Proposta para Fase 2 do Programa de Pesquisa e Desenvolvimento Serviços Avançados - Grupos de Trabalho (GTs) 2020

GT-Periscope: Uma Ferramenta para Predição de Ataques por Meio da Identificação de Bots e Vulnerabilidade de Segurança (Fase 2)

Wagner Aparecido Monteverde

23 de Abril de 2020

1. Título

GT-Periscope: Uma Ferramenta para Predição de Ataques por Meio da Identificação de Bots e Vulnerabilidades de Segurança (Fase 2)

2. Coordenador Geral

WAGNER APARECIDO MONTEVERDE
EarlySec – CyberSecurity Segurança Cibernética
LinkedIn: https://www.linkedin.com/in/wagnermonteverde

Email: wagner@earlysec.com
Telefone: +55 44 9 9953-9690

3. Assistente de Inovação

Marlon Fernandes Antonio
EarlySec – CyberSecurity Segurança Cibernética
LinkedIn: linkedin.com/in/marlon-fernandes-antonio-a343ba126

Email: marlonfa@gmail.com
Telefone: +55 18 9 9653-2529

4. Resumo

Este projeto foca no avanço tecnológico e comercial da ferramenta Sherlock-X, o Mínimo Produto Viável (MVP) resultante da fase 1 do GT-Periscope. Seguindo a metodologia de Steven Blank e com base em entrevistas, alcançou-se na fase 1 maturidade na definição dos clientes, no entendimento de suas necessidades e, consequentemente, na delimitação de foco de atuação da ferramenta proposta. Assim, a ferramenta Sherlock-X é capaz de identificar vulnerabilidades de segurança e dispositivos maliciosos (bots) na rede, tal como suas interações, contribuindo para a predição de ataques distribuídos de negação de serviço (DDoS) e outros ataques. Com base neste MVP, o objetivo maior nesta fase 2 do GT-Periscope versa o avanço de seus testes no ambiente operacional do *Early Adopter* e PoP-PR, e o seu incremento com o desenvolvimento da análise de vulnerabilidades da rede interna e a correlação entre vulnerabilidades e entre estas e os dispositivos apontados como bots. Além disso, trabalharemos para definir a melhor abordagem de distribuição e coleta de tráfego de rede pelos sensores e na implantação da ferramenta na plataforma NasNuvens da RNP para comercialização. Em paralelo ao desenvolvimento técnico, uma estratégia de comercialização e *marketing* será desenvolvida e aplicada.

5. Abstract

This project focuses on the technological and commercial advancement of Sherlock-X, the Minimum Viable Product (MVP) resulting from the phase 1 of GT-Perisope. Following Steven Blank's methodology and based on interviews, we have reached a maturity in phase 1 related to the customers definition, the understanding of their main needs and, then, the delimitation of the focus of the proposed tool. Thus, the Sherlock-X tool is able to identify security vulnerabilities and malicious devices (bots) on the network, as well as their interactions, contributing to the prediction of Distributed Denial of Service (DDoS) attacks and other attacks. Based on this MVP, the main goal in this phase 2 of GT-Periscope lies in advancing the MVP tests in the operational environment of an *Early Adopter* and PoP-PR, and improving it with the development of internal vulnerability analysis, the correlation between vulnerabilities and between devices pointed out as bots. Furthermore, we will work to define the best approach for the distribution and collection of network traffic by sensors and in the inclusion of the Sherlock-X tool in the RNP's NasNuvens platform for commercialization. In parallel with technical development, a commercialization and marketing strategy will be developed and applied.

6. Link do vídeo-pitch https://youtu.be/e6BXA_2ZLyo

7. Parcerias e respectivas contrapartidas

Este projeto será executado em parceria com o Centro de Ciência de Segurança Computacional (CCSC) da Universidade Federal do Paraná (UFPR) sob a liderança da

