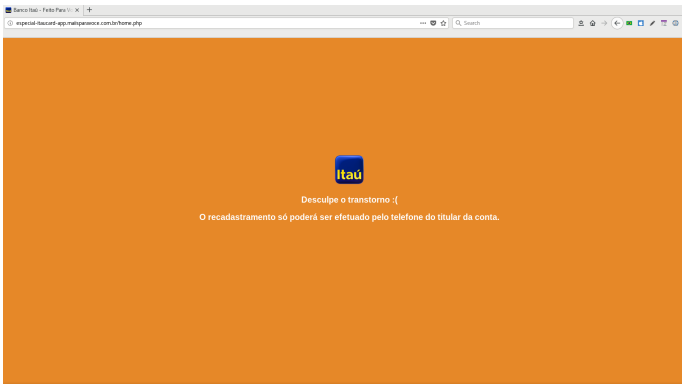


Fonte: Assolini (2018)

[13]http://especial-itaucard-app.maiisparavoce.com.br

Figura 2.3: Exemplo de Smishing com restrição de acesso à dispositivos móveis

(a) User-Agent Desktop



(b) User-Agent Mobile

Fonte: O Autor

2.4.6 Vhishing

Vhishing, ou Voice Phishing, é uma categoria de phishing cujo atraque é realizado através de ligações telefônicas. O atacante liga para vítima imitando um funcionário de uma organização legítima para solicitar informações confidenciais, instruir a vítima à acessar um site falso ou configurar um servidor DNS malicioso em sua rede.

2.5 Infraestrutura do Phishing

A infraestrutura do phishing é composta de host, domínio e certificado, sendo esses dois últimos apenas se aplicáveis, o que torna possível o fraudador coletar os dados das vítimas. O fraudador ainda pode usar uma infraestrutura própria ou se utilizar de um site comprometido para hospedar sua página de Phishing. Um site comprometido é um web-sites legítimo, que sofreu algum ataque e teve sua integridade comprometida. Sobre controle do atacante, este site que até então tinha um comportamento legitimo começa a ser utilizado para atividades maliciosas.

No caso da infraestrutura própria, muitas vezes ela é escolhida pelo atacante por dois motivos:

1. Aumentar a credibilidade da página, com domínios semelhantes ao do site legítimo, ou com certificados válidos.

2. Influenciar o tempo no qual o site falso fica online como, por exemplo, se o fraudador escolher um host que seja mais lento para tratar os violações do seus termos de serviços.

Os fatores que levam um atacante a utilizar um site comprometido como sua infraestrutura são vários. Os mais comuns são:

1. Grande quantidade de sites vulneráveis, seja por:
    - Plugins desatualizados
    - Frameworks desatualizados
    - Usuário padrão
2. Falta de recursos para contratar uma infraestrutura própria
3. Site possui domínio favorável ao ataque

Um ponto negativo de utilizar um site comprometido como infraestrutura do phishing é que ele pode prejudicar a engenharia social, e tende a cair mais rápido. Já que, além do host, o próprio dono real do site pode remover o conteúdo malicioso do ar.

CAPÍTULO 3

Metodologia

Neste capítulo será descrita a metodologia levada em consideração para a elaboração deste trabalho, visando alcançar o objetivo proposto no mesmo.

3.1 Coleta e Classificação

Para alcançar os objetivos deste trabalho será realizado uma avaliação em cima de Smishing reais, coletados através do phishtank de forma automatizada, e de outras fontes de maneira manual. Os critérios para a elegibilidade do Smishing para a avaliação são: Estar online no momento da análise, ser um site malicioso, estar em português brasileiro, não ser duplicado, e ter características de um Smishing. Desta forma, as características são:

- Presença de termos mobile, sms, token, celular, itoken, way no HTML ou no domínio;
- Ser acessível apenas através de user-agent mobile;
- Ter restrição de acesso pelo tamanho da tela;
- Características visuais as quais indique que o site foi projetado para celular e não para computador.

Para ser considerado um Smishing, o site em questão deve ser compatível com, no mínimo, uma das características citadas acima.

3.1.1 Coleta Automática

A coleta automática será feita através de um script[1] em Ruby[2], que irá coletar as urls enviadas de uma lista de usuários. Após a coleta, o script irá salvar informações do registro do domínio, a captura de tela da página, informações do IP e informações do certificado. Para as informações do IP será utilizando a API[3] rest do Shodan[4]. Após a coleta de evidências, as informações serão salvas em uma planilha online, onde será feito a filtragem de URLs aceitas, ou não, para a avaliação.

[1] "Em Informática, script é um conjunto de instruções em código, ou seja, escritas em linguagem de computador. É uma linguagem de programação que executa diversas funções no interior de um programa de computador."(SIGNIFICADO, 2013)

[2] Linguagem de programação

[3] Interface de programação de aplicações

[4] Mecanismo de busca para dispositivos conectados a internet (SHODAN, 2018).

3.1.1.1 Infraestrutura

Para que essa coleta automática seja possível, foi criado uma VPS[5], com o centOS7[6] como seu sistema operacional. Nessa VPS foi instalado o Docker[7], com dois contêineres, o primeiro contêiner é um proxy para o Tor[8], configurado para que o nó de saída seja no Brasil. O segundo contêiner foi configurado com o Ruby, para poder rodar o script.

Essa infraestrutura foi escolhida por dois principais motivos, o primeiro foi a disponibilidade, já que a empresa, que disponibiliza o serviço de VPS, possui vários sistemas de redundância para rede elétrica e para provedor de internet. O segundo motivo foi a praticidade e segurança do Docker, pois, com alguns comandos, toda a infraestrutura já estava ativa e, caso a infraestrutura seja comprometida, ficaria contido no contêiner sem afetar o host.

A escolha do Tor partiu da necessidade de ter uma saída anonimizada e com o IP de origem do Brasil, já que alguns sites falsos restringem o acesso apenas ao Brasil para dificultar a detecção.

3.1.1.2 Usuários no PhishTank

Para a produção deste trabalho foi pesquisado, através de fontes abertas, usuários que postassem Phishing diariamente, e de sua maioria, focados no público brasileiro. Os usuários escolhidos foram:

- DefesaDigital
- ShinobiPhish
- dms
- gambroz
- csirtbb
- ruipatricio

3.1.1.3 Preenchimento da Planilha

O script será responsável pelo preenchimento automático, das urls coletadas, das seguintes colunas na planilha:

- Id no PhishTank
- URL
- Host

[5] Servidor Virtual Privado
[6] Sistema Operacional baseado no GNU/linux
[7] O Docker é uma virtualização de Sistema Operacional baseado em contêineres
[8] The onion router

- Registrar
- Certificadora
- Data de Criação do domínio

3.1.2 Coleta Manual

Além da coleta automática, o autor do trabalho será responsável de coletar Smishing de outras fontes abertas, de forma manual, e adicionar essas URLs na planilha. Fontes essas, como: Twitter, grupos de segurança, notícias de jornal e blog. Nos casos das URLs inseridas de forma manual, no lugar do ID do PhishTank, será colocado o indicador MANUAL seguido de um número sequencial. Por exemplo: Manual1, Manual2 e Manual3.

3.1.3 Planilha Online

Com objetivo de armazenar e classificar as URLs obtida,s tanto na coleta automática quanto na manual, foi utilizado uma planilha online no Google Docs[9]. Todas as URLs presentes na avaliação desse trabalho, sem exceção, se encontrará classificada nessa planilha .

3.1.3.1 Colunas da Planilha

À planilha terá as seguintes colunas, em ordem da esquerda para à direita:

- ID PhishTank
- URL
- CERT
- Host
- Registrar
- Date Domain
- Disponível?
- Smishing?
- Duplicado?
- Pt-Br?
- Aceito?
- Alvo

[9]Conjuntos de aplicações para escritório do Google

- Site Comprometido?
- Restrição por User-Agent?
- Restrição por tamanho da tela?
- SMS solicita Dados?
- Induz Pânico à vítima?
- Induz Euforia à vítima?

3.1.4 Critérios de aceitação e exclusão

Para uma URL ser aceita, terá que ter resposta positiva para as seguintes colunas da planilha:

- Disponível?
- Smishing?
- URL Única?
- Pt-Br?

Caso alguma coluna desta seja negativa, a URL não será elegível para a avaliação.

3.1.4.1 Critérios para URL ser considerada duplicada

Para uma URL ser considerada duplicada ela precisa estar no mesmo host e diretório. Ou seja, mesmo que o protocolo da requisição, ou o arquivo mude, ela será considerada duplicada. Sendo assim, as 4 URls abaixo seriam consideradas uma só:

URLs
http://algumhost.com/algum/diretorio/home.php
https://algumhost.com/algum/diretorio/home2.php
https://algumhost.com/algum/diretorio/home3.php
http://algumhost.com/algum/diretorio/finalizar.php

Tabela 3.1: Exemplo de URLs duplicadas

Enquanto que as 4 URLs abaixo não seriam consideradas duplicadas, e todas entrariam na avaliação:

URLs
http://algumhost.com/algum/diretorio1/home.php
https://algumhost.com/algum/diretorio2/home.php
https://algumhost.com/algum/diretorios/home.php
http://algumhost.com/outrodiretorio/home.php

Tabela 3.2: Exemplo de URLs não duplicadas

3.2 Goal Question Metric

A metodologia escolhida para esse trabalho foi a Goal Question Metric, ou GQM, pois é uma metodologia indicada para situações onde é necessário avaliar um conjunto de dados sobre um conjunto de regras sem perder o foco (BASILI; CALDIERA; ROMBACH, 1999). Para alcançar o objetivo, a GQM divide-se em três níveis: O nível conceitual, o nível operacional e o nível quantitativo.

O nível conceitual é onde se encontra o objetivo (Goal), e ele é definido para um objeto. Objeto esse que pode ser um produto, recurso ou processo. Esse objetivo deve ser definido sobre um conjunto de regras de qualidade, de vários pontos de vista e para um ambiente específico (BASILI; CALDIERA; ROMBACH, 1999).

O nível operacional é onde se encontram as perguntas (Questions). Nele é formulado um conjunto de questões com o propósito de alcançar o objetivo definido no nível conceitual. Nesse nível podem ser formuladas diversas perguntas para atingir o objetivo (BASILI; CALDIERA; ROMBACH, 1999).

O nível quantitativo é onde se encontram as métricas (Metrics). Métricas essas que devem ser associadas a todas as questões, para respondê-las de forma quantitativa. As métricas podem ser objetivas ou subjetivas, e podem ser utilizadas para responder mais de uma questão (BASILI; CALDIERA; ROMBACH, 1999).

