Universidade Federal do Paraná

Aryane Ast dos Santos

Um estudo preliminar de e-mail não-solicitado recebido pelo DINF/UFPR

Curitiba - PR

2017

Universidade Federal do Paraná

Aryane Ast dos Santos

Um estudo preliminar de e-mail não-solicitado recebido pelo DINF/UFPR

Monografia apresentada junto ao curso de Ciência da Computação, do Departamento de Informática, do Setor de Ciências Exatas, como requisito parcial para a obtenção do título de Bacharel.

Orientador: Prof. Dr. André Ricardo Abed Grégio

Curitiba - PR

2017

Agradecimentos

Aos meus pais pela formação, ao professor Grégio pela paciência e ao Dmitri pelo apoio.

Resumo

Spam é o email não-solicitado que chega na caixa de entrada do usuário por motivos tão diversos como mala direta, venda de produtos ilícitos/controlados/falsificados, golpes ou propostas, e como meio de disseminação de programas maliciosos (*malware*). O *spammer*, para propagar seu *malware* e obter informações sensíveis das vítimas (e.g., credenciais), envia mensagens com assuntos que despertam a curiosidade dos usuários, levando-os a executar anexos ou acessar links para conteúdos maliciosos. Tais conteúdos, uma vez atuantes no sistema, podem ser tanto sites clonados que apresentam formulários para que a vítima forneça suas informações, programas com interfaces gráficas que solicitam informações de bancos online, ou mesmo cavalos-de-Tróia que executam de forma oculta a fim de coletar dados que o usuário digita. Para auxiliar na mitigação do *spam*, é necessário conhecer o tipo de mensagem recebida por cada domínio ou rede. Neste trabalho, faz-se uma análise preliminar do *spam* recebido pelo Departamento de Informática da UFPR, de modo a se descobrir algumas tendências ou peculiaridades dessas mensagens. Foram coletadas 7870 mensagens rotuladas como *spam*, as quais tiveram suas características, i.e., campos da mensagem (cabeçalho e corpo do email), extraídas e armazenadas em um banco de dados.

Palavras-chave: Segurança computacional; spam; detecção de email; malware

Abstract

Spam is the unsolicited email message that arrives at user's inbox motivated by direct sales, illicit/restrict/fake products offers, scams or proposals, as well as a way to spread malware. To propagate malware and obtain sensitive information from their victims (e.g., credentials), spammers send messages with subjects intended to lure users into executing an attachment, or to access a link leading to malicious content. These contents, once installed into the victim's system, may be either cloned sites with forms to collect victims informations, or graphical intergace based programs that request online banking data, or even Trojan horses that run in a hidden way to collect users' pressed keys. To aid in spam mitigation, we need to know the type of messages received by each domain/network. In this work, we perform a preliminary analysis of spam received by UFPR's Department of Informatics to discover its trends or peculiarities. We collected 7870 messages labeled as spam, whose features, i.e., email fields such as head and body, were extracted and stored in a database. With this database, we discovered useful information, such as what countries are related to the domains that sent more spam to DInf (based on a dataset collected between April/2016 and Jun/2017), presence of attachments and their detection as malware or not, presence of links, its domains and associated redirection that may lead a user to the attacker's actually intended site etc.

Keywords: Computer security, spam, email detection, malware

Sumário

Capítulo 1

Introdução

Spam é o envio massivo de emails não autorizados. Enquanto campanhas legítimas de propaganda são toleradas pelos consumidores por serem encaradas como um preço a ser pago pelo acesso ao conteúdo, emails de *spam* são impostos ao consumidor—vítima, nesse caso—sem oferecer nenhum benefício e sem permitir que a vítima possa cancelar o recebimento de tais mensagens não solicitadas [22]. Mensagens de *spam* acarretam em tempo perdido, pois a vítima precisa percorrer sua caixa de entrada repleta de emails irrelevantes e por vezes não encontrar os que são legítimos e importantes.

Além de promover golpes e propagandas de mercadorias ilícitas, controladas ou falsificadas, emails de *spam* continuam sendo um dos maiores vetores para disseminação de *malware* e outras formas de crime virtual [17]. Programas maliciosos podem ser distribuídos de duas maneiras principais: através de *spammers* que configuram anúncios maliciosos cujo intuito é levar a vítima a acessar um link no *spam* para tentar explorar as vulnerabilidades dos navegadores ou convencendo as vítimas a instalar o *malware* por conta própria via execução de anexos, tornando o *spam* atrativo ao usuário [24] [17].

Spam acarreta em muitos problemas para empresas, provedores e usuários. De acordo com a Cartilha de Segurança para Internet do CERT [4], os usuários sofrem com a perda de mensagens importantes, dado que eles podem ler as mensagens legítimas com atraso ou apagá-las por engano; com a visualização de conteúdo impróprio ou ofensivo; gasto desnecessário de tempo; não recebimento de emails nos casos em que é utilizado algum serviço que limite o tamanho da caixa postal: os *spam* lotam a caixa de entrada, impossibilitando o recebimento de novas mensagens até que algumas mensagens sejam apagados; e classificação errada de mensagens, pois num

sistema de filtragem de *spam* com regras ineficientes, há o risco de mensagens legítimas serem classificadas como *spam* e serem automaticamente apagadas, movidas para quarentena ou redirecionadas para outra pasta de email.

Já as empresas e provedores costumam enfrentar outros tipos problemas, tais como impacto na banda, pois o volume de tráfego gerado pelos *spams* faz com que seja necessário aumentar a capacidade dos *links* de conexão com a Internet; má utilização dos servidores de email, porque boa parte dos recursos dos servidores de email, como tempo de processamento e espaço em disco são consumidos no tratamento de mensagens não solicitadas; investimento extra em recursos, tais como sistemas de filtragem e contratação de mais técnicos especializados e nos casos onde um provedor tem usuários envolvidos em envio de *spam* ele pode ter a rede incluída em listas de bloqueio, o que prejudica o envio de emails pelos demais usuários resultando em perda de clientes.

Do total de *spams* reportados ao CERT.br entre os anos de 2003 à 2015 [5], houve um aumento de 43% no envio de *spam* de 2008 até 2010, conforme pode ser visto na Figura 1.1. 2010 foi o ano no qual se atingiu o maior nível de envio de spam, um total de 4.745.295 ocorrências reportadas ao Spamcop e outras fontes não citadas. Parte disso pode ser atribuída pela democratização da Internet, que é bem exemplificado pela popularização das redes sociais: apenas em 5 meses de 2009 houve um aumento de 96% nos usuários do Facebook, segundo uma consultoria do Ibope para o blog *IDG Now!* [6].

O Brasil esteve desde 2012 em quinto lugar no ranking da Spamhaus [1] como um dos países que mais produzem *spam*. É provável que esteja nesta lista desde antes de 2012, porém as informações salvas no Wayback Machine do Internet Archive datam a partir de 2012 apenas. O Wayback Machine é um banco de dados digital criado pela ONG Internet Archive e que arquiva mais de 298 bilhões de páginas da Web desde 1996, permitindo ao usuário visualizar versões de páginas tal como eram no passado [16]. A verificação dos registros salvos no Wayback Machine mostra que, desde 2012, o Brasil oscilou neste ranking da quinta posição até a décima colocação, em 2 de junho de 2017.

