Proposta para Grupo de Trabalho 2019

GT-Periscope: Uma Ferramenta para Predição de Ataques DDoS por Meio da Identificação Precoce de Botnets

Michele Nogueira Lima

31 de Março de 2019

1. Título

GT-Periscope: Uma Ferramenta para Predição de Ataques DDoS por Meio da Identificação Precoce de Botnets

2. Coordenador Acadêmico MICHELE NOGUEIRA LIMA
Universidade Federal do Paraná
Lattes: http://lattes.cnpq.br/7862253799240671
Email: michele.nogueira@ufpr.br Telefone:
+55 41 3361-3262

3. Assistente de Inovação WAGNER APARECIDO MONTEVERDE
EarlySec – CyberSecurity Segurança Cibernética
LinkedIn: http://lattes.cnpq.br/3683794753942639
Email: wagner.ap.monteverde@gmail.com

Telefone: +55 44 9 9953 9690

4. Tema(s)

Esta proposta de projeto se encaixa na interseção entre os seguintes temas do edital:

- Cibersegurança: sistemas de predição de ataques
- Monitoramento de redes: detecção de padrões atípicos de redes utilizando técnicas de processo de grafos causais

5. Resumo

Este projeto atua na predição de ataques distribuídos de negação de serviço (DDoS), que são um problema em evolução com a Internet das Coisas. Estes ataques visam suspender serviços importantes da rede, resultando em perdas morais e financeiras significativas para as organizações. Nosso objetivo é desenvolver uma ferramenta de detecção de redes de dispositivos infectados por softwares maliciosos (botnets), geradoras de ataques DDoS. Através da detecção das botnets, como um periscópio, é possível indicar de forma precoce a preparação de um ataque e iniciar ações contra ele. A partir da coleta do tráfego da rede em tempo real, a ferramenta extrai estruturas relacionais entre os dispositivos identificados, infere comunidades e determina níveis de causalidade de determinados dispositivos sobre outros, conseguindo identificar os dispositivos de maior influência.

6. Abstract

This project focuses on predicting Distributed Denial of Service (DDoS) attacks, which are an evolving problem with the Internet of Things. These attacks aim at denying important network services, resulting in significant moral and financial losses for organizations. Our goal is to develop a network detection tool for detecting networks of devices infected by malicious software (botnets) that generate DDoS attacks. By detecting botnets, as a periscope, it is possible to early indicate the preparation of an attack and initiate actions against it. From the collection of real-time network traffic, the tool extracts relational structures between the identified devices, infers communities and determines causality levels of certain devices over others, managing to identify the most influential devices.

7. Parcerias

- **Universidade Carnegie Mellon, EUA** – a equipe do Prof. Dr. José M.F. Moura irá nos auxiliará na evolução e aperfeiçoamento dos algoritmos de análise de casualidade usando a técnica de processamento de sinais em grafos.
- **Instituto Federal de Catarinense (IFC)** – a equipe do instituto, liderada pelo mestre Mateus Pelloso, irá auxiliar na construção do ambiente de teste e nos testes da ferramenta.
- **Start-up EarlySec** – na liderança de Wagner Monteverde, a start-up irá auxiliar na construção e acompanhamento do modelo de negócio e transferência tecnológica.
- **Universidade Federal do Paraná** – a equipe de professores na UFPR, instituição proponente desta proposta, é composta pela Profa. Dra. Michele Nogueira Lima (coordenadora da proposta) e pelo Prof. Dr. Aldri Luiz dos Santos.

8. Definição do problema e do público impactado

O paradigma da Internet das Coisas (*Internet of Things* -- IoT) vem se expandindo e oferecendo serviços relevantes para as pessoas. A IoT representa uma vasta gama de dispositivos (coisas) capazes de se conectar à Internet para prover serviços inteligentes por meio da troca de uma grande quantidade de dados em tempo real. A popularização no uso desses dispositivos, ex. computadores de bordo de um veículo, *smartphones*, sistemas embarcados em refrigeradores, dispositivos vestíveis e outros, vem impulsionando a concepção do conceito da *Internet of Everything* (IoE), em que além da relação entre as coisas, também considera as relações entre as pessoas, processos e dados. Por meio desta relação, a IoE explora a íntima relação entre estas entidades, podendo prover serviços ainda mais relevantes para as pessoas e gerando oportunidades econômicas sem precedentes para empresas, indivíduos e países. Entretanto, a concretização do conceito da IoE está intrinsecamente atrelada à resolução de questões resultantes da própria IoT, sendo uma das principais questões a segurança cibernética, particularmente, a confiabilidade dos serviços.

