UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Proposta de Implementação do Protocolo *NetFlow* como Mecanismo Proactivo de Detecção de *Botnets* Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação

***Caso de Estudo**:* Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet)

Autor

Cossa, Jorge Rodrigues

Supervisor da Faculdade

Eng. Délcio Arnaldo Chadreca (MsC)

Supervisor da Instituição

Eng. Leonel Nhavene

Maputo, Junho 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Proposta de Implementação do Protocolo *NetFlow* como Mecanismo Proactivo de Detecção de *Botnets* Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação

Caso de Estudo: Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet)

Autor

Cossa, Jorge Rodrigues

Supervisor da Faculdade

_____

Eng. Délcio Arnaldo Chadreca (MsC.)

Supervisor da Instituição

_____

Eng. Leonel Nhavene

Maputo, Junho 2025

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

TERMO DE ENTREGA DE RELATÓRIO DE TRABALHO DE LICENCIATURA

Declaro que o estudante Jorge Rodrigues Cossa entregou no dia ___/06/2025, às 03 cópias do seu relatório de Trabalho de Licenciatura com referência _____, intitulado: Proposta de Implementação do Protocolo *NetFlow* como Mecanismo Proactivo de Detecção de *Botnets* Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação. Caso de Estudo: Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet)

Maputo, ____ de Junho de 2025

A Chefe da Secretaria do DEEL

_____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

DECLARAÇÃO DE HONRA

Declaro, sob compromisso de honra, que o presente trabalho é da minha autoria, para fins de culminação do curso. Todo o conteúdo do trabalho apresentado foi desenvolvido com base em pesquisas, investigação do referencial teórico e um caso de estudo. As fontes de informação e referências utilizadas foram devidamente citadas e estão de acordo com as normas de citação e referenciação estabelecidas pela faculdade.

Adicionalmente, declaro que este trabalho não foi submetido, no todo ou em parte, em nenhuma outra instituição ou para obtenção de qualquer outro grau académico.

Maputo, ____ de Junho de 2025

Autor

_____

(Jorge Rodrigues Cossa)

DEDICATÓRIA

Dedico este trabalho ao meu Pai

Rodrigues Ernesto Cossa

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, o provedor de todas as coisas, pela dádiva da vida, pela saúde e pela sabedoria que me guiaram ao longo desta jornada. Sua presença foi essencial em cada etapa deste trabalho.

Aos meus pais, expresso minha eterna gratidão pelo amor incondicional, pelo cuidado e pela educação que me proporcionaram. Vocês são meu porto seguro e os responsáveis pela formação dos valores que guiam minha vida.

Ao meu tio, João Zibia, agradeço pelo apoio, carinho e incentivo, que foram fundamentais para meu crescimento acadêmico e pessoal.

Aos meus irmãos, primos e amigos, que representam minha família estendida e minha fonte de inspiração constante. Agradeço especialmente a Nazish, Deape, Flávio Cossa, Laura Zibia, Teresa Nhambumbo, Salésio Mussane, Joaquim Langane e, com destaque, a minha amada namorada Ofélia Nhaca, o Júlio Chinavane e o Simão Canze. Cada um de vocês, com sua presença e apoio, tornou este percurso mais leve e significativo.

À Universidade Eduardo Mondlane, sou grato pela oportunidade de desenvolvimento acadêmico e pessoal. Agradeço, em especial, ao meu supervisor, Eng. Délcio Arnaldo Chadreca (MsC.), pela orientação, paciência e pelo suporte indispensável durante a realização deste trabalho.

Minha gratidão também se estende à equipa do INAGE, IP/MoRENet, pela recepção calorosa e pelo apoio técnico e moral ao longo deste processo. Menciono com apreço o Eng. Leonel Nhavene, a Dra. Inalda Ernesto, o Eng. Belito Sitoe, o Eng. Zacarias Maganda, o Eng. Mercídio Huo, a Eng. Mercia Nhamutocue, o Dr. Ivan Ribeiro, a Dra. Dilma Monjane e o Dr. Emídio Nguale.

Por fim, agradeço à TaQUICK Delivery e à confiança depositada em mim por seus líderes e colegas. Em especial, ao Sr. Paulo Steytler, à Sra. Gisela Steytler e Paula Rodrigues, cujo apoio foi inestimável ao longo desta caminhada.

A todos que, directa ou indirectamente, contribuíram para a realização deste trabalho, deixo minha gratidão mais sincera.

EPÍGRAFE

“Não é o mais forte quem sobrevive, nem o mais inteligente,

mas o que melhor se adapta às mudanças.”

Leon C. Megginson (1963)

RESUMO

O ciberespaço é um ambiente de interacção entre diversas infraestruturas de redes de computadores, onde ameaças cibernéticas são verificadas e representam desafios para a segurança. As *Botnets* estão entre as principais ameaças do ciberespaço, destacando-se pela capacidade de realizar ataques em larga escala e se infiltrar em infraestruturas de rede sem serem detectadas, comprometendo sistemas críticos.

O presente estudo teve como principal objectivo propor a implementação do protocolo *NetFlow* como uma solução proactiva para a detecção de *Botnets* baseada na análise de tráfego de rede, com foco na infraestrutura de sistemas de informação da MoRENet (Rede de Instituições de Ensino Superior e de Investigação de Moçambique). Entretanto, para alcançar os objectivos do estudo, foi realizada uma pesquisa mista, isto é, qualitativa e quantitativa, e para recolha de dados recorreu-se a pesquisa documental, bibliográfica, assim como entrevistas e questionário direccionadas à equipe técnica do CSIRT (Equipe de Resposta a Incidentes de Segurança de Computadores) da MoRENet.

Entretanto, o estudo revelou que a implementação do protocolo *NetFlow* é uma solução proactiva para a detecção de *Botnets* na infraestrutura da MoRENet, destacando-se pela capacidade de análise detalhada do tráfego em tempo real, baixo custo, escalabilidade e integração com ferramentas de segurança existentes. A solução demonstrou ser capaz de identificar padrões anômalos associados a servidores de comando e controle (C&C) de *Botnets*, reduzindo a dependência de intervenção manual e permitindo respostas rápidas a incidentes, com impacto mínimo no desempenho da rede. Além disso, a solução não apenas mitiga ameaças associados a *Botnets*, mas também oferece uma visão das actividades que ocorrem na rede MoRENet, o que fortalece a capacidade de monitorização e resposta a incidentes emergentes.

Diante do exposto, recomenda-se a melhoria contínua da solução proposta, desde a actualização da infraestrutura, testes de desempenho e capacitação de profissionais para lidar com novas ameaças e tecnologias de segurança cibernética. Assim como, o desenvolvimento de estudos locais sobre incidentes cibernéticos para apoiar nas futuras pesquisas e práticas de detecção de *Botnets*.

Palavras-chave: Segurança cibernética, *NetFlow*, *Botnets*, Tráfego de rede, MoRENet

ABSTRACT

Cyberspace is an environment of interaction between various computer network infrastructures, where cyber threats are verified and pose security challenges. Botnets are among the main threats in cyberspace, standing out for their ability to carry out large-scale attacks and infiltrate network infrastructures undetected, compromising critical systems.

The main objective of this study was to propose the implementation of the NetFlow protocol as a proactive solution for detecting Botnets based on analysing network traffic, with a focus on the information systems infrastructure of MoRENet (Mozambique Higher Education and Research Institutions Network). However, to achieve the objectives of the study, mixed research was carried out, i.e. qualitative and quantitative, and data collection used documentary and bibliographical research, as well as interviews and questionnaires directed at the technical team of MoRENet's CSIRT (Computer Security Incident Response Team).

Meanwhile, the study revealed that the implementation of the NetFlow protocol is a proactive solution for detecting Botnets in MoRENet's infrastructure, and stands out for its ability to analyse traffic in detail in real time, low cost, scalability and integration with existing security tools. The solution proved capable of identifying anomalous patterns associated with Botnet command and control (C&C) servers, reducing dependence on manual intervention and enabling rapid responses to incidents, with minimal impact on network performance. In addition, the solution not only mitigates threats associated with Botnets, but also offers a view of the activities taking place on the MoRENet network, which strengthens the ability to monitor and respond to emerging incidents.

In view of the above, it is recommended that the proposed solution be continuously improved, from updating the infrastructure, performance testing and training professionals to deal with new cyber security threats and technologies. As well as the development of local studies on cyber incidents to support future research and practices for detecting Botnets.

Keywords: Cybersecurity, NetFlow, Botnets, Network traffic, MoRENet

GLOSSÁRIO DE TERMOS

Algoritmos de Geração de Domínios (DGAs): é uma técnica usada por *malware* para criar um grande número de nomes de domínio que podem ser usados para comunicação de comando e controlo (C&C).

Botnet: é a abreviatura de rede de *robots*. O termo *robot*, ou *bot*, é um termo genérico para programas automatizados que executam tarefas sem a intervenção do utilizador.

Botmaster: é uma pessoa/grupo de pessoas que controla remotamente as *Botnets* e emite comandos para servidores comando e controlo (C&C) e *bots* numa rede. É também designado por controlador de *Botnets* ou pastor de *bots*.

Cibercriminoso: indivíduos ou grupos que utilizam a tecnologia e a *Internet* para perpetrar actividades ilegais, como acesso não autorizado a sistemas ou redes de computadores.

Ciberespaço: espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores (…) conjunto de sistemas de comunicação electrônicos que transmitem informações provenientes de fontes digitais ou destinadas a digitalização.

Cron job: é uma tarefa criada usando o *cron*, uma ferramenta para agendar e automatizar tarefas futuras em nos sistemas operacionais baseados no *Unix*.

CSIRT: é uma organização responsável por receber, analisar e responder a notificações de incidentes de segurança informática e actividades levantadas por qualquer utilizador, empresa, agência governamental ou organização.

DNS Blacklisting: é um mecanismo de listar e bloquear endereços IP ou domínios associados a comportamentos indesejados, como o envio de *spam*.

Domain-Flux: é uma técnica usada por *hackers* para obscurecer suas operações, alterando constantemente o nome de domínio do servidor envolvido em actividades maliciosas.

Fast-flux: consiste em ter múltiplos endereços IP associados a um nome de domínio, que são alterados de forma constante e em pouco tempo.

Honeynet: também conhecido como '*zoo*', o *honeynet* é uma rede de *honeypots*, com diferentes sistemas.

NetFlow: é uma tecnologia da Cisco IOS que fornece estatísticas sobre os pacotes que trafegam pelo roteador (*router*), e permite a monitorização da rede e da segurança, o planeamento da rede, a análise do tráfego.

NFDump: com a ajuda do seu *daemon nfcapd*, captura dados de *NetFlow* e armazena-os em ficheiros em colector *NetFlow*.

Nfcapd: é o *daemon* de captura de *NetFlow* das ferramentas *NFDump*.

Malware: refere-se a todo *software* que tenha sido alterado ou desenvolvido com o intuito de prejudicar um sistema de informação, danificando dispositivos, roubando informação ou por outras assumir controlo do mesmo, seja a nível individual ou a nível organizacional.

Servidor de Comando e Controlo (C&C): é um computador controlado por um atacante ou cibercriminoso que é utilizado para enviar comandos a sistemas comprometidos (máquinas *Bots*) por *malware* e receber dados roubados de uma rede alvo.

Spambots: é um tipo específico de *bot* que envia mensagens de *spam*, sendo que pode postar *spam* em vários lugares onde os usuários interagem *online*, como plataformas de mídia social ou fóruns.

Zero Day: é um termo amplo que descreve as vulnerabilidades de segurança recentemente descobertas que os *hackers* podem usar para atacar sistemas.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

C&C - Comando e Controlo

CSIRT GOV - Equipe de Resposta a Incidentes de Segurança de Computacionais do Governo

DDoS - *Distributed Denial of Service* - Negação de Serviço Distribuído

FFSN - *Fast-Flux Service Networks* - Redes de serviços de fluxo rápido

DNS - *Domain Name System* - Sistema de Nomes de Domínio

DDNS - *Dynamic Domain Name System* - Sistema de Nomes de Domínio Dinâmico

HTTP - *Hyper Text Transfer Protocol*- Protocolo de Transferência de Hipertexto

INAGE, IP - Instituto Nacional de Governo Electrónico, Instituto Público

IoT - *Internet of Things* - Internet das Coisas

IRC - *Internet Relay Chat*

NSM - *Network Security Monitor* - Monitor de Segurança de Rede

nCSIRT - Equipas de Resposta a Incidentes de Segurança Computacionais Nacional

MoRENet - *Mozambique Research and Education Network* - Rede de Instituições de Ensino Superior e de Investigação de Moçambique

P2P - *Peer-to-Peer* – Par-a-Par /Ponto-a-Ponto

PoP - *Point of Presence* - Pontos de Presença

PENSC - Política Nacional de Segurança Cibernética e a Estratégia Nacional de Segurança Cibernética

RDNS - *Recursive Domain Name System* - Sistema de Nomes de Domínio Recursivo

SI - Sistema de Informação

SSH - *Secure Shell*

TIC - Tecnologias da Informação e Comunicação

TCP - *Transmission Control Protocol* - Protocolo de Controlo de Transmissão

UDP – *User Datagram Protocol* - Protocolo de Datagramas do Usuário

CAPÍTULO I: INTRODUÇÃO

1.1. Contextualização

O desenvolvimento tecnológico é uma das coisas mais notáveis nessas últimas décadas, trazendo grandes benefícios, valores, para a sociedade. Segundo O'Regan, (2016), a sociedade observou um avanço na tecnologia nas últimas décadas do século XX, onde destacou uma evolução de equipamentos, *softwares*, protocolos, arquitecturas, trazendo melhorias de vida de muitos cidadãos, diminuindo o número de tarefas e elevando-se a produtividade, o que se torna constrangedor e custoso imaginar o mundo actual e moderno sem a tecnologia.

A medida que a tecnologia avança e a digitalização das infraestruturas aumenta, surgem novos desafios, particularmente na área da segurança cibernética. O ciberespaço demostra-se como um ambiente vital para a comunicação, o compartilhamento de informações e a realização de actividades globais, sendo assim, susceptível a ameaças emergentes que representam um desafio e riscos a integridade da segurança dos sistemas críticos.

Entretanto, os ataques cibernéticos estão em constante evolução, representando uma ameaça a todos activos presentes no ciberespaço, seja um individuo, uma organização (governamental ou não governamental), uma instituição, uma empresa, entre outros. Observa-se que as infraestruturas de sistema de informação (SI) mais robustas são grandes alvos de ataques cibernéticos, sendo que o objectivo poderá ser a sabotagem, a exploração de recursos, a busca de informações sensíveis que resultam em extorsão, entre outros vários aspectos.

Entre diversas ameaças no ciberespaço, ataques de *Botnets* se destacam como prejudiciais e difíceis de serem detectadas, dada sua capacidade de se infiltrar em sistemas críticos, infectando dispositivos e controlando-os para realizar actividades maliciosas em destaque ataques cibernéticos de larga escala.

O ciberespaço moçambicano, não fica isento dos ataques cibernéticos, e a medida que o País avança na transformação digital, a segurança cibernética tem se tornado uma prioridade. Entretanto, tem-se despertado uma atenção voltada ao estudo e adoção de

mecanismos de segurança de informação, com o objectivo de identificar e mitigar as diversas ameaças emergentes no ciberespaço. Um exemplo, é o incidente cibernético que abalou os intervenientes ciberespaço moçambicano, onde segundo o jornal O País (2022), afirmou que “cerca de trinta (30) sites de instituições do Governo ficaram mais de 14 horas indisponíveis, depois de um ataque cibernético do grupo Yemeni Hackers, um exército de terroristas digitais. Não há registo de um ciberataque desta dimensão em Moçambique.”. Esse incidente levantou preocupações sob os activos no ciberespaço, quanto a protecção das infraestruturas críticas do País diante dos ataques cibernéticos.

Em resposta as ameaças cibernéticas, diversas abordagens são utilizadas como mecanismo de segurança para infraestruturas de SI. No contexto das *Botnets*, que se caracterizam pelo uso da infraestrutura de SI para efectuar ataques, têm sido desenvolvidos diferentes mecanismos de detecção. De acordo com Ribeiro (2020, p. 21), “uma das soluções mais comuns para detecção de *Botnets*, consiste em desenvolver sistemas para analisar o tráfego da rede e identificar componentes maliciosos.”.

No entanto, essas soluções muitas vezes são projectados para monitorar e examinar o tráfego de rede em busca de padrões que possam indicar a presença de *Botnets* ou outras actividades cibernéticas suspeitas na infraestrutura. Diversas ferramentas de análise de tráfego de rede, como o *Zeek*, *SFlow*, *NetFlow*, podem ser aplicadas de forma a complementar a segurança da infraestrutura, aproveitando as vantagens que cada uma delas oferece para criar um mecanismo de defesa robusto, que seja capaz de detectar e mitigar as ameaças cibernéticas emergentes.

O presente trabalho visa abordar sobre o estudo da implementação de uma solução de segurança cibernética em uma infraestrutura de sistema de informação (SI), onde dá-se enfase a um mecanismo proactivo de detecção de *Botnets*. O mecanismo segue com a proposta de implementação do protocolo *NetFlow* que desempenha um papel fundamental na detecção de *Botnets*. O tráfego de rede colectado pelo protocolo *NetFlow* será a base da identificação e correlacção de actividades de servidores e comando e controlo (C&C) *Botnets*. Embora as principais abordagens deste estudo tenham sido delineadas, a pesquisa não se limita ao que foi mencionado, pois agregará também algumas técnicas e ferramentas auxiliares para o armazenamento, análise, correlacção, detecção, monitoramento e visualização dos dados de eventos relacionados com os

servidores C&C *Botnets*. O caso de estudo da pesquisa será conduzido na MoRENet (*Mozambique Research and Education Network* - Rede de Instituições de Ensino Superior e de Investigação de Moçambique), parte integrante do INAGE, IP (Instituto Nacional de Governo Electrónico, Instituto Público).

1.2. Problematização

Com o crescente número de dispositivos conectados no ciberespaço, tem emergido novas ameaças cibernéticas. Dentre essas, ameaças destacam-se as redes *Botnets*, que constituem actualmente uma das ameaças cibernéticas de mais rápido crescimento global, comprometendo desde redes domésticas até infraestruturas críticas. O relatório "*Threat Intelligence Report*" publicado pela Nokia (2023), afirma que as actividades maliciosas de *Botnet* de IoT aumentaram drasticamente, tendo o número de dispositivos IoT (*Bots*) envolvidos em ataques DDoS impulsionados por *Botnets* aumentado cerca de 200.000 para aproximadamente 1 milhão de dispositivos em um ano, um aumento cinco vezes desde o ano 2022. Aumento esse caracterizado pela aderença massiva no uso de dispositivos IoT por parte dos consumidores em todo o mundo, principalmente após o início do conflito Rússia-Ucrânia, sendo ataques DDoS impulsionados por *Botnets* usados para interromper redes de telecomunicações, bem como outras infraestruturas e serviços críticos, gerando mais de 40% de todo o tráfego DDoS hoje.

Esse cenário de ameaças *Botnets* também apresentam implicações para o contexto Moçambicano, especialmente para infraestruturas de redes críticas como a da MoRENet. No entanto, as soluções de segurança em Moçambique poderão enfrentar desafios, em ataques semelhante a *Botnets,* que já representam uma ameaça no ciberespaço africano*,* onde segundo a Trend Micro (s.d, citado por Richard, 2021), no relatório "*African Cyberthreat Assessment Report"*, afirma que vítimas de *Botnets* em África têm uma média de 3.900 detecções mensais, com cerca de 50.000 detecções no total, onde os agentes de ameaças em África estão a implementar campanhas de *spam* com *Trojans* como o *Emotet*, *Lokibot*, *Agent Tesla*, *Fareit*, etc (…), sendo uma das razões para a expansão das operações DDoS evolvendo *Bots*, tendo o cibercrime como um serviço disponível através dos ambientes da *Web* aberta e escura.

Diante do exposto, ataques *Botnets* demostram ser uma ameaça de preocupação global para as infraestruturas digitais, sendo que a sua protecção é uma tarefa fundamental. Para a infraestrutura de rede de grande escala como a MoRENet o desafio é maior, pois pode ser vulnerável a esse ataque, onde a tomada de medidas de prevenção e mitigação dos seus sistemas de informação é essencial, principalmente devido a demanda dos dados processados e o dano causado por um ataque cibernético envolvendo *Botnets*.

A MoRENet é um projecto do Governo de Moçambique, voltada a Instituições de Ensino Superior, de investigação e do ensino técnico-profissional. Existe na MoRENet uma equipa de resposta a incidentes cibernéticos "CSIRT[1] da Academia" composta por profissionais de cibersegurança, que monitoram os diversos eventos que ocorrem pela infraestrutura de SI da MoRENet, e desenvolvem mecanismos de segurança contra eventuais actividades maliciosas "Ciberataques". Poucas organizações dispõem de mecanismos dedicados para detecção de *Botnets*, e o CSIRT da Academia tem o dever de englobar essas soluções na sua infraestrutura. A introdução dessa capacidade não só eleva o patamar de segurança da informação na MoRENet, como também serve de referência inovadora para outras instituições. Uma solução de detecção de ameaças *Botnets* é essencial, pois poderá preencher uma lacuna crítica na defesa cibernética da infraestrutura da MoRENet, protegendo os seus activos e serviços críticos.

1.2.1. Pergunta de pesquisa

Prodanov & Freitas (2013, p. 43), afirmam que a pesquisa sempre parte de um problema, de uma interrogação, uma situação para a qual o repertório de conhecimento disponível não gera resposta adequada. É "uma questão, uma dúvida que se apresenta à nossa consideração para ser respondida e solucionada." (Prodanov & Freitas, 2013, p. 85).

O presente trabalho se concentrará na seguinte pergunta de pesquisa:

- Como a implementação do protocolo *NetFlow* pode auxiliar na detecção proactiva de *Botnets* na infraestrutura de sistemas de informação do Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet)?

[1] CSIRT - *Computer Security Incident Response Team* - Equipe de Resposta a Incidentes de Segurança de Computadores

1.3. Objectivos

1.3.1. Objectivo geral

- Propor a implementação do protocolo *NetFlow* como mecanismo proactivo de detecção de *Botnets* baseada na análise de tráfego de rede na infraestrutura de sistemas de informação do Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet).

1.3.2. Objectivos específicos

- Avaliar o cenário da segurança cibernética em Moçambique, bem como no contexto global, e as ameaças de *Botnets* no ciberespaço;
- Identificar as práticas e técnicas disponíveis para a detecção e mitigação de *Botnets* em uma infraestrutura de sistema de informação;
- Elaborar uma proposta de solução com foco na implementação do protocolo *NetFlow* para a detecção de *Botnets*, fundamentada na análise das amostras de tráfego de rede do INAGE, IP/MoRENet;
- Verificar a eficácia da proposta de implementação do protocolo *NetFlow* na detecção proactiva de *Botnets*, por meio da análise de dados colectados na infraestrutura de rede da INAGE, IP/MoRENet.

1.4. Metodologia de pesquisa

Para Gerhardt & Silveira (2009, p. 31), “a pesquisa científica é o resultado de um inquérito ou exame minucioso, realizado com o objectivo de resolver um problema, recorrendo a procedimentos científicos.”.

1.4.1. Quanto aos objectivos

Quanto ao objectivo de estudo, foram utilizadas a pesquisa exploratória e a pesquisa descritiva. A pesquisa exploratória, segundo Gil (2008), é uma pesquisa desenvolvida para proporcionar maior identificação dos conceitos fundamentais tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores. Já a pesquisa descritiva, conforme Triviños (1987), o pesquisador deve conter uma série de informações da sua pesquisa, pois a pesquisa descritiva descreve

com exatidão os factos e fenômenos de determinada realidade. No contexto deste estudo, a pesquisa exploratória foi essencial para investigar práticas e técnicas, como o uso do protocolo *NetFlow* para a detecção e mitigação de incidentes relacionados com *Botnets*. Por sua vez, a pesquisa descritiva possibilitou a caracterização do cenário da segurança cibernética em Moçambique e da infraestrutura do INAGE, IP/MoRENet, proporcionando fundamentos para a análise dos desafios enfrentados face as ameaças cibernéticas emergentes no ciberespaço.

1.4.2. Quanto a natureza

Quanto à natureza, o estudo caracteriza-se como uma pesquisa aplicada, que segundo Prodanov & Freitas (2013), a pesquisa aplicada objectiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos, envolvendo verdades e interesses locais. A pesquisa aplicada, foi fundamental para o estudo, pois procura-se reunir e analisar os conhecimentos científicos para a resolução de um problema específico, as ameaças representadas por *Botnets* no contexto da segurança cibernética em Moçambique, culminando na proposta da implementação de uma solução tecnológica "protocolo *NetFlow*" como um mecanismo de detecção de *Botnets* na infraestrutura do INAGE, IP/MoRENet. No entanto, o estudo oferecesse uma solução prática que poderá contribuir para a melhoria da segurança da rede, alinhando-se aos interesses e desafios do cenário moçambicano.

1.4.3. Quanto a abordagem

Quanto à abordagem, o estudo utiliza a pesquisa mista, isto é, qualitativa e quantitativa. Segundo Gerhardt & Silveira (2009), a pesquisa qualitativa preocupa-se com aspectos da realidade que não podem ser quantificados, ou seja, não se preocupa com representatividade numérica, centrando-se na compreensão e explicação da dinâmica das relações sociais. Já a pesquisa quantitativa, de acordo com Prodanov & Freitas (2013), utiliza-se de parâmetros estatísticos "linguagem matemática", onde deve-se formular hipóteses e classificar a relação entre as variáveis para garantir a precisão dos resultados, apresentando dados reais no processo de análise e interpretação. No estudo, a pesquisa qualitativa foi essencial para compreender cenário da segurança cibernética no caso de estudo, com base nas percepções e experiências dos técnicos sobre a

ocorrência de ameaças cibernéticas na infraestrutura do INAGE, IP/MoRENet, tendo em conta as *Botnets*, as práticas e desafios na detecção e mitigação das ameaças, permitindo uma análise detalhada dos dados fornecidos. Por outro lado, a pesquisa quantitativa foi fundamental para a análise dos dados colectados na infraestrutura do INAGE, IP/MoRENet, utilizando estatísticas que permitem quantificar e interpretar os dados, fornecendo fundamentos sobre a ocorrência de ameaças cibernéticas e de actividades *Botnets* na rede.

1.4.4. Quanto ao procedimento

Quanto ao procedimento, o estudo utiliza a pesquisa bibliográfica, documental, a pesquisa-ação e o estudo de caso.

I. Pesquisa bibliográfica

A pesquisa bibliográfica, segundo Fonseca (2002, citado por Gerhardt & Silveira, 2009), refere-se as pesquisas feitas a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de *web sites*, entre outros, tendo o pesquisador uma interacção directa com material. Esse método foi essencial para fundamentar teoricamente o trabalho, através de diversos estudos e referências, tendo em conta a segurança cibernética no ciberespaço moçambicano, a natureza das redes *Botnets*, e as técnicas de análise de tráfego de rede na detecção de *Botnets*.

II. Pesquisa documental

A pesquisa documental, segundo Gil (2008), assemelha-se muito à pesquisa bibliográfica. A única diferença entre ambas está na natureza das fontes (…). a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objectivos da pesquisa. No contexto deste estudo, a pesquisa documental foi fundamental para acesso a fontes primárias, como documentos, relatórios técnicos, políticas de segurança cibernética, entre outros, que forneceram dados relevantes e actualizados no contexto da pesquisa e do caso de estudo em torno da segurança cibernética em especial as ameaças *Botnets*. Essa abordagem permitiu complementar as informações obtidas por meio da pesquisa bibliográfica, permitiu enriquecer os dados para a pesquisa e a sua proposta de solução.

III. Estudo de caso

Para o estudo de caso, conforme Fonseca (2002, citado por Gerhardt & Silveira, 2009), é "caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social." No entanto, o INAGE, IP/MoRENet foi o objecto de análise para o presente estudo, permitindo uma investigação detalhada da sua infraestrutura de SI no cenário da segurança cibernética.

IV. Pesquisa-Acção

Por fim, a pesquisa-acção, onde de acordo com por Gerhardt & Silveira (2009), é um tipo de investigação social com base empírica que é concebida e realizada em estreita associação com uma acção ou com a resolução de um problema colectivo no qual os pesquisadores e os participantes representativos da situação ou do problema estão envolvidos de modo cooperativo ou participativo. No contexto do presente estudo, a pesquisa-acção proporcionou uma interacção directa entre o pesquisador e os profissionais responsáveis pela gestão da infraestrutura de rede do INAGE, IP/MoRENet. Essa colaboração permitiu não apenas a identificação dos desafios relacionados à detecção de *Botnets*, mas também a implementação e teste prático do protocolo *NetFlow* em um ambiente de teste, facilitando a troca de conhecimentos e a adaptação da solução proposta às necessidades da infraestrutura.

1.4.5. Técnicas de colecta de dados

Quanto às técnicas de colecta de dados, o estudo utilizou a entrevista e o questionário. Segundo Gil (2008, p. 109), a entrevista é a técnica em que o investigador se apresenta frente ao investigado e lhe formula perguntas, com o objectivo de obtenção dos dados que interessam à investigação. Por outro lado, de acordo com o Gerhardt & Silveira (2009, p. 69), o questionário é um instrumento de colecta de dados constituído por uma série ordenada de perguntas que devem ser respondidas por escrito pelo informante, sem a presença do pesquisador. Essas técnicas foram importantes para o estudo, pois a entrevista permitiu uma interacção com profissionais de segurança cibernética e de redes, e o questionário possibilitou ampliar o alcance da colecta de dados, permitindo a obtenção de respostas padronizadas que facilitaram a análise quantitativa, sobre os desafios enfrentados na MoRENet no combate às *Botnets*.

1.5. Estrutura do trabalho

A estrutura do trabalho é composta por capítulos que englobam os seus subcapítulos:

- **CAPÍTULO I: INTRODUÇÃO** – Este capítulo é a base inicial do trabalho, onde é apresentada a visão geral do tema. São apresentados: a contextualização; a problemática; os objectivos; a metodologia de pesquisa; e a estrutura do trabalho.
- **CAPÍTULO II: REVISÃO DA LITERATURA** – Este capítulo é reservado a estudos e pesquisas relacionados ao tema, trazendo termos-chave e conceitos fundamentais em uma abordagem de estudo. A revisão da literatura aborda três (3) aspectos: – a segurança cibernética no ciberespaço moçambicano; – as *Botnets*; – as soluções de análise de tráfego de rede na detecção de *Botnets*.
- **CAPÍTULO III: CASO DE ESTUDO** – Este capítulo detalha o caso de estudo conduzido na MoRENet, parte integrante do INAGE, IP. É também abordado a situação ou cenário actual da segurança cibernética na MoRENet, as acções exercidas consoante a incidentes cibernéticos, em foco as actividades *Botnets.*
- **CAPÍTULO IV: SOLUÇÃO PROPOSTA** – Este capítulo descreve de forma detalhada a solução proposta desenvolvida para o problema identificado da pesquisa. Serão apresentadas as etapas para a implementação do protocolo *NetFlow*, incluindo as práticas, as ferramentas e as configurações. A solução proposta será discutida com ênfase na sua adequação ao cenário actual da MoRENet, considerando os desafios e as necessidades específicas do ambiente.
- **CAPÍTULO V: ANÁLISE DOS DADOS E DISCUSSÃO DE RESULTADOS** – Este é o capítulo é reservado a análise dados e discussão dos resultados obtidos a partir do estudo. Envolve a análise detalhada dos dados colectados e apresentados sobre a situação actual do caso do estudo a MoRENet mediante ao problema da pesquisa. Por fim, é discutido as etapas da elaboração do estudo, os resultados obtidos desde a formulação do problema até a solução proposta.
- **CAPÍTULO VI: CONSIDERAÇÕES FINAIS** – Este é o capítulo final do trabalho, onde apresenta as conclusões gerais da pesquisa, as recomendações e os constrangimentos obtidos durante a pesquisa.

