Análise de Mecanismos de Guerra Cibernética através do Desenvolvimento de uma Arquitetura Conceitual para a Criação de Social Botnet e de um Método para Facilitar sua Infiltração

Vanessa Quadros G. Leite
Instituto Militar de Engenharia - IME
Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, 22290-270
vanessaquadros@cos.ufrj.br

Ronaldo Moreira Salles
Instituto Militar de Engenharia - IME
Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, 22290-270
salles@ime.eb.br

RESUMO

Ao mesmo tempo que a Internet e a transformação digital facilitam a comunicação e trazem maior eficiência para o mundo, elas implicam no surgimento de diversos riscos desconhecidos e dinâmicos, sendo muito deles relacionados ao acesso das informações e manipulação das massas. Em função disso, são corriqueiros os casos de uso de ciberataques centrados na manipulação de informações com objetivos políticos, incluindo o propósito de intervir em processos eleitorais de outros países. Com base nisto, os objetivos desta pesquisa são estudar e analisar as *social botnets* como estrutura de ataques cibernéticos, de forma a melhor compreender a sua dinâmica e assim poder desenvolver métodos mais eficazes de defesa e combate a essas ameaças. Isso será feito através da criação de uma arquitetura conceitual para a geração de uma social e da definição de um método para facilitar a infiltração dos *socialbots* em uma rede social. Como resultado da execução da *social botnet*, serão analisados e elencados os fatores que devem ser considerados para utilizar o Facebook como um ambiente de atuação dos robôs sociais e também pontos de atenção que a defesa brasileira deverá ter em relação ao ciberespaço do país.

Palavra-chave: Social Botnet; Arquitetura; Guerra Cibernética; Infiltração; Redes Sociais.

ABSTRACT

While the Internet and digital transformation facilitate communication and bring greater efficiency to the world, they imply the emergence of several unknown and dynamic risks, many of which relate to information access and mass manipulation. As a result, cyberattacks focused on manipulating information for political purposes are commonplace, including the purpose of intervening in electoral processes in other countries. Based on this, the objectives of this research are to study and analyze social botnets as a structure

of cyber attacks, in order to better understand their dynamics and thus to develop more effective methods of defending and combating these threats. This will be done by creating a conceptual architecture for social generation and defining a method to facilitate socialbots infiltration into a social network. As a result of the execution of the social botnet, we will analyze and list the factors that should be considered in order to use Facebook as an environment for social robots and also points of attention that the Brazilian defense should have in relation to the country's cyberspace.

Keywords: Social Botnet; Architecture; Cyber War; Infiltration; Social Networks.

Como Citar:
LEITE, Vanessa 1; SALLES, Ronaldo 2. Análise de Mecanismos de Guerra Cibernética através do Desenvolvimento de uma Arquitetura Conceitual para a Criação de Social Botnet e de um Método para Facilitar sua Infiltração. In: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 19., 2019, Rio de Janeiro, RJ. **Anais** [...]. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

1. INTRODUÇÃO

A transformação digital traz eficiência para o mundo. Entretanto, ao mesmo tempo, provoca uma série de riscos ainda desconhecidos associados ao vazamento de informações e que impactam diversos setores que lidam diretamente com o armazenamento de dados [1]. Isso porque, de acordo com o CEO da Pentagono *Cyber Insurance Advisors* [1], existem atualmente duas vezes mais aparelhos conectados do que pessoas, sendo que tais equipamentos não apresentam segurança adequada.

Em função disso, os ataques cibernéticos e as falhas de segurança na Web são considerados itens de constante preocupação para os governos e entidades [2]. Um exemplo de mecanismo capaz de amplificar os ataques, sendo também considerado uma das armas cibernéticas sofisticadas de guerra deste século [3], são as *botnets*, nos quais os indivíduos responsáveis pela ação maliciosa se infiltram nos computadores em todo o mundo com softwares para realizar os ataques coordenados. [4]

Um ataque similar ao citado pode ser realizado nas redes sociais, utilizando a estrutura de uma *social botnet*. Neste ataque existe um indivíduo ou sistema mal-intencionado *botmaster* ou controlador com acesso a uma ou mais contas da *Online Social Network* (OSN), sendo este modo pelo qual interage com a mídia social. As atividades que um controlador pode executar através de uma *social botnet* são delimitadas pelo conjunto de ações que o OSN disponibiliza para qualquer usuário legítimo. [5]

Um dos grandes riscos inerentes a uma *social botnet* é a sua capacidade de: infectar diferentes sistemas operacionais (Linux, Windows, MacOS) [6, 7]; capturar as credenciais dos usuários de diferentes mídias mídias sociais, como ocorreu com o Koobaface [6]; influenciar pessoas em grande escala [8], principalmente durante a divulgação de campanha política, já que algumas referências indicam a possibilidade de terem utilizado esse tipo de estrutura com objetivos eleitorais [9, 10, 11].

Em função da sua facilidade de atuação na camada social do ciberespaço, uma *social botnet* pode ser utilizada como arma cibernética de um país para influenciar uma outra nação, como ocorreu na eleição do Trump, onde há indícios da atuação da Rússia

através do uso de *socialbots* para que ele fosse eleito nos Estados Unidos [12, 13].

