ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM GABRIEL VILLAR DA COSTA

PROTEÇÃO CIBERNÉTICA:
PROPOSTA DE UM LABORATÓRIO PARA ANÁLISE DE ARTEFATOS CIBERNÉTICOS

Rio de Janeiro
2021

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM GABRIEL VILLAR DA COSTA

PROTEÇÃO CIBERNÉTICA:
PROPOSTA DE UM LABORATÓRIO PARA ANÁLISE DE ARTEFATOS CIBERNÉTICOS

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

Rio de Janeiro
2021

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Com GABRIEL VILLAR DA COSTA**

Título: **PROTEÇÃO CIBERNÉTICA: PROPOSTA DE UM LABORATÓRIO PARA ANÁLISE DE ARTEFATOS CIBERNÉTICOS.**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Gestão Operacional, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ CONCEITO: _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **CARLOS ANDRÉ DOS SANTOS MEIRELLES DE ANDRADE - Maj** Cmt Curso e Presidente da Comissão	
_____ **THIAGO FERRAZ DE BARROS PERES - Maj** 1º Membro	
_____ **GLAUCO GONÇALVES DA SILVA - Cap** 2º Membro e Orientador	

_____
GABRIEL VILLAR DA COSTA – Cap
Aluno

RESUMO

A Guerra Cibernética continua recebendo destaque internacional, muito devido à sua grande capacidade de influência em diversos setores como político e econômico. Dentro desse universo, a utilização de programas maliciosos, também conhecidos como *malwares*, com as mais diversas finalidades, desde espionagem, vazamento de informações e comprometimento de infraestruturas críticas também vem crescendo exponencialmente. Face a isso, cabe ao Exército Brasileiro adequar a proteção cibernética dos seus meios de Tecnologia das Informações e Comunicações, principalmente, no controle e identificação dos *malwares* utilizados pelos adversários tanto em situações de guerra como não-guerra. Para isso, essa pesquisa propõe a criação de um laboratório para teste de artefatos cibernéticos que possa ser acessado por determinados integrantes para a verificação rápida e simples de possíveis vetores de *malwares*.

Palavras-chave: Cibernética, *Malware*, Laboratório

ABSTRACT

The Cyber War continues to receive international prominence, largely due to its great capacity for influence in various sectors such as political and economic. Within this universe, the use of malicious programs, also known as malwares, with the most diverse purposes, from espionage, information leakage and the compromise of critical infrastructures has also been growing exponentially. In view of this, it is up to the Brazilian Army to adapt the cyber protection of its Information and Communications Technology assets, mainly in the control and identification of malware used by opponents in both war and non-war situations. This research proposes the creation of a laboratory for testing cybernetic artifacts that can be accessed by certain members for the quick and simple verification of possible malware vectors.

Keyword: Cybernetic, Malware, Laboratory

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

Uma das mudanças mais notáveis do Século XXI em relação à tecnologia é o uso cada vez maior de sistemas informatizados conectados em redes. Devido à rapidez da transmissão e a capacidade de um maior volume de informações, a adoção desses meios em operações militares nos últimos anos é um caminho natural da evolução do combate moderno.

Logicamente, o advento de novas tecnologias trouxe também o surgimento de novas ameaças, dentre elas o uso recorrente de programas de computador criados para atividades maliciosas diversas, popularmente conhecidos como *malwares*, abreviação em inglês de *malicious software* (programa malicioso). Esses programas podem comprometer um dispositivo isolado, um servidor ou até mesmo toda uma rede de computadores.

A finalidade de um *malware* é designada particularmente pelo seu desenvolvedor, podendo ser desde roubo de informações até comprometimento e destruição de estruturas físicas. Como foi observado em 2010, no Irã, o *Stuxnet* foi um *malware* projetado para controlar as centrífugas de enriquecimento de urânio iranianas provocando danos intencionais às usinas nucleares (LOPES, 2014).

Um caso recente de uso de malware teve grande repercussão no Brasil no ano passado, onde o Superior Tribunal de Justiça teve seu acervo de processos criptografado, indisponibilizando por dias diversos sistemas do tribunal, suspendendo todos os prazos processuais administrativos, cíveis e criminais durante esse período (BOSCO,2020).

Somente no 1º semestre de 2020, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br), grupo de resposta de incidentes mantido pelo Comitê Gestor de Internet no País, foi reportado sobre 55.645 incidentes envolvendo códigos maliciosos em território nacional.

.

1.1 PROBLEMA

Dentro desse cenário, a Doutrina Militar de Defesa Cibernética, publicada em 2014 pelo Ministério da Defesa (MD), fundamentou a doutrina de Guerra Cibernética do Exército Brasileiro (EB), ao relacionar capacidades que devem ser alcançadas em diversos

escalões. Em uma de suas capacidades operativas, o Manual de Campanha Guerra Cibernética descreve o seguinte sobre a Proteção Cibernética:

> Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente (BRASIL, 2017, p. 3-4).

1.1.1 **Antecedentes do Problema**

Dentro da atividade de Proteção Cibernética, a tarefa de Teste de Artefatos Cibernéticos é descrita como “Testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos” (BRASIL, 2017, p. 4-4). Sendo muito efetivo a utilização de um laboratório especializado para essa determinada tarefa.

Os artefatos cibernéticos podem ser entendidos como “equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataques cibernéticos” (BRASIL, 2017, p. 2-1). Sendo coerente então enquadrar os *malwares* desenvolvidos por adversários contra nossos sistemas como artefatos cibernéticos.