Os ataques distribuídos de negação de serviço (DDoS) são uma grande ameaça de segurança cibernética que comprometem o provimento de serviços na Internet, podendo resultar em perdas financeiras e morais significativas para as empresas e organizações ao interromper a disponibilidade de seus serviços. A indisponibilidade dos serviços é um problema crítico, pois falhas nesse contexto podem mesmo colocar em risco a vida de pessoas, diante do crescente uso da Internet no suporte a aplicações críticas. De acordo com o estudo realizado por Sachdeva et al. [1][2], a indisponibilidade de serviços na rede causa em média prejuízos financeiros maiores que US$ 30 milhões por ano. Esses ataques vêm avançando em quantidade, volume e técnicas, principalmente com o advento das chamadas botnets móveis, isto é, redes formadas por dispositivos móveis ou portáteis (que são a base da IoT) infectados. No Brasil, o CERT.br[1] ressaltou um aumento de 138% na quantidade de ataques DDoS em 2016 [3]. No geral, tais ataques geram volumes de dados inesperados, chegando a Terabytes, a fim de sobrecarregar os recursos nos servidores ou enlaces da rede empregando técnicas cada vez mais sofisticadas. Com a IoT, os atacantes exploram os recursos disponíveis nos sistemas computacionais, a largura de banda e a diversidade resultante da distribuição geográfica das coisas. Outro aspecto é a maior abrangência geográfica das botnets móveis, resultante da natureza que dos dispositivos que as compõem (dispositivos móveis/portáteis e heterogêneos) e que são facilmente infectados devido às suas vulnerabilidades de segurança.

Com a sofisticação contínua e rápida das técnicas utilizadas por esses ataques, os sistemas de detecção tradicionais se limitam a ataques DDoS em estágios avançados ou quando o alvo já está comprometido. Além disso, esses sistemas possuem limitações sérias ao tratar ataques DDoS desconhecidos (*zero-day* ou *unknown attacks*), resultando em altas taxas de falso negativo. No geral, as abordagens embasam-se em técnicas de mineração de dados, modelos estatísticos e análise do perfil do tráfego da rede, redes neurais e modelos de Markov. Por exemplo, a ferramenta SeVen, resultante do GT-ACTIONS/RNP (2014-2016), tratou ataques DDoS com o foco na camada de aplicação tomando como base a elaboração do perfil de tráfego da rede associadas à aplicação de telefonia IP. Entretanto, em geral, os sistemas tradicionais ainda dependem de treinamentos prévios, muitos deles *offline*, ou do conhecimento sobre o comportamento dos ataques. Isto concentra a atuação dessas soluções aos ataques previamente conhecidos ou quando o ataque já está ocorrendo, o que pode ser tarde demais para se tomar uma ação e coibir o início do ataque conforme demonstra nosso

[1] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). https://www.cert.br/.

modelo e resultados descritos em [4]. Assim, a predição não supervisionada torna-se crucial para evitar custos e perdas resultantes de ataques DDoS [5][6][7], ainda mais os ataques desconhecidos potencializados pelo uso de dispositivos da IoT.

Neste contexto, é importante salientar que as *botnets* desempenham grande parte do trabalho na preparação e geração dos ataques DDoS, pois nelas um *botmaster* coordena e comanda remotamente os dispositivos infectados (bots/robôs), sem o conhecimento e consentimento dos seus proprietários, indicando quem deve ser o alvo do ataque e o momento de início dos ataques. Uma botnet é um conjunto destes dispositivos (fixos ou móveis) infectados e ela é uma das grandes preocupações do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Ipê e de várias agências de segurança no mundo inteiro, diante do advento da IoT. Os dispositivos da IoT são facilmente infectados e seus protocolos, como o CoAP, são suscetíveis ao mascaramento IP *(IP spoofing)*, uma das técnicas utilizadas na geração de ataques DDoS. No último relatório anual de incidentes de segurança na Rede Brasileira de Ensino e Pesquisa disponibilizado pelo CAIS, ressalta-se que os incidentes de segurança da informação relacionados às botnets continuaram sendo a principal ocorrência na rede acadêmica brasileira. As redes comercial e acadêmica brasileiras, por exemplo, foram um dos principais alvos da botnet coordenada por dispositivos infectados com o malware BASHLINE em 2017. Ainda na rede acadêmica brasileira, foram registradas cerca de 20 mil notificações de dispositivos realizando atividades maliciosas típicas de dispositivos infectados por bots ou de comando e controle (C&C). O Brasil é visto diariamente na lista dos 10 países com mais IPs suspeitos de participarem de botnets. A