Um outro caso onde houve uso de *socialbot*, um software de automação preparado para interagir com seres humanos nas mídias sociais, que inclusive é capaz de imitar e de influênciar o comportamentos dos usuários legítimos [14], foi observado num processo de pregão online do governo dos Estados Unidos em 2010 [15]. Nele havia solicitação de prestação de um serviço de gerenciamento de personas cibernéticas online cujo software permitiria que cada operador as gerenciasse e forneceria um contexto, histórico, detalhes de suporte e presenças cibernéticas que sejam técnica, cultural e geograficamente consistentes [15].

Neste contexto é que se insere o presente trabalho, cujo objetivo é estudar e analisar as *social botnets* como estrutura de ataques cibernéticos através da criação de uma arquitetura conceitual e de uma método para a criação de *socialbots* independente da arquitetura proposta, capaz de facilitar a infiltração do *socialbot* na rede social a ser explorada. Assim, será possível que terceiros desenvolvam métodos mais eficazes de defesa e combate a essas ameaças. É válido ressaltar que nesta pesquisa, será explorado o Facebook por ser a rede social mais utilizada no mundo [16].

2. TRABALHOS RELACIONADOS

A literatura apresenta diversos trabalhos sobre a criação de *socialbots* e *social botnets*, mas poucos com atuação no Facebook em função da sua complexidade de exploração devido às limitações de sua API [17]. Alguns deles serão apresentados a seguir.

[18] executam ataques à privacidade baseados em amigos em comum em uma rede social, utilizando grafos e um *dataset* com vários atributos sintéticos dos usuários. Desta forma, descobriram um usuário malicioso é capaz de lançar ataques de privacidade que identificam amigos e vizinhos distantes de um usuário específicio. Também analisam as várias estruturas de ataque passíveis de utilização para a construção de estratégias para explorá-lo.

[19] analisam as vulnerabilidades de uma OSN para a criação de *social botnet*. Para isso, os autores executaram os testes por oito semanas, utilizando a arquitetura que propuseram com base na API do Facebook e alcançando uma taxa de infiltração de 80% de sucesso de contas falsas nesta rede social. Também é observado que a simulação mostra que um invasor usando apenas um nó atacante pode identificar mais de 60% dos amigos de um usuário.

Apesar do resultado obtido, a criação dos *socialbots* com capacidade de publicar conteúdos de usuários legítimos selecionados aleatoriamente, a fim de imitar o comportamento humano, facilita na detecção desses, visto que os interesses ou as ações de um *socialbot* podem ser contraditórias. Outro problema observado é que o artigo é totalmente embasado na API do Facebook, que está cada vez mais restritiva com o passar dos anos [17]. Isso implica na criação de novas técnicas de exploração.

Já [5] empregam uma abordagem com uso de *malware* para construção de *bots* no Facebook e GooglePlus. Desta forma, para tornar estes robôs ativos na *botnet* Elisa, eles devem ser utilizados por uma vítima ao interagir com alguma OSN. Esta *botnet* usa esteganografia para esconder seus comandos dentro das mensagens das vítimas, tornando assim o conteúdo publicado mais confiável para os amigos das mesmas. A limitação

presente neste artigo é dificuldade da *botnet* Elisa conseguir ampliar a sua rede de amigos e, consequentemente, de atuação, já que a sua propagação exclusivamente através de *malware*, não sendo apresentada nenhuma solução para que exista interação dos *bots* em novos ciclos sociais.

[20] utilizam contas legítimas no Twitter como *socialbots*. Para a construção da *social botnet*, eles compraram contas no Twitter e desenvolveram o *botmaster* em Java, utilizando o protocolo OAuth e a própria API desta rede social. Assim, foi possível executar todas as operações do Twitter em nome de todos os robôs sociais de modo que esses apresentassem comportamentos similares ao usuários legítimos. Conforme já sinalizado em outro momento, o uso exclusivo de APIs limita a atuação da *social botnet*, em função das atualizações e restrições que possam surgir.

Em [21] é previsto que um *rootkit* de automação de teste web (WTAR) seja um meio para a concepção de *socialbots* maliciosos. Eles implementaram estes robôs sociais em algumas mídias sociais (Facebook, Twitter e Weibo) e validaram a ameaça. Para isso, analisaram os comportamentos dos protótipos em um ambiente de laboratório e na Internet. Também acompanharam os relatórios dos antivírus amplamente utilizados.

Além dos *socialbots* de [21] serem baseados em WTAR, independente da rede social, também podem imitar comportamento humano através de um automatizador de testes. Entretanto, a pesquisa mostrou limitação, visto que ao utilizar um *malware* como base da pesquisa e caso a máquina fosse desligada, a inicialização deveria ser manual e a atividade do *bot* era suspensa.

3. MÉTODO DE INFILTRAÇÃO DE UMA *SOCIAL BOTNET*

Com o objetivo de inserir os *socialbots* com maior facilidade em uma rede social, criou-se um método para a geração dos perfis, algo que não foi observado nos trabalhos relacionados a este tema, através do levantamento do comportamento dos usuários brasileiros na Internet, sobretudo nas mídias sociais. Desta forma, foram utilizadas como base as informações presentes em [22], com os seguintes dados estatísticos segmentados por:

1. Idade: A maior parte dos usuários das mídias sociais estão na faixa etária entre os 15 e 44 anos, conforme a Tabela 1.