Desde o dia primeiro de janeiro de 2013, as operadoras brasileiras estão cumprindo uma regra do Comitê Gestor da Internet (CGI.br) que consiste em bloquear a porta 25 das conexões domésticas [10]. Essa medida teve como objetivo diminuir a quantidade de *spam* enviada por computadores domésticos, o que parece ter sido

[1] Organização internacional que rastreia *spam*

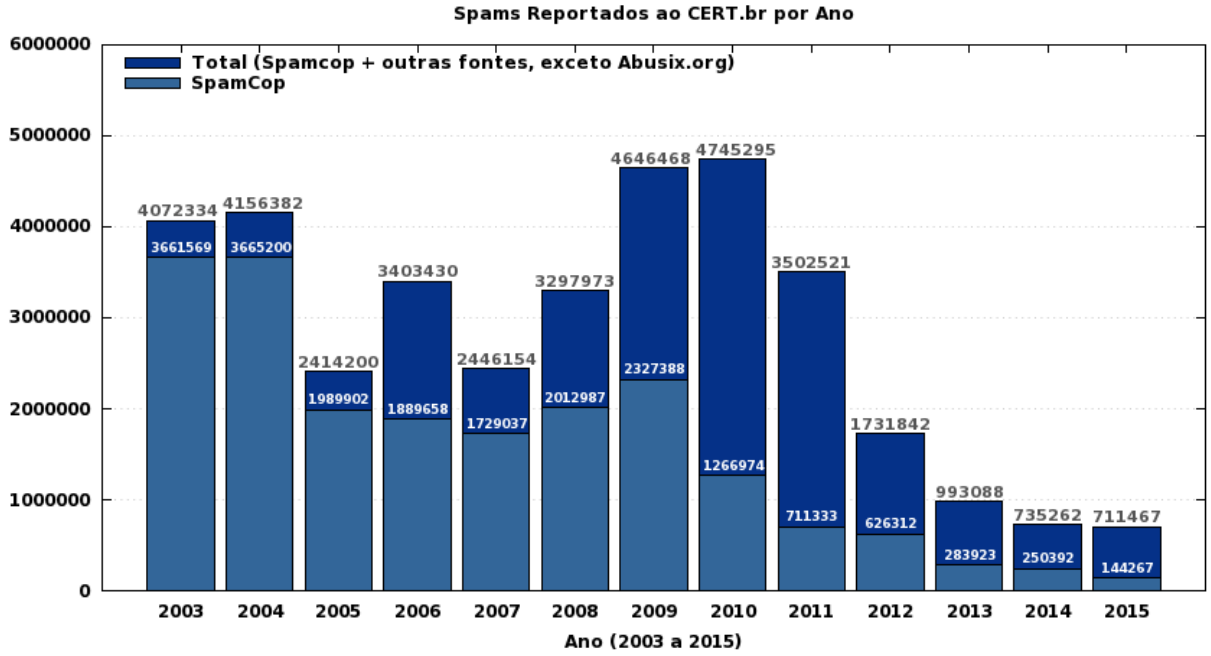

Figura 1.1: Número de spams reportados ao CERT entre 2003 e 2015.

frutífero, uma vez que o Brasil caiu em duas posições no final de 2013 na lista da Spamhaus. Coincidentemente, a quantidade de spams, mundialmente falando, também despencou, porém dessa vez vertiginosamente, como pode ser visto na Figura 1.1, uma vez que apesar da medida ter entrado em vigor em 2013, ela já vinha sendo gradualmente adotada. Como alternativa, o CGI.br recomenda que os usuários enviem emails através da porta 587, que exige autenticação.

O combate ao *spam* pode ser feito de várias formas, algumas delas discutidas no Capítulo 2. Entretanto, para se ter sucesso, é necessário conhecer o tipo de mensagem recebida por cada rede/instituição. Neste trabalho, *spams* recebidos recentemente (2016-2017) pelo servidor de email do DInf/UFPR nas contas de um professor e dois alunos foram coletados e destrinchados, para que se pudesse observar seu formato, características inerentes e presença ou não de anexos e links que levam à instalação de programas maliciosos. O objetivo dessa análise é observar as tendências do *spam* do DInf, de modo a auxiliar na criação de regras eficientes para bloqueio, bem como para se identificar o tipo de mensagem não-solicitada da qual esta rede específica é alvo.

Este trabalho está dividido da seguinte forma: no Capítulo 2, é mostrada uma breve conceituação teórica dos assuntos abordados nesse trabalho; no Capítulo 3, apresenta-se a metodologia de coleta de informações aplicadas ao conjunto de *spams* disponível, bem como os resultados da análise feita para se identificar algumas ten-

dências observadas nesses *spams*; no Capítulo 4, discute-se as considerações finais deste trabalho e aponta-se algumas direções para trabalhos futuros.

Capítulo 2

Conceituação teórica

Neste capítulo, serão abordados conceitos básicos sobre *spam*, como é realizada a varredura de arquivos através da ferramenta VirusTotal de forma a se identificar *malware* e algumas técnicas utilizadas atualmente para auxiliar na defesa contra *spam*, nas Seções 2.1, 2.2 e 2.3, respectivamente.

2.1 Spam

Um *spam* pode ser entendido como uma mensagem não-solicitada enviada para uma pessoa, grupo ou servidor de email. Indivíduos com intenções suspeitas que disparam o envio de tais mensagens são chamadas de *spammers*. Essas mensagens são enviadas por anunciantes que podem oferecer esquemas de enriquecimento, produtos duvidosos ou que não interessam ao destinatário, promoção atividades ilegais, entre outros. A intenção costuma ser fazer o usuário gastar dinheiro, promover contrabando ou obter informações sensíveis.

A rápida disseminação da Internet e a ampla disponibilidade de serviços gratuitos de email ofereceram uma forma fácil e barata de enviar e receber mensagens. Um dos lados negativos disso é o *spam*, porque com ele é possível obter um meio eficiente e economicamente viável de alcançar um grande público, substituindo-se de modo eficiente (em amplitude) a mala direta. O *spammer* praticamente não tem custos para enviar emails e obter visualizações [21].

Os *spammers* podem obter listas de endereços de email de algumas formas. Muitos se inscrevem em grupos de notícias para obter a lista dos participantes, os endereços também podem ser obtidos a partir de mecanismos de busca que vasculham

toda a Internet procurando pelo caracter "@", o que indica um endereço de email. Os programas que fazem isso são chamados de *spambots* [18]. Outra fonte são os sites criados especificamente para “atrair” endereços de email. Por exemplo, um *spammer* cria um site que diz "Ganhe um milhão de reais!!! Apenas insira seu endereço de email aqui". Há também sites que explicitamente perguntam aos seus usuários, normalmente no momento do cadastro, se eles gostariam de receber *newsletters* dos parceiros. Se o usuário clicar que sim, seu email é vendido para um *spammer*. Esse é o chamado *opt-in email marketing*.

O *spammer* precisa de um meio para disseminar suas mensagens e conseguir atuar. Ele pode fazer isso de dois modos: a partir de um servidor de email legítimo, de onde o remetente é autenticado, ou então ele pode utilizar um *open mail relay*. Para obter sucesso no primeiro modo, o *spammer* necessita obter uma conta válida no servidor que originará as mensagens. Quanto ao segundo modo, um *open mail relay* é um servidor SMTP configurado para que através dele possam ser trocadas mensagens de email provenientes de e para qualquer usuário da Internet, não apenas entre os usuários da rede local [9], tornando mais fácil o envio.

Quando a quantidade de *spam* na rede começou a se elevar, em meados dos anos 90, os *spammers* viram nesse tipo de servidor uma ferramenta para expandir a disseminação de seus conteúdos maliciosos [7]. O funcionamento é simples para o *spammer*, dado que ele simplesmente envia uma mensagem com o conteúdo malicioso e uma grande lista de destinatários para o servidor em questão, o qual é então é responsável pela retransmissão da mensagem para todos os endereços incluidos na mensagem inicial.

Dessa forma, os *spammers* conseguem repassar uma enorme quantidade de *spam* de maneira simples, pois todo o esforço computacional e banda necessários para o envio em massa são provenientes do servidor de email atingido. Aliado à isso, eles conseguem também mascarar sua identidade, uma vez que as mensagens enviadas parecem ser provenientes de uma fonte segura e/ou legítima. Entretanto, cabe ressaltar que isto somente é possível se esse tipo de servidor não fizer a autenticação do emissor do email [8].

A alternativa inicial para barrar esta prática foi a adoção de *blacklists*. Uma vez que o servidor malicioso é identificado, ele é adicionado à lista negra e os servidores de email que querem se proteger dos *spams*, de posse dessa *blacklist*, bloqueiam qualquer mensagem proveniente dos servidores afetados. Servidores com *open relay* ainda são encontrados através de ferramentas automatizadas que estão disponíveis

na rede. Também é possível testar se um servidor de email de email específico está com *open relay* [9], por exemplo, acessando-se http://www.mailradar.com/openrelay/ e inserindo o número IP do *host* no campo apropriado e clicando em "*Test*".