Figura 1 apresenta estatísticas referentes ao dia 29 de Março de 2019, extraídas do site *botnet-tracker blogspot*[2]. O Brasil nesse dia, assim como em vários outros, se encontra na sexta posição entre os países com mais IPs suspeitos de participarem de botnets.

Figura 1 – Dez países com mais IPs suspeitos como bots no dia 29 de Março de 2019

1	China	2212
2	United States	1772
3	Viet Nam	732
4	France	717
5	Russian Federation	700
6	Brazil	644
7	India	559
8	Indonesia	520
9	South Korea	280
10	Thailand	230

Diante disso, percebemos a importância em detectar as botnets e identificar os bots para a rede acadêmica e de pesquisa brasileira, ainda mais observando essas como fontes geradoras de ataques DDoS. Advogamos que quão cedo seja a detecção das botnets e a identificação dos bots, maiores são as chances de evitar o início do ataque em si e os danos potenciais causados por ele. Assim, são necessários métodos online capazes de detectar botnets e identificar os bots antes do lançamento do ataque DDoS e da exaustão dos recursos da vítima, visando manter a disponibilidade da rede e o funcionamento dos serviços oferecidos por empresas e organização na Internet. Por métodos online, entendemos aqueles que trabalham de forma contínua e embasados em algoritmos com custo computacional, na terminologia big-*O*, de *O(1)*, ou seja, dada uma entrada, a saída é imediata. A detecção de botnets tem por objetivo verificar a existência de atividade dos bots na rede, mas não necessariamente identifica quais dispositivos da rede são os bots. A identificação dos bots tem como objetivo apontar claramente os bots, isto é, discriminar quais dispositivos estão infectados e com potencial de atacar a rede. A detecção da botnet é o primeiro

[2] http://botnet-tracker.blogspot.com. Último acesso: 29 de Março de 2019.

passo na identificação dos bots; a identificação dos bots é um segundo passo importante para ações que coíbam precocemente os ataques DDoS.

9. Proposta de solução do problema com destaque para a visão de negócio e a visão do produto

Este projeto tem como objetivo desenvolver e transferir a tecnologia de uma ferramenta de predição de ataques DDoS através da detecção de botnets geradoras desses ataques e da identificação dos bots, considerando sua relação com a Internet das Coisas. Através da detecção das botnets, como um periscópio, é possível indicar de forma precoce a preparação de um ataque e iniciar ações contra ele. Esta ferramenta será desenvolvida ao longo de 12 meses e estará fundamentada na(s): (i) metodologia de Ciência de Segurança; (ii) experiência teórica e prática da equipe na proposição de soluções de predição[3]; (iii) atividades de pesquisa do projeto "PROA: Predição de Ataques DDoS na IoT", programa CNPq/Universal; (iv) experiência da start-up em transferência tecnológica e desenvolvimento de sistemas de predição de ataques; e (v) cooperação técnica da equipe com pesquisadores da Universidade Carnegie Mellon (CMU), EUA, no tema (o cooperação se restringe a questões técnicas e não de negócio).

A ferramenta proposta seguirá três etapas integradas de operação: (a) medições e preparação dos dados para análise em tempo real; (b) predição dos ataques através da detecção da botnet e identificação dos bots; e (c) emissão de alertas e filtragem. O sistema recebe como entrada dados brutos do tráfego da rede, filtra esses dados e compõe séries temporais correspondentes a períodos (janelas) de medições. Para cada janela, as séries temporais sevem de entrada para o cálculo de uma matriz de influências entre os dispositivos identificados, a qual representa relações de causalidade e suporta a identificação de comunidades. O cálculo é realizado seguindo a técnica de processo causal em grafos (*Causal Graph Process* - CGP) desenvolvido pela equipe da Universidade Carnegie Mellon, parceiros internacionais desta proposta, e adaptado por nós para o uso na detecção de botnets e identificação de bots. Com base na análise da matriz de influências, a ferramenta emite um alerta para o administrador da rede, podendo enviar as informações dos dispositivos identificados como bots ou iniciar um sistema de filtragem de pacotes provenientes dos dispositivos identificados como bots. A seguir apresentamos detalhes de cada uma dessas etapas.

