

Command and Control

João Marques, Maria Martins,
Mário Nascimento e Rebeca
Sampaio

Índice:

01

...

Descrição do Problema

02

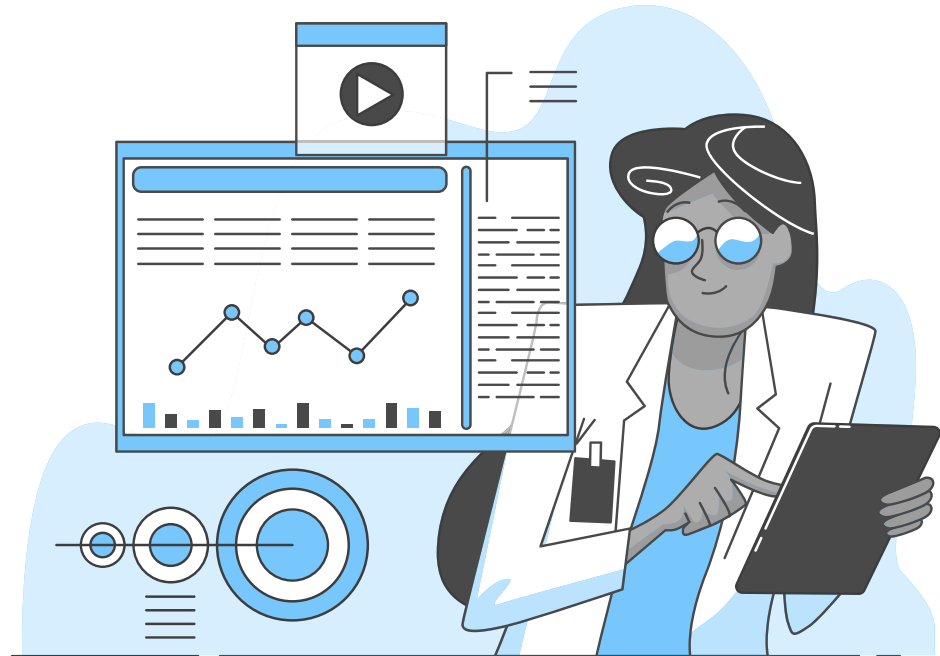
...

Descrição da Solução

03

...


Gráfico de Gantt

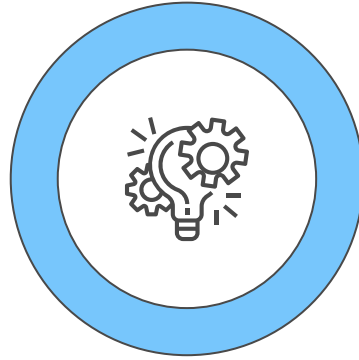




01

Descrição do Problema





C2

Através deste sistema, é possível gerir de forma eficaz um vasto número de máquinas comprometidas, potencializando a realização de testes de penetração mais eficientes, ao melhorar significativamente a comunicação e a coordenação entre os operadores e os sistemas alvo.

...

Casos de Uso



Teste de Penetração

Gera um relatório de segurança

...



Formação em Cibersegurança

Treinar especialistas em segurança

...

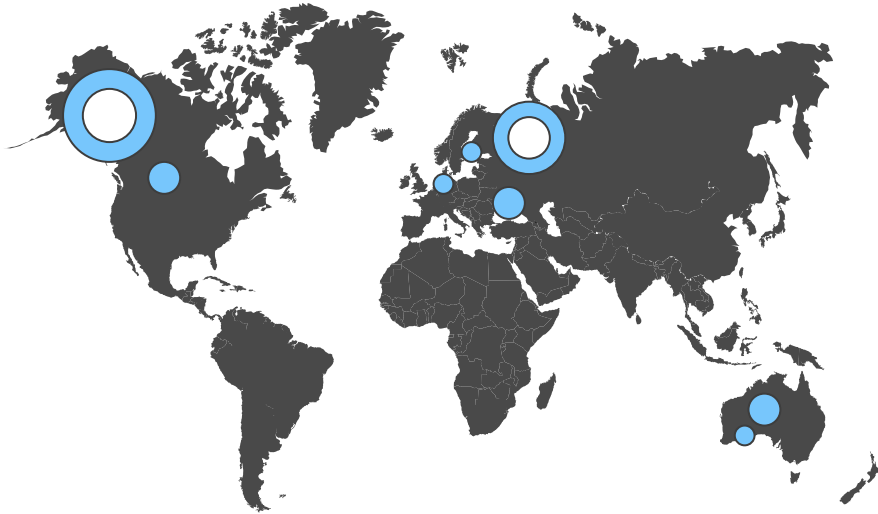
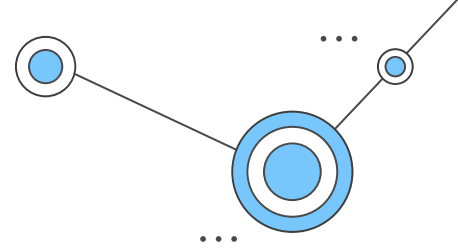


Investigação de Cibersegurança

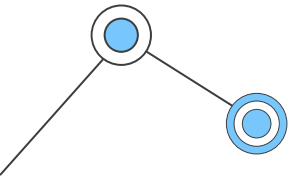
Permite o foco em áreas importantes

...

