WALISSON MENDES FERREIRA

INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS EM UMA INSTITUIÇÃO FINANCEIRA

LAVRAS – MG

2022

WALISSON MENDES FERREIRA

INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS EM UMA INSTITUIÇÃO FINANCEIRA

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Bacharelado em Ciência da Computação para a obtenção do título de Bacharel.

Prof. DSc. Maurício Ronny de Almeida Souza

Orientador

LAVRAS – MG

2022

Ficha catalográfica elaborada pela Coordenadoria de Processos Técnicos

da Biblioteca Universitária da UFLA

Ferreira, Walisson Mendes

Inteligência de Ameaças Cibernéticas em uma Instituição Financeira / Walisson Mendes Ferreira. 1^a ed. rev., atual. e ampl. – Lavras : UFLA, 2022.

47 p. : il.

Relatório de estágio(graduação)–Universidade Federal de Lavras, 2022.

Orientador: Prof. DSc. Maurício Ronny de Almeida Souza.

Bibliografia.

1. TCC. 2. Monografia. 3. Dissertação. 4. Tese. 5. Trabalho Científico – Normas. I. Universidade Federal de Lavras. II. Título.

CDD-808.066

WALISSON MENDES FERREIRA

INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS EM UMA INSTITUIÇÃO FINANCEIRA

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Bacharelado em Ciência da Computação para a obtenção do título de Bacharel.

APROVADA em 09 de Setembro de 2022.

Prof. DSc. Raphael Winckler de Bettio	UFLA
Bel. Diego Arcanjo Lopes	UNA

Prof. DSc. Maurício Ronny de Almeida Souza
Orientador

LAVRAS – MG
2022

Dedico a minha familia e amigos. Em especial aos meus pais. Roseli e Alencar.

AGRADECIMENTOS

Agradeço primeiramente a minha mãe Roseli e meu pai Alencar, que sempre me apoiaram e forneceram todo o suporte para chegar até aqui.
Ao Prof. DSc. Maurício Ronny de Almeida Souza, pela orientação durante a escrita do presente documento.
A Universidade Federal de Lavras, que forneceu todo o material físico e humano, para que eu pudesse conquistar esse Título.
A todos meus amigos que me apoiaram e transformaram o processo até aqui mais que especial.

RESUMO

O trabalho relata as atividades de segurança de ameaças de inteligência em uma instituição financeira que atua no setor bancário brasileiro. A empresa conta com um aplicativo para dispositivos móveis, de forma que, todos os seus produtos e serviços são disponibilizados no mesmo visando facilitar a vida financeira dos usuários. A instituição como forma de proteção às ameaças cibernéticas, possui um setor de segurança da informação. O setor de segurança da informação é responsável por manter a integridade, disponibilidade e confiabilidade de todos os dados, evitando que ameaças cibernéticas impeçam a instituição de operar e fornecer os serviços normalmente. O objetivo deste trabalho é descrever as atividades desenvolvidas pelo autor durante o estágio supervisionado realizado na instituição. Desempenhando atividades relacionadas a inteligência de ameaças de segurança cibernéticas, onde é elucidado como ocorre a análise, investigação e documentação de artefatos maliciosos e vulnerabilidades identificadas em uma instituição financeira. Exemplificando o uso das ferramentas, UrlScan, VirusTotal, AlienVault e MISP. O estágio foi realizado no período de outubro/2021 à junho/2022, totalizando 1000 horas. Como resultados pode-se observar que a instituição possui processos bem definidos. Esses processos permitem que a análise de ameaças, seja de vulnerabilidade, seja de artefatos maliciosos, seja feita de forma eficiente. Permitindo que o estagiário aplique os fundamentos teóricos em prática e também desenvolver maior conhecimento e habilidades em inteligência de ameaças cibernéticas.

Palavras-chave: Relatório de estágio, Segurança da informação, Inteligência de ameaças cibernéticas

ABSTRACT

The work related to security activities from intelligence threats in a financial institution that operates in the Brazilian banking sector. The company has an application for mobile devices, where all its products and services are made available to allow all financial operations. The institution as a form of protection against cyber threats, has an information security sector. The information security sector is responsible for keeping all data safe, availability and reliability of security security that the institution operating and providing the services normally prevent the institution from operating and providing the security services. The purpose is to develop activities developed by the author, with the aim of carrying out dangerous activities in the institution, with the purpose of carrying out dangerous activities in the institution, with the purpose of carrying out dangerous activities in the investigation, investigation and investigation work dangerous in artificial intelligence . identified in a financial institution. Exemplifying the use of the tools, UrlScan, VirusTotal, AlienVault and MISP. The study was carried out from October/2021 to June/2022, totaling 1000 hours. As the results can be observed that the institution has processes well itself. These processes allow the analysis of threats, whether risky or dangerous risks, done efficiently. Allowing the intern to apply the theoretical foundations in practice and also develop knowledge and skills in cyber threat intelligence.

Keywords: Internship report, Security information, Cyber threat intelligence

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Empresas do setor bancário tem como objetivo fornecer para pessoas e empresas operações financeiras de forma facilitada. Dessa forma, o número de ameaças cibernéticas focadas no setor bancário e financeiro aumentou cerca de 333% entre fevereiro a abril de 2019, o Brasil é o principal foco dos cibercriminosos (ROLFINI, 2022).

Instituições financeiras e outras empresas do setor financeiro tem sido um dos principais alvos de ataques cibernéticos (E-VAL, 2022). Isso ocorre pela abundancia de informações confidenciais contidas nos arquivos dos clientes, especialmente transações de pagamento online. Segundo a Febraban (2022) segurança da informação é uma das prioridades do setor bancário no Brasil. Segundo estimativas, as instituições financeiras investem cerca de R$ 2 bilhões anualmente para o fortalecimento e melhoria nos sistemas de tecnologia voltados à segurança da informação. Correspondendo a 10% dos valores totais gastos no setor de tecnologia (FEBRABAN, 2022).

Essas instituições então, como forma de proteção à ameaças cibernéticas, dispõem de um setor responsável pela segurança da informação. O setor de segurança da informação é responsável por manter a integridade, disponibilidade e confiabilidade de todos os dados, evitando que ameaças cibernéticas impeçam a instituição de operar e fornecer os serviços normalmente.

Neste contexto, o objetivo deste documento é descrever as atividades desenvolvidas pelo autor durante o estágio supervisionado realizado em uma instituição financeira. O objetivo do estágio era desempenhar atividades relacionadas à segurança cibernética, onde era responsável por analisar, investigar e documentar artefatos maliciosos e vulnerabilidades que eram identificadas. O estágio foi realizado no período de outubro/2021 à junho/2022, totalizando 1000 horas.

1.1 Contexto do estágio

O estágio foi desenvolvido em uma instituição que atua no ramo financeiro bancário, considerada de grande porte. Onde atualmente fornece todos os seus serviços e produtos de forma 100% digital. Os serviços e produtos fornecidos pela instituição são centralizados em um único aplicativo para dispositivos móveis onde os serviços e produtos são: Serviço que permite a realização de opera-

ções e investimentos na bolsa de valores[1]; Serviços voltados a seguros imobiliários e veiculares; Provê uma conta totalmente digital que permite que seja gerenciado todos gastos e aquisições dos clientes.

Atualmente a empresa conta com mais de quatro mil (4000) colaboradores. Divididos em formas de equipes responsáveis por produtos. O setor de segurança da informação possui aproximadamente 50 colaboradores, divididos em equipes de segurança de operações, segurança ofensiva, segurança forense, segurança em nuvem e a equipe de resposta a incidentes.

O estagiário atuou na equipe de *Inteligência de Ameaças*. Para o início das atividades é realizada uma reunião de alinhamento onde são definidas as atividades que serão desenvolvidas. Com o projeto definido as tarefas são divididas em pequenas partes, onde as tarefas priorizadas são iniciadas de imediato. É reservado tempo para tarefas que podem aparecer no decorrer do projeto, visto que há atividades que são realizadas sob demanda. Para o acompanhamento das atividades são marcadas reuniões diárias onde a equipe aborda o que foi desenvolvido em detalhes, apresenta impedimento para a realização da tarefa e também dúvidas. Ao final de cada projeto é realizada uma reunião onde são apresentados os resultados obtidos durante o desenvolvimento do projeto.

1.2 Organização do Trabalho

O presente trabalho visa relatar as experiências e atividades desenvolvidas durante o período de estágio. Desta forma o documento se encontra organizado no sistema de capítulos, onde no Capítulo 1 é feita uma introdução da empresa onde o estágio foi realizado, descrevendo seu funcionamento e uma breve definição dos objetivos do estágio. O Capítulo 2 aborda uma explicação inicial sobre os conceitos e tecnologias utilizadas durante a execução das atividades propostas. O Capítulo 3 relata de forma detalhada as atividades que foram desenvolvidas durante o projeto de estágio. Elucidando a forma como são identificados e analisados *ransomwares*, *malwares* e vulnerabilidades. Apresenta como é realizado o uso de ferramentas de código aberto para o enriquecimento e compartilhamento de informações de segurança. Por fim, o Capítulo 4 apresenta uma conclusão contendo as habilidades que foram desenvolvidas, as dificuldades enfrentadas e a forma como os conhecimentos acadêmicos adquiridos foram utilizados de forma prática no mercado de trabalho.

[1] https://www.b3.com.br/pt_br/

2 CONCEITOS E TECNOLOGIAS

Este capítulo descreve alguns conceitos e tecnologias acerca da segurança da informação, inteligência em fontes abertas e inteligência de ameaças. Estes conceitos são importantes para o entendimento das atividades explicitadas no capítulo 3.

2.1 Segurança da Informação

A segurança da informação é definida como a proteção de dados de propriedade das organizações contra diversas ameaças, seja física ou lógica. Com o objetivo de mitigar riscos e garantir a continuidade das operações. Para ALVES (2006), a Segurança da Informação "visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios". A segurança da informação pode ser dividida em duas partes (ALVES, 2006):

- Informação: É o conteúdo de valor para a empresa ou profissional. São ativos muito importantes, que necessitam de cuidados especiais e restrições de acesso.
- Segurança: É a percepção de proteção contra perigos, ameaças e incertezas.

Para que seja possível realizar a proteção dos dados contra ameaças, sejam internas ou externas, é necessário que haja garantia de alguns princípios básicos de segurança da informação. Como descrito pela norma NBR ISO/IEC-17799(Norma Nacional de Segurança de Informação) ISO (2000), a proteção da informação é crucial, sendo caracterizada por: Confidencialidade; Integridade; Disponibilidade.

A "Confidencialidade" garante que somente pessoas autorizadas possam acessar as informações. Restringindo a permissão de divulgação de informação sem autorização prévia. Por sua vez, a "Integridade" garante que as informações não sejam alteradas ou violadas. Por fim, a " Disponibilidade" é a garantia do acesso da informação no momento desejado. Implica no funcionamento correto da rede e sistema.

A segurança da informação é dividida em frentes de atuação distintas. Cada parte é essencial em uma instituição (JUNIOR, 2020), sendo :

- *Cyber blue team*: É o grupo responsável por realizar a análise dos sistemas de informação com o intuito de garantir a segurança. Garantindo que todas as medidas de segurança sejam eficazes, identificando falhas de segurança e verificando todas as medidas de segurança. O *cyber blue team* deve possuir uma grande quantidade de habilidades, os quais devem incluir ativos como: monitoramento constante, análise forense digital, tratamento e resposta de incidentes e fatores de inteligência de ameaças com grande maturidade JUNIOR (2020).

- *Cyber red team*: Segundo (JUNIOR, 2020) o *red team* representa o atacante para o *cyber blue team*. Tem como objetivo avaliar a segurança da informação baseada na inteligência. Desta forma é examinado de forma extensiva os recursos de detecção de ameaças e respostas a incidentes do *cyber blue team*. O *cyber red team* simula ataques com condições reais, empregando as mesmas técnicas, táticas e procedimentos de adversários criminais. Sendo garantido assim que todas as iterações sejam o mais realista quanto possível, testando tecnologia, humanos e procedimento.