a) Medições e preparação dos dados para análise em tempo real

Esta etapa engloba a coleta do fluxo de dados da rede, a definição do tamanho da janela de tempo e a filtragem dos dados (extração de característica). Assume-se o funcionamento em modo promíscuo para a interface de rede do hardware em que a ferramenta estiver sendo executada. A coleta do fluxo de dados da rede ocorre continuamente através de ferramentas de monitoramento de rede, tais como (mas não exclusivas) tshark e tcpdump. O fluxo de dados da rede é registrando em um arquivo em memória que segue o formato de uma série temporal e contém a indicação do momento da coleta do dado e valor observado. Esse arquivo contém dados observados dos dispositivos detectados na captura por um determinado período de tempo (chamado do janela). As análises ocorrerão sobre janelas de coleta de tamanho T. O tamanho da janela de dados deve ser definido pelo administrador da rede por tempo, por exemplo, T segundos (ou minutos), ou por quantidade de amostras, por exemplo, quantidade de pacotes coletados. Uma vez definido se a janela será por tempo ou por quantidade de elementos, o seu tamanho poderá ser auto-ajustável. O intervalo entre as observações

[3] O Centro de Ciência de Segurança Cibernética (CCSC)/UFPR possui duas dissertações defendidas sobre as quais se embasa esta proposta de projeto nos temas de predição de ataques de negação de serviço distribuído e detecção de botnets.

também é definido pelo administrador da rede e pode oferecer maior ou menor precisão na classificação de botnets geradoras de ataques DDoS. Os dados observados e registrados nas séries temporais serão, em um primeiro momento, a soma da quantidade de pacotes ou a soma do tamanho dos pacotes por intervalo, porém uma melhor definição desta característica precisará ser realizada durante a execução do projeto. Cada janela oferecerá uma série temporal como entrada para o algoritmo de cálculo de influências, que resulta em uma matriz N x N, em que N corresponde ao número de dispositivos identificados na série temporal de entrada. Os valores indexados na matriz correspondem à magnitude de interrelações entre os dispositivos. Assumiremos em um primeiro momento que a similaridade na magnitude de interrelações entre os dispositivos representa também a coordenação entre eles.

b) Predição dos ataques através da detecção da botnet e identificação dos bots

Esta fase de operação da ferramenta se apoia no método de Processo de Grafos Causais (*Causal Graph Process* - CGP) que é descrito como um processo autorregressivo multivariado atuando sobre uma série temporal no qual seus coeficientes são filtros de grafos. Ou seja, através de autorregressão e cálculos de coeficientes de autocorrelação, o método evidencia as interrelações entre variáveis. Neste projeto, as variáveis representam os dispositivos da rede, a partir de uma única entrada (a série temporal). Diferente dos processos convencionais de autorregressão, o método CGP não assume a propriedade de Markov nas observações das variáveis nas séries temporais. O CGP assume que todas as variáveis são dependentes. No contexto abordado, isto significa que o conjunto de amostras da série temporal de entrada no tempo *t* é influenciado de alguma forma pelo conjunto de sinais matriz de entrada no tempo *t-1*.

Com base nos valores de entrada, considerando que as observações das variáveis nas séries temporais têm influência umas sobre as outras e sobre si mesmas, o CGP utiliza o método dos mínimos quadrados e encontra as funções que apresentam o menor erro residual das autoregressões. O CGP calcula a autoregressão de ordem 2 (ou lag-2) nas observações dos dispositivos, ou seja, ele utiliza duas cópias atrasadas em uma e duas amostras respectivamente das observações de cada dispositivo para encontrar as funções que representam o comportamento observado. Ao final, os valores dos coeficientes estimados pelas funções após um número de iterações são utilizados nas estimativas da autocorrelação entre essas variáveis. Essas estimativas são calculadas utilizando o cálculo da convolução entre os modelos encontrados das autoregressões resultando em uma matriz de interrelações dos dispositivos e possibilitando a inferência da causalidade entre elas.

