Byte RAT
04/28/25

Made by:
Apophenia;
Ace;
Horus;
Kurt;

Byte RAT é um sistema de acesso remoto (RAT) desenvolvido pesquisas em segurança cibernética. Projetado para operar em ambientes Windows, o Byte RAT utiliza um bot no Discord como servidor de comando e controle (C2), oferecendo uma abordagem discreta e moderna para a administração remota.

O objetivo principal do Byte RAT é fornecer controle completo sobre máquinas remotas, permitindo a execução de comandos, transferência de arquivos, captura de informações sensíveis e ações de manipulação do sistema, sempre priorizando a estabilidade e o stealth durante a operação.

A arquitetura do projeto separa claramente o cliente (vítima) e o servidor (bot Discord), garantindo escalabilidade, segurança e organização de código, permitindo que cada módulo de funcionalidade seja desenvolvido, mantido e atualizado de forma independente.

ROADMAP SIMPLIFICADO DE FASES DO PROJETO

Não estão listadas todas as funções, porém é obvio em qual tópico elas devem se encaixar na prioridade.

Fase 1: Estrutura base do Byte RAT

1 - Criar o bot do discord

- Bot funcional que conecta no servidor.

2 - Sistema de autenticação

- Verificar ID de quem pode controlar o bot.

3 - Cliente básico Windows

- Um .exe que se conecta com o bot.

4 - Sistema de comandos

- Criar uma base **sólida** para receber comandos.

Fase 2: Comandos Essenciais

1 - CMD

- Executar um comando no cmd que ira retornar uma saida no bot do discord.

2 - Upload

- Enviar arquivos do discord para máquina da vítima.

3 - Download

- Baixar arquivo da máquina vítima.

4 - Screenshot

- Capturar tela e enviar imagem.

5 - SystemInfo

- Capturar informações básicas do sistema (OS, IP, CPU, RAM, ETC).

6 - MessageBox

- Mostrar uma mensagem na tela da vítima.

Fase 3: Funções de coleta (stealer)

1 - Wifipass

- Capturar senhas de wifi salvas.

2 - Browserpass

- Capturar senhas salvas em navegadores (chrome, edge, brave, etc).

3 - Listprocess

- Listar processos que estão rodando no computador da vítima.

4 - Killprocess

- Matar processo em execução.

5 - Keylogger

- Capturar teclas pressionadas de tempo em tempo.

Fase 4: Funções Troll / Destruição

1 - Blackout

- Tela preta.

2 - Tela azul

- Simula uma tela azul.

3 - Speak

- Falar usando TTS (Text to speech).

4 - Deletefile

- Apagar arquivos específicos.

5 - Openurl

- Abrir url no navegador.

Fase 4: Estabilidade e stealth

1 - Stealth mode

- Ocultar janelas (por exemplo não abrir CMD visível).

2 - Anti Erro

- Prevenir que erros ou falhas desconectem o cliente.

3 - Reconexão

- Se cair tenta reconectar o bot.