Tabela 1: Distribuição de usuários das Mídias sociais no Brasil a partir da faixa etária. [22]

Faixa Etária	Taxa
menos de 15 anos	17%
15 até 24 anos	22,4%
25 até 34 anos	23,2%
35 até 44 anos	20,9%
45 até 55 anos	11,6%
mais de 55 anos	4,9%

2. Sexo: O uso das mídias sociais por homens é praticamente igual à taxa de mulheres, já que eles representam 50,5% dos usuários no Brasil [22].

3. Localidade: A região Sudeste corresponde à quase metade dos usuários do país atuantes nas Mídias Sociais [22]. Em função disso, levando em consideração os dados presentes na Tabela 2, as vinte cidades mais populosas do Brasil [23] foram distribuídas aleatoriamente entre as regiões as quais pertencem.

Tabela 2: Distribuição de usuários das Mídias sociais com base nas regiões do Brasil. [22]

Região	Taxa
Norte	4,2%
Nordeste	15,9%
Centro-Oeste	9,9%
Sudeste	49,7%
Sul	20,2%

A geração dos atributos dos perfis simulados foi realizada de modo independente para cada um dos critérios apresentados acima. Isso ocorre porque existe uma dificuldade inerente de encontrar os dados unificados, como por exemplo é a porcentagem das idades com relação à cada região e estado. Desta forma, para a criação das contas falsas, o responsável por controlar os *socialbots* deverá definir as credenciais dos usuários.

Os dados destes usuários, como nome, devem ser criados com base em [24], no qual mostra os vinte nomes femininos e masculinos mais comuns categorizados pelas décadas. Já em relação aos sobrenomes, usa-se [25], onde lista os trinta sobrenomes mais comuns no país, que em alguns casos foram combinados de forma aleatória entre si.

Os emails utilizam como base o nome ou possível apelido daquele nome, separado por ".", com nomes do meio abreviados, último sobrenome escrito por inteiro e os dois últimos dígitos do ano de nascimento. Como pode ocorrer do email já existir, quando este cenário ocorre, repete-se os dois números até não existir mais conflito.

Já em relação à distribuição por mês de nascimento no qual o indíviduo nasceu, como a base de dados de [26] não aponta dados anteriores à 1994, foram escolhidas as informações mais recentes. Desta forma, foram calculadas as porcentagens com base no total de 3.017.668 brasileiros nascidos em 2015, agrupados por mês do nascimento. O resultado deste cálculo pode ser observado na Tabela 3.

Após o cadastro, em alguns perfis sugere-se a inclusão de uma foto pessoal, antecedentes e interesses. Os antecedentes e interesses precisam ser definidos a partir de gostos populares ou regionais. Com base em [6], a fim de disfarçar-se como uma conta legítima, os perfis mais aprimorados se juntam a vários grupos sociais a partir de palavras-chave que representem referências populares, como grupos que discutem sobre alguma vertente política.

Conforme é possível observar, o método descrito para facilitar a infiltração da *social botnet* em uma rede social é adaptável para qualquer nacionalidade, devendo apenas buscar as informações com as entidades responsáveis pelo mapeamento do comportamento dos cidadãos, para em seguida distribuir e caracterizar os *socialbots* com base no método que foi descrito neste capítulo.

Tabela 3: Porcentagens dos brasileiros nascidos em 2015 e agrupados por mês de nascimento

Mês	Taxa de Porcentagem
Janeiro	8,4%
Fevereiro	8%
Março	9,2%
Abril	8,7%
Maio	8,9 %
Junho	8,4%
Julho	8,4%
Agosto	8,1%
Setembro	8,3% Outubro 8%
Novembro	7,6%
Dezembro	8%

4. CONSTRUÇÃO DA *SOCIAL BOTNET*

4.1. Modelo Adversário

O atacante, ou *botmaster*, é um entidade maliciosa (indivíduo ou sistema) que tem acesso para comandar uma ou mais contas de redes sociais. Através de suas contas, o *botmaster* ou controlador interage com a rede social. Suas ações são limitadas pelo conjunto legítimo de ações que a mídia social a ser explorada disponibiliza para qualquer usuário. Destaca-se que não houve difusão de *malware* e nem tão pouco a execução de qualquer ação que pudesse causar algum tipo de dano.

4.2. Arquitetura Conceitual Proposta

Durante a criação da arquitetura conceitual para a construção de uma *social botnet* e para a execução de suas atividades em uma rede social, foi realizada uma divisão semântica em cada dos seus componentes. A primeira parte representa a criação de perfis, ou seja, contempla as atividades de criação de emails e contas da rede social.

O trabalho nesta etapa é diretamente proporcional ao tamanho da *social botnet* a ser criada, então indica-se o uso de automatizadores capazes de preencher campos de página web, para que a criação de contas seja de um modo parcialmente ou totalmente automático. O modo como a automatização será tratada, se será parcial ou completa, depende da robustez da arquitetura implementada e da rede social a ser avaliada. Por exemplo, o Facebook realiza diferentes tipos de confirmação de um perfil e isso ocorre de acordo com o fornecedor de email. No caso do Outlook, Yahoo e Gmail, o processo é através de uma URL (*Uniform Resource Locator*) a ser acessada por email. Com outros provedores, como Prontmail, é enviado um código que deve ser digitado pelo usuário.