Dentro do contexto deste projeto, a matriz estimada indica as influências entre os dispositivos da rede identificados em uma janela de tempo. Logo, os dispositivos que apresentem maior relação positiva de influência sobre os demais dispositivos apontam os bots. Seguindo a mesma lógica, os dispositivos que apresentem maior relação negativa de influência sobre os demais dispositivos podem indicar as vítimas. Desta forma, segue-se que quanto maior a similaridade na magnitude de relação entre os dispositivos, maior a coordenação entre eles. Quanto maior sua coordenação, maiores as chances de fazerem parte de uma mesma botnet. Utilizando limiares nas análises, essas magnitudes indicam claramente os bots da botnet. Desta forma, este método consegue detectar a botnet e os bots, tal como objetivamos.

c) Emissão de alertas e filtragem

De posse da matriz de influências, é possível identificar a lista de bots, caso uma botnet seja detectada em uma determinada janela de tempo. Em caso de detecção, a lista pode ser enviada ao administrador da rede através de um alerta ou iniciar um processo de filtragem de pacotes provenientes dos dispositivos identificados como bots.

Nesta última situação, os dispositivos ficariam em quarentena e seus fluxos de rede seriam monitorados. Uma visualização gráfica da lista de bots e suas relações também poderão ser apresentadas ao administrador da rede, ex. Figuras 2 e 3.

Exemplos de uso

Para fins de ilustração do uso do método na detecção de botnets e identificação de bots, as Figuras 2 e 3 indicam resultados alcançados por nós utilizando bases de dados *offline* contendo tráfegos de rede reais com e sem a ocorrência de ataques DDoS. A Figura 2 mostra os resultados de um cenário ocorrido na Universidade da República Tcheca (CTU) com dispositivos infectados (bots) e que após a infecção manual dos mesmos, os bots são coordenados para gerar um ataque DDoS contra a vítima. A figura mostra os resultados para o período de dois minutos totais, considerando duas situações: com limiar aplicado aos resultados na matriz de inferências e sem limiar. Quando utilizado um limiar na análise da matriz de inferências, o método foi capaz de detectar a existência da botnet e identificar apenas os bots. Quando não foi utilizado um limiar, o método indicou a existência da botnet, além de também indicar a vítima e um dispositivo classificado como "outro".

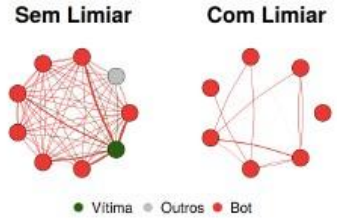

Figura 2 – Exemplo da detecção da botnet pelo método

A Figura 3 mostra os resultados de um cenário em que tínhamos inicialmente a certeza de não possuir uma botnet e foi utilizado como prova de conceito. Neste cenário, nenhum dos dispositivos identificados na rede foram classificados como bots, da mesma forma, nenhuma botnet foi detectada, conforme esperado. Na figura, todos os dispositivos são classificados como "outros" uma vez que não são bots, nem vítima.

Figura 3 – Prova de conceito

Visões de negócio e de produto

No contexto cada vez mais sofisticado e dinâmico com a popularização da IoT, as empresas e organizações necessitam de ferramentas de segurança cibernética que acompanhem essa dinamicidade e tenham flexibilidade nas suas configurações. Cada vez, as ferramentas de detecção de ataques DDoS e botnets precisam ser efetivas e se adaptarem rapidamente contra os efeitos inesperados de ataques DDoS conhecidos e também desconhecidos. O que se oferece com este projeto é o desenvolvimento de uma ferramenta fortemente embasada em resultados científicos, que se demonstraram eficientes para o propósito, e com um grande potencial de negócio e evolução ao longo dos anos. Diferente de outras ferramentas, esta toma como entrada dados simples e básicos do tráfego da rede (ex. tamanho do pacote, origem e destino, e outros). Além disso, ela não requer o conhecimento prévio do padrão de tráfego do ataque ou mesmo informações sobre o seu funcionamento.