GQM	ID	Valor
GOAL	G	Analisar URls de smishing com o propósito de definir o panorama atual de smishing no contexto do Brasil
Question	Q1	Os fraudadores utilizam infraestrutura própria ou comprometida ao realizar ataques de smishing?
Metric	M1	Porcentagem de sites comprometidos
Question	Q2	Quais empresas os fraudadores mais utilizam para montar a sua infraestrutura
Metric	M2	Host mais utilizados para hospedar o smishing
Metric	M3	Empresas que registram domínios mais utilizado para registrar o domínio malicioso
Metric	M4	Empresa que mais emite certificado para o smishing
Question	Q3	Quais são as empresas alvo desse tipo de ataque
Metric	M5	Empresas focadas pelo ataque
Question	Q4	O smishing é um ataque mais direcionado?
Metric	M6	Restrição de acesso por User-Agent
Metric	M7	Restrição de acesso por Tamanho de Tela
Metric	M8	A mensagem induz pânico ao usuário no contexto de um dispositivo pessoal
Metric	M9	A mensagem induz euforia ao usuário no contexto de um dispositivo pessoal
Metric	M10	O emissor solicita por SMS que o usuário forneça ou atualize seus dados

Tabela 3.3: Goal Question Metric do trabalho

Baseando-se nas definições de Basili, Caldiera e Rombach (1999), foi definido um conjunto GQM para esse trabalho de graduação. Esse conjunto pode ser observado na tabela 3.3. Foram definidos um total de 4 perguntas e 10 métricas para auxiliar a atingir o objetivo traçado. As medições propostas para esta avaliação, foram realizadas pelo autor deste trabalho.

CAPÍTULO 4

Resultado

Neste capítulo será apresentado os resultados gerados pela avaliação proposta neste trabalho. Uma lista completa das URLs aceitas, pode ser visualizada no apêndice A.1. No total foram avaliadas 526 URls, destas 88 foram consideradas elegíveis para a avaliação.

4.1 Q1) Os fraudadores utilizam infraestrutura própria ou comprometida ao realizar ataques de Smishing?

Esta primeira pergunta tem como objetivo entender se os atacantes preferem utilizar uma infraestrutura própria, ou se preferem sites de terceiros que tiveram sua segurança comprometida e por conta disto estão sobre o controle do fraudador. É importante entender esse aspecto do ataque pois, como mencionado anteriormente no capítulo de referencial teórico, as duas opções tem suas vantagens e desvantagens para o Atacante.

Para conseguir responder essa pergunta foi utilizado a métrica M1, porcentagem de sites comprometidos. Para determinar se um site foi comprometido ou registrado pelo fraudador, as informações do domínio foram levadas em conta. Informações tais como: Data de criação, Nome do registante, informações de contato do registrante e semelhança do domínio com sites legítimos.

4.1.1 M1) Porcentagem de sites comprometidos

Comprometido?	Número de Sites	Porcentagem
Sim	23	26.14%
Não	65	73.86%

Tabela 4.1: Porcentagem de sites comprometidos.

Como é possível ver na tabela 4.1, a grande maioria de sites utilizados em ataques de Smishing, avaliados neste trabalho, são sites em que o atacante utiliza-se de infraestrutura própria. Isto pode indicar uma grande facilidade dos fraudadores de adquirir os recursos necessários para esse tipo de ataque.

4.2 Q2) Quais empresas fraudadores mais utilizam para montar a sua infraestrutura

Essa questão aborda quais as empresas os atacantes mais se utilizam para montar as infraestruturas utilizadas nos ataques de Smsihing. Para essa questão serão levados em conta as empresas de hospedagem, de registro de domínio e certificadora de domínio. Já que esse foi considerado o trio básico para um ataque de Smishing.

Para essa pergunta só serão levados em contas os sites que não foram comprometidos, ou seja que o próprio atacante montou a infraestrutura.

4.2.1 M2) Os hosts mais utilizados para hospedar Smishing

A primeira métrica utilizada para responder esta pergunta(Q2) é quais empresas de os atacantes se utilizam mais para hospedar os seus sites fraudulentos. Na tabela 4.2 é possível ver as 10 empresas de hospedagem mais utilizadas por atacantes, das URLs contidas nesta avaliação. Na imagem 4.1 é possível visualizar todas as empresas de hospedagem utilizadas por atacantes nesta avaliação.

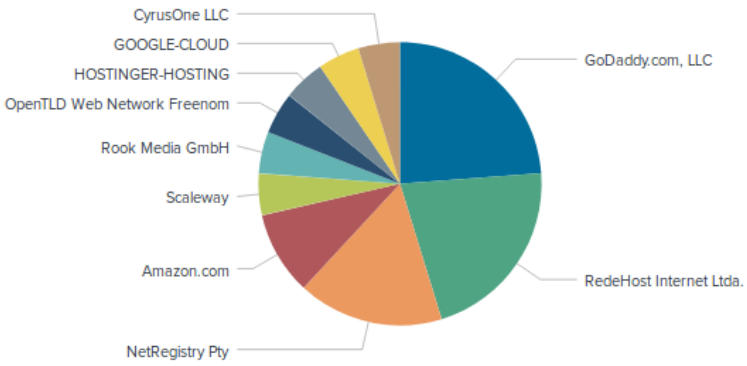
Hosts	Quantidade	Porcentagem
GoDaddy.com, LLC	10	15.384615%
RedeHost Internet Ltda.	9	13.846154%
NetRegistry Pty	7	10.769231%
Amazon.com	4	6.153846%
Scaleway	2	3.076923%
Rook Media GmbH	2	3.076923%
OpenTLD Web Network Freenom	2	3.076923%
HOSTINGER-HOSTING	2	3.076923%
GOOGLE-CLOUD	2	3.076923%
CyrusOne LLC	2	3.076923%

Tabela 4.2: Top 10 empresas de hospedagem mais utilizadas por atacantes.

As empresas de hospedagem mais utilizadas pelos atacantes são em grande maioria, única exceção é a RedeHost, empresas estrangeiras e de grande porte. É possível que por serem grandes empresas, receberem bastantes chamados, o seu tempo de resposta à incidentes cibernéticos sejam mais elevados, ou simplesmente nessas empresas os atacantes tem maior facilidade para usufruir de seus serviços.

A empresa mais utilizada para hospedagem de Smishing pelos fraudadores foi a Godaddy, é fácil encontrar diversos relatos na internet sobre a lentidão da Godaddy para desativar conteú-

Figura 4.1: Gráfico em pizza das empresas de hospedagem.

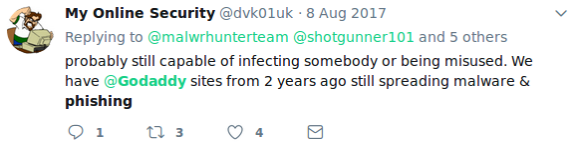


Fonte: O Autor

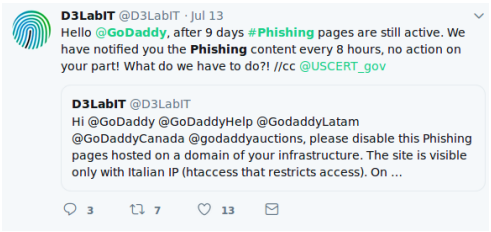
dos maliciosos reportados à eles. Na figura 4.2 é possível ver o relato de dois usuários da rede social Tweet sobre a demasiada demora da Godaddy para remover o conteúdo reportado. É provável que este seja o principal possível que os atacantes recorram à Godaddy para hospedar os seus sites fraudulentos, pois quanto maior o tempo online maior é a probabilidade de uma possível vítima cair no golpe.

Figura 4.2: Relato de pesquisadores de segurança no Tweet, sobre a lentidão da GoDaddy para remoção de conteúdo malicioso

(a) Relato do @dvk01uk



(b) Relato do @D3LabIT



Fonte: O Autor

4.2.2 M3) Empresas que registram domínios mais utilizado para registrar o domínio malicioso

Esta métrica leva em consideração as empresas mais utilizadas para registro de domínios maliciosos. Nesta métrica não foram considerados as URLs que eram só ip, ou seja não tinham domínio. Na tabela 4.3 é possível observar as empresas de registro mais utilizadas pelos atacantes nas URLs avaliadas neste trabalho. Na imagem 4.3 é possível observar todas as empresas

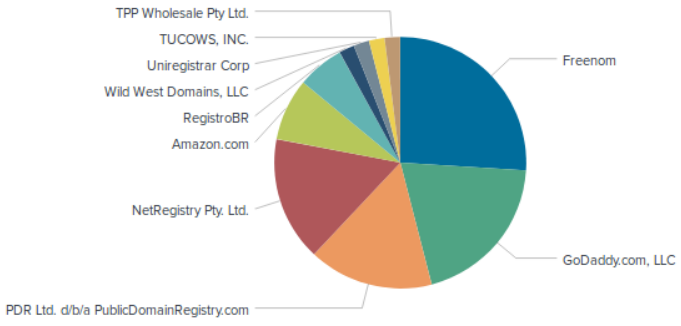
de registro de domínios utilizadas pelos atacantes.

A empresa mais utilizada para registrar os domínios maliciosos das URLs desta avaliação foi a Freenom. Que segundo a própria (FREENOM, 2018) é a maior, e única , empresa de hospedagem que oferece registro de domínio totalmente gratuito. A empresa realiza registro de domínios de graça para os seguintes TLDs[1]: .tk, .ml, .qg, .cf e .ga. Além da gratuidade a realização de novos cadastro na Freenom é demasiadamente fácil e rápida. Tornam-se assim a principal escolha para registro de domínio malicioso do fraudadores, que tiveram suas URLs avaliadas neste trabalho.

Empresa que registrou o domínio	Quantidade	Porcentagem
Freenom	13	22.413793%
GoDaddy.com, LLC	10	17.241379%
PDR Ltd. d/b/a PublicDomainRegistry.com	8	13.793103%
NetRegistry Pty. Ltd.	8	13.793103%
Amazon.com	4	6.896552%
RegistroBR	3	5.172414 %

Tabela 4.3: Empresas de Registrar que apareceram mais de uma vez na avaliação.

Figura 4.3: Gráfico em pizza das empresas de registro de domínios.



Fonte: O Autor

4.2.3 M4) Empresa que mais emite certificado para Smishing

Esta é a última métrica da Q2, e nela é abordado as empresas que mais emitiram certificados para páginas falsas. Para essa métrica só serão consideradas as URLs, contidas nesta avaliação,

[1]Domínios de alto nível

que possuem certificados válidos. Na tabela 4.4 é visível as certificadoras que mais apareceram, nos Smishing contidos neste trabalho.