2.1.1 Vulnerabilidade

Uma vulnerabilidade é definida como condição que, quando explorada por um atacante pode resultar em uma violação de segurança. Segundo Sêmola (SÊMOLA, 2014) são fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

As vulnerabilidades são falhas que não provocam nenhum incidente, pois são elementos passivos, necessitando de um fator favorável ou agente causador.Do ponto de vista de Sêmola (SÊMOLA, 2014) , são exemplos de vulnerabilidade:

- Físicas: A falta de recursos de mitigação e prevenção em ambientes com ativos ou informações estratégicas, como extintores, detectores de fumaça e outros recursos de combate a incêndio.

- Naturais: Locais com equipamentos eletrônicos próximos a locais propensos a desastres naturais, como incêndios, terremotos entre outros, como aumento de umidade e temperatura, falta de energia etc.
- Hardware: Computadores suscetíveis à poeira, à umidade, à sujeira e ao acesso indevido a recursos que são protegidos de forma inadequada e podem sofrer com defeitos de componentes ou componentes mal configurados.
- Software: Erros na instalação, codificação ou configuração de sistemas e aplicativos, que podem acarretar em acessos indevidos, perda de dados, indisponibilidade de recursos e vazamento de informações.
- Humanas: Falta de conscientização e treinamento de pessoas, avaliação psicológica adequada, problemas anteriores, má-fé ou descontentamento de um funcionário, à não execução de rotinas de segurança ou erros e omissões que coloque as informações em risco.

2.1.2 *Malware*

Segundo Andrea et. al. (CANI ANDREA; GAUDESI, 2014) *malware* são softwares com intenção maliciosa, programados para coletar informações confidenciais, obter acesso a sistemas privados ou interromper operações legítimas em computadores. *Malware* ou códigos maliciosos são programas desenvolvidos especificamente para executar ações danosas e atividades maliciosas em um computador.

Existem diversos tipos de *malware*, sendo eles:

- Cavalos de tróia: São programas que se apresentam falsamente por um programa benigno com o intuito de enganar a vítima. Normalmente são carregados com funções maliciosas ativadas com a inicialização do aplicativo. São espalhados geralmente por meio da engenharia social.
- *Rootkit*: São programas que tem como premissa padrão permanecer oculto evitando a detecção. Os pacotes possuem software que permite essa ocultação do sistema operacional e fique oculto do usuário. Os rootkits podem impedir que o processo esteja presente na lista de processos do sistema.

- *Backdoor*: É um método de contornar métodos tradicionais de autenticação. Uma vez instalado no sistema comprometido, o backdoor permite o acesso posteriormente de forma invisível ao usuário. Backdoor podem ser instalados por cavalos de Tróia, worms ou outros métodos.

- *Worm*: É software malicioso autônomo que consegue se replicar sem infectar arquivos. Esse software é transmitido pela rede de forma independente.

- Vírus: É a forma mais comum de *malware*. Normalmente oculto dentro de outros programas. Pode gerar cópias de si mesmo para impedir a remoção. Desta forma podem executar ações maliciosas no hospedeiro. Majoritariamente a forma de funcionamento é destrutiva.

As formas de defesa variam de acordo com o tipo de *malware*. Em sua maioria podendo ser evitada por um sistema de proteção, como antivírus, atualizações regulares dos programas e isolamento dos sistemas infectados.

2.1.3 *Ransomware*

Segundo a TrendMicro (TRENDMICRO, 2022) *ransomware* é um tipo de *malware* que não permite que o acesso do usuário seja realizado normalmente no sistema. Impedindo que o sistema seja utilizado, até o pagamento do resgate. O *ransomware* é um *malware* do tipo cripto virologia (Utilização da criptografia para criar softwares maliciosos). Ameaçando a publicação de dados pessoais da vítima. Os ataques normalmente utilizam um *malware* disfarçado como arquivo legítimo para o usuário.

Enquanto alguns *ransomwares* simples podem bloquear o sistema sem danificar nenhum arquivo, *malwares* mais avançados usam uma técnica chamada "extorsão criptoviral", a técnica consiste na criptografia dos dados exigindo pagamento para liberação dos dados.

2.2 Inteligência de Ameaças Cibernéticas

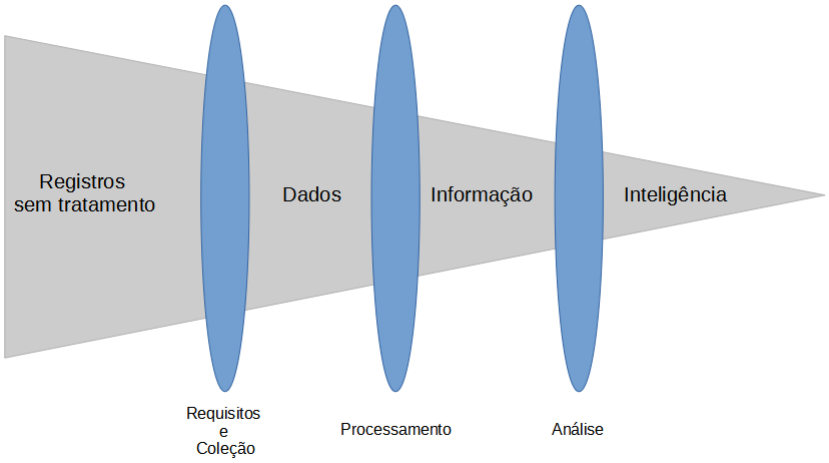
Segundo GARTNER (2016) a inteligência de ameaças é o conhecimento baseado em evidências, incluindo contexto, mecanismos, indicadores, implicações e conselhos acionáveis, sobre uma ameaça ou perigo existente ou emergente para ativos que podem ser usados para informar decisões

sobre a resposta do sujeito a essa ameaça ou perigo. A inteligência são dados obtidos através de um processo lógico e analítico, geralmente por meio de um processo humano que avalia os dados no contexto e produz uma saída utilizável.

Ferramentas de segurança que fornecem registro de todas as informações que são trafegadas diariamente nos sistemas. Porém a quantidade de dados que é coletada, torna impossível o processo de análise dessas informações (KASPERSKY, 2022). É necessário um sistema gerenciado de segurança, que verifica e correlaciona os dados encontrados com fontes de inteligência, para transformar essas informações em algo que permite identificar incidentes. Na figura 2.3 é ilustrado como a inteligência de ameaças trabalha com os dados.

Figura 2.1 – Relacionamento dos dados, informação e inteligência

.



Fonte: Adaptação de ABU Md Sahrom; SELAMAT (2018)

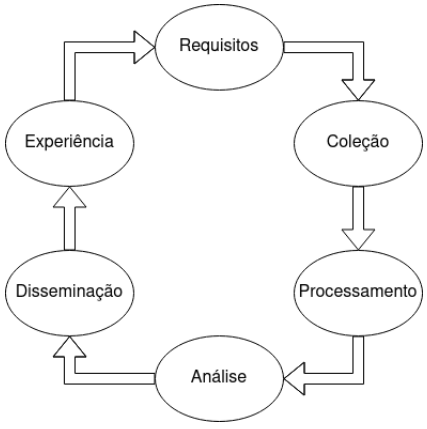
O processo de inteligência de ameaças é um grande desafio, pois as ameaças estão em constante evolução, demandando que os processos sejam adaptados e decisões sejam tomadas de forma rápida e acertiva. Segundo a CROWDSTRIKE (2022) o ciclo de inteligência de ameaças provê uma estrutura que permite que sejam realizadas respostas rápidas e precisas em ameaças modernas, assim otimizando os recursos. Com a rápida mudança do cenário de ameaças é necessário uma arquitetura que seja efetiva e possa suprir todos os tipos de necessidades. Também segundo a CROWDSTRIKE (2022) o ciclo de inteligência de ameaças possui seis estágios, sendo eles: Requisitos, coleção, proces-

samento, análise, disseminação, experiência. O estágio de requisitos é um estágio crucial para o ciclo de inteligência de ameaças, pois define a metodologia e objetivos que serão empregadas durante uma operação especifica. Durante esta fase de planejamento, algumas perguntas devem ser respondidas, sendo elas:

- Quais os atacantes e motivações de ataque?
- Qual a superfície de ataque?
- Quais ações específicas devem ser tomadas para fortalecer suas defesas contra um ataque futuro?

No estágio de coleção a coleta de informações é iniciada para satisfazer os objetivos definidos. Com base nos objetivos, são buscadas informações sobre diversos tipos de registros e locais. Ao fim da coleta de dados brutos, o estágio de processamento adequa todos os dados que foram coletados. Sendo realizado um refinamento em todas as informações. Após os dados serem atualizados e refinados. O estágio de análise busca responder às questões do estágio de requisitos. O estágio de disseminação necessita que a análise realizada seja compartilhada. De forma a apresentar os resultados obtidos de forma sucinta. O estágio final do ciclo de inteligência de ameaças envolve obter os pontos negativos e positivos de todo o ciclo, para que possam ser analisados. Isso provê uma melhora nos pontos necessários do ciclo de inteligência.

Figura 2.2 – Ciclo de vida inteligência de ameaças



Adaptado (SOCRADAR, 2022)

A arquitetura citada anteriormente ocorre de forma cíclica, onde a versão anterior sempre melhora a próxima versão. Desta forma, permite que esses processos sejam eficientes para ameaças modernas. Na figura 2.2 é ilustrado como o processo é realizado.

2.2.1 Técnicas, Táticas e Procedimentos

Segundo Ken Dunham (DUNHAM KEN;LUCAS, 2017) técnicas, táticas e procedimentos, ou TTP, são padrões de atividades ou métodos associados a um agente especifico ou grupo de agentes de ameaça. Segundo Abel Yeboah-Ofori (YEBOAH-OFORI ABEL;ISLAM, 2018) TTP é uma forma de representação do comportamento ou modo de operação do adversário ou ator de ameaça. Onde aproveita recursos, comportamentos e explorações específicos do adversário que pode ser utilizado em vitimas. As técnicas, táticas e procedimentos coletam informações sobre ameaças cibernéticas, sobre padrões de ataque, recursos implantados e explorações. Essa técnica é importante para identificar atores de ameaça. Desta forma visa fornecer a inteligência de ameaças sobre os motivos dos adversário, efeitos pretendidos e impactos que podem ser gerados.

Para que os TTP possam auxiliar no processo de inteligência de ameaças cibernéticas, devem ser armazenados de maneira aplicável e eficiente. Desta forma os dados são interconectados com correlação em plataformas de inteligência, como o MISP, discutido na seção 2.3.4.

Para comparar os TTP e aproveitá-los no processo de inteligência de ameaças cibernéticas, eles devem ser armazenados de maneira eficiente e aplicável. Isso geralmente inclui um conjunto de dados interconectados com correlação cruzada em uma plataforma de inteligência de ameaças. Os indicadores mais proeminentes são:

- Anomalias e divergências encontradas em atividades de usuários privilegiados.
- Sinais de atividade suspeita em login.
- Solicitações de DNS desviantes.
- Tráfego de internet com comportamento anomálo.
- Atividade incomum no tráfego de rede, seja de entrada ou saída.

- Anormalidades geográficas.
- Aumento no volume de leitura em banco de dados.
- Respostas HTML incomuns.
- Alteração de perfis em dispositivos móveis.
- Sinais de atividade de negação de serviço.
- Pacote de dados inseridos de forma incorreta.
- Tráfego de aplicações conflitantes.
- Número de solicitações superior ao comum.
- Alterações incomuns em registros no sistema.

2.2.2 Indicadores de Comprometimento

Os indicadores de comprometimento (IOC - *Indicators of Compromised*) são artefatos observados em um sistema operacional ou rede, indicando uma invasão do computador (GOV, 2022). Assim como há evidências físicas, os indicadores de comprometimento são evidências digitais. Essas pistas digitais ajudam profissionais de segurança da informação a identificar ameaças de segurança e atividades maliciosas, como violação de dados, ameaças internas ou ataques de *malware*. Os indicadores são coletados analisando artefatos maliciosos encontrados. Os indicadores permitem que seja feita a mitigação de incidentes de segurança ou artefatos, pois permite que seja identificado e/ou localizados. Os IOC mais comuns são HASH md5, domínio C2, chave de registro e nome de arquivo, este último mais complicado por estar mudando constantemente.Os HASH md5 é um valor de 128 bits utilizado para a criptografia; Domínio C2, ou comando e controle, são formas de distribuir malware via e-mail com o intuito de obter o controle total do sistema.