CAPÍTULO II: REVISÃO DA LITERATURA

Este capítulo, é reservado ao desenvolvimento do referencial teórico, estudos e pesquisas relacionados ao tema, trazendo termos-chave e conceitos fundamentais em uma abordagem de estudo.

2.1. Segurança cibernética em Moçambique

A segurança cibernética ou cibersegurança actua dentro de um Espaço Cibernético "Ciberespaço". A evolução do ciberespaço em Moçambique, representa um marco muito importante para o desenvolvimento das infraestruturas tecnológicas no País. De acordo com Miguel (2015, citado por Cepik & Marcelino, 2021, p. 8), "a evolução do ciberespaço moçambicano começou em 1933, com a primeira emissão analógica do Rádio Clube de Moçambique.". Entretanto, a medida que o ciberespaço evolui, surgem novos desafios para segurança dos activos digitais, com destaque as ameaças cibernéticas emergentes que exploram diversas vulnerabilidades existente no ciberespaço. Tal como sustenta a ITU (2007, citado por Cepik & Marcelino, 2021), que a existência de vulnerabilidades e/ou ameaças afecta a segurança de diferentes actores no ciberespaço e do próprio ciberespaço. Nesse contexto, a Cibersegurança é o termo adoptado para a defesa, protecção e resposta a incidentes decorrentes numa infraestrutura de SI. De acordo com a CNCS (2019), define a Cibersegurança sendo:

> Conjunto de medidas e acções de prevenção, monitorização, detecção, reacção, análise e correcção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. (p.16).

A Cibersegurança garante a segurança dos activos no ciberespaço, evitando possíveis riscos, seja de baixo ou alto nível. Segundo von Solms & van Niekerk (2013), a segurança cibernética tem a obrigação de proteger mais do que apenas as informações, dados ou os recursos dos sistemas de informação de um usuário ou de qualquer entidade, pois, não protege apenas o ciberespaço, mas também garante a protecção de todos que lá actuam. Nesse contexto, a cibersegurança apresenta abordagens fundamentais que asseguram a protecção dos sistemas de informação contra diversos ataques cibernéticos no ciberespaço, estabelecendo a confidencialidade, integridade e disponibilidade.

Moçambique participa do evento Índice Global de Segurança Cibernética (GCI) realizado pela União Internacional de Telecomunicações (UIT), onde segundo a Política e Estratégia Nacional de Segurança Cibernética (2021), no relatório de 2018, Moçambique esteve entre os países abaixo em nível de Segurança Cibernética, ocupando a posição 132 em um universo de 194 países. No relatório de 2020, Moçambique subiu 9 posições, tendo passado da posição 132 em 2018 para a posição 123 no universo de 194 países.

Ano	Pontuação regional	Classificação regional	Pontuação global	Classificação global
2018	0.158	26	0.158	132
2020	24.181	23	24.181	123

2020

Pontuação geral	Medidas Legais	Medidas Técnicas	Medidas Organizacionais	Desenvolvimento de capacidades	Medidas de cooperação
24.181	7.46	8.19	4.62	3.92	0

Tabela 1. Moçambique no Índice Global de Segurança Cibernética 2018 e 2020

Fonte: Adaptado pelo autor com base em dados do *Global Cybersecurity Index* (ITUPublications, 2018, 2020)

No mesmo contexto, a Política e Estratégia Nacional de Segurança Cibernética (2021), destaca que a posição obtida nos dois relatórios demostra o compromisso crescente de Moçambique e do Governo com a segurança cibernética a nível nacional, regional, continental e global, aumentando a consciência da sociedade sobre a importância das dimensões de segurança cibernética e o nível de envolvimento do País no desenvolvimento e na segurança do espaço cibernético. No entanto, esse compromisso reflete a necessidade de implementar políticas de prevenção, protecção das infraestruturas críticas do País, e fortalecer a capacidade resposta aos incidentes cibernéticos emergentes no ciberespaço.

2.1.1. Ciberataques

A evolução dos sistemas de informação e a crescente dependência da sociedade em relação a eles, tende a conduzir os agentes mal-intencionados a efectuarem actividades ilegais, procurando explorar as vulnerabilidades e desestabilizar o espaço cibernético. Esse tipo de actividade é designada por ciberataque “ataque cibernético”.

Segundo Powell et al., (2022, p. 3), definem o ciberataque como “um ataque através do ciberespaço, que visa a utilização do ciberespaço por uma empresa com o propósito de perturbar, desactivar, destruir ou controlar maliciosamente um ambiente/infraestrutura informática; ou destruir a integridade dos dados ou roubar informações controladas.”.

É importante que os activos que exploram o ciberespaço garantam a segurança dos seus sistemas de informação, de forma a prevenir potenciais ataques cibernéticos. Nesse contexto, Moçambique tem registado um aumento no número de activos no seu ciberespaço, marcados pela evolução da digitalização, o que impõe desafios para a segurança dos activos, refletidos no crescimento dos números de ciberataques. Como evidenciado na seguinte citação:

“Moçambique está enfrentando uma ameaça crescente de cibercriminalidade, com uma média de 1,5 milhão de ataques cibernéticos por mês (…) essa situação requer atenção imediata e acção estratégica para proteger a infraestruturas do país (…)” (INTIC, 2023b).

De acordo com a Positive Technologies (2023), revela os ciberataques em Africa no início de 2022 ao primeiro semestre de 2023, entre os vários sectores da economia, sendo que nos ataques os cibercriminosos têm como alvo computadores, servidores e equipamentos de rede (85%). Os recursos da *Web* são alvo de 15% dos ataques, sendo que, envolvem diferentes tipos de *malwares* como *Ransomware, RATs* “*Botnets*”, entre outros mostrado na Figura 1:

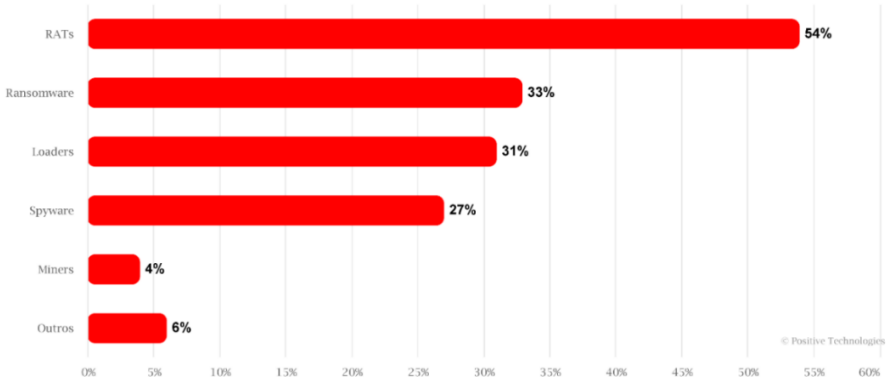


Figura 1. Tipos de *malware* (ataques de *malware* bem-sucedidos em organizações)

Fonte: Adaptado pelo autor (Positive Technologies, 2023)

Os *malware* apresentados na Figura 1 actuam no ciberespaço Moçambicano, refletindo uma enorme ameaça aos activos lá presentes. Diante disso, são descritos alguns

ataques que ocorreram ao longo dos últimos anos, onde segundo Marcelino (2021, p. 121), afirma que “desde 2015 a 2017, Moçambique sofreu ataques do tipo *brute-force*, *Compromised, Malware Dissemination*, *Scanner*, *Defacements*, *Redefacements* e outros.”. No entanto, INAGE (2020c, citado por Cepik & Marcelino, 2021), afirma que moçambique registou mais de 90% foram ataques não-direcionados, nomeadamente: *phishing*, *spam* e *malware* (*vírus*, *worms*, *trojans* e *Bots*) sendo que, os órgãos governamentais e universidades sofreram ataques tipo DDoS e *web defacement*. No período de 2019 á 2020, além do aumento de ataques não-direccionados, foram detectados ataques persistentes, incluindo *ransomware*, *spyware* e quebras de chaves criptográficas, em redes governamentais, empresas e no sistema financeiro.

Esses ataques evidenciam uma diversidade das ameaças cibernéticas têm impactado diferentes sectores no ciberespaço moçambicano. Essas ocorrências demonstram não apenas a complexidade crescente dessas ameaças, mas também a constante evolução das tácticas empregadas por cibercriminosos. Com base em dados colectados, abaixo estão os ataques ou ameaças cibernéticas decorrentes no ciberespaço moçambicano:

Categoria	Ameaças	Ataques
Malware	*Vírus, Worms, Trojans, Ransomware, Spyware*	— —
Engenharia Social	*Phishing, Smishing, Vishing*	—
Negação de Serviço	—	*DDoS*
Web Defacement	—	*Web defacement*
Botnets	*Trojans, Worms, Spyware*	*DDoS, Phishing, Backdoors*

Tabela 2. Ameaças cibernéticas no ciberespaço Moçambicano

Fonte: Elaborado pelo autor com base em dados fornecidos por Cepik & Marcelino (2021) e Marcelino (2021)

Nas estatísticas de *Malwares* apresentadas pela Positive Technologies (2023) conforme ilustrado na Figura 1, destaca-se o *malware RATs* com 54% em ataques a organizações africanas. Trata-se de um tipo de *malware* de acesso remoto perigoso utilizado por cibercriminosos para controlar máquinas infectadas, onde geralmente é um vector de ataque relacionado com servidores de comando e controlo (C&C) *Botnets*. Entretanto, é crucial que os autores de securitização no ciberespaço moçambicano implementarem os mecanismos de segurança robustos focados em ataques de proliferação de *Botnets* e os

malwares envolvidos na execução do mesmo. Essa acção previne a execução de ataques como negação de serviço distribuídos (DDoS), roubo de informações, e distribuição de *malware* em larga escala protegendo os seus activos.

2.1.2. Políticas e legislação de segurança cibernética

Grandes desafios têm sido travados pelo governo Moçambicano para manter a estabilidade do ciberespaço, com foco no seu plano estratégico de segurança cibernética. Em 2021, o Conselho de Ministros de Moçambique, aprovou a Política Nacional de Segurança Cibernética e a Estratégia Nacional de Segurança Cibernética (PENSC). Segundo o Conselho de Ministros: Resolução n.º 69/2021 (2021), a PENSC é um instrumento que irá orientar os esforços de Moçambique na resolução dos novos problemas trazidos pela revolução tecnológica, garantindo a regulamentação de funcionamento do espaço cibernético, o desenvolvimento de capacidade institucional e operacional em matéria de segurança cibernética, a protecção de infraestruturas críticas e activos de informação, o ordenamento da coordenação e colaboração institucional em matéria de segurança cibernética e a promoção de boas práticas no uso das TIC. O Anexo 3 apresenta as leis regulatórias para segurança cibernética em Moçambique.

No entanto para a securitização do espaço cibernético Moçambicano, foram estabelecidos objectivos pela PENSC, sendo um deles estabelecer um mecanismo Nacional de promoção, partilha, cooperação e coordenação em matérias de segurança cibernética, tendo como uma das iniciativas a criação de um Rede Nacional de CSIRT.

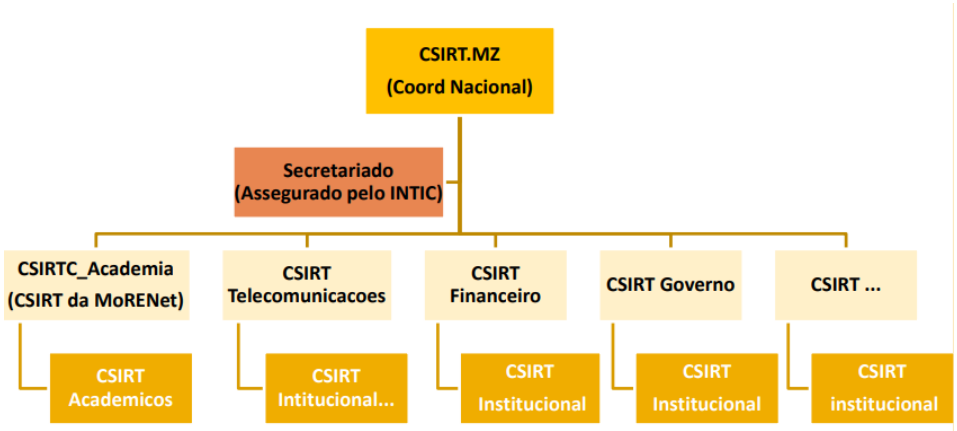


Figura 2. Modelo Hierárquico da Rede Nacional de CSIRT

Fonte: (INTIC, 2023a)

A Figura 2 ilustra o modelo hierárquico da rede Nacional de CSIRT, destacando o nCSIRT e outros CSIRTs que compõem o ciberespaço moçambicano, como o CSIRT do Governo (CSIRT.GOV) e o CSIRT da Academia.

2.2. *Botnets*

O ciberespaço é um ambiente complexo, repleto de diversas ameaças cibernéticas. Apesar da implementação de mecanismos de segurança em infraestruturas de SI, a defesa contra ataques cibernéticos continua sendo um grande desafio, dada a crescente sofisticação das técnicas utilizadas por cibercriminosos. Um exemplo claro, são as *Botnets*. Segundo Ciampa (2014), um ou mais computadores infectados por uma *Botnet* (robô) também conhecido como "*zombies*" eles podem carregar ou transportar consigo uma elevada cargas de *malwares* como cavalos de Troia, *worms*, vírus entre outros, sendo que o computador infectado fica sob o controlo de um atacante.

As *Botnets* representam uma ameaça cibernética perigosa, pois permitem que o cibercriminoso controle várias máquinas comprometidas em simultâneo, sem que os utilizadores percebam. De acordo com Elisan & Hypponen (2013), o cibercriminoso que possui controlo sobre uma rede de *Bots* é conhecido como *Botmaster*.

Um computador ou máquina é comprometida e se torna um *zombie* quando entra em contacto com algum servidor *Botnet*. Existem diversos servidores *Botnets* no ciberespaço sendo eles denominados servidores de comando e controlo (*C&C ou C2*). Segundo Elisan & Hypponen (2013, p. 58), "um servidor comando e controlo (C&C) é um recurso online que altera ou influencia o comportamento dos *Bots*. É o meio pelo qual uma rede de *Bots* é controlada. O *Botmaster* emite instruções para os *Bots* através do servidor C&C da *Botnet,* que serve como interface do *Botmaster* para a *Botnet*.". Essas instruções definem as acções que as máquinas *Bots* devem executar dentro de uma rede *Botnet*.

No entanto, Elisan & Hypponen (2013), enfatizam que o servidor C&C é o componente mais crítico da rede de *Botnets*, pois é nele que reside a capacidade do *Botmaster* controlar e coordenar as acções rede de *Botnets*. Contudo, só é considerada uma rede de *Botnets* quando temos presente o servidor C&C, diferente disso, temos num grupo descoordenado de máquinas independentes comprometidas por *malware*, pois, a capacidade de controlo é uma das principais características de uma rede de *Botnets*.

2.2.1. Arquitectura da rede *Botnets*

A arquitetura de uma rede *Botnet* envolve diferentes abordagens para o funcionamento do seu servidor de controle e comando (C&C), onde segundo Elisan & Hypponen (2013, p. 60), “a estrutura do C&C de uma *Botnet* define como os comandos e as informações importantes são disseminados para os *Bots*.”. Essa garante que os *Bots* recebam as instruções adequadas e operem conforme desejado pelo *Botmaster*. Contudo, os autores Elisan & Hypponen (2013, p. 60), apresentam três (3) tipos de arquitecturas de C&C.

I. Arquitectura centralizada

A arquitectura centralizada é a primordial em redes de *Botnets*. Segundo Shinan et al., (2021), na arquitectura centralizada, o servidor C&C é a ponte de comunicação entre o *Botmaster* e as máquinas *Bots*, isto é, o *Botmaster* tem controlo das maquinas *Bots* a partir de um único ponto (o servidor C&C). Conforme Shinan et al., (2021), destaca que:

- a principal vantagem a coordenação eficaz na comunicação entre as máquinas *Bots* para o seu *Botmaster*, onde facilita a monitorização e o tempo de reação entre o *Botmaster* e as máquinas *Bots*.
- uma vez identificado o servidor C&C, é muito fácil de se derrubar. Também pode sofrer um único ponto de falha, devido a um ataque de DDoS, e o *Botmaster* deixa de poder comunicar com as máquinas *Bots* quando um servidor é derrubado.

II. Arquitectura descentralizada

A arquitectura centralizada caracteriza-se pelo um único ponto de conexão (servidor C&C) entre o *Botmaster* e a máquina *Bot*, sendo uma fragilidade da arquitectura. No entanto, conforme Elisan & Hypponen (2013, p. 61), “os cibercriminosos perceberam isso e criaram uma estrutura de C&C mais resistente, que introduz redundância através de vários nós de C&C. Esse é conhecido como uma arquitectura C&C descentralizada.”.

Na arquitetura descentralizada, conforme Shinan et al., (2021, p. 4), “cada máquina *Bot* pode estabelecer ligações com outras máquinas *Bots* e estes comportam-se como servidores e clientes.”. Isso significa que os *Bots* se comunicam directamente entre si, sendo que, o *Botmaster* pode controlar a rede *Botnet* a partir de outro nó.

Nesse contexto, Hachem et al., (2011), sustentam que a arquitectura descentralizada é muito mais difícil de descobrir e desmantelar. No entanto, o autor observa algumas

limitações como a falta de garantias quanto à entrega das mensagens ou à latência na comunicação entre os nós, pela concepção complexa dos sistemas P2P.

III. Arquitectura híbrida

A presente arquitectura espelha a criatividade dos cibercriminosos diante a criação de novas metodologias de ataque cibernéticos, onde proporciona mais desafios a adopção de mecanismos de segurança para a detecção e mitigação desse tipo de ameaça. Segundo Elisan & Hypponen (2013), os cibercriminosos reconhecendo as vantagens e desvantagens das arquitecturas de C&C de *Botnet* centralizada e descentralizada, sob certas condições dos seus objectivos, para aumentar as hipóteses de sucesso de ter uma rede *Botnet* com maior impacto desse tipo de ataque, os cibercriminosos implementaram uma arquitectura C&C que utiliza as arquitecturas de C&C centralizada e descentralizada. Essa é denominada arquitectura C&C híbrida.

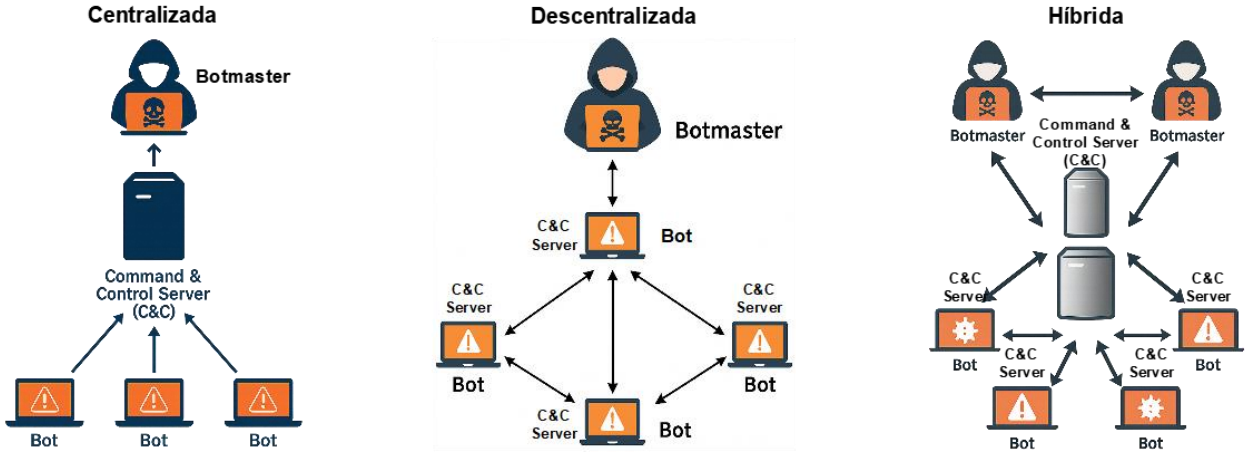


Figura 3. Exemplo das arquitecturas de redes *Botnets*

Fonte: Adaptado pelo autor com base em Shinan et al., (2021) e Ogu et al., (2019)

2.2.2. Principais protocolos da rede *Botnets*

As redes *Botnets* utilizam diferentes protocolos para coordenar as actividades entre os dispositivos infectados *Bots* e os servidores de C&C, variando conforme a arquitetura.

Protocolo	Descrição e Caracteristicas	Arquitectura
IRC (*Internet Relay Chat*)	Comunicação por meio de mensagens de texto em tempo real na *Internet*, com baixa latência, comunicação anônima e fácil configuração.	Centralizada

HTTP (*Hyper Text Transfer Protocol*)	Mistura o tráfego da *Botnet* com tráfego normal da *web*, dificultando a detecção e contornando facilmente *firewalls* e IDS.	Centralizada
P2P (*Peer-to-Peer*)	Comunicação directa entre máquinas *bots*, sem ponto único de falha. São difíceis de detectar e são muito resilientes.	Descentralizada
DNS (*Domain Name System*)	Comunicação entre máquinas *bots* e servidores C&C com uso de fluxos rápidos de domínio (*domain-flux*) e fluxo rápido de IP (*fast-flux*). Dificulta a detecção com alterações em registros NS, geração dinâmica de domínios via DGA e uso de *proxies* maliciosos.	Centralizada Descentralizada

Tabela 3. Protocolos de comunicação utilizados em redes *Botnets*

Fonte: Adaptado pelo autor com base em Shinan et al., (2021) e Hachem et al., (2011)

2.2.3. Ataques da rede *Botnets*

Ataques de Redes *Botnets* podem impactar e instabilizar uma variedade de serviços em uma infraestrutura crítica, com um poder de ataque elevado. Um exemplo desse ataque ocorreu em 2016, como sustentam White et al., (2021), uma *Botnet* designada *Mirai* foi autor de um ataque cibernético de larga escala em DDoS, tendo como vítimas empresas *OVHcloud* e o *Krebs on Security*. Esse foi conhecido como um dos maiores ataques DDoS em rede *Botnet*, que atingiu um pico sem precedentes de 1 Tbps e estima-se que tenha usado cerca de 145.000 dispositivos.

I. Negação de serviço distribuídos (DDoS - *Distributed Denial of Service***)**

Termos como "paralisar", "inundar" e "sobrecarregar" são utilizados para descrever ataques do tipo DDoS (*Distributed Denial of Service* - Negação de Serviços Distribuídos), onde conforme Gupta & Dahiya (2021), afirmam que nesse ataque o tráfego malicioso é gerado a partir de múltiplas fontes distribuídas, sendo que o tráfego é enviado por máquinas *Bots* que fazem parte de uma rede de máquinas comprometidas.

No entanto, Barbosa et al., (2014, p. 109), sustentam que “este tipo de ataque necessita de uma estrutura que pode ser provida inteiramente pela arquitectura padrão de uma *Botnet*, onde os *bots* são utilizados para sobrecarregar o alvo de acordo com as instruções do responsável pela coordenação geral do ataque.”. Nesse contexto, entende-

se que através dessa estrutura, os *Bots* podem executar o ataque de forma coordenada, e quanto maior for o número de dispositivos mais amplificada é o ataque.

II. Envio de *Spam*

Dos diferentes ataques existentes no ciberespaço, temos o ataque *spam*, um dos grandes autores maliciosos mais persistentes e generalizados do ciberespaço. De acordo com Elisan & Hypponen (2013, p. 66), os *Bots* geradores de *spam* são chamados *spambots*. As *Botnets* são uma ferramenta eficiente para a propagação de mensagens *spam* em massa, que tentam enganar as vítimas, onde segundo Ogu et al., (2019), destacam que o *spam* de *Botnets* está envolvida no envio e disseminação diária de grandes quantidades de *spamware* e procura explorar utilizadores ingénuos, normalmente através de *e-mails*.

III. Espionagem e roubo de informações

As redes *Botnet* não são apenas usadas para realizar ataques DDoS ou enviar *spam*. Elas também são utilizadas para realizar a espionagem cibernética e roubo de informações ou dados sensíveis. De acordo com Hachem et al., (2011), algumas redes de *Botnets* além de capturar o tráfego que passa pelas máquinas comprometidas (*Bots*), também podem captar actividades de comandos efectuados pelas máquinas das vítimas.

Essas técnicas demonstram a capacidade de o atacante explorar vulnerabilidades para colectar informações de forma discreta em grande quantidade. De acordo com Ogu et al., (2019), revelam que esta rede de *Botnets* é utilizada para extrair informações através da *Internet* em grandes quantidades, numa base diária e estão também presentes nas operações de espionagem de cibercrime coordenados.

2.2.4. Técnicas de detecção de *Botnets*

A implementação de metodologias de segurança em infraestruturas de sistemas de informação tem-se revelado uma prioridade fundamental na protecção da informação. Nesse contexto, técnicas de detecção de ameaças de redes de *Botnets* representam um desafio contínuo devido à sua natureza sofisticada e agressiva. Shinan et al., (2021), afirmam que tem havido um interesse crescente em abordagens relacionadas à detecção de *Botnets*. Contudo, a Figura 4 apresenta técnicas de detecção de redes de *Botnets*.

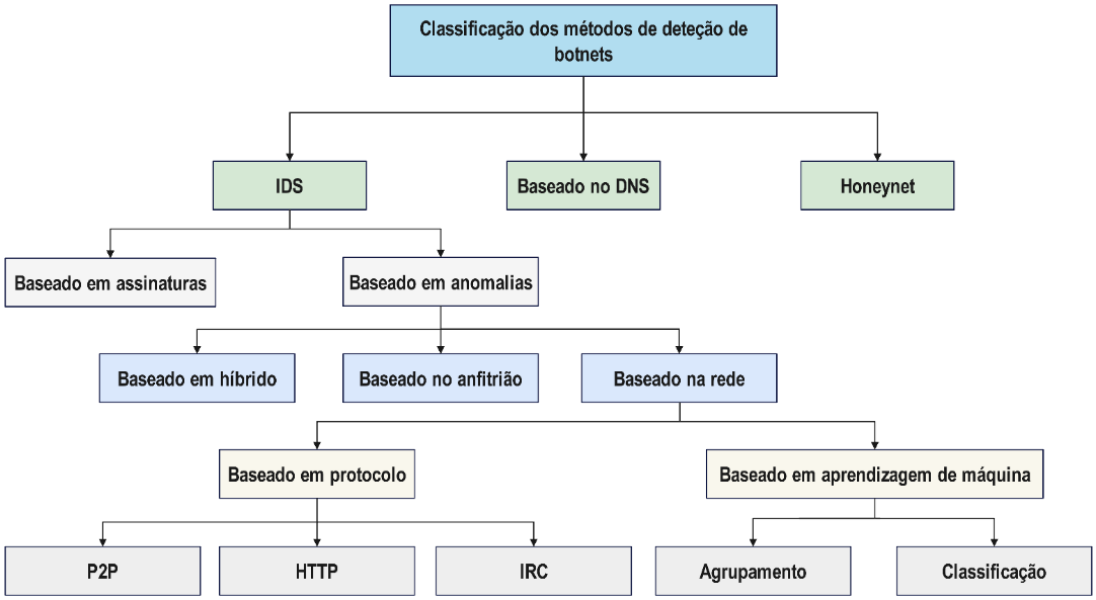


Figura 4. Classificação das técnicas de detecção de redes de *Botnets*

Fonte: Adaptado pelo autor com base em Shinan et al., (2021)

I. Sistemas de Detecção de Intrusão (IDS - *Intrusion Detection Systems*)

Uma das metodologias usadas em segurança cibernética, são os Sistemas de Detecção de Intrusões (IDS - *Intrusion Detection Systems*), que segundo Sadiqui (2020, p. 102), "é um detector que pode analisar pacotes que trafegam por uma ou mais conexões de rede para detectar actividades suspeitas". No entanto, para a identificação ameaças associadas a redes de *Botnets*, o IDS usa duas (2) abordagens: detecção baseada na assinatura e a baseada na anomalia.

a) Baseado na assinatura (*Signature-based IDS*)

A detecção baseada em assinaturas de acordo com Mammunni (2020), é a forma mais simples de detecção que utiliza as assinaturas/padrões específicos, tais como, sequências de bytes/instruções no tráfego de rede para a detecção de *Botnets*. Essa analisa e compara padrões conhecidos de ameaças, como sustentam Asha et al., (2016), baseia-se na comparação das informações recolhidas de redes de *Botnets* (armazenada em um banco de dados) com os pacotes capturados, que são extraídas determinadas informações como endereço IP e as portas (origem e destino).

Um aspecto a ser considerado fundamentado por Shinan et al., (2021), essa técnica de detecção necessita de actualizações frequentes, sendo facilmente violado ou modificado

por ataques polimorfos, como *Zero Day*. Além disso, só é eficiente para detecção de *Botnets* conhecidas, pois suas características de ataque já estão previstas em um banco de dados de assinaturas, sendo ineficaz contra *Botnets* desconhecidos (*Zero Day*).

b) Baseado na anomalia (*Anomaly-based IDS*)

A técnica de detecção baseada na anomalia é uma abordagem a análise do tráfego de rede para a identificação de padrões de comportamento suspeitos. De acordo com Asha et al., (2016), as anomalias são o comportamento inesperado na rede e não o normal, e a detecção baseada na anomalia utiliza o comportamento da rede para identificar as *Botnets*, sendo feita uma comparação do comportamento da rede actual e anterior. O novo comportamento é aceite ou utilizado para iniciar eventos de detecção de anomalias. Segundo Karim et al., (2014), a ideia básica vem da análise de várias irregularidades no tráfego de rede, incluindo o tráfego que passa por portas invulgares, alta latência, aumento do volume de tráfego, e o comportamento do sistema que indica actividades maliciosas na rede. Entretanto, diferente das técnicas baseados em assinaturas que se limita em ameaças conhecidas, Mammunni (2020), sustenta que a técnica baseada em anomalia é capaz de detectar *Botnets* e ataques previamente desconhecidos, superando a limitação da outra abordagem de detecção. A detecção baseada na anomalia, está subdividida em (3) três métodos, sendo baseada: na rede, no anfitrião e em híbrido.

- **Detecção de anomalias baseada na rede (*Network-Based IDS* - NIDS):** De acordo com Kizza (2024), NIDS é responsável por detectar trafego anómalo, que possa ser considerado não autorizados e prejudiciais na rede. No contexto da detecção de *Botnets*, Asha et al., (2016), afirmam que máquinas *Bots* apresentam padrões de tráfego semelhantes, o que facilita distingui-los do tráfego normal.
- **Detecção de anomalias baseada no anfitrião (*Host-Based IDS* - HIDS):**.De acordo com Kizza (2024), é uma técnica voltada para identificar actividades maliciosas em uma máquina. Monitora registos (*logs*) do sistema operacional, e compara as novas entradas de registos com assinaturas de ataque, indicando actividades ilegítimas. Segundo Xu et al., (2011, citado por Karim et al., 2014), pode ser utilizada para verificar se uma máquina está ou não infectada pelo *Bot*.

- **Detecção de anomalias baseada em Híbrido (***Hybrid-Based IDS***):** A detecção baseado em hibrido conforme Shah et al., (2015), pode ajudar a detectar anomalias e utilizações abusivas, combinando a detecção de anomalias baseado no anfitrião (HIDS) e a detecção de anomalias baseado na rede (NIDS).