Profa. Michele Nogueira. O grupo de pesquisa CCSC continuará dando apoio à inovação e ao desenvolvimento tecnológico deste projeto através de avanços científicos e tecnológicos, embasados em princípios acadêmicos e em conhecimento de anos de experiência do grupo, consolidando assim a transferência tecnológica para a StartUp. Ainda, o grupo assistirá este projeto com a disponibilização da infraestrutura física para desenvolvimento e testes, tal como a comunicação e o relacionamento com o ponto de presença da RNP no Paraná (PoP-PR). Em reuniões com o coordenador técnico do PoP-PR, Christian Lyra, verificamos a viabilidade de testes da ferramenta na infraestrutura do PoP-PR, o qual nos ofereceu ajuda e apoio com os mesmos, além do acesso aos dados do tráfego da rede. Também, como contrapartida da StartUp EarlySec, a empresa coloca à disposição desta fase 2 do GT-Periscope um valor de US$ 15,000.00 (quinze mil dólares) em créditos na nuvem da Amazon Web Service (AWS) para uso em atividades do projeto. Além disso, o salário do assistente de inovação e de um assistente de desenvolvimento, nível 2, será custeado pela Start Up. Como este projeto é uma continuidade da fase 1, a equipe foi consolidada com membros que possam auxiliar ativamente nas principais atividades da fase 2 que são a evolução de desenvolvimento do MVP, definição dos sensores de tráfego, análise de vulnerabilidades da rede interna e mecanismos de correlação de vulnerabilidades, e a adequação da ferramenta para sua oferta na plataforma NasNuvens da RNP. Vale ainda mencionar que a StartUp EarlySec presta suporte ao sistema de resposta a incidentes do CAIS, desenvolveu uma nova versão deste sistema e também desenvolveu um outro sistema de segurança para o CAIS. Ressaltamos que apesar da equipe não ter instituições de diferentes estados da federação, esta é a equipe que consideramos capacitada para a execução do GT (fase 2), já com experiência em sua interação a partir das atividades desenvolvidas na fase 1 do GT-Periscope.

8. Descrição da evolução do MVP com destaque para a entrada na loja virtual

O mercado de segurança de redes e da informação está em crescimento no Brasil e no mundo impulsionado pelo Marco Civil da Internet e as leis de privacidade. Na Europa o Regulamento Geral sobre a Proteção de Dados (GDPR) e no Brasil a Lei Geral de Proteção dos Dados (LGPD) têm sido grandes impulsionadores de venda para produtos e serviços de Segurança de Redes e da Informação. Grandes empresas geralmente possuem setores responsáveis pela segurança de sistemas e da informação, porém elas focam em ações reativas contra ataques e pagam um alto preço para aquisição de ferramentas e contratação de profissional qualificado. Além disso, ressalta-se que esta é a realidade apenas parte dessas empresas.

Existe uma grande quantidade de empresas no Brasil que não possui acesso a controles de Segurança ou quando possuem focam em soluções reativas de detecção de ataques ou controle de acesso. Com a entrada em vigor da LGPD no Brasil estas empresas terão de implementar controles de segurança, de preferência pró-ativos, para se adequarem à nova lei. Utilizando a metodologia de Steven Blank, que toma como base inúmeras entrevistas com potenciais clientes e pessoas de influência na área, constatamos a ausência de acesso a serviços de segurança cibernética pelos seguintes motivos: *(i)* falta de mão-de-obra qualificada; *(ii)* alto custo de mão-de-obra qualificada; *(iii)* alto custo de soluções de segurança disponíveis no mercado (sendo a grande maioria soluções estrangeiras e reativas); *(iv)* soluções de complexa operação e; *(v)* negligência e desconhecimento de diretores e acionistas sobre o tema.

Desta forma através das entrevistas realizadas na Fase 1 do GT-Periscope, verificou-se que empresas de pequeno e médio porte em diferentes setores (ex. provedores de serviço e de acesso, seguradoras e outros) com alguma estrutura de TI são potenciais clientes para a solução desenvolvida, que visa a automatização dos serviços de Segurança da rede, por meio de uma plataforma de serviço acessível e com uma abordagem pró-ativa de predição e proteção. Este é um mercado ainda pouco explorado. Segundo os dados do SEBRAE [1], existem cerca de 6,4 milhões de estabelecimentos no Brasil, sendo 99% deles empresas de pequeno porte, se mostrando um vasto mercado a ser explorado.

Empresas de médio e pequeno porte, como apontado nas entrevistas realizadas, não possuem um nível de maturidade em Segurança de Redes e da Informação pelos motivos apresentados no segundo parágrafo desta proposta. Por conta disso, essas empresas têm dificuldade em gerir seus recursos computacionais, não têm conhecimento sobre suas próprias falhas e vulnerabilidades de segurança (internas e externas), não conseguem identificar e muito menos predizer atividade maliciosa em sua rede e dispositivos, nem se proteger de possíveis ataques. Como exemplo recente, uma reportagem de 15 de Abril de 2020 do blog NetLab360.com alerta os usuários de serviço de Internet por por fibra sobre a possibilidade de seus roteadores serem bots (ou seja, estarem infectados) e participarem da Moobot, uma nova família de botnets evoluída da conhecida botnet Mirai [2]. Existe um alto custo de casos de invasões perdas de dados paralisação de operação devido a incidentes cibernéticos.