2.3 Ferramentas de Ameaças cibernética

Na instituição financeira, as seguintes ferramentas são utilizas para apoiar o processo de inteligência, o AlienVault e VirusTotal para análise de IOC e dominios; O urlscan para análise detalhada de URL; e o MISP, plataforma de compartilhamento de *malwares* e vulnerabilidades. As seguintes sub sessões descrevem detalhes das ferramentas.

2.3.1 AlienVault

O alienvault [1] é uma plataforma web que permite analisar indicadores de comprometimento de código aberto AlienVault (2022). Desta forma, a plataforma permite que sejam realizadas análises de indicadores de comprometimento fornecidos por especialistas de segurança do mundo todo. A plataforma utiliza uma combinação de processamento de linguagem natural e aprendizado de máquina para automatizar a coleta e a correlação de dados de ameaças.

A plataforma possui a capacidade de processar e identificar inúmeras ameaças, sendo elas: Vulnerabilidades e Exploits; Ataques de força bruta; Ataques de negação de serviço; Detecção de *malware*; Ataques em nível de rede; Sondagem e Varredura do Sistema;Atividade Maliciosas.

Esses dados que são inseridos pelos especialistas de segurança, fornecem um panorama completo das ameaças. Permitindo identificar a origem da ameaça, grupos que estão utilizando, quais as técnicas, táticas e procedimentos sendo utilizados. Desta forma a plataforma permite correlacionar informações fornecidas por pessoas do mundo todo.

A plataforma correlaciona e recebe os dados das ameaças em forma de pulsos. Os pulsos fornecem um resumo da ameaça, indicadores de comprometimento relacionados, uma visão do software visado e outros detalhes que permitem identificar a ameaça (ALIENVAULT, 2022) . Os indicadores disponibilizados pela plataforma constituem uma ameaça ou definem uma sequência de ações que podem ser usadas para realizar ataques a dispositivos de rede e computadores. Os IOC de pulso incluem: endereços IP; Domínios; Nome do host; HASH de arquivo(MD5; SHA1, SHA256, PEHASH etc.);número da CVE; URL; endereços de e-mail; caminhos de arquivo;nomes dinâmicos.

[1] otx.alienvault.com

2.3.2 VirusTotal

O VirusTotal [2] é uma plataforma web que analisa e verifica indicadores de comprometimento, domínios e arquivos (TOTAL, 2022). As verificações realizadas contam com mais de 70 antivírus e serviços de bloqueio de URL e domínios, além de uma infinidade de ferramentas que extrai as assinaturas analisadas. Segundo Total (2022) qualquer usuário pode submeter um arquivo para análise na plataforma.

A ferramenta oferece diversos métodos de envio de arquivos, includindo, a interface web pública primária, utilizando sistemas de *desktop*, extensões ou API(*Application Public Interface – Interface Pública da Aplicação* programáticas. Assim como os arquivos, as URL podem ser enviados por vários meios diferentes, incluindo a página da Web do VirusTotal, as extensões do navegador e a API.

O site realiza a análise dos arquivos e URL enviadas fornecendo detalhes sobre os antivírus que detectam os artefatos analisados. Os relatórios gerados são compartilhados com os usuários da plataforma, que definem se o conteúdo é realmente prejudicial. Dessa forma, as informações que são dispostas na plataforma são validadas e permite identificar falsos positivos. São dispostas na plataforma ferramentas para pesquisas complexas baseadas em critérios para identificar e acessar amostras de arquivos prejudiciais para estudos adicionais. Isso permite descobrir e analisar novas ameaças e criar novas mitigações e defesas.

2.3.3 Urlscan

O Urlscan [3] é um website que realiza análise e escaneamento de sites, a ferramenta fornece informações detalhadas sobre os mesmos GILGER (2022). O site possui processos automatizados, de forma que, o acesso da URL como um usuário comum e registra todas as atividades de navegação criadas pela página. Isso inclui recursos como Javascript, CSS e outros. São identificados os domínios e URL contatados durante a análise.

[2] www.virustotal.com
[3] https://urlscan.io/

Como forma de prevenção, o site realiza a captura da tela do site analisado. Desta forma, reduz as chances de acessar uma página que possua um conteúdo malicioso. O site conta com um registro de mais de quatrocentos domínios e marcas monitoradas. De forma, se houver algum contato com esses domínios, será categorizado como potencialmente malicioso.

2.3.4 MISP

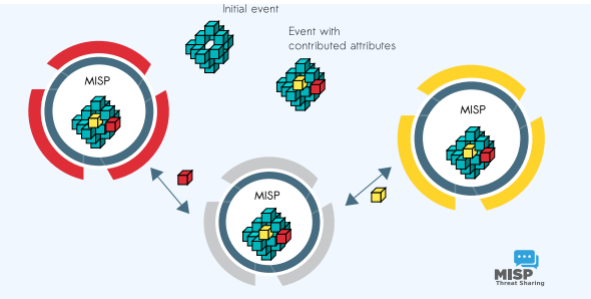
Segundo a CertBr (2022) o MISP é tanto uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, quanto um conjunto de padrões abertos para compartilhamento destas informações. A plataforma permite que sejam coletadas informações de parceiros, analistas e ferramentas de segurança (MISP, 2022). Desta forma é possível relacionar e enriquecer casos que estão sendo analisados. A ferramenta atende diferentes tipos de áreas de segurança, permitindo que possam compartilhar informações, sendo elas(MISP, 2022):

- Analistas de *Malwares*: Permite que sejam compartilhados indicadores das análises realizadas.
- Analistas de Segurança: permite identificar, verificar e utilizar indicadores de segurança, como indicadores de comprometimento.
- Analistas de Inteligência: A plataforma fornece ferramentas e recursos para reunir informações especificas sobre grupos maliciosos.
- Analistas de Fraudes: São fornecidas ferramentas para o compartilhamento de indicadores de fraudes financeiras.

Na plataforma cada caso criado é denominado “evento”. Desta forma, é possível contribuir adicionando os “atributos”, que são informações adicionais que são inseridas no eventos com o intuito de agregar mais informações. Na figura 2.3 é ilustrado como são feitas as contribuições.

Figura 2.3 – Eventos compartilhados no MISP

.



Fonte: https://www.misp-project.org

A plataforma possui diferentes níveis de compartilhamento de informação. Desta forma, é possível manter a confiabilidade e integridade dos dados que são inseridos. Os níveis de compartilhamento são (MISP, 2022):

- Somente organização: Os eventos e informações que são compartilhadas nesse nível, podem ser acessados apenas por membros da organização que criou o evento no MISP.
- Apenas comunidade: Usuários que integram a comunidade da plataforma podem visualizar os eventos, incluindo organizações que possuem conexões com os servidores.
- Comunidades conectadas: Usuários e organizações que utilizam o MISP podem visualizar os eventos e também todos os membros conectados com a organização.
- Todos: Sendo o nível mais permissivo. Permite que todos que possuem o MISP possam visualizar os eventos.

Por ser um projeto de software livre, modificações podem ser realizadas e adequadas a forma de uso desejada. Possui integração com diversas ferramentas e plataformas diferentes. Sendo utilizadas por organizações de segurança pelo mundo todo.

3 INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS EM INSTITUIÇÃO FINANCEIRA

Este Capítulo descreve atividades de inteligência de ameaças cibernéticas desenvolvidas na instituição financeira. As atividades desenvolvidas pelo estagiário consistiam em três frentes de trabalho: a análise de artefatos e práticas maliciosas (Seção 3.1); análise de vulnerabilidades envolvendo sistemas e aplicações internas da instituição (Seção 3.2) e Fontes abertas de inteligência (Seção 3.3)

Para a realização destas atividades, inicialmente o estagiário foi submetido a treinamentos e estudos. Estes treinamentos e estudos envolveram a realização de cursos nas plataformas utilizadas na instituição e estudos internos de plataformas desenvolvidas na instituição.

O estagiário foi alocado no Time de Resposta a Incidentes, que constitui a primeira linha de ação para incidentes de segurança na instituição. O time de resposta a incidentes possui três frentes de trabalho: Time de Sentinelas, (ii) Time de Engenharia de Dados, e (iii) Time de Inteligência. O Time de Sentinelas (i) é responsável pela análise, detecção e tratamento dos incidentes que ocorrem internamente na instituição. O "Time de Engenharia"(ii) é responsável por receber, automatizar e criar casos de uso para a detecção e prevenção de incidentes, com a utilização de um gerenciador de logs para eventos de segurança. O "Time de Inteligência"(iii) responsável por identificar e analisar artefatos maliciosos e vulnerabilidades para a prevenção e agregação de conhecimento nos casos criados.

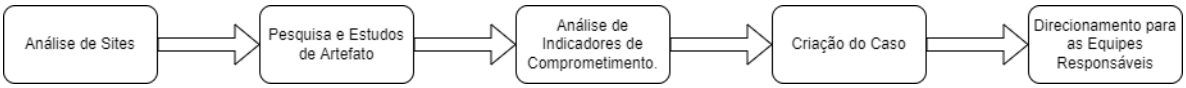
As seções a seguir descrevem de forma detalhada os fluxos de atividades referentes à análise de artefatos e práticas maliciosas (Seção 3.1), (ii) análise de vulnerabilidades envolvendo sistemas internos da instituição (Seção 3.2) e Inteligência em Fontes Abertas (Seção 3.3).

3.1 Análise de Artefatos e Práticas Maliciosas

Artefatos maliciosos são muito comuns em toda a internet, e existem com o intuito de adquirir algum acesso, informação, controle sobre máquinas ou até mesmo sistemas completos. Esse tipo de software pode causar grandes problemas se não detectado de forma prematura. Desta forma, foi incumbido ao estagiário a atividade de aprender sobre como esses artefatos são criados e utilizados, sejam eles *scripts*, aplicativos ou sites que ao serem acessados realizam o download de artefatos maliciosos que podem se aproveitar de brechas no sistema e realizar ataques. O trabalho de análise de artefatos e práticas maliciosas consiste na identificação, análise e documentação de ameaças na forma

de *malware*, ransomwares e phishing. O fluxo de tarefas para o desenvolvimento deste trabalho é apresentado na Figura 3.1.

Figura 3.1 – Fluxo de Trabalho análise de artefatos e práticas maliciosas



Fonte: Do autor.

A atividade de “Análise de Sites” consiste em identificar *malware* e *ransomwares* sendo utilizados por grupos maliciosos. Em seguida, a atividade de “Pesquisa e Estudo de Artefatos” consiste em analisar URL sendo utilizadas para a distribuição de artefatos maliciosos Na atividade de “Análise de Indicadores de Comprometimento"consiste em analisar *HASH* e outras assinaturas provenientes dos artefatos maliciosos. Então, na atividade de “Criação do Caso” todas as informações coletadas são agrupadas e organizadas onde é criado um documento detalhado sobre o artefato Finalmente, a atividade de “Direcionamento para Equipes Responsáveis” onde os dados encontrados são enviados aos times responsáveis para tratamento.

As subseções seguintes descrevem cada atividade desenvolvida em detalhes.