II. Sistema de Nomes de Domínio (DNS - *Domain Name System***)**

As redes de *Botnets* utilizam a consulta DNS como meio de comunicação com seus servidores de C&C. Recorrer a análise do tráfego DNS, torna-se fundamental para identificar actividades relacionadas a redes de *Botnets*, metodologia conhecida como detecção de *Botnets* baseada em DNS, que abrange diferentes técnicas como:

- Identificação de Domínios Algoritmicamente Gerados (DGAs): Li et al., (2017), menciona que entre as diversas formas de *Botnets*, as baseadas em DGAs, são umas das mais destrutivas e difíceis de detectar. Nessa, estudos recentes têm focado na análise do tráfego DNS para identificar *Botnets* baseados em DGAs;
- Detecção de Fluxos Maliciosos de DNS: Perdisci et al. (2009 citado por Alieyan et al., 2017), propuseram a detecção de anomalias de serviços de fluxo rápido (*Fast-Flux Service Networks* - FFSN), centrada na análise passiva de traços DNS recursivos (*Recursive* DNS - RDNS), pois *Botmasters* utilizam vários nomes de *Domain-Flux*, com vista a escapar da lista negra de domínios (*DNS Blacklisting*);
- Análise de Comportamento de Resolução DNS: Shinan et al., (2021), afirmam que a através do monitoramento da execução de consultas DNS pode-se detectar as redes de *Botnets*, sendo que a consulta feita pelas máquinas *Bots* é normalmente feita através de um fornecedor de DNS dinâmico (*Dynamic DNS* - DDNS).

III. *Honeynet*

Outra metodologia usada para a detecção de anomalias relacionadas a redes *Botnet* é a implementação de um sistema *Honeynet*. Conforme Karim et al., (2014), uma *Honeynet* é geralmente utilizada para recolher informações de máquinas *Bots* para análise posterior, a fim de medir a tecnologia utilizada, as características e a intensidade do ataque gerado pela rede *Botnet*. Assim sendo, as informações recolhidas das máquinas

Bots são utilizadas para descobrir o servidor de C&C envolvido, as susceptibilidades desconhecidas, as técnicas, e ferramentas utilizadas pelo atacante (*Botmaster*).

2.3. Soluções de análise de tráfego rede na detecção de *Botnets*

As *Botnets* utilizam componentes da infraestrutura de redes para comunicar-se com servidores de comando e controlo (C&C) e para interagir com outras redes de *Botnets*. De acordo com Ribeiro (2020, p. 21), "uma das soluções mais comuns para detecção de *Botnets* consiste em desenvolver sistemas para analisar o tráfego da rede e identificar componentes maliciosos.". Neste contexto, a análise de tráfego de rede surge como aliado muito fundamental na identificação e mitigação de anomalias relacionados a *Botnets*, através da monitorização e inspeção do tráfego de rede, detectando padrões e comportamentos que podem indicar a presença de *Botnets*.

2.3.1. Soluções de análise de tráfego rede

I. *NetFlow*

O *NetFlow* é um protocolo desenvolvido pela Cisco Systems, Inc. De acordo com a Cisco Systems, Inc (2013), o *NetFlow* é uma tecnologia da Cisco IOS que fornece estatísticas sobre os pacotes que trafegam pelo roteador (*router*), onde o mesmo fornece dados que permitem a monitorização da rede e da segurança, o planeamento da rede, a análise do tráfego e a contabilidade IP. Segundo Claise (2004), destaca que os serviços *NetFlow* fornecem aos administradores de rede acesso a informações de fluxo IP das suas redes de dados. Dispositivos de rede como roteadores e *switches*, recolhem dados de fluxo e exportam para os colectores, dispositivo externo denominado: "colector *NetFlow"*.

No contexto do *NetFlow*, existe uma terminologia designada fluxo IP (*IP Flow*), que é definido como "um conjunto de pacotes IP que passam por um ponto de observação na rede durante um determinado intervalo de tempo." Claise (2004, p. 04). De acordo com a Cisco Systems, Inc., (2006), um fluxo IP é baseado num conjunto de 5 a 7 atributos de pacotes IP, esses que compõem ou que são utilizados pelo *NetFlow*, nomeadamente: endereço IP de origem; endereço IP de destino; porta de origem; porta de destino; tipo de protocolo da camada 3; classe de serviço; e interface do roteador ou do *switch*. Esta metodologia de determinação de um fluxo é escalável, pois uma grande quantidade de

informações de rede é condensada numa base de dados *NetFlow* denominada *cache NetFlow*. A Figura 5 ilustra a criação de um fluxo no *cache NetFlow*:

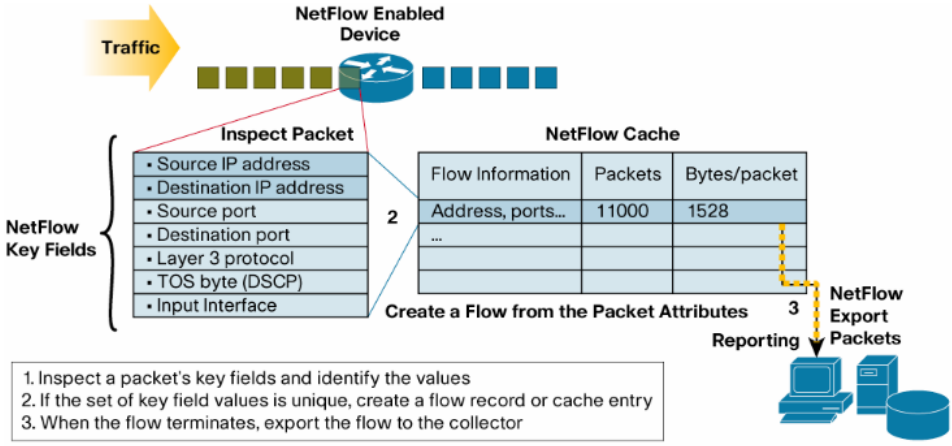


Figura 5. Criação de um fluxo na *cache* do *NetFlow*

Fonte: Cisco Systems, Inc, (2008)

- Endereço de origem: indica quem está a originar o tráfego;
- Endereço de destino: indica quem está a receber o tráfego;
- Portas: caracterizam a aplicação que está a utilizar o tráfego;
- Classe de serviço: avalia a prioridade do tráfego;
- Interface do dispositivo: mostra como o tráfego é utilizado pelo dispositivo de rede;
- Total de pacotes e *bytes*: Indica a quantidade total de tráfego gerado.

O *NetFlow* é composto pelos seguintes componentes no seu funcionamento:

- Exportador *NetFlow*: Segundo Claise (2004), monitoriza os pacotes que entram num ponto de observação e cria fluxos a partir dos pacotes. As informações dos fluxos são exportadas sob a forma de registos de fluxo para o colector *NetFlow*;
- Colector *NetFlow*: "recebe registos de fluxo de um ou mais exportadores. Processa o(s) pacote(s) de exportação recebido(s), ou seja, analisa e armazena as informações do registo de fluxo. Os registos de fluxo podem ser opcionalmente agregados antes de serem armazenados no disco rígido." (Claise, 2004, p. 4);
- Analisador *NetFlow*: "é uma ferramenta que processa e analisa registos *NetFlow* recebidos e armazenados por um colector de fluxo. Essa análise de fluxo de tráfego permite que crie uma imagem do tráfego e do volume da rede." (IBM, s.d.).

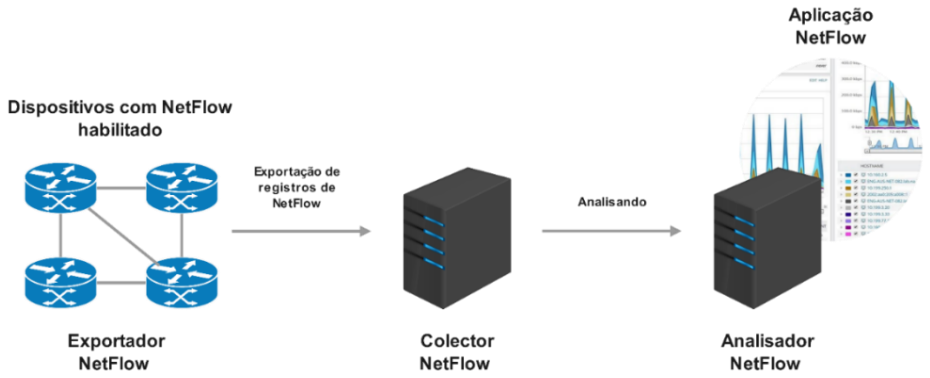


Figura 6. Demonstração simplificada do funcionamento de *NetFlow*

Fonte: Adaptado pelo autor com base em (IPCisco, s.d.)

II. *Zeek*

"O *Zeek*, anteriormente conhecido como *Bro*, é uma plataforma de monitorização do tráfego de rede que foi desenvolvida em 1994 por Vem Paxson do Centro de Investigação da *Internet* (ICIR) no Instituto Internacional de Ciência da Computação (ICSI)." (Roshandel, 2022, p. 7). De acordo com Zeek Documentation (2024), o *Zeek* é utilizado como monitor de segurança de rede (NSM) para apoiar investigações de actividades suspeitas ou maliciosas, sendo que suporta uma ampla gama de tarefas de análise de tráfego além do domínio da segurança, incluindo medição de desempenho e solução de problemas. O *Zeek* caracteriza-se por gerar um conjunto extenso e exaustivo de registos (*logs*) que descrevem a actividade da rede, incluindo *logs* ligações na rede e transcrições da camada de aplicação. Estes registos incluem, as sessões HTTP com seguintes detalhes: URIs solicitados, cabeçalhos de chave, tipos MIME e respostas do servidor; as solicitações de DNS com respostas; os certificados SSL, entre outros.

Nesse contexto, Muhammad et al., (2023), ressalta que o *Zeek* gera muitos registos no seu sistema, sendo o *conn.log* o registo mais importante na detecção de anomalias, isso porque o *conn.log* é o primeiro registo gerado no estabelecimento de uma ligação, pelo que o *conn.log* é a base dos outros registos gerados pelo *Zeek*. O *conn.log* mantém alguns registos gerados a partir da camada 3 e da camada 4 no modelo OSI (*Open Systems Interconnection*). Abaixo alguns registos importantes na execução do *Zeek*:

- conn.log (conexão): Regista as conexões TCP, UDP e ICMP;
- dhcp.log (concessão): Regista as concessões DHCP de endereços IP;

- dns.log (actividade): Regista as actividades relacionadas ao DNS;
- http.log (requisições e respostas): Regista as requisições e respostas do HTTP;
- ftp.log (actividade): Regista actividades relacionadas ao FTP.

a) Arquitectura do *Zeek*

A arquitetura do *Zeek* é composta por dois componentes principais: o seu Motor de Eventos ou Núcleo (*Event Engine*) e o Interpretador de *Scripts* (*Script Interpreter*). De acordo com Zeek Documentation (2024), categoriza-os da seguinte forma:

- Motor de eventos (*event engine*): reduz o fluxo de pacotes de entrada numa série de eventos de nível superior. Estes eventos reflectem a actividade da rede em termos neutros, em termos de política, ou seja, descrevem o que foi visto, mas não o porquê, ou se é significativo;
- Interpretador de *Scripts* (*Script Interpreter*): executa um conjunto de manipuladores de eventos escritos na linguagem de *script* personalizada do *Zeek.* Estes *scripts* podem exprimir a política de segurança de um sítio, por exemplo, as acções a tomar quando o monitor detecta diferentes tipos de actividade.

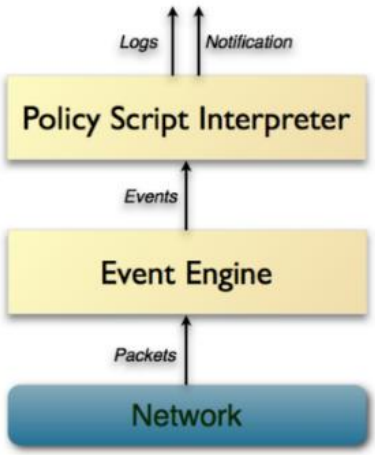


Figura 7. Arquitectura do *Zeek*

Fonte: Zeek Documentation (2024)

Entretanto, Zeek Documentation (2024), destaca que o *Zeek* por padrão inclui funcionalidades incorporadas para uma série de tarefas de análise e detecção, incluindo a extração de ficheiros de sessões HTTP, a detecção de *malware* através da interface com registos externos, a detecção de ataques SSH de força bruta, e muito mais. A

linguagem de *script* do *Zeek* proporciona um conjunto muito amplo de abordagens diferentes para detectar actividades maliciosas na rede, onde inclui a detecção de uso indevido semântico, detecção de anomalias e análise comportamental.

III. *sFlow*

"O *sFlow* foi desenvolvido pela *InMon Inc*. e tornou-se um padrão industrial definido na RFC 3176." (B. Li et al., 2013, p. 55). Segundo Phaal et al., (2001), o *sFlow* é uma tecnologia para monitorizar o tráfego em redes de dados que contêm *switches* e roteadores. O *sFlow* define os mecanismos de amostragem implementados em um agente *sFlow* para monitorizar o tráfego, o MIB *sFlow* para controlar o agente *sFlow* e o formato dos dados de amostra utilizados pelo agente *sFlow* quando encaminha os dados para um colector de dados central. Contudo, o sistema de monitorização *sFlow* consiste em agente *sFlow* (incorporado num *switch*, roteador ou numa sonda autónoma) e num colector de dados central, ou analisador *sFlow*. De acordo com Phaal et al., (2001), os três (3) parâmetros no funcionamento do *sFlow*, tem as seguintes características:

- Mecanismo de amostragem: o agente *sFlow* utiliza a amostragem para capturar estatísticas de tráfego e os encaminha através dos datagramas *sFlow* para um analisador *sFlow*;
- MIB *sFlow:* define uma interface de controlo para um agente *sFlow* que fornece um mecanismo normalizado para o controlar e configurar remotamente;
- Formato dos Dados de Amostra: especifica um formato para o agente *sFlow* enviar dados de amostragem a um colector de dados central.

Na Figura 8 são apresentados os elementos básicos do sistema *sFlow,* conforme descrito por Phaal & Lavine (2004):

- Agente *sFlow*: fornece uma interface para configurar as instâncias *sFlow* num dispositivo via linha de comando e/ou SNMP;
- Colector *sFlow*: recebe datagramas *sFlow* de um ou mais agentes *sFlow* e configura instâncias *sFlow* utilizando configurações fornecidas pelo Agente *sFlow*;
- Datagrama *sFlow*: é um datagrama UDP que contém os dados de medição e informações sobre a fonte e o processo de medição.

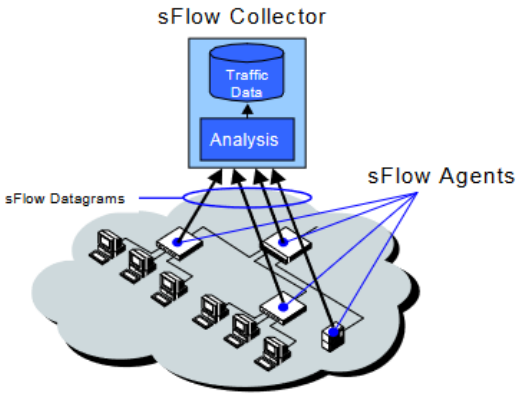


Figura 8. Elementos básicos do sistema *sFlow*

Fonte: sFlow (2003)

2.3.2. Análise das soluções na detecção de *Botnets*

Durante o subcapítulo 2.3.1, foram apresentados três (3) diferentes tipos de soluções de análise de tráfego de rede: *NetFlow, Zeek* e *sFlow*. Essas soluções destacam-se por sua capacidade de monitorar o tráfego de rede, permitindo a colecta e análise de dados que refletem o comportamento da rede. Além disso, são aplicáveis em diversos cenários, a identificação de anomalias, a otimização de desempenho, entre outros.

De acordo com Amini et al., (2014), em seu artigo sobre uma abordagem para a detecção de *Botnets* utilizando registos de dados do protocolo *NetFlow* e técnica de *clustering*, afirmam que os mecanismos baseados no protocolo *NetFlow* para a detecção de *Botnets* contém algumas vantagens em relação a outras soluções, como o baixo volume de dados, a simplicidade de cálculo, o menor número de falsos positivos, entre outros aspectos. No entanto, é importante frisar que esse mecanismo pode enfrentar algumas limitações, como sustentam Bilge et al., (2012), os sistema de detecção de redes de *Botnets* baseado na análise dos dados *NetFlow* pode produzir resultados de conter alguns falsos positivos, pela sua natureza de poder fornecer informações limitadas sobre as actividades reais que são realizadas numa rede.

Por outro lado, temos abordagens de detecção de *Botnets* utilizando o *Zeek* como solução. Gallagher (2021), em sua tese centra-se numa solução de detecção de *malware*, relacionado a servidores C&C *Botnets* utilizando o *Zeek*, que busca máquinas infectadas *Bots* com a utilização de dados de fluxo de rede sob a forma de registos de ligação *Zeek,* esse é responsável por gerar *logs* de conexões que capturam actividades

detalhadas da rede. No entanto, Gallagher (2021), afirma que devido a capacidade do *Zeek* registar todos os aspectos de uma conexão de rede, é possível identificar padrões de tráfego rede que possam indicar actividades de *Botnets*.

Para completar, Lu & Wang (2016), desenvolveram um mecanismo de defesa contra o ataque de inundação DDoS baseado em *Botnet* através da combinação da Rede Definida por *Software* (SDN) e da tecnologia de fluxo de amostra (*sFlow*). O mecanismo concentra-se em um algoritmo de detecção baseado na inferência estatística utilizando os dados de tráfego de rede colectados pelo *sFlow*, onde o algoritmo é capaz de identificar ataques de DDoS orquestrados por *Botnets* originado em ambiente SDN ao analisar a distribuição e colaboração dos fluxos de rede.

As soluções apresentadas revelam diferentes mecanismos para a detecção de *Botnets*. Cada uma pode oferecer vantagens ou limitações, dependendo do contexto de aplicação. A tabela a seguir resume esses aspectos com base em diferentes estudos:

Característica	*NetFlow*	*Zeek (Bro)*	*sFlow*
Tipo de Dados Colectados	Colecta metadados dos fluxos de rede	Análise detalhada do tráfego de rede	Colecta amostras de pacotes de dados
Falsos Positivos e Negativos	Moderado, colecta informações básicas dos fluxos de rede	Baixo, devido à riqueza dos dados capturados	Alto, devido a perda de pacotes críticos da rede
Flexibilidade de Análise	Limitada, metadados oferecem dados menos detalhados	Alta, permite análise personalizada e criação de *scripts*	Moderada, análise eficiente, mas com menor profundidade
Escalabilidade	Alta, em redes de grande porte	Moderada, pois pode exigir mais recursos	Alta, em redes grande volume de tráfego
Eficácia na Detecção de *Botnets*	Boa, identifica padrões anômalos e suspeito no tráfego	Excelente, devido à inspeção profunda de pacotes	Moderada, pode perder eventos devido à amostragem
Documentos Relacionados	Amini et al., (2014); Barbosa et al., (2014); Bilge et al., (2012).	Muhammad et al., (2023); Roshandel, (2022); Zeek Documentation, (2024).	B. Li et al., (2013); Lu & Wang (2016); sFlow (2003).

Tabela 4. Características de soluções para detecção de anomalias em redes

Fonte: Adaptado pelo autor

CAPÍTULO III: CASO DE ESTUDO

Este capítulo, é reservado a apresentação do Caso de Estudo. O caso de estudo se concentra no projecto MoRENet (Rede de Instituições de Ensino Superior e de Investigação de Moçambique), está que está afecto ao INAGE, IP (Instituto Nacional do Governo Electrónico, Instituto Público). A escolha do caso de estudo deu-se na oportunidade de ilustrar as abordagens teóricas discutidas ao longo da pesquisa acerca da “segurança cibernética”.

3.1. Instituto Nacional do Governo Electrónico, Instituto Público (INAGE, IP)

O Instituto Nacional de Governo Electrónico, Instituto Público, abreviadamente designado por INAGE, IP, criado pelo Decreto nº61/2017 de 6 de Novembro e ajustado pelo Decreto nº35/2022 de 22 de Julho, é uma pessoa colectiva de direito público, de categoria A, responsável pela coordenação e prestação de serviços de Governo Electrónico, dotada de personalidade jurídica, autonomia administrativa, financeira e patrimonial, com a missão fundamental de prestar serviços públicos digitais com vista a melhorar a eficiência, eficácia e modernização da Administração Pública na sua interacção com o cidadão.

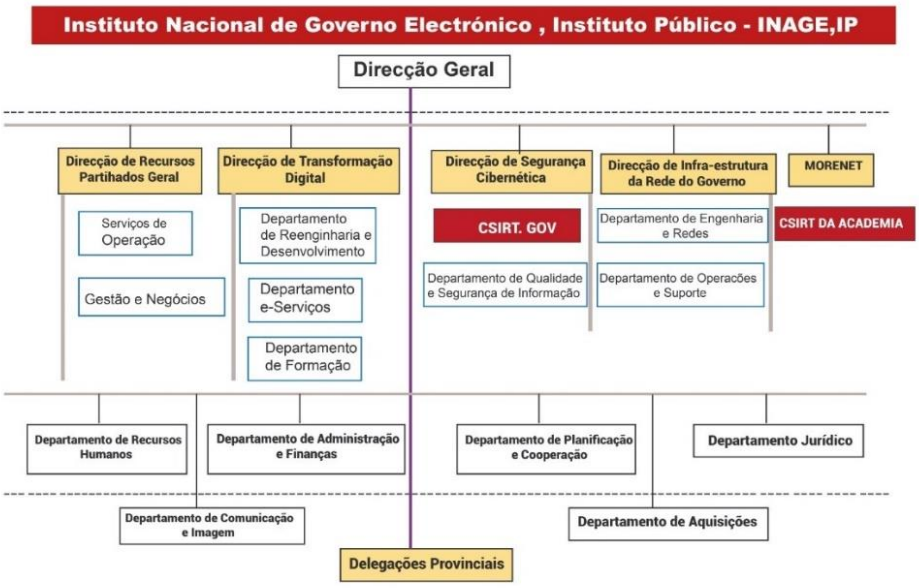


Figura 9. Organograma INAGE, IP

Fonte: (INAGE, IP, s.d.)

3.1.1. Rede de Instituições de Ensino Superior e de Investigação de Moçambique (MoRENet)

A MoRENet (*Mozambique Research and Education Network* - Rede de Instituições de Ensino Superior e de Investigação de Moçambique), foi estabelecida como projecto pelo Ministério da Ciência e Tecnologia, em 2005. A MoRENet é uma rede de comunicação de dados de âmbito Nacional que interliga instituições acadêmicas do ensino superior, de investigação e do ensino técnico-profissional, e se propõe a usar as Tecnologias de Informação e Comunicação (TICs) para facilitar a troca e disseminação de conhecimento, promover a investigação, reduzir a distância entre investigadores, docentes, estudantes e outros profissionais da academia e aproximar as instituições científicas ao cidadão e ao sector privado.

I. Objectivos

- Prestar serviços de interconexão entre as instituições beneficiárias e de acesso à *Internet* para as Instituições Nacionais de Ensino Superior, de Ensino Técnico Profissional, e Pesquisa, com sustentabilidade económica;
- Interligar o Sistema Nacional de Ensino Superior, de Ensino Técnico Profissional, e da Ciência, Tecnologia e Inovação para o mundo exterior através do estabelecimento de parcerias institucionais com outras redes de Ensino Superior e Pesquisa em África, Europa, Ásia e América;
- Servir de mecanismo de divulgação e de transferência de conhecimento e de tecnologias entre os membros da comunidade académica em Moçambique; e
- Promover a colaboração entre as instituições nacionais de Ensino Superior, de Ensino Técnico Profissional, de Pesquisa, e o Sector Privado.

II. Missão e Visão

- Missão: “Integrar as instituições nacionais de ensino superior, de ensino técnico profissional, e de investigação numa rede nacional de comunicação de dados de alto desempenho, disponibilizando serviços de qualidade, seguros com sustentabilidade económica, tecnológica e institucional de modo a constituir-se como um parceiro fundamental no desenvolvimento da comunidade académica e científica Moçambicana.”.

- Visão: “Ser uma plataforma comum para fornecer serviços partilhados de comunicação de dados de alto desempenho, seguros e a custos acessíveis para as instituições de ensino superior, de ensino técnico-profissional, e de investigação.”.

III. Serviços

São serviços da MoRENet os seguintes:

- Conectividade; Sistemas e aplicações; CSIRT; HPC – Computação de Alto Desempenho; Academia; e Serviço Partilhado.

IV. Estrutura da rede MoRENet

A topologia actual da rede MoRENet é composta por seis (06) Pontos de Presença (PoPs) distribuídos pelo país e conectados em malha através de ligações dedicadas com capacidades entre 200 Mbps e 500 Mbps. Um número considerável de instituições beneficiárias da MoRENet, entre instituições de Ensino Superior, de Investigação e do Ensino Técnico Médio Profissional, estão conectadas aos PoPs através de ligações dedicadas com capacidades compreendidas entre 20 Mbps e 54 Mbps, quatro (4) ligações dedicadas de 155 Mbps cada, que conectam a rede MoRENet ao provedor de trânsito internacional – *UbuntuNet Alliance* e ainda uma (1) ligação dedicada de 54 Mbps que conecta a rede MoRENet ao ponto de troca de trafego nacional (MozIX – *Mozambique Internet Exchange*).

Os seis (06) Pontos de Presença (PoPs), estão situados na:

- Cidade de Maputo – edifício sede do Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profissional actualmente Ministério das Comunicações e Transformação Digital – PoP do MCTESTP (MCTD);
- Província de Maputo, distrito da Manhiça – edifício da Empresa Nacional de Parques de Ciência e Tecnologia– PoP de Maluana;
- Cidade da Beira – instalações da Universidade Pedagógica, campus da Ponta-Géa – PoP da Beira;
- Cidade de Nampula – instalações da Universidade Pedagógica, campus de Napipine – PoP de Nampula;

- Cidade de Tete – instalações da Universidade Pedagógica, campus de Cambinde – PoP de Tete;
- Cidade de Lichinga – instalações da Universidade Pedagógica, campus Chiuaula – PoP de Lichinga.

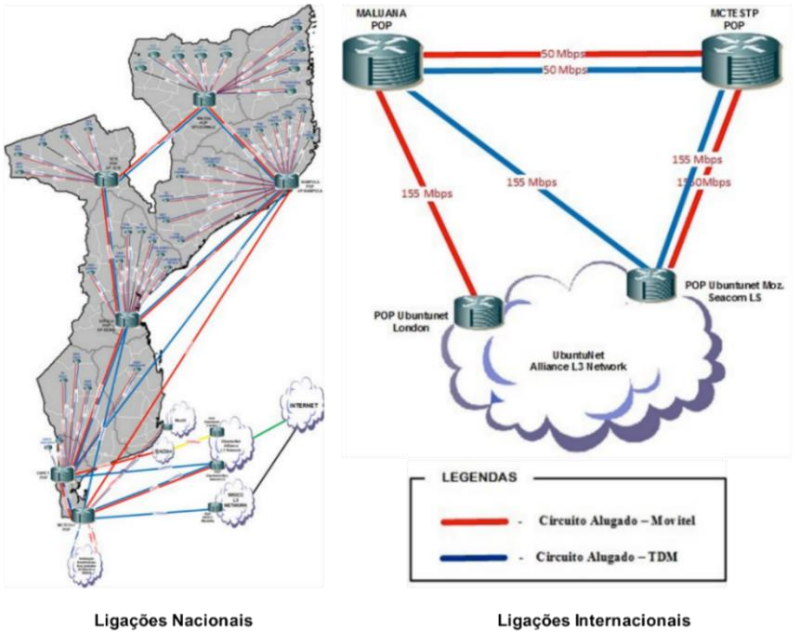


Figura 10. Ligações Nacionais e Internacionais

Fonte: Adaptado pelo autor com base no Modelo de Negocio da MoRENet (2017)

Dos seis (6) PoPs, os PoPs de Maluana e MCTESTP (MCTD) apresentam-se como os principais, sendo listado alguns dos equipamentos presentes nesses PoPs e as suas especificações no Anexo 4.

V. MoRENet CSIRT (CSIRT da Academia)

Nas suas acções de estabelecimento de infraestrutura de conectividade e interligação das instituições académicas e de investigação, a MoRENet tem as suas atenções voltadas a questões de segurança de dados e de informação dos seus membros bem como para a própria infraestrutura da rede. A MoRENet-CSIRT designada CSIRT da Academia foi estabelecida a 03 de Novembro de 2018 e é membro da rede Nacional de CSIRTs. O CSIRT da Academia é o Equipa de Resposta a Incidentes de Segurança Cibernética da MoRENet para a comunidade académica e científica Nacional, sendo membro da rede Nacional de CSIRTs (Figura 2).

- Objectivo:

  “O objectivo principal é estabelecer um único ponto de contacto para todos os incidentes de segurança envolvendo os membros da MoRENet e coordenar o tratamento e resposta a incidentes e a troca de informações críticas entre as várias partes interessadas.”.

- Missão:

  “Coordenar a resposta a incidentes de segurança cibernética no seio da comunidade académica e científica nacional, prestar assistência na resolução de incidentes de segurança, disseminar alerta de ameaças eminentes, promover o estabelecimento de CSIRTs nos seus constituintes, bem como melhorar o conhecimento geral das técnicas de segurança entre os membros.”.

As gamas de endereços IP abrangidos no âmbito de actuação do CSIRT da Academia são:

- 41.94.0.0/16; 196.3.96.0/21; 196.13.101.0/24; 2C0F:F140::/32.

3.1.2. Apresentação de dados: Situação actual da MoRENet

O processo de apresentação de dados de acordo com Barbetta (1998, p. 66, citado por Zanella, 2013), “compreende a organização dos dados de acordo com as ocorrências dos diferentes resultados observados”, onde ao longo da descrição de dados podem ser ilustrados gráficos e tabelas. No entanto, como mencionado no subcapítulo 1.4.5, as técnicas escolhidas de recolha de dados, é a entrevista e o questionário, dirigido a equipa dos profissionais do CSIRT da MoRENet. Essas técnicas permitiram obter percepções sobre o estado actual da segurança cibernética na infraestrutura da MoRENet, com destaque a ameaças associadas a redes *Botnets*.

I. Situação da Segurança Cibernética na MoRENet (CSIRT da Academia)

Quanto ao estado actual da segurança cibernética na infraestrutura da MoRENet, conforme os profissionais da MoRENet que participaram do questionário e da entrevista, 67% dos respondentes avaliaram a segurança cibernética como moderada (média), e 33% avaliaram como boa. Porém, foi revelado alguns desafios e preocupações fundamentais, onde segundo um entrevistado:

"o estado actual da área de segurança na MoRENet ainda não atingiu um nível óptimo, pois existem alguns défices. Primeiramente, há uma escassez de profissionais capacitados para operar nessa área na MoRENet. Além disso, as questões relacionadas à assistência em segurança às instituições beneficiárias, também impactam negativamente a na segurança da infraestrutura."

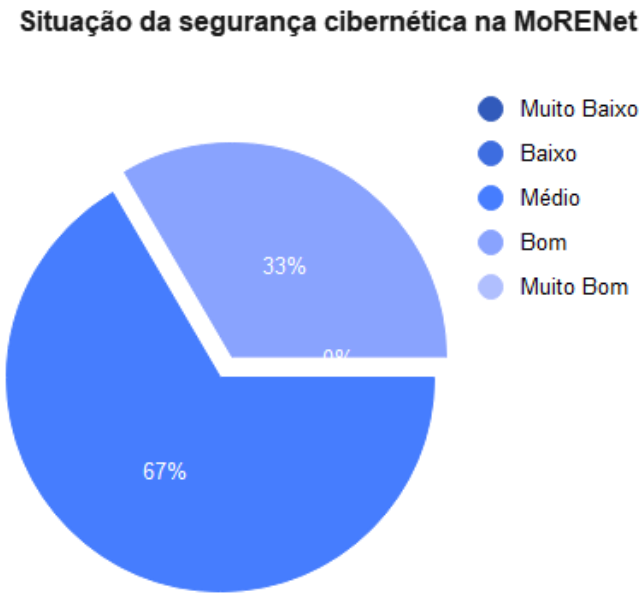


Figura 11. Avaliação da situação actual da segurança cibernética na MoRENet

Fonte: Elaborado pelo Autor

Nessa, é apresentado a seguir dois (2) pontos levantados que visam a compreender mais fundo a situação da segurança cibernética na MoRENet, destacando:

a) Principais ameaças cibernéticas na MoRENet

A MoRENet como uma rede de grande escala, enfrenta várias ameaças cibernéticas que podem comprometer a segurança dos dados e a integridade dos sistemas. Com base na recolha de dados realizada aos profissionais entrevistados, foram identificadas cinco (5) principais categorias de ameaças cibernéticas recorrentes na infraestrutura: o *phising* ou *spear phising*, exploração de vulnerabilidades, *malware*s (*ransomwares)*, ataques força bruta e exploração remota (*Botnets*). No entanto, dentre as ameaças apresentadas os profissionais destacaram como mais preocupantes os ataques de *phising*/*spear phising*, tentativas de acesso de ssh por força bruta, e exploração remota que envolve máquinas infectadas por *Botnets*, sendo a mais frequente na infraestrutura da MoRENet.