O segundo componente refere-se à execução da *social botnet*", já que após o levantamento dos trabalhos relacionados, foi concluído que um *socialbot* consiste em um

perfil de uma OSN e no *software* que automatiza a forma como ele interage com os outros usuários. A partir dos componentes apresentados, foi possível obter a seguinte arquitetura conceitual:

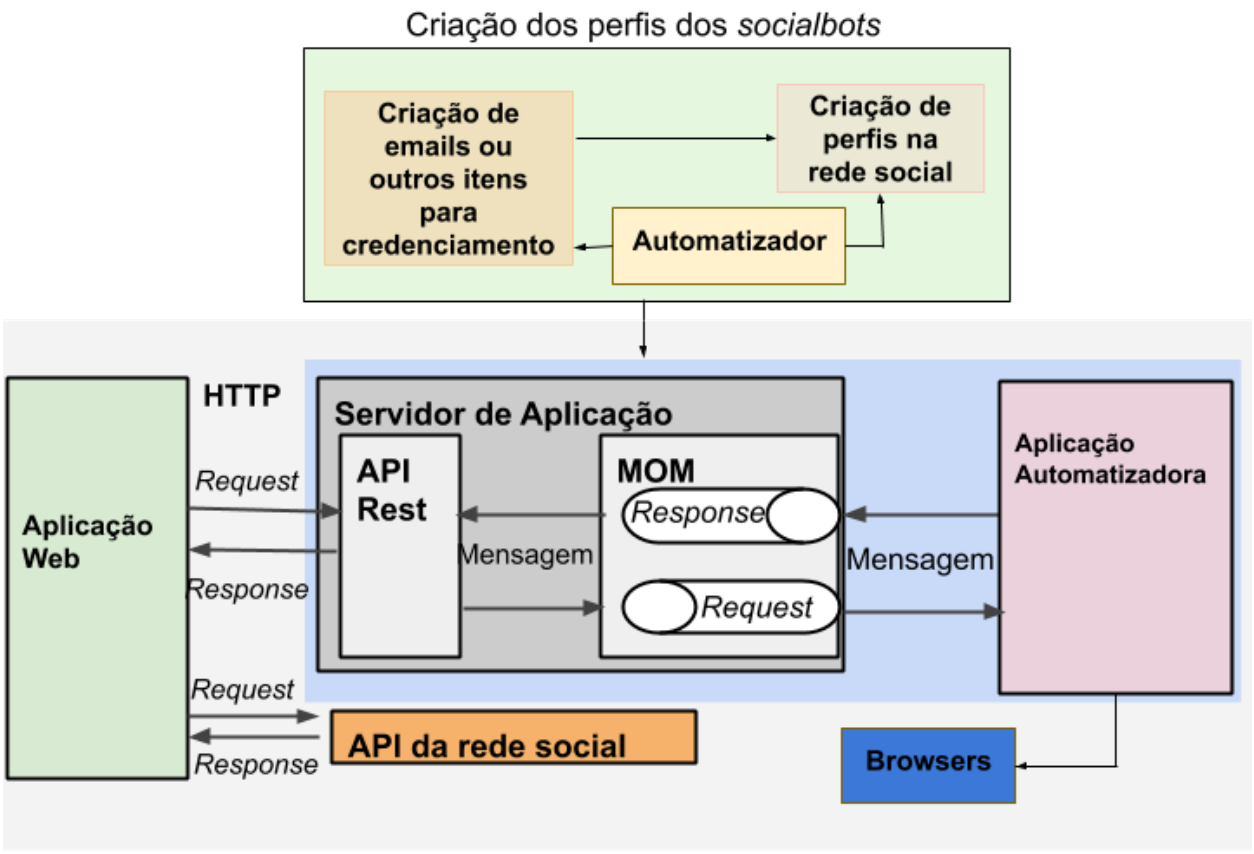

Figura 1: Estruturação das etapas "criação dos perfis dos *socialbots*"e "execução da *social botnet*"na Arquitetura Conceitual.

Nesta arquitetura não há a especificação dos componentes, somente a indicação dos papéis de cada um deles, o que faz com que ela possa ser aplicada em qualquer rede social que possua uma API. Isso porque, na Figura 1 é sinalizada a existência de uma aplicação web que funcionaria sobre a respectiva API da rede social a ser explorada, com a comunicação entre as ambas partes através de requisições do protocolo HTTP. Estas requisições utilizariam uma linguagem reconhecida por *browser*, como JavaScript.

Além disso, há uma camada (retângulo azul claro) que permite que as demais partes do projeto evoluam independentemente umas das outras. Optou-se, portanto, por propor uma arquitetura orientada a serviços, o que sugere o desenvolvimento de uma API REST. Essa é a responsável por receber as requisições HTTP da interface web, enviá-las a um *Message Oriented Middleware* (MOM). Ele é capaz de receber e armanzenar a mensagem enviada de um lugar e de repassá-la para um outro lugar. Assim, ele envia o pedido à um automatizador responsável por processar o pedido e respondê-lo de forma adequada.