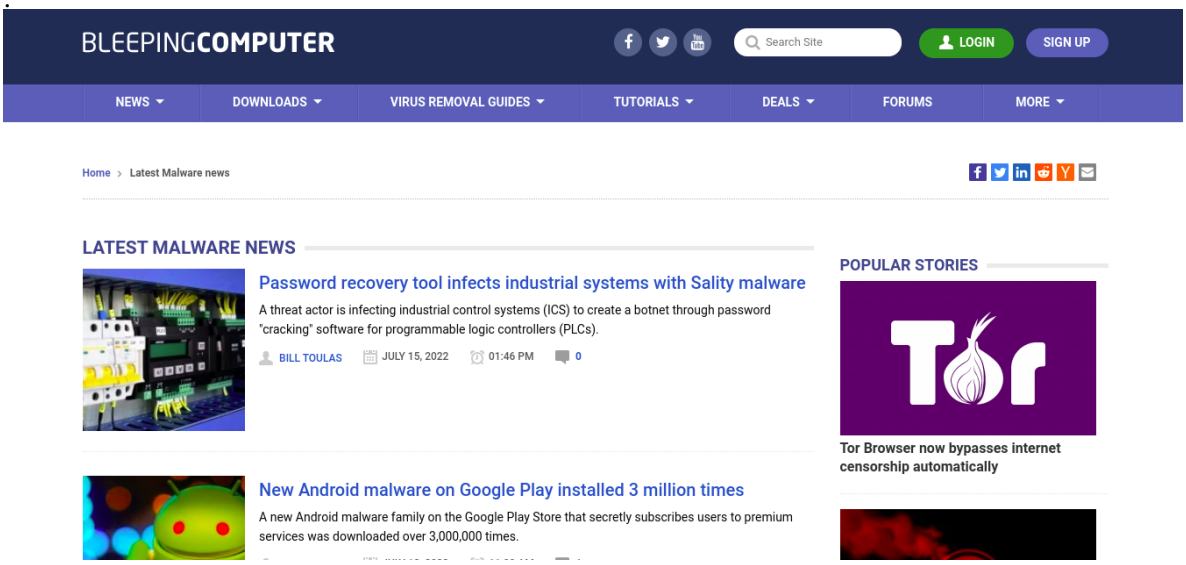
3.1.1 Análise de Sites

Há sites que divulgam diariamente notícias sobre *malware* e *ransomwares* atuais em uso por grupos criminosos. Desta forma, as atividades de análise de artefatos e práticas maliciosas é iniciado pela análise desses sites para a coleta de informações sobre possíveis ameaças que devem ser antecipadas pela organização. Normalmente, é utilizado um conjunto de sites de empresas especializadas em segurança, como Kaspersky[1] e McAffe[2]. Durante as atividades do estagiário, os principais sites utilizados para a coleta dessas informações eram BleepingComputer[3] (Figura 3.2), ThreatPost [4](Figura 3.3) e Welivesecurity [5](Figura 3.4). Os sites informam onde foram detectados inicialmente os *ran-*

[1] www.kaspersky.com
[2] www.mcaffe.com
[3] https://www.bleepingcomputer.com/tag/malware
[4] https://threatpost.com/category/malware-2/
[5] https://www.welivesecurity.com/br/

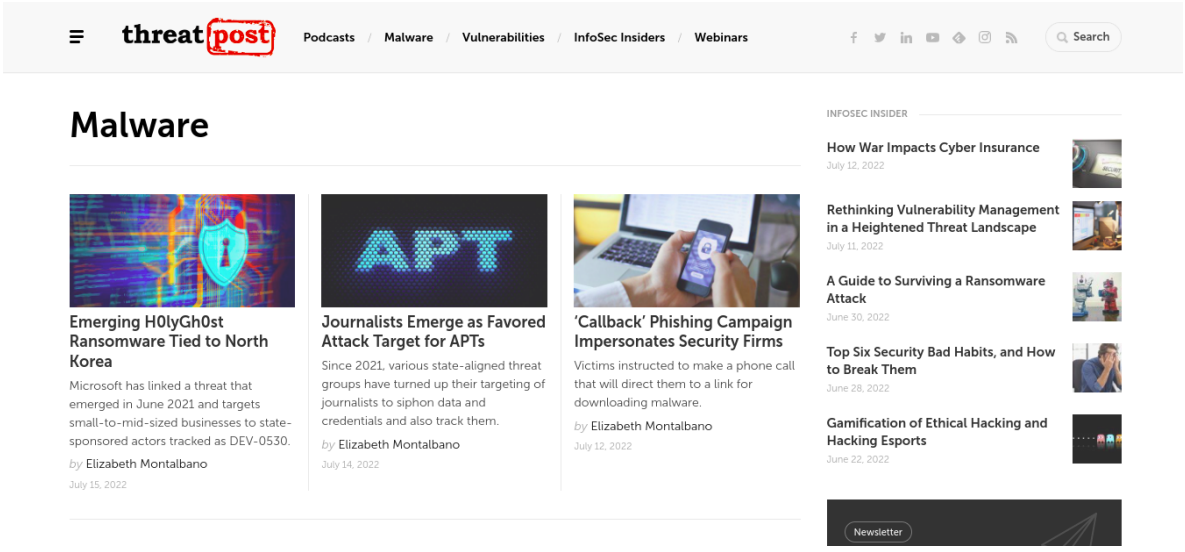
somwares e *malware*, a forma como são utilizados, o seu *modus operandi* e a forma de identificar e prevenir a instituição dos artefatos.

Figura 3.2 – Página do site Bleeping Computer sobre *malware*



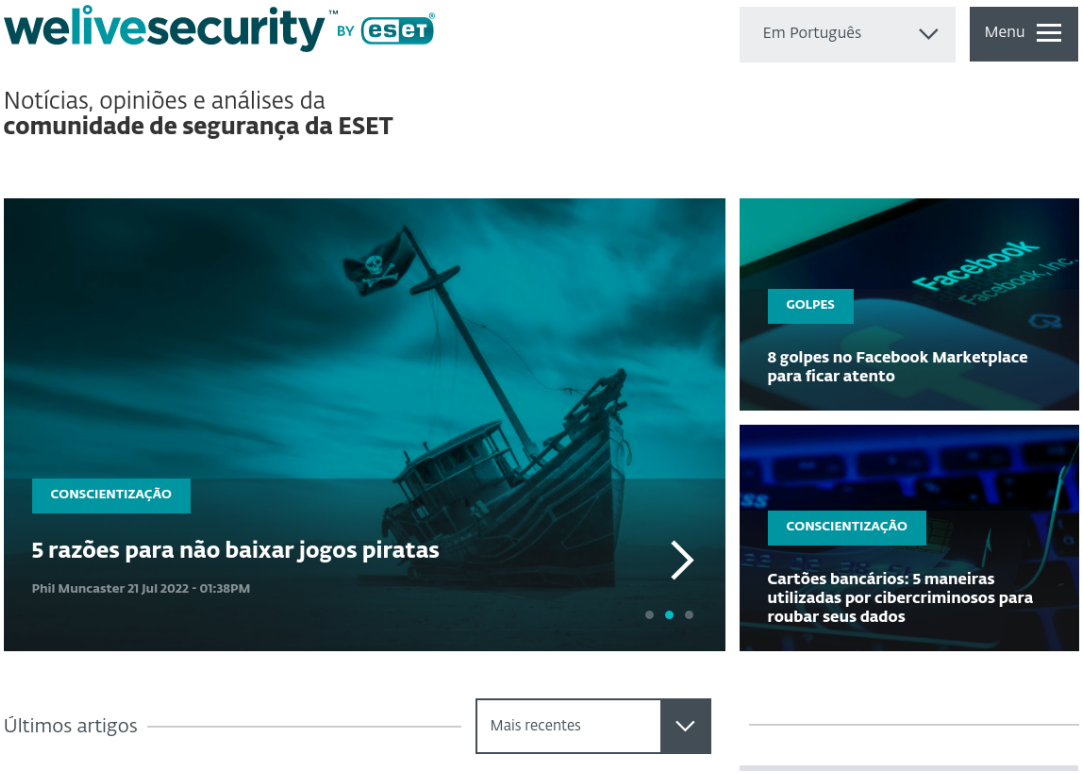
Fonte: www.bleepingcomputer.com.br

Figura 3.3 – Página do site ThreatPost sobre *malware*



Fonte: www.threatpost.com.br

Figura 3.4 – Página do site welivesecurity sobre *malware*



Fonte: www.welivesecurity.com.br

Diariamente, o estagiário realizava a leitura das últimas publicações relacionados a *malware* e *ransomwares* nos sites supracitados, com o intuito de identificar ameaças potenciais. Com base nesta leitura era feita a triagem dos artigos relevantes. Para cada artefato analisado, era necessário verificar os tipos de dispositivos afetados (servidores ou máquinas pessoais), e categorizar a ameaça por nível de criticidade. Os níveis de criticidade considerados são, “critico”, “alto”, “médio” e “informativo”.

Para cada nível de criticidade, uma estratégia de tratamento era aplicada. Os itens classificados como “Informativo” são apenas de prevenção, pois prematuramente é identificado que não apresenta ameaça ao ecossistema da instituição. Os itens classificados como “Médio” e “Altos” são inseridos em uma fila de atendimento, sendo atendidos normalmente conforme o fluxo da Figura 3.1. Por fim, os itens classificados como “Críticos”, são tratados de forma emergencial e imediata.

Um exemplo de ameaça identificada pelo estagiário foi o *malware* “Mekotio” utilizado pelo grupo Gamaredon[6]. A ameaça foi identificada inicialmente em uma postagem do site ThreatPost conforme Figura 3.5.

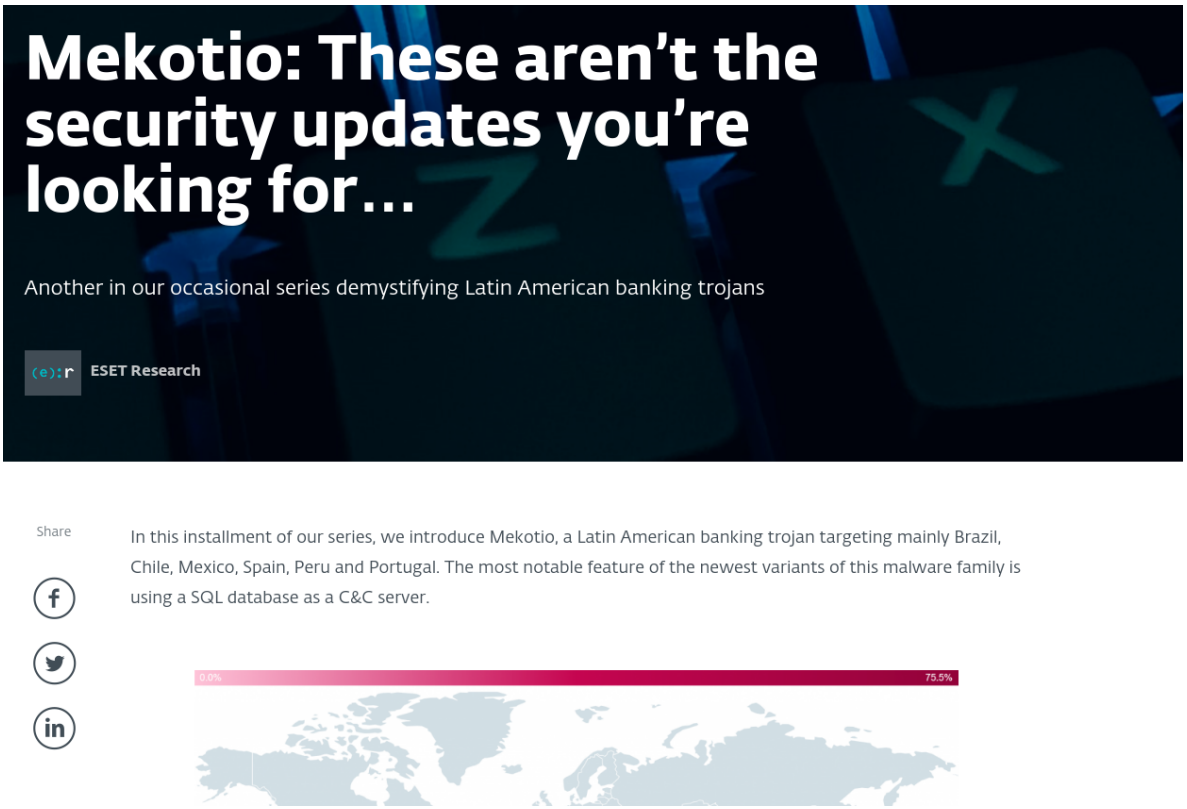
Figura 3.5 – Informação do *Malware* Mekotio

Fonte: https://threatpost.com/mekotio-banking-trojan-campaign/175981/

A ameaça foi classificada inicialmente como “Alto”, pois esse *malware* é utilizado no setor financeiro e tendo como foco instituições do Brasil. O artigo escrito no site forneceu algumas informações relevantes sobre o *malware*. Com a identificação do novo *malware*, novos sites são utilizados para complementar a pesquisa. Os sites fornecem informações coletadas por sistemas e/ou analisadas por especialistas em seguranças. No *malware* Mekotio foram analisados em média dez sites e relatórios diferentes com o intuito de agrupar o maior número de informação possível.