Certificadora	Quantidade	Porcentagem
Let's Encrypt	5	45.454545%
cPanel, Inc.	3	27.272727%
GoDaddy.com, Inc.	1	9.090909%
DigiCert Inc	1	9.090909%
COMODO CA Limited	1	9.090909 %

Tabela 4.4: Empresas certificadoras mais utilizadas em Smishing.

Dois fatos são bem nítidos ao visualizar à tabela 4.4: Pouquíssimos Smishing utilizam-se de certificados e a Let's Encrypt é a certificadora mais usada, com uma vantagem considerável para a segunda posição, pelos responsáveis pelos ataques de Smishing. É provável que este fato aconteça, por conta da gratuidade e praticidade de emitir um certificado através da Let's Encrypt. A Let's Encrypt apenas válida se a pessoa que está gerando o certificado possui controle sobre o domínio que o certificado será emitido. Tornando-se assim fácil para um fraudador registrar um domínio suspeito e gerar um certificado válido para ele.

4.3 Q3) Quais são as empresas alvo deste tipo de ataque?

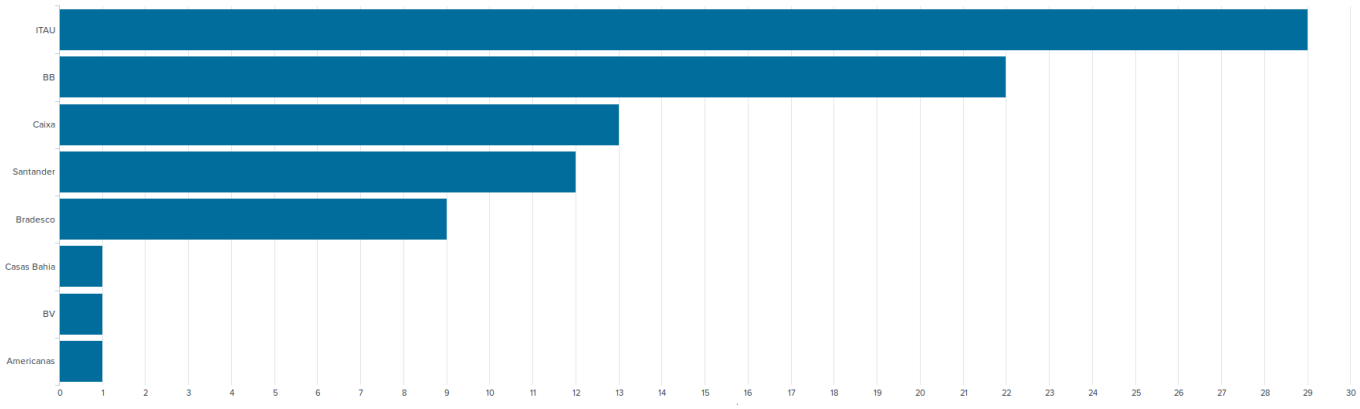
Esta pergunta tem como objetivo determinar, quais empresas os fraudadores focam mais ao realizar ataques de Smishing. Com isso saber qual setor, ou áreas, os atacantes tem mais interesse.

4.3.1 M5) Empresas focadas pelo Ataque

Esta métrica leva em consideração todas as empresas que foram atingidas, pelos Smishings selecionados para esta avaliação. Na imagem 4.4 é possível identificar as empresas que mais foram focadas pelo atacantes. Fica claro que o principal alvo dos fraudadores é o setor financeiro. As duas únicas empresas que não são do setor financeiro são lojas onlines, porém a objetivo dos atacantes não é roubar as credenciais de acesso destas lojas. O objetivo principal é utilizar elas para atrair possíveis vítimas, e roubar os dados de cartão de crédito.

A empresa mais atingida por estes ataques foi o Banco Itaú com quase um terço a mais de ataques que o segundo colocado, o banco do Brasil. Já era esperado que a empresa mais atingida por Smishing fosse uma empresa do setor financeiro. Por serem empresas que lidam com dinheiro diretamente, às informações confidenciais dos seus clientes são mais facilmente monetizadas pelos fraudadores. Além de que estas informações têm um potencial de dano muito maior, do que credenciais, ou informações sigilosas, de outros tipos de empresas onlines.

Figura 4.4: Empresas atingidas pelos ataques de Smishing.



Fonte: O Autor

4.4 Q4) O smishing é um ataque mais direcionado?

Esta pergunta tem como objetivo de esclarecer se os ataques de Smishing são mais direcionados que ataques de Phishing tradicionais, via e-mail. Para auxiliar a resposta desta pergunta, foram traçadas 4 métricas. Sendo elas: M6,M7,M8,M9 E M10

4.4.1 M6) Restrição de acesso por User-Agent

Essa métrica foi definida para determinar a porcentagem de Smishing que utilizam restrição de User-agent, User-agent é um parâmetro do protocolo HTTP que serve para indicar qual o dispositivo utilizado. Ou seja, uma restrição por User-agent seria quando o atacante validasse o User-agent e deixasse a página falsa visível apenas para os User-agents de dispositivos móveis.

Provavelmente os atacantes se utilizam-se desta técnica para que os seus site falsos fiquem mais tempo online e demorem mais para serem descobertos e reportados para os responsáveis[2].

Na tabela 4.5 é possível visualizar que aproximadamente 30% das URLs analisadas neste trabalho utilizaram-se de restrição por User-Agent

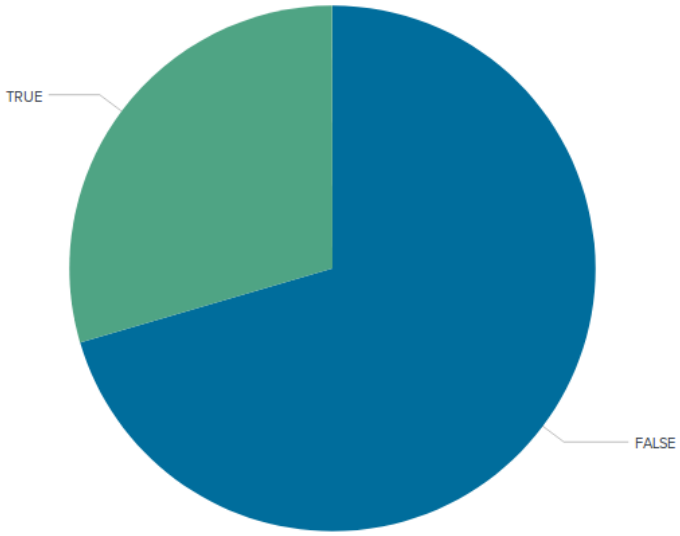
Restrição por User-Agent?	Número de Sites	Porcentagem
Sim	26	29.54%
Não	62	70.46%

Tabela 4.5: Porcentagem de Smishing com restrição por User-Agent.

[2]Os responsáveis são qualquer pessoa/entidade capaz de retirar o site do ar.

A porcentagem de URLs com restrição por User-Agent é , consideravelmente, alta e mostra que quase um terço das campanhas de Smishing analisadas neste trabalho tinha uma restrição por User-agent.

Figura 4.5: Representação gráfica das campanhas que usam restrição por User-Agent.



Fonte: O Autor

4.4.2 M7) Restrição de acesso por tamanho de tela

A porcentagem de Smishing que utilizam restrição de tamanho de tela, é uma técnica utilizada por fraudadores com objetivo de evitar o acesso por pessoas que não sejam possíveis vítimas.

É provável que os atacantes se utilizem desta técnica para que os seus site falsos fiquem mais tempo online e demorem mais para serem descobertos e reportados para os responsáveis. Essa técnica pode ser tanto implementada no JavaScript ou CSS da página falsa. Um exemplo de implementação desta técnica é a imagem 2.3.

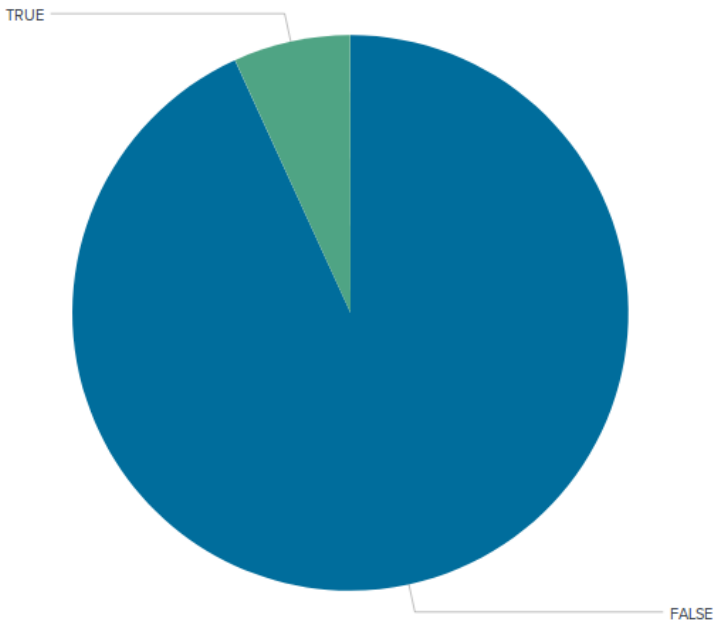
Na tabela 4.6 é possível observar que uma porcentagem baixa de URLs tem restrição por tamanho de tela.

Restrição por Tamanho de Tela?	Número de Sites	Porcentagem
Sim	6	6,8%
Não	82	93,2%

Tabela 4.6: Porcentagem de Smishing com restrição por tamanho de tela.

É provável que este resultado seja pelo fato de ser uma técnica nova e ainda não muito difundida pelos atacantes. Este tipo de restrição é mais eficiente que a restrição de acesso por User-Agent, principalmente se for implementada no CSS. Pois um simples plugin no navegador que altere a requisição HTTP é o suficiente para contornar a restrição por User-Agent.

Figura 4.6: Representação gráfica das campanhas que usam restrição de tela.



Fonte: O Autor

4.4.3 M8) A mensagem induz pânico ao usuário no contexto de um dispositivo pessoal.

Esta métrica é para determinar se os fraudadores utilizam engenharia social nas mensagens enviadas para as possíveis vítimas, para causar pânicos nas mesmas e fazer com que elas confiem mais facilmente na mensagem e no site fraudulento.

Como este trabalho não abordou as mensagens SMS originais das campanhas de Smishing, foi adotado outra estratégia para poder coletar essa métrica. A partir da mensagem exibida no HTML do Smishing, que foi determinado se aquela campanha originou ou não de uma mensagem que causasse pânico na possível vítima. Para que esta métrica fosse possível, foi determinado que O HTML da página falsa possuísse alguma das seguintes afirmações: Mencionar Bloqueio de conta, Mencionar multa, Solicitar atualização cadastral, mencionar desbloqueio da conta.