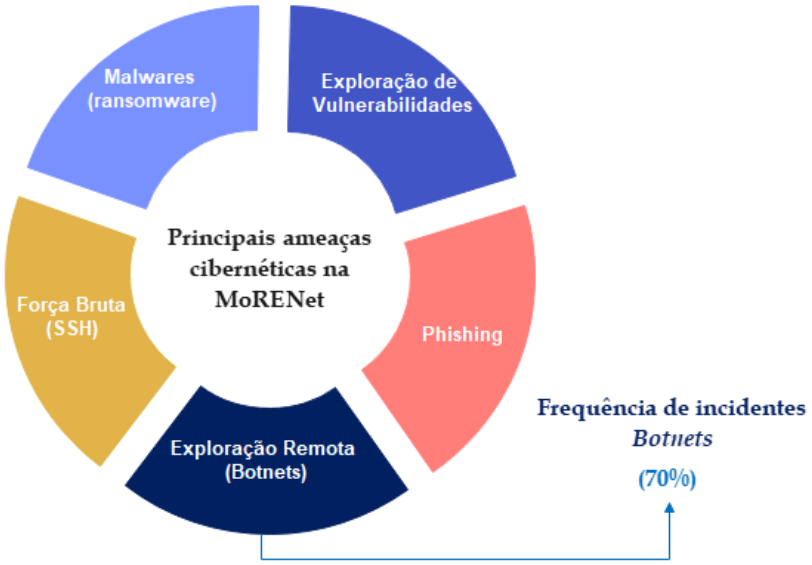


Figura 12. Principais ameaças cibernéticas na MoRENet

Fonte: Elaborado pelo Autor

No mesmo contexto, profissionais destacaram que enfrentam frequentemente incidentes relacionados a *Botnets* na infraestrutura da MoRENet, representando cerca de 70% dos incidentes observados através de máquinas infectadas por *malware Botnet*. Segundo um dos entrevistados destacou que:

> "*incidentes envolvendo Botnets na rede tem um impacto directo na performance dos serviços oferecidos, e em alguns casos, resulta em ataques a redes externas através de máquinas infectadas na infraestrutura, estando envolvidos em uma rede de Botnets de ataques DDoS*"

b) Monitoramento de rede e pontos críticos de vulnerabilidades

A infraestrutura de rede da MoRENet sendo ampla, pode tornar-se suscetível a uma variedade de ameaças cibernéticas. Procurou-se colher informações sobre os pontos críticos e de vulnerabilidades que comprometem a segurança. A partir das respostas fornecidas nas entrevistas e questionários, permitiu colher dos profissionais da MoRENet informações relacionadas infraestrutura de rede sendo destacado o monitoramento do tráfego de rede e às vulnerabilidades identificadas.

Quanto ao monitoramento e captura do tráfego de rede, a MoRENet realiza essa actividade regularmente como parte de suas práticas de segurança. No entanto, os entrevistados revelaram que essa actividade permite a colecta de estatísticas sobre o

volume de tráfego gerado na rede, em determinados períodos de tempo, o que contribui para o acompanhamento do desempenho da rede e de comportamentos anômalos.

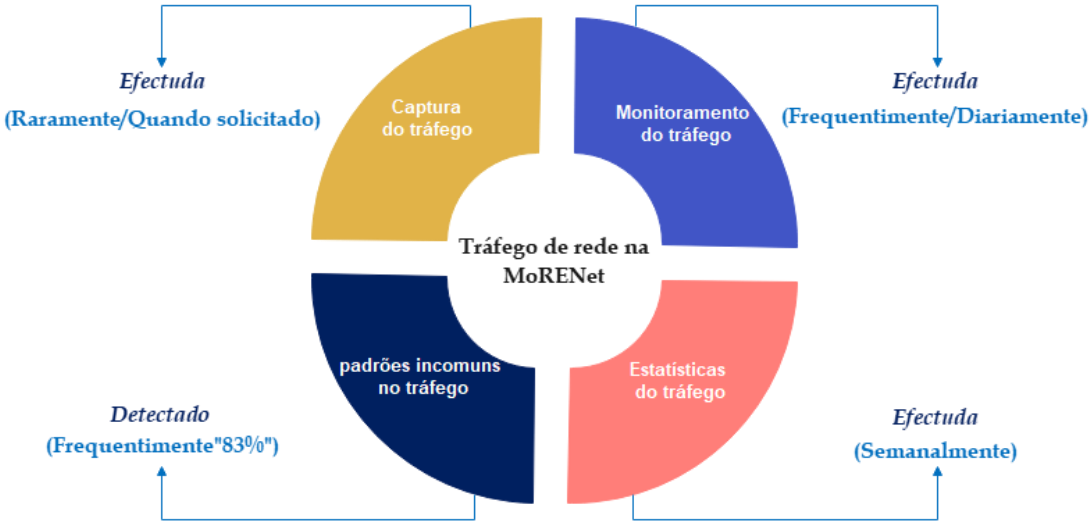


Figura 13. Monitoramento de tráfego de rede na MoRENet

Fonte: Elaborado pelo Autor

Importa referir, que foi relatado a observância de padrões incomuns no tráfego de pacotes, destacando-se picos repentinos de actividade de rede e volume de tráfego anômalo. Essa percepção foi confirmada por 83% dos respondentes, como relatado:

> "*temos observado padrões incomuns no nosso tráfego de rede, principalmente em períodos noturnos em que a rede devia estar mais acessível e fluída. Esses padrões estão ligados a altos picos de tráfego de rede, com variações bastante incomuns.*"

Quanto aos pontos críticos de vulnerabilidades na infraestrutura da rede da MoRENet, foi mencionado fragilidades em equipamentos de rede, com destaque para a falta de actualizações, e também as vulnerabilidades em aplicativos utilizados pelos beneficiários da MoRENet. Onde segundo um entrevistado:

> "*uma questão preocupante, é que muitos dos nossos equipamentos de rede estão desactualizados, com contratos de suporte expirados. Isso dificulta a realização de actualizações e manutenções, deixando-os expostos a vulnerabilidades conhecidas que podem ser exploradas. Além disso, os aplicativos usados pelos beneficiários da MoRENet também apresentam pontos fracos, principalmente quando não recebem actualizações regulares. A falta de actualizações de*

melhorias de segurança pode colocar em risco a integridade e a confidencialidade dos dados."

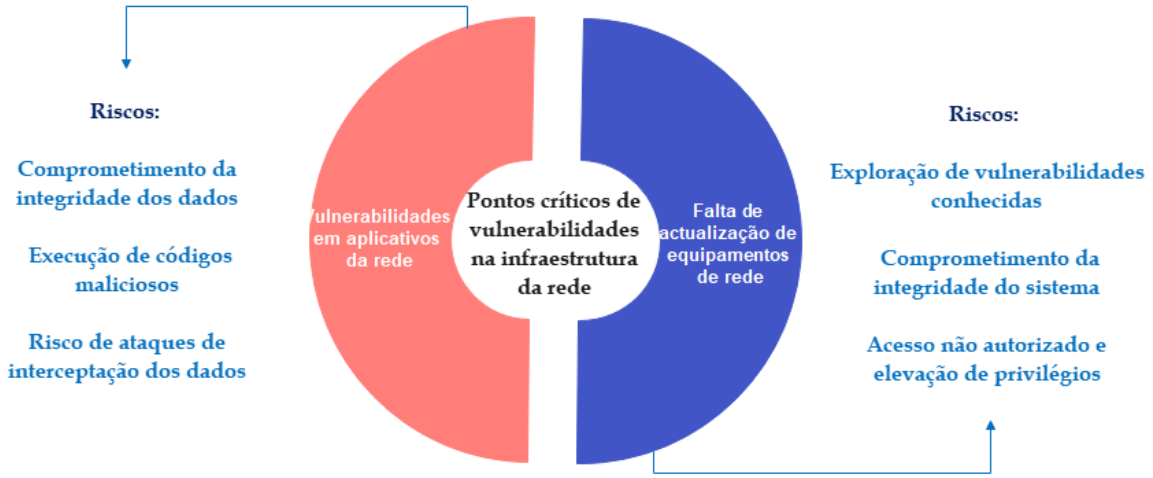


Figura 14. Pontos críticos de vulnerabilidades na infraestrutura da rede da MoRENet

Fonte: Elaborado pelo Autor

II. Percepção das Medidas de Segurança na Infraestrutura da MoRENet

a) Principais ferramentas implementadas na MoRENet

Durante a recolha de dados, foram reveladas diversas ferramentas e soluções de segurança implementadas e em operação na infraestrutura da MoRENet, utilizadas como mecanismos de detecção e mitigação de ameaças cibernéticas. Essas ferramentas permitem o acompanhamento contínuo de eventos, a gestão de incidentes e a identificação das actividades suspeitas na infraestrutura de rede, incluindo as actividades relacionadas a *Botnets.* No entanto, alguns desafios foram destacados quanto à utilização dessas ferramentas. Conforme um dos entrevistados:

"é importante destacar que muitas das soluções (ferramentas) disponíveis na MoRENet não são suportadas, pois uma parte significativa delas é de código aberto, limitando sua utilização e implementação em determinadas circunstâncias. Isso impacta muito na protecção da infraestrutura contra as ameaças cibernéticas"

b) Uso das ferramentas na detecção e mitigação de ameaças cibernéticas na MoRENet

As ferramentas de segurança implementadas na MoRENet, apresentadas no ponto anterior, são avaliadas de formas variadas pelos profissionais, sobretudo no que diz

respeito à facilidade de operação e à eficiência no seu uso para detecção e mitigação de ameaças cibernéticas.

Quanto detecção de ameaças cibernéticas os profissionais entrevistados afirmam que as ferramentas implementadas apresentam uma eficácia moderada na identificação de anomalias, podendo detectar ameaças recorrentes no ciberespaço. No entanto, destacam que essas ferramentas se mostram mais eficiência na detecção de anomalias já conhecidas, tendo limitações na identificação de novos tipos de ameaças, como o caso das ameaças envolvendo redes *Botnets*.

Quanto mitigação de ameaças cibernéticas os profissionais entrevistados afirmam que embora as ferramentas implementadas na infraestrutura permitam a detecção de incidentes, a resposta e mitigação da maioria dos incidentes, ainda depende da intervenção manual, criando morosidade na resolução de incidentes críticos. Entretanto, destaca-se a necessidade de automação na resposta de alguns incidentes, podendo contribuir para uma reacção rápida frente às ameaças detectadas na infraestrutura.

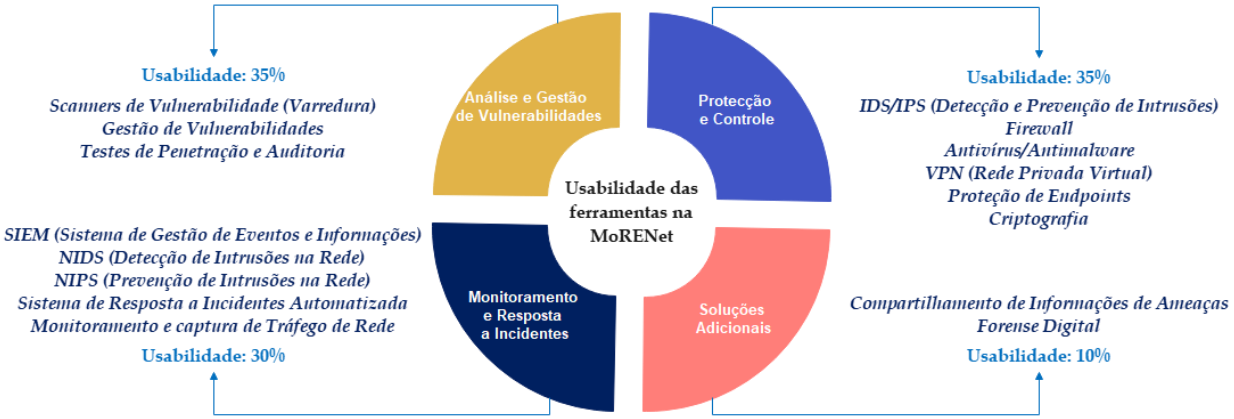


Figura 15. Níveis de usabilidade das ferramentas implementadas na MoRENet

Fonte: Elaborado pelo Autor

No Anexo 5, é apresentada a Tabela A5 - 1 e Tabela A5 - 2, que descrevem as soluções de segurança adotadas na MoRENet e sua aplicabilidade contra ameaças cibernéticas.

III. Incidentes de Segurança na MoRENet

Um passo importante nessa actividade é colher percepções dos profissionais da MoRENet em relação a incidentes de segurança. No entanto será apresentado a seguir dois (2) pontos fundamentais são levantados, sobre incidentes na MoRENet.

a) Incidentes cibernéticos relacionados a *Botnets* na MoRENet

Os profissionais da MoRENet relataram que cerca 70% dos incidentes de segurança registados numa estimativa de 1 á 2 anos, estão relacionados a ataques de redes *Botnets*. Essas provem de denúncias vindo de fontes externas sobre máquinas na infraestrutura da MoRENet atacando as suas redes externas, infectadas por um tipo de *malware*, e exploradas remotamente para a execução de ataques como DDoS e espionagem de dados. Um indício claro de actividades de *Botnets* na infraestrutura:

> "*Sim! Já tivemos incidentes de clientes que sofreram ataques DDoS ligados a redes Botnets na MoRENet, que teve impactos negativos na performance dos serviços oferecidos. Em outras, registamos denúncias vindo de fontes externas, como parceiros CSIRTs, sobre máquinas da nossa infraestrutura participando de ataques contra redes externas, com mais registo ataques DDoS e espionagem de dados, ligados a redes Botnets, máquinas infectadas por malwares Botnets*"

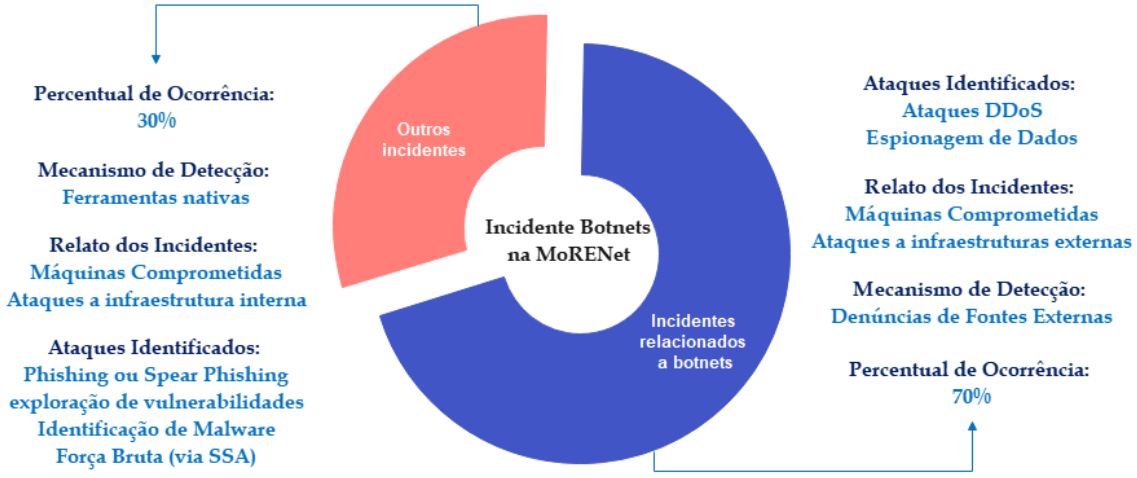


Figura 16. Incidentes cibernéticos *Botnets* na infraestrutura da MoRENet

Fonte: Elaborado pelo Autor

Os outros 30% está voltado outros diferentes tipos ameaças envolvendo dispositivos infectados por *malware* e ataques do tipo *phising*. Os ataques *phising* afectam especialmente os utilizadores finais da MoRENet e envolvem técnicas de engenharia social para enganar e induzir o utilizador a fornecer informações sensíveis, como credenciais de autenticação. Como forma de mitigação, são ministradas campanhas de conscientização e sensibilização aos utilizadores finais para que saibam identificar tentativas de *phishing*.

b) Constrangimentos na detecção e mitigação de *Botnets*

Os profissionais entrevistados identificaram diversos constrangimentos operacionais e técnicos, mas entre os principais obstáculos, destaca-se a dificuldade em identificar servidores de comando e controlo (C&C) *Botnets* na infraestrutura da MoRENet. A seguir, são apresentados abaixo alguns dos principais constrangimentos na identificação de servidores C&C *Botnets*:

- A ausência de uma técnica directa de detecção de *Botnets*, sendo um dos maiores desafios a ser cumprido para a segurança da infraestrutura da MoRENet.
- O volume elevado de dados na rede da infraestrutura da MoRENet, pois exige de maior capacidade tecnológica para o processamento e tratamento dos dados colectados, para a detecção anomalias relacionadas com as *Botnets*;

Citação de um Entrevistado:

> "*Um dos maiores desafios que enfrentamos é a ausência de uma técnica directa para a detecção de Botnets, além do grande volume de dados que precisamos analisar diariamente. Além disso, a limitação financeira para a aquisição das soluções e a exigência de tecnologia ou capacidade de equipamentos para a implementação dessas soluções são uma barreira significativa na procura de soluções de detecção e mitigação de Botnets. Por fim, mencionar a resistência a mudança e a limitação de pessoal capacitado na área influencia directamente.*"

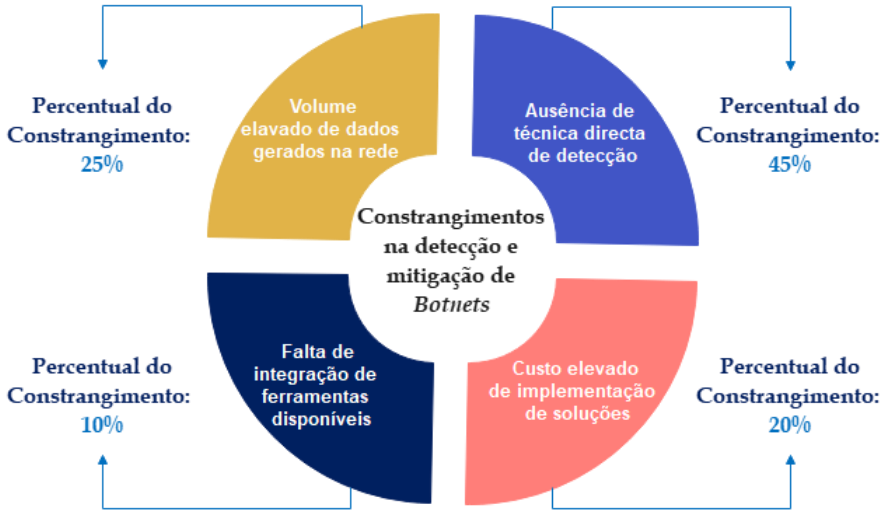


Figura 17. Nível de constrangimentos na detecção e mitigação de *Botnets*

Fonte: Elaborado pelo Autor

CAPÍTULO IV: SOLUÇÃO PROPOSTA

Este capítulo, é reservado a apresentação da solução proposta. Descreve detalhadamente a solução proposta desenvolvida para o problema identificado na presente pesquisa, a detecção de *Botnets* na infraestrutura da MoRENet.

4.1. Descrição da proposta de solução

A proposta de solução baseia-se em um mecanismo proactivo de identificação e mitigação de actividades suspeitas e anômalas associadas a *Botnets* em uma infraestrutura de sistema de informação. No entanto, a proposta de solução é centrada na Implementação do Protocolo *NetFlow* como ferramenta principal para a colecta e análise de tráfego de rede na Infraestrutura do INAGE, IP/MoRENet. O processo envolve várias etapas, desde a colecta de dados de tráfego de rede e de servidores C&C, análise e correlacção até a visualização dos resultados, contando com a integração de diferentes ferramentas auxiliares para garantir uma abordagem proactiva na detecção de *Botnets*.

4.1.1. Justificativa da escolha do *NetFlow* como solução proposta

No subcapítulo 2.3 foram apresentados três (3) soluções de análise de tráfego de rede, nomeadamente o *NetFlow*, o *Zeek* e o *sFlow*. Cada solução apresenta características específicas quanto ao modo de funcionamento, sendo estas descritas na Tabela 4, com a necessidade avaliar qual solução se adequa a realidade da infraestrutura de sistema de informação da MoRENet, sobretudo no contexto da detecção de *Botnets*.

Abaixo apresentado-se uma tabela de comparação das três (3) soluções, com base nos critérios técnicos descritos na Tabela 4, tendo em consideração a compatibilidade com o ambiente tecnológico da infraestrutura do INAGE, IP/MoRENet. Para facilitar a interpretação, os valores qualitativos foram representados por cores na Tabela 5, correspondendo a: Vermelho: Mau; Azul-claro: Razoável; e Verde: Bom.

Com base nas características apresentadas de cada solução, é possível identificar suas respectivas vantagens e limitações. Para o contexto da pesquisa, a escolha deve recair sobre a solução que melhor responda aos critérios técnicos estabelecidos, considerando a realidade operacional da infraestrutura da MoRENet.

Critério de Avaliação	*NetFlow*	*Zeek (Bro)*	*sFlow*
Compatibilidade com Equipamentos	Alta	Média	Alta
Tipo de Dados Colectados	Metadados	Pacotes Detalhados	Amostras de Pacotes
Eficácia na Detecção de *Botnets*	Alta	Muito Alta	Média
Falsos Positivos e Negativos	Médio	Baixo	Alto
Flexibilidade de Análise	Média	Muito Alta	Média
Complexidade de Implementação	Baixa	Alta	Média
Escalabilidade	Alta	Média	Muito Alta
Desempenho em Redes Cisco	Alta	Médio	Alta
Custo de Implementação	Baixo	Médio-Alto	Médio
Impacto na Performance da Rede	Baixo	Alto	Baixo
Integração com Ferramentas	Alta	Alta	Alta
Suporte Técnico	Amplo	Amplo	Moderado
Licença	*Open Source*	*Open Source*	*Open Source*
	Mau	Razoável	Bom

Tabela 5. Avaliação das soluções disponíveis de análise de tráfego de rede

Fonte: Adaptado pelo autor

Dentre as três (3) soluções apresentadas o **protocolo *NetFlow*** foi a solução escolhida para a implementação de um mecanismo proactivo de detecção de *Botnets* na infraestrutura da MoRENet. A escolha do *NetFlow* baseou-se nos seguintes factores:

- Compatibilidade com equipamentos: possui suporte nativo aos equipamentos Cisco existentes na infraestrutura da MoRENet, o que facilita sua implementação.
- Tipo de dados colectados e Análise: realiza a colecta de metadados detalhados dos fluxos de rede, o que reduz a complexidade no processo de análise de dados;
- Complexidade e Custo de implementação: apresenta baixa complexidade e custo de implementação, podendo ser rapidamente operacionalizado na infraestrutura da MoRENet, sem causar interrupções nos serviços;
- Escalabilidade e Flexibilidade: é altamente escalável e adequada à infraestrutura da MoRENet, pois processa volumes elevados de tráfego sem afectar o desempenho da rede;

- Integração com ferramentas: possibilita a integração com diversas ferramentas de análise e visualização dados, tornando-o eficiente para actividades de segurança, como a detecção de *Botnets* na infraestrutura.

Entretanto, embora o *Zeek* e *sFlow* também apresentem critérios positivos que as tornam ferramentas valiosas para a análise de tráfego de rede em diversos cenários, é fundamental considerar suas limitações em relação às necessidades a alguns critérios de avaliação estabelecidos. Ambas oferecem características robustas, como alta capacidade de integração, escalabilidade, porém, apresentam pontos negativos em alguns critérios cruciais para o contexto da MoRENet, que são apresentados a seguir:

I. *Zeek*:

- Tipo de dados colectados e Análise: oferece análise detalhada do tráfego, mas com elevado consumo de recursos da infraestrutura, especialmente em redes de grande porte, o que pode impactar negativamente a performance;
- Complexidade de implementação: apresenta elevada complexidade e requer conhecimento técnico avançado, o que poderá prolongar o tempo de configuração e representar uma barreira à sua implementação, além dos desafios futuros na manutenção;
- Custo de implementação: o alto consumo de recursos pode exigir investimentos adicionais na actualização da infraestrutura para garantir funcionamento adequado do *Zeek*, ou, por outras, pode afectar o desempenho da rede.

II. *sFlow*:

- Tipo de dados colectados e Análise: colecta apenas amostras de pacotes, o que limita na captura de comunicações de curta duração, e pode comprometer a detecção de *Botnets*, quando comparado ao *NetFlow*, que fornece metadados detalhados dos fluxos de rede
- Falsos Positivos e Negativos: apresenta um número elevado de falsos negativos, devido a perda de pacotes críticos da rede na colecta de dados.

Embora *Zeek* e *sFlow* sejam ferramentas adequadas em diversos contextos, o *NetFlow* destaca-se por melhor atender às necessidades específicas dos critérios de avaliação estabelecidos tendo em conta ao cenário analisado no estudo de caso.

4.1.2. Recursos necessários para a implementação do *NetFlow*

Para uma implementação bem-sucedida de uma solução tecnológica como o *NetFlow,* depende da minuciosa identificação e planeamento dos recursos necessários. Neste contexto, três (3) recursos essenciais foram identificados como determinantes para a detecção de *Botnets* infraestrutura da MoRENet com base no protocolo *NetFlow*.

I. Recursos tecnológicos

A infraestrutura tecnológica constitui a base operacional da proposta. Entretanto, torna-se indispensável a disponibilidade de equipamentos de rede compatíveis com o protocolo *NetFlow*, servidores de alto desempenho para processamento de dados, bem como ferramentas específicas para a colecta, análise e visualização dos dados. Esses recursos permitirão a colecta de metadados de rede, o tratamento dos dados e a identificação dos padrões de tráfego anômalos que podem indicar actividades associadas a *Botnets*.

No entanto, cada recurso de infraestrutura tecnológica necessários para a implementação da presente proposta encontram-se especificado no Anexo 4.

II. Recursos humanos

A alocação de recursos humanos qualificados é fundamental, e que detenham competências técnicas sendo responsáveis pela configuração, a operação contínua e manutenção da solução de detecção proactiva de *Botnets* com base no protocolo *NetFlow*. Os perfis profissionais alinhados às necessidades da solução são:

- Especialista em Segurança da Informação;
- Analista de SOC (*Security Operations Center*);
- Administrador de Rede;
- Desenvolvedor ou Analista de Dados.

No Anexo 6 são apresentadas as qualificações associadas a cada um dos perfis profissionais identificados. Para complementar, foi elaborado um plano de capacitação e manutenção contínua, com foco nos recursos humanos definidos.

a) Plano de treinamento e capacitação

O presente plano, é essencial para garantir que a equipe envolvida na implementação da solução proposta esteja devidamente preparada para a sua operacionalização. Tem como objectivo proporcionar aos profissionais o domínio das ferramentas, técnicas e

processos relacionados à análise de tráfego de rede utilizando o protocolo *NetFlow*, bem como capacitá-los para a adoção de novas ferramentas que possam aprimorar a solução. O conteúdo do plano de treinamento pode ser consultado no Anexo 6.

b) Plano de manutenção

O plano de manutenção tem como finalidade assegurar a continuidade operacional e o desempenho positivo da solução proposta na infraestrutura da MoRENet. No plano são definidas as actividades, responsabilidades e recursos necessários para manter a solução, incluindo a actualização de componentes, a introdução de novas ferramentas e a verificação regular do desempenho da solução na infraestrutura da MoRENet. O conteúdo do plano de manutenção pode ser consultado no Anexo 6.

III. Recursos financeiros

A definição de recursos financeiros para a presente solução proposta, baseou-se no levantamento de um orçamento adequado, capaz de sustentar suas exigências operacionais. Dado que infraestrutura da MoRENet já dispõe de equipamentos para a implementação da solução, o custo inicial estimado será reduzido. Adicionalmente, as ferramentas utilizadas são de código aberto (*open source*), eliminando a necessidade de investimento em licenças de *software*. Os profissionais alocados para implementação da solução, são quadro da MoRENet e não gera custos adicionais de contratação.

Foram estimadas como principais despesas:

- à capacitação da equipe técnica, com um custo estimado em 350.000 MZN, que visa garantir a qualificação necessária para a operação da solução;
- à manutenção e suporte, com um custo estimado em 480.000 MZN para o primeiro ano, sendo base de remuneração da equipe responsável pela operação e suporte contínuo da solução e pela mitigação de ameaças.

Categoria	Descrição	Custo estimado
Capacitação da Equipe	Treinamento para operação da solução	350.000 MZN
Manutenção e Suporte	Custos operacionais e suporte contínuo	480.000 MZN
Total estimado	----------	830.000 MZN

Tabela 6. Custos na implementação da solução na infraestrutura da MoRENet

Fonte: Adaptado pelo autor

É importante destacar que os valores estimados podem cobrir e como não cobrir as despesas definidas, dependendo das necessidades específicas durante a implementação e operação da solução.

4.1.3. Cronograma para implementação da solução na MoRENet

A implementação da solução proposta será realizada de forma faseada, abrangendo sete (7) etapas, desde a planificação até a manutenção sem comprometer o funcionamento da infraestrutura da MoRENet. O cronograma contém uma duração estimada de dez (10) semanas e está detalhado no Anexo 7, onde se encontram especificadas as actividades, os responsáveis e os respectivos prazos de execução.

4.1.4. Arquitectura da proposta da solução

A proposta de solução é baseada em mecanismos que seguem diversas metodologias para a sua implementação. Nessa, a arquitectura da solução proposta para a detecção de *Botnets,* foi projectada integrando diferentes componentes que trabalham em conjunto, sendo apresentado na ilustração abaixo:

I. Captura e colecta de amostras de tráfego de rede
    a. Implementação do protocolo *NetFlow*;
    b. Configuração do *NfDump*.

II. Análise e correlacção de dados
    a. Colecta de informações de servidores de C&C por meio de um *script*;
    b. Implementação de *script* de análise e correlacção de dados:
        i. Execução do *NFDump* para análise do tráfego de rede colectado;
        ii. Correlacção com informações de servidores de C&C colectado.

III. Monitoramento e Visualização
    a. Envio dos dados para um sistema de gestão de dados (SIEM):
        i. *Elasticsearch*: para indexar os registos gerados durante a correlacção;
        ii. *Kibana:* para visualizar os resultados da análise e correlacção.