Importante ainda salientar que a atividade de Proteção Cibernética além de ser de caráter permanente, é de responsabilidade de estruturas operativas como o Batalhão de Comunicações (B Com) e Companhia de Comunicações (Cia Com), os quais não necessariamente estarão dotados de elementos especialistas para a tarefa de Teste de Artefatos Cibernéticos.

1.1.2 **Formulação do Problema**

Diante dos argumentos mencionados anteriormente, chegamos ao seguinte problema que será objeto dessa pesquisa: **De que forma os elementos do nível tático sem especialistas ou equipamentos podem realizar a tarefa de Teste de Artefatos Cibernéticos atendendo suas necessidades?**

1.2 OBJETIVOS

Com o intuito de chegar à resolução do problema proposto, foram levantados os seguintes objetivos que nortearam o desenvolvimento deste trabalho:

1.2.1 **Objetivo Geral**

Propor a criação de um laboratório para Teste de Artefatos Cibernéticos por acesso remoto por elementos responsáveis pela atividade de Proteção Cibernética.

1.2.2 **Objetivos Específicos**

Para alcançar o objetivo geral, foram levantados os seguintes objetivos específicos que permitiram uma estruturação lógica e completa da pesquisa realizada:

a) Identificar os principais tipos de *malwares* e suas finalidades;

b) Propor estrutura, equipamentos e sistemas necessários para a criação do laboratório; e

c) Verificar as capacidades presentes, para esse tipo de atividade, nas Organizações Militares (OM) de Comunicações.

1.3 **Questões de Estudo**

Correlacionando os objetivos dessa pesquisa juntamente com o problema apresentado, foram elencadas as seguintes questões de estudo para orientar a pesquisa rumo a uma solução:

a) Quais os principais tipos de *malwares* e suas finalidades?

b) Como estruturar um laboratório de Teste de Artefatos Cibernéticos?

c) As OMs de Comunicações possuem pessoal com capacidade para realizar essa tarefa sem apoio externo?

1.4 METODOLOGIA

1.4.1 **Objeto formal de estudo**

A presente pesquisa teve como objeto de estudo a proposta da criação de um laboratório de Teste de Artefatos Cibernéticos para acesso remoto pelos elementos responsáveis pela atividade de Proteção Cibernética, para isso, foram utilizadas ferramentas de coleta de dados e pesquisa bibliográfica, de informações não mais antigas que do ano 2010.

O alcance da pesquisa constitui em dois seguimentos: a pesquisa de estruturas, equipamentos e sistemas necessários para a criação do laboratório; e o processo de utilização do laboratório pelos elementos do nível tático. Pretende-se que o estudo alcance uma evolução da Proteção Cibernética.

Os limites para a pesquisa foram definidos pelo atendimento à doutrina exclusiva da Guerra Cibernética, respeitando suas características e peculiaridades. Fez se jus delimitar um espaço de tempo aproximadamente de 12 anos devido à constante evolução de tecnologia dos sistemas informatizados.

Em relação às variáveis foi possível apontar como a doutrina de Guerra Cibernética como a variável independente (VI) e sua variável dependente (VD) a viabilidade do laboratório para teste de artefatos cibernéticos, ou seja, de acordo com os conceitos estabelecidos pela Doutrina Militar Terrestre foi possível verificar uma maior ou menor viabilidade da utilização.

1.4.2 **Amostra**

A aplicação de questionário a respeito do tema em estudo e posterior análise dos resultados, abrangeu todas as Organizações Militares de Comunicações no níveis Unidades e Subunidades diretamente subordinas a uma Brigada, Divisão de Exército ou Comando Militar de Área.

O objetivo do questionário foi de avaliar os resultados obtidos pela pesquisa bibliográfica em comparação com os dados obtidos como respostas.

1.4.3 **Delineamento da pesquisa**

Foi realizada uma pesquisa aplicada com abordagem descritiva de cunho qualitativo, com a existência de parte quantitativa como instrumento de apoio. Para isso, um levantamento de dados com uso de questionários foi executado em amostras selecionadas. Para a apreciação dos resultados, foi aplicado o método comparativo na busca pela elucidação das questões deste estudo.

1.4.4 **Procedimentos para revisão da literatura**

Para a revisão da literatura foram consultados os manuais que regulam as ações cibernéticas pelo Exército Brasileiro, assim como outras pesquisas e bibliografias relevantes nas áreas de proteção cibernética e análise de malware.

O objetivo da revisão foi elencar parâmetros a serem alcançados pelo laboratório que atendam as prerrogativas da Doutrina Militar Terrestre.

1.4.5 **Procedimentos Metodológicos**

Os grupos amostrais foram contatados por seus endereços eletrônicos, disponíveis no *site* do Departamento Geral do Pessoal (DGP).

As respostas obtidas com as amostras dos grupos foram comparadas aos resultados obtidos pela pesquisa bibliográfica de modo a servir de parâmetro para ratificar as conclusões obtidas pelo método comparativo de estudo das diversas fontes bibliográficas.

1.4.6 **Instrumentos**

Foi aplicado um questionário de perguntas ao grupo já listado com a finalidade de estabelecer padrões medianos, principalmente pelo uso de perguntas fechadas com a possibilidade de complemento as respostas.

1.4.7 **Análise dos Dados**

Após a computação dos resultados do questionário, foi realizado o trabalho de tabulação, interpretação dos dados e análise qualitativa deles. Buscando-se identificar os padrões medianos dentre as respostas das Organizações Militares que possuem militares capacitados ao teste de artefatos cibernéticos, contrapondo-os as respostas das OMs que não possuem.