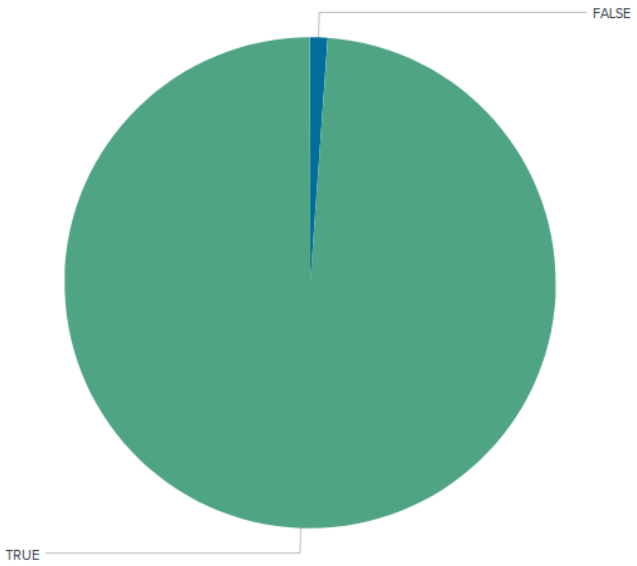
É possível visualizar na tabela 4.7 que a grande maioria das campanhas estudadas na avaliação deste trabalho pretendia causa pânico em suas possíveis vítimas. Provavelmente isso se

Causa pânico?	Número de Sites	Porcentagem
Sim	86	99%
Não	2	1%

Tabela 4.7: Porcentagem de Smishing que pretendem causar pânico nas possíveis vítimas.

deve ao imediatismos do SMS, os atacantes se aproveitam deste fator importante do SMS e adicionam o pânico para baixar a guarda das suas possíveis vítimas.

Figura 4.7: Representação gráfica das campanhas que causam pânico.



Fonte: O Autor

4.4.4 M9) A mensagem induz euforia ao usuário no contexto de um dispositivo pessoal.

Esta métrica é bastante similar a M8, no sentido que para avaliar ela também seria necessário as mensagens SMS originais dos golpes. Similar também ao que se refere a solução, para ela também foi determinado alguns parâmetros no HTML da página falsa para constituir esse métrica. Sendo esses parâmetros a identificação das seguintes situações no HTML: Mostrar uma oferta imperdível, fazer menção à ser a última oportunidade da possível vítima aproveita a situação e fazer menção a taxas de juros muito baixas. Se algumas destas pontos for encontrado

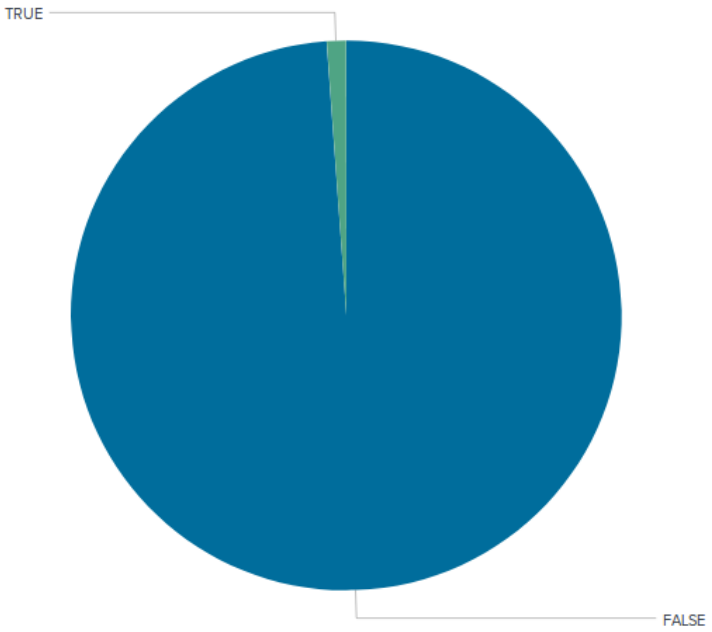
no Smishing, ele será considerado como causador de euforia na possível vítima.

Causa Euforia?	Número de Sites	Porcentagem
Sim	2	1%
Não	86	99%

Tabela 4.8: Porcentagem de Smishing que pretendem causar euforia nas possíveis vítimas.

É possível observar na tabela 4.9 que o número de campanhas que causam euforia, nas possíveis vítimas é extremamente baixo. É provável que se esse estudo fosse realizado durante o mês de novembro, devido ao período de Black Friday[3] os resultados fossem bem diferentes. Os atacantes possivelmente ficariam mais tentados a utilizar a Black Friday como tema das suas campanhas maliciosas, e criar mais páginas falsas imitando as lojas onlines brasileiras.

Figura 4.8: Representação gráfica das campanhas que causam euforia.



Fonte: O Autor

[3]Período em a maioria das lojas fazem grandes liquidações.

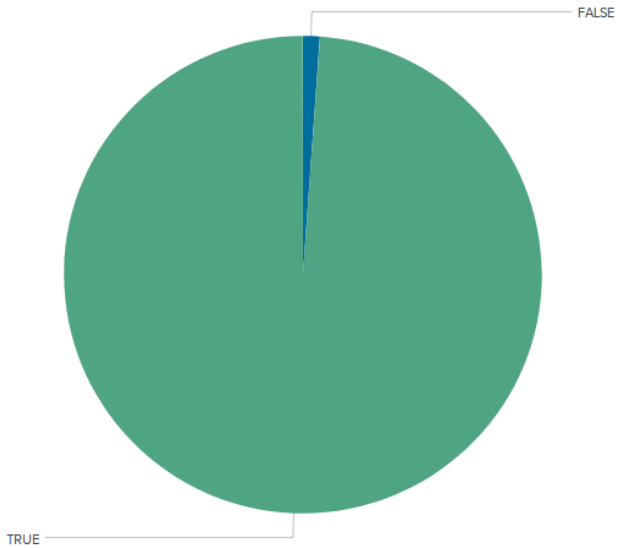
4.4.5 M10) O emissor solicita por SMS que o usuário forneça ou atualize seus dados.

A métrica M10 também compartilha dos problemas é soluções das métricas M9 e M8. Sendo o seu objetivo principal determinar se os fraudadores tem como foco maior as credenciais de acesso das suas possíveis vítimas. Para determinar se é esse o interesse ou não dos atacantes, será levar em conta alguns comportamentos do Smishing. Como por exemplo: Ele mencionar atualização cadastral, credenciais de acessos serem as únicas informações solicitadas e informar que a conta está bloqueada ou que algum mecanismo de controle de acesso expirou.

Solicita dados?	Número de Sites	Porcentagem
Sim	86	99%
Não	2	1%

Tabela 4.9: Porcentagem de Smishing que tem como objetivo principal solicitar dados das suas vítimas.

Figura 4.9: Representação gráfica das campanhas que solicitam dados.



Fonte: O Autor

É bastante expressivo a quantidade de URLs que tem como o foco principal solicitar credenciais de acesso de suas possíveis vítimas. Provavelmente esse alto número se deva ao fato que a grande maioria das campanhas sejam focadas no setor financeiro, e as credenciais de

acesso são as informações mais sensíveis nesse caso. Em posse destas informações o atacante consegue impersonar a vítima e causar um prejuízo, muitas vezes grande.

CAPÍTULO 5

Conclusão

O objetivo principal deste trabalho de graduação foi realizar uma avaliação de várias URLs de Smishing para determinar qual o panorama atual deste tipo de golpe especificamente no Brasil. Para auxiliar nesta avaliação foi definido um conjuntos de perguntas e métricas, conjuntos esses baseados na metodologia GQM. Para que esta avaliação fosse possível, foi montado uma infraestrutura composta por dois containers do Docker. Sendo o primeiro container responsável pela utilização da rede Tor, a rede Tor foi escolhida por dois motivos principais: Burlar uma possível restrição de ip, já que nela é possível escolher qual país você quer para seu ip de saída, e manter o anonimato do autor deste trabalho. O segundo container, é o container responsável pela execução do script de coleta das URls. Foi utilizado a metodologia de containers, para a infraestrutura deste trabalho, com o intuito de proteger a máquina em caso de qualquer possível comprometimento.

Durante o decorrer desta avaliação foram encontradas certas dificuldades, dificuldades essas relacionadas à coleta e disponibilidade dos casos de Smishing. Não foi possível ter acesso às mensagens de fraude utilizadas neste tipo de golpe, alguns Smishing caíram antes de poderem ser analisados, restrição de fontes de Phishing brasileiros, bloqueio do Phishitank ao IP do Tor depois de um determinado tempo e curto período para coletar as URLs. As soluções adotadas pelo autor, para minimizar, ou resolver, estas dificuldades foram: Analisar o código fonte da página falsa de maneira mais aprofundada,para poder realizar deduções sobre a mensagem original; diminuir o tempo em que o script era executado, e o autor visualizar mais vezes a planilha por dia; conseguir o maior número de usuários do Phishitank que possuíssem uma cadencia alta de envios e que em sua grande maioria estes envios fossem de sites focando o publico brasileiro; criação de um script para trocar a saída do Tor à cada 12 horas.

O cenário atual de Smishing no Brasil constitui-se de sites, em sua grande maioria, com infraestrutura construída pelo autor do ataque, em empresas que oferecem serviços gratuitos ou que demoram bastante para poder retirar o conteúdo malicioso do ar. Além disto, os atacantes utilizam técnicas, de engenharia social ou programação, para aumentar a efetividade do golpe e dificultar a detecção dele por pesquisadores de segurança, empresas de anti-vírus, equipes de resposta à incidentes equipes de suporte das empresas de hospedagem e registro dos domínios . Neste trabalho, mais de um terço das URLs tinha alguma restrição de acesso, e todas as URLs se utilizavam de engenharia social para baixar a guarda das possíveis vítimas.

5.1 Possíveis trabalhos futuros

Algumas sugestões para possíveis trabalhos futuros são:

- Realização de uma avaliação com um período de tempo mais longo;
- Realizar um trabalho que compare diretamente o Phishing e Smishing, com o intuito de determinar qual dos dois ataques é mais utilizado, e qual dos dois ataques tem a melhor efetividade;
- Realizar análise aprofundada nas mensagens SMS, ou enviadas via aplicativo de mensagens, com o objetivo de entender o fluxo do golpe do começo ao fim. Além de identificar outras características deste tipo de ataque, que são perceptíveis apenas com a análise da mensagem inicial;
- Realizar um trabalho focado em sites comprometidos e as causas deste comprometimento.

