Nader Sleiman

nader.sleiman@gmail.com | +30 6987397156

github | linkedin

Skills

Fields	Leadership | Native | Reverse Engineering | Blockchain | Frontend | Backend
Programming Languages	Rust | C++ | C | Asm x86/x64 | C# | Java | Python | Javascript | Lua

Experience

Blitz.gg (company)

Feb 2020 - Aug 2022

Principal Software Engineer | Head of Reverse Engineering — *Los Angeles, CA*

- Lead the dev team in improving on major parts of the Blitz's App : One of the most popular in-game coaching app used by millions of players.

- Reverse-engineered Epic Game's most popular game **"Fortnite"**'s packet replay system to be able to get real-time data from the game in the least intrusive fashion via replay files, which requires finding their decryption keys from within the game's memory.

- Optimized the electron-based desktop client performance by tweaking the front-end (JS/React) and writing native NAPI modules(C++) to leverage multi-threading and achieve optimal native speeds.

- Created a very low-latency IPC model based on Window's shared memory capabilities for communicating between the client and the games, which also served as an infrastructure for communicating to the game chromium rendered buffers and controllers events to be able to display and interact with in-game overlays.

- Protected the application against altering and distributing ADs free versions.

- Reduced servers costs by cutting down on data size by switching over from the JSON format to a Schema based Flatbuffers format (near raw binary size) with a custom ID system.

Solana Blockchain

Jan 2023 - Present

Co-founder of a highly profitable private automated arbitrage trader

- Actively working on a private Solana fork targeted for arbitrage optimization and performance boosting for highly competitive trading.

- Wrote a custom Geyser Plugin which allows for a very low latency inter-process communication.

- Maintaining an on-chain program that helps with trades.

- Actively researching and studying the up-to-date code base.

Windows Internals / Reverse Engineering

2013 - present

Practising reverse engineering and learning about windows internals for many years.

- Wrote Kernel-mode drivers for many purposes including:
  - Bypassing aggressive UM (Ring3)/KM(Ring0-) mode based protections.
  - Protecting UM applications.
  - Leveraging hypervisors for more advanced approaches like memory hiding/faking

- Wrote Undetected cheats for many games including **LoL**, **Fortnite**, **Apex**, **PUBG** **CS:GO**.

- Familiarity with Windows internals.

- Familiarity with dynamic and static analysis with the help of debuggers, static and dynamic analysis tools not limited to but including **OllyDbg**, **X86/64 dbg**, **IDA Pro**, **Re-class** ..

Notable Solo Projects

TFT Awareness
Sep 2019 - Dec 2019

*A standalone in-game coaching app for the popular Riot's Game **"TeamFight Tactics"***

- Reverse-Engineered **League Of Legends**'s Riot Games most popular game's client which is shared with that of TeamFight Tactics (**TFT**). Wrote non-invasive read-only- based code to read data from the game's runtime memory.

- Wrote an automatic offsets updater which runs on the game's unpacked binary to search for up-to-date game offsets to be able to access the right game data consistently across game updates which saves the need for manual amendments.

- Worked a system for in-game rendering overlay rendering and input translation based on an external headless chromium instance.

- **Riot Games** showed me their feedback that they were quite impressed, but I had to change some features to make it **ToS** compatable.

Hackemon
August 2016 - Jan 2017

*A fully-featured botting platform for Niantec's **PokemonGo** mobile game.*

- Wrote a packet-based emulation system to perform a remote headless human-like emulation.

- Used google maps API to restrict emulation movements to valid street paths to counter anti-human detection.

- Designed the UI with Java FX

Education

Bachelor of Computer Science
Jan 2009 - Sep 2012

American University of Science and Technology — *Beirut, LB*

Actively researching & Learning
Forever

Always learning and seeking the latest tech in various domains.