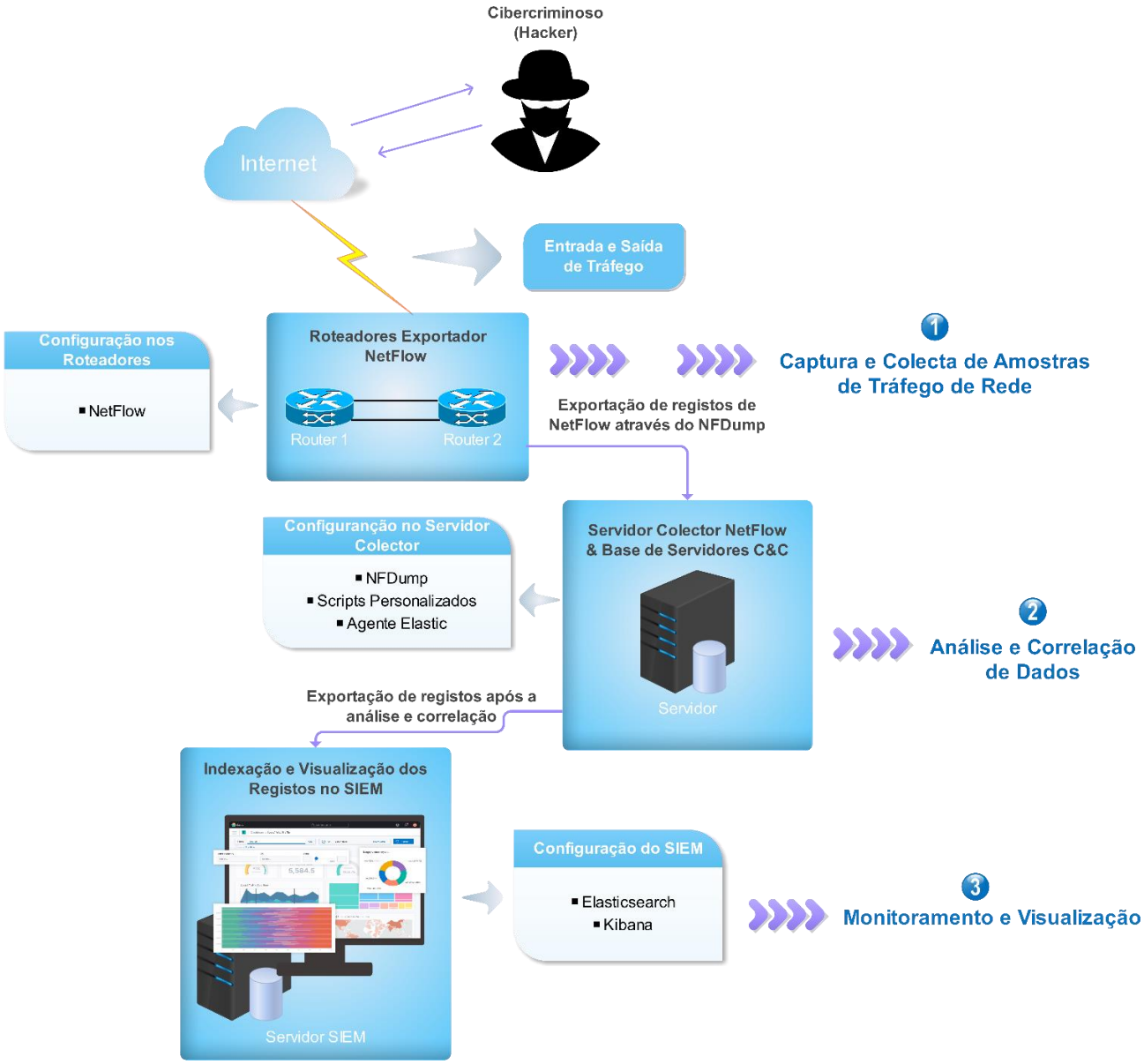


Figura 18. Arquitectura da solução proposta para implementação de *NetFlow* como mecanismo de detecção de *Botnets*

Fonte: Elaborado pelo Autor

4.1.5. Captura e colecta de amostras de tráfego de rede

Conforme apresentado na arquitetura da solução (subcapítulo 4.1.4), a fase inicial dessa implementação concentra-se na captura e colecta de amostras de tráfego de rede da infraestrutura da MoRENet. Definiu-se algumas estratégias para que as amostras de tráfego capturadas sejam representativas e suficientes para uma análise que permitirá a identificação de possíveis actividades de redes *Botnets*.

I. Pontos de captura de amostra de tráfego de rede nos PoP's da MoRENet

A primeira etapa do processo de captura de amostras de tráfego da infraestrutura da MoRENet, envolve a identificação e selecção dos pontos estratégicos de rede. Como apresentado no subcapítulo 3.1.1, a MoRENet dispõe de seis (06) PoPs distribuídos pelo País. Dentre esses, destacam-se dois (2) PoP's "o do MCTESTP (MCTD) e de Maluana" que concentram o fluxo de entrada e saída do tráfego nacional e internacional, possibilitando pontos estratégicos para a captura total do tráfego de rede.

II. Implementação do *NetFlow*

Após a identificação dos pontos estratégicos de captura de tráfego, a etapa seguinte consiste na implementação do protocolo *NetFlow* em dois (2) dispositivos de rede, especificamente nos roteadores de borda da infraestrutura da MoRENet: o Cisco ASR 1002 HX, localizado no PoP do MCTESTP (MCTD), e o Cisco ASR 1004, localizado no PoP de Maluana. As especificações técnicas detalhadas desses equipamentos encontram-se apresentadas no Anexo 4.

O *NetFlow* permite o monitoramento de grandes volumes de trafego com menor impacto no desempenho da rede, onde segundo Holzmacher (2023), diferente de soluções como o *Zeek* que se concentram na análise de pacotes de rede, o *NetFlow* se concentra na análise de dados de fluxo de rede, que é uma visão de alto nível da actividade da rede. A análise de tráfego de rede utilizando o *NetFlow*, irá basear-se na captura dos fluxos de rede necessários para a detecção de actividades relacionadas a *Botnets*. Essa captura será executada por meio de filtros, configurados directamente na interface dos dispositivos de rede por meio do painel de controlo ou via linha de comando. Contudo, o foco principal é colectar informações relacionadas com o endereço IP (origem e destino), portas (origem e destino), protocolos, número de pacotes e *timestamps*.

A configuração do *NetFlow* será feita através de um conjunto de comandos que define:

- A configuração do registo de fluxos: determinar os fluxos de dados a serem monitorados ou registados as informações do tráfego de rede;
- A configuração do exportador de fluxos: definir do endereço do colector para o qual os dados de fluxo serão enviados;

- A configuração do monitor de fluxos: combinação das definições do registo e do exportador de fluxo;
- A configuração da interface: Associa monitor de fluxo a uma interface no roteador que será responsável pela o colecta de dados de fluxo.

Um aspecto importante a considerar são as possíveis políticas de segurança implementados na infraestrutura de rede da MoRENet, como *firewalls*, que em alguns casos podem interferir no funcionamento do *NetFlow*, bloqueando e limitando a colecta de amostras de tráfego de rede. No entanto, cada etapa de configuração do protocolo *NetFlow* nos roteadores da MoRENet, pode ser verificada no Anexo 8. Além disso, o anexo apresenta os resultados esperados após a execução dos comandos de verificação da configuração do *NetFlow*.

III. Configuração do *NFDump* no colector *NetFlow*

Após a implementação do *NetFlow* é necessário configurar um mecanismo capaz de colectar, processar e analisar dados de fluxo de rede gerados pelo protocolo *NetFlow*. Para tal será usada uma ferramenta de linha de comando denominada *NFDump.*

O *NFDump*[2] será muito essencial para a análise e processamento de registos do *cache NetFlow,* actuando como o analisador *NetFlow*. Através dele é feita a filtragem, classificação e organização dos dados *NetFlow* de acordo com critérios definidos. De acordo com o Mathur et al., (2018), o *NFDump*, com a ajuda do seu *daemon nfcapd*, captura dados de *NetFlow* e armazena-os em ficheiros em um colector *NetFlow*. A instância do *nfcapd* associa-se ao fluxo de rede e mantém o registo de dados ao longo do tempo, permitindo que se análise desses dados a posterior. O *NFDump* será instalado em um servidor colector *NetFlow*: HP Proliant DL380 gen7, localizado no PoP de Maluana com sistema operativo baseados em *Linux*. As especificações técnicas detalhadas desses equipamentos encontram-se apresentadas no Anexo 4.

A configuração do *NFDump* envolve a:

- instalação do *NFDump* através da linha do comando do servidor colector *NetFlow*;

[2] NFDUMP (sourceforge.net)

- criação de um directório nomeadamente “TEMPORARIO” e definição de permissões. No directório serão armazenados os dados capturados pelo *NetFlow*;
- configuração do *nfcapd* indicando directório de armazenamento e a porta para qual irá escutar para receber dados *NetFlow*;

Utilizando *cron jobs* (ferramenta de agendamento e automação de tarefas no *Linux*) no colector *NetFlow,* configura-se uma tarefa que procura arquivos no directório “TEMPORARIO” que tenham sido modificados há mais de um dia e os apaga. Essa configuração pode ser verificada no Anexo 11.

No entanto, cada configuração do *NFDump* no colector *NetFlow*, pode ser verificada no Anexo 8. Além disso, o anexo apresenta os dados colectados e armazenados usando o *NFDump* no colector *NetFlow*. A Figura 19, ilustra o cenário da topologia das configurações efectuadas na primeira parte da arquitectura da proposta de solução, conforme descrito no presente subcapítulo 4.1.5.

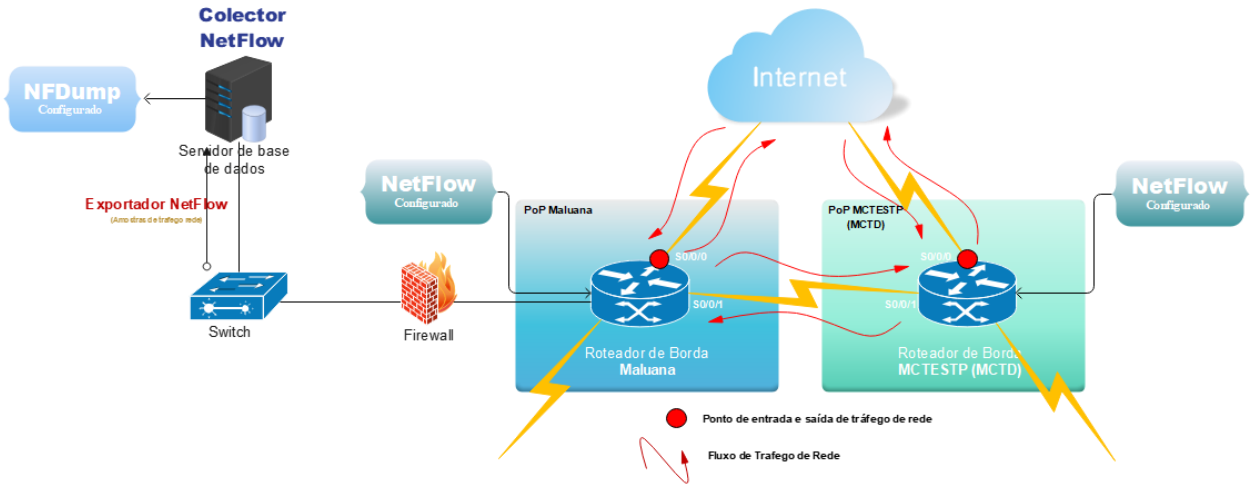


Figura 19. Cenário da topologia com o *NetFlow* e *NFDump* configurado

Fonte: Elaborado pelo Autor

4.1.6. Análise e correlacção de dados

Concluída a primeira etapa descrita na arquitetura da proposta de solução, segue-se para a segunda fase que se concentra na análise e correlacção dos dados capturados e armazenados no colector *NetFlow*. Contudo, essa etapa é fundamental para o processamento das amostras de tráfego capturadas e armazenados, correlacionando-as com informações sobre servidores de C&C *Botnets*.

I. Colecta de informações de servidores de C&C

Existem diversos servidores de C&C *Botnets* distribuídas pelo ciberespaço. A colecta de informações sobre servidores de C&C *Botnets* é fundamental para a detecção de *Botnets*. Essa actividade será realizada por meio duas (2) fontes principais de segurança cibernética:

- Plataformas de Compartilhamento de Ameaças, foram identificados os sites *ThreatFox* e *FeodoTracker* que disponibilizam indicadores de comprometimento (IOCs) em formatos CSV e JSON, referentes a servidores de C&C *Botnets*;
- Informações de parceiros (CSIRT's e SOC's), que fornecem listas actualizadas de servidores de C&C *Botnets* em formatos CSV.

As informações colectadas de servidores de C&C *Botnets* são armazenadas em um ficheiro de texto (C2.txt), com a seguinte organização:

- a data de início da actividade ou da descoberta do servidor C&C *Botnet*;
- o endereço IP da *Botnet*;
- a porta da *Botnet*;
- o estado da *Botnet* (*online* ou *offline*);
- registo de último dia *online* da *Botnet* segundo a fonte da informação; e
- o nome da *Botnet*.

O processo de colecta de informações sobre servidores de C&C *Botnets* baseia-se em quatro (4) *scripts* personalizados em *Python* (.Py) implementados no colector *NetFlow*, com funções específicas de:

- Colecta de dados: dois (2) *scripts Python* (*threatfox.py* e *feodotracker.py*) extraem e filtram dados das plataformas *ThreatFox* e *FeodoTracker*, armazenando-os em ficheiros de texto com estrutura organizacional apresentada acima;
- Unificação de dados: um (1) *script Python* (*merge_last_week.py*) unifica toda informação colectada durante a semana em um único ficheiro de texto (txt);
- Actualização de dados: o *script Python* (*addNewInfo_C2.py*) insere novos dados de servidores C&C *Botnets* no ficheiro C2.txt colectados semanalmente.

A execução dos *scripts* será feita automaticamente, utilizando *cron jobs* no colector *NetFlow* (Anexo 11), garantindo que seja efectuada a colecta e actualização contínua dos dados de servidores C&C *Botnets*. No entanto, a configuração e a aplicação dos *scripts* personalizados no colector *NetFlow*, pode ser verificada no Anexo 9.

II. Análise e correlacção de dados com informações de servidores de C&C

A análise e correlacção de dados com as informações de servidores de C&C constitui o núcleo da segunda etapa da solução, onde são identificadas correspondências que indicam actividades de *Botnets* na MoRENet. Entretanto, é utilizado um *script* personalizado em *Python* no colector *NetFlow*, denominado "*find_C2.py*", que desempenha três (3) funções principais:

a) Analisar o tráfego de rede capturado

A primeira função do *script* consiste em analisar os dados de tráfego capturados pelo *NetFlow* e armazenados utilizando *NFDump*. O *script* executa o *NFDump* sobre os arquivos *NetFlow* capturados e armazenados no directório "TEMPORARIO" extraindo informações relevantes, nomeadamente*:* endereços IP de origem e destino, portas utilizadas, protocolos e *timestamp*.

b) Correlacionar com os dados dos servidores de C&C *Botnets*

A segunda função do *script* consiste na correlacção entre os fluxos de rede analisados com as informações de servidores de C&C armazenados no ficheiro C2.txt:

- Carregamento dos servidores de C&C: o *script* lê C2.txt, criando um dicionário denominado "*suspect_ips*" com IPs suspeitos e o nome da *Botnet* correspondente;
- Comparação dos fluxos de rede: os IPs de origem e destino extraídos dos fluxos são comparados com os IPs suspeitos do dicionário;
- Identificação de correspondências: existindo correspondência, são extraídos os dados do fluxo, incluindo o IPs e portas (origem e destino), protocolo, *timestamp* e a *Botnet*, sinalizando uma possível actividade de redes *Botnets* na MoRENet.

c) Gerar *logs* de detecção com base nos resultados obtidos

A última função do *script* é gerar um registo (*log*) de detecção denominado "*detected_C2.log*" com os resultados da correlacção. Ao detectar uma correspondência

com um servidor de C&C, armazena: *timestamp* do evento, IP de origem e porta, IP de destino e porta, protocolo e o tipo de *Botnet* associado.

Para garantir a execução do *script find_C2.py*, é configurado um *cron job* no colector *NetFlow* (Anexo 11), permitindo a análise e correlacção contínua dos dados de tráfego com servidores C&C *Botnets*. No entanto, a configuração e a aplicação do *script* personalizado *find_C2.py*, pode ser verificada no Anexo 9.

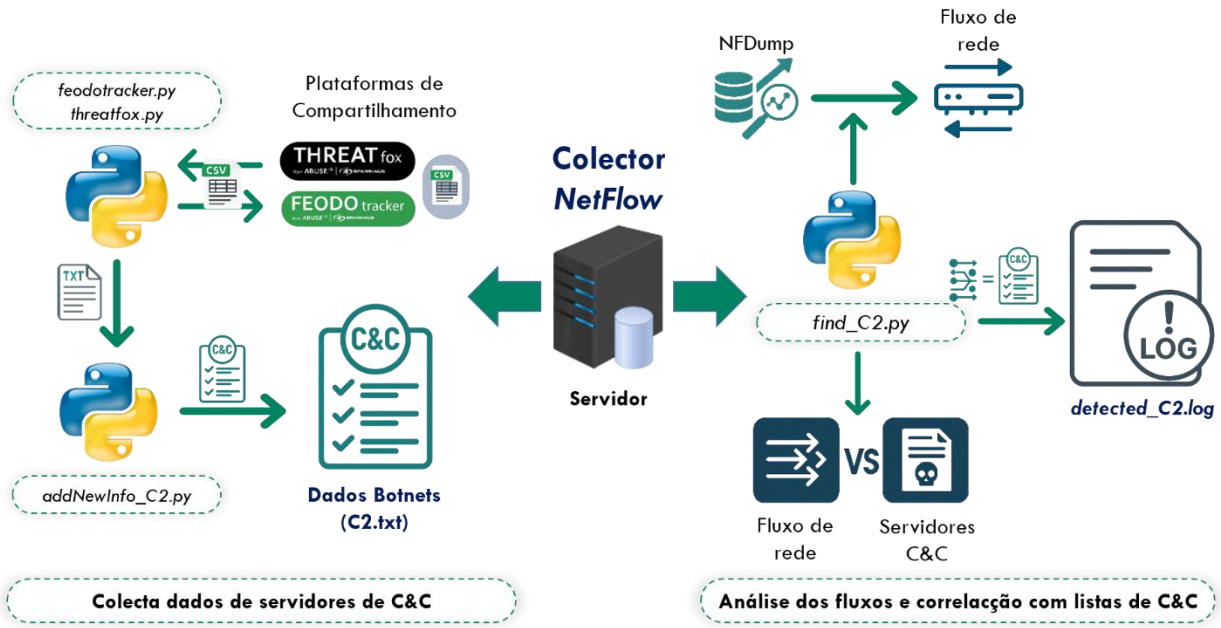


Figura 20. Cenário da fase da análise e correlacção de actividades *Botnets*

Fonte: Elaborado pelo Autor

4.1.7. Monitoramento e visualização

A etapa de monitoramento e visualização dos resultados da análise e correlacção de dados na detecção de *Botnets* na MoRENet, envolve uma solução de Gestão de Informações e Eventos de Segurança (*SIEM - Security Information and Event Management*), já operacional na MoRENet, denominado *SecurityOnion*, que integra ferramentas o "*Elasticsearch* e *Kibana"*, para exibir graficamente os eventos detectados.

I. Indexação dos registos gerados na análise e correlacção de dados

No subcapítulo 4.1.6 foi apresentado o mecanismo de análise e correlacção dos dados que resulta na saída de um registo (*log*), denominado *detected_C2.log*, que contém as correspondências ou padrões que indicam actividades de servidores C&C *Botnets*.

Nessa etapa, procede-se a indexação do registo *detected_C2.log* na ferramenta *Elasticsearch*. Segundo Elastic Stack (s.d), *Elasticsearch* o coração do *Elastic Stack*, é um motor de busca e análise distribuído, projectado para pesquisar, indexar, armazenar e analisar grandes volumes de dados de forma eficiente em tempo quase real.

a) Instalação do *Elastic Agent* no colector *NetFlow*

A primeira etapa consiste na instalação do *Elastic Agent* no servidor colector *NetFlow*, responsável por enviar os dados do registo *detected_C2.log* ao *Elasticsearch*. Para tal, são executados comandos na linha de comando do colector *NetFlow*, conforme apresentado no Anexo 10, que incluem:

- o *download* do *Elastic Agent* dentro do servidor colector *NetFlow*;
- a instalação do *Elastic Agent* com base na *url* do servidor *Fleet* do *SecurityOnion* (https:// <IP do servidor>:porta).

b) Configuração do *Elastic Agent* no colector *NetFlow*

Essa etapa envolve a configuração de parâmetros que especificam quais informações o *Elastic Agent* irá enviar para o *Elasticsearch* no ficheiro "*elastic-agent.yml*" (Anexo 10):

- definição do endereço IP do servidor *Elasticsearch* que receberá os dados vindo do *Elastic Agent*;
- especificação da política de colecta de registos, especificando o caminho do registo *detected_C2.log* que será monitorado e transmitido para indexação.

c) Criação de política no *Elasticsearch* para indexação de dados dos registos

A criação de uma política de colecta no *Elasticsearch* para a indexação dos registos recebidos, estabelece como os dados serão armazenados e estruturados para consulta e análise. Os passos incluem:

- definir o índice onde registos recebidos serão armazenados no *Elasticsearch*;
- criar a política de indexação do registo, incluindo o mapeamento dos campos, que especifica o tipo de dado, o *timestamp*, endereços IP, entre outros.

No entanto, a configuração e a aplicação da indexação dos registos gerados na análise e correlacção de dados, pode ser verificada no Anexo 10.

II. Monitoramento e visualização dos registos indexados no *Elasticsearch*

Após a indexação dos registos no *Elasticsearch*, a monitorização e visualização dos dados são realizadas por meio do *Kibana,* ferramenta integrante do *Elastic Stack.* Conforme, Elastic Stack (s.da), *Kibana* permite buscar, observar e proteger dados, analisando *logs* e identificando vulnerabilidades de segurança através de gráficos, tabelas, painéis, entre outros, facilitando a análise de *insights* (percepções) ocultos.

a) Configuração do *Kibana* para visualização dos dados indexados

Após a indexação dos dados do registo *detected_C2.log* no *Elasticsearch*, para possibilitar o monitoramento e visualização dos resultados é fundamental:

- Selecionar o índice que contém os dados *netflow-srv*, e configurar o ambiente para análise das informações provenientes do registo buscando os campos relevantes como *timestamp*, IP de origem e porta, IP de destino e porta, protocolo e a *Botnet*.

b) Criação de *Dashboards* interativos

Essa etapa envolve a criação de *dashboards* interativos que permitirá a visualização intuitiva dos resultados da análise e correlacção das actividades *Botnets* na infraestrutura da MoRENet. Essa etapa inclui:

- adicionar e organizar os componentes do *dashboard*, o "*layout*" contendo elementos como: tabelas, gráficos, mapas, entre outros;
- criar filtros e consultas que permitirão efectuar buscas avançadas e visualizações por parâmetros como IP de origem/destino, tipo de *Botnet,* entre outros.

Na Figura 21 são apresentados os *dashboards* para o monitoramento e visualização de actividades *Botnets* na infraestrutura da MoRENet.

4.1.8. Riscos na implementação e operação da solução proposta

Na implementação de uma solução tecnológica deve-se tomar em conta os potencias riscos, que podem comprometer o desempenho e os resultados esperados. Esses riscos podem variar desde falhas técnicas, sobrecarga de dispositivos, interrupção na colecta do tráfego de rede para a detecção de *Botnets*, entre outros. Os riscos identificados e suas respectivas medidas de mitigação encontram-se detalhados no Anexo 12.

Figura 21. *Dashboards* das tabelas, gráficos e mapas das actividades *Botnets* na rede da MoRENet

Fonte: Adaptado pelo Autor com base no *Elasticsearch*

A Figura 22 ilustra o cenário final após a implementação da solução proposta.

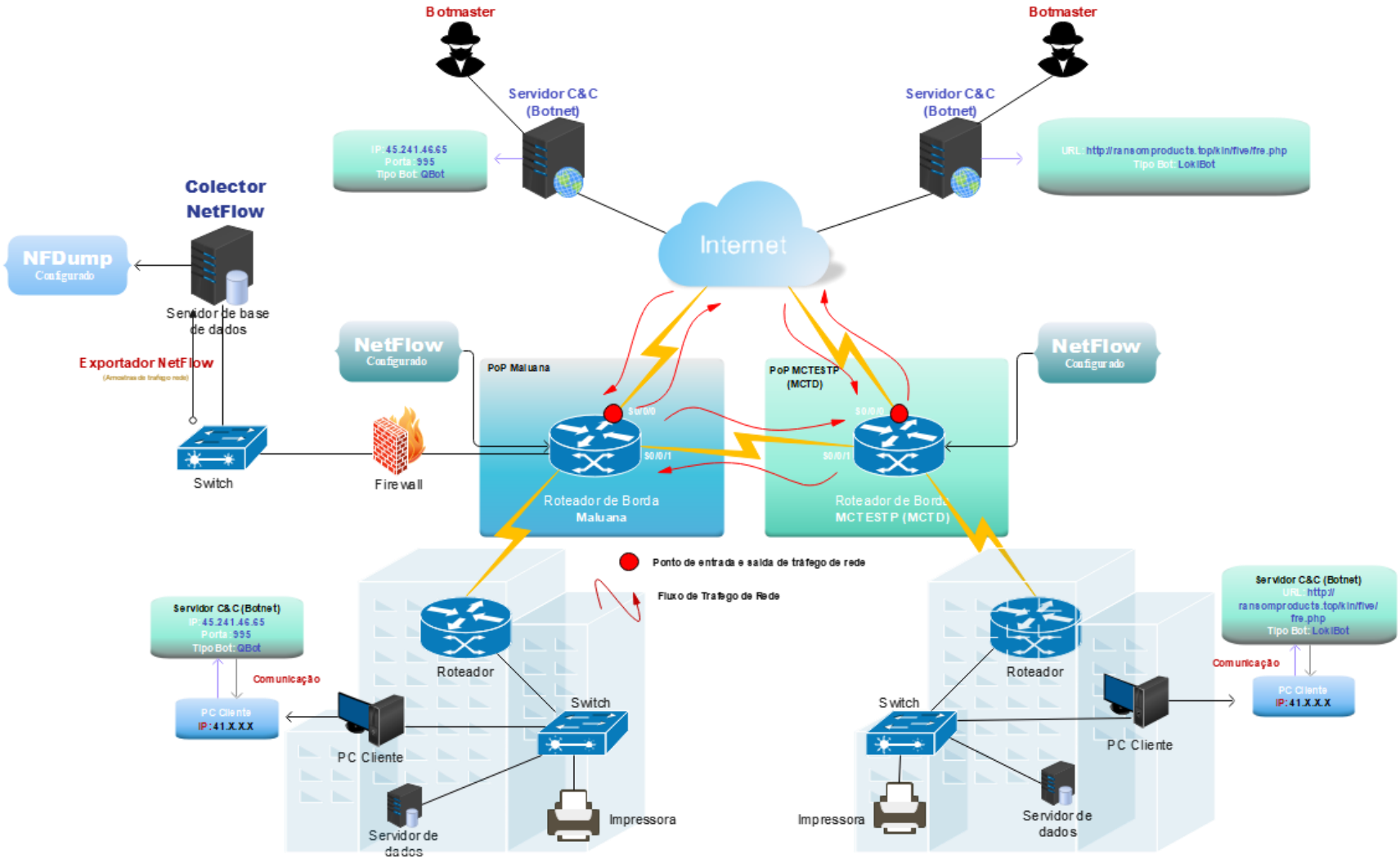


Figura 22. Topologia do cenário final da implementação da solução proposta na infraestrutura da MoRENet

Fonte: Elaborado pelo Autor

CAPÍTULO V: ANÁLISE DOS DADOS E DISCUSSÃO DE RESULTADOS

Este capítulo é reservado à análise dos dados recolhidos e à discussão dos principais resultados obtidos ao longo da pesquisa.

5.1. Análise dos dados: Percepções da situação actual da MoRENet

O processo de análise de dados é definido por Kerlinger, (2001, p. 353), como “a categorização, ordenação, manipulação e sumarização de dados”. Tem por objectivo reduzir grandes quantidades de dados brutos a uma forma interpretável e mensurável. A análise de dados fundamenta-se nas percepções dos profissionais de segurança do CSIRT da MoRENet, conforme descrito no subcapítulo 3.1.2.

I. No contexto da situação actual da segurança cibernética na MoRENet

A avaliação obtida dos profissionais da MoRENet aponta um percepção moderada sobre a actual situação de segurança cibernética na infraestrutura. Essa reflete um reconhecimento positivo das políticas e práticas de segurança já estabelecidas, que constituem uma base sólida para a protecção dos activos contra ameaças emergentes no ciberespaço global quanto no moçambicano. Entretanto, persistem desafios notáveis em relação a profissionais capacitados na área de segurança e ao suporte aos seus beneficiários o que compromete a capacidade de resposta em cenários de incidentes cibernéticos na infraestrutura.

II. No contexto das principais ameaças cibernéticas e vulnerabilidades de rede

A análise das principais ameaças cibernéticas emergentes evidencia a ocorrência de ataques cibernéticos contra a infraestrutura rede MoRENet. Caracterizam-se em ataques de curto prazo com vista a comprometimento imediato, como também de longo prazo com vista a explorar e comprometer a integridade do sistema. Tal cenário reforça a necessidade de definição de estratégias de segurança para a detecção e mitigação contínua dessas ameaças.

E quanto às vulnerabilidades críticas da rede, identificam-se fragilidades na gestão da infraestrutura. Essas lacunas podem comprometer a resiliência da rede diante das ameaças cibernéticas e evidenciam a necessidade de implementar práticas de gestão dos activos e possíveis actualizações na rede para minimizar os pontos vulneráveis.

III. No contexto das principais ferramentas implementadas na MoRENet

A análise das principais ferramentas implementadas na infraestrutura da MoRENet destaca um conjunto de soluções de segurança que operam de forma contínua no monitoramento rede, e abrangem diferentes camadas oferecendo suporte fundamental às actividades de prevenção, detecção e resposta a incidentes cibernéticos.

Contudo, os dados revelam que embora as soluções desempenhem um papel essencial na protecção da infraestrutura, sua eficácia varia, quanto à detecção e mitigação das ameaças cibernéticas. Nesse sentido, os profissionais entrevistados destacaram dois (2) aspectos determinantes no desempenho dessas ferramentas: a capacidade de detecção de ameaças e a eficácia na mitigação de incidentes, pois, aponta-se a existência de limitações específicas na detecção de ameaças emergentes, a semelhança das ameaças envolvendo redes de servidores de comando e controlo (C&C) *Botnets*.

IV. No contexto dos incidentes cibernéticos relacionados a *Botnets* e interconexão com outras ameaças na MoRENet

A infraestrutura da MoRENet apresenta registos de incidentes cibernéticos relacionados a redes *Botnets*, que correspondem cerca de 70% dos casos observados. Esses envolvem tanto ataques dirigidos à infraestrutura, quanto a exploração de activos internos para a participação em ataques *Botnets* contra redes externas. Esse cenário evidencia o impacto das actividades *Botnets* na infraestrutura da MoRENet, o que compromete o desempenho dos serviços, a integridade da rede e tornando-se vulnerável a ataques de larga escala, como DDoS, e a práticas de espionagem de dados.

Os incidentes restantes estão associados a ameaças recorrentes na infraestrutura da MoRENet. Essas ameaças actuam muitas vezes como vectores de entrada para ataques de *Botnets*, uma vez que as *Botnets* combinam diversas técnicas de ataque cibernéticos.

V. No contexto dos constrangimentos na detecção e mitigação de *Botnets*

Os profissionais da MoRENet revelaram diversos constrangimentos na detecção e mitigação de *Botnets*. Esses abrangem limitações técnicas e financeiras, como a ausência de uma técnica directa de detecção, a dificuldade de análise do elevado volume de dados e a escassez de profissionais especializados para operar soluções avançadas

de monitoramento e resposta. Tais desafios exigem uma abordagem minuciosa no desenho e implementação de estratégias de detecção. Superar essas barreiras será fundamental para que a MoRENet desenvolva uma postura mais proactiva e resiliente em cibersegurança, elevando sua capacidade de identificar não apenas *Botnets*, mas também outras ameaças cibernéticas emergentes no ciberespaço.

5.2. Discussão dos resultados da pesquisa

A discussão dos resultados constitui uma etapa essencial na estrutura de uma pesquisa científica. Como destaca Gil (2002), uma pesquisa "desenvolve-se ao longo de um processo que envolve inúmeras fases, desde a formulação do problema até a apresentação dos resultados". O presente estudo, aborda a “proposta de implementação do protocolo *NetFlow* como mecanismo proactivo de detecção de *Botnets* baseada na análise de tráfego de rede em na infraestrutura de sistema de informação do INAGE, IP/MoRENet”, sendo que a discussão será conduzida com foco nas principais fases do desenvolvimento do trabalho.