Os resultados foram expressos em forma de quadros e gráficos. A tabulação final, constituindo-se da coleta de dados e a pesquisa bibliográfica, pretende mostrar um entendimento da forma que o objetivo geral desse estudo poderá ser aplicado

1.5 JUSTIFICATIVA

A relevância deste estudo fundamenta-se na ausência de trabalhos de Proteção Cibernética, que considerem a tarefa de Teste de Artefatos Cibernéticos, face as novas capacidades e possibilidades dos *malwares* na atualidade.

As vantagens a serem obtidas por meio deste estudo são apresentar uma proposta de um laboratório de análises de artefatos, face ao novo cenário mundial de utilização de redes de computadores, e atender as necessidades de elementos do nível tático sem pessoal, sistemas e equipamentos especializados.

Além disso, o estudo encontra amparo no Programa Estratégico do Exército Defesa Cibernética, no objetivo de dotar o EB da infraestrutura necessária para desenvolver eficazmente todo o espectro de atividades cibernéticas, particularmente visando a proteger e defender os ativos de informação da Força nas áreas de Segurança Cibernética, Defesa Cibernética e Guerra Cibernética.

2. REFERENCIAL TEÓRICO

A presente revisão da literatura foi utilizada para fundamentar os conceitos apresentados nessa pesquisa, de forma que se possa chegar ao mais próximo do estado da arte em um laboratório para Teste de Artefatos Cibernéticos. Buscou-se ainda com essa revisão abordar as questões de estudo em sua totalidade.

2.1 GUERRA CIBERNÉTICA

A Guerra Cibernética pode ser considerada um dos multiplicadores do poder de combate para o Exército Brasileiro, pois permeia as diversas funções de combate muito em face da transversalidade (BRASIL, 2017, p. 1-2).

Importante então apresentar as Estruturas Operativas da Guerra Cibernética no contexto de suas responsabilidades para uma melhor compreensão de como o objetivo dessa pesquisa busca uma integração à Doutrina Militar Terrestre.

Dentro do nível tático, a Força Terrestre Componente (FTC) deverá ser apoiada por uma Estrutura de Guerra Cibernética (Etta G Ciber), isso inclui o próprio planejamento e assessoramento das ações cibernéticas, tendo em vista que os elementos das OM componentes da Etta G Ciber serão integrantes do Estado-Maior de uma FTC. Um comparativo dessas OMs e das suas reponsabilidades pode ser observado em sequência:

QUADRO 1: Estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.

Batalhão de Comunicações (B Com)			X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Fonte: BRASIL, 2017, p. 3-3.

No Quadro 1 é possível observar com clareza o elevado destaque ao qual a Proteção Cibernética recebe sendo de responsabilidade de todos seus componentes, inclusive das OMs integrantes da FTC, mesmo que um nível menos complexo somente com a proteção preventiva.

2.2 MALWARES COMO ARTEFATOS CIBERNÉTICOS

Malwares são todos os *softwares* criados com a intenção de prejudicar e/ou danificar um sistema, computador ou rede. Com milhões de programas maliciosos espalhados pela Internet e mais diversos tipos encontrados todos os dias, a análise de

malware é crítica para qualquer profissional que responde por incidentes de segurança (SIKORSKI; HOGIN, 2012). Sendo ainda um trabalho de alta complexidade, a análise de malware possui uma demanda grande por profissionais qualificados para essa tarefa específica.

2.2.1 **Tipos de Malwares**

Dentro das finalidades e comportamentos dos diversos tipos de Malwares eles podem ser agrupados nas seguintes categorias (SIKORSKI; HOGIN, 2012):

a) ***Backdoors***: código que se instalam em computadores permitindo o acesso remoto por um atacante. *Backdoors* geralmente permitem ao invasor se conectar com ou sem nenhum tipo de autenticação e executar comandos na máquina.

b) ***Botnet***: são similares aos *backdoors*, no sentido de permitirem um invasor se conectar ao sistema, mas todos os computadores infectados recebem as mesmas instruções de um único servidor de Comando e Controle.

c) ***Downloader***: código que existe somente para realizar o *download* de outro código malicioso. *Downloaders* são normalmente utilizados por invasores para conseguir um primeiro acesso ao sistema, o programa então recebe e instala códigos maliciosos adicionais.

d) ***Information-stealing malware***: são *malwares* que coletam informações do computador de uma vítima e mandam para o invasor. Esses tipos de *malwares* são usualmente empregados para obter acesso a contas de e-mails e de sistemas bancários.

e) ***Launcher***: programas maliciosos que iniciam outros programas maliciosos. Normalmente utilizam técnicas não tradicionais para iniciar outros *malwares* com o intuito de garantir furtividade no sistema.

f) ***Rootkit***: Códigos maliciosos que escondem outros códigos. Usualmente comparados com *backdoors* por permitir acesso remoto ao invasor, com o diferencial de serem relativamente difíceis de serem encontrados pela vítima.

g) ***Scareware***: *malware* desenvolvido para assustar um usuário infectado a pagar ou comprar alguma coisa. Normalmente informa ao usuário que existem códigos maliciosos no seu sistema e a única maneira de removê-los é

comprando um determinado *software*, quando na verdade o programa vendido não realiza nenhuma ação a não ser remover o *scareware*.

h) ***Spam-sending malware***: *malware* que infecta a máquina de um usuário e a utiliza para enviar *spam*.

i) ***Worms ou Virus***: códigos maliciosos que fazem cópias de si mesmo e infectam outros computadores.

Os *malwares* podem ser classificados em mais de uma categoria das mencionadas acima. Podem inclusive serem classificados quanto ao alvo do *malware*, em massa ou direcionado (SIKORSKI; HOGIN, 2012). Alvos em massa significa que o programa tenta infectar o maior número possível de vítimas em diversos sistemas diferentes, em alvos direcionados o programa é desenvolvido para infectar um usuário ou organização específica.