Esta ferramenta poderá ser comercializada para organizações públicas e privadas. Uma visão de modelo de negócio passível de ser seguido pela start-up é a comercialização da ferramenta por um determinado valor e associar esta venda a contratos de atualizações periódicas, em que poderia se ajustar o tipo de características da rede a serem coletadas dependendo de novas visões de ataques DDoS a serem conhecidos. Em paralelo, a start-up pode comercializar o serviço de detecção de botnets a partir da análise do tráfego da rede das organizações. Neste caso, a ferramenta estaria disponível em uma arquitetura de computação em nuvem e seria necessária a construção de uma interface para receber os dados do tráfego da rede da organização

contratante (cabe ressaltar que a construção desta interface não está sendo considerada no escopo deste projeto).

10. Ambiente para validação da solução proposta

A fim de avaliar a ferramenta proposta, serão realizados testes na infraestrutura física de rede existente no Centro de Ciência de Segurança Computacional (CCSC) da UFPR, incluindo o uso de equipamentos de IoT, tais como sensores de ambiente, sensores médicos e outros. Em um primeiro momento, consideraremos testes de validação da implementação seguindo (i) individualmente cada fase de operação da ferramenta; e (ii) a execução integrada das três fases de operação. Em um segundo momento, testaremos o funcionamento da ferramenta com dados de tráfego da rede extraídos previamente (chamados de dados *offline*). Como exemplo de dados para esta validação estão o dataset "DDoS Attack 2007" Dataset do *Center for Applied Internet Data Analysis* (CAIDA), EUA, conseguidos graças à parceria com a CMU. Em um terceiro e último momento, a validação empregará a coleta de dados da rede em tempo real. Para esta última etapa, os comportamentos de botnets serão emulados em um ambiente controlado e construído para o projeto pela equipe do IFC e também será utilizada uma infraestrutura remota da RNP, tal como FIBRE ou PlanetLab para testes.

A validação da ferramenta ocorrerá em dois tipos de ambientes, um local (controlado) e outro remoto. Para o ambiente local será desenvolvida uma rede de dados IoT implementada em um simulador/emulador de redes e com a integração de dispositivos reais existentes no CCSC, a fim de empregar conjuntos de dados controlados com fluxo de rede contendo tráfegos de botnet e de serviços da rede. Durante a simulação/emulação do fluxo da rede os dados serão coletados e analisados por meio de séries temporais geradas a partir das características (*features*) definidas durante a pesquisa. Dessa forma, a solução proposta identificará as atividades da botnet, bem como dos respectivos bots no tráfego da rede, predizendo os ataques. A simulação/emulação permitirá analisar diferentes cenários e avaliar o desempenho da ferramenta em cada um deles, antes de levar validar a ferramenta no ambiente remoto.

As implementações do projeto priorizarão a utilização de software e ferramentas livres (ex. shell script, R, entre outros), com o objetivo de possibilitar a reprodução da pesquisa em e pelas instituições parceiras na construção desta solução. Para o desenvolvimento do ambiente de validação local, é necessário 1 (um) computador e um bolsista classificado como Assistente de desenvolvimento 3. Todas as implementações serão documentadas e entregues junto à ferramenta ao final do projeto, assim como serão criados manuais de uso da ferramenta.

11. Cronograma de marcos

A seguir é apresentado o cronograma de marcos para o projeto proposto, considerando o período de 1 ano (de 01/06/2019 a 31/05/2020). Os prazos e as atividades a serem realizadas são descritos a seguir. É importante ressaltar que, além desses marcos e atividades, a equipe está ciente que precisará realizar em paralelo as demais entregas definidas no item 9 do edital seguindo os seus prazos.

1. **Revisita do Estado da Arte:** revisitar o estado da arte sobre técnicas de detecção de botnets geradoras de DDoS e técnicas de geração de comunidades existentes e possam ser aplicadas ao projeto. (01/06/2019 a 30/06/2019)

2. **Relatório de Prospecção:** relatório contendo o estado da arte das tecnologias envolvidas e um comparativo entre elas, bem como uma análise das soluções de mercados concorrentes. (Até 01/07/2019)

3. **Relatório da Visão de Negócios e Produto:** relatório descrevendo as visões de negócio e produto, contendo arquitetura para o produto mínimo viável, incluindo requisitos de hardware e software. (Até 30/08/2019)