2.2 Varredura de arquivos

O VirusTotal é um serviço online disponível para acesso que analisa arquivos executáveis, o que permite identificar vírus, *worms*, *Trojans* e outros tipos de códigos maliciosos através de mecanismos de antivírus. Atualmente são utilizados 63 antivírus [1] de empresas diferentes. Tal identificação é muitas vezes feita por meio da busca por “assinaturas” maliciosas dentro dos executáveis suspeitos.

Uma assinatura de vírus é uma sequência contínua de bytes presentes no arquivo que representa o “comportamento” infeccioso do *malware*. Se essa assinatura estiver presente em uma das bases de dados consultada pelo VirusTotal, tem-se um resultado positivo para um provável *malware*. As assinatures de *malware* das soluções de antivírus presentes no VirusTotal são atualizadas periodicamente conforme são desenvolvidas e distribuídas pelas companhias de antivírus [3] participantes.

O VirusTotal é oferecido de forma livre/gratuita aos usuários finais, desde que não seja utilizado para fins comerciais, porém de forma limitada (quantidade de consultas). Também é oferecida aos usuários uma API pública que permite a automatização da varredura de arquivos, a qual foi utilizada neste trabalho. O funcionamento da API é explicado a seguir.

A primeira requisição feita à API pelo usuário submete o arquivo a ser inspecionado. A resposta contém informações se o item pesquisado não está presente na base de dados do VirusTotal, se ainda está na fila para análise ou se já é possível recuperar o relatório com a análise. Um exemplo de relatório em JSON contendo os resultados do scan é apresentado no Listing 2.1 e contém, dentre outras informações, o número de antivirus/datasets que informam que o arquivo é malicioso *positives*, o total de bases consultadas (*total*), e os detalhes de cada antivírus consultado (*scans*), se é positivo ou não e o resultado. É importante notar que muito frequentemente as soluções de antivírus vão gerar falsos-positivos, ou seja, detectar como maliciosos arquivos inofensivos.

```
{
    "md5": "fca512814e5891d6ac63adfdd5235587",
    "permalink": "https://www.virustotal.com/file/f716...c1e/analysis/1492702353/",
    "positives": 32,
    "resource": "f71691cd16de0e3d3fa8fc278b7341e14bbbbf44169e98367543edda0ab88c1e",
    "response_code": 1,
    "scan_date": "2017-04-20 15:32:33",
    "scan_id": "f71691cd16de0e3d3fa8fc278b7341e14bbbbf44169e98...88c1e-1492702353",
    "scans": {
        "ALYac": {
            "detected": true,
            "result": "Trojan.JS.Agent.PCW",
            "update": "20170420",
            "version": "1.0.1.9"
        },
        "AVG": {
            "detected": true,
            "result": "JS/Downloader.Agent.68_M",
            "update": "20170420",
            "version": "16.0.0.4769"
        },
        ...
        "nProtect": {
            "detected": false,
            "result": null,
            "update": "20170420",
            "version": "2017-04-20.02"
        }
    },
    "sha1": "bc6ce30bfb47767d17da2a61a02385d36b2cb620",
    "sha256": "f71691cd16de0e3d3fa8fc278b7341e14bbbbf44169e98367543edda0ab88c1e",
    "total": 59,
    "verbose_msg": "Scan finished, information embedded"
}
```


Listing 2.1: Exemplo de resposta recebido com o uso da API do VirusTotal

2.3 Ferramentas de defesa

Para evitar *spam*, são utilizados comumente alguns métodos baseados em filtragem de emails, em geral instalados e configurados pelos admnistradores de redes/sis-

temas na própria instituição onde o servidor de email se encontra. Há filtros baseados em listas e em conteúdo [15]. Nos filtros baseados em listas, os remetentes são divididos em confiáveis e não-confiáveis (*spammers*). Dessa forma, o filtro permite que as mensagens sejam entregues ou bloqueadas, de acordo com o grupo ao qual o remetente pertence. Já os filtros baseados em conteúdo buscam termos ou frases específicas na composição dos textos do email para determinar se a mensagem é *spam* ou legítima, esta última também chamada de *ham*. A seguir, ambos os tipos de filtros citados são descritos com mais detalhes.

2.3.1 Filtros baseados em listas

Uma *blacklist* é uma lista com entradas de endereços de email ou IP que foram utilizados anteriormente para enviar *spam*. Assim que uma mensagem chega, o filtro verifica se o IP ou endereço de email está na *blacklist*, que é gerada e mantida localmente. Se o endereço estiver, a mensagem é considerada *spam* e rejeitada. Um lado negativo é que elas podem identificar erroneamente remetentes legítimos como *spammers*. Esses são os chamados falsos positivos e podem acontecer se um *spammer* estiver enviando lixo a partir de um endereço de IP que também é utilizado por usuários legítimos.

Também pode ser utilizada uma *whitelist*, que é oposta ao método de *blacklist*. Nesse tipo de serviço, é mantida uma lista de usuários confiáveis dos quais mensagens podem ser recebidas. Geralmente a *whitelist* é utilizada em conjunto com algum outro método. Algumas aplicações *antispam* utilizam uma variação desse sistema chamada de *whitelist* automática, que consiste de verificar o endereço de email de um remetente desconhecido e, se ele não tem histórico de enviar *spam*, a mensagem é enviada normalmente e adicionada à *whitelist*, liberando o rementente em questão.

Já uma *real-time blackhole list* é muito parecida com uma *blacklist*, porém a lista é gerada e alimentada por outra empresa, sendo assim um serviço terceirizado, requerendo menos manutenção por parte da organização contratante. Desse modo, quando uma nova mensagem chega, o serviço de filtragem local se conecta ao sistema contratado que contém as listas e faz a verificação do endereço de emails e IP de origem, permitindo ou não a entrega da mensagem. Assim como *blacklists*, *real-time-blackhole lists* também podem gerar falsos-positivos se os *spammers* utilizarem um endereço IP legítimo para enviar lixo eletrônico.

As *greylists* se baseiam no fato de que muitos *spammers* tentam enviar *spam* mas-

sivamente uma vez apenas. O servidor de destino inicialmente rejeita as mensagens de usários desconhecidos e envia uma mensagem de erro pro servidor que enviou o email. Se houver outra tentativa de enviar mensagens, coisa que a maioria usuários dos servidores legítimos vão tentar, a *greylist* assume que a mensagem não é *spam* e deixa ela seguir para a caixa de entrada do destinatário. Quando isso ocorre, o IP ou email do remetente é adicionado à uma lista de remetentes confiáveis (*whitelist*), liberando-o temporariamente para novos envios (funciona como uma cache de usuários legítimos: enquanto o remetente liberado enviar mensagens, ele permanecerá na lista; se este ficar muito tempo sem enviar uma mensagem, sua “entrada” na lista expira e o processo se reinicia na próxima vez em que este enviar nova mensagem).

2.3.2 Filtros baseados em conteúdo

Dentre os filtros de conteúdo, destacam-se os baseados em palavras, os heurísticos e os Bayesianos. Os filtros baseados em palavras são os mais simples desse tipo de filtragem. Eles bloqueiam todos os emails que contenham certos termos, podendo ser uma forma simples, porém eficiente de combater lixo eletrônico. Porém se forem mal configurados, bloqueando palavras muito comuns, podem gerar inúmeros falsos-positivos. Para tentar se esquivar desse tipo de filtro, muitos *spams* apresentam grafia errada de palavras, por exemplo "vi@gra"ao invés de "viagra"e outras trocas simples que fazem com que a expressão regular não realize adequadamente o casamento do padrão esperado.

Um filtro heurístico é uma evolução do de palavras. Ao invés de apenas verificar palavras específicas, o filtro heurístico utiliza-se de um conjunto de regras para analisar vários termos da mensagem em questão. O filtro atribui pontos a palavras ou termos da mensagem de acordo com fatores pré-definidos. Se a quantidade de pontos ultrapassa um limite definido pelo administrador, a mensagem é caracterizada como *spam* e bloqueada. Tem funcionamento rápido, porém também podem gerar falsos-positivos dependendo das combinações de palavras do email que aumentem a pontuação da mensagem como um todo.

