Intro

Every gamer has a story from a recent game where they've witnessed or fallen victim to an obvious cheat by another player. Maybe it's an autoaim or account mining. Maybe they've exploited the rules or purchased a stat boost or exceeded the maximum XP somehow. These players might be downloading software to perform these hacks or they might even be finding ways to hack the system themselves, breaking into the servers and finding vulnerabilities and sniffing packets to find more ways to give their characters a boost or an edge. Well, here are the 7 best/worst video game hacks.

7. DoSers, booters, cheaters

I feel like for any game created, there will be a way to cheat for it. It all depends on the type of game, who's playing the game, and how the system or game was created. This might mean anyone from your basic player to your advanced programmer having the ability or want to get better at the game—especially when they get bored or frustrated.

With DoSers, they usually just want to get the game to themselves or want to get back at a specific player or party. They'll use a DOS (denial of service) attack on their opponents to get their system to shut itself down or slow down the system to make the player easier to kill or manipulate in-game. Because a denial of service attack specifically targets the player's home system rather than the game, there's little risk of it getting bigger than expected and wiping out the game or an unintended target. DOS attacks are also usually temporary. A quick reboot and the system should be back to normal.

Booters will often find a way to get inside the system to specifically boot one player off the server. Say you're playing Apex: Legends and a player is annoying you. You can, if you trust your Googling skills, download software to specifically target this one player and clog their network and/or force the game to boot them regardless of the system they're using. This