O cenário atual nas empresas é de grande desconhecimento sobre sua própria situação. Isto se refletiu na entrevista que tivemos com profissionais de TI de uma grande empresa de telecomunicação provedora de acesso à Internet em todo Brasil. Os profissionais afirmaram suspeitar das vulnerabilidades existentes em dispositivos de sua infraestrutura, principalmente, dispositivos legados devido à aquisições e à evolução do seu parque tecnológico, porém eles não têm o mapeamento dessas vulnerabilidades e necessitam de uma ferramenta automatizada para realizar este mapeamento e análise continuamente. Esses dispositivos com vulnerabilidades podem inclusive participar de botnets, sem o conhecimento desses profissionais. Portanto, o produto gerado pela fase 1 e, esperançosamente, pela fase 2 deste projeto oferecerá para essas empresas: *(i)* a gestão contínua e automatizada de vulnerabilidades de segurança em seus recursos computacionais; *(ii)* a identificação de dispositivos infectados (bots) e a predição de atividade maliciosa na rede da empresa (e seus clientes, por exemplo, no caso de provedores de acesso); *(iii)* uma ferramenta para lidar com incidentes através do gerenciamento integrado; *(iv)* a abstração sobre a complexidade técnica de predição e identificação de problema de segurança, suprindo a carência de mão-de-obra especializada; (v) a medição do risco cibernético.

Hoje, existem plataformas comerciais que ajudam empresas a detectar problemas de segurança, entre elas estão os SIEM e SOAR, porém estas soluções são reativas, ou seja, só apontam o problema de segurança e ataque quando este já está ocorrendo, são de complexa operação, exigindo mão-de-obra qualificada, além de ter um preço pouco acessível para empresas de pequeno e médio porte. Plataformas integradas e de inteligência contra ameaças existem, porém são de fabricantes internacionais, sendo custosas para o cliente brasileiro. Essas ferramentas possuem os seguintes pontos negativos: *(i)* dificuldade de operação, exigindo mão-de-obra especializada; *(ii)* preço inacessível para maioria das empresas de médio e pequeno porte; *(iii)* ausência de

parecer integrado sobre situação e nível de risco da empresa; *(iv)* treinamento e suporte complexos por não serem em português.

As empresas de pequeno e médio porte, organizações públicas de uma forma geral, possuem uma deficiência em questões de gestão da Segurança cibernética. Em entrevistas realizadas, iniciativas isoladas foram detectadas, porém tais iniciativas são demasiadamente trabalhosas, pouco eficientes e baseadas em equipamentos de rede com configurações ultrapassadas . A detecção de vulnerabilidades e a detecção reativa de atividade maliciosa são satisfeitas através da contratação de serviços de consultorias para realização de auditorias realizadas e documentadas manualmente. Tais auditorias não proveem um recurso em tempo real e contínuo para o gerenciamento, controle e tratamento de incidentes. Estas fornecem relatórios muitas vezes interpretados de forma incorreta pelos responsáveis dentro das empresas. Além disso, tais auditorias de segurança são feitas entre grandes intervalos de tempo, resultando em lacunas de segurança, devido ao fato de diariamente surgirem novas vulnerabilidades, infecção de dispositivos e descobertas de falhas. Por fim, as ferramentas de segurança como SOAR e SIEM são pouco utilizados e mal interpretados devido à sua complexidade de operação acarretando uma falsa sensação de segurança.

O MVP resultante da fase 1 do GT-Periscope é parte de uma plataforma mais abrangente de Segurança de Redes e da Informação capaz de abstrair a complexidade técnica da área por meio de emprego de tecnologia inovadora de identificação e predição de atividade maliciosa e de bots na organização. Além disso, ela fornece meios para uma gestão inteligente e centralizada de Segurança. O objetivo da abstração da complexidade técnica é suprir a mão-de-obra escassa e cara na área, proporcionando maior acessibilidade a controles de Segurança para negócios de pequeno e médio portes. O serviço oferecido abstrai a complexidade de análise de comportamento malicioso na rede interna da organização gerando uma análise em alto nível e apontando medidas corretivas; fornece a identificação de bots na rede e sua interação com outros dispositivos, além de permitir a gerência de acordo com seu nível de criticidade da vulnerabilidade; fornece um índice de risco para organização a partir do cenário detectado; fornece um ambiente de resposta a incidentes de segurança integrado, além da capacidade de integrações para abstrair a complexidade de sistemas de detecção de intrusão, WAF e Firewall.