5.2.1. Identificação do problema

A identificação do problema constitui a base para o desenvolvimento continuo para a presente pesquisa. De acordo com Prodanov & Freitas (2013, p. 43), afirmam que “a pesquisa científica é a realização de um estudo planeado, sendo o método de abordagem do problema o que caracteriza o aspecto científico da investigação.”.

A presente pesquisa baseia-se nos desafios da segurança cibernética no ciberespaço moçambicano. Diante disso, são identificadas ameaças cibernéticas, entre elas ataques como *phishing*, *spam*, *malwares*, entre outros (descrito no subcapítulo 2.1.1), tendo foco os ataques envolvendo as redes *Botnets*, autor de diferentes tipos de ataques de larga escala e de danos imensuráveis no ciberespaço, podendo causar impactos significativos em uma infraestrutura de rede. Contudo, torna-se fundamental estudar essa tipo de ameaça, como sustenta o Marcelino (2021, p. 121), a “ocorrência que representa uma ameaça ou um ataque cibernético pode ser considerado um incidente cibernético que pode escalar para um conflito no espaço cibernético.”.

Para o estudo do problema envolvendo ataques de *Botnets*, foi identificado a MoRENet como o caso de estudo da pesquisa (descrito no subcapítulo 3.1.1). A MoRENet é uma rede de larga escala no ciberespaço moçambicano que conecta diversas instituições beneficiárias. Tem a segurança cibernética como um dos serviços essenciais oferecidos pelo CSIRT da MoRENet, que actua como ponto central de contacto e resposta para incidentes de segurança na comunidade académica e científica nacional.

Entretanto, a problemática da pesquisa revela que as actividades de redes de *Botnets* representam um dos problemas mais persistentes e complexos em infraestruturas de redes de grande porte, a semelhança da MoRENet. Descreve as *Botnets*, autores de maiores ataques no ciberespaço global tanto Africano, infectando diversos dispositivos para ataques de larga dimensão em infraestruturas que gerem um enorme volume de tráfego, comprometendo serviços e sistemas críticos. Esse cenário contribuiu na fundamentação da pesquisa sobre as actividades de redes de *Botnets* no ciberespaço moçambicano, abordando a questão: - Como a implementação do protocolo *NetFlow* pode auxiliar na detecção proactiva de *Botnets* na infraestrutura de sistemas de informação do Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet)?

5.2.2. Revisão da literatura

De acordo com Prodanov & Freitas (2013), a revisão da literatura tem papel fundamental na pesquisa científica, sendo ela o ponto de partida que reúne o conhecimento produzido em pesquisas anteriores, destacando conceitos, procedimentos, resultados, discussões e conclusões relevantes para a pesquisa em questão. A revisão da literatura do estudo foi voltada ao fornecimento de bases teórica, estruturando-se em três (3) fases principais.

I. Segurança cibernética em Moçambique

A primeira fase da revisão da literatura apresenta as características do ciberespaço moçambicano em termos da segurança cibernética (descrito no subcapítulo 2.1), destacando-se os conceitos fundamentais, a evolução, engrenagem e o cenário do ciberespaço moçambicano. De seguida aborda os principais ataques cibernéticos emergentes, bem como, as políticas e as leis de segurança cibernética voltadas à securitização do ciberespaço nacional.

II. *Botnets*

A segunda fase aborda a natureza das redes *Botnets* (descrito no subcapítulo 2.2), abordando os conceitos, arquitecturas, principais protocolos e tipos de ataques. Essas abordagens são essenciais para o entendimento geral das *Botnets*, pois permitem compreender como as redes *Botnets* operam em infraestruturas de SI. Foram ainda apresentadas técnicas de detecção das redes *Botnets* com base na classificação de Shinan et al., (2021), que inclui abordagens por IDS, DNS e *Honeynet*.

III. Soluções de análise de tráfego de rede na detecção de *Botnets*

A terceira fase apresenta as diferentes soluções de análise de tráfego de rede (descrito no subcapítulo 2.3), nomeadamente: - o *NetFlow*, o *Zeek* e o *sFlow*. As *Botnets* têm como peculiaridades o uso de tráfego de rede para efectuar e coordenar as suas acções. Nesse contexto, busca-se avaliar através de estudos eficácia de cada solução na detecção de redes *Botnets* em uma infraestrutura de rede.

5.2.3. Caso de estudo

Conforme Gil (2008), o estudo de caso é caracterizado por uma análise profunda e exaustiva de um ou poucos objectos de pesquisa, permitindo um conhecimento detalhado que seria difícil de alcançar por meio de outros tipos de delineamentos, como um estudo de uma entidade, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social. O caso de estudo da presente pesquisa se concentra é um projecto do Governo de Moçambique, nomeadamente MoRENet (Rede de Instituições de Ensino Superior e de Investigação de Moçambique), está que está afecto ao INAGE, IP (Instituto Nacional do Governo Electrónico). A MoRENet contém uma infraestrutura de larga escala que desempenha um papel de relevo no ciberespaço moçambicano, oferecendo diversos serviços como a conectividade para diversas instituições beneficiárias, como as universidades, centros de pesquisa entre outros.

Um dos serviços da MoRENet é a segurança cibernética através do CSIRT da MoRENet, responsável pela gestão de incidentes de segurança e de implementar medidas de protecção para assegurar a integridade e disponibilidade na rede. No entanto, apresenta-se a situação actual da MoRENet em termos da segurança cibernética (descrito no

subcapítulo 3.1.2), com base nas percepções dos profissionais da MoRENet recolhidos através do questionário e da entrevista. O levantamento inclui desde a situação da segurança cibernética até à ocorrência de incidentes associados a redes *Botnets*, o que contribuiu na avaliação da proposta de implementação do protocolo *NetFlow* para a detecção de *Botnets* na infraestrutura da MoRENet, tendo em conta que a detecção dessas ameaças continua a ser um desafio crítico na sua infraestrutura da MoRENet.

5.2.4. Proposta de solução

De acordo com Prodanov & Freitas (2013), a solução proposta é uma conjectura de ideias ou teorias deduzidas a partir das proposições "hipóteses ou premissas" sujeitas a testes, onde, a pesquisa engloba um conjunto de acções, propostas para encontrar a solução para um problema, as quais têm por base procedimentos racionais e sistemáticos. A presente pesquisa propõe a implementação do protocolo *NetFlow* como uma solução proactiva para a detecção de *Botnets* na infraestrutura de sistemas de informação da MoRENet, conforme sustenta o Ribeiro (2020, p. 21), "uma das soluções mais comuns para detecção de *Botnets* consiste em desenvolver sistemas para analisar o tráfego da rede e identificar componentes maliciosos.".

A solução proposta (descrita no subcapítulo 4.1) vem do superposto do problema identificado e recorrente no ciberespaço global bem como moçambicano, relacionado com ameaças cibernéticas em destaque as redes de *Botnets*. O protocolo *NetFlow* se destacou durante a pesquisa por sua capacidade de monitorar e analisar fluxos de tráfego de rede; fornecendo informações detalhadas sobre o comportamento dos dispositivos conectados. Essas informações mostram-se fundamentais para a identificação de anomalias e ataques cibernéticos, especialmente aqueles associados a actividades de *Botnets*.

A construção e implementação da solução baseou-se na análise da situação actual da MoRENet e foi estruturada nas seguintes etapas:

- Justificativa da escolha do *NetFlow*, em comparação com *Zeek* e *sFlow*;
- Definição dos recursos necessários, sendo tecnológicos, humanos e financeiros;
- Apresentação do cronograma de implementação da solução proposta;
- Descrição da arquitectura da proposta, abrangendo:

- Captura e colecta de tráfego de rede;
- Análise e correlação com servidores de C&C (*Botnets*);
- Monitoramento e visualização dos resultados;

- Identificação dos riscos operacionais da solução proposta;
- Ilustração da topologia do cenário final após a implementação da solução.

I. Funcionamento da solução na infraestrutura da MoRENet (Impactos, Limitações e Melhorias)

A escolha do protocolo *NetFlow* como proposta de solução para a detecção de *Botnets* na infraestrutura da MoRENet, foi fundamentada em diversos critérios técnicos e operacionais. Conforme apresentado na Tabela 5, o *NetFlow* destacou-se como solução adequada para uma infraestrutura de grande porte como a da MoRENet, devido a sua capacidade de gerar metadados de tráfego em larga escala com baixo impacto no desempenho da rede, além de sua compatibilidade nativa com os equipamentos Cisco em operação na infraestrutura da MoRENet. Conforme sustenta o Amini et al., (2014), no fluxo de rede, o *NetFlow* regista descrições de alto nível das ligações à *Internet* (metadados), como IPs de origem e destino, portas e protocolos, mas não os dados efetivamente transferidos.

Entretanto, a colecta de tráfego de rede através do *NetFlow*, observa algumas limitações importantes de destacar que podem afectar na precisão de detecção de anomalias associadas a *Botnets* na infraestrutura da MoRENet. Conforme mencionado no subcapítulo 2.3.2, Bilge et al., (2012), afirma que “sistemas de detecção de redes de *Botnets* baseado na análise dos dados *NetFlow* pode produzir resultados de conter alguns falsos positivos, […]”, isto devido à natureza limitada das informações extraídas.

Diante disso, é essencial considerar não apenas os benefícios, mas também os impactos e limitações operacionais da solução ao decorrer do seu funcionamento na infraestrutura, sobretudo na actividade primordial, a detecção de comunicações *Botnets*. Além disso, identificam-se pontos de melhoria que podem contribuir para a otimização e evolução da solução proposta. O Anexo 13 apresenta os impactos, limitações e pontos possíveis de melhorias da solução proposta.

CAPÍTULO VI: CONSIDERAÇÕES FINAIS

Este capítulo, é reservado a apresentação das considerações finais da pesquisa, com foco nas conclusões obtidas e as recomendações para futuras acções na temática apresentada pela pesquisa.

6.1. Conclusão

O estudo desenvolvido na presente monografia propôs a implementação do protocolo *NetFlow* como mecanismo proactivo de detecção de *Botnets*, baseado na análise de tráfego de rede na infraestrutura de sistemas de informação do Instituto Nacional de Governo Electrónico (INAGE, IP/MoRENet), tendo sido concluído que:

A problemática da segurança cibernética tem se mostrado como um tema de grande preocupação para o mundo, principalmente diante das ameaças emergentes como as *Botnets*, Moçambique não é excepção. Em análise ao cenário actual de cibersegurança no ciberespaço moçambicano, que é marcado por um aumento significativo de ataques cibernéticos e uma expansão do acesso à *Internet*, esta descreve a adopção de medidas adequadas para proteger os seus activos digitais. A proposta apresentada neste trabalho alinhou-se a essa necessidade, oferecendo uma nova abordagem para a detecção de ameaças, as *Botnets*, que representam um risco crescente para as infraestruturas de redes de grande escala no ciberespaço moçambicano, como a da MoRENet que interliga instituições acadêmicas do ensino superior, de investigação e do ensino técnico-profissional com recurso as Tecnologias de Informação e Comunicação (TICs).

Face as práticas e técnicas disponíveis para a detecção e mitigação de *Botnets* são destacadas uma combinação de diferentes técnicas, como sistemas de detecção de intrusão (IDS), análise de tráfego DNS e *Honeynets*. No contexto da MoRENet, essas abordagens podem ser utilizadas com base nas ferramentas já implementadas na infraestrutura que desempenham um papel importante na monitorização e na resposta a incidentes cibernéticas. No entanto, com a implementação da solução proposta pode-se complementar essas práticas e técnicas destacadas durante a pesquisa, proporcionando uma análise detalhada do tráfego de rede em tempo real e permitindo a identificação rápida de padrões anômalos e actividades suspeitas, fortalecendo a segurança de uma infraestrutura de SI como a da MoRENet.

Com base no exposto, a implementação do protocolo *NetFlow* foi apresentada como solução proposta. A proposta se destaca em diversos aspectos, com base aos critérios de avaliação estabelecidos que o relacionam as outras soluções apresentadas como o *Zeek* e o *SFlow*, tomando em conta aos dados colectados na infraestrutura do INAGE, IP/MoRENet. A solução denota como pontos fortes do protocolo *NetFlow* a sua compatibilidade com a infraestrutura existente, baixo custo de implementação, a escalabilidade e capacidade de integração com outras ferramentas de segurança. A mesma é descrita em diversas abordagens que permitem a identificação de padrões de tráfego associados a servidores de comando e controle (C&C) de *Botnets*, reduzindo a dependência de intervenção manual, e a visualização de resultados que proporciona a tomada de decisões e a resposta rápida a incidentes. Além disso, a solução proposta demonstrou baixo impacto no desempenho da rede, o que é fundamental para sua aplicação em ambientes de grande escala, semelhante à da MoRENet.

Os resultados obtidos com a análise da solução proposta, demostram a capacidade do protocolo *NetFlow* de correlacionar informações de tráfego rede com diversas listas de servidores C&C conhecidos para a detecção proactiva de *Botnets*. Esses resultados destacaram o potencial da solução proposta para fortalecer a segurança cibernética em uma infraestrutura, e mostraram-se eficiente na capacidade de resposta a ameaças cibernéticas em redes que gerem um grande volume de tráfego. Entretanto, a solução proposta não apenas mitiga os riscos associados a *Botnets*, mas também promove a conscientização sobre a importância da segurança cibernética, a necessidade de investimentos em tecnologias e capacitação de recursos humanos.

6.2. Recomendações

Diante da pesquisa, com base nos resultados obtidos e na análise das limitações identificadas, diversas recomendações são apresentadas visando contribuir para o avanço de futuras pesquisas, estando organizadas em dois (2) contextos:

I. No contexto da pesquisa

- A produção estudos locais focados nas actividades e impactos das *Botnets* no ciberespaço moçambicano, visando fornecer fundamentos teóricos para futuras pesquisas sobre essas ameaças;

- A elaboração de relatórios de incidentes cibernéticos envolvendo redes *Botnets* em Moçambique, como forma a aprimorar o entendimento sobre essas ameaças no contexto nacional.

II. No contexto do caso de estudo (MoRENet**)**

- O estudo contínuo de aprimoramentos na solução proposta descrita na presente pesquisa, explorando a integração com outras ferramentas e técnicas de detecção para enriquecer a sua abordagem na detecção de *Botnets*;
- O fortalecimento a infraestrutura por meio da actualização dos equipamentos tornando-a mais robusta, podendo ser capaz de ampliar a capacidade de análise do tráfego de rede na detecção de ameaças emergentes, incluindo as *Botnets*;
- A realização de testes de desempenho para avaliar o impacto operacionais da solução proposta na infraestrutura de rede da MoRENet;
- A contratação de mais profissionais qualificados e capacitação da equipa de segurança da MoRENet, para poder lidar com as novas ameaças emergentes, e acompanhar as novas soluções ou tecnologias de segurança cibernética.

6.3. Constrangimentos

Durante o desenvolvimento da presente pesquisa, foram identificados diversos constrangimentos que, em certa medida, impactaram o processo de elaboração e aprofundamento do estudo. A seguir, destacam-se:

- A escassez de estudos locais sobre a segurança cibernética no ciberespaço moçambicano, o que dificultou o acesso a informações específicas para o contexto da pesquisa;
- O número reduzido de participantes na colecta de dados e o acesso restrito a certas informações sobre cenário da segurança cibernética na MoRENet, o que impactou na análise abrangente;
- As integrações entre o *NetFlow* e as ferramentas adicionais, envolveram desafios técnicos que podia ser mais explorado e não foram, aspectos fundamentais na aplicação da solução que não puderam ser abordados de forma aprofundada.

REFERENCIAS BIBLIOGRÁFICAS

1. Alieyan, K., ALmomani, A., Manasrah, A., & Kadhum, M. M. (2017). A survey of botnet detection based on DNS. Neural Computing and Applications, 28(7), 1541–1558. https://doi.org/10.1007/s00521-015-2128-0
2. Amini, P., Azmi, R., & Araghizadeh, M. (2014). Botnet Detection using NetFlow and Clustering. 3(2).
3. Asha, S., Harsha, T., & Soniya, B. (2016). Analysis on botnet detection techniques. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), 1–4. https://doi.org/10.1109/RAINS.2016.7764411
4. Barbosa, K. R. S., Martins, G. B., Souto, E., & Feitosa, E. (2014). Botnets: Características e Métodos de Detecção Através do Tráfego de Rede.
5. Bilge, L., Balzarotti, D., Robertson, W., Kirda, E., & Kruegel, C. (2012). Disclosure: Detecting botnet command and control servers through large-scale NetFlow analysis. Proceedings of the 28th Annual Computer Security Applications Conference, 129–138. https://doi.org/10.1145/2420950.2420969
6. Cepik, M. A. C., & Marcelino, H. M. (2021). Segurança cibernética em Moçambique: Conceitos, infraestrutura e desafios de implementação. Carta Internacional, 16(3), e1130–e1130.
7. Ciampa, M. (2014). Security+ guide to network security fundamentals (5th Ed). Cengage Learning.
8. Cisco Systems, Inc. (2006). Introduction to Cisco IOS® NetFlow—A Technical Overview. 16.
9. Cisco Systems, Inc. (2008). Introduction to Cisco IOS® Flexible NetFlow. 21.
10. Cisco Systems, Inc. (2013). Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3S. 232.
11. Claise, B. (2004). Cisco Systems NetFlow Services Export Version 9 (Request for Comments RFC 3954). Internet Engineering Task Force. https://doi.org/10.17487/RFC3954

12. CNCS, C. N. de C. (2019). CNCS - Quadro Nacional de Referência para a Cibersegurança. https://www.sgeconomia.gov.pt/noticias/cncs-quadro-nacional-de-referencia-para-a-ciberseguranca.aspx
13. Conselho de Ministros: Resolução n.o 69/2021. (2021). Boletim da República- Política de Segurança Cibernética e Estratégia da sua Implementação. https://www.intic.gov.mz/wp-content/uploads/2022/05/BR_253_I_SERIE_12.o-SUPLEMENTO_2021_Politica-de-Seguranca-Cibernetica-e-Protecao-e-Estrategia-da-sua-Implementacao.pdf
14. Elastic Stack. (s.da). Kibana—Your window into Elastic. https://www.elastic.co/guide/en/kibana/current/introduction.html
15. Elastic Stack. (s.db). What is Elasticsearch? [Learn/Docs/Elasticsearch/Reference/8.14]. https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html
16. Elisan, C. C., & Hypponen, M. (2013). Malware, rootkits & botnets: A beginner's guide. McGraw-Hill.
17. Gallagher, C. R. (2021). Machine Learning for Malware Botnet Detection in IoT Devices.
18. Gerhardt, T. E., & Silveira, D. T. (2009). Métodos de Pesquisa. PLAGEDER.
19. Gil, A. C. (2002). Como elaborar projetos de pesquisa.
20. Gil, A. C. (2008). Métodos e técnicas de pesquisa social. Atlas. https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf
21. Gupta, B., & Dahiya, A. (2021). Distributed Denial of Service (DDoS) attacks: Classification, attacks, challenges and countermeasures (First edition). CRC Press.
22. Hachem, N., Ben Mustapha, Y., Granadillo, G. G., & Debar, H. (2011). Botnets: Lifecycle and Taxonomy. 2011 Conference on Network and Information Systems Security, 1–8. https://doi.org/10.1109/SAR-SSI.2011.5931395

23. Holzmacher, G. (2023, November 6). Zeek vs NetFlow: Why Léargas chose Zeek. Léargas Security. https://www.leargassecurity.com/zeek-vs-netflow-why-leargas-chose-zeek-over-netflow/
24. IBM. (s.d). What is NetFlow? | IBM. https://www.ibm.com/topics/netflow
25. INAGE, IP. (s.d). O INAGE – INAGE, IP. https://www.inage.gov.mz/index.php/o-inage/
26. INTIC. (2023a). Cerimonia de Lançamento da Pagina Web e dos Serviços do CSIRT Nacional (nCSIRT.MZ-CC). https://www.intic.gov.mz/wp-content/uploads/2023/04/INTIC-Apresentacao-CSIRT-cerimonia-de-lancamento.pdf
27. INTIC. (2023b, September 20). Ataques Cibernéticos atingem 1,5 Milhão por mês em Moçambique – Instituto Nacional de Tecnologias de Informação e Comunicação. https://www.intic.gov.mz/ataques-ciberneticos-atingem-15-milhao-por-mes-em-mocambique/
28. INTIC. (s.d). Propostas de Leis – Instituto Nacional de Tecnologias de Informação e Comunicação. https://www.intic.gov.mz/propostas-de-lei-em-curso/
29. IPCisco. (s.d). What is NetFlow? | 4 Steps NetFlow Cisco Configuration ⋆ IpCisco. IPCisco. https://ipcisco.com/lesson/netflow-and-netflow-configuration/
30. ITUPublications. (2018). Global Cybersecurity Index. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
31. ITUPublications. (2020). Global Cybersecurity Index. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
32. Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: Review, future trends, and issues. Journal of Zhejiang University SCIENCE C, 15(11), 943–983. https://doi.org/10.1631/jzus.C1300242
33. Kerlinger, F. N. (2001). Metodologia Da Pesquisa Em Ciencias Sociais: Um Tratamento Conceitual. Epu.
34. Kizza, J. M. (2024). *Guide to Computer Network Security* (6th ed. 2024). Springer International Publishing. https://doi.org/10.1007/978-3-031-47549-8
35. Li, B., Gunes, M. H., Bebis, G., & Springer, J. (2013). A supervised machine learning approach to classify host roles on line using sFlow. Proceedings of the First Edition

Workshop on High Performance and Programmable Networking, 53–60. https://doi.org/10.1145/2465839.2465847

36. Li, X., Wang, J., & Zhang, X. (2017). Botnet Detection Technology Based on DNS. Future Internet, 9(4), Article 4. https://doi.org/10.3390/fi9040055
37. Lu, Y., & Wang, M. (2016). An Easy Defense Mechanism Against Botnet-based DDoS Flooding Attack Originated in SDN Environment Using sFlow. Proceedings of the 11th International Conference on Future Internet Technologies, 14–20. https://doi.org/10.1145/2935663.2935674
38. Mammunni, S. R. (2020). An overview of botnet and its detection techniques. 8(3).
39. Marcelino, H. M. (2021). Segurança cibernética e ciberdefesa em Moçambique: Fundamentos, características e desafios.
40. Mathur, L., Raheja, M., & Ahlawat, P. (2018). Botnet Detection via mining of network traffic flow. Procedia Computer Science, 132, 1668–1677. https://doi.org/10.1016/j.procs.2018.05.137
41. Modelo de Negocio da MoRENet. (2017).
42. Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. Procedia Computer Science, 217, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339
43. Nokia. (2023). Relatório de inteligência de ameaças da Nokia descobre que a atividade maliciosa de botnet de IoT aumentou drasticamente | Nokia. https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/
44. O País. (2022, February 21). Portais do Governo “hackeados”, mas sem perda de informações, confirma o INAGE - O País—A verdade como notícia. https://www.opais.co.mz/portais-do-governo-hackeados-mas-sem-perda-de-informacoes-confirma-o-inage/
45. Ogu, E. C., Ojesanmi, O. A., Awodele, O., & Kuyoro, ‘Shade. (2019). A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far. Information, 10(11), Article 11. https://doi.org/10.3390/info10110337

46. O'Regan, G. (2016). Introduction to the history of computing: A computing history primer. Springer Berlin Heidelberg.
47. Phaal, P., & Lavine, M. (2004). sFlow Version 5. https://sflow.org/sflow_version_5.txt
48. Phaal, P., Panchen, S., & McKee, N. (2001). InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks (RFC3176; p. RFC3176). RFC Editor. https://doi.org/10.17487/rfc3176
49. Política e Estratégia Nacional de Segurança Cibernética. (2021, December 31). Política e Estratégia Nacional de Segurança Cibernética – Instituto Nacional de Tecnologias de Informação e Comunicação. https://www.intic.gov.mz/politica-de-seguranca-cibernetica-e-protecao-e-estrategia-da-sua-implementacao/
50. Positive Technologies. (2023, July 28). Cybersecurity threatscape of African countries 2022–2023. Ptsecurity.Com. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/
51. Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A., Zheng, K., & Zopf, M. (2022). Protecting information and system integrity in industrial control system environments: Cybersecurity for the manufacturing sector (NIST SP 1800-10; p. NIST SP 1800-10). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.1800-10
52. Prodanov, C. C., & Freitas, E. C. de. (2013). Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico | Cleber Cristiano Prodanov; Ernani Cesar de Freitas | download. 277.
53. Ribeiro, G. H. (2020). Detecção de botnets utilizando classiĄcação de fluxos contínuos de dados. 113.
54. Richard, L. (2021). African Cyberthreat Assessment Report. https://www.interpol.int/en/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf
55. Roshandel, S. (2022). Performance Analysis of a Graph-based Anomaly Detector and the Zeek Intrusion Detection System. 38.
56. Sadiqui, A. (2020). *Computer network security*. ISTE Ltd. https://zlib.pub/download/computer-network-security-218b0ntadc50

57. sFlow. (2003). Traffic Monitoring using sFlow. https://sflow.org/sFlowOverview.pdf
58. Shah, A., Khiyal, M., & Awan, M. (2015). Analysis of Machine Learning Techniques for Intrusion Detection System: A Review. International Journal of Computer Applications, 119, 19–29. https://doi.org/10.5120/21047-3678
59. Shinan, K., Alsubhi, K., Alzahrani, A., & Ashraf, M. U. (2021). Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review. Symmetry, 13(5), Article 5. https://doi.org/10.3390/sym13050866
60. TRIVIÑOS, A. N. S. (1987). Introdução à Pesquisa em Ciências Sociais—A Pesquisa Qualitativa em Educação. Atlas.
61. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
62. White, J., Jha, P., & Norman, D. (2021, July 29). Blog | The Mirai Botnet—Tips to Defend Your Organization. CIS. https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/
63. Zanella, L. C. H. (2013). Metodologia de Pesquisa (3rd ed.). http://arquivos.eadadm.ufsc.br/EaDADM/UAB_2014_2/Modulo_1/Metodologia/material_didatico/Livro%20texto%20Metodologia%20da%20Pesquisa.pdf
64. Zeek Documentation. (2024). Zeek Documentation—Book of Zeek (v7.0.1). https://docs.zeek.org/en/current/

ANEXOS

Anexo 1: Questionário aos profissionais da MoRENet

Abaixo está apresentado o questionário que foi dirigido aos profissionais da MoRENet, para a recolha de dados sobre a percepção da situação actual da infraestrutura de rede da MoRENet.

[Mensagem do Questionário]

Prezado,

Primeiramente agradecer por dedicar o seu tempo para participar deste questionário. O objectivo do questionário é obter informações sobre o estado da segurança cibernética na infraestrutura da MoRENet.

É de ressaltar que todas as informações fornecidas serão fundamentais e utilizadas para fins acadêmicos relacionados a elaboração do Trabalho de Licenciatura com o tema "Proposta de Implementação do Protocolo *NetFlow* como Mecanismo Proactivo de Detecção de *Botnets* Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação".

As respostas dadas não serão divulgadas ou compartilhadas com terceiros, sendo só utilizadas para fins investigação para o trabalho de culminação do curso!

Por favor, responda às perguntas abaixo de acordo com sua experiência e área de especialização:

Questionário aos Profissionais da MoRENet

Prezado,

Primeiramente agradecer por dedicar o seu tempo para participar deste questionário. O objectivo do questionário é obter informações sobre o estado da segurança cibernética na infraestrutura da MoRENet.É de ressaltar que todas as informações fornecidas serão serão fundamentais e utilizadas para fins acadêmicos relacionados a elaboração do Trabalho de Licenciatura com o tema "Proposta de Implementação do Protocolo NetFlow como Mecanismo Proativo de Detecção de Botnets Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação".As respostas dadas não serão divulgadas ou compartilhadas com terceiros, sendo só utilizadas para ¬ns investigação para o trabalho de culminação do curso!Por favor, responda às perguntas abaixo de acordo com sua experiência e área de especialização:

1 Genêro:

: *Selecione apenas uma resposta*

◯ Masculino ◯ Feminino

2 Cargo ou Função no CSIRT da Academia:

: *Por favor, selecione apenas uma opção*

◯ Analista de Segurança Cibernética ◯ Especialista em Redes ◯ Consultor de Segurança ◯ Especialista em Resposta a Incidentes

◯ Administrador de Sistema

◯ Outra (especifique, por favor) _____

3 Experiência em segurança cibernética

: *Por favor, selecione apenas uma resposta*

◯ Menos de 1 ano ◯ 1 a 3 anos ◯ 4 a 6 anos ◯ 7 a 10 anos ◯ Mais de 10 anos

4 Tempo de Trabalho no CSIRT da Academia:

: *Por favor, selecione apenas uma resposta*

◯ Menos de 1 ano ◯ 1 a 3 anos ◯ 4 a 6 anos ◯ 7 a 10 anos ◯ Mais de 10 anos

5 Como avalia o estado actual da segurança cibernética na infraestrutura da MoRENet?

: *Select one answer*

◯ Muito Baixo ◯ Baixo ◯ Médio ◯ Bom ◯ Muito Bom

6 Já presenciou ou tem conhecimento de incidentes relacionados a Botnets na infraestrutura da MoRENet?

: *Por favor, selecione apenas uma resposta*

◯ Nunca ◯ Raramente ◯ Algumas vezes ◯ Frequentemente ◯ Sempre

7 Acredita que o CSIRT da Academia está preparada para lidar com Botnets e outras ameaças cibernéticas?

: *Por favor, selecione apenas uma resposta*

◯ Sim ◯ Talvez ◯ Não

8 Com que frequência a equipe de CSIRT realiza análises de vulnerabilidade na infraestrutura?

: *Por favor, selecione duas (2) opcções no máximo*

☐ Diariamente ☐ Semanalmente ☐ Mensalmente ☐ Trimestralmente ☐ Somente após um evento de segurança (incidentes cibernéticos)

9 Como avalia o nível de eficácia das ferramentas de análise e gestão de vulnerabilidades utilizadas pelo CSIRT na detecção de anomalias?

: *Por favor, selecione apenas uma resposta*

◯ Muito Baixa ◯ Baixa ◯ Média ◯ Alta ◯ Muito Alta

10 Em sua opinião, a equipe do CSIRT é capaz de detectar actividades relacionadas a Botnets com as ferramentas actualmente implementadas?

: *Por favor, selecione apenas uma opção*

◯ Totalmente incapaz ◯ Incapaz ◯ Neutro ◯ Incapaz ◯ Totalmente capaz

11 O CSIRT da MoRENet realiza testes para avaliar se a infraestrutura está comprometida por anomalias, como Botnets?

: *Por favor, selecione apenas uma resposta*

◯ Nunca ◯ Raramente ◯ Algumas vezes ◯ Frequentemente ◯ Sempre

12 Na infraestrutura de rede da MoRENet existem mecanismos ou ferramentas para capturar e analisar o tráfego de rede?

: *Por favor, selecione apenas uma resposta*

◯ Sim ◯ Não

13 Qual é o seu nível de conhecimento sobre o protocolo NetFlow?

: *Por favor, selecione apenas uma resposta*

◯ Muito Baixa ◯ Baixa ◯ Média ◯ Alta ◯ Muito Alta

14 A gestão da infraestrutura de rede da MoRENet inclui estatísticas sobre o volume total de tráfego de rede que passa pela rede?

: *Por favor, selecione apenas uma resposta*

◯ Sim ◯ Não

15 Se a resposta for sim, com que frequência são colectadas essas estatísticas?

: *Por favor, selecione apenas uma resposta*

◯ Diariamente ◯ Semanalmente ◯ Mensalmente ◯ Quando solicitado

◯ Outro (especifique, por favor) _____

16 Com que frequência se observa padrões incomuns no tráfego de rede?

: *Por favor, selecione apenas uma resposta*

◯ Nunca ◯ Raramente ◯ Algumas vezes ◯ Frequentemente ◯ Sempre

17 Quais são os principais obstáculos na implementação de novas soluções de segurança, como o NetFlow para a detecção de Botnets?