2.2.2 **Fases de Análise de Malware**

Como dito anteriormente, a análise de malwares é uma tarefa complexa e com escassez de profissionais especializados, podendo seus trabalhos inerentes serem divididos em fases crescentes de especialização do analista. Essas fases são as seguintes:

a) **Análise Automática**: fase menos complexa e sem necessidade de grande especialização. Focada em utilização de ferramentas automáticas pelo operador em um ambiente propício e controlado para a tarefa, fornecendo normalmente um relatório sobre o programa malicioso. Antivírus podem entrar nessa categoria, no entanto não são eficientes contra *malwares* muito recentes ou direcionados para uma determinada vítima.

b) **Análise Estática**: fase com leve a média complexidade para um analista, onde algumas informações são levantadas sem a execução do artefato. Devido ao refinamento constante dos *malwares*, dificilmente extrairá todas as informações possíveis sobre o programa malicioso.

c) **Análise Dinâmica**: fase com média a alta complexidade, requer profissional com bom nível de especialização. Fornece muitas informações ao executar o *malware* observando diversos aspectos de comportamento, no entanto exige muito mais tempo para sua análise.

2.3 FERRAMENTAS DE ANÁLISE DE MALWARE

Em um panorama mais simples, a utilização de produtos comerciais para análises automáticas poderia ser considerada satisfatória, ferramentas online como o *VirusTotal* (https://www.virustotal.com) demonstram elevado grau de confiabilidade em seus resultados como na Figura 1 a seguir demostrando a detecção do *WannaCry*, responsável por um dos maiores ataques de *ransomware* da história no ano de 2017:

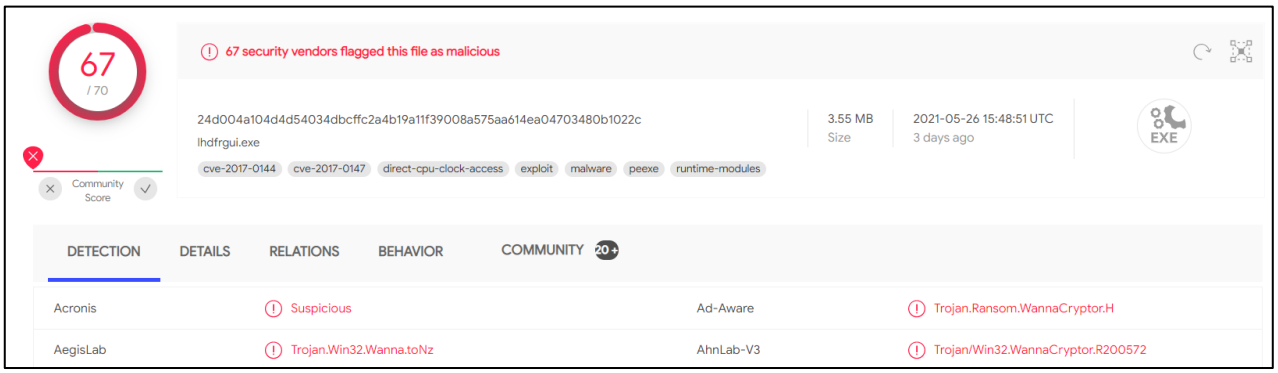

Figura 1: Relatório de detecção do *malware WannaCry*.
Fonte:https://www.virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/detection

É possível observar que o *VirusTotal* informa que 67 de um total de 70 ferramentas de detecção de malwares acusaram o artefato como malicioso, com uma taxa de detecção extremamente eficiente para diversos tipos de programas maliciosos. A solução, porém, disponibiliza publicamente os relatórios dos programas analisados inclusive de arquivos presentes e submetidos a partir de domínios do EB, conforme pode ser verificado na Figura 2:

Figura 2: Relatório de detecção do arquivo “AtualizadorBancoSiscofisOmOpV2.exe”.
Fonte:https://www.virustotal.com/gui/file/eae3375f87771503191bbbbd99d3f9d3bf75721078530e885aec495dd01f99b1/detection

Possivelmente, algum usuário dentro da rede interna do Exército Brasileiro (EBNet) fez o *upload* de um executável relacionado ao Sistema de Controle Físico (SISCOFIS). Sendo comum ainda encontrar relatórios e outros documentos com informações de militares no *VirusTotal*, submetidos provavelmente por usuários preocupados estarem em posse de arquivos infectados.

Importante ressaltar que a plataforma *VirusTotal*, funciona como uma ferramenta de compartilhamento de informações de malwares submetidos por seus usuários, sendo permitido a visualização integral dos arquivos disponíveis na plataforma aos clientes que possuem o plano empresarial pago.

Com essa observação, entende-se que um método mais seguro para, dentro da atividade de Proteção Cibernética, realizar a tarefa de Teste de Artefatos Cibernéticos, seria utilizar uma ferramenta de Código Livre com administração do próprio EB.

2.3.1 **Cuckoo Sandbox**

A ferramenta *Cuckoo Sandbox* é um programa de Código Livre que permite administrar diversos ambientes virtualizados com a finalidade de executar programas suspeitos de maneira automatizada em um ambiente seguro, gerando um relatório ao final com diversas informações levantadas e um score de 0 a 10 do nível de risco do artefato.

Sendo um projeto independente iniciado em 2010 por um pequeno grupo de desenvolvedores e pesquisadores, cresceu em sua relevância no cenário mundial de análises de *malwares* e, hoje, ainda é ponto de referência para criação de laboratórios voltados exclusivamente à análise automática de artefatos cibernéticos.