CAPÍTULO 6

Assinaturas

José Durval Carneiro Campello Neto
Aluno

Vinicius Cardoso Garcia
Orientador

APÊNDICE A

Lista de URLs Aceitas para a avaliação

Na tabela A.1, logo abaixo, se encontra toda as URLs aceitas para este trabalho. A orientação da tabela foi altera, para que a mesma coubesse nas páginas deste trabalho.

Tabela A.1: URLs Aceitas para a avaliação

IDS	URLS
5827979	http://104.196.191.148/itau
5825744	http://187.99.219.3:422/itau30horas/
5816904	http://198.46.198.139/bb.com.br/
5836782	http://212.47.229.179/caixa/
5837500	http://217.61.14.117/inicio.php
5829730	http://51.158.67.118/
5816900	http://acesso-aphome.com/BB-desbloqueio/redir.php
5836783	http://activelink.in/wp-content/themes/pessoa-fisica/
5840767	http://agafer.com.br/Multiplus-Bradesco/
5827752	http://ajudatualizacao-itau-app.maisparavocesempre.com.br/
5829357	http://akamawa.unusa.ac.id/banco.bradescocom/
5836381	http://appacesso.top/bdobrasil/mobi_two.php
5819385	http://atendimobile.ml/pf/
5766449	http://atualize-cadas-bb.hol.es/brasil/
5830778	http://bancodobrarsil.com/BB/notificacao.html
5837989	http://bancoitau-cl.tcslegals.com/
1785451	http://bbpromocao.vacau.com/bb/acessoseguro
5827149	http://caixacefverfinfo-cc.umbler.net/c/
5838214	http://caixagovapp.site/
5838431	http://centralatendimentoaocliente-com.umbler.net/xamp/
5827429	http://clienteappdesbloqueio-com.umbler.net/
5833687	http://clientebb.cf
5818906	http://clienterelacoescomclientes.info/loginclienteseguros/login.do2562.html
5833261	http://clientesegurancaseg1.com/segurancadocliente1/login.do2562.html
2022393	http://countryimoveis.com.br/SIIBC/internetbanking/caixa.gov.br-processa/
5837671	http://davincihombre.es/web/wwwbanco.bradesco.com.br//atendimento_bradesco/home.php
5827171	http://desbloqueio.itau20cadastramento.ml/
5836719	http://ec2-54-205-120-64.compute-1.amazonaws.com/9D713DH913DH13D1H3D/acesso/
5829354	http://emporioopticomt.com.br/banco.bradesco.com.br/

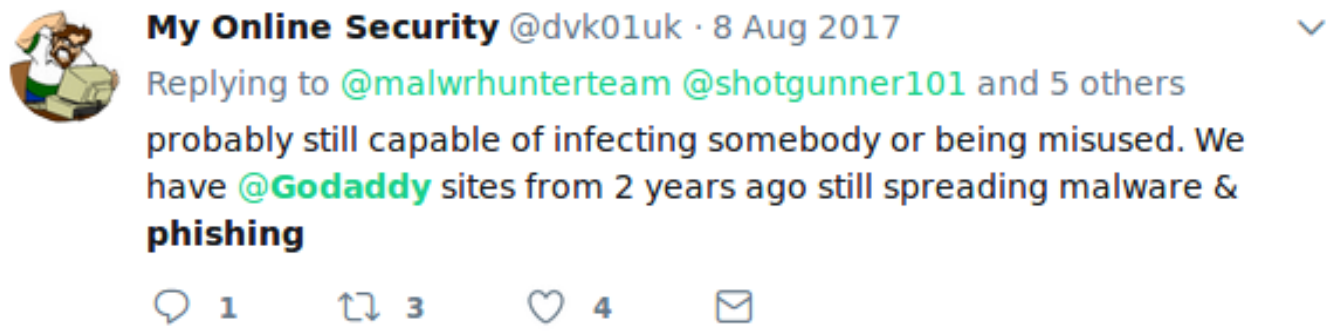
5827176	http://especial-itaucard-app.maiisparavoce.com.br/
5837783	http://file-top.ru/acessomobi/
5827958	http://imovelcorret.gq/c@/?cliente=sbt@sbt.com.br
5826093	http://itafaturadigital.com/promocao/descontao/card/home.php
5828437	http://itau-com.cf/
5828287	http://itauypontos.com/envio1.?php
5838803	http://magazineluazul.com/santa/
5840373	http://m-americanas-oferta.com
5836797	http://minha.bv.com.br.login.wpys.online/v2/1/
5829760	http://mobi-app.umbler.net/atualizacao/
1943224	http://modulodeatualizacao.freeiz.com/Segurancabra/
5836493	http://multiconsp.com.br/01Multiplus-Caixa-Resgate-de-pontos/Expiracao-Pendente-de-Resgate.jpg/
5827390	http://multiplus-itau-card.com/promocao/descontao/card/home.php
5838441	http://pmm.ac.in/wwwbanco.bradesco.com.br/
1304565	http://portalbb.h16.ru/confirma/
5827607	http://promo-itau-plus.com/promocao/descontao/card/home.php
5829717	http://registerempresas.ga/c@/?cliente=sbt@sbt.com.br
5834130	http://regularizacaodoclientecomseguranca.com/segurocadastro/carregandosms.php
5835837	https://activelink.in/pessoa-fisica/
5217626	http://santander-seguranca.ga
5837752	https://comprarsemprebem.com/Magazine/santa/
5837751	https://comprecertosempre.com/Magazine/santa/
5815940	http://segurancadosclientesregularize.info/alertascodes/#
5837472	http://segurannncas.ddns.net/mobile/
5826633	http://serve-org.com/cf/credenciais.html
5826702	http://servico-on-sms.ga/sms/seguranca_30horas/mobi.php
5835598	http://seudescontoconjunto.com.br/mobile/login.php?skullid=MjE5OTM4NzY2Jjc=
5827956	https://faturaitau.com/login.php
5806546	https://mareabilitacao.com.br//convenios-5565656/pagina-santander-way/idd255151151/
5829761	https://moduloatualiza.ml/
5829755	http://smscaixa-com.umbler.net/
5828131	https://phone-br.com/2018/acesso.php

5829715	https://pj-sincronismoempresa.com/mobile/acesso.php
5829510	https://portalseguro.gq/caixa
5829302	https://promo-itau-card-br.com/promocao/descontao/card/home.php
MANUAL1	https://secure75.securewebsession.com/app-sms.com/home-caixa/mobile/
5839454	https://seguro3.sfo2.digitaloceanspaces.com/seguranca.html
5826749	https://servico-on-sms.ga/sms/seguranca_30horas/pf/mobi_I.php
5836435	https://www.bbestiloacesso.org/
5836917	http://tudo-o-que-voce-precisa-com.umbler.net/http/
5829351	http://users.atw.hu/balassafa/banco.bradesco.com.br/atendimento_bradesco/
5825743	http://validar-itau.serveirc.com:422/itau30horas
5825795	http://viralereal.com/itau/cc/confirma.php
5828465	http://witau.com/
5835362	http://www.acesse-pbb-mobi.tk/taxa-debito-sms/bb/pessoa-fisica/session.php
5406876	http://www.avisobbsms.cf/bb-app/
5836856	http://www.bbestilocliente.net/clientes/l/EAakBeqzLI5i6xeN892NPsQQ/tbu1VM6UMTqPTzGbz2BlqQ/ql4P2tNeaK1YXH7HzbyGBg
5822350	http://www.bbnet-online.com
5839444	http://www.chimae.co.kr/bbs/mobile/
2633461	http://www.gas-srl.it/SincroniaRenovada-Itau30Horas-2014/
5839451	http://www.graeffimoveis.com.br/site/img/mobile
5838435	http://www.hoszivattyu.egylap.hu/wwwbanco.bradesco.com.br/atendimento_bradesco/home.php
5833786	http://www.hrw.cl///ambiente_seguro/Sincronizar
5839786	http://www.it-gas.ru/assets/images/acessarxphome/
1931945	http://www.londonshop.com.br/Bradesco.com.br/
5836797	http://www.netbb-online.com
5817892	http://www.suacasamaischique.com.br/mobile/login.php
5837720	http://www.taxpark.com/mainfile/images/ID/Portal/Way.af_Smiles-Gol.dll=login.AF_Login/cadastrando.php
2603953	http://www.tsrpc.org/images-c/?BancodoBrasil

