Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

Sistema de Auto-Reposição de ficheiros / Anti-Ransomware

Sistemas Distribuídos

Pedro Rosa

Link do github: https://github.com/luissilva60/SistemasDistribuidos

Autores:

Ricardo Abrantes Nº20201033 M01

Luís Silva Nº20200606 M01

Pedro Santos Nº20200942 M01

Salvador Marchante Nº20200239 M01

22 de setembro de 2022, Lisboa.

Introdução

O Ransomware é algo bastante comum hoje em dia, o que nos leva a aumentar a segurança de ficheiros que possam ser alvos do mesmo, então decidimos implementar um sistema de auto-reposição de ficheiros de forma a combater o Ransomware. Uma modificação não autorizada de um sistema de ficheiros é algo que se deseja evitar, seja devido a ataques de Ransomware ou outra causa. O que se pretende é criar um sistema que detecte alterações não autorizadas de ficheiros armazenados e os reponha, caso se detete que foram acessos não autorizados. Tanto para as empresas como para os utilizadores privados, ransomware é uma ameaça bastante significativa, daí querermos criar este sistema para reduzir a presença desta ameaça.

Solução

Como solução para este problema, teremos primeiramente que fazer cópias de todos os ficheiros para que o sistema tenha um backup caso seja roubado ou editado. O sistema irá comparar as duas cópias do ficheiro e se forem diferentes irão ser implementadas as medidas de segurança.

Enquadramento

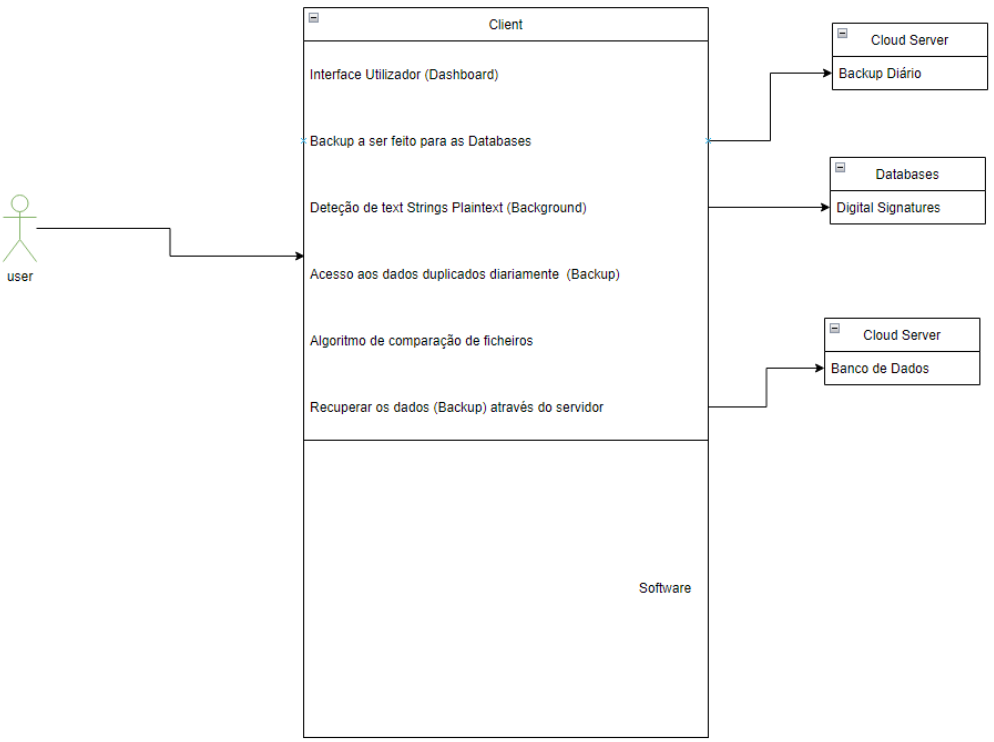
Primeiramente, é extremamente necessário ter este sistema de forma distribuída, pois caso um sistema falhe o outro já está lá para que este sistema não deixe de operar. Segundamente, qualquer processo, computador ou rede pode falhar, independentemente dos outros. Portanto, cada componente precisa de conhecer as maneiras possíveis que os componentes de que dependem podem falhar e ser projetado de forma a tratar cada uma dessas falhas apropriadamente. Terceiramente, a presença de múltiplos usuários num sistema distribuído é uma fonte de pedidos concorrentes para os seus recursos. Em ambiente competitivo, cada recurso deve ser projetado para manter a consistência nos estados de seus dados.

Requisitos Técnicos

Para os requisitos técnicos do nosso sistema de anti-ransomware, teremos inicialmente de ter informação sobre os ficheiros na base de dados. Depois o objetivo seria sempre que são detectadas mudanças não autorizadas nos ficheiros, o sistema deveria repor os ficheiros para exatamente como estavam antes, através dum modelo tolerante a faltas. Faremos isto através de uma web app com html, css e javascript, e utilizando postgresql para construir a base de dados.

Arquitetura do Sistema

Para que o sistema seja tolerante a faltas, precisamos de ter duas (ou mais) bases de dados sincronizadas, cada uma delas ligada a dois (ou mais) servidores, que estarão ligados a dois (ou mais) clientes que estariam conectados a uma reverse proxy (tendo esta também uma segunda via, para o caso da principal falhar).



A maior parte dos ataques ransomware vêm de email ou mensagens spam que contêm links URL ou ficheiros anexados maliciosos. Quando o utilizador carrega no link ou abre o ficheiro, o vírus executa um ficheiro que rapidamente encripta documentos e faz com que estes sejam inutilizados.

Ao prevenir os utilizadores de aceder a estes links URL e ficheiros, a tecnologia anti-ransomware consegue prevenir a maior parte destes ataques. Mas como os ataques estão constantemente a evoluir isto pode ser um enorme desafio para cada ameaça de ransomware que surja. É por isso que a tecnologia anti-ransomware também deve fornecer soluções para minimizar o impacto que cada um destes ataques faz quando bem sucedidos.

Planeamento

Inicialmente iremos tentar compreender melhor como funciona a deteção de ransomware. Segundamente, o sistema irá fazer uma backup diária automática dos ficheiros do cliente. Depois vamos proceder à realização de alguns experimentos de modo a desenvolver um algoritmo que atue consoante a deteção e que passos irá seguir. Em seguida, iremos avançar para a parte em que é preciso importar dados da nuvem, pois os dados haviam sido comprometidos e encontram-se encriptados. Por último, esse backup irá ser substituído pelos dados comprometidos.

Contudo, iremos construir uma Web App (Dashboard) e iremos implementar estas funcionalidades descritas e todos os requisitos necessários e úteis, tais como o servidor de backup e o algoritmo de comparação de ficheiros.

Bibliografia

Crowdstrike (2022). 21 Março, 2022
Disponível em
https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-detection/

Delinea (2021). 2021
Disponível em https://delinea.com/blog/ransomware-mitigation