Portanto, não há um acoplamento de nenhum componente da arquitetura, para

que caso seja necessário qualquer tipo de alteração futura, essa poderá ocorrer sem que as demais partes sejam afetadas, como por exemplo, uma alteração das tecnologias utilizadas. Além disso, há a aplicação automatizadora, que representa o código a ser desenvolvido de acordo com as ações passíveis de execução dos *socialbots* na rede social escolhida. Estas ações consistem nas funcionalidades disponibilizadas pelas OSNs para os seus usuários.

4.3. Execução da *social botnet*

4.3.1. Criação dos perfis dos *socialbots*

Para executar a *social botnet* com base na arquitetura proposta, foi necessário criar os *socialbots*. É válido ressaltar que a implementação da arquitetura conceitual foi direcionada para a exploração do Facebook, por ser a rede social mais utilizada no mundo [16].

Durante o processo de criação de contas de usuário em uma rede social, foi observado que um endereço de email ou número de celular são necessários primeiro para validar e, em seguida, ativar a conta através deste email ou da inserção de um código recebido por mensagem para a confirmação da criação da conta. Após a confirmação, seu proprietário a ativa e define suas preferências seguindo uma URL de ativação enviada por e-mail ou por mensagem. Consequentemente, para criar os *socialbots*, é preciso superar estes obstáculos. Em relação aos emails, existem as seguintes soluções possíveis:

- uso de emails temporários;
- utilização de provedores comuns que não limitam o número de contas de e-mail criadas por sessão de navegação ou endereço IP (por exemplo, MailRu[1]);
- aplicação de provedores, por exemplo ProntonMail[2], que não solicitam celulares para atestar a criação da conta, pedindo assim apenas as credenciais do usuário e um email para recuperação, sendo o email um item não obrigatório;
- emprego de fornecedores clássicos que solicitam celular para confirmar a criação de conta, como Yahoo ou Gmail;

As duas primeiras abordagens foram também descritas em [19], e funcionam até hoje. A terceira foi analisada durante o estudo e foi vista sua efetividade durante a execução do mesmo. Enquanto a última foi empregada para dificultar a detecção em função do amplo uso destes provedores.

Como [19] exemplifica apenas 10MinuteEmail[3] e MailRu sendo uma solução temporária e um provedor comum sem limitação na quantidade de contas respectivamente, para definir qual solução de email temporário seria aplicada, na tabela 4 foram avaliadas algumas ferramentas.

Também houve a tentativa de utilizar números de celular temporários. Esses são números não associados a nenhum indivíduo específico, obtidos através de sites que

[1]https://e.mail.ru/login
[2]https://protonmail.com/
[3]https://www.10minutemail.com/10MinuteMail/index.html?dswid=8568

Tabela 4: Avaliação do efetividade de uso de soluções de emails no Facebook e no Twitter.

Ferramenta	Atuação sobre o Facebook	Atuação sobre o Twitter
https://temp-mail.org/	Não funciona	Funciona
https://tempail.com/	Funciona	Funciona
https://app.inboxbear.com/	Não funciona	Funciona
https://pt.emailfake.com/	Não funciona	Funciona
https://www.guerrillamail.com/	Não funciona	Funciona
https://10minutemail.com/	Não funciona	Funciona
https://www.mohmal.com/	Funciona	Funciona
https://www.crazymailing.com/	Não Funciona	Funciona

fornecem o serviço de recebimento de mensagem. Algum sites, como *Receive* SMS Online [4] e *Receive Free* SMS Online[5], fornecem este tipo de serviço ao disponibilizarem um mesmo número para diversos usuários. Entretanto, quando os celulares temporários foram utilizados para criar contas, tanto o Facebook quanto o Twitter os identificaram e os classificaram como inválidos ou não existentes. A única solução de celular temporário testada que funcionou bem com estas redes sociais foi o MyTrashMobile [6]. Esta ferramenta apresenta o diferencial de disponibilizar números de telefone individuais para os seus usuários, de modo que ninguém mais os poderá utilizar.

Em relação à ativação da conta, observou-se que a mesma não era impeditiva para o uso do perfil em nenhuma das redes sociais, pois o novo perfil conseguia interagir normalmente com os demais usuários e realizar as ações através das funcionalidades que o Twitter e o Facebook disponibilizam para os perfis legítimos. Então não houve um preocupação em automatizar este processo.

É importante ressaltar que esta primeira etapa da implementação utilizou o Selenium[7], que é um conjunto de ferramentas utilizado principalmente para automatizar testes de aplicações web. Entretanto, ele não se limita a isso, já que que pode ser usado para automatizar qualquer tipo de tarefa efetuada em um navegador [27].

Através do uso desta ferramenta, foi possível automatizar o processo de criação das contas de email ou dos perfis do Facebook. Entretanto, nos casos onde ocorriam algum tipo de validação, as atividades referentes à ela foram executadas manualmente, como quando acontecem as verificações após a criação de emails providos por fornecedores clássicos (Gmail, Yahoo ou Outlook) ou de perfis de usuários no Facebook.