C2

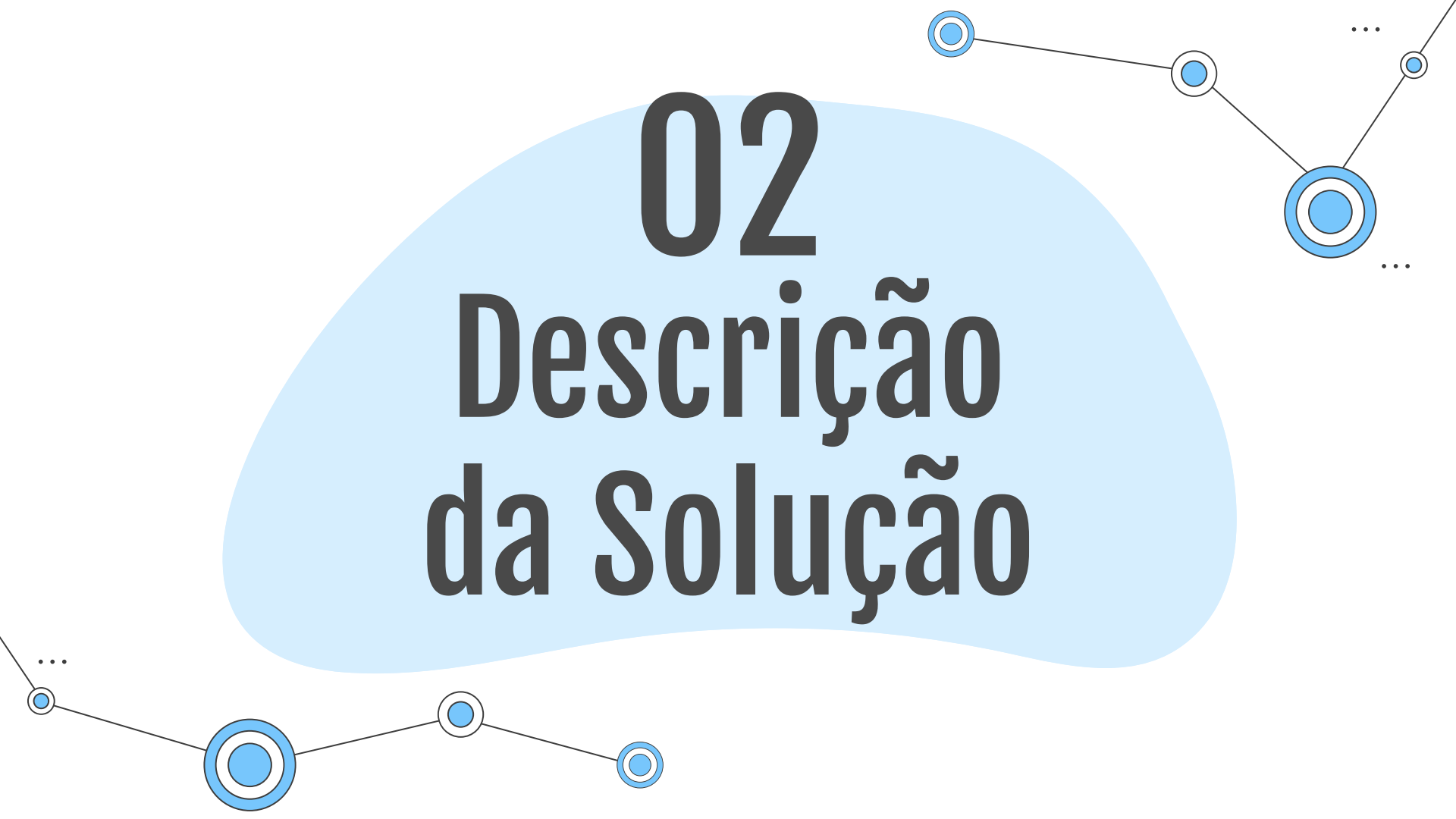


Os operadores podem conectar-se todos ao servidor, independentemente da sua localização, para interagir e controlar máquinas.