Já os filtros Bayesianos, como o nome sugere, utilizam-se de meios estatísticos para classificar as mensagens. O filtro inicialmente precisa ser treinado para que aprenda a discernir *spam* de *ham*, e isso é feito de forma manual com o usuário adicionando mensagens recebidas em listas de *spam* ou de mensagens confiáveis. O filtro então vai povoando duas listas: termos presentes em mensagens reais e os

presentes em mensagens de spam. A partir disso, quanto maior for a base utilizada para classificar, maior é a chance de se classificar corretamente.

Além dos filtros mencionados de listas e conteúdo, há outros métodos, como sistemas de resposta, filtros colaborativos, sistemas de busca de domínio, filtros baseados em países e filtros de URL [2].

2.3.3 Outros métodos

Em um sistema de resposta ou desafios, antes de uma mensagem ser efetivamente enviada, o remetente recebe testes que devem ser resolvidos para só então o email ser enviado. Se o desafio for realizado com sucesso, o que pode ser um CAPTCHA, por exemplo, o endereço do remetente entra numa lista de remetentes confiáveis, de forma que os futuros emails dele sejam aceitos. Como *spammers* utilizam-se de métodos automatizados para o envio de uma grande carga de *spams*, raramente o email de confirmação é visualizado, quem dirá resolvido. Consequentemente, a mensagem de *spam* é rejeitada pouco tempo após o envio.

Nos filtros colaborativos, milhões de usuários sinalizam mensagens entre *spam* e *ham*. Se muitos usuários classificarem uma mensagem como sendo maliciosa, o sistema passa a rejeitar automaticamente essa mensagem para os demais membros.

Com os sistemas de busca de domínio (*DNS lookup systems*), são feitas verificações se o nome do domínio presente no email do remetente realmente existe. O sistema também realiza uma pesquisa reversa de DNS através do endereço de IP de onde a mensagem foi enviada. Esta pesquisa revela o nome do domínio associado ao servidor em questão.

Alguns servidores de email rejeitam mensagems provenientes de países de onde um grande número de mensagem de *spam* são enviadas. Isso é feito analizando-se o endereço de IP do remetente da mensagem duvidosa. Também são filtradas mensagens a partir da busca de URLS nas mesmas: se alguma URL encontrada estiver presente em alguma *blacklist* conhecida, a mensagem é recusada.

É importante ressaltar que nenhuma técnica é uma solução completa para o problema de *spam* e cada uma tem suas vantagens e desvantagens, havendo um compromisso entre rejeitar minimamente emails legítimos (falsos-positivos) e não rejeitar todos os *spams* (falsos-negativos).

2.3.4 SpamAssassin

SpamAssassin é um programa antispam que pode ser configurado para uso tanto em servidores de email quanto para uso individual [14]. Ele utiliza várias técnicas de detecção de *spam* combinadas, como *blacklists*, bases de dados online, análise de DNS, filtros Bayesianos, aplicações de regras baseados em expressões regulares que casam com o corpo ou cabeçalho das mensagens de email (que é basicamente um filtro de palavras mais elaborado), entre outros, o que aumenta a chance de uma classificação mais correta.

A análise de cada nova mensagem consiste em realizar uma bateria de testes com o email recebido. Cada teste possui uma pontuação específica (*score*) e ao final de todos os testes, a pontuação da mensagem é utilizada para classificar o email como *spam* ou não. Um *score* alto significa que a mensagem tem alta probabilidade de ser considerada *spam*, assim como um *score* baixo diminui a probabilidade disso.

Terminados os testes, são adicionados novos cabeçalhos na mensagem para informar a pontuação final (nível de *spam*) e os testes no qual a mensagem foi reprovada (se é que ela foi reprovada). De acordo com os valores padrão, se a mensagem apresentar uma pontuação maior que 5 ela é direcionada à um arquivo chamado *bulk*, na pasta *mail*; e se a pontuação for maior que 14 a mensagem é direcionada ao arquivo *spam*, também na pasta *mail* [12]. Os *scores* podem ser positivos ou negativos, com valores positivos indicando *spam* e negativos *ham*. Quanto maior o valor, maior a probabilidade de ser considerado *spam*.

2.3.5 Sender Policy Framework

Muitos *spammers* se utilizam de uma brecha no protocolo SMTP que permite a qualquer computador enviar mensagens se passando por outro endereço. O *Sender Policy Framework* ou SPF é um sistema que evita que outros domínios enviem emails não-autorizados em nome de um outro domínio [13]. Ele é utilizado como tentativa de controle de emails forjados, isto é, emails que parecem ser originados de domínios existentes e confiáveis mas na verdade são *spams*.

O funcionamento ocorre da seguinte maneira: quando uma nova mensagem chega, o sistema verifica no cabeçalho da mensagem o endereço de IP do servidor SMTP de onde ela foi enviada. A partir disso, é realizada uma busca desse IP numa lista de IPs confiáveis, que é disponibilizada pelo domínio da mensagem em questão, ou seja,

os endereços nos quais o administrador do domínio autoriza o envio de mensagens. Essa lista é encontrada nos registro de DNS do domínio da mensagem recebida.

Capítulo 3

Metodologia e resultados

Na Seção 3.1, serão discutidas as etapas referentes à obtenção e processamento dos dados de *spam*; na Seção 3.2, são apresentados os resultados obtidos da análise sobre os dados obtidos anteriormente. Também são realizadas análises sobre os anexos e URLs contidos nos *spams* nas seções 3.3 e 3.3.1.

3.1 Base de dados utilizada

Para o desenvolvimento deste trabalho, foi utilizada uma base de dados rotulada manualmente como *spam*, contendo emails datando de abril de 2016 a junho de 2017. Essas mensagens consideradas como *spam* foram fornecidas por um professor do DInf, por um aluno formando do curso com privilégios adiministrativos na rede do departamento e pela autora deste trabalho. As mensagens de *spam* vieram de três origens: seleção manual de mensagens que eram claramente *spam*, mas que não foram barradas por nenhum filtro e acabaram na caixa de entrada dos usuários supracitados que forneceram o conjunto de dados; caixa "JUNK" do Thunderbird; regras de `procmailrc`. Utilizando o cliente de emails Thunderbird, foram exportados todos os arquivos no formato `eml`. O formato `eml` é uma extensão para email no padrão RFC 822 [23] que define uma mensagem eletrônica. Uma mensagem eletrônica consiste de duas partes: cabeçalho e corpo, separados por uma linha em branco. Os campos do cabeçalho permitem que o corpo da mensagem seja quebrado em partes, cada parte em uma linha. O propósito disso é descrever o conteúdo da mensagem sem alterar a própria mensagem. Uma mensagem de email, então, possui uma parte de cabeçalho seguido de uma ou mais partes de corpo de mensagem.

A partir desses arquivos `eml` considerados como *spam*, foi escrito um *parser* de email, para obter todas as informações de cabeçalho e conteúdo das mensagens e armazená-las em arquivos JSON, de forma a ficar mais fácil obter informações como a origem, se o email é multiparte, possui anexo, qual o tipo do anexo, dentre outras. Dados os arquivos JSON, foi escolhido armazená-los em um banco de dados não relacional, no caso o MongoDB, que é próprio para armazenar documentos.

Os arquivos estão divididos em *header* e *content*, assim como os próprios emails. Em *header* estão armazenados todos os campos de cabeçalho, já em *content* além do próprio conteúdo do corpo do email, foram adicionados alguns campos para controle. O campo *url* é um booleano que informa se existem URLs no corpo do email, quando existem, o campo *url-list* armazena uma lista contendo todas as URLs encontradas no corpo do email. O mesmo é feito quanto à anexos: *attachment* informa se o email em questão possui anexo, e se for o caso, *attachment-list* contém a lista de anexos. Também para auxiliar na busca, os campos *multipart* e *type* foram adicionados, para informar se o corpo do email é composto de múltiplas partes e o tipo MIME do conteúdo. O email em si está armazenado em *body*, que pode conter uma única parte ou uma lista, no caso de multipartes. Utilizando a inferência de esquema do próprio MongoDB, é possível visualizar o esquema acima descrito no Apêndice A. Vale notar que apesar do esquema mostrar campos do cabeçalho, nenhum email contém todos esses campos, apenas um subconjunto variável dos apresentados.