A *social botnet* foi implementada com base na arquitetura conceitual proposta, sendo criado uma ferramenta responsável por realizar as atividades da *socialbot* e fornecer uma interface de gerenciamento dos perfis de teste para o controlador. A implementação desta arquitetura permitiu a realização das seguintes ações:

Além de realizar as ações disponíveis para o usuário comum, também foi im-

[4]http://receive-sms-online.com/
[5]http://receivefreesms.com/
[6]https://pt.mytrashmobile.com
[7]http://www.seleniumhq.org/

Tabela 5: As possíveis ações a serem executadas através da ferramenta de gerenciamento dos *socialbots* nos seus respectivos perfis e nos perfis de terceiros.

Ação	Próprio Perfil	Perfil de Terceiros
Curtir conteúdo	Sim	Sim
Postar conteúdo	Sim	Sim
Inserir fotos em álbuns	Sim	Não se aplica
Comentar	Sim	Sim
Responder Comentário	Sim	Sim
Aceitar e recusar amigos	Sim	Não se aplica
Adicionar lista de amigos	Sim	Não se aplica
Ativar, desativar ou remover perfil	Sim	Não se aplica

plementada a funcionalidade de agendamento de ações, no qual um determinado perfil legítimo tinha suas ações clonadas, de modo que as suas atividades fossem replicadas por um ou vários *socialbots* na data escolhida para execução.

Portanto, os conteúdos a serem utilizados nas ações dos *socialbots* poderiam ser gerados de modo manual ou automático. No primeiro caso, o conteúdo é gerado manualmente pelo controlador da *social botnet*. Já o segundo, é realizado através do agendamento das execuções das atividades inclusas num arquivo de entrada. No caso deste estudo, o arquivo a ser utilizado foi fornecido pelo [28], que o gerava através do criação de um aplicativo usado por usuários do Facebook. Portanto, a implementação da arquitetura conceitual satisfaz também a geração de conteúdo automático.

A atuação da *social botnet* contemplou um período em dias corridos superior à doze semanas e com cerca de 80 *socialbots*. Dentre eles, 30 foram criados sem lógica e 50 o utilizaram o método sugerido neste estudo . O uso de metodologia para infiltração foi importante para minimizar riscos dos ‘socialbots serem excluídos do Facebook, já que foi possível manter a quantidade de pelo menos 50 perfis ativos (todos utilizando o método de infiltração proposto neste artigo) durante o experimento.

No período que a *social botnet* estava ativa, foram mapeadas mais de 3000 interações com usuários legítimos. Observou-se que os perfis mais atraentes, sobretudo mulheres, apresentavam mais solicitações de amizade e interações. Por exemplo, em um perfil feminino com faixa etária inferior à 30 anos, 101 pedidos de solicitação de amizade foram aceitos em 1 dia e em apenas 4 minutos, 83 aceites de pedidos foram realizados sem qualquer tipo de bloqueio pelo Facebook. Além disso, este mesmo perfil apresentava cerca de 200 perfis adicionados em cerca de 3 dias e também foi sugerido um encontro por um usuário, onde um usuário aparentemente legítimo repassou o seu número de celular.

Também notou-se que até mesmo os perfis sem fotos e com variedade de ações bastante limitadas, recebiam solicitações de amizade por perfis brasileiros aparentemente legítimos, o que indica o quão os brasileiros são vulneráveis nas redes sociais.

Durante a execução da *social botnet*, foi possível notar algumas políticas de segurança que visavam limitar ações suspeitas, sejam elas relacionadas aos provedores de email ou ao Facebook. A criação do perfil ou validação no Facebook a partir número de celular, é algo que sofre uma forte verificação, pois a identificação de números celulares temporários na maioria dos casos ocorria imediatamente.

A validação foi também observada quando os perfis utilizam como credencial o email e são criados sem a inserção de qualquer informação pessoal e sem execução de ações no Facebook. Nestes casos, a conta é excluída em menos de uma semana ou, para utilizá-la, é necessário inserir um número de celular válido.

Em relação ao uso de uma mesma máquina com um IP fixo para o processo de automatização na criação das contas do Facebook, não foi observada nenhuma restrição neste contexto, já que foi permitido criar mais de vinte contas em um único dia. Normalmente, a limitação existia por parte dos provedores de emails clássicos, como o Hotmail, Gmail ou Yahoo. O primeiro restringia a criação de cinco emails por dia por números de celulares. O segundo permitia por dia a geração de duas contas com um mesmo número de celular.

Já o terceiro, no primeiro dia de uso permitiu a criação de dez contas com o mesmo celular. Posteriormente, surgiu um bloqueio que durou dois dias e, em seguida, foi permitido criar cinco contas de email por dia sem o bloqueio aparecer novamente. Mesmo com o apontamento destas questões relacionadas aos provedores de emails, não foi possível indicar se o não bloqueio por IP pelo Facebook se manteria caso fosse usada uma quantidade maior de contas de email.