[6] https://www.enigmasoftware.com/pt/gamaredongroup-remocao/

Figura 3.6 – Informação do Grupo Gamaredon



Fonte: https://www.welivesecurity.com/br/2020/08/14/mekotio-analise-desta-familia-de-malware-bancario-que-e-direcionada-ao-brasil/

3.1.2 Pesquisa e Estudo de Artefatos

A pesquisa e estudo de artefatos é essencial para verificar se as informações encontradas são válidas. Ao fim da atividade de análise de sites é necessário enriquecer as informações encontradas nos sites ou fóruns. Algumas informações encontradas podem não ser relevantes para o caso, sendo feita então uma filtragem dos dados. A filtragem realizada tem como objetivo selecionar informações acerca do ransomware ou *malware* que foi encontrado, sendo categorizadas em: Modo de operação; Forma de distribuição; TTP.

O modo de operação fornece informações de como funcionam os *ransomwares* ou *malware*, os arquivos ou softwares que são atingidos. A forma de distribuição fornece as URL dos sites encontrados

que estão hospedando ou compartilhando o artefato que foi encontrado. Os TTP são um conjunto de informações contidos na tabela mittre [7], que fornece quais os tipos de ataque que o ransomware ou *malware* irá realizar dentro do sistema.

O processo de filtragem fornece informações que permitem uma análise e pesquisa mais profunda. Essa pesquisa é feita para que os dados sobre o *malware* e ransomware que foi identificado, sejam o mais completo possível, a fim de facilitar as análises e bloqueios.

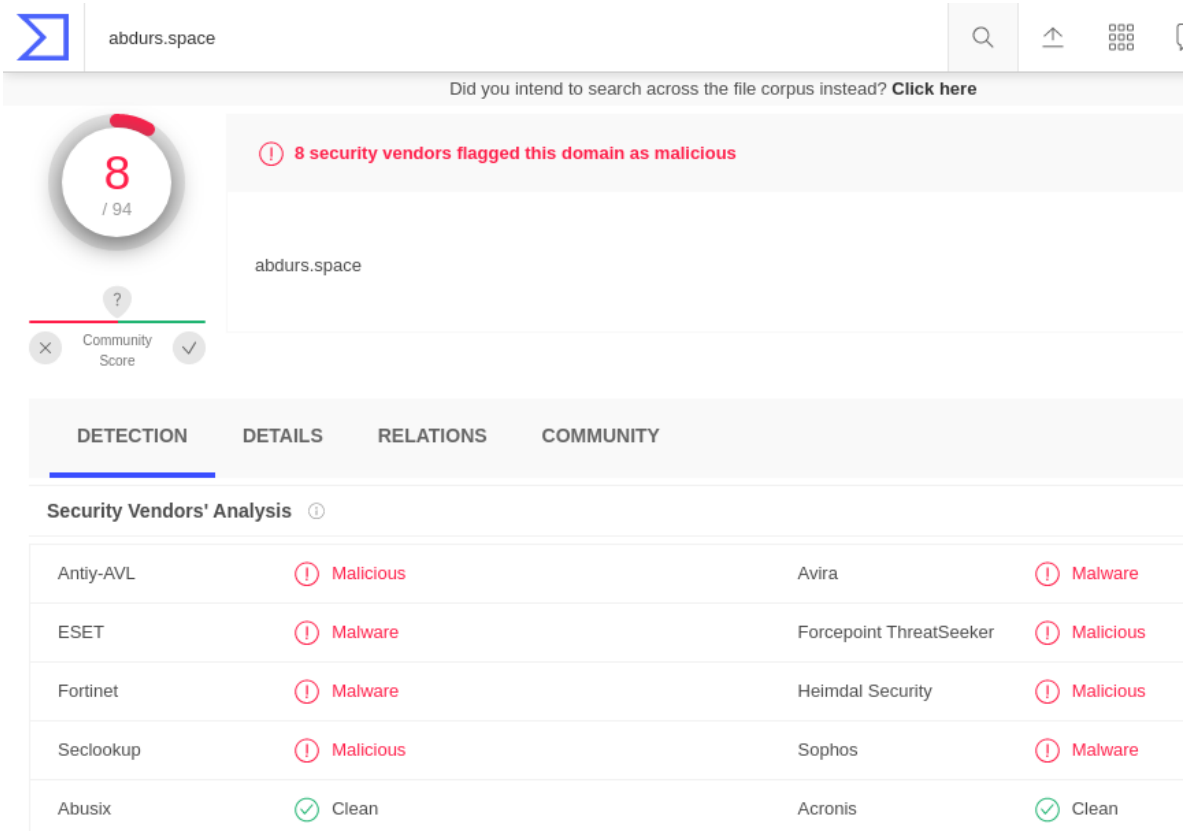
Como atividade inicial todas as URL que foram encontradas anteriormente são analisadas. Essas URL são inseridas em plataformas ou sites que fornecem detalhes e informações sobre os domínios que foram encontrados. O Virustotal definido na seção 2.3.2, fornece a reputação das URL que foram encontradas. O Urlscan definido na seção 2.3.3, permite acessar detalhes do responsável pelo domínio, país de origem e tecnologias utilizadas.

Durante a execução da tarefa o estagiário utiliza o Urlscan para verificar maiores informações sobre o domínio, proprietário, data de registro do domínio. Em paralelo a atividade de verificação de domínio é feita a análise de reputação utilizando o Virustotal.

O estagiário participou da análise do *malware* “Pterodo”, onde foram encontrados domínios que estavam sendo utilizados para a distribuição. Utilizando o Virustotal foi possível analisar a reputação das URL que foram identificadas. Na Figura 3.7 é ilustrado uma das URL que foram encontradas e a análise que o site fornece. Foi averiguado que a URL possui uma baixa reputação, um dos indícios que está sendo utilizado de forma suspeita. O site informa também as ferramentas que consideram que o link possui um comportamento suspeito.

[7] www.mittreattack.com

Figura 3.7 – Informação do *malware* Pterodo usado pelo Grupo Gamaredon



Fonte: www.virustotal.com

Como a URL apresentava caráter suspeito, foi necessário realizar uma pesquisa sobre o responsável pela URL. Foi utilizado o site Urlscan [8] para que fosse feita a análise sobre o domínio. Utilizando a ferramenta, foi possível identificar quando a URL foi disponibilizada para acesso e país de origem. Sabe-se que o *malware* "Pterodo" pertence a família Gamaredon. Família esta que possuía inúmeras formas de distribuição do artefato. Ao finalizar a análise, foi anexado ao caso todas as informações que foram levantadas, para que posteriormente fosse enviada aos times responsáveis.

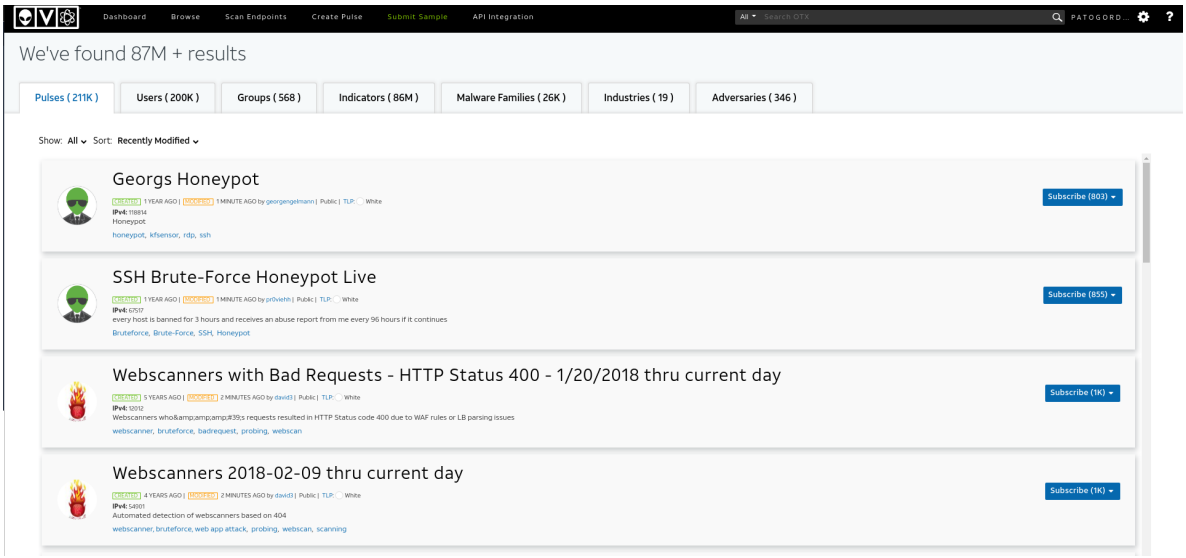
[8] urlscan.io

3.1.3 Análise de Indicadores de Comprometimento

A atividade de análise de indicadores de comprometimento ocorre paralelamente com a pesquisa e estudo de artefatos. Nessa atividade são analisados os HASH e assinaturas que foram encontradas durante a análise dos sites. Os indicadores de comprometimento são evidências que permitem identificar um artefato, ransomware ou *malware*. No time de inteligência as informações que são anexadas aos casos são os HASH.

O time de inteligência estuda as informações que foram encontradas nos sites, identificando *ransomwares* e *malware* que estão afetando sistemas e sendo utilizados, onde de forma preventiva é feita a proteção contra essas ameaças. Para que a análise seja feita é utilizada a plataforma AlienVault [9]. O AlienVault fornece detalhes a respeito dos HASH encontrados. Permitindo que seja possível identificar o *malware* ou ransomware a qual o HASH pertence. Os dados que a plataforma possui são inseridos por especialistas de segurança que realizam as análises dos artefatos que encontram. Em casos de artefatos que já foram analisados por outros especialistas em segurança, a ferramenta fornece a correlação que foi feita. Na Figura 3.8 é ilustrado a página inicial da plataforma.