: *(Selecione todas as opções que se aplicam)*

◯ Falta de orçamento ◯ Falta de treinamento ◯ Constrangimentos técnicos ◯ Resistência à mudança ◯ Outros

Anexo 2: Entrevista aos profissionais do CSIRT da MoRENet

Agradecer a disponibilidade dos profissionais do CSIRT da MoRENet de participar desta entrevista. O objectivo é obter dados acerca dos desafios e práticas enfrentados pela equipe do CSIRT na detecção e mitigação de ameaças cibernéticas, incluindo ataques *Botnets* na infraestrutura da MoRENet. As respostas fornecidas serão fundamentais para a elaboração do Trabalho de Licenciatura intitulado “Proposta de Implementação do Protocolo *NetFlow* como Mecanismo Proactivo de Detecção de *Botnets* Baseada na Análise de Tráfego de Rede em uma Infraestrutura de Sistema de Informação”.

Frisar que as respostas dadas não serão divulgadas ou compartilhadas com terceiros, sendo só utilizadas para fins investigação para o trabalho de culminação do curso!

1. Qual é a sua percepção sobre o estado actual da segurança cibernética na infraestrutura de sistemas de informação da MoRENet?
2. Em termos de tráfego de rede, é feito o monitoramento em tempo real? Quais padrões incomuns mais observados no tráfego monitorado?
3. Na sua opinião, quais são as principais vulnerabilidades ou pontos fracos da infraestrutura de rede da MoRENet em relação à segurança cibernética?
4. A equipe do CSIRT já lidou com incidentes relacionados a *Botnets* na MoRENet? Se sim, qual foi o impacto mais significativo de uma actividade de *Botnets* na infraestrutura da MoRENet?
5. Que ferramentas de análise e gestão de vulnerabilidades são utilizadas pelo CSIRT?
6. Qual é o seu nível de conhecimento sobre o protocolo *NetFlow* e como ele pode ser utilizado na análise de tráfego de rede?
7. Quais são os principais obstáculos que enfrentados ao se implementar novas soluções de segurança na infraestrutura da MoRENet? Existem constrangimentos técnicos e operacionais na implementação?
8. Com as ferramentas ou soluções actualmente implementadas na infraestrutura, a equipe do CSIRT da MoRENet consegue detectar com eficácia anomalias, incluindo actividades relacionadas a *Botnets*?

Anexo 3: Leis regulatórias no ciberespaço Moçambicano

Nº	Documento	Referência	Estado
1	Regulamento de Controlo de Tráfego de Telecomunicações	Decreto n.º 75/2014, de 12 de Dezembro	Aprovado
2	Lei de Telecomunicações	Lei n.º 4/2016, de 3 de Junho	Aprovado
3	Lei de Transacções Electrónicas	Lei n.º 3/2017, de 9 de Dezembro	Aprovado
4	Regulamento do Quadro de Interoperabilidade de Governo Electrónico	Decreto n.º 67/2017, de 1 de Dezembro	Aprovado
5	Política para a Sociedade da Informação	Resolução n.º 17/2018, de 21 de Junho	Aprovado
6	Regulamento de Protecção do Consumidor do Serviço de Telecomunicações	Decreto n.º 44/2019, de 22 de Maio	Aprovado
7	Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais	Resolução n.º 5/2019, de 20 de Junho	Ratificada
8	Regulamento de Segurança de Redes de Telecomunicações	Decreto n.º 62/2019, de 1 de Agosto	Aprovado
9	Política e Estratégia Nacional de Segurança Cibernética	Resolução n.º 69/2021, de 31 de Dezembro	Aprovado
10	Regulamento do Sistema de Certificação Digital de Moçambique	Decreto n.o 59/2019, de 1 de Dezembro	Aprovado
11	Código Penal	Lei n.º 24/2019, de 24 de Dezembro	Aprovado
12	Regulamento do Domínio .mz	Decreto n.º 82/2020, de 10 de Setembro	Aprovado
13	Proposta da Lei de Segurança Cibernética		Pendente
14	Proposta de Lei de Crimes Cibernéticos		Pendente
15	Proposta de Lei de Protecção de Dados		Pendente
16	Convenção de Budapest		Pendente

Tabela A3 - 1. Leis regulatórias para segurança cibernética em Moçambique

Fonte: Adaptado pelo autor com base em dados fornecidos por (Conselho de Ministros: Resolução n.º 69/2021 2021) (PENSC), (INTIC, s.d)

Anexo 4: Especificações dos principais equipamentos nos PoPs de Maluana e MCTESTP (MCTD)

Equipamento	Especificações

Router - Cisco ASR 1004		
	Formato	Montável em *rack*, 4U
	Processador	Processador Cisco *QuantumFlow* (QFP)
	Largura de banda	10 até 40 Gbps
	Interface	Suporta SPA (Adaptadores de Porta Compartilhada), 4 portas Gigabit Ethernet integradas
	Redundância	Fontes de alimentação redundantes
	Memória	4 GB DRAM RP1 8 GB DRAM RP2
	Sistema Operacional	Cisco IOS XE
	Peso	15,88 kg

Router - Cisco ASR 1002 HX		
	Formato	Montável em *rack*, 2RU
	Processador	Processador Cisco *QuantumFlow* (QFP)
	Largura de banda	Até 100 Gbps
	Interface	6 x 10 GE fixas, suporta até 4 interfaces modulares
	Redundância	Fontes de alimentação redundantes
	Memória	16 GB DRAM (expansível)
	Sistema Operacional	Cisco IOS XE
	Peso	19,05 kg

Switch - Cisco 3750 x series		
	Formato	Montável em *rack*, 1U
	Portas	24 ou 48 portas Gigabit Ethernet
	Uplinks	Opções modulares de *uplink* (1GE ou 10GE)
	Empilhamento (*Stacking)*	Até 9 *switches* com tecnologia Cisco *StackWise*
	Suporte PoE/PoE+	Disponível em modelos selecionados

	Capacidade de Comutação	160 Gbps
	Redundância	Fontes de alimentação redundantes
	Sistema Operacional	*Software* Cisco IOS
	Peso	7,0 kg
	Fonte de Alimentação	Opções de 350W, 715W, 1100W (redundantes)

Server - HP Proliant DL380 gen7		
	Formato	Montável em *rack*, 2U
	Processador	Intel Xeon série 5600
	Memória	Até 192 GB DDR3
	Discos	Suporta até 16 SFF ou 8 LFF drives
	Interface de Rede	4 portas GbE embutidas
	Redundância	Fontes de alimentação e ventoinhas redundantes e *hot plug*
	Sistemas Operacionais	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware
	Peso	27,22 kg
	Fonte de Alimentação	Opções de 460W, 750W, 1200W (redundantes)

Server - HP Proliant DL380 gen8		
	Formato	Montável em *rack*, 2U
	Processador	Intel Xeon E5-2600 / E5-2600 v2
	Memória	Até 768 GB DDR3
	Discos	Suporta até 8 SFF ou 4 LFF drives
	Interface de Rede	4 portas GbE embutidas
	Redundância	Fontes de alimentação e ventoinhas redundantes e *hot plug*
	Sistemas Operacionais	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware
	Peso	15,5 kg
	Fonte de Alimentação	Opções de 460W, 750W, 1200W (redundantes)

Tabela A4 - 1. Especificações dos equipamentos nos PoPs da MoRENet

Fonte: Adaptado pelo autor

Anexo 5: Soluções de segurança cibernética e sua aplicabilidade na MoRENet

a) Principais soluções de segurança cibernética adoptadas na MoRENet

Categorias	Ferramentas
Monitoramento e Resposta a Incidentes	*Wazuh, SecurityOnion, Elastic Stack (ELK), RTIR, Ansible*
Gestão de Vulnerabilidades e Auditoria (*PenTest*)	*Nessus, OpenVAS, Nmap, Nikto, Metasploit, Kali Linux*
Detecção e Prevenção de Intrusões (IDS/NIDS/NIPS)	*Zeek, Suricata, Snort*
Protecção de Infraestrutura e *Endpoints*	*pfSense, PaloAlto, Kaspersky, Bitdefender, OpenVPN, Wazuh*
Criptografia e VPN	*OpenSSL, GlobalProtect (PaloAlto), OpenVPN*
Forense e Compartilhamento de Ameaças	*Autopsy, MISP*

Tabela A5 - 1. Principais soluções de segurança cibernética na MoRENet

Fonte: Elaborado pelo Autor

b) Aplicabilidade das soluções contra ameaças cibernéticas na MoRENet

Ameaças	Métodos de Ataques	Ferramenta de Mitigação
Phishing e Engenharia Social	*Phishing* de credenciais, Falsificação de identidade	RTIR - gestão de incidentes, rastreando e-mails maliciosos
Exploração de Vulnerabilidades	Exploração de Vulnerabilidades de *software* e de configuração	OpenVAS –identificação de falhas ou vulnerabilidades. Wazuh (SIEM) – Monitoramento e alerta em tempo real.
Malwares (*ransomwares*)	Injeção de *malwares*, Criptografia de dados, sequestro de sistemas	Wazuh (SIEM) – Detecção e correlação de eventos anômalos (*malwares*) para resposta rápida.
Ataques Força Bruta (acesso remoto)	Tentativas de *login*, ataque de dicionário, quebra de credenciais	Wazuh (SIEM) – Análise de registos (*logs*) e alertas de comportamento anômalo.
Exploração Remota / *Botnets* (Máquinas *Bot's*)	DDoS, controlo remoto de máquinas *Bots*, propagação de *Botnets*	RTIR – Gestão de incidentes e resposta a ataques externos envolvidos em redes *Botnets*

Tabela A5 - 2. Soluções de segurança contra ameaças cibernéticas na MoRENet

Fonte: Elaborado pelo Autor

Anexo 6: Plano de treinamento para implementação e manutenção da solução na MoRENet

a) Perfis de profissionais para a implementação da solução proposta na infraestrutura da MoRENet

Perfil Profissional	Função	Qualificações Necessárias	Quantidade
Especialistas em Segurança da Informação	Configuração inicial do Protocolo *NetFlow* infraestrutura de rede da MoRENet Integração com SIEM (*SecurityOnion*, *ELK Stack*) Monitoramento de dados colectados na rede para a detecção de ameaças como *Botnets*	-Nível Superior em Engenharia Informática, Ciência da Computação ou áreas relacionadas; -Experiência mínima de 2 anos em actividades de SOC/CSIRT com: Arquitetura e Protocolos de Segurança: TLS/SSL, IPSec, VPN, SAML, OAuth Ferramentas de Segurança: SIEM, IDS/IPS, *Firewall* Gestão de Riscos e *Compliance*: LGPD, GDPR, ISO 27001, NIST, PCI-DSS Análise de Vulnerabilidades: *Nmap*, *Nessus*, *OpenVAS*, *Metasploit* Forense Digital: *Autopsy*, *Volatility*, FTK, *Wireshark* Pentest/Testes de Intrusão: Kali Linux, OWASP Top 10 -Possuir certificações como CCNA *Security*, CISSP, CEH, ISO/IEC 27001 ou CompTIA *Security+*	2
Analistas de SOC (*Security Operations Center*)	Monitoramento de alertas em tempo real para a detecção de ameaças como *Botnets* Investigação de incidentes na infraestrutura da MoRENet Coordenação de respostas a ameaças como *Botnets*	-Nível Superior em Engenharia Informática, Ciência da Computação ou áreas relacionadas; -Experiência mínima de 2 anos em actividades de SOC/CSIRT com: Monitoramento de Segurança: uso de SIEMs como *SecurityOnion*, *Wazuh*, *Elastic Stack* (ELK) Análise de *Logs* e Eventos: Investigação de alertas gerados por: *Firewall*, IDS/IPS, Antivírus, EDR/XDR Protocolos e Arquitetura de Redes: TCP/IP, DNS, HTTP, VPNs, IPSec, TLS/SSL Detecção e Resposta a Incidentes (SOC Tier 1, Tier 2) Ferramentas de Defesa e Análise: SIEM, EDR/XDR, *Firewall*, IDS/IPS e *Threat Intelligence*	1

		Forense Digital e Análise de *Malware*: *Wireshark*, *Volatility*, *Autopsy*, *YARA* Automação e *Scripting*: *Python*, *Bash* -Certificações como CEH, GCIH, GSEC ou CySA+	
Administradores de Rede	Configuração inicial do Protocolo *NetFlow* infraestrutura de rede da MoRENet Garantir desempenho eficiente do *NetFlow* na Infraestrutura da MoRENet Configuração e manutenção dos equipamentos de rede	-Nível Superior em Engenharia Informática, Engenharia de Telecomunicações ou áreas relacionadas. -Experiência mínima de 3 anos com conhecimento avançado em: Protocolos de Rede: TCP/IP, DNS, DHCP, BGP, OSPF, MPLS, SNMP Administração de servidores Linux Segurança de Rede: *Firewalls*, VPNs, IDS/IPS Monitoramento e Diagnóstico: *Zabbix*, *NetFlow* Gerenciamento de Redes: VLANs, QoS, SDN, Wi-Fi -Certificações como Cisco CCNA/CCNP, CompTIA *Network+*	2
Desenvolvedores ou Analistas de Dados	Configuração de ferramentas de análise de dados (*ELK Stack*) Desenvolvimento e manutenção de *scripts* para automação de processos Desenvolver *dashboards* e relatórios gerenciais	-Nível Superior em Engenharia Informática, Engenharia de Telecomunicações ou áreas relacionadas. -Experiência mínima de 4 anos com conhecimento avançado em: Linguagens de Programação para Análise de Dados: *Python* (*Pandas*, *NumPy*, *Scikit-learn*), SQL Manipulação e Transformação de Dados: SQL, ETL DevOps para Dados: *Docker*, *Kubernetes*, *Terraform* Certificações como *Azure Data Engineer Associate*	2

Tabela A6 - 1. Perfis de profissionais para a implementação da solução proposta

Fonte: Elaborado pelo autor

b) Plano de treinamento para implementação da solução

Perfil Profissional	Tópicos do Treinamento	Objectivos do Treinamento	Método de Treinamento
Especialistas em Segurança da Informação	Configuração inicial do *NetFlow* e *NFDump*	Garantir colecta precisa de dados de rede	Teórico e Laboratório prático
	Integração do *NetFlow* com ferramentas adicionais	Configurar ferramentas para detecção de *Botnets*	
	Políticas de segurança	Implementar políticas de segurança cibernética	
Analistas de SOC (*Security Operations Center*)	Monitoramento e análise de alertas	Praticas de monitoramento e análise de incidentes cibernéticos para a detecção de anomalias (*Botnets* ou outras)	Simulações e exercícios práticos
	Resposta a incidentes de segurança	Coordenação e mitigação de incidentes cibernéticos na infraestrutura	
	Correlacção de eventos	Otimização e interpretação de alertas e eventos na infraestrutura (*Botnets*)	
Administradores de Rede	Configuração de equipamentos de rede	Garantir a configuração dos equipamentos de rede	Teórico e Laboratório prático
	Configuração e otimização do desempenho do *NetFlow*	Configurar o *NetFlow* na infraestrutura e testar o seu desempenho na rede	
	Segurança na transmissão de dados	Manter segurança na colecta de tráfego na rede	
Desenvolvedores ou Analistas de Dados	Integração de *scripts* com *NetFlow*	Desenvolver *scripts* para automatizar a correlacção de dados colectados	Laboratório prático
	Configuração de *dashboards* no *Kibana* (analista de dados)	Configurar o painel de visualização dos dados correlacionados	

Tabela A6 - 2. Plano de treinamento para implementação da solução proposta

Fonte: Elaborado pelo autor

c) Plano de treinamento para manutenção da solução

Perfil Profissional	Tópicos do Treinamento	Objectivos do Treinamento	Método de Treinamento
Especialistas em Segurança da Informação	Segurança na colecta de dados	Assegurar a colecta de dados e segurança na transmissão do tráfego de rede	Simulações e Laboratório prático
	Funcionamento do *NetFlow* e integração com soluções novas	Manter e melhorar a solução para a detecção *Botnets* e de anomalias emergentes	
	Ajustes de políticas de monitoramento	Alinhar políticas às melhores práticas	
Analistas de SOC (*Security Operations Center*)	Investigação de incidentes	Melhorar a correlacção de eventos e alertas na infraestrutura (*Botnets*)	Simulações e exercícios práticos
	Revisão das plataformas de monitoramento	Manter o funcionamento das plataformas de monitoramento de ataques *Botnets*	
Administradores de Rede	Manutenção preventiva de equipamentos	Garantir a disponibilidade dos equipamentos para funcionamento da solução	Simulações e Laboratório prático
	Otimização e controle de desempenho do *NetFlow*	Reduzir falhas e perda de dados de tráfego de rede (falsos negativos e positivos)	
	Actualizações do protocolo *NetFlow*	Manter o protocolo *NetFlow* e as suas dependências actualizadas	
Desenvolvedores ou Analistas de Dados	Otimização de *Dashboards* (analista de dados)	Melhorar visualização de dados da correlacção de *Botnets*	Simulações e Laboratório prático
	Manutenção de *scripts* de correlacção	Garantir o funcionamento e precisão na correlacção de *Botnets*	
	Ajustes na visualização de dados	Adaptar os dados disponibilizados para a análise as necessidades de segurança	

Tabela A6 - 3. Plano de treinamento para manutenção da solução proposta

Fonte: Elaborado pelo autor

Anexo 7: Cronograma para implementação da solução na MoRENet

Etapa	Descrição	Duração Estimada	Responsáveis
Planificação	Definição de requisitos, escopo e estratégias de implementação.	2 semanas	Gestor do Projecto; Equipe de Segurança
Instalação e Configuração do *NetFlow*	Configuração do *NetFlow* e integração com a infraestrutura existente.	1 semanas	Administradores de Rede
Implementação das Ferramentas	Instalação, integração e configuração das ferramentas complementares (*NFDump*, *ELK Stack*, *Scripts*, etc).	2 semanas	Profissionais de Segurança, Rede, Desenvolvedores / Analistas de dados
Testes e Validação	Verificação da funcionamento e desempenho da solução implementada.	2 semanas	Equipe de Segurança; Analistas SOC
Operação da Solução	Início da operação da solução com monitoramento e detecção de *Botnets* activo.	Contínuo	Todos equipa de profissionais envolvido
Capacitação da Equipe	Treinamento específico para operação e manutenção da solução.	3 semanas	Profissionais Internos/Externos
Manutenção Contínua	Atividades regulares de monitoramento, suporte e actualizações.	Contínuo	Profissionais Internos/Externos

Tabela A7 - 1. Cronograma para implementação da solução proposta

Fonte: Elaborado pelo autor

Anexo 8: Configurações da etapa da captura e colecta de amostras de tráfego de rede

a) Configurações da implementação do *NetFlow*

Configuração *NetFlow* nos Roteadores (PoP do MCTESTP (MCTD) e de Maluana)

Definição dos campos de tráfego de rede serem monitorados e colectados.		
Configuração do registo de fluxo *(Flow Record*)		
	Comando	Objectivo
1	R1(config)# flow record <*record-name*> R1(config)# flow record MoRENet-CSIRT	Cria um novo registo de fluxo com um nome de registo Nome registo = "MoRENet-CSIRT"
2	R1(config-flow-record)# match ipv4 source address	Captura o endereço IP de origem dos pacotes IPv4
4	R1(config-flow-record)# match ipv4 destination address	Captura o endereço IP de destino dos pacotes IPv4
5	R1(config-flow-record)# match ipv4 protocol	Captura o protocolo IPv4
6	R1(config-flow-record)# match transport destination-port	Captura a porta de destino do transporte
7	R1(config-flow-record)# match transport source-port	Captura a porta de origem do transporte
8	R1(config-flow-record)# match ipv4 tos	Captura o campo *Type of Service* (ToS) dos pacotes IPv4
9	R1(config-flow-record)# collect counter bytes	Colecta o número total de *bytes* transmitidos
10	R1(config-flow-record)# collect counter packets	Colecta o número total de pacotes transmitidos
11	R1(config-flow-record)# collect timestamp sys-uptime first	Colecta o *timestamp* do primeiro pacote visto (*sys-uptime*)
12	R1(config-flow-record)# collect application name	Colecta o nome da aplicação

Definição de onde os dados *NetFlow* colectados serão enviados		
Configuração do exportador de fluxos (*Flow Exporter*)		
	Comando	Objectivo
1	R1(config)# flow exporter <*exporter-name*> R1(config)# flow exporter MoRENet-CSIRT	Cria um novo exportador de fluxo com um nome Nome = "MoRENet-CSIRT"

2	R1(config-flow-exporter)# destination <*IP_address*>	Especifica o endereço IP do colector *NetFlow* para onde os dados serão exportados
4	R1(config-flow-exporter)# source <interface> → (e.g. use a Loopback)	Define a interface de origem usada para enviar os dados *NetFlow* (neste caso, a *interface Loopback0*)
5	R1(config-flow-exporter)# transport udp <*udp-port*>	Define o protocolo de transporte (UDP) e a porta (x) usada para enviar os dados *NetFlow* ao colector

Combinação do registo e o exportador de fluxo		
Configuração do monitor de fluxo (*Flow Monitor*)		
	Comando	Objectivo
1	R1(config)# flow monitor <*monitor-name*> R1(config)# flow monitor MoRENet-CSIRT	Cria um novo monitor de fluxo com um nome Nome = "MoRENet-CSIRT"
2	R1(config-flow-monitor)# record <*exporter-name*> R1(config-flow-monitor)# record MoRENet-CSIRT	Associa o registo de fluxo criado ao monitor de fluxo. Registo de fluxo = "MoRENet-CSIRT"
3	R1(config-flow-monitor)# exporter <*exporter-name*> R1(config-flow-monitor)# exporter MoRENet-CSIRT	Associa o exportador de fluxo criado ao monitor de fluxo. Monitor de fluxo = "MoRENet-CSIRT"
4	R1(config-flow-monitor)# cache timeout active <*seconds*> R1(config-flow-monitor)# cache timeout active 60	Define o tempo limite do cache ativo. Isso significa que os fluxos serão exportados a cada 60 segundos.

Aplicar monitor de fluxo a uma interface específica (*captura tráfego de entrada e saída*)		
Configuração da interface		
	Comando	Objectivo
1	R1(config)# interface <*type-number*>	Configura a interface ou subinterface
2	R1(config-subif)# description LINK to <*Link*>	Adiciona uma descrição à interface, indicando a ligação
3	R1(config-subif)# encapsulation dot1Q <*sub-interface*>	Define a encapsulação VLAN 802.1Q com o ID da VLAN xyz

4	R1(config-subif)# ip flow monitor <*monitor-name*> input	Aplica o monitor de fluxo MoRENet-CSIRT ao tráfego de entrada na interface.
5	R1(config-subif)# ip flow monitor <*monitor-name*> output	Aplica o monitor de fluxo MoRENet-CSIRT ao tráfego de saída na interface.

Tabela A8 - 1. Configurações do *NetFlow* nos roteadores da MoRENet

Fonte: Adaptado pelo autor

b) Resultados da implementação do *NetFlow*

A Figura A8 - 1 apresenta os resultados esperados após a execução dos comandos de verificação, os quais permitem confirmar a correcta aplicação das configurações do *NetFlow* nos roteadores do PoP do MCTESTP (MCTD) e de Maluana.

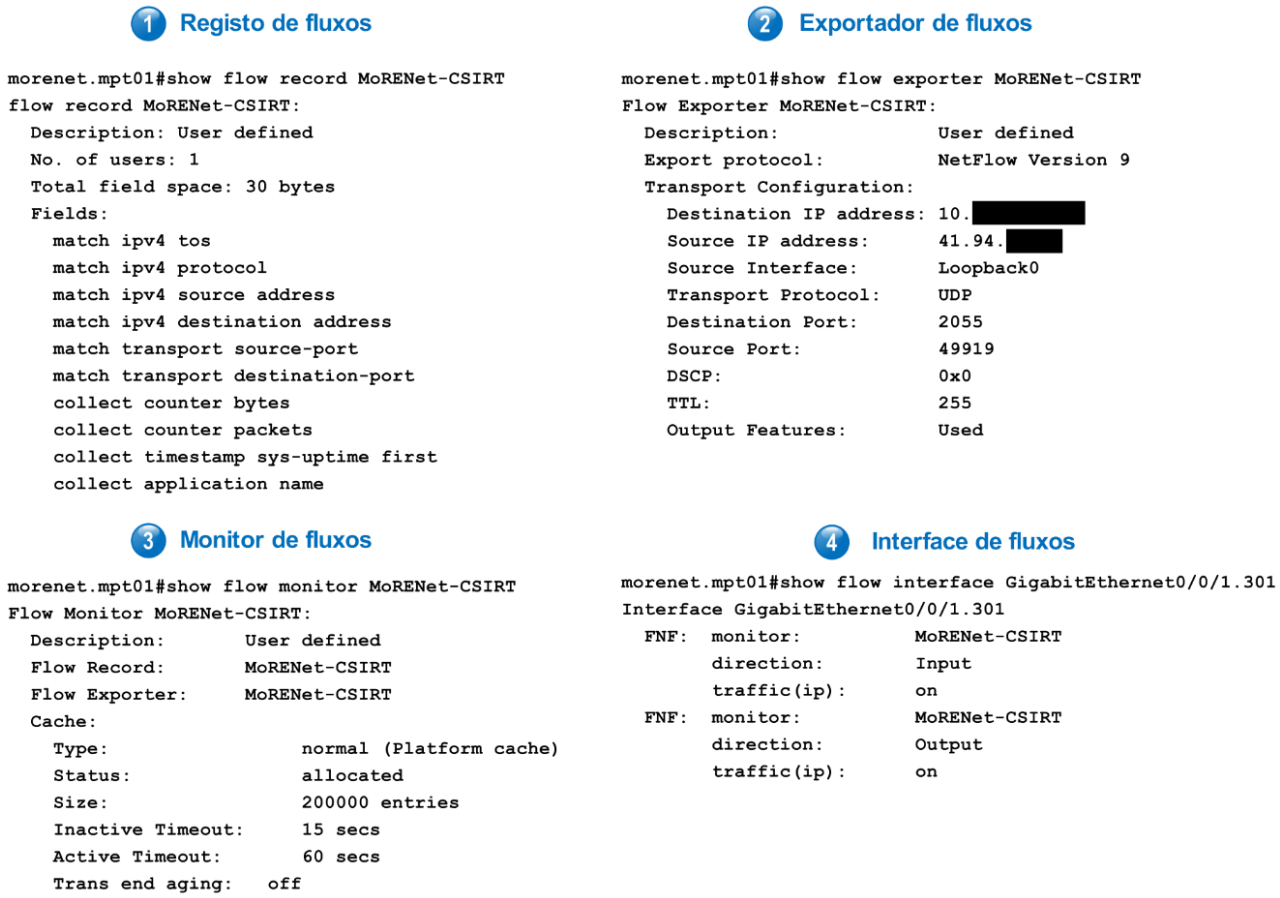


Figura A8 - 1. Verificação das configurações do *NetFlow* nos roteadores

Fonte: Adaptado pelo Autor

c) Configurações da implementação do *NFDump*

Após a configuração do *NetFlow* nos dispositivos de borda, é necessário a configurar o destino de exportação dos fluxos de rede colectados. Para esse fim, será configurada a ferramenta *NFDump,* responsável pelo armazenamento das amostras de tráfego colectadas para o servidor colector *NetFlow* localizado no PoP de Maluana.

Instalação do *NFDump*	
sudo apt-get -y install nfdump	instala o pacote *NFDump* no sistema

Directório para Armazenamento dos Dados *NetFlow*	
sudo mkdir -p /TEMPORARIO	Cria a pasta /TEMPORARIO para armazenar os arquivos de dados *NetFlow*
sudo chown -R <username>:<group> /TEMPORARIO	Altera as permissões para um certo usuário e grupo, permitindo que eles tenham acesso de leitura e escrita

Configuração *nfcapd* no Arquivo default.conf	
nano /etc/nfdump/default.conf	Os dois (2) comandos abrem o arquivo de configuração padrão do *NFDump* para edição.
vim /etc/nfdump/default.conf	

```
# - Any cache_dir, user and group values defined above needs to be
#   repeated here in an according option (-l/-M, -u, -g).
#   Remember, shell expandsion will not work when using systemd.
# - Do not use the -D and -P options, they are already set internally.
#
options='-l /TEMPORARIO -p 2055'
```

Foi adicionada uma linha com a seguinte instrução: options='-l /TEMPORARIO -p 2055'

A instrução adicionada define o diretório base onde os dados *NetFlow* serão armazenados e a porta UDP na qual o *nfcapd* escutará para receber dados *NetFlow*

Inicialização e Habilitação do Serviço *NFDump*	
systemctl enable nfdump.service	configura o sistema para iniciar automaticamente o serviço *NFDump* durante a inicialização
systemctl start nfdump.service	o comando inicia o serviço *NFDump*

Tabela A8 - 2. Configurações do *NFDump* no servidor colector *NetFlow*

Fonte: Adaptado pelo autor

d) Resultados da implementação do *NFDump*

Conforme ilustra a Figura A8 - 2*, é* possível verificar os arquivos pela ferramenta *NFDump*, sendo nomeados de usando a convenção "*nfcapd"*, indicando que se tratam de capturas de fluxos de dados *NetFlow*.

Os nomes dos arquivos encontram-se em um formato padronizado, incluindo ano, mês, dia, hora e minuto da colecta. Por exemplo, o arquivo denominado nfcapd.202410051725 refere-se a uma captura realizada em (ano: 2024, mês: 10, dia: 05, hora: 17, minuto: 25). Essa estrutura de nomeação contribui para a organização e análise temporal dos fluxos de tráfego de rede capturados pelo *NetFlow*, permitindo a identificação precisa do momento da colecta e armazenamento.