APÊNDICE B

Relatos Sobre a Godaddy

Figura B.1: Exemplo de relato sobre a Godaddy do usuário @dvk01uk

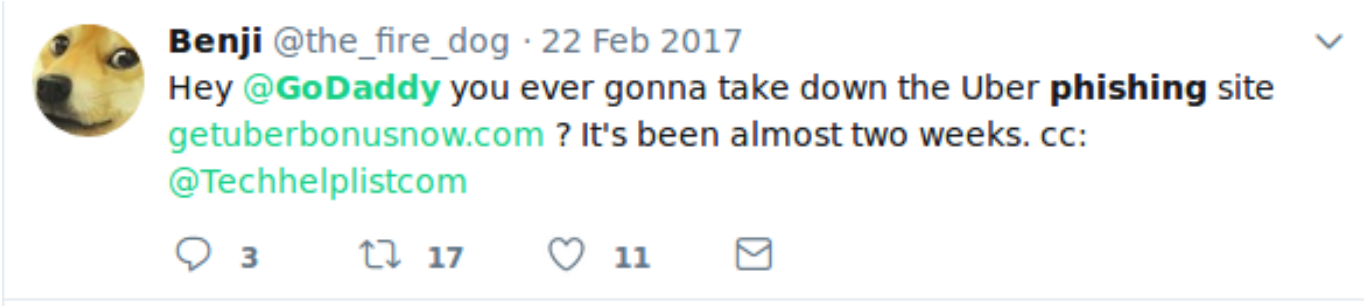


Fonte: O Autor

Figura B.2: Exemplo de relato sobre a Godaddy do usuário @D3LabIT

Fonte: O Autor

Figura B.3: Exemplo de relato sobre a Godaddy do usuário @the$_{f}ire)dog$

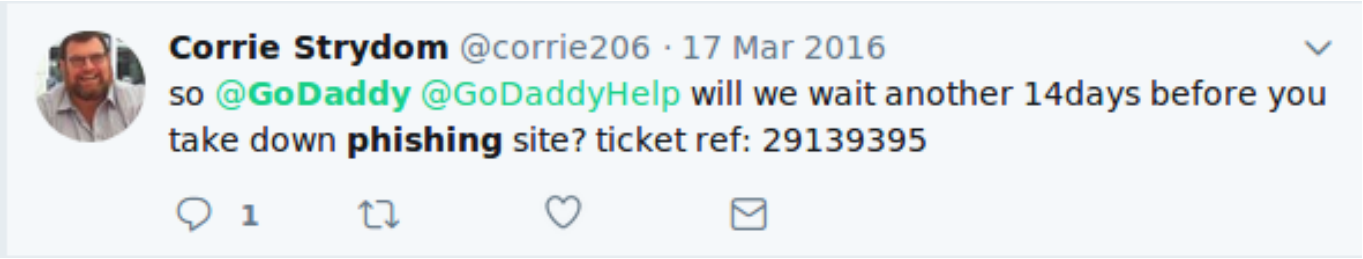


Fonte: O Autor

Figura B.4: Exemplo de relato sobre a Godaddy @itskimbotem

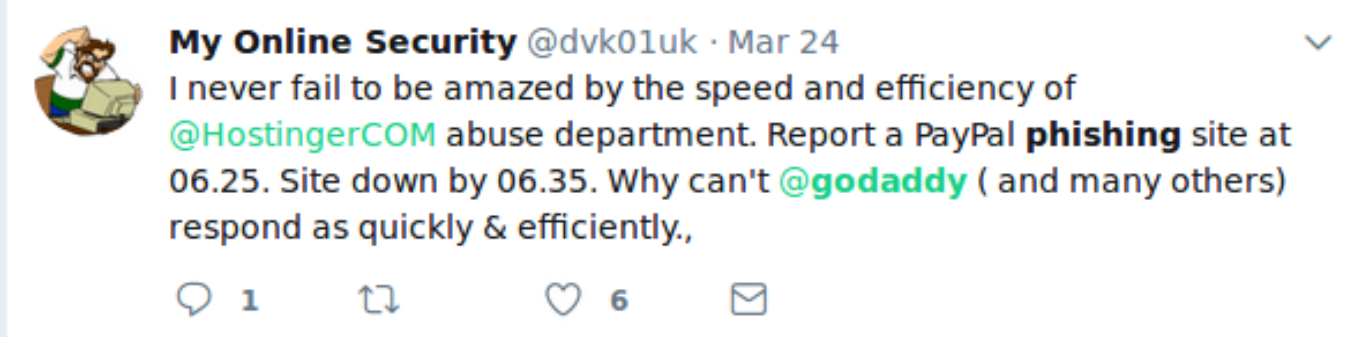
Fonte: O Autor

Figura B.5: Exemplo de relato sobre a Godaddy do usuário @corrie206



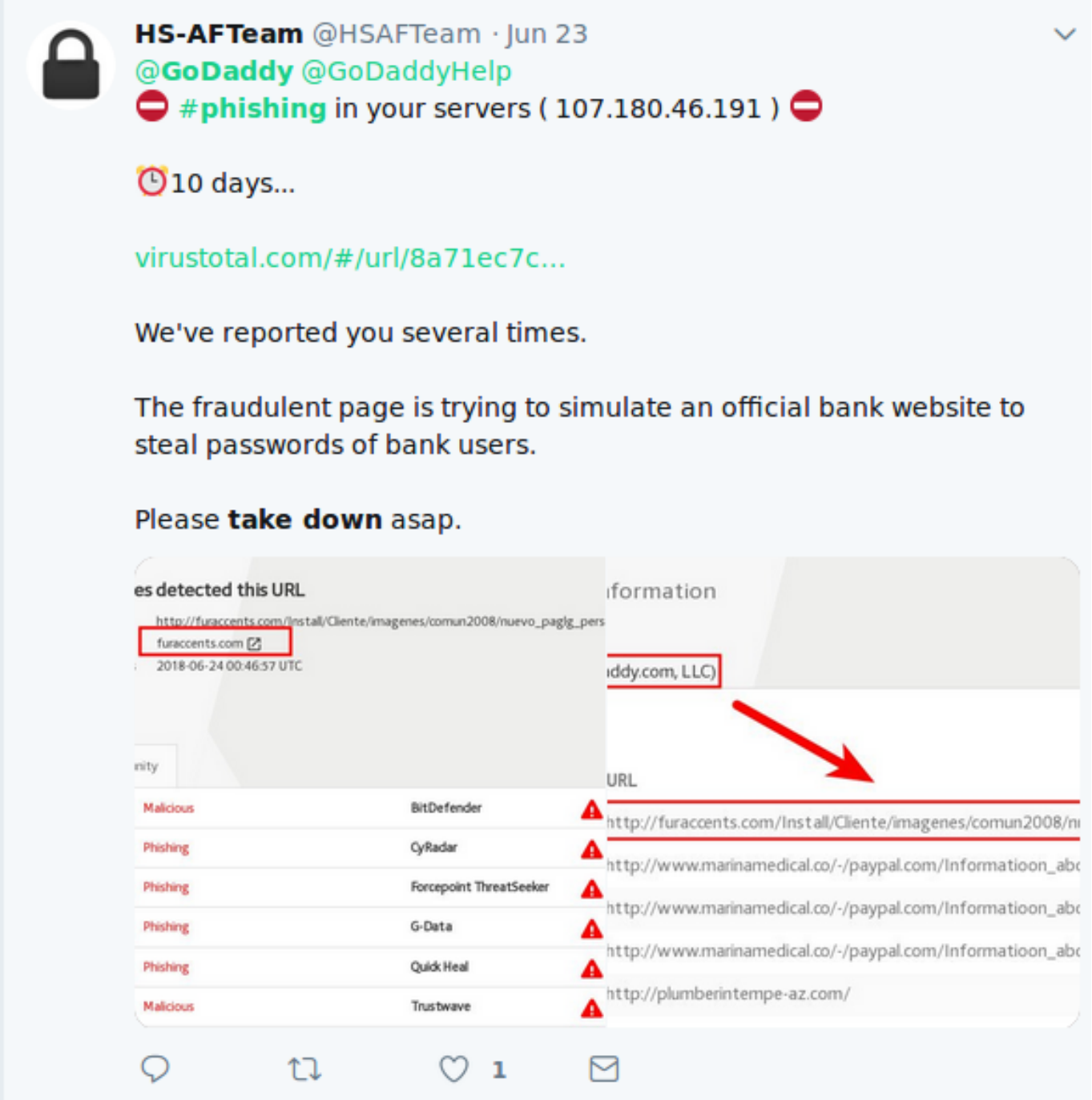
Fonte: O Autor

Figura B.6: Exemplo de relato sobre a Godaddy do usuário @dvk01uk



Fonte: O Autor

Figura B.7: Exemplo de relato sobre a Godaddy do usuário @HSAFTeam

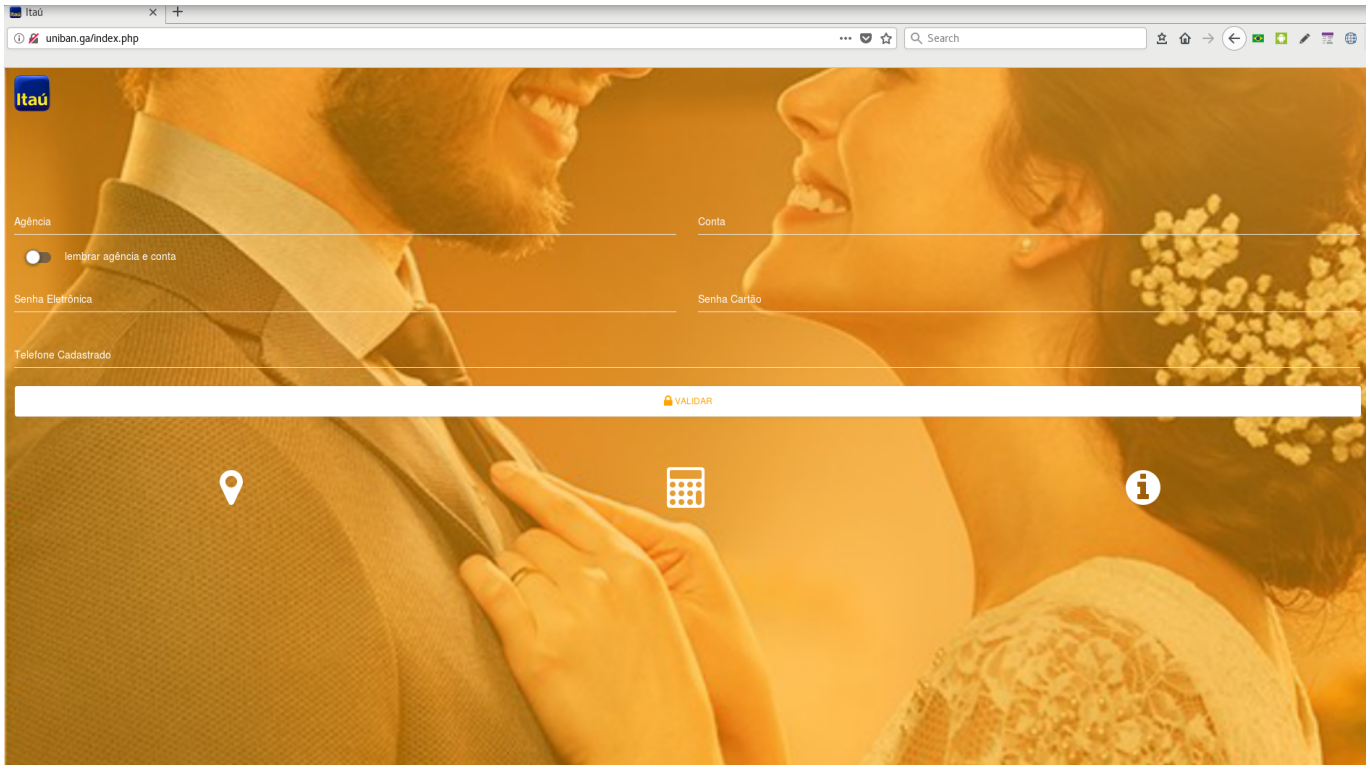


Fonte: O Autor

APÊNDICE C

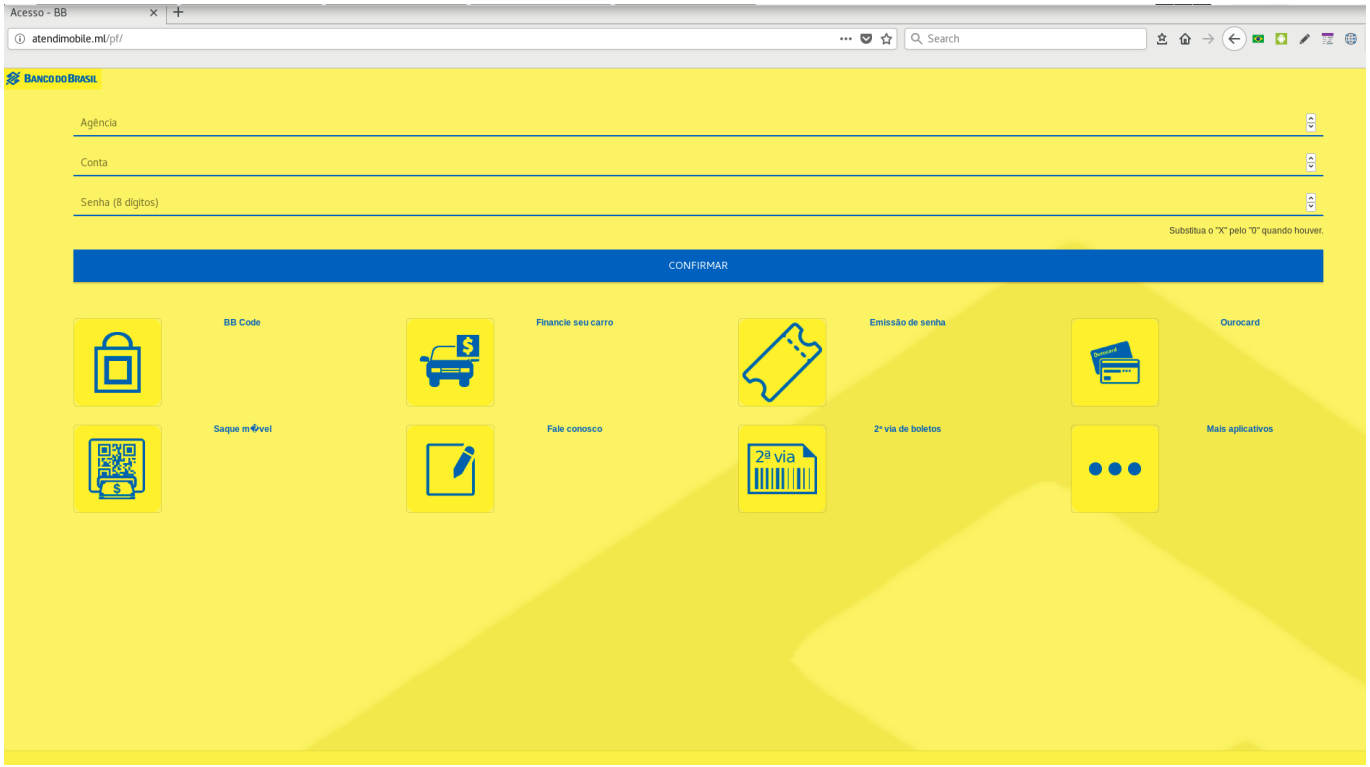
Exemplos de Tela de Smishing

Figura C.1: Exemplo de Smishing focando o Itau



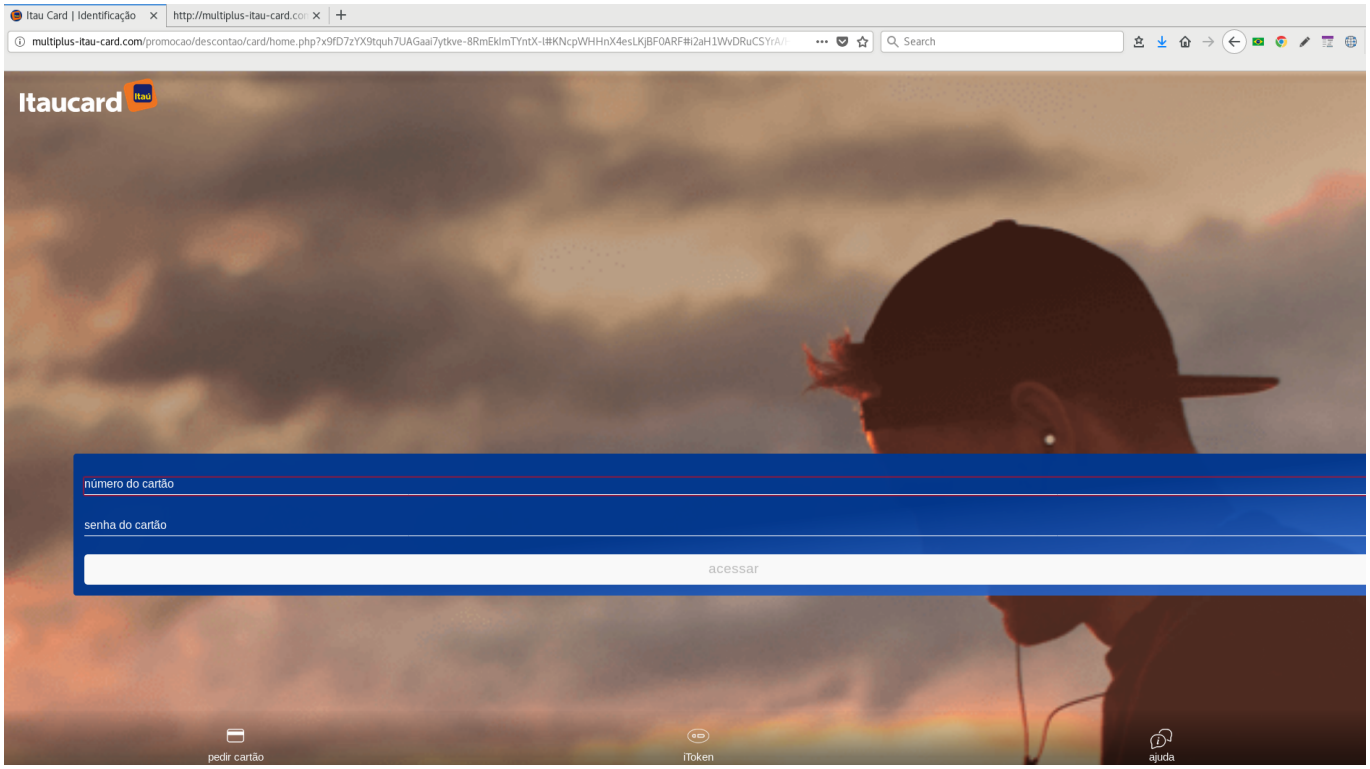
Fonte: O Autor

Figura C.2: Exemplo de Smishing focando o Banco do Brasil



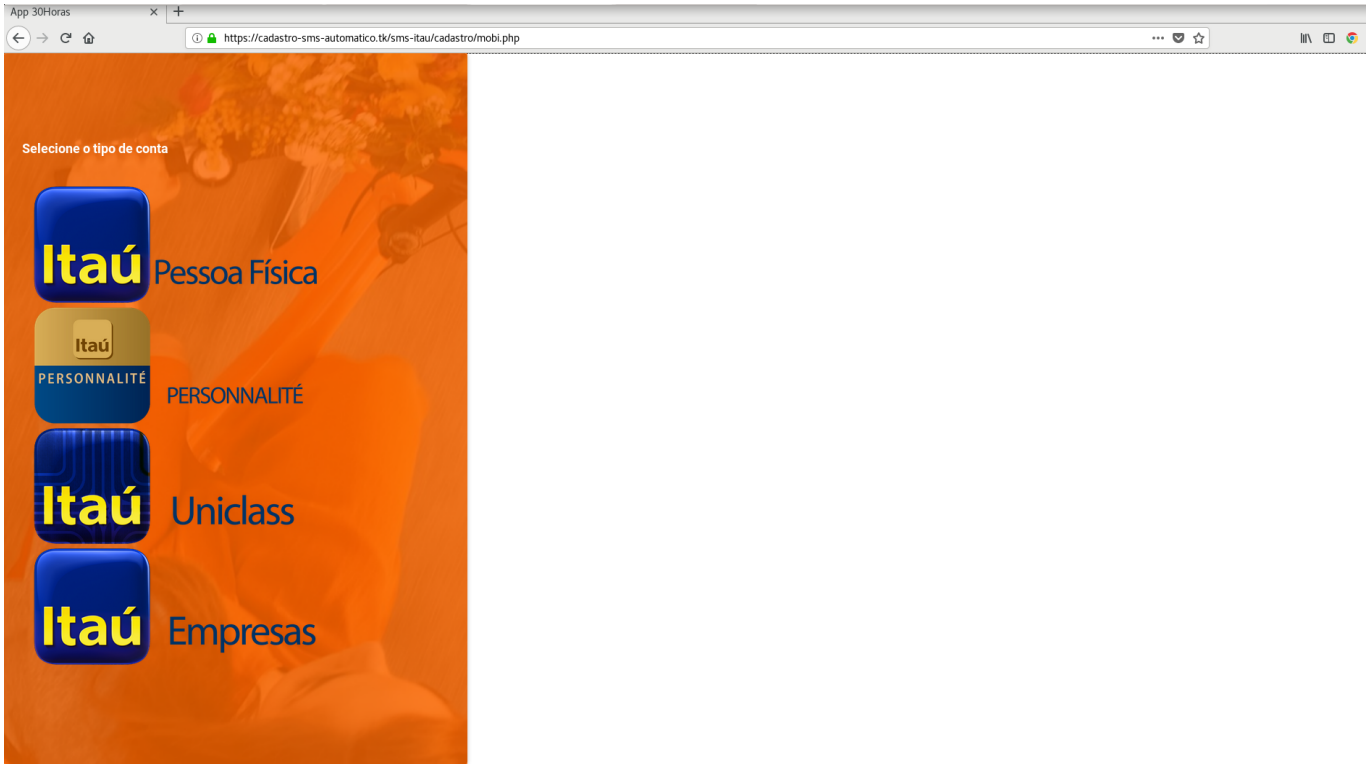
Fonte: O Autor

Figura C.3: Exemplo de Smishing focando o Itau



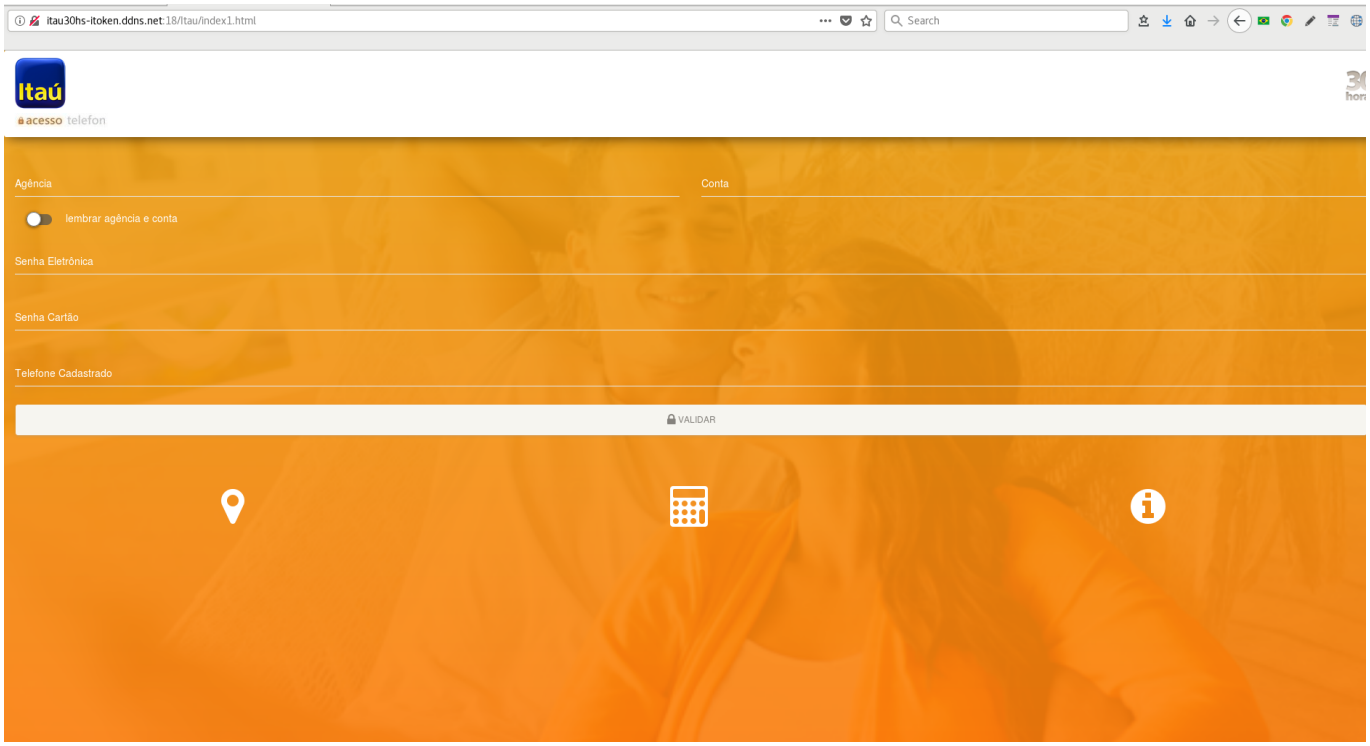
Fonte: O Autor

Figura C.4: Exemplo de Smishing focando o Itau



Fonte: O Autor

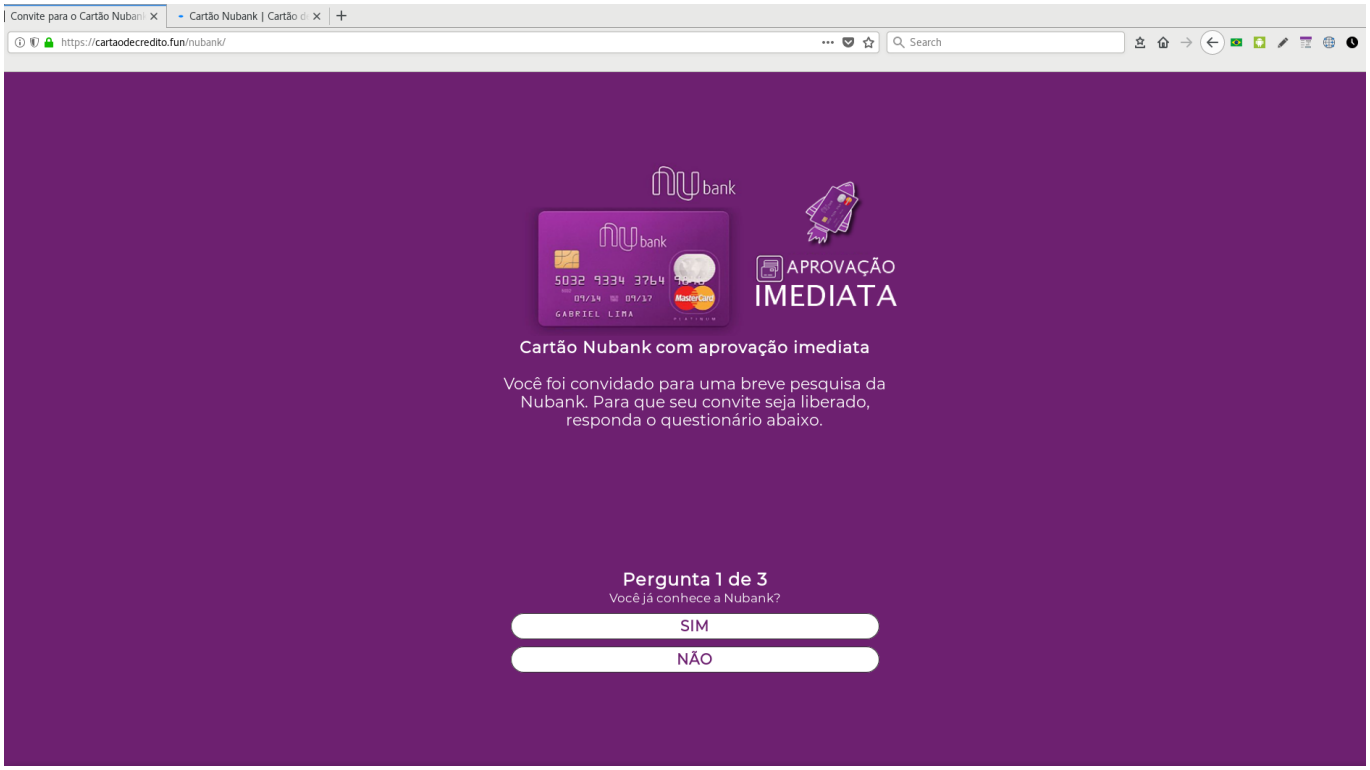
Figura C.5: Exemplo de Smishing focando o Itau



Fonte: O Autor

Figura C.6: Exemplo de Smishing focando o Itau

Figura C.7: Exemplo de Smishing focando o Nubank



Fonte: O Autor

Referências Bibliográficas

ALENCAR, G. D.; LIMA, M. F. de; FIRMO, A. C. A. A perspectiva de análise comportamental como forma de combate à engenharia social e phishing. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 3, 12 2013. IBEPES (Instituto Brasileiro de Estudos e Pesquisas Sociais). http://dx.doi.org/10.5329/resi.2013.1203008. page.33