Figura 3.8 – Página inicial do site alienvault

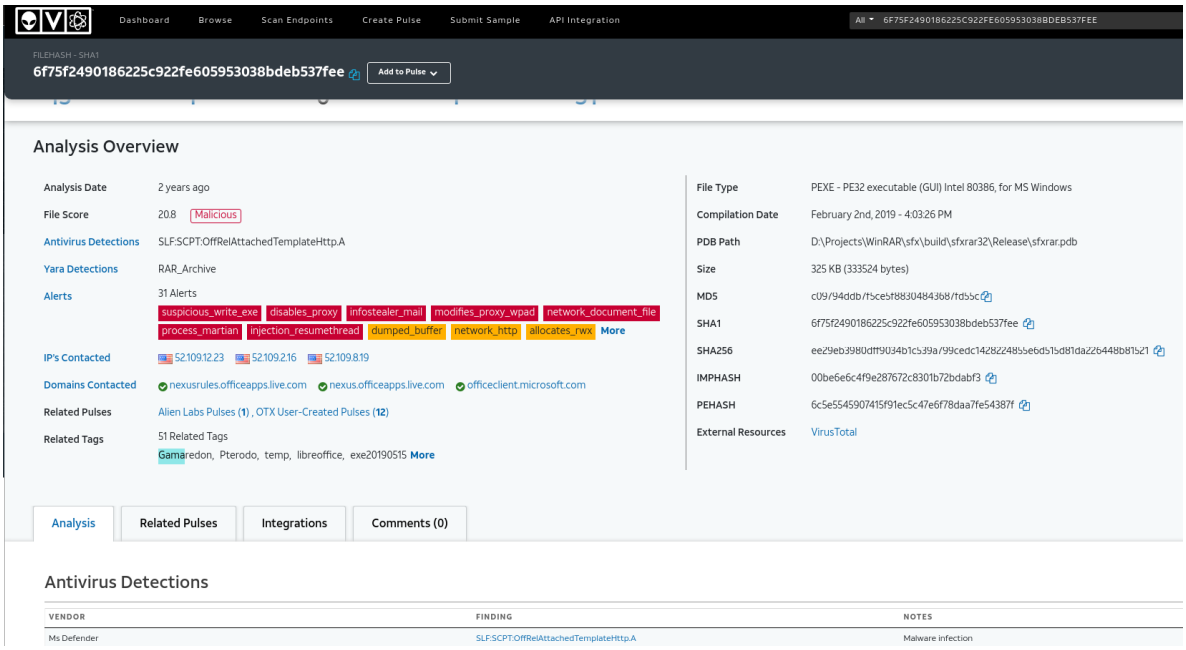


Fonte: otx.alienvault.com

[9] https://otx.alienvault.com/dashboard

Dentro da instituição, o estagiário agrupava todos os indicadores de comprometimento encontrados na análise dos sites. Foi realizada então uma análise inicial utilizando o Alienvault [10] para verificar se os HASH encontrados já foram mapeados e analisados anteriormente. Quando os indicadores de comprometimento já foram analisados anteriormente, a plataforma apresenta outros indicadores que se referem ao mesmo artefato que foi analisado. Há também na plataforma, o mapeamento de famílias de *ransomwares* ou *malwares* e identificação de grupos maliciosos, que permitem encontrar novos indicadores de comprometimento. A Figura 3.9 ilustra uma análise dos indicadores de comprometimento relacionados ao Gamaredon realizada pelo estagiário utilizando a plataforma do Alienvault.

Figura 3.9 – Análise do IOC que pertence ao gamaredon



Fonte: otx.alienvault.com.br

O HASH inserido na plataforma, fornece detalhes sobre qual o artefato que possui essa assinatura. *Ransomwares* e *malwares* podem ser utilizados por mais de um grupo. A página ilustrada na

[10] otx.alienvault.com

Figura 3.9 apresenta a etiqueta relacionada ao grupo malicioso Gamaredon. Com todas as informações analisadas é anexado ao caso todos os indicadores de comprometimento analisados.

3.1.4 Criação do Caso

A criação do caso é a consolidação de todos os dados que foram analisados. Quando criados podem ser direcionados aos times responsáveis para o devido tratamento. O caso é um documento que reúne todas as informações encontradas pelo time de inteligência. As informações que são inseridas no documento são: Resumo do artefato (i); Modo de Operação (ii); Forma de Distribuição (iii); TTP (iv); Indicadores de comprometimento (v);

O "Resumo do artefato" (i) consiste em criar um pequeno resumo com as informações do artefato, com pais e área de atuação, por exemplo financeira. O "Modo de operação" (ii) apresenta como o *malware* ou ransomware afeta o sistema e os arquivos que são normalmente afetados.Os "TTPs" (iv) informam sobre as técnicas e táticas que os grupos que utilizam o ransomware realizam para afetar os sistemas.A "Forma de distribuição" (iii) e "Indicadores de comprometimento" (v) fornecem as URL que distribuem os artefatos e as assinaturas dos artefatos que estão sendo utilizados.

O estagiário tinha como tarefa a criação do caso reunindo todas as informações que foram analisadas e levantadas durante o estudo do artefato, sendo ransomware ou *malware*.

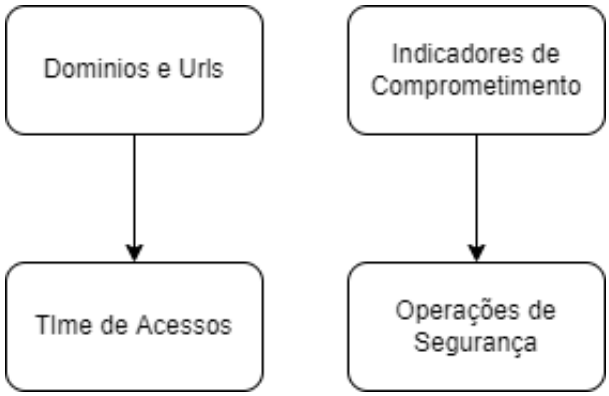
3.1.5 Direcionamento para Equipes Responsáveis.

O direcionamento para as equipes é a fase final da análise de *malware* e *ransomwares*. Após a criação do caso é feito o direcionamento para os times responsáveis. O Time de Acessos é responsável por realizar o bloqueio das URL que foram encontradas pelo time de inteligência. Na instituição, o bloqueio das URL consideradas suspeitas impede que qualquer máquina da instituição realize o acesso.

O Time de Operações de Segurança realiza o bloqueio de assinaturas de software que são considerados suspeitos ou maliciosos. Essas assinaturas são inseridas em softwares que realizam o escaneamento de todas as máquinas da instituição em busca de algum software malicioso.

Na Figura 3.10 é apresentado os dados que o time de inteligência envia aos times responsáveis após as análises.

Figura 3.10 – Direcionamento dos dados para os times responsáveis



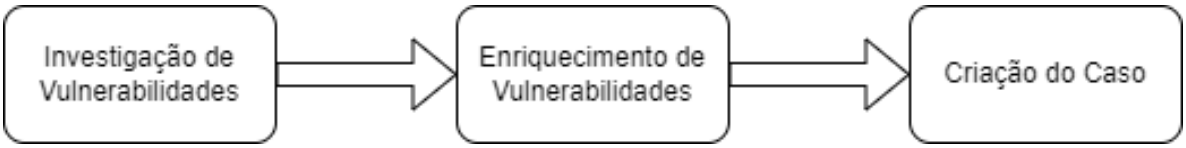
Fonte: Do Autor.

O estagiário era responsável por separar as informações que foram criadas no caso criado. Para o Time de Acesso são enviadas as URL juntamente com as evidências de reputação de cada URL que foi enviada. As informações que são enviadas para o time de operações de segurança devem conter a assinatura do artefato analisado. Se na criação do caso for identificado a família ou grupo malicioso que utiliza o *malware*ou *ransomware*, deve ser informado para que possa ser inserido nas ferramentas e criado uma correlação entre as informações já existentes.

3.2 Análise de Vulnerabilidades

O trabalho de análise de vulnerabilidades consiste na identificação, análise e documentação de vulnerabilidades que são encontradas em ferramentas ou sistemas. O fluxo de tarefas para o desenvolvimento deste trabalho é apresentado na Figura 3.11 As próximas subseções detalham cada tarefa.

Figura 3.11 – Fluxo de Trabalho Análise de Vulnerabilidades



Fonte: Do autor.

De forma similar ao que é praticado com a análise de práticas maliciosas, as vulnerabilidades são brechas em sistemas e ferramentas que permitem uma vasta gama de possibilidades para que um atacante. Vulnerabilidades são registradas em sites que identificam e as catalogam. São definidos padrões de nomenclatura para cada vulnerabilidade descoberta, onde são reconhecidas por todas as instituições. As vulnerabilidades são identificadas como "CVE" (*Commom Vulnerabilities Exposures*). Uma CVE é descrita com o ano e seu número de registro, por exemplo "*CVE-2022-36956*".

A atividade de "Investigação de Vulnerabilidades" consiste em analisar e investigar vulnerabilidades que possam afetar a instituição. Em seguida, a atividade de "Enriquecimento de Vulnerabilidades" consiste em pesquisar e agregar detalhes às vulnerabilidades encontradas. Finalmente, na atividade de "Criação do Caso" é criado um documento com as informações levantadas e direcionado para o time responsável.

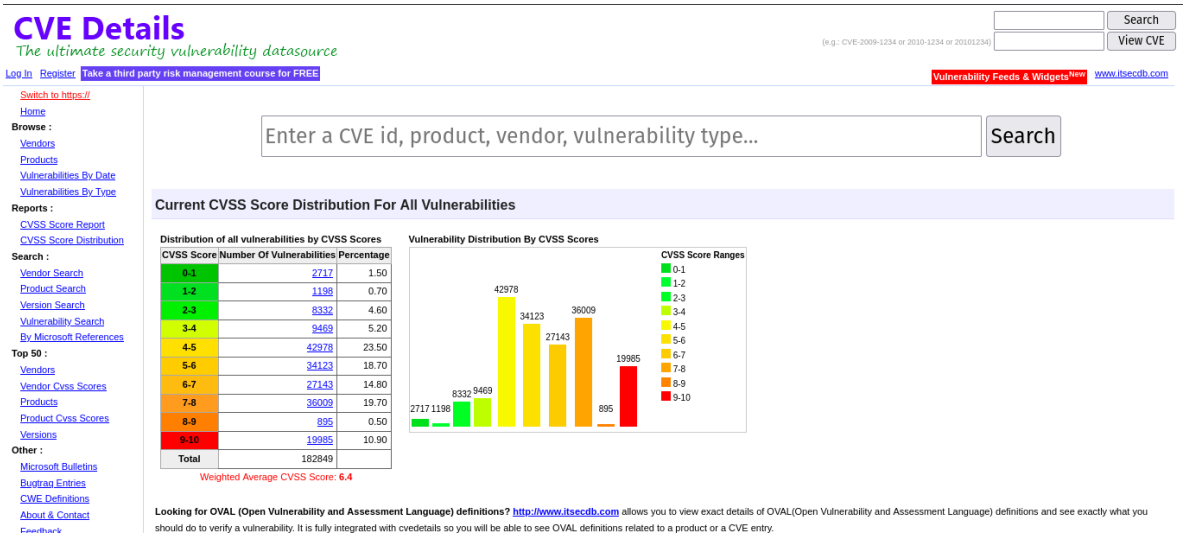
As subseções seguintes descrevem cada atividade desenvolvida em detalhes.

3.2.1 Investigação Vulnerabilidades

Diariamente, há sites que divulgam vulnerabilidades encontradas em sistemas ou softwares.Para que a instituição esteja sempre segura é necessário que todas as vulnerabilidades de risco sejam analisadas. A investigação de vulnerabilidades é iniciada pela coleta de informações em sites que publicam novas vulnerabilidades encontradas. Diferentemente da análise de sites em *malwares* ou *ransomwares*, a análise de vulnerabilidades verifica sites que são especializados. A informação é inserida no site apenas após a homologação.

Na instituição são utilizados sites especializados em vulnerabilidades. Os sites fornecem uma perspectiva inicial sobre as novas vulnerabilidades encontradas. Para a análise dentro da instituição um dos sites utilizados é o *cvedetails*. [11] Na figura 3.12 é apresentado a página inicial do site.

Figura 3.12 – Página inicial do site cvedetails



Fonte: www.cvedetails.com

O site fornece inicialmente uma perspectiva geral do número de vulnerabilidades encontradas categorizadas por nível de criticidade. Essa escala de criticidade é medida de zero a dez. Vulnerabilidades categorizadas do nível zero ao três, são apenas informativas. Entre os níveis quatro e seis, são vulnerabilidades de nível médio. Ao alcançar um nível sete ou superior, o nível de criticidade é considerado alto. Essas vulnerabilidades são consideradas críticas, sendo necessário atenção e mitigação imediata. Os níveis nove e dez, são consideradas vulnerabilidades *zero day*, onde o comprometimento do sistema é iminente.