02

Descrição da Solução



Descrição genérica da solução

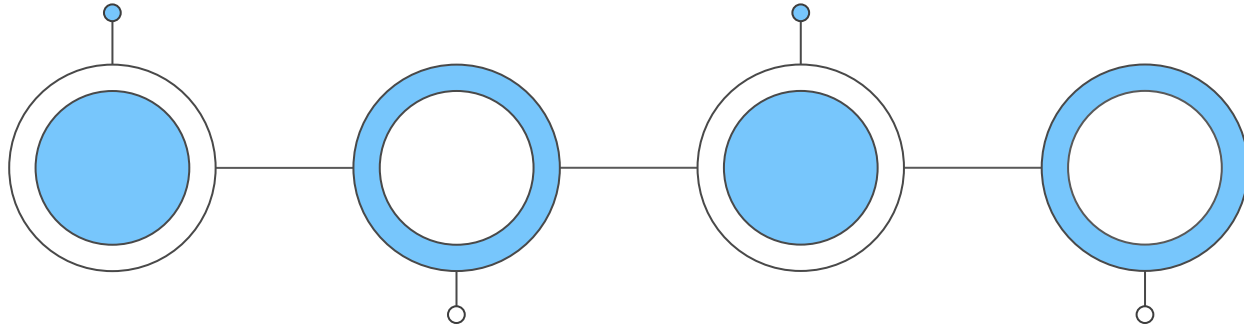
A arquitetura do sistema baseia-se na integração de um servidor C2, a sua interface para os atacantes e beacons, promovendo uma comunicação bidirecional. Os beacons, uma vez implementados nos sistemas comprometidos, estabelecem um canal de comunicação contínuo com o servidor C2, ficando à espera de instruções.

...

Enquadramento nas UC's – Sistemas Operativos

Gestão de processos e
threads

Gestão de recursos



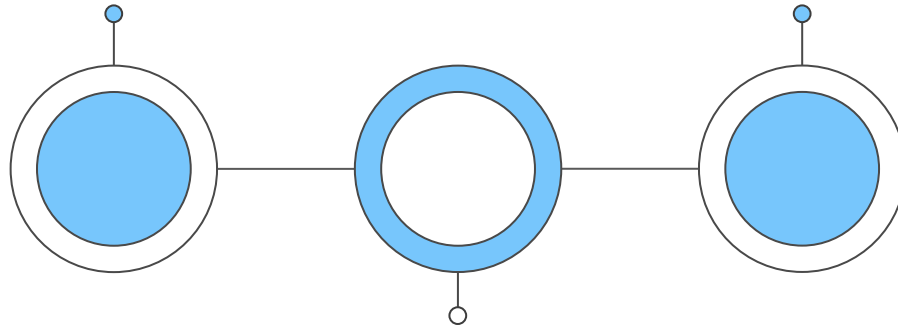
Comunicação IPC

Segurança e isolamento

Enquadramento nas UC's – Compiladores

Criação de código

Análise Léxica e Sintática



Optimização de código

Requisitos Técnicos



Python



C e Assembly



Conhecimento em
Redes e Protocolos
de Comunicação

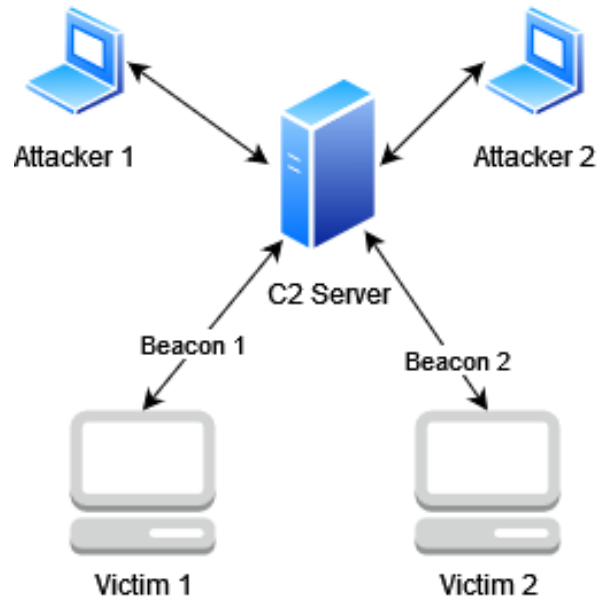


Criptografia

Requisitos

id	Descrição	Categoria
RF1	Comunicação bidirecional entre beacon e C2	Must have
RF2	Interface shell personalizada	Must have
RF3	Controlo individual e de grupo sobre as máquinas	Must have
RF4	Deteção de ambientes virtualizados e de teste	Must have
RF5	Criação de um relatório de estado de segurança da maquina	Must have
RF6	Modulos customizados, permitindo keylogging, exfiltração de dados	Must have
RF7	Comunicação bidirecional entre cliente e C2	Should have
RF8	Criação de interface de texto	Should have
RF9	Capacidade de interpretar código personalizado como payloads	Should have
RF10	Modulos de ransomware e enumeração	Should have
RF11	Movimento lateral	Nice to have
RF12	Escalamento de privilégios	Nice to have
RF13	Mecanismos contra reverse-engineering	Nice to have
RF14	Interpretador de linguagem de programação personalizada	Nice to have
RF15	Comunicação segura com RSA + AES256	Nice to have
RF16	Integração com plataformas de segurança	Nice to have

Arquitetura



Tecnologías a utilizar



VSCode



Git



SSL/TLS



OpenSSL

03

Gráfico de Gantt



**Obrigada pela
atenção!**

