1300 - Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits

Saturday at 13:00 in Track 3
45 minutes | Demo, Exploit
Manfred (@_EBFE)*Security Analyst at Independent Security Evaluators*

In theme with this year's DEF CON this presentation goes through a 20 year history of exploiting massively multiplayer online role-playing games (MMORPGs). The presentation technically analyzes some of the virtual economy-devastating, low-hanging-fruit exploits that are common in nearly every MMORPG released to date. The presenter, Manfred (@_EBFE), goes over his adventures in hacking online games starting with 1997's Ultima Online and subsequent games such as Dark Age of Camelot, Anarchy Online, Asherons Call 2, ShadowBane, Lineage II, Final Fantasy XI/XIV, World of Warcraft, plus some more recent titles such as Guild Wars 2 and Elder Scrolls Online and many more!

The presentation briefly covers the exploit development versus exploit detection/prevention arms race and its current state. Detailed packet analysis and inference on what the code looks like server side in order for some of the exploits to be possible is presented.

This presentation includes a live demonstration of at least one unreleased exploit to create mass amounts of virtual currency in a recent and popular MMORPG.
Manfred (@_EBFE)
Manfred (@_EBFE) has been reverse engineering and exploiting MMORPGs for 20 years. During that time, he ran a successful business based solely on exploiting online games in order to supply virtual goods to retailers. He has reverse engineered communication protocols for over 22 well known and popular MMORPGs and in certain cases circumvented anti tampering and software/hardware fingerprinting countermeasures. Manfred is currently a security researcher and analyst at Independent Security Evaluators (@ISEsecurity).

@_EBFE

#defcon25/by_track/track3/saturday   #defcon25/By_Day/_saturday