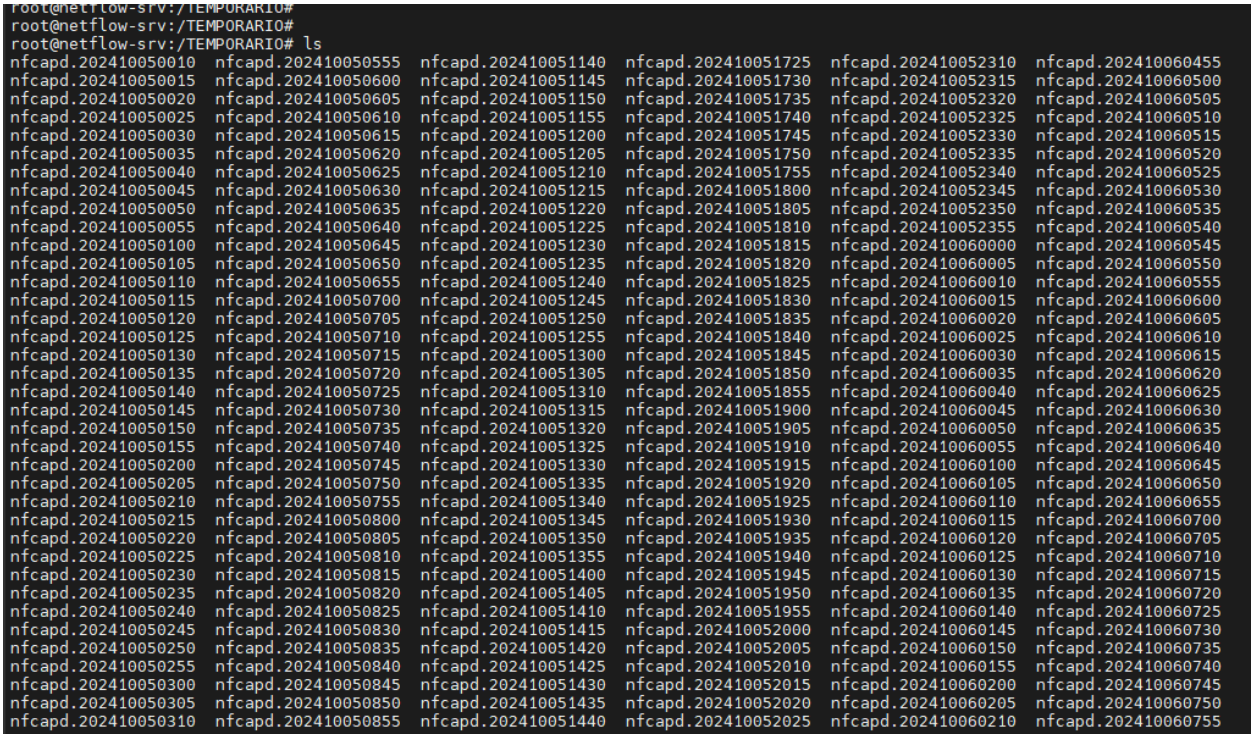


Figura A8 - 2. Dados colectados e armazenados usando o *NFDump* no colector *NetFlow*

Fonte: Adaptado pelo Autor com base no servidor colector *NetFlow*

Anexo 9: Configurações da etapa da análise e correlacção de dados

a) *Scripts* personalizados para a colecta de dados

Abaixo são apresentados dois (2) *scripts* personalizados uma com função de actualizar novos dados no ficheiro C2.txt colectados semanalmente e a outra de colectar dados de servidores de C&C *Botnets* nas plataformas de compartilhamento de ameaças.

addNewInfo.py

```
import os
import shutil
from datetime import datetime


def backup_file(file_path, backup_folder):
    #"""Faz o backup de um arquivo para a pasta de backup com a data atual."""
    if not os.path.exists(backup_folder):
        os.makedirs(backup_folder)

    base_name = os.path.basename(file_path)
    backup_name = f"{os.path.splitext(base_name)[0]}_{get_current_date()}.txt"
    backup_path = os.path.join(backup_folder, backup_name)

    shutil.copy(file_path, backup_path)
    print(f"Backup de {file_path} salvo como {backup_path}")

def append_file(source_file, target_file):
    #"""Adiciona o conteúdo de source_file ao final de target_file."""
    with open(source_file, 'r') as src, open(target_file, 'a') as tgt:
        tgt.write(src.read())
    print(f"Conteúdo de {source_file} adicionado a {target_file}")

#Processa a data actual
def get_current_date():
    # Obtém a data atual
    return datetime.now().strftime("%Y-%m-%d")

def main():
    # Caminho para os arquivos
    file1 = '/Netflow/C2.txt'
    file2 = '/Netflow/Colecta_Dados_C2/Dados_Unidos_Semana/merged_last_week_'+ get_current_date() +'.txt'

    # Diretório de backup
    backup_folder = '/Netflow/Colecta_Dados_C2/Backup_C2'

    # Realiza o backup dos arquivos
    backup_file(file1, backup_folder)
    #backup_file(file2, backup_folder)

    # Adicionar conteúdo de file2 a file1
    append_file(file2, file1)


if __name__ == "__main__":
    main()
```

Figura A9 - 1. *Script* personalizado para actualizar dados no ficheiro C2.txt

Fonte: Elaborado pelo Autor

Feodotracker.py

```
import requests
import datetime
import io

#função que baixa dados CSV Botnet, Grava em um documento e em outro para a união (merge) da informação obtida
def fetch_feodo_tracker_data():
    # URL do FeodoFox para baixar os dados CSV
    url = 'https://feodotracker.abuse.ch/downloads/ipblocklist.csv'

    # Faz a solicitação HTTP para obter os dados
    response = requests.get(url)

    # Verifica se a solicitação foi bem-sucedida
    if response.status_code == 200:
        # Extrai os dados do corpo da resposta
        data = response.text

        # Salva os dados em um arquivo de texto
        save_to_file(data, 'Dados_FeodoTracker\C2_NewGET_Feodo_' + get_current_date() + '.txt')
        print("Dados do FeodoFox coletados com sucesso e salvos no arquivo.")
        merge_file_feodo(data, 'Dados_Organizados\C2_NewMERGE_' + get_current_date() + '.txt')

    else:
        print("Erro ao obter os dados do FeodoTracker")

# Salva em arquivos de textos
def save_to_file(data, filename):
    # Salva os dados em um arquivo de texto
    with open(filename, 'w') as file:
        file.write(data)

# Merge file feodo
def merge_file_feodo(data, filename):
    # Salva os dados em um arquivo de texto
    with open(filename, 'a') as file:
        # Itera sobre cada linha do texto
        for linha in data.split('\n'):
            # Verifica se a linha contém a data e hora no formato especificado
            if linha.strip().startswith('"20'):
                # Verifica se a linha não está vazia
                if linha.strip():
                    # Escreve a linha no novo arquivo
                    file.write(linha)

    print("Dados filtrados do arquivo feodo salvos no arquivo merge")



#Processa a data actual
def get_current_date():
    # Obtém a data atual
    return datetime.datetime.now().strftime("%Y-%m-%d")

#função main
def main():
    # Chama as funções de coleta de dados
    fetch_feodo_tracker_data()

#main()

if __name__ == "__main__":
    main()
```

Figura A9 - 2. *Script* personalizado para colectar dados C&C *Botnets*

Fonte: Elaborado pelo Autor

A Figura A9 - *3* ilustra os *scripts* personalizados armazenados no colector *NetFlow* para a colecta de informações nas plataformas de compartilhamento de ameaças, em busca de servidores de C&C *Botnets* e a actualização no ficheiro de base de dados C2.txt. Esses foram descritos no subcapítulo 4.1.6.

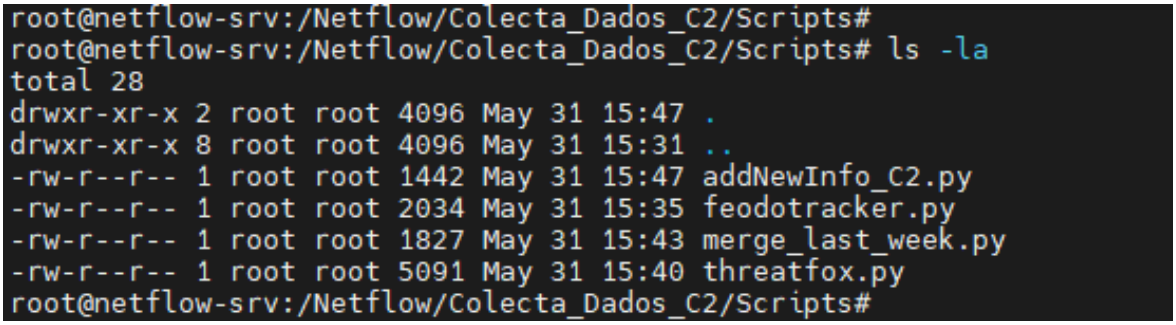


Figura A9 - 3. Ilustração dos *scripts* personalizados armazenados no colector *NetFlow*

Fonte: Adaptado pelo Autor com base no servidor colector *NetFlow*

b) *Scripts* personalizados para a análise e correlação de *Botnets*

Com os dados colectados e armazenados de servidores de C&C *Botnets*, busca-se identificar correspondências ou padrões que denunciam e indicam actividades de redes de *Botnets* na infraestrutura da MoRENet. Para isso, foi implementado um *script* personalizado de análise e correlação, nomeadamente *find_C2.py*, visa identificar padrões de comunicação de *Botnets* presentes nos fluxos de tráfego da rede.

A execução do *script* gera como saída um ficheiro de log denominado *detected_C2.log,* que contém os registos das possíveis correspondências entre o tráfego capturado e os indicadores de comprometimento relacionados a servidores C&C *Botnets*.

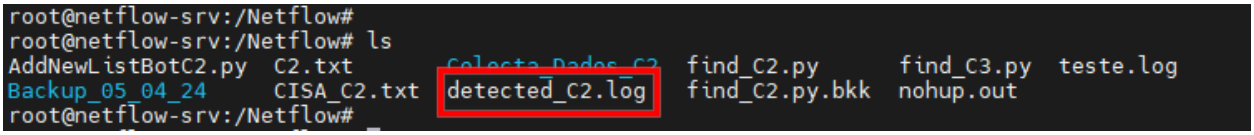


Figura A9 - 4. *Script find_C2.py* e ficheiro *detected_C2.log* no colector *NetFlow*

Fonte: Adaptado pelo Autor com base no servidor colector *NetFlow*

A Figura A9 - 4 acima ilustra o *script find_C2.py* e o respectivo ficheiro de saída o registo *detected_C2.log*, após sua execução no servidor colector *NetFlow*.

find_C2.py

```
import subprocess
import re

def load_suspect_ips(filename):
    """ Carrega a lista de IPs suspeitos e o malware associado de um arquivo. """
    suspect_ips = {}
    with open(filename) as file:
        for line in file:
            if line.startswith('"') and '","' in line:
                parts = line.strip().strip('"').split('","')
                ip, malware = parts[1], parts[5]
                suspect_ips[ip] = malware
    return suspect_ips

def generate_and_scan_netflow_logs(command, suspect_ips, output_file):
    """ Gera logs do NetFlow e escaneia para IPs suspeitos, salvando os resultados em um arquivo. """
    with open(output_file, 'w') as output:
        process = subprocess.Popen(command.split(), stdout=subprocess.PIPE)
        for line in iter(process.stdout.readline, b''):
            line = line.decode()
            if line.strip():
                # Regex para extrair detalhes do log, incluindo IPs, portas, protocolo e timestamp
                match = re.search(r'(?P<timestamp>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}).*?'
                                  r'(?P<src_ip>\b(?:\d{1,3}\.){3}\d{1,3}\b):(?P<src_port>\d+).*?'
                                  r'(?P<dst_ip>\b(?:\d{1,3}\.){3}\d{1,3}\b):(?P<dst_port>\d+).*?'
                                  r'(?P<protocol>\b\w+\b)', line)
                if match:
                    src_ip, dst_ip = match.group('src_ip'), match.group('dst_ip')
                    if src_ip in suspect_ips or dst_ip in suspect_ips:
                        malware = suspect_ips.get(src_ip, suspect_ips.get(dst_ip, "Unknown"))
                        output.write(f"{match.group('timestamp')}, "
                                     f"{src_ip}:{match.group('src_port')}, "
                                     f"{dst_ip}:{match.group('dst_port')}, "
                                     f"{match.group('protocol')}, "
                                     f"{malware}\n")

# Caminho para o arquivo de IPs suspeitos
ip_file = '/Netflow/C2.txt'
suspect_ips = load_suspect_ips(ip_file)

# Comando para gerar logs do NetFlow
nfdump_command = "nfdump -R /TEMPORARIO/"

# Arquivo para salvar as atividades suspeitas detectadas
output_file = '/Netflow/detected_C2.log'

# Gerar e escanear logs do NetFlow
generate_and_scan_netflow_logs(nfdump_command, suspect_ips, output_file)
```

Figura A9 - 5. *Script* personalizado para análise e correlacção de *Botnets*

Fonte: Elaborado pelo Autor

Anexo 10: Configurações da etapa de monitoramento e visualização

a) Instalação do *ELastic Agent* no servidor colector *NetFlow* e no *Elasticsearch*

No servidor colector *NetFlow:*

- Instalação e configuração do *Elastic Agent* no colector *NetFlow*

Download do *Elastic Agent*
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.1-linux-x86_64.tar.gz

Descompactar o arquivo
tar xzvf elastic-agent-8.16.1-linux-x86_64.tar.gz

Instalar o *Elastic Agent*
cd elastic-agent-8.16.1-linux-x86_64 sudo ./elastic-agent install --url=https://10.x.x.x:8220 --enrollment-token=bzl5NDJZd0JSTnFEMWRLZ0VkeV86cWpVVzVxcTdSWEtoWnowdlMwdnI0Zw== --insecure

Tabela A10 - 1. Instalação do *Elastic Agent* no servidor colector *NetFlow*

Fonte: Adaptado pelo autor

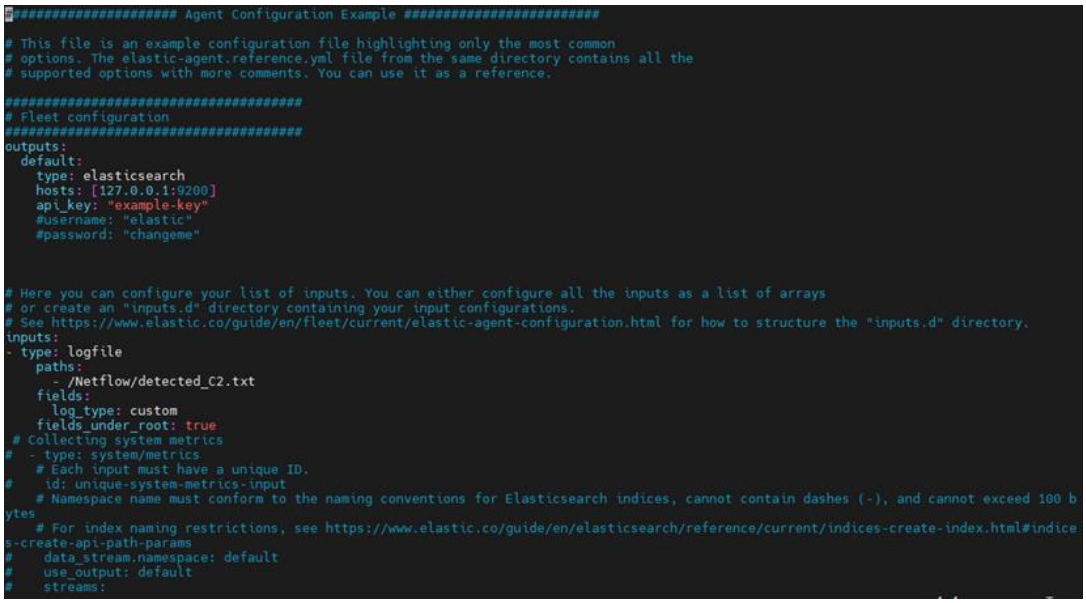


Figura A10 - 1. Configuração do *Elastic Agent* no servidor colector *NetFlow*

Fonte: Adaptado pelo Autor com base no servidor colector *NetFlow*

Na plataforma *Elasticsearch*:

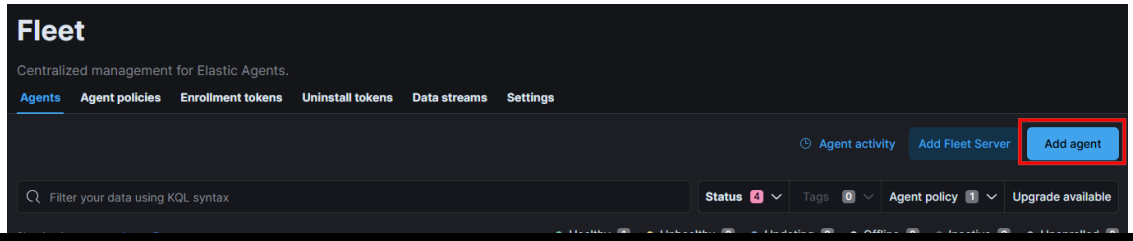
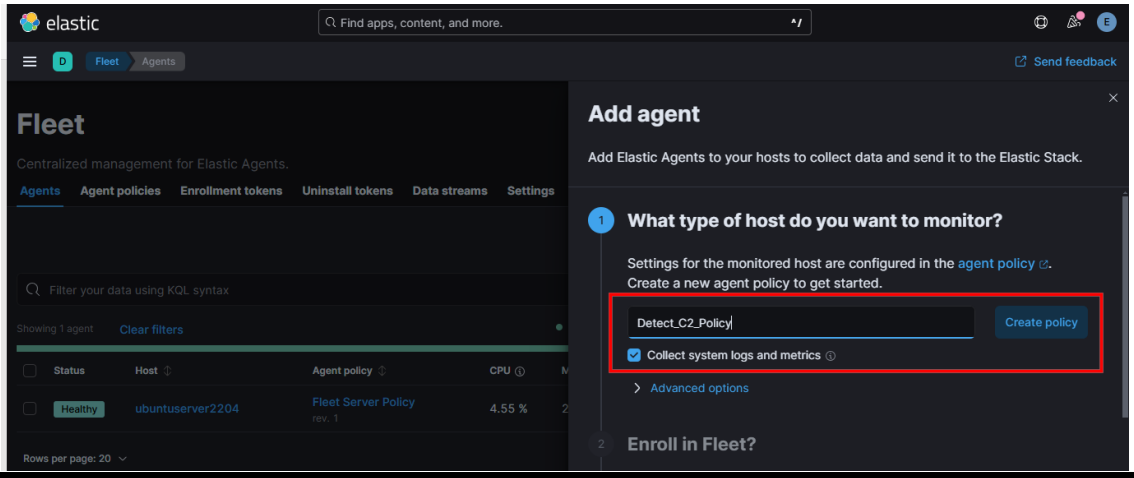
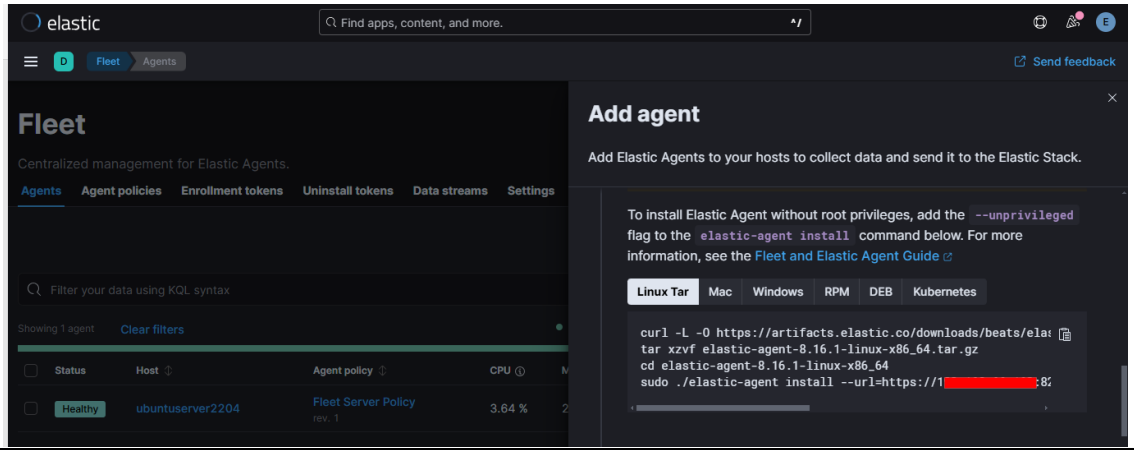
Adicionar o *ELastic Agent* no *Elasticsearch*
Usando o Fleet adiciona-se o *Elastic Agent* com o nome do índice denominado *netflow-srv* no *Elasticsearch que será instalado no servidor colector NetFlow*

Política de Indexação do *Agent*
Adicionar a política de Indexação denominada *Detect_C2_Policy*

Comandos de instalação do *Elastic agent*
Copiar os comandos de instalação do *Elastic agent* para efectuar no *servidor* colector *NetFlow*


Tabela A10 - 2. Configuração do *Elastic Agent* no *Elasticsearch*

Fonte: Adaptado pelo autor

A Figura A10 - 2 ilustra o *Elastic Agent* configurado e integrado no *Elasticsearch*, com o nome do índice denominado *netflow-srv* no *Elasticsearch*, junto da política de Indexação criada denominada *Detect_C2_Policy*:

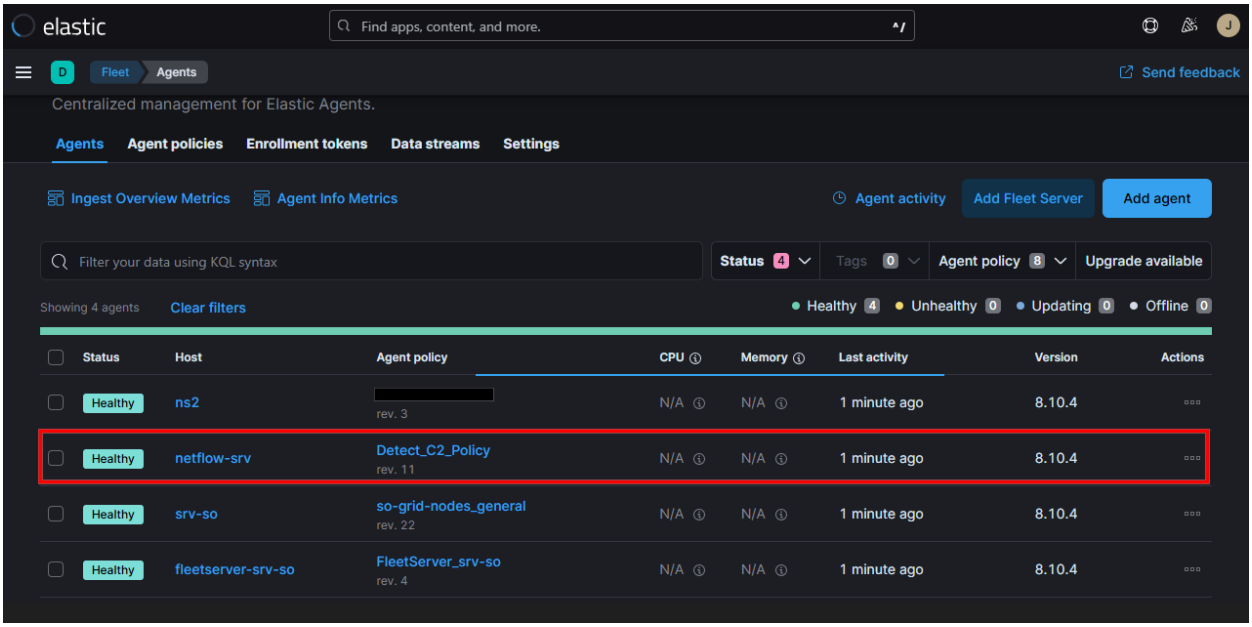


Figura A10 - 2. *Elastic Agent* configurado e integrado no *Elasticsearch*

Fonte: Adaptado pelo Autor com base no *Elasticsearch*

Anexo 11: Agendamento de tarefas com o *cron job*

A configuração de um *cron job* consiste em adicionar uma linha no arquivo *crontab* no *Linux* com a definição da tarefa a ser executada, seguindo o seguinte formato:

- M (Minuto) H (Hora) D (Dia) M (Mês) DS (Dia da Semana) C (Comando)

Adicionar as entradas do *cron job*	
crontab -e	Abre o *crontab* adição de novas entradas

Tabela A11 - 1. Comando para configurar um *Cron job* no *Linux*

Fonte: Elaborado pelo Autor

a) *Cron job* – Execução automatizada de *scripts* personalizados de colecta de informações de servidores de C&C

Tipo de *Script*		Cron Job	Hora	Resultado
Colecta de Dados	*ThreatFox*	Segunda, Quarta, Sexta-feira	23h:50min	Colectado:*ThreatFox_data.txt* Filtrado: *C2_Merge_data.txt*
	FeodoTracker	Segunda-feira	23h:40min	Colectado: *FeodoTracker_data.txt* Filtrado: *C2_Merge_data.txt*
Unificação dos Dados		Terça-feira	23h:30min	Unificado: *C2_MergeAll_data.txt*
Actualização de dados C&C		Terça-feira	23h:45min	Actualizado: *C2.txt*
Comando				
40 23 * * 1 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/feodotracker.py				
50 23 * * 1,3,5 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/threatfox.py				
30 23 * * 2 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/merge_last_week.py				
45 23 * * 2 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/addNewInfo_C2.py				

Tabela A11 - 2. *Cron jobs* e arquivos de saída dos *scripts* personalizados

Fonte: Elaborado pelo Autor

No entanto a execução dos *cron jobs* é diferenciada, sendo que, o *ThreatFox* três (3) vezes por semana devido às atualizações rápidas dos seus dados (um intervalo de dez (10) minutos), enquanto que o restante é executado uma vez por semana.

b) *Cron job* – execução automatizada do *script* personalizado de análise e correlacção de dados com informações de servidores de C&C

Tipo de *Script*	Cron Job	Hora	Saída do registo
Análise e Correlacção de tráfego de rede com servidores C&C	Todos os dias	00h:30min	Actualizado: *detected_C2.log*
Comando			
30 0 * * * /usr/bin/python3 /Netflow/find_C2.py			

Tabela A11 - 3. *Cron job* e arquivo de saída do *script* de análise e correlacção

Fonte: Elaborado pelo Autor

c) *Cron job* – Apagar dados no directório "TEMPORARIO"

Tipo de *cron job*	*Cron Job*	Hora	Resultado
Apagar arquivos no directório TEMPORARIO	Todos os dias	00h:10min	Apaga todos os arquivos que tenham sido modificados há mais de um dia
Comando			
10 0 * * * /usr/bin/find /TEMPORARIO/* -mtime +0 -type f -delete			

Tabela A11 - 4. *Cron job* para apagar arquivos no directório TEMPORARIO

Fonte: Elaborado pelo Autor

d) *Cron job* – visão geral de tarefas de automação configuradas no colector *NetFlow*

É ilustrado na Figura A11 - 1 o cenário da definição dos *cron jobs* no servidor colector *NetFlow*.

```
# m h  dom mon dow   command
#58 23 * * * /usr/bin/rm /Netflow/C2.txt;
#0 0 * * * /usr/bin/wget https://feodotracker.abuse.ch/downloads/ipblocklist_aggressive.csv -O /Netflow/C2.txt;
10 0 * * * /usr/bin/find /TEMPORARIO/* -mtime +0 -type f -delete;
30 0 * * * /usr/bin/python3 /Netflow/find_C2.py;
40 23 * * 1 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/feodotracker.py;
50 23 * * 1,3,5 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/threatfox.py;
30 23 * * 2 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/merge_last_week.py;
45 23 * * 2 /usr/bin/python3 /Netflow/Colecta_Dados_C2/Scripts/addNewInfo_C2.py;
root@netflow-srv:~#
```

Figura A11 - 1. *Cron jobs* definidos no servidor colector *NetFlow*

Fonte: Adaptado pelo Autor com base no servidor colector *NetFlow*

Anexo 12: Riscos e medidas de mitigação na implementação da solução

A tabela abaixo apresenta os riscos identificados na implementação da solução proposta para a detecção proactiva de *Botnets* na infraestrutura da MoRENet, juntamente com as respectivas medidas de mitigação.

Riscos Potenciais	Descrição	Medidas de Mitigação
Falhas de hardware	Falhas nos dispositivos, como roteadores, *switches* ou servidores, podem interromper o a colecta, análise e correlacção de dados para detecção de *Botnets*	Realizar manutenções preventivas regulares em equipamentos da infraestrutura da MoRENet
Sobrecarga de recursos	Elevado de volume de tráfego gerado na rede, pode sobrecarregar os dispositivos ao processar exportar fluxos *NetFlow*	Dimensionar adequadamente os recursos de *hardware*, como memória e CPU
Erros nos *script*s	*Scripts* automatizados para a colecta, análise e correlacção de dados podem conter falhas de execução, comprometendo a detecção de *Botnets* na infraestrutura da MoRENet	Monitorar e testar *script*s extensivamente em ambientes simulados
Problemas de integração e compatibilidade	Integração do *NetFlow* com as diferentes ferramentas, poderá enfrentar falhas de versões, problemas de desempenho ou falhas de configuração	Validar compatibilidade entre as ferramentas auxiliares para a implementação da solução proposta
Interrupções e perda de dados	Falhas inesperadas durante a colecta ou armazenamento do tráfego de rede, podem resultar em perda parcial ou total de informações críticas para análise e correlacção de ameaças *Botnets*.	Otimização nos parâmetros de exportação do *NetFlow*
		Implementar mecanismos de *backup* e verificação da integridade dos dados

Tabela A12 - 1. Riscos e medidas de mitigação na implementação da solução

Fonte: Elaborado pelo Autor

Anexo 13: Avaliação operacional da solução proposta com base no protocolo *NetFlow*

Impactos da solução na infraestrutura tecnológica	
Impacto	Descrição
Melhoria no monitoramento	Aumento da capacidade de detecção de actividades maliciosas na rede
Baixo consumo de recursos	O *NetFlow* gera apenas metadados, reduzindo a carga nos dispositivos
Integração com ferramentas na infraestrutura	Exploração de ferramentas de segurança existentes na infraestrutura da MoRENet para a integração com o *NetFlow*, ampliando a análise e detecção de ameaças
Mecanismos redundantes	*Script*s automatizados de colecta e armazenamento, aumentando a resiliência da infraestrutura frente a falhas e interrupções

Impactos da solução na equipa de segurança	
Impacto	Descrição
Auxílio no monitoramento	Facilita a supervisão contínua das actividades de rede na infraestrutura
Necessidade de capacitação	Exigência de treinamento técnico para que desenvolvam novas habilidades, especialmente em análise de dados
Automação de tarefas	Permite os técnicos se concentrem em outras tarefas, como a correlacção de eventos e resposta a incidentes

Tabela A13 - 1. Impactos operacionais e técnicos da solução proposta

Fonte: Elaborado pelo Autor

Limitações identificadas na aplicação do *NetFlow*	
Limitação	Descrição
Colecta de metadados de tráfego	Conforme Amini et al., (2014) o *NetFlow* colecta somente metadados de tráfego, isto é, não verifica ou inspeciona o conteúdo dos pacotes. Isso pode limitar sua capacidade de detectar ataques mais sofisticados de *Botnets*
Dependência de ferramentas adicionais	A análise de dados colectados pelo *NetFlow*, conta com auxílio de ferramentas ou técnicas adicionais para realização da correlacção e detecção de ameaças *Botnets*
Latência na análise de dados	Em situações de tráfego intenso como em horários de pico ou ataques DDoS a grande quantidade de fluxos registrados pode sobrecarregar o colector *NetFlow* e atrasar a execução dos *scripts* de análise dos dados colectados, comprometendo o processo de correlacção e detecção de ameaças *Botnets*
Falsos positivos	Como apontado por Bilge et al., (2012), soluções baseadas apenas em *NetFlow* estão sujeitas a alertas falsos. Embora o *NetFlow* apresente menor taxa de falsos positivos em comparação a soluções como o *sFlow*, durante a fase da correlação do fluxo capturado com listas de IP's maliciosos, poderá observar-se padrões de tráfego legítimo com comportamentos similares aos de tráfego de servidores C&C, sendo interpretados como maliciosos. No entanto, Bilge et al., (2012), é mencionam ainda que mesmo uma taxa de classificação incorrecta inferior a uma fracção de um (1) por cento pode resultar em um número elevado de falsos alarmes
Falsos Negativos	o *NetFlow,* por apresentar limitação na visibilidade de tráfego e por não inspecionar o conteúdo dos pacotes, pode comprometer a detecção de redes *Botnets* que utilizam técnicas avançadas. Isso pode resultar na não identificação de comunicações ocultas realizadas por *Botnets*, essas mencionadas por Hachem et al., (2011) no subcapítulo 2.2.2, técnicas que utilizam estratégias como fluxos rápidos de domínio (*Domain-Flux*) e fluxo rápido de IP (*fast-flux*) para a execução das suas actividades na rede

Tabela A13 - 2. Limitações operacionais da solução proposta

Fonte: Elaborado pelo Autor com base em estudos de autores Amini et al., (2014), Bilge et al., (2012) e Hachem et al., (2011)

Pontos de melhoria da solução proposta	
Melhoria	Descrição
Sistema de *backup* redundante	Implementar um sistema de *backup* automático, redundante para garantir a disponibilidade dos dados colectados, assegurando a continuidade da análise mesmo em caso de falhas no sistema
Integração com outras tecnologias	Integrar o protocolo *NetFlow* com outras tecnologias complementares, para permitir análises mais profundas, permitindo elevar a capacidade de identificação de tráfego malicioso associados as redes *Botnets*
Validação com múltiplas fontes de inteligência	Validar de dados de servidores de C&C com múltiplas fontes *de threat intelligence*, plataformas como MISP, OTX de forma automatizada para aumentar a cobertura da base (C&C) utilizada na correlação

Tabela A13 - 3. Melhorias na operacionalização da solução proposta

Fonte: Elaborado pelo Autor