3.2 Tendências encontradas no spam do DInf

A partir da base de dados pré-processada, isto é, a dissecção dos emails em campos, foi possível extrair algumas características interessantes sobre as mensagens recebidas. A seguir, discute-se o que foi observado nos *spams* coletados.

A visualização geográfica dos países que enviam lixo eletrônico tem como objetivo facilitar a interpretação dos dados por um analista humano. A geração dos gráficos se baseou na utilização da biblioteca GeoLite2 do MaxMind com a biblioteca *python-geoip-geolite2*[1]. A partir dessa informação, utilizando os endereços IPs dos remetentes obtidos no campo de cabeçalho *Received*, foi possível gerar um mapa que mostra os locais de origem dos envios de *spam*.

Foi feito um *ranking* considerando os dez países que mais apareceram como envi-

[1] http://pythonhosted.org/python-geoip/

adores de *spam*, mostrado na Tabela 3.1. Do total de 7.870 *spams*, não foram encontrados países correspondentes para os IPs contidos em Received em 2.457 casos. No *ranking* da Tabela 3.1, foram desconsiderados esses casos cuja origem não pôde ser identificada, de forma que as porcentagens se referem ao total de 5.413 países que foram rastreados com sucesso segundo a API utilizada.

Posição no ranking	**País**	**Spams enviados**	**Porcentagem**
1	Brasil	2.784	51,4%
2	Estados Unidos	1.986	36,6%
3	Dinamarca	125	2,3%
4	Romênia	78	1,4%
5	China	76	1,4%
6	Noruega	52	0,9%
7	Bulgária	52	0,9%
8	Hong Kong	45	0,8%
9	Canadá	32	0,5%
10	Itália	26	0,4%

Tabela 3.1: Ranking dos países que mais enviaram *spam* ao DInf de acordo com a amostra coletada.

O *top 10* de países que mais enviaram *spam* para o Departamento de Informática é composto por Brasil, Estados Unidos, Dinamarca, Romênia, China, Noruega, Bulgária, Hong Kong, Canadá e Itália, de um total de 36 países. Em primeiro lugar do *ranking* está o Brasil, com 2.784 envios e por último a Itália, com 26.

Na Figura 3.1, é possível visualizar o mapa contendo todos os países, assim como as respectivas intensidades: quanto mais emails foram enviados a partir do país em questão, mais intensa é a cor. Fica marcante a presença do Brasil e Estados Unidos, que são os líderes do *ranking*.

Figura 3.1: Envio de spam por país.

Para facilitar a visualização dos outros países que também contribuíram com o *spamming* recebido por usuários do email do DInf, foram retirados da lista o Brasil e os Estados Unidos. Assim é possível visualizar com maior clareza, na Figura 3.2, a contribuição dos demais países.

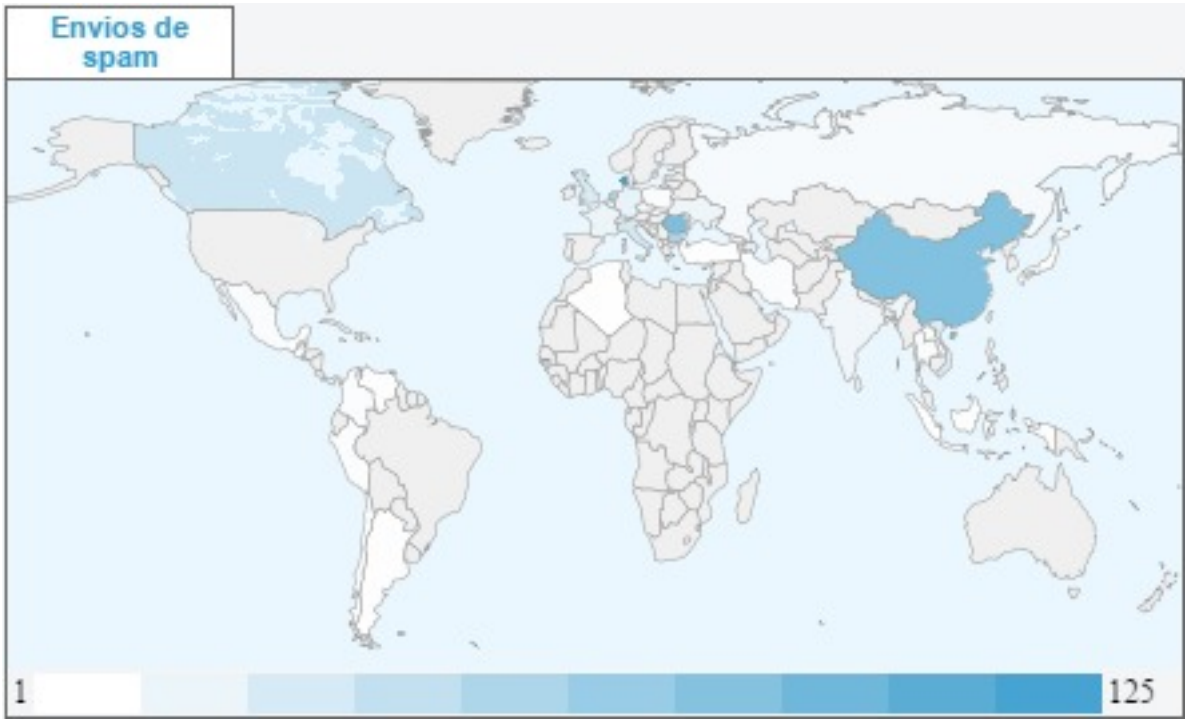

Figura 3.2: Envio de spam por país - exceto Brasil e EUA.

Além disso, verificou-se o assunto dos e-mails para identificar os idiomas nos quais possivelmente as mensagens dos *spams* são escritos. Para tanto, utilizou-se a biblioteca de detecção de idiomas `langdetect`[2], que é um *port* da detecção de idiomas do Google. Conforme Figura 3.3, a predominância é do português, com 97% das ocorrências, seguido pelo inglês, com 2,35%, após isso o espanhol com uma fração mínima de 0,15%, o que corresponde à 6 (seis) emails. Os 0,5% restantes dizem respeito à emails com o campo de assunto todo númerico, o que não pode ser identificado pelo `langdetect`.

[2]https://pypi.python.org/pypi/langdetect

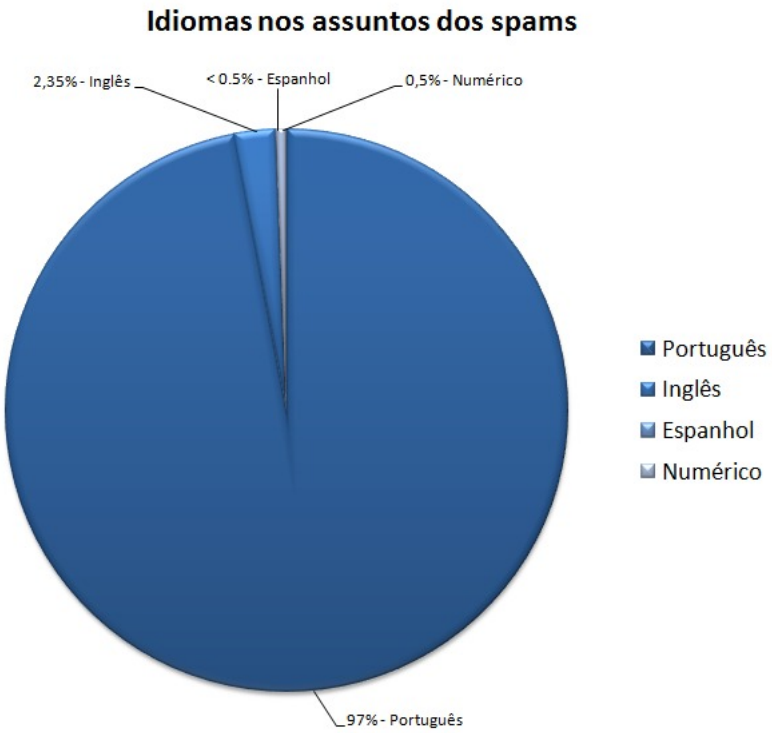

Figura 3.3: Idiomas retirados do campo *Subject* dos emails.