A instituição utiliza o site para verificar vulnerabilidades que foram registradas. As vulnerabilidades registradas possuem informações que permitem uma análise prévia do serviço exposto. As submissões que são analisadas inicialmente são as consideradas de criticidade alta e *zero day*. Para uma primeira análise dos casos são coletadas informações consideradas relevantes pela instituição. O

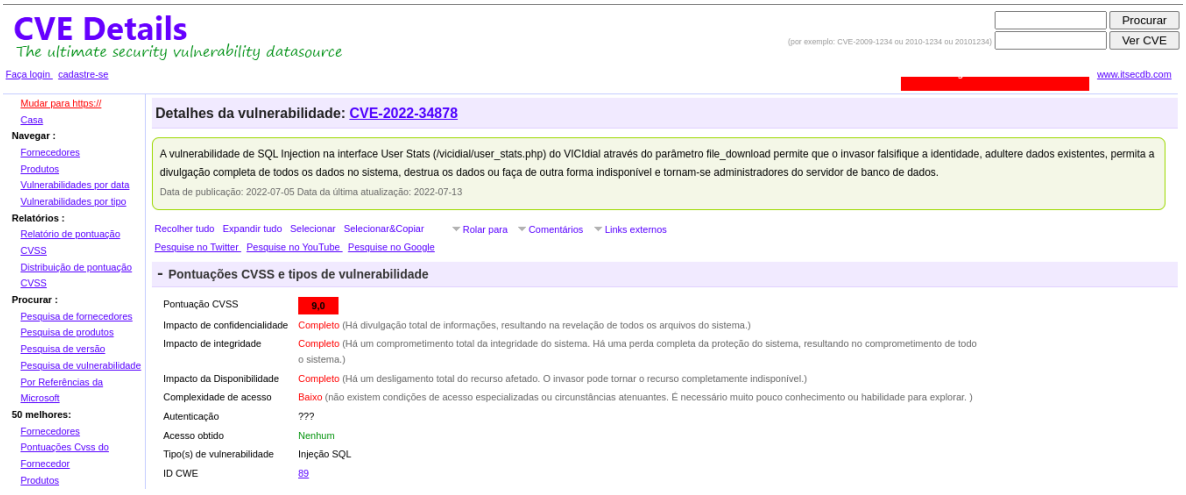
[11] www.cvedetails.com

site fornece uma visão geral acerca dos detalhes utilizados para o tratamento da vulnerabilidade. As informações coletadas são: Pontuação CVSS(i); Impacto de integridade(ii); Impacto de Confidencialidade(iii); Complexidade de Acesso(iv); Tipo de vulnerabilidade(v).

A “Pontuação CVSS”(i) é o sistema de pontuação de vulnerabilidade comum que é a métrica convencional utilizada para medir a criticidade de uma vulnerabilidade. O “Impacto de integridade”(ii) é a perda de proteção do sistema, resultando em perda total do sistema. De forma similar o “Impacto de integridade”(iii) informam se os arquivos do sistema podem ser acessados podendo gerar um vazamento de dados. A “Complexidade de acesso”(iv) informa o nível de dificuldade de exploração da vulnerabilidade, vulnerabilidades com baixo nível de complexidade permite que um maior número de atores maliciosos explorem a vulnerabilidade. O “Tipo de vulnerabilidade”(v) fornece quais serviços os sistemas afetados fornecem.

Na figura 3.13 é ilustrado os detalhes apresentados pela plataforma sobre uma vulnerabilidade.

Figura 3.13 – Informações fornecidas pelo site cvedetails

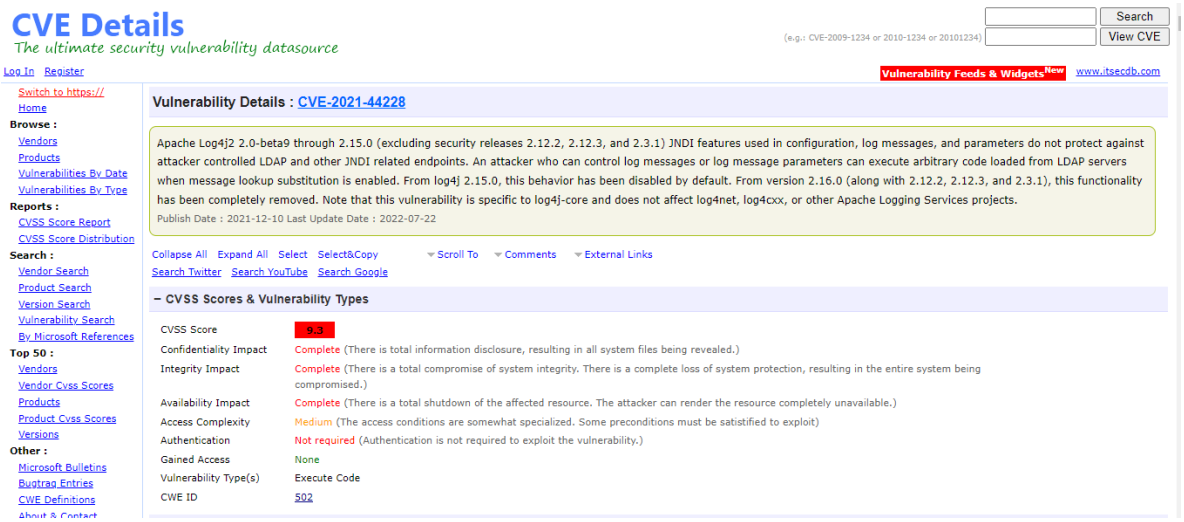


Fonte: www.cvedetails.com

O estagiário, durante o desenvolvimento da tarefa identificou uma vulnerabilidade que posteriormente foi categorizada como *zero day*. Foi feita a análise inicial da vulnerabilidade para a coleta de informações. Durante a análise foi identificado que a vulnerabilidade era de fácil replicação. Os im-

pactos de integridade e confidencialidade que a vulnerabilidade apresentava a definiu como prioridade. A imagem 3.14 apresenta as informações que foram identificadas.

Figura 3.14 – CVE-2021-44228 - Apache Log4j2



Fonte: www.cvedetails.com

3.2.2 Enriquecimento de Vulnerabilidades

Ao encerrar a atividade de investigação inicial da vulnerabilidade é necessário encontrar um enriquecimento das informações que foram identificadas. A tarefa realizada anteriormente apresenta apenas informações gerais sobre a vulnerabilidade. Para que a instituição possa verificar se a vulnerabilidade encontrada afeta sistemas internos é necessário a coleta de informações detalhadas. Informações estas que não são apresentadas nos sites analisados anteriormente. Uma análise completa da vulnerabilidade permite uma ação preventiva eficiente. São realizadas buscas sobre a vulnerabilidade com o intuito de identificar os sistemas afetados. A identificação dos sistemas afetados permite uma análise preventiva com o intuito de identificar se a instituição utiliza softwares vulneráveis. Para que as vulnerabilidades possam ser analisadas pelos times responsáveis são necessárias informações como:Forma de exploração (i); Versões dos Sistemas afetados (ii); Forma de mitigação (iii);

A “Forma de exploração” (i) permite entender como a vulnerabilidade é realizada e quais os indicadores identificam possíveis tentativas de exploração da vulnerabilidade. As “versões dos sis-

temas afetados" (ii) possibilita uma análise nos sistemas internos de forma a identificar se a versão utilizada pela instituição é afetada pela vulnerabilidade. Quando são identificadas vulnerabilidades com criticidades altas e *zero day*, os especialistas em segurança e até a empresa mantenedora do sistema disponibilizam formas de contenção e mitigação (iii). Estas formas de contenção e mitigação podem ser provisórias até a resolução, ou atualizações emergenciais. Ao obter as informações necessárias sobre a vulnerabilidade. O estagiário realizava o tratamento das informações para que os times necessários pudessem tratar posteriormente.

No caso identificado pelo estagiário referente a "CVE-2021-44228" 3.14, as informações necessárias foram obtidas em sites que que fornecem maiores detalhes sobre as vulnerabilidades. No site ThreatPost [12] foram realizadas investigações e análises sobre a vulnerabilidade. Na Figura 3.15 é ilustrado as informações apresentadas. Com a investigação realizada pelo site foi possível identificar os sistemas vulneráveis, juntamente com a forma de exploração e mitigação temporária da vulnerabilidade.

[12] www.threatpost.com

Figura 3.15 – ThreatPost Log4J

Fonte: www.threatpost.com

3.2.3 Criação do Caso

Ao fim de todo o processo de investigação e detalhamento da vulnerabilidade é iniciado a criação do caso. O caso reúne todas as informações que foram identificadas e analisadas sobre a vulnerabilidade. Para que seja possível realizar a prevenção da vulnerabilidade na instituição, o caso é enviado para os times responsáveis. O time responsável pelo tratamento da vulnerabilidade com o caso detalhado pode realizar as análises sem maiores problemas. A análise consiste em analisar a forma de exploração da vulnerabilidade nos sistemas que foram informados. Caso a vulnerabilidade atinja a instituição os dados das versões afetadas oferecem um panorama geral do número de máquinas vulneráveis. As formas de mitigação oferecem uma contenção preventiva dos sistemas afetados.

Na instituição, o time responsável pelo tratamento das vulnerabilidades é o time de segurança ofensiva. Com o caso podem realizar todos os testes da vulnerabilidade e também realizar a mitigação caso os sistemas sejam afetados. O estagiário, ao criar os casos com as informações da vulnerabilidade, direciona para o time de segurança ofensiva. O caso referente a vulnerabilidade encontrada pelo estagiário forneceu detalhes que permitiram a mitigação preventiva da vulnerabilidade.

3.3 Inteligência em Fontes Abertas

O trabalho de inteligência em fontes abertas consiste na utilização de ferramentas de código aberto, para auxiliar no desenvolvimento das tarefas internas e compartilhamento de informações pelo time de Inteligência. As fontes abertas de informações permitem que o time de inteligência consiga agregar maiores informações nas análises. Essas informações podem ser geradas por ferramentas de código aberto. Com informações que são compartilhadas por diversos especialistas de segurança, do mundo todo.

Um artefato ou vulnerabilidade pode ser totalmente analisado utilizando fontes abertas. Na instituição as fontes abertas são utilizadas de forma complementar, onde são verificados os dados obtidos na instituição com os compartilhados em fontes abertas. Desta forma então se obtém um novo ponto de vista.

Para o compartilhamento da informação na instituição é utilizado o MISP descrito na seção 3.3.1. São compartilhados os casos que são analisados internamente, juntamente com seus respectivos IOC. O estagiário ao finalizar a criação de casos de artefatos maliciosos e vulnerabilidades insere os dados obtidos juntamente com as etiquetas corretas. A subseção seguinte elucida a forma de utilização do MISP na instituição.

