A modificação do jogo analisada, disponível em TerjeBruoygard/TerjeMods, segue o modelo de desenvolvimento imposto pela Bohemia Interactive e utiliza a linguagem Enforce Script, disponibilizada pela mantenedora do motor do jogo. O mod tem como objetivo permitir que membros de um mesmo grupo visualizem uns aos outros na interface do jogo e no mapa, por meio da exibição de marcadores visuais.

Contexto e Funcionamento

A modificação analisada é o **Terje Party Mod** para o jogo DayZ, cuja finalidade é permitir a formação de grupos (*partys*) entre jogadores dentro do ambiente do jogo. O mecanismo de funcionamento observado segue o seguinte fluxo:

- Jogador **A** interage (tecla **F**) com o Jogador **B**, enviando um convite de party;
- Jogador **B** interage (tecla **F**) com o Jogador **A**, aceitando o convite;
- A party é criada e os jogadores passam a se visualizar mutuamente por meio de marcadores na interface e no mapa.

Observação de Comportamento Anômalo

Durante testes empíricos, foi identificado um comportamento inconsistente após a **formatação completa do computador**, com remoção de todas as pastas e dados locais. Na situação observada:

- O jogador analisado **não visualizava mais a party**, como se não estivesse em grupo;
- Um outro jogador ainda **visualizava o primeiro jogador como membro da party**;
- Não houve qualquer ação explícita de remoção de grupo por parte do servidor.

Essa assimetria levou à hipótese inicial de que **as informações de party não são integralmente armazenadas ou validadas no servidor**, mas dependem de dados persistidos localmente no cliente.

Investigação Técnica

Monitoramento de Arquivos

Foi realizado o monitoramento do processo do DayZ durante a criação de uma party, utilizando ferramentas de observação de sistema (Microsoft Task Manager / Monitor de Recursos / Process Explorer), com o objetivo de identificar acessos a arquivos locais relevantes.

Como resultado, foi identificado o acesso recorrente ao arquivo:

`TerjeParty.dat`

Esse arquivo era aberto e modificado no momento da criação ou atualização de uma party.

Análise do Arquivo

O arquivo `TerjeParty.dat` foi analisado por meio de um **editor hexadecimal**, sendo observada uma estrutura binária consistente após a formação de uma party, indicando armazenamento de dados de configuração local.

Estrutura do Arquivo

O formato do arquivo segue um layout determinístico:

- **Cabeçalho inicial (4 bytes, int32, little-endian):**
  - Representa a quantidade total de GUIDs armazenados no arquivo.
- **Entradas sequenciais por GUID:**
  - 4 bytes (int32, little-endian) indicando o tamanho **N** da string do GUID;
  - **N bytes** contendo o GUID em formato **UTF-8**, sem terminador adicional.

Cada GUID representa um identificador de jogador e é armazenado como uma **string Base64 (URL-safe)**, e não como um valor binário fixo.

O comportamento de escrita observado consiste na simples **adição de novas entradas ao final do arquivo**, sendo necessário apenas atualizar o contador inicial de GUIDs para manter a consistência do formato.

Propriedades Observáveis

- O layout do arquivo é **simples, sequencial e determinístico**, facilitando o parsing manual;
- A estrutura baseada em `[contagem → tamanho → string]` permite **inserções e modificações diretas**, desde que o cabeçalho seja ajustado;
- Os dados são armazenados localmente em formato legível (Base64), **sem criptografia ou validação de integridade** embutida no próprio arquivo.

Essas características explicam tanto o desaparecimento de partys após a exclusão de dados locais quanto a possibilidade de recriação manual das mesmas.

Exploração da Estrutura

Durante a análise, foi possível identificar dentro do `TerjeParty.dat`:

- O número total de IDs armazenados;
- A lista completa de GUIDs correspondentes aos membros da party.

Foi identificado que o GUID utilizado pelo DayZ é derivado do **SteamID** do jogador por meio do seguinte processo:

`SteamID → SHA-256 → Base64 (URL-safe) → GUID`

Exemplo observado:

- SteamID: `76561198012345678`
- SHA-256: `c991f9c7f37b12d7b3deddeb607ab338af88f4cbd253171c02cce3b...`
- GUID (Base64 URL-safe): `yZH5x_N7Etez3t3rYHqzOK-I9MvSUxccAszjtPnnRlc`

Exploit / Prova de Conceito

A partir da compreensão completa da estrutura do arquivo `TerjeParty.dat`, foi possível:

- Escrever manualmente entradas de GUID no arquivo;
- Criar **partys customizadas localmente** sem interação legítima no jogo;
- Inserir jogadores em uma party **apenas com o conhecimento de seus SteamIDs**.

Após a modificação manual do arquivo, o jogo reconhecia os jogadores inseridos como membros válidos da party, demonstrando que **não há validação robusta no lado do servidor** quanto à composição do grupo.

A prova de conceito e os experimentos realizados estão documentados em:

https://github.com/PSalleSDev/TerjeExp

Nota do Redator

Este documento foi elaborado com **caráter estritamente técnico, acadêmico e imparcial**, tendo como objetivo exclusivo a **análise e documentação de comportamentos observáveis** nos sistemas que compõem a modificação avaliada. A produção deste material **não possui finalidade lucrativa**, nem visa a exposição indevida, descredibilização ou prejuízo à iniciativa ou a seus mantenedores.

A motivação central deste trabalho é **contribuir para o fortalecimento do mod**, apoiando sua evolução contínua e a manutenção de um ambiente mais **seguro,**

confiável e estável para todos os participantes.

A divulgação das observações e análises aqui apresentadas ocorre no contexto de **compartilhamento de conhecimento técnico**, com a intenção de auxiliar os mantenedores do mod na identificação de pontos de melhoria, mitigação de riscos e aprimoramento das práticas adotadas. Parte-se do princípio de que a transparência técnica e o diálogo construtivo são ferramentas fundamentais para a sustentabilidade e maturidade de projetos comunitários e colaborativos.

Este documento deve ser interpretado como uma **contribuição positiva e colaborativa**, orientada à promoção de boas práticas de segurança e à entrega de uma experiência de jogo de qualidade à comunidade, pautada na **confiança mútua** entre mantenedores e jogadores.