1400 - XenoScan: Scanning Memory Like a Boss

Saturday at 14:00 in Track 4
45 minutes | Demo, Tool
Nick Cano*Hacker*

XenoScan is the next generation in tooling for hardcore game hackers. Building on the solid foundation from older tools like Cheat Engine and Tsearch, XenoScan makes many innovations which take memory scanning to a whole new level.

This demo-heavy talk will skip the fluff and show the power of the tool in real-time. The talk will demonstrate how the tool can scan for partial structures, detect complex data structures such as binary trees or linked lists, detect class-instances living on the heap, and even group detected class instances by their types. Additional, these demos will take a look at the tool's extensibility by working not only on native processes, but also on Nintendo games running in emulators. You're not all game hackers, so the talk will also show how XenoScan can be useful in the day-to-day workflow of reverse engineers and hackers.

When I'm not doing demos, I'll be drilling down to the low-level to talk about the nitty gritty details of what's happening, how it works, and why it works.

By the end of the talk, you'll see the true power of a well-made, smart memory scanner. You'll be empowered to use it in your day to day hacking, whether that is on games, malware, or otherwise. For those of you that are really interested in the tool, it is completely open-source and all development is done on an interactive livestream, meaning you can participate in and learn from future development.
Nick Cano
Nick Cano is the author of "Game Hacking: Developing Autonomous Bots for Online Games" (No Starch Press), a Senior Security Architect at Cylance, and a life-long programmer and hacker. Programming since the age of 12 and hacking games since the age of 15, Nick has a strong background with both software development and Reverse Engineering. Nick has a history developing and selling bots for MMORPGs, advising game developers on hardening their games against bots, and making innovations in the EDR space for next-gen AV companies.

@nickcano93
https://github.com/nickcanohttp://www.nostarch.com/gamehacking
https://www.livecoding.tv/darkstar_xeno

#defcon25/by_track/track4/saturday #defcon25/By_Day/_saturday