A estratégia organizada para introduzir o serviço no mercado possui duas frentes. A primeira consiste na aproximação com associações de classe, como por exemplo associações de provedores regionais, pois estes possuem uma grande relevância na entrega de Internet pelo Brasil e possuem grandes problemas de Segurança, sendo até alvo de ações de conscientização e formação do NIC.BR através de palestras e cursos realizados em eventos dessas associações de classe*. A segunda frente consiste em publicidade e marketing digital, abordando o tema LGPD e Segurança de Redes e da Informação, visto que empresas de pequeno e médio porte também terão que se adequar e necessitam implementar controles de segurança técnicos oferecidos pela plataforma. O marketing digital irá gerar Leads para alimentar o funil de venda da empresa, que irá comercializar a solução.

Desta forma o serviço oferecido pretende satisfazer a necessidade do público alvo fornecendo um serviço que permita a implantação de mecanismos de segurança na organização capaz de abstrair a complexidade técnica através da aplicação da

tecnologia gerada nesta proposta. Esta plataforma irá situar a organização sobre seu risco atual, proporcionando à empresa uma visão para gerir as vulnerabilidades e incidentes de segurança, além de detectar ações suspeitas em sua rede. O modelo de negócios adotado para geração de receitas é o de Software como um Serviço (SaaS). Este serviço será oferecido através da plataforma NasNuvens da RNP disponível para acesso via Internet. O serviço será comercializado através de planos com contrato para pagamento mensal ou anual para cada perfil de cliente. A definição do melhor modelo de comercialização e dos preços é uma atividade prevista dentro da execução deste projeto. Porém, a título de referência da nossa ideia apontamos abaixo o conjunto de planos que imaginamos oferecer e valores. Identificamos também que para pagamentos anuais, oferecemos desconto na ordem de 10% a 15%. As condições e planos do serviço a título de referência são os seguintes:

Plano Startup (valor para pagamento mensal de R$ 25,00 por ativo):

Receberá a avaliação de risco da rede, obtendo como resultado o índice de risco da organização, resposta a incidentes e uma lista de vulnerabilidades externas. Limite de dispositivos e recursos analisados de até 20.

Plano Basic (valor para pagamento mensal de R$ 19,00 por ativo):

Receberá a avaliação de risco da rede, obtendo como resultado o índice de risco da rede, resposta a incidentes e uma lista de vulnerabilidades internas. Limite de dispositivos e recursos analisados pela plataforma de até 50.

Plano PRO (valor para pagamento mensal de R$ 14,00 por ativo):

Receberá a avaliação de risco da rede, obtendo como resultado o índice de risco da rede, resposta a incidentes e uma lista de vulnerabilidades internas. Limite de dispositivos e recursos analisados pela plataforma de até 100.

Plano Enterprise (valor para pagamento mensal de R$ 11,00 por ativo):

Receberá a avaliação de risco da rede, obtendo como resultado o índice de risco da rede, resposta a incidentes e uma lista de vulnerabilidades internas. Também terá uma análise contínua e online do tráfego IP identificando possíveis bots na rede e lista de vulnerabilidades na rede externa que devem ser tratadas para prevenir ataques. A quantidade de limite de dispositivos e recursos analisados pela plataforma é 200.

Plano 360 sob encomenda

A partir de 200 ativos uma análise da infraestrutura da rede pode ser requisitada a fim de se preparar uma proposta adequada.

A ferramenta produzida na fase 1 deste GT como MVP está sendo denominada de Sherlock-X. Ela já possui página web em https://sherlock-x.com.b r. Para facilitar a comercialização aos clientes do sistema RNP, a ferramenta Sherlock-X estará disponível na loja virtual da RNP, o NasNuvens. Particularmente, para o sistema RNP, acreditamos que esta ferramenta seja de grande valia para as instituições de ensino e pesquisa, os hospitais, os parques e polos tecnológicos, pontos de presença e as demais instituições envolvidas, as quais muitas vezes não possuem mão-de-obra especializada na área de cibersegurança, necessitam fazer uma análise e prevenção automatizada de sua infraestrutura de TI, porém precisam de soluções de segurança eficiente, automatizadas

e fáceis para atender às suas necessidades de segurança sem perder o foco principal de duas atividades.