3.3 Análise de anexos e URLs

Neste trabalho, são considerados arquivos potencialmente executáveis aqueles anexos cujo MIME-type indica o tipo "*application*". Na maioria dos casos costuma ser um arquivo do tipo *zip* que pode conter um executável (para MS-Windows) ou outro tipo de código, como Java ou JavaScript.

Do total de 7.870 *spams* coletados, 182 possuem arquivos anexos. Este número baixo em relação à quantidade de emails inspecionados pode ser explicado uma vez que a maioria dos sistemas inspeciona automaticamente anexos em busca de *malware*, o que força os *spammers* a procurar alternativas, como por exemplo a utilização de *links* externos, que não são tão facilmente escaneados como os arquivos são. Conforme comentado anteriormente, a maioria dos anexos analisados neste trabalho são do tipo *zip*, o que reflete uma medida adicional dos *spammers* para prevenir que suas mensagens e arquivos sejam instantaneamente marcados como maliciosos, uma vez que arquivos compactados não são rapidamente inspecionados pelos antivírus [20].

A grande maioria dos *spams* com anexos, analisados pelo título, são de caráter financeiro. Em português, fazem menção à boletos, notas fiscais, faturas a serem pagas, débidos pendentes e comprovantes de depósitos. As exceções se referem à postagem de objetos pelos Correios, decisões judiciais, comunicados de advogados e outros títulos inconclusivos que despertam a curiosidade do leitor.

Todos os arquivos foram submetidos ao VirusTotal para análise de *malware*, o que retornou resultados bem detalhados, elaborados a partir de bases diversas. Apesar do VirusTotal contar com 62 bases para consulta de *malware*, foi observado que nem sempre todas elas são utilizadas. Dessa forma, para cada aquivo anexo, temos um número variável de vereditos se o arquivo é malicioso ou não. Diante dessa natureza dos dados de retorno do VirusTotal, a métrica que se adotou foi a de número de positivos de conteúdo malicioso pelo total de antivírus consultados, uma vez que os antivírus não necessariamente concordam entre si.

Na Figura 3.4, temos no eixo y o número de anexos nos emails pela taxa de detecção de malware, no eixo x. Dos 182, apenas 19 tiveram uma taxa de detecção acima de 0,5 (de um total possível entre zero e um), e nenhum deles teve uma taxa de detecção elevada: a maior foi de 0,67. Desses 19, 3 contêm duplicatas, uma vez que a vítima pode receber o mesmo email várias vezes ao longo dos dias, com uma pequena variação no título, por exemplo um email contendo um boleto para ser pago pode ser enviado mais de uma vez sob um assunto diferente, indicando ser um anexo diferente, quando na verdade não é.

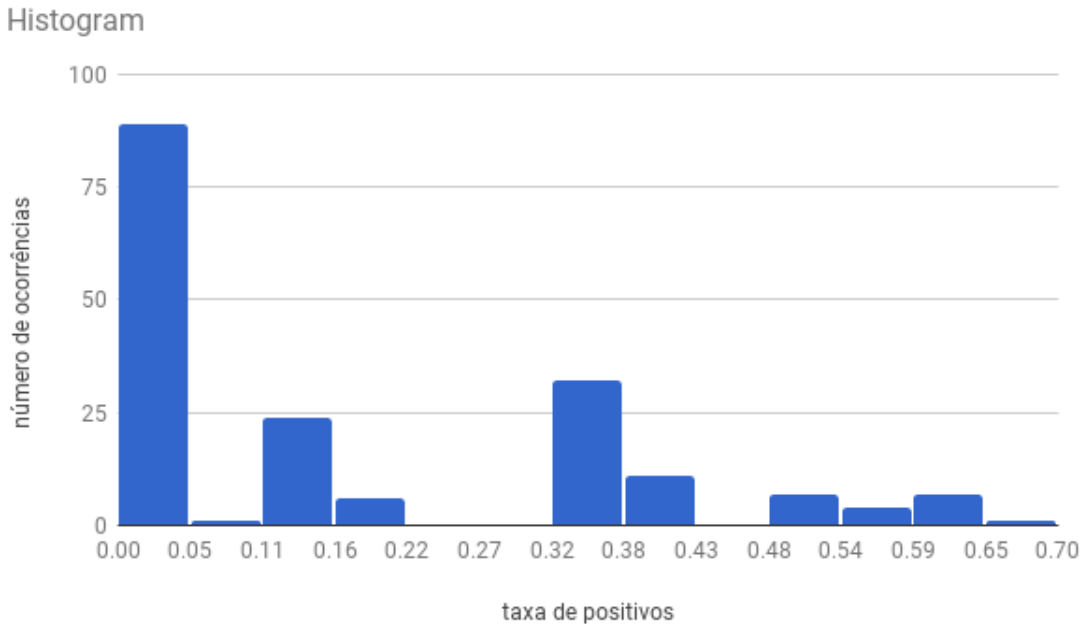

Figura 3.4: Número de anexos por taxa de detecção do VirusTotal.

Dentre os resultados de rótulos atribuídos a programas maliciosos obtidos do VirusTotal, o que mais apareceu foram *Trojans* relacionados à PDF advindos por *phishing*, o que pode ser visto nas posições 1, 5, 6 e 10 da Tabela 3.2), o que faz total sentido com o tipo de *malware* esperado em um email.

Posição no ranking	**Malware**	**Ocorrências**	**Porcentagem**
1	Trojan.PDF.Phish.kc	124	6.4%
2	Other:Malware-gen [Trj]	86	4.7%
3	RDN/Generic.dx	83	4.5%
4	PDF_PHISH.YTUGG	64	3.5%
5	Trojan.PDF.Phishing.MM	63	3.4%
6	Trojan.PDF.Phishing	41	2.2%
7	UnclassifiedMalware	37	2.0%
8	Malware_Generic.P0	34	1.8%
9	PDF/Phishing.A.Gen	33	1.8%
10	Trojan:PDF/Phish	32	1.7%
restantes	-	1220	67,1%

Tabela 3.2: Rótulos mais frequentes de malware advindos do VirusTotal

Para mostrar consisência, também foram obtidos os rótulos mais frequentes dentro os anexos a partir de apenas uma fonte, o antivírus Kaspersky, o que pode ser visto na Tabela 3.3. Em consonância com o resultado geral dos rótulos mais frequentes, a maior ocorrência entre os exemplares individualmente (mais de 80%) é a detecção como *Trojan-Phishing*. Isso suporta a hipótese de que os anexos enviados às vítimas são em sua maioria voltados à roubar dados sensíveis, como credenciais de serviços na Internet, e.g., contas de email, usuário/senha de bancos online, redes sociais, etc.

O rótulo *Null* indica que o arquivo analisado não é malicioso e, segundo o antivírus Kaspersky foi o que ocorreu em quase metade das submissões ao VirusTotal. Em segundo lugar encontram-se *Trojans* relacionados à PDF vindos de *phishing*, assim como também ocorrem na Tabela 3.2. *Phishing* é uma prática fraudulenta de enviar emails alegando ser de empresas de boa reputação para induzir as vítimas à revelarem informações pessoas, como senhas e detalhes de cartões de crédito [11].

Malware	Ocorrências	**Porcentagem das ocorrências**
Null	90	49.45%
Trojan.PDF.Phish.kc	62	34.06%
Trojan.PDF.Phish.pj	9	4.94%
HEUR:Trojan.Win32.Generic	9	4.94%
HEUR:Trojan-Downloader.Script.Generic	5	2.74%
HEUR:Trojan.Java.Agent.gen	4	2.19%
HEUR:Trojan.Script.Agent.gen	2	1.09%
Trojan-Downloader.JS.Cryptoload.axn	1	0.55%

Tabela 3.3: Frequência de rótulos de malware Kaspersky

Se o número de emails com anexo é baixo em relação ao total de *spams* utilizados neste trabalho, o número de *spams* com *hyperlinks* é bem maior, sendo de 7.411, ou seja, quase a totalidade da base utilizada. Cada email tem uma média de 15 *hyperlinks*.

