**Projeto 3**

Universidade de Aveiro

Departamento de Eletrónica, Telecomunicações e Informática

Segurança Informática nas Organizações



Equipa 32

Bruno Silva - 97931

Marta Oliveira - 97613

Miguel Ferreira - 93419

Pedro Coutinho - 93278

**Sumário Executivo**

Após uma deteção de uma alteração pouco usual na *virtual machine* do nosso cliente houve uma investigação detalhada da *VM* para perceber o que sucedeu. Conseguimos averiguar que foi vítima de um ataque informático.

A seguir apresentaremos um resumo dos principais aspetos do mesmo.

**Resumo:**

**Dados e análise:**

**Conclusão:**

**Relatório do ataque**

**Acesso Inicial: Como?**

O atacante aproveitou-se de serviços remotos externos para conseguir aceder e persistir na rede da vítima. Ele utilizou a interface do *Docker* onde não é requerida autenticação.

Neste tipo de ambiente, conseguiu aceder a *logs* para ganhar credenciais e executar comandos (scripts) dentro de contêiners para obter poder de execução remota.

**Brute force**

**DDOS**