4. **Levantamento de Requisitos e Especificação de Software da Ferramenta:** os requisitos da ferramenta serão levantados e documentados, assim como serão especificados os softwares e as características a serem seguidos. (01/07/2019 a 31/08/2019)

5. **Definição das Características do Fluxo da Rede e Ajuste do Método Base:** serão definidas as características do fluxo da rede a serem extraídas e que servirão de base para a construção das séries temporais. No momento, o método base utiliza o tamanho dos pacotes como característica base. Esta característica foi aplicada, por exemplo, para a obtenção dos resultados preliminares apresentados na Seção 9. Entretanto, nesta atividade definiremos as características a serem utilizadas na ferramenta e, caso necessário, ajustar o método. (01/09/2019 a 31/10/2019)

6. **Implementação da Ferramenta:** desenvolvimento propriamente dito da ferramenta seguindo os requisitos e especificações (01/08/2019 a 30/11/2019)

7. **Preparação dos Ambientes, Local e Remoto, de Validação:** instalação dos softwares necessários para a validação, treinamento e atualização da equipe sobre o uso dos softwares e dos ambientes de validação, busca por datasets com ataques, emulação de botnets, e outros. (01/08/2019 a 31/12/2019)

8. **Testes e Validação:** testes de validação da implementação da ferramenta, considerando individualmente cada fase de operação; e a execução integrada das três fases de operação. Após os primeiros testes, serão realizados testes para validação de funcionamento da ferramenta com dados de tráfego da rede extraídos previamente (dados *offline*). Por fim, a validação considerará a coleta de dados da rede em tempo real no ambiente local e no ambiente remoto da RNP. (01/12/2019 a 31/05/2020)

9. **Ajustes na Implementação da Ferramenta após Testes:** desenvolvimento de ajustes necessários na ferramenta a partir da análise dos primeiros resultados de testes (01/01/2020 a 31/05/2020)

10. **Escrita dos Relatórios de Atividades Mensais:** relatório mensal contendo uma breve descrição das atividades realizadas por cada membro contratado da equipe.

12. Recursos financeiros

12.2. Infraestrutura

12.2.1. Créditos no serviço compute@RNP

Descrição do Recurso (Máquina virtual ou Armazenamento)	**S.O./Distr** (Linux ou Windows)	**Qtde. do recurso**	**Mês Inicial**	**Mês Final**	**Qtd. Meses**	**Valor em R$ por mês**	**Valor em R$ total**
Máquina virtual	Linux	1	12/2019	05/2020	6	550,78	3.304,68
Máquina virtual	Linux	1	11/2019	11/2019	1	275,39	275,39
						Subtotal	3.580,07

12.2.2. Equipamentos

Descrição	Instituição de Destino	Qtd.	Valor em R$ estimado
Desktop Modelo i7 (Core i7 - 8GB - 500 GB) + Kit teclado e mouse com fio	IFC	1	6.000,00
Notebook 14” Modelo i5 (Core i5 - 8GB - SSD 256GB)	UFPR	2	11.800,00
Monitor	UFPR	5	3.560,00
		Subtotal	R$ 21.360,00

13. Referências

[1] Mansfield-Devine, S. (2015). The growth and evolution of DDoS. Network Security, 2015(10):13–20.

[2] Sachdeva, M., Singh, G., Kumar, K. e Singh, K. (2010). DDoS Incidents and their Impact: A Review. The International Arab Journal of Information Technology, Vol. 7, No. 1, pages 14-20, January 2010.

[3] CERT.br registra aumento de ataques de negação de serviço em 2016. http://www.nic.br/noticia/releases/cert-br-registra-aumento-de-ataques-de-negacao-deservico-em-2016/. [Último acesso em Março/2019].

[4] Santos, A. A., Nogueira, M. e Moura, J. M. (2017). A stochastic adaptive model to explore mobile botnet dynamics. IEEE Communications Letters, 21(4):753–756.

[5] Holgado, P., Villagra, V. A. e Vazquez, L. (2017). Real-time multistep attack prediction based on hidden markov models. IEEE Transactions on Dependable and Secure Computing.

[6] Kwon, D., Kim, H., An, D. e Ju, H. (2017). DDoS attack volume forecasting using a statistical approach. IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pages 1083–1086. IEEE.

[7] Nezhad, S. M. T., Nazari, M. e Gharavol, E. A. (2016). A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks. IEEE Communications Letters, 20(4).