Para fazer uma análise com o VirusTotal utilizando a API pública, com um total de 114.599 URLs a serem consultadas, levando em consideração a limitação de consultas do VirusTotal, ficaria inviável obter os resultados em tempo hábil. Isso ocorre porque, uma vez que há uma versão paga da API, a consulta gratuita em lote fica bastante prejudicada (baixa prioridade de análise na fila, erros frequentes na entrega dos resultados, impossibilidade de se realizar muitas consultas de um mesmo ID cadas-

trado, etc.). Além disso, como domínios que aparecem em *spam* e contêm *malware* são costumeiramente reportados e retirados do ar, não é simples verificar a potencial maliciosidade apenas pela submissão da URL para o VirusTotal. Dessa forma, optou-se pela análise dos tipos de domínio utilizados pelos *spammers* nos links enviados junto com as mensagens, dado que a base estava previamente rotulada.

3.3.1 Domínios mais frequentes

Para evitar o bloqueio do *spam* e ainda assim maximizar o sucesso dos ataques ou golpes, em vez de anexos, os *spammers* inserem em suas mensagens links que encaminham o usuário para sites clonados, formulários ou repositórios de código malicioso. Tal link de preferência é de algum domínio legítimo invadido anteriormente ou de algum serviço de nuvem, visando fazer com que o *spam* deixe de ser entregue à vítima devido ao fato de um desses links estar em alguma lista de bloqueio. A Tabela 3.4 mostra os 10 domínios mais frequentes dos links encontrados nos *spams* da base coletada.

Domínio	**Ocorrências**	**Porcentagem**
redirect-pg.s3-website-us-east-1.amazonaws.com	31.581	30,3%
redirect-pf.s3-website-us-east-1.amazonaws.com	30.450	29,2%
redirect-ph.s3-website-us-east-1.amazonaws.com	25.895	24,8%
redirect-pj.s3-website-us-east-1.amazonaws.com	5.770	5,5%
leadsturbo.com.br	1.068	1,0%
parceiroafiliado.com.br	577	0,5%
191.53.150.230	568	0,5%
www.divbx.com	489	0,4%
promocaonoemail.com.br	485	0,4%
app.crowmod.com.br	478	0,4%

Tabela 3.4: Maiores ocorrências de domínios nas URLs

Foram selecionados os domínios das URLs em questão, e foi nisso que se descobriu que muitas das URLs eram strings em branco. Após remover as vazias, obteve-se o total de 104.072 URLs e domínios. Dos domínios obtidos, apenas 963 são únicos. Foi montada uma lista dos domínios mais frequentes da Tabela 3.4, o que nos mostra que os serviços de *cloud* da Amazon lideraram o *ranking*. Os Amazon Web Services totalizam quase 90% dos domínios tal como eles aparecem nos emails. Isso indica

uma tendência dos spammers de utilizar serviços na *cloud*, pois eles mascaram as URLs verdadeiras incluindo o link para um serviço legítimo e que teoricamente não pode ser bloqueado, porém o utilizando para redirecionar o acesso do usuário para o real site malicioso.

Uma vez que tem sido comum a utilização de URLs encurtadas, serviços de redirecionamento, e *mail marketing*, se a confiança for posta na URL tal como aparece no *spam*, o usuário fica sem saber onde está clicando. Para isso a solução utilizada neste trabalho foi de seguir a URL até que ela não redirecione mais, a fim de se identificar qual o real domínio pretendido pelo *spammer* para suas vítimas.

Para monitorar os redirecionamentos, a partir de uma amostra contendo 15.976 URLs foram seguidas essas URLs utilizando a biblioteca urllib2 do Python. Dessa amostra, apenas 7.051 puderam ser seguidas, resultando em URLs finais. O maior número de ocorrêwncias são de propagandas da Arezzo. Outras marcas e empresas reconhecidas também constam na lista exibida na Tabela 3.5, mas o mais interessante mesmo são os 3 domínios *pricerem*. Não foram encontradas informações sobre o que o site se destina a fazer, não há nada além da mensagem "It works!"do Apache, mas aparentemente parece um site dedicado a hospedar *marketing* eletrônico.

Domínio	**Porcentagem das ocorrências nas URLs da amostra**
www.arezzo.com.b	11.0%
v2.afilio.com.br	8.4%
www.marcyn.com.br	8.2%
www.ordenato.com.br	5.5%
vr.tj.pricerem.com.br	5.0%
www.nike.com.br	3.1%
vr.tg.pricerem.com.br	2.6%
www.boticario.com.br	2.6%
vr.ls.pricerem.com.br	2.6%
www.cvc.com.br	2.6%

Tabela 3.5: Maiores ocorrências de domínios nas URLs já redirecionadas

Capítulo 4

Conclusão

Neste trabalho, foram coletados 7.870 mensagens de email de usuários do DInf — um professor, um formando bolsista da administração de redes e sistemas do Departamento e a aluna autora do presente texto. Tais mensagens estavam previamente rotuladas como *spam* pelos usuários que as forneceram e foram, todas elas, recebidas em seus emails institucionais de domínio `inf.ufpr.br`. Os "rótulos" de *spam* foram atribuídos principalmente de três maneiras distintas: as mensagens estavam separadas na caixa "JUNK" do cliente de email dos usuários; o usuário as identificou como *spam* em sua caixa de entrada, significando que a ferramenta antispam do cliente de email não funcionou adequadamente; as mensagens foram separadas como *spam* via regras personalizadas do `procmailrc` dos usuários.

Os *spams* coletados foram, então, destrinchados segundo os campos definidos no protocolo de concepção de um email e, posteriormente, inseridos em um banco de dados não relacional. A partir deste banco, foi possível verificar quais emails continham anexos e quais continham URLs. Nos que continham anexos (182 de 7.870), o objetivo era encontrar aqueles detectados como programas maliciosos. Portanto, os arquivos contidos em anexos foram enviados ao VirusTotal e os rótulos de detecção recebidos mostraram que boa parte dos anexos foi identificada como *Trojan* e *phishing*. As URLs coletadas nos emails, 114.599 no total, foram analisadas por domínio e por redirecionamento. Os domínios mais utilizados por *spammers* são os da nuvem da Amazon, enquanto que os redirecionamentos mostraram que o maior número de ocorrências vem de marcas e empresas amplamente reconhecidas pelo público, além de uma empresa que parece (pois não há nenhuma informação sobre ela na página inicial) hospedar propagandas mais duvidosas.

Por fim, com o conjunto de dados disponível, pôde-se observar que a maioria dos

spams são enviados de domínios dentro do Brasil e que a linguagem identificada na quase totalidade dos assuntos dos *spams* recebidos é o Português.

4.1 Trabalhos futuros

A análise realizada neste trabalho foi preliminar no sentido em que foram observadas tendências mais gerais das mensagens de *spam* recebidas pelo DInf/UFPR. Alguns desdobramentos possíveis deste trabalho são:

- Criação automática de listas "supervisionadas" de domínios potencialmente enviadores de *spam*;
- Desenvolvimento de mecanismos para elaboração de *ranking* de mensagens suspeitas baseados em regras dinâmicas e, consequentemente, apoio à implementação de regras de bloqueio dinâmicas;
- Análise aprofundada das URLs presentes nos *spams* recebidos, bem como a resolução dos redirecionamentos de maneira a fomentar uma ferramenta automatizada que analise e/ou classifique tais URLs;
- Treinamento e classificação de mensagens legítimas e não-solicitadas a fim de se produzir detectores auxiliados por algoritmos de aprendizado de máquina.

Referências Bibliográficas

[1] About virustotal. [Online; acessado em 10-Jun-2017].. Disponível em https://www.virustotal.com/en/about/.

[2] Anti-spam techniques. [Online; acessado em 10-Jun-2017].. Disponível em https://en.wikipedia.org/wiki/Anti-spam_techniques.

[3] Antivirus fundamentals: Viruses, signatures, disinfection. [Online; acessado em 10-Jun-2017].. Disponível em https://blog.kaspersky.com/signature-virus-disinfection/13233/.

[4] Cartilha de segurança para a internet. [Online; acessado em 10-Jun-2017].. Disponível em https://cartilha.cert.br.

[5] Estatísticas de notificações de spam reportadas ao cert.br. [Online; acessado em 30-Jun-2017].. Disponível em https://www.cert.br/stats/spam/.