ASSOLINI, F. *Ataques de SMiShing afetam usuários de mobile banking no Brasil*. [S.l.], 2016. Disponível em: <https://securelist.lat/ataques-de-smishing-afetam-usuarios-de-mobile-banking-no-brasil/83594/>. Acesso em: 05.09.2018. page.11

ASSOLINI, F. [S.l.], 2018. Disponível em: <https://twitter.com/assolini/status/1009441547702677504>. Acesso em: 05.09.2018. page.77

BASILI, V. R.; CALDIERA, G.; ROMBACH, H. D. The goal question metric approach. In: . [S.l.: s.n.], 1999. page.1515, page.1616

BERG, A. Cracking a social engineer. In: . [S.l.: s.n.], 1995. page.33

BERNZ. *THE COMPLETE SOCIAL ENGINEERING FAQ!* [S.l.], 1996. Disponível em: <http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se11.html>. Acesso em: 02.11.2018. page.33

CARVALHO, C. A. C. de. *COMPETÊNCIA DA JUSTIÇA FEDERAL NOS CRIMES CIBERNÉTICOS:*. [S.l.], 2013. Disponível em: <https://www.jfpe.jus.br/noticias/anexos/competencia_da_justica_federal_nos_crimes_ciberneticos.pdf>. Acesso em: 02.11.2018. page.44

FREENOM. [S.l.], 2018. Disponível em: <https://www.freenom.com/pt/aboutfreenom.html>. Acesso em: 09.11.2018. page.2020

GRANGER, S. *Social Engineering Fundamentals, Part I: Hacker Tactics*. [S.l.], 2001. Disponível em: <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em: 20.10.2018. page.33

HERMAN, S. N. Os desafios do crime cibernÉtico1. *REVISTA ELETRÔNICA DE DIREITO PENAL E POLÍTICA CRIMINAL - UFRGS*, v. 1, n. 1, 2013. page.44

HONG, J. The state of phishing attacks. *Communications of the ACM*, v. 55, n. 1, p. 74–81, 1 2012. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/2063176.2063197. page.44

KUMARAGURU, P. et al. School of phish: a real-word evaluation of anti-phishing training. In: *SOUPS*. [S.l.: s.n.], 2009. page.44