Uma questão importante observada foi que após os perfis do Facebook serem criados, confirmados e terem um período de uso recorrente igual ou superior à uma semana, dificilmente existia alguma validação posterior em relaçâo às ações que executavam. Isso porque em uma amostra de 100 perfis de teste com fotos e que realizavam apenas o compartilhamento de conteúdo desde a sua criação, o Facebook identificou apenas 8% destes perfis. Outro exemplo de ausência de verificação ocorreu durante a inserção de imagens de repositórios públicos, já que o Facebook não os reconheceu como falsos.

Desta forma, observa-se que a parte crítica para a geração da *social botnet* é constituída das etapas que consistem na criação das contas no Facebook e a respectiva validação das mesmas. Isso foi observado principalmente porque diferentes soluções para a criação e validação das contas foram abordadas.

5. CONSIDERAÇÕES FINAIS

Neste artigo foi proposta uma arquitetura conceitual para criar uma *social botnet* independente da rede social a ser explorada. Assim, através do estudo e análise das *social botnets*, é possível desenvolver métodos mais eficazes de defesa e combate a essas ameaças.

Em termos de complexidade dos trabalhos relacionados, ela difere-se por ser capaz de proporcionar uma série de atividades a serem realizadas pelos *socialbots* que não foram observadas nas outras *social botnets* analisadas, como a capacidade de clonar as ações de um usuário legítimo.

Esta arquitetura também se mostrou como solução híbrida, que envolve tanto o uso das APIs das redes sociais (algo observado nos trabalhos relacionados) como a utilização de soluções independentes destas APIs, evitando assim que a arquitetura torne-se inviável em função de alguma atualização na API da rede social.

Além disso, a execução da *social botnet* e a implementação do método para facilitar a infiltração dos *socialbots*, também evidência os pontos de atenção que a Desfesa Nacional deve ter em relação ao ciberespaço do Brasil. Isso porque foi observado o quão

vulnerável estão os brasileiros diante da possibilidade de exploração de uma *social botnet*, já que houve interação com perfis com características que facilmente os identificam como falsos, como ausência de fotos e nomes. Acredita-se que isso seja preocupante por ser passível de exploração por ciberataques centrados na manipulação de informações com objetivos políticos, incluindo o propósito de intervir em processos eleitorais.

Uma contribuição esperada desta pesquisa é a disponibilização de um relatório a ser enviado para o Facebook, de modo que eles possam aprimorar a segurança desta rede social, já que durante a execução da *social botnet*, observou-se que algumas ações dos *socialbots* não foram detectadas.

5.1. Trabalhos Futuros

Como trabalhos futuros, propõe-se a inclusão de inteligência artificial (IA) para mapeamento do comportamento de uma determinada nação em uma rede social, bem como interação automática a partir de tópicos interesse com base no perfil (sexo, idade) e nacionalidade.

Além disso, ao integrar a arquitetura proposta com o *chatbot*, que é um software para realizar uma comunicação informal entre um humano e um computador [29], é permitido uma conversa entre os *socialbots* com os usuários legítimos em tempo real, aprimorando ainda mais o comportamento destes robôs sociais e tornando ainda mais complexa a sua identificação no contexto de Guerra Cibernética.

Embora a inclusão de *malware* seja capaz de aprimorar a solução proposta, tal abordagem não foi utilizada por questões éticas. Tal aperfeiçoamento apoiaria a aquisição de contas a serem utilizadas pelos robôs sociais, exigindo uma maior completude da análise realizada neste estudo e das ações a serem realizadas pela área de defesa cibernética para que a detecção e a proteção do ciberespaço nacional.

Um outro ponto que pode ser explorado é a inclusão de mecanismos de detecção de outras *social botnets* a partir da interação dessas com a *social botnet* proposta neste estudo. Desta forma, além de haver um meio de ataque ao inimigo, a evolução desta arquitetura seria capaz de também defender o ciberespaço brasileiro no escopo das redes sociais.

6. REFERÊNCIAS BIBLIOGRÁFICAS

[1] FENACOR. *Risco Cibernético é uma preocupação mundial.* 2018. 4 ago. de 2018. Disponível em: <https://www.fenacor.org.br/noticias/risco-cibernetico-e-uma-preocupacao-mundial>. 2

[2] WENDT, E. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. *Revista Brasileira de Inteligência*, Abril 2011. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIG%C3%8ANCIA-CIBERN%C3%89TICA-E-SEGURAN%C3%87A-VIRTUAL-alguns-aspectos.pdf>. 2

[3] VELANDIA, K. *Quais são as sofisticadas armas cibernéticas da guerra do século 21?* 2017. 5 mar. de 2017. Disponível em:

<https://www.bbc.com/portuguese/internacional-39149203>. 2

[4] FENG, X. X.; PENG, Y.; ZHAO, Y. L. The analysis of botnet based on http protocol. In: *Materials Science and Engineering*. [S.l.]: Trans Tech Publications, 2011. v. 179, p. 575–579. 13 jul. de 2016. 2

[5] COMPAGNO, A. et al. Boten elisa: A novel approach for botnet c&c in online social networks. In: *2015 IEEE Conference on Communications and Network Security (CNS)*. [S.l.: s.n.], 2015. p. 74–82. 2, 3

[6] THOMAS, K.; NICOL, D. M. The koobface botnet and the rise of social malware. In: *2010 5th International Conference on Malicious and Unwanted Software*. [S.l.: s.n.], 2010. p. 63–70. 2, 5