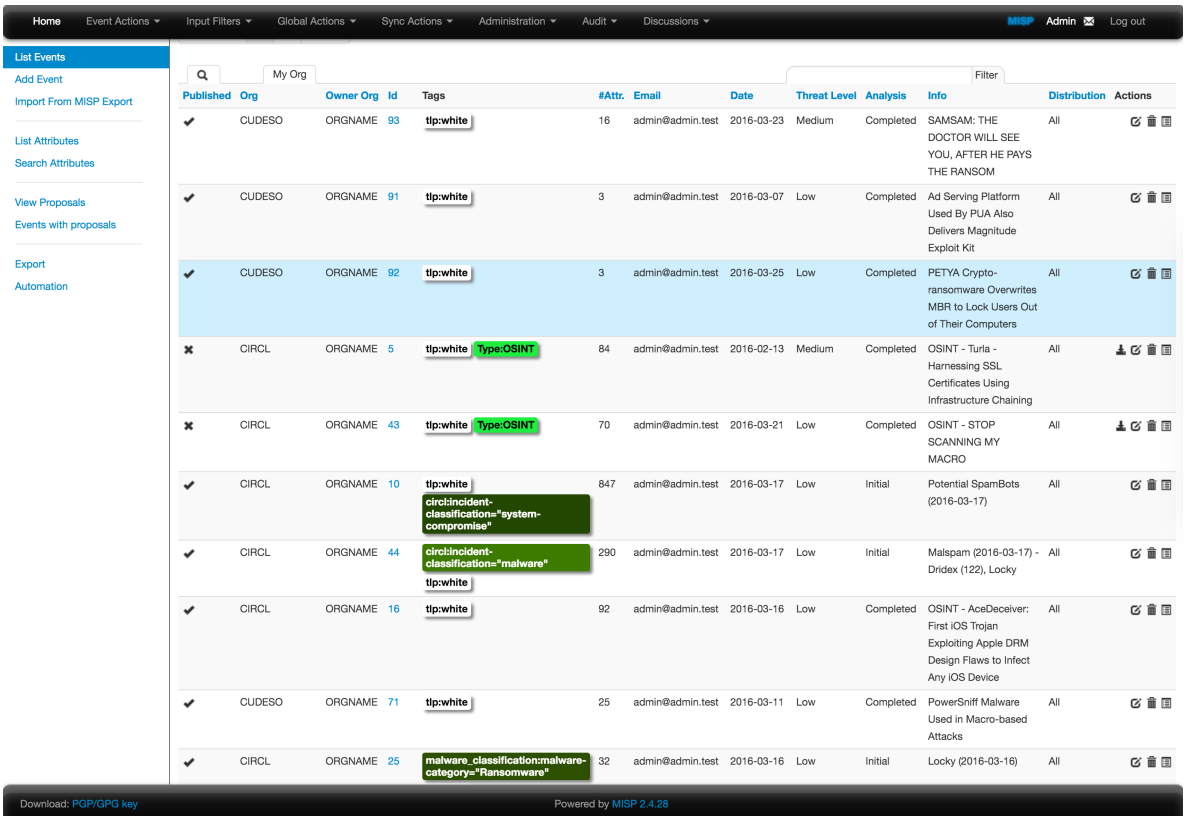
3.3.1 MISP

O MISP é uma ferramenta de compartilhamento de informações de segurança distribuída na forma de software livre. Na instituição, o MISP é utilizado para compartilhar , internamente e externamente, os casos que foram criados e analisados. Os casos que são compartilhados são: *Malwares*(i); *Ransomwares*(ii); Vulnerabilidades(iii); Proteção de Marca(iv);

Os “*Malwares*”(i) que são compartilhados na ferramenta, são os casos que foram criados anteriormente pelo time de inteligência, onde são inseridos principalmente os indicadores de comprometimento encontrados e as táticas utilizadas. Nos “*Ransomwares*”(ii) são compartilhados os casos identificados anteriormente pela instituição onde são inseridos na plataforma as URL e indicadores de comprometimento aos quais identificou-se os *ransomwares*. As “Vulnerabilidades”(iii) são casos criados pelo time de inteligência internamente, onde são compartilhados informações sobre as CVE que foram identificadas, as ferramentas que estão sendo exploradas e a forma de mitigação definida internamente. Por fim, a “Proteção de Marca”(iv) são URL ou domínios encontrados se passando pela instituição com o intuito de aplicar fraudes ou *phishings*. Os casos compartilhados no MISP, contém os domínios que foram encontrados e também sua reputação.

O estagiário era responsável por submeter os casos que foram analisados e criados dentro da instituição no MISP. Para consumir as informações que são publicadas por outras instituições, é utilizado um conjunto de ferramentas criadas pelo time de engenharia de dados, que fornece de forma completa e formatada para uso do time.

Figura 3.16 – Página inicial do MISP



Fonte: www.bridewellconsulting.com/misp-open-source-threat-intelligence-platform

Na figura 3.16 é ilustrado a página inicial do MISP, onde são apresentados os eventos compartilhados pelas instituições conectadas. “Evento” é a forma que a ferramenta intitula cada informação que é compartilhada. Cada evento apresentado possui informações da organização que compartilhou a informação. Os rótulos são definidos pela instituição que realizou a publicação do evento, como por exemplo definir como *malware* ou *ransomware*. O nome do evento possui um resumo de quais informações estão sendo compartilhadas. O número de atributos são as informações correlatas que a instituição possui sobre o evento.

Cada instituição segue um padrão próprio para publicar os eventos no MISP. Na instituição são utilizados rótulos que identificam qual o tipo de informação está sendo compartilhada, como por

exemplo, ransomware ou vulnerabilidade. O nome do evento é definido pelo tipo do evento e o nome dado pelos especialistas, como por exemplo “Ransomwmare RedAlert”.

3.4 Considerações Finais

Este capítulo apresentou os processos de trabalho referentes à inteligência de ameaças aos quais o estagiário atuou na instituição financeira. Todos os processos que são realizados na instituição possuem processos bem definidos, o que permite que tanto a análise de artefatos, quanto a análise de vulnerabilidades possa ser feito de forma eficiente. Os processos definidos permitiram que o processo de aprendizado fosse facilitado. Por ser uma área da segurança contida em um contexto específico possui muitos desafios. Analisar artefatos e vulnerabilidades que não possuem muitas informações apresenta um grande desafio, pois é necessário uma análise precisa e dados que permitam identificar e proteger os sistemas da instituição.

A utilização de ferramentas criadas com o software livre apresentou novos conceitos que se projetaram como desafios, pois não possui uma equipe de suporte que possa auxiliar em problemas decorrentes. Desta forma todos os problemas que são identificados na ferramenta é necessário correção interna, ou recorrer a comunidade mantenedora do projeto.

Foi um processo de aprendizagem intenso e interessante. Além de todo o conteúdo teórico que foi aprendido durante a graduação. Houve demanda de um estudo adicional em processos e ferramentas de segurança. Para que as tarefas pudessem ser desempenhadas com qualidade e excelência. O principal desafio durante o estágio foi a aplicação dos conceitos aprendidos na inteligência de ameaças em prática.

4 CONCLUSÃO

Este relatório de estágio descreveu as atividades desenvolvidas pelo autor durante estágio supervisionado realizado em uma instituição financeira. As atividades desenvolvidas concentraram-se na área de segurança de ameaças, e foram realizadas no período de outubro/2021 à junho/2022. O estágio desenvolvido permitiu a aplicação dos conhecimentos acadêmicos no mercado de trabalho. As principais experiências adquiridas durante o processo foram as seguintes:

- Durante a análise de *Malwares* e *Ransomwares*, permitiu-se o conhecimento de procedimentos e ferramentas necessárias para o desenvolvimento da atividade dentro de uma instituição financeira.
- Com o desenvolvimento dos trabalhos de segurança foi possível direcionar os estudos teóricos de forma a complementar os estudos acadêmicos.
- As tarefas de análise, seja de artefatos ou vulnerabilidades, permitiram que o estagiário desenvolvesse um senso crítico, onde o estagiário é capaz de questionar e analisar de forma inteligente situações.
- As tarefas de enriquecimento proporcionaram o desenvolvimento de habilidades de pesquisa e análise de informações em ferramentas de segurança.
- A criação dos casos permitiu entender e desenvolver habilidades sobre redigir documentos de segurança.

Durante o desenvolvimento do estágio, a formação acadêmica proporcionou fundamentos teóricos que permitiram que o estagiário desempenhasse as tarefas sem muitas dificuldades. As disciplinas “Redes de Computadores” e “Algoritmos em Grafos” forneceram os fundamentos necessários para entender quais os dados eram analisados, como são obtidos e a forma que a correlação era realizada.

A instituição por sua vez proporcionou um novo ponto de vista para o estagiário em relação aos conhecimentos teóricos que foram aprendidos. Desta forma foi possível fixar os conceitos de forma mais efetiva.

REFERÊNCIAS

ABU MD SAHROM; SELAMAT, S. R. A. A. Y. R. **Cyber Threat Intelligence – Issue and Challenges**. Malaysia: Indonesian Journal of Electrical Engineering and Computer Science, 2018. Disponível em: <https://www.researchgate.net/publication/322939485_Cyber_Threat_Intelligence_-_Issue_and_Challenges/download>. Acesso em: 12 ago. 2022.

ALIENVAULT. **Alienvault**. ATT Alien Labs, 2022. Disponível em: <https://otx.alienvault.com/faq>.

ALVES, G. A. **Segurança da Informação: uma visão inovadora da gestão**. 1. ed. Rio de Janeiro: Ciência Moderna Ldta, 2006.

CANI ANDREA; GAUDESI, M. S. E. S. G. T. A. Towards automated malware creation: Code generation and code integration. **SAC 2014: Symposium on Applied Computing**, I, n. 1, p. 157–160, 2014. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/2554850.2555157?casa_token=yXpBZ53nXWYAAAAA:UC-E37UB0p6ndWeNnr6gui_mc4Pqkg5QaEa0WRgHsiu9eXG3vEqUk1Gec9xMHs2sS3Zm1HeEXzQ9>. Acesso em: 19 ago. 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANçA NO BRASIL. **Misp CertBR**. São Paulo, 2022. Disponível em: <https://cert.br/misp/>. Acesso em: 20 ago. 2022.

CROWDSTRIKE. **Threat Intelligence**. CrowdStrike, 2022. Disponível em: <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>. Acesso em: 10 ago. 2022.

DUNHAM KEN;LUCAS, C. **TTPs Within Cyber Threat Intelligence**. Optiv, 2017. Disponível em: <https://www.optiv.com/explore-optiv-insights/blog/tactics-techniques-and-procedures-ttps-within-cyber-threat-intelligence>. Acesso em: 10 ago. 2022.

E-VAL, T. **O setor financeiro está sob ataques cibernéticos: bancos, Fintechs e Pix em risco**. E-VAL Tecnologia, 2022. Disponível em: <https://www.evaltec.com.br/o-setor-financeiro-esta-sob-ataques-ciberneticos-bancos-fintechs-e-pix-em-risco/>.

FEBRABAN. **Segurança da informação é prioridade para o setor financeiro**. Federação Brasileira dos Bancos, 2022. Disponível em: <https://noomis.febraban.org.br/temas/seguranca/seguranca-da-informacao-e-prioridade-para-o-setor-financeiro>.

GARTNER, G. **How Gartner Defines Threat Intelligence**. Gartner Research, 2016. Disponível em: <https://www.gartner.com/en/documents/3222217>.

GILGER, J. **urlscan**. urlscan, 2022. Disponível em: <https://urlscan.io/>.

GOV, C. **Indicadores de Comprometimento**. CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, 2022. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/noticias/2021/indicadores-de-comprometimento>.

JUNIOR, J. A. d. A. **Identificação de Competências dos Cyber Red Teams Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética**. Universidade Federal de Brasilia: Malware Information Sharing Platform, 2020. Disponível em: <https://repositorio.unb.br/bitstream/10482/40003/1/2020_Jos%C3%A9AugustodeAlmeidaJunior.pdf>. Acesso em: 12 ago. 2022.

KASPERSKY. **O que é inteligência de ameaças? Definição e explicação**. Kaspersky, 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/threat-intelligence>. Acesso em: 28 ago. 2022.

MISP. **MISP**. Malware Information Sharing Platform, 2022. Disponível em: <https://www.misp-project.org/>. Acesso em: 10 ago. 2022.

ROLFINI, F. **Cibercrime: ataques no Brasil aumentam mais de 300pandemia**. Olhar Digital, 2022. Disponível em: <https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/>.

SEGURANçA DA INFORMAçãO. **Norma ISO/IEC 17799:2000**: Disponivel em http://www.informabr.com.br/nbr.htm acesso em 09 ago. 2022. Rio de Janeiro, 2000. 22 p.

SOCRADAR. **5 Stages of The Threat Intelligence Lifecycle**. Socradar, 2022. Disponível em: <https://socradar.io/5-stages-of-the-threat-intelligence-lifecycle/>. Acesso em: 28 ago. 2022.

SÊMOLA, M. **Gestão de segurança da informação: Uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier Editora Ltda, 2014.

TOTAL, V. **VirusTotal**. Chronicle Security, 2022. Disponível em: <https://www.virustotal.com/gui/home/upload>.

TRENDMICRO. **Definition of Ransomware**. TrendMicro, 2022. Disponível em: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>.

YEBOAH-OFORI ABEL;ISLAM, S. **Cyber Security Threat Modeling for Supply Chain Organizational Environments**. Future Internet, 2018. Disponível em: <https://www.researchgate.net/publication/331540145_Cyber_Security_Threat_Modeling_for_Supply_Chain_Organizational_Environments>. Acesso em: 10 ago. 2022.