A quantidade de ambientes, capacidade de armazenamento são totalmente dependentes da organização que esteja utilizando o programa, possuindo uma interface intuitiva (Figura 3) para os usuários que estejam submetendo as amostras de artefatos cibernéticos.

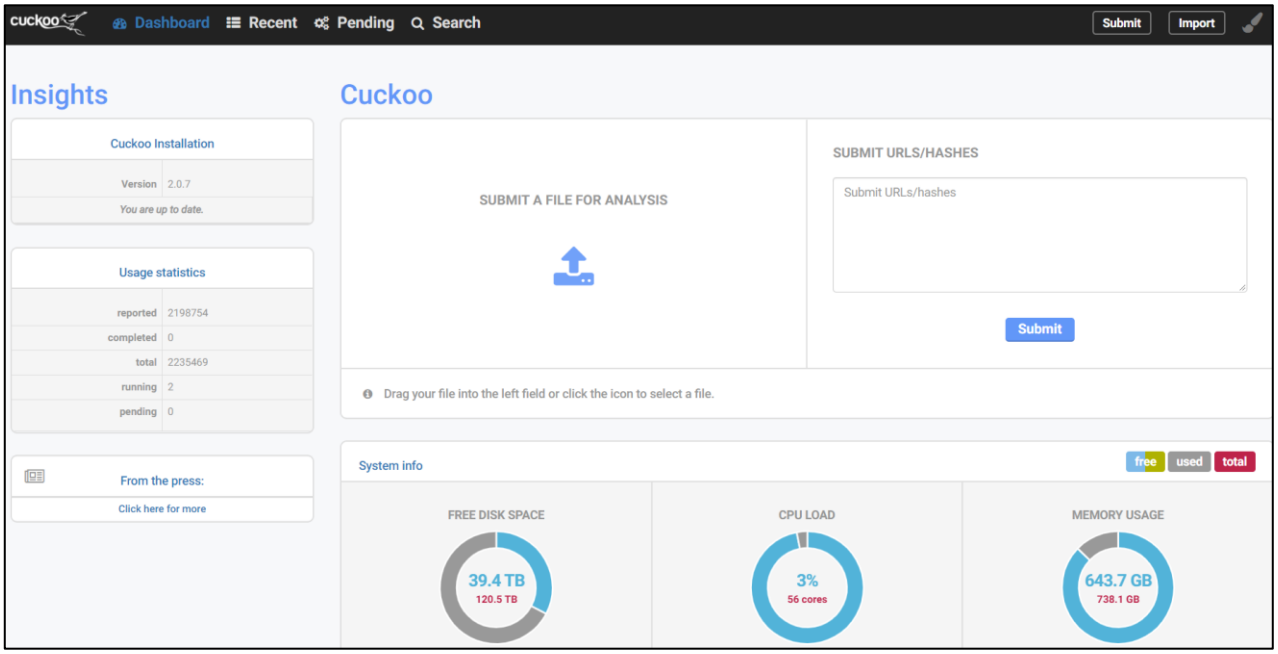

Figura 3: *Cukoo Sandbox* CERT-EE.
Fonte: https://cuckoo.cert.ee/

Dentro do Nível Tático, não há necessidade de disponibilizar a plataforma para a Internet, podendo ser utilizado usando a EBNet ou, dependendo das políticas de segurança, somente dentro do nível FTC ou outro escalão considerado, contanto que o órgão responsável pelo oferecimento da plataforma tenha capacidade de material e pessoal para administrar o serviço.

2.3.2 Proposta de um laboratório

A Figura 4 a seguir mostra um exemplo de como pode ser organizado laboratório para atingir os objetivos da tarefa de Teste de Artefatos Cibernéticos, em uma FTC, de maneira eficiente e de fácil acesso aos escalões considerados. Não sendo uma estrutura definitiva, pois tem flexibilidade para se ajustar principalmente às demandas ou limitações do escalão considerado. Sendo esta uma proposta, que na visão do autor, tem melhor capacidade de atender diferentes cenários:

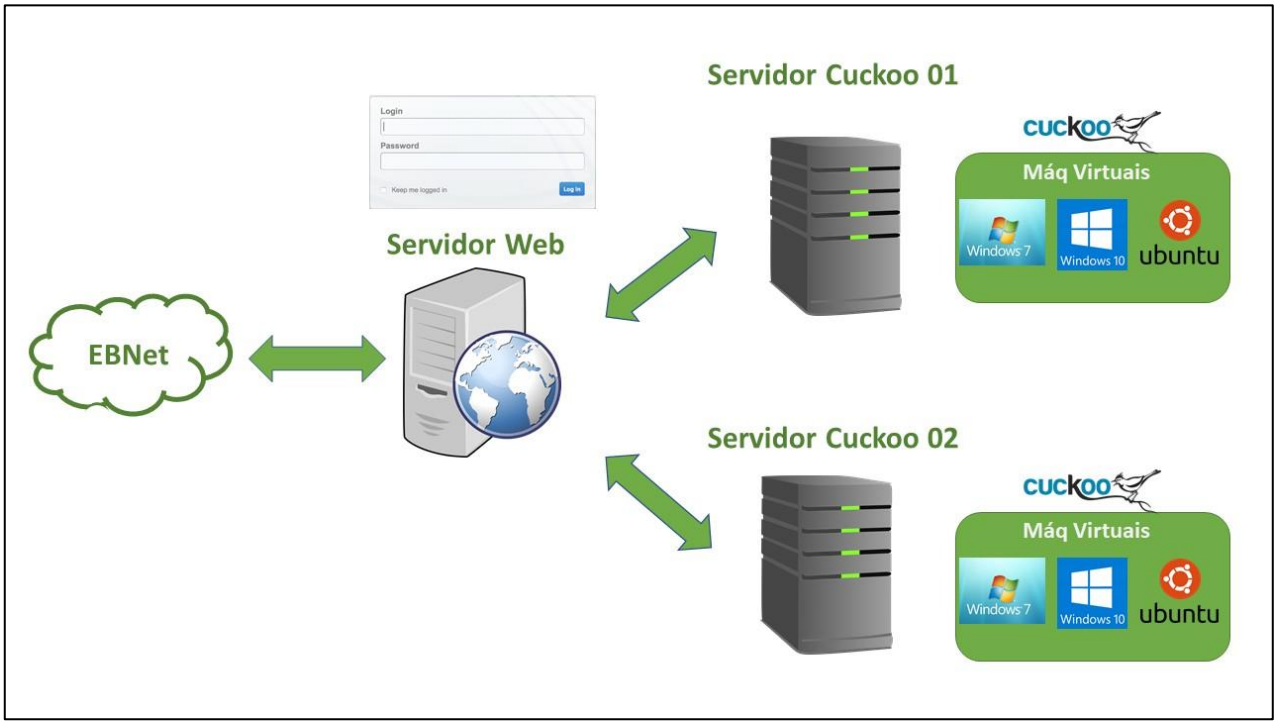

Figura 4: Proposta de um laboratório automatizado para análise de artefatos cibernéticos
Fonte: Autor, 2021

Podendo ser disponibilizado tanto na EBNet quanto na rede operativa de uma FTC, o laboratório pode ser constituído por 02 (dois) servidores Linux com o Cuckoo Sandbox possuindo, no mínimo, 02 (duas) Máquinas Virtuais Windows 7 e 02 (duas) Máquinas Virtuais Windows 10, sendo essas as versões mais utilizadas do Windows 10 atualmente e maiores alvos de *malwares*. Deve estar presente também uma Máquina Virtual Linux Ubuntu em cada servidor do Cuckoo Sandbox, pois apesar de em menores quantidades, o Sistema Operacional Linux pode também ser alvos de *malwares*, como por exemplo o *botnet Mirai*.

O acesso ao sistema seria através de um servidor Web com uma página requisitando um usuário e senha válidos, para maior segurança do sistema. Em relação aos requisitos do sistema, irão depender exclusivamente da demanda do laboratório, um comparativo possível seria com o servidor do Time de Resposta de Incidentes de Rede da Estônia (CERT-EE), o qual disponibiliza publicamente na Internet o seu servidor Cuckoo Sandbox. O *hardware* do servidor do CERT-EE possui 120 TB de armazenamento, 56 núcleos de processamento e 738 GB de memória.

3. ANÁLISE E RESULTADOS

Foi realizado o seguinte questionário em grupo de amostra constituído por pelo menos um oficial possuidor do curso de Guerra Cibernética em todos os B Com e Cia Com do EB.

O único questionamento foi sobre a quantidade de militares que possuíam o curso de Guerra Cibernética para Oficiais ou para Sargentos, considerando que através dessa especialização possuam a capacidade de analisarem artefatos cibernéticos no presente momento em situação de real emprego de suas OMs apoiando o escalão superior. No Gráfico 1 a seguir podemos ver a distribuição de militares com o curso de Guerra Cibernética por OM de comunicações:

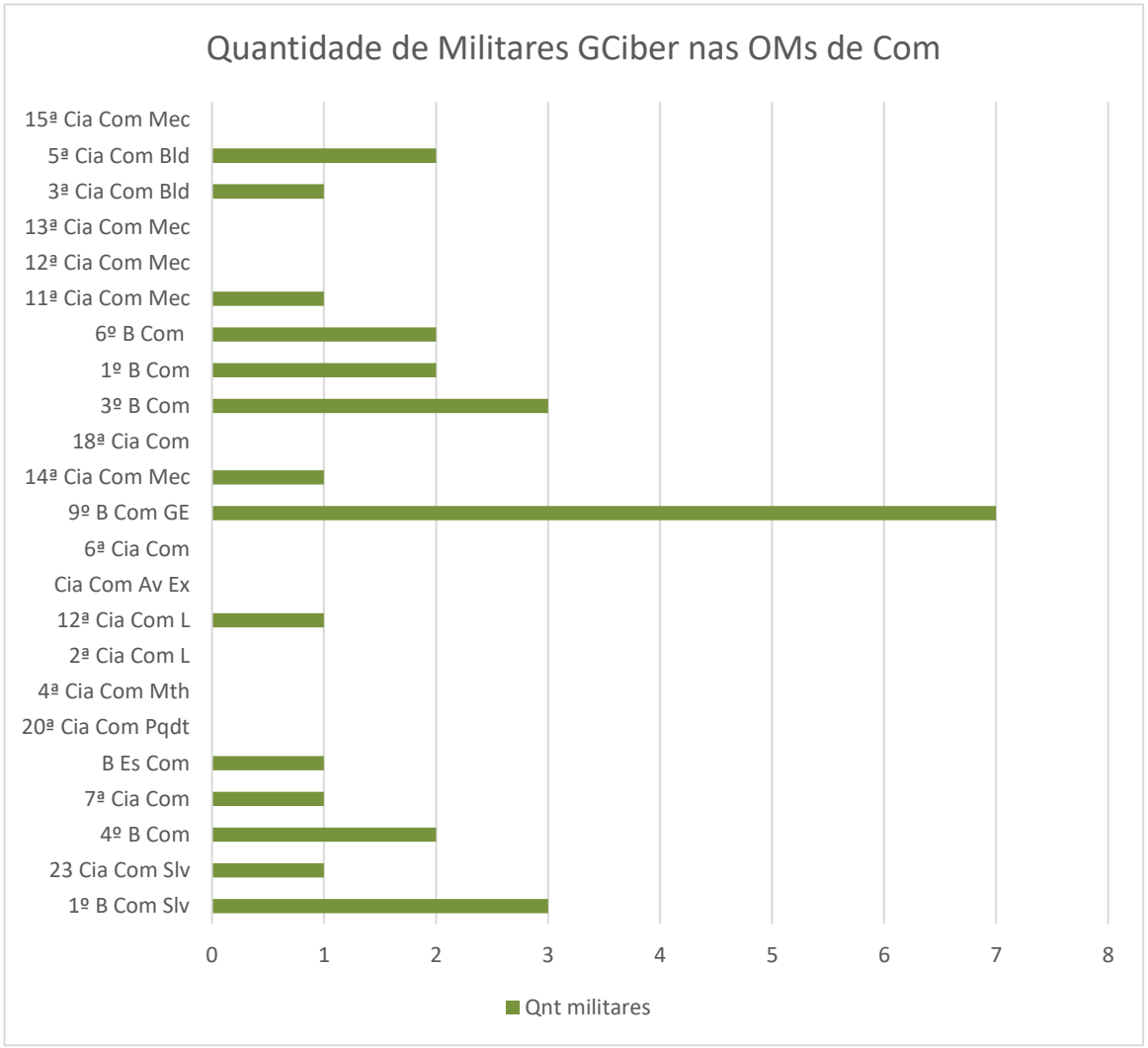

Gráfico 1: Quantidade de militares com o Curso de Guerra Cibernética nas OMs de Comunicações
Fonte: Autor, 2021

É possível observar que 9 (nove) das 23 (vinte e três) unidades e subunidades de Comunicações não possuem nenhum militar com curso de especialização de Guerra Cibernética. Mesmo que não seja regra para a OM possuir um militar especializado com curso para executar suas tarefas relacionadas a Proteção Cibernética, ainda sim é um indicativo de que a OM poderá ter deficiências de prestar essa proteção a todo o escalão considerado.

Importante ainda destacar que no 9º B Com GE, por ser o único do gráfico que tem responsabilidade tanto de Proteção quanto de Exploração Cibernética (BRASIL, 2017, p. 3-3), é coerente possuir mais elementos que as demais OMs.

O 1º BGE não foi incluído na relação devido a sua subordinação direta ser ao Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx) e não a um Comando Militar de Área, Divisão de Exército ou Brigada.

4. CONSIDERAÇÕES FINAIS E SUGESTÕES

O presente trabalho teve como objetivo norteador a proposta da criação de um laboratório para Teste de Artefatos Cibernéticos por acesso remoto por elementos responsáveis pela atividade de Proteção Cibernética prevista na Doutrina Militar Terrestre. E como delimitação para alcançar o objetivo geral, foram enumerados objetivos específicos que permitiram uma estruturação lógica e completa da pesquisa realizada.

No item 2.1 foi realizado uma revisão das Estruturas Operativas de G Ciber relacionando suas atividades cibernéticas e responsabilidades a luz do Manual de Campanha EB70-MC-10.232 GUERRA CIBERNÉTICA, dando grande destaque aos Batalhões de Comunicações e Companhias de Comunicações que devem realizar a proteção cibernética dos sistemas de informação do grande comando apoiado ou da grande unidade.

Visando identificar os principais tipos de *malwares* e suas finalidades, para compreender que tipo de artefatos são ameaças para as operações e como suas complexidades devem ser trabalhadas na proteção cibernética, foram elencados no item 2.2.1 os tipos seguindo a literatura atual de análise de malware.

Podemos elencar ainda como os tipos de malwares mais preocupantes ao serem encontrados nos sistemas de informações em operações os *backdoors* e *Information-stealing* devido à natureza sigilosa com que trabalham e principalmente com as capacidades de coletarem informações sensíveis e de espionagem. Outro tipo de *malware* prejudicial às operações são os *Virus* e *Worms* devido a suas capacidades de se espalharem e, muitas das vezes, estarem associados a *ransomwares* que criptografam arquivos dos usuários solicitando resgate em dinheiro para retornar o acesso dos arquivos novamente à vítima.

No item 2.3.2 pode se verificar uma proposta de laboratório para Teste de Artefatos Cibernéticos que poderia ser acessado pela EBNet remotamente pelos elementos de uma FTC ou outros escalões considerados, sendo uma sugestão tanto em software quando em hardware baseados no servidor do Time de Resposta de Incidentes de Rede da Estônia (CERT-EE).

Em relação a utilização do laboratório em operações, uma ideia geral seria submeter anexos recebidos em e-mails de remetentes desconhecidos, programas

executáveis e instaladores, além de arquivos compartilhados por aplicativos de mensagens ou *links* para *download*. A sequência das ações pode ser orientada com o seguinte fluxograma:

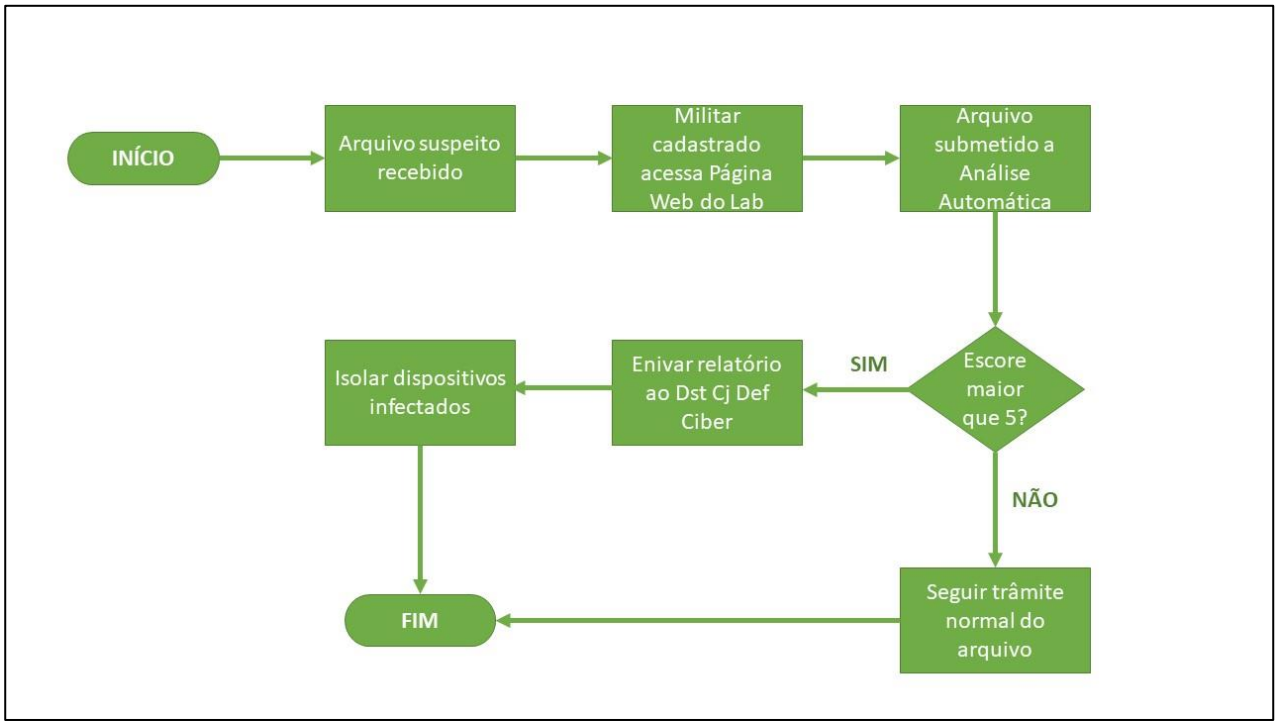

Figura 5: Fluxograma para utilização do Laboratório
Fonte: Autor, 2021

Com a verificação da quantidade de militares com o Curso de Guerra Cibernética nas Organizações Militares de Comunicações, onde mais da metade delas só possuem 1 (um) ou nenhum militar especialista na área, podemos inferir que provavelmente essas unidades e subunidades não conseguiriam atender plenamente suas tarefas de Proteção Cibernética atualmente.

Neste sentido, podem ser realizados treinamentos prévios às operações para as OMs sem nenhum militar especializado, com o objetivo de aprender o uso básico do laboratório e a filtragem de arquivos suspeitos, além de boas condutas para a Proteção Cibernética dentro de suas áreas de responsabilidades.

Com isso, a utilização de um laboratório para análise automática de Artefatos Cibernéticos como proposto nesse trabalho, pode permitir o cumprimento dessa tarefa prevista da Proteção Cibernética mesmo quando a Estrutura Operativa responsável não possua recursos materiais e humanos específicos para isso.

Sugere-se como aprofundamento desse trabalho o teste da estrutura apresentada em exercícios operacionais primeiramente em um nível Brigada e em seguida em um nível

Divisão de Exército, precedidos por instruções de utilização avançada da plataforma para os elementos das Cia Com e B Com responsáveis, e instruções básicas para o restante dos usuários do sistema.

Por fim, este trabalho ainda tenta despertar o interesse em outras pesquisas que visem a automação de outras Tarefas de Proteção Cibernética listadas no Manual de Guerra Cibernética EB70-MC-10.232, para que o Exército Brasileiro possa consolidar uma estrutura de Guerra e Defesa Cibernética robusta e próxima ao estado da arte.

REFERÊNCIAS BIBLIOGRÁFICAS

BOSCO, Natália. **Ataque de hackers ao STJ é o mais grave da história no país**. Correio Braziliense, 2020. Disponível em: <https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html>. Acesso em: 15 fev. 202

BRASIL. Exército. Comando de Operações Terrestres. **EB70-MC-10.232**. Guerra Cibernética. 1ª ed. Brasília, DF, 2017.

_____. Ministério da Defesa. **MD31-M-07**. Doutrina Militar de Defesa Cibernética. 1ª ed. Brasília, DF, 2014b

_____._____. **MD33-M-02**. Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas; Brasília, 2008a.

_____. Núcleo de Informação e Coordenação do Ponto Br. **Estatísticas dos Incidentes Reportados ao CERT.br Janeiro a Junho de 2020**. Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-jun/total.html>. Acesso em: 15 fev. 2021.

CLARKE, Richard A; KNAKE, Robert K. **Cyber War: The Next Threat to National Security and What To Do About It**. New York: HarperCollins. 2010

CERT-EE. **Computer Emergency Response Team Estonia**, disponível em <https://www.ria.ee/en/cyber-security/cert-ee.html. Acesso em 17 jul 2021.

LOPES, Gills Vilar; OLIVEIRA, Carolina Fernanda Jost de. **Stuxnet e Defesa Cibernética Estadunidense à luz da análise de Política Externa**. Revista Brasileira de Estudos de Defesa, 2014.

SIKORSKI, M.; HOGIN, A. **Pratical Malware Analysis**. 5. ed. [S.l.]: No Starch Press, 2012.

VIRUSTOTAL. **Virus Total**, disponível em <https://www.virustotal.com/>. Acesso em 17 jul 2021.