[7] TANNER, B. K. et al. Koobface: The evolution of the social botnet. In: *2010 eCrime Researchers Summit*. [S.l.: s.n.], 2010. p. 1–10. ISSN 2159-1237. 2

[8] GOGA, O.; VENKATADRI, G.; GUMMADI, K. P. *The Doppelgänger Bot Attack: Exploring Identity Impersonation in Online Social Networks*. 2015. 23 jan. de 2018. Disponível em: <https://people.mpi-sws.org/ gummadi/papers/impersonators_IMC2015.pdf>. 2

[9] POSTER, T. W. *Obama Raised Half a Billion Online*. 2016. 3 mai. de 2016. Disponível em: <http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html>. 2

[10] DAPP, F. *Robôs, Redes Sociais e Política no Brasil*. 2017. 20 ago. de 2017. Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>. 2

[11] GOVEIA, F. *Conversas citando Aécio no twitter*. 2014. 15 mai. de 2014. Disponível em: <http://www.labic.net/blog/internet-2/bots-contra-a-sociedade/>. 2

[12] TIMES, T. N. Y. *he Fake Americans Russia Created to Influence the Election*. 2017. 07 set. de 2017. Disponível em: <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html>. 3

[13] BBC. *Para CIA e FBI, 'Rússia teria agido em eleições nos EUA para promover vitória de Trump'*. 2016. 10 dez. de 2016. Disponível em: <https://www.bbc.com/portuguese/brasil-38275572>. 3

[14] FERRARA, E. et al. The rise of social bots. *CoRR*, abs/1407.5225, p. 96–104, 2014. 3

[15] CARNEIRO, J. M. E. A guerra cibernética: uma proposta de elementos para formulação doutrinária no exército brasileiro. *Escola de Comandante e Estado-Maior do Exército*, Outubro 2012. Disponível em: <http://www.eceme.eb.mil.br/images/IMM/producao_cientifica/teses/joao-marinonio-enke-carneiro.pdf>. 3

[16] STATISTA. *Facebook - Statistics & Facts*. 2018. 03 jan. de 2018. Disponível em: <https://www.statista.com/topics/751/facebook/>. 3, 8

[17] DOUGLAS, C. G. A. *Extração de dados em redes sociais usando Python*. 2017. 21 set. de 2017. Disponível em: <http://www.linc.ufpa.br/fabricasistemas/cursoextracao/materiais/3.%20Twitter%20e%20Facebook%20API.pdf>. 3

[18] JIN, L.; JOSHI, J. B. D.; ANWAR, M. Mutual-friend based attacks in social network systems. *Comput. Secur.*, Elsevier Advanced Technology Publications, Oxford, UK, UK, v. 37, p. 15–30, set 2013. ISSN 0167-4048. 8 de ago. de 2016. Disponível em: <http://dx.doi.org/10.1016/j.cose.2013.04.003>. 3

[19] BOSHMAF, Y. et al. Design and analysis of a social botnet. *Comput. Netw.*, v. 57, n. 2, p. 556–578, 2013. 3, 8

[20] ZHANG, J. et al. The rise of social botnets: Attacks and countermeasures. *IEEE Transactions on Dependable and Secure Computing*, PP, n. 99, p. 1–1, 2017. ISSN 1545-5971. 4

[21] HE, Y. et al. Understanding a prospective approach to designing malicious social bots. *Security and Communication Networks*, Security Comm., v. 2, p. 1–18, 2015. 4

[22] ALEX, B. *2015 Brazil Digital Future in Focus*. 2015. 18 mai. de 2015. Disponível em: <https://www.comscore.com/por/Insights/Apresentacoes-e-documentos/2015/2015-Brazil-Digital-Future-in-Focus>. 4, 5

[23] EXAME. *As 200 cidades mais populosas do Brasil*. 2014. 5 jul. de 2017. Disponível em: <https://exame.abril.com.br/brasil/as-200-cidades-mais-populosas-do-brasil/>. 5

[24] IBGE. *Censo Demográfico 2010*. 2010. 2 jan. de 2018. Disponível em: <https://censo2010.ibge.gov.br/nomes/#/ranking>. 5

[25] PROCOB. *Censo Demográfico 2010*. 2015. 23 dez. de 2017. Disponível em: <https://www.procob.com/os-sobrenomes-mais-comuns-do-brasil/>. 5

[26] DATASUS. *Nascidos Vivos - Brasil*. 2015. 30 nov. de 2017. Disponível em: <http://tabnet.datasus.gov.br/cgi/deftohtm.exe?sinasc%2Fcnv%2Fnvuf.def>. 5

[27] PROJECT, S. *SeleniumHQ*. 2012. 4 jun. de 2016. Disponível em: <https://www.seleniumhq.org/docs/>. 9

[28] FERREIRA, M. L. Metodologia para execução de engenaria social automatizada. Rio de Janeiro, p. 60, 2018. 03 mai. de 2018. Disponível em: <s.n>. 10

[29] SHAWAR, B. A.; ATWELL, E. Chatbots: are they really useful? In: *Ldv forum*. [S.l.: s.n.], 2007. v. 22, n. 1, p. 29–49. 12