[6] Número de usuários do facebook no brasil dobra em cinco meses. [online; acessado em 30-jun-2017].. Disponível em http://idgnow.com.br/internet/2009/10/21/numero-de-usuarios-do-facebook-dobra-no-brasil-em-5-meses-diz-ibope/.

[7] Open mail relay - wikipedia. [Online; acessado em 30-Jun-2017].. Disponível em https://en.wikipedia.org/wiki/Open_mail_relay.

[8] open relay (insecure relay or a third-party relay). [Online; acessado em 30-Jun-2017].. Disponível em http://searchnetworking.techtarget.com/definition/open-relay.

[9] Open relay test. [Online; acessado em 30-Jun-2017].. Disponível em http://www.mailradar.com/openrelay/.

[10] Operadoras brasileiras vão bloquear porta 25 para envio de emails. [online; acessado em 30-jun-2017].. Disponível em https://tecnoblog.net/120929/brasil-porta-25-bloqueio/.

[11] Phishing definition. [Online; acessado em 12-Jul-2017].. Disponível em http://searchsecurity.techtarget.com/definition/phishing.

[12] Prevenindo-se contra spams com o spamassassin. [Online; acessado em 30-Jun-2017].. Disponível em http://blog.webinhost.com.br/blog-dicas/prevenindo-com-o-spamassassin/.

[13] Sender policy framework - wikipedia. [Online; acessado em 10-Jul-2017].. Disponível em https://pt.wikipedia.org/wiki/Sender_Policy_Framework.

[14] Spamassassin - wikipedia. [Online; acessado em 10-Jul-2017].. Disponível em https://en.wikipedia.org/wiki/SpamAssassin.

[15] Ten spam-filtering methods explained. [Online; acessado em 10-Jun-2017].. Disponível em http://www.techsoupcanada.ca/en/learning_center/10_sfm_explained.

[16] Wayback machine. [Online; acessado em 30-Jun-2017].. Disponível em http://web.archive.org/.

[17] Mamoun Alazab e Roderic Broadhurst. An analysis of the nature of spam as cybercrime. *Cyber-Physical Security*, páginas 251–266. Springer, 2017.

[18] Marshall Brain. How spam works. [Online; acessado em 10-Jun-2017].. Disponível em http://computer.howstuffworks.com/internet/basics/spam1.htm.

[19] David H Crocker. Rfc822-standard for the format of arpa internet text messages, 1982. *WWW Document, URL http://www. faqs. org/rfcs/rfc822. html, accessed*, 26, 2000.

[20] Paulo Lício de Geus Heitor Ricardo Alves de Siqueira, André Ricardo Abed Grégio. Automated Analysis and Characterization of Spam and Malicious Content. Relatório técnico, Instituto de Computação da Unicamp, 2016.

[21] Govind Rammurthy. Spam. [Online; acessado em 10-Jun-2017].. Disponível em http://www.mwti.net/products/pdfs/White%20Paper%20Spam%20.doc.pdf.

[22] Justin M Rao e David H Reiley. The economics of spam. *The Journal of Economic Perspectives*, 26(3):87–110, 2012.

[23] Yakov Rekhter e Tony Li. A Border Gateway Protocol 4 (BGP-4). RFC 1654, RFC Editor, August de 1982. Disponível em `http://www.rfc-editor.org/rfc/rfc1654.txt`.

[24] Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, e Giovanni Vigna. The dark alleys of madison avenue: Understanding malicious advertisements. *Proceedings of the 2014 Conference on Internet Measurement Conference*, páginas 373–380. ACM, 2014.

Apêndices

Apêndice A

Esquema

A.1 Esquema

```
root
|- _id:  struct
| |- oid:  string
|- content:  struct
| |- attachment:  boolean
| |- attachment-list:  array
| | |- element:  struct (containsNull = true)
| | | |- body:  string
| | | |- type:  string
| |- body:  string
| |- multipart:  boolean
| |- type:  string
| |- url:  boolean
| |- url-list:  array
| | |- element:  string (containsNull = true)
|- header:  struct
| |- ACM_local[3125389]:  string
| |- Abuse-Reports-To:  string
| |- Authentication-Results:  string
| |- Content-Description:  string
| |- Content-Disposition:  string
| |- Content-Transfer-Encoding:  string
```

```
| |- Content-Transfer-encoding:  string
| |- Content-Type:  string
| |- Content-type:  string
| |- DKIM-Signature:  string
| |- Date:  string
| |- Delivered-To:  string
| |- Disposition-Notification-To:  string
| |- EM-Campaign:  string
| |- EM-Task:  string
| |- Errors-To:  string
| |- Feedback-ID: string
| |- From:  string
| |- Importance:  string
| |- In-Reply-To:  string
| |- List-ID: string
| |- List-Unsubscribe:  string
| |- MIME-Version:  string
| |- Message-ID: string
| |- Message-Id:  string
| |- Mime-Version:  string
| |- Organization:  string
| |- Priority:  string
| |- Received:  string
| |- Received-SPF: string
| |- References:  string
| |- Reply-To:  string
| |- Return-Path:  string
| |- Sender:  string
| |- Subject:  string
| |- To:  string
| |- User-Agent:  string
| |- X-Abuse-Info:  string
| |- X-Abuse-Report:  string
| |- X-AntiAbuse:  array
| | |- element:  string (containsNull = true)
| |- X-Authenticated-Sender:  string
```

```
| |- X-BYPSHEADER: string
| |- X-Binding:  string
| |- X-Bogosity:  string
| |- X-Campaign:  string
| |- X-CampaignID: string
| |- X-Complaints-To:  string
| |- X-EMKT-ID: string
| |- X-EOPAttributedMessage:  string
| |- X-Exchange-Antispam-Report-CFA-Test:  string
| |- X-Exchange-Antispam-Report-Test:  string
| |- X-Feedback-ID: string
| |- X-Forefront-Antispam-Report:  string
| |- X-Forefront-PRVS: string
| |- X-Forwarded-Message-Id:  string
| |- X-Get-Message-Sender-Via:  string
| |- X-LCID: string
| |- X-Library:  string
| |- X-MS-Exchange-CrossTenant-FromEntityHeader:  string
| |- X-MS-Exchange-CrossTenant-Id:  string
| |- X-MS-Exchange-CrossTenant-OriginalArrivalTime:  string
| |- X-MS-Exchange-CrossTenant-OriginalAttributedTenantConnectingIp:  string
| |- X-MS-Exchange-Transport-CrossTenantHeadersStamped:  string
| |- X-MS-Office365-Filtering-Correlation-Id:  string
| |- X-MS-TrafficTypeDiagnostic:  string
| |- X-MSMail-Priority:  string
| |- X-Mailer:  string
| |- X-Mailer-Info:  string
| |- X-Mailer-LID: string
| |- X-Mailer-MID: string
| |- X-Mailer-RecptId:  string
| |- X-Mailer-SID: string
| |- X-Mailer-Sent-By:  string
| |- X-Microsoft-Antispam:  string
| |- X-Microsoft-Exchange-Diagnostics:  array
| | |- element:  string (containsNull = true)
| |- X-MimeOLE: string
```

```
| |- X-Original-From:  string
| |- X-Original-To:  string
| |- X-OriginalArrivalTime:  string
| |- X-Originating-Email:  string
| |- X-PHP-Originating-Script:  string
| |- X-PHP-Script:  string
| |- X-Priority:  string
| |- X-SMScore:  string
| |- X-SM_EnvelopeFrom:  string
| |- X-SM_Proxy:  string
| |- X-SM_RECEIVED_ON: string
| |- X-Sender:  string
| |- X-Source:  string
| |- X-Source-Args:  string
| |- X-Source-Dir:  string
| |- X-Virus-Scanned:  string
| |- X-campaignid:  string
| |- X-cid:  string
| |- X-elqPod:  string
| |- X-elqSiteID: string
| |- X-iGspam-global:  string
| |- X-mailer:  string
| |- X-rpcampaign:  string
| |- X_elemento:  string
| |- X_emailId:  string
| |- X_empresa:  string
| |- X_resumenId:  string
| |- content-type:  string
| |- dkim-signature:  string
| |- emcodigo:  string
| |- proxyid:  string
| |- secodigo:  string
| |- to:  string
```

Figura A.1: Esquema