PROPOSTA DE UMA SOLUÇÃO PARA O MONITORAMENTO DE PROCESSOS E IDENTIFICAÇÃO DE SOFTWARES MALICIOSOS

(Autores e Afiliações)
Marcelo Marchioro Cordeiro, discente de graduação, Universidade Federal do Pampa, Campus Bagé
Mateus Oliva Soares, discente de graduação, Universidade Federal do Pampa, Campus Bagé

Erico Marcelo Hoff do Amaral, docente, Universidade Federal do Pampa

e-mail primeiro autor- marcelocordeiro.aluno@unipampa.edu.com.br

Malwares, são softwares responsáveis por um elevado número de incidentes em empresas, universidades, hospitais, sistemas governamentais, sistemas de uso pessoal entre outros ambientes, ele trata-se de qualquer tipo de software desenvolvido intencionalmente para fins maliciosos, que executa ações dessa natureza sem o conhecimento do usuário. Nos últimos anos houve um aumento no registro de incidentes ocasionado por software malicioso, isso se decorre por diversos fatores, como por exemplo a pandemia de COVID-19 que forçou muitas empresas a se adaptarem, de forma abrupta, a modalidade de trabalho home office. Essa obrigação exigiu que todo o processo fosse executado da forma mais rápida possível causando assim o surgimento de vários sistemas vulneráveis que puderam ser explorados para se realizar todos os tipos de ataques cibernéticos, principalmente um tipo de programa mal-intencionado, o ransomware, que podem ser bastante lucrativos para os delinquentes. Com base nestes incidentes, relacionados a programas maliciosos é possível reconhecer uma grande demanda por ferramentas que auxiliem na defesa dos sistemas buscando bloquear ou diminuir os danos pelas ações desses softwares. Este trabalho tem como objetivo propor e implementar uma ferramenta que seja capaz de realizar ações que possibilitam mitigar a ação de malwares através de monitoramento de processos, chamadas de sistemas, uso de recursos de hardware e comportamentos suspeitos em computadores pessoais. Com base nesses objetivos iniciou-se a pesquisa, com a classificação da metodologia científica adotada um estudo dedutivo onde busca-se entender o problema geral da área de segurança da informação e de sistemas para assim chegar no entendimento do problema final que este trabalho busca propor uma alternativa de solução que na questão desse projeto são os malwares. A abordagem do problema adotada foi a quali-quantitativa que se usa de estratégias qualitativas e quantitativas, pois é preciso se basear em uma quantidade grande de dados que já existem, mas também precisa explorar uma vertente nova de pesquisa pois os malwares estão inovando e trazendo novidades de uma forma bastante acelerada. A base dos objetivos utilizada foi a exploratória pois busca-se entender o problema e a solução através de estudo de casos já existentes e com base em bibliografias sobre o assunto. Logo os procedimentos técnicos são norteados pela base dos objetivos, por tanto trata-se de pesquisas bibliográficas e estudos de casos. Logo em seguida foi realizado um levantamento bibliográfico e definição de uma arquitetura para a solução proposta, seguindo da sua modelagem. Tendo essas etapas concluídas foi possível estudar as tecnologias viáveis para a implementação do protótipo da ferramenta e escolher a que melhor atende as necessidades. Na sequência do estudo de tecnologias viáveis deu-se preferência para o uso da linguagem de programação python 3 pois atende todas as necessidades do projeto e apresenta um bom desempenho, também é uma

plataforma de desenvolvimento limpa, poderosa e orientada a objetos. O Python possuí um conjunto de bibliotecas e frameworks com funcionalidades implementadas, caracterizando-se como um recurso eficiente para o desenvolvimento da arquitetura proposta. Uma dessas bibliotecas que foi usada no projeto foi a process and system utilities, ela é gratuita e de livre uso e nos disponibiliza funções que permitem realizar o monitoramento detalhada de diversos recursos de hardware e dos processos que estão rodando em uma máquina tornando esse processo menos complexo de implementar e já sendo otimizada e consumindo pouco recurso computacional, em complemento a isso foi adotado a framework PyQt devido a mesma disponibiliza diversos módulos que combinado com a biblioteca pyside nos permite criar um designer moderno e responsivo para aplicação. A partir do reconhecimento das tecnologias para o desenvolvimento, implementou-se um projeto piloto para monitorar e avaliar processos ativos e componentes de hardware em um sistema operacional Windows. Concluiu-se preliminarmente a viabilidade de monitorar componentes de hardware sendo assim possível utilizar essas métricas como parâmetro para auxiliar na detecção de processos suspeitos. Visto este ser um estudo em andamento, pretende-se, como trabalhos futuros, implementar as funcionalidades essenciais para mitigar as ações de um malware, testar a solução desenvolvida, avalia sua execução em questão de assertividade e consumo de recursos do sistema e validar se a solução de fato cumpre os objetivos.

Palavras-chave: Malware, Segurança da informação, Monitoramento de processos, Segurança de sistemas.