MITNICK, K. D. *The art of deception*. [S.l.]: Indianapolis, IN, 2002. ISBN 978-0-471-23712-9. page.33

ORGILL, G. L. et al. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: *Proceedings of the 5th Conference on Information Technology Education*. New York, NY, USA: ACM, 2004. (CITC5 '04), p. 177–181. ISBN 1-58113-936-5. Disponível em: <http://doi.acm.org/10.1145/1029533.1029577>. page.33

PETSAS, T. et al. Two-factor authentication: Is the world ready?: Quantifying 2fa adoption. In: *Proceedings of the Eighth European Workshop on System Security*. New York, NY, USA: ACM, 2015. (EuroSec '15), p. 4:1–4:7. ISBN 978-1-4503-3479-2. Disponível em: <http://doi.acm.org/10.1145/2751323.2751327>. page.55

PHISHTANK. [S.l.], 2018. Disponível em: <https://www.phishtank.com/faq.php\#whatisphishtank>. Acesso em: 03.09.2018. page.22

ROSA, A. *O que é um Virtual Host, Server Block ou Virtual Server?* [S.l.], 2016. Disponível em: <https://adrianorosa.com/blog/webserver/o-que-e-um-virtual-host-server-block-ou-virtual-server.html>. Acesso em: 07.11.2018. page.66

SCHNEIER, B. *Semantic Attacks: The Third Wave of Network Attacks*. [S.l.], 2000. Disponível em: <http://www.schneier.com/crypto-gram-0010.html\#1>. Acesso em: 03.09.2018. page.33, page.44

SHODAN. [S.l.], 2018. Disponível em: <https://www.shodan.io/>. Acesso em: 03.09.2018. page.1111

SIGNIFICADO. [S.l.], 2013. Disponível em: <https://www.significados.com.br/script/>. Acesso em: 09.09.2018. page.1111

SONI, P.; FIRAKE, S.; MESHRAM, B. B. A phishing analysis of web based systems. *Proceedings of the 2011 International Conference on Communication, Computing Security - ICCCS '11*, 2011. ACM Press. http://dx.doi.org/10.1145/1947940.1948049. page.33

ZHANG, Y. et al. Phinding phish : Evaluating anti-phishing tools. In: . [S.l.: s.n.], 2006. page.44