Assim, através da ferramenta Sherlock-X, essas instituições conseguirão analisar as vulnerabilidades em suas redes e infraestrutura de TI de forma automatizada e ainda identificar se existem bots em sua rede e poderão agir contra a participação de seus dispositivos em redes de bots da Internet (botnets), contribuindo para a segurança da própria instituição e das demais na Internet, implementando dessa forma controles de segurança aptos para atender à LGPD e assim evitando multas e sanções decorrentes do não cumprimento da Lei no quesito Segurança da Informação. A ferramenta Sherlock-X encontra-se em seu estágio de MVP e nesses últimos meses da fase 1, espera-se implantá-la em uma empresa de pequeno porte que se voluntariou como *Early Adopter*. Isto dito consideramos como principais fases na evolução desse MVP, a serem desenvolvidas na fase 2 deste projeto, como:

1- Teste em larga escala da ferramenta Sherlock-X, considerando ambientes reais como este do *Early Adopter* e também do PoP-PR, como os quais a equipe já entrou em contato, possuem o interesse e demonstraram a viabilidade de implantarmos nossa ferramenta a título experimental em seus ambientes;

2- - Aprimoramento e testes de uma técnica de análise de vulnerabilidades da rede interna e correlação de vulnerabilidades a fim de complementar a análise de vulnerabilidades da rede externa;

3- - A definição de posicionamento e características dos sensores para coleta de tráfego de rede que servirá de entrada para análise de nossa ferramenta;

4- - Implementação de controles internos de limitação de acordo com os planos de venda definidos.

5- - A inclusão e configuração da ferramenta Sherlock-X na plataforma NasNuvens da RNP a fim de ser comercializada. Para a inclusão, uma análise do ambiente e entendimento da plataforma serão necessários a fim de delimitarmos as necessidades de ajustes de implementação e softwares.

9. Cronograma de marcos

Até 15/06/2020 - Especificação de Equipe e Equipamentos: o GT apresentará a lista de membros da equipe, seus dados pessoais e demais informações importantes para a contratação dos bolsistas. Também serão apresentados os requisitos dos equipamentos necessários à realização das atividades do GT.

Entre 01/07/2020 e 17/07/2020 - Reunião Inicial: participação na reunião entre o GT e a RNP, onde o coordenador geral apresentará a visão inicial da proposta de Fase 2, incluindo melhorias propostas ao produto e negócio, visão da oferta ao Sistema RNP.

Entre 01/07/2020 e 31/07/2020 - Processo de Proteção e Licenciamento da Tecnologia: daremos continuidade ao processo de proteção da tecnologia junto à RNP e para a StartUp que ficará responsável por comercializar a tecnologia desenvolvida.

Entre 01/07/2020 e 30/09/2020 - Teste em larga escala da ferramenta Sherlock-X:

Serão realizados testes em ambientes reais como este do *Early Adopter* e também do PoP-PR, com os quais a equipe já entrou em contato e demonstraram possuir o interesse e a viabilidade técnica para implantarmos nossa ferramenta a título experimental em seus ambientes operacionais.

Entre 01/07/2020 e 30/09/2020 - Capacitação para o Desenvolvimento da Modelagem do Produto/Serviço: participação nas sessões de treinamento e mentorias para o desenvolvimento produto/serviço, modelagem de vendas e canais, em especial a loja virtual da RNP para a divulgação e oferta do novo produto do GT.

Entre 01/09/2020 e 30/12/2020 - Testes da análise de vulnerabilidades da rede interna: Aprimoramento e testes de uma técnica de análise de vulnerabilidades da rede interna e correlação de vulnerabilidades a fim de complementar a análise de vulnerabilidades da rede externa.

Até 15/10/2020 - Plano de Desenvolvimento da Modelagem do Produto/Serviço: o grupo apresentará o plano para desenvolver a modelagem do produto/serviço que deverá ser implementado ao longo da fase 2 do GT com o objetivo de divulgar a proposta de valor para segmentos de clientes, visando capturar interessados e validar o modelo com foco no Sistema RNP.

A partir de 15/10/2020 - Atualização da Landing Page: atualização da *landing page* da solução desenvolvida no contexto do GT, com o intuito de atrair o interesse de potenciais clientes.

Atividade - Entre 16/10/2020 e 30/10/2020 - Webinar de Apresentação para RNP: apresentação executiva para os colaboradores da RNP com o propósito de apresentar a solução e o negócio desenvolvido para o Sistema RNP.

Entrega - Entre 01/07/2020 e 31/12/2020 - Inclusão do Produto na Loja Virtual da RNP para disponibilização da oferta: o GT realizará durante esse período o processo de cadastro do produto na loja virtual da RNP, adequando-se ao processo de autenticação da plataforma, bem como a barra de navegação do NasNuvens, formulação dos termos e políticas do produto do GT entre outros instrumentos como: termo de uso, política de privacidade, descrição do serviço, modelos de oferta do serviço, mecanismos de precificação, processo de atendimento ao usuário e adequações às legislações pertinentes. Esta atividade será realizada com apoio da equipe RNP que gerencia e opera a loja virtual.

Entre 01/01/2021 e 28/02/2021 - Implementação de limitação de acordo com os planos de venda: Implementação de controles internos de limitação de acordo com os planos de venda definidos.

Entre 01/01/2021 e 30/06/2021 - Oferta Inicial para o Sistema RNP: o GT irá operacionalizar o produto ofertado no NasNuvens. Este período servirá como validação

dos processos de suporte e atendimento aos clientes do Sistema RNP. O GT definirá e monitorará indicadores para avaliar a aceitação de seu produto junto ao Sistema RNP.

Até 30/03/2021 - Ficha Técnica e Comercial do Produto para o Sistema RNP: o GT produzirá uma ficha técnica e comercial do produto a ser ofertado ao Sistema RNP, destacando as evoluções técnicas obtidas na fase 2, os resultados e aprendizados com a implementação do plano de desenvolvimento da modelagem do produto/serviço.

Entre 01/05/2021 e 30/05/2021 - Demonstração no Workshop RNP (WRNP): o GT demonstrará os resultados do produto do GT durante o Workshop da RNP.

Entre 01/05/2021 e 30/05/2021 - Apresentação Final do Produto para o Sistema RNP: equipe do GT fará uma apresentação do produto para avaliação da RNP.

Até 30/06/2021 - Código-fonte e Documentação do Produto para o Sistema RNP: o grupo deverá entregar a última versão do código-fonte desenvolvido no ambiente de desenvolvimento colaborativo da RNP e documentação técnica e manuais de uso e instalação/configuração da solução.

Além desses marcos, o coordenador geral irá apresentar mensalmente um relatório de atividades de cada membro contratado da equipe. Da mesma forma, mensalmente a equipe do GT apresentará para a equipe da RNP, em reuniões de acompanhamento, evidências de avanços no desenvolvimento da ferramenta e avanços na disseminação do produto e resultados dessa disseminação.

10. Recursos financeiros

10.2. Infraestrutura

A soma dos créditos no serviços compute@RNP e dos equipamentos está no valor de **R$ 24.430,32**.

10.2.1. 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 Extra Grande	Linux	1	01/10/2020	31/05/2021	8	680,79	5.446,32
						Subtotal	5.446,32

10.2.2. Equipamentos

Utilizamos a configuração padrão descrita no Anexo 4. Equipamentos solicitados serão destinados ao grupo de pesquisa.

Descrição	**Instituição de Destino**	**Qtd.**	**Valor em R$ estimado**
Desktop Modelo i7 (Core i7 - 16GB - SSD 256GB) + Kit teclado e mouse com fio	UFPR	03	10.808,00
Monitor 24”	UFPR	03	3.150,00
Notebook 14” Modelo i7 (Core i7 - 8GB - SSD 256GB). Incluso: Garantia 3 anos Complete Care, com coberta acidental e troca de peças onsite.	UFPR	01	5.026,00
		S ıbtotal	18.984,00

Referências

[1] Pequenos negócios em números. https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-emnumeros,12e8794363447510VgnVCM1000004c00210aRCRD. [Último acesso em Abril/2020].

[2] Multiple fiber routers are being compromised by botnets using 0-day. https://blog.netlab.360.com/multiple-fiber-routers-are-being-compromised-by-botnets-u sing-0-day-en/. [Último acesso em Abril/2020].

[3] Relatório Anual de Incidentes de Segurança na Rede Brasileira de Ensino e Pesquisa 2017. [Último acesso em Abril/2020] http://docente.ifsc.edu.br/mello/livros/seguranca/12_rnp_ra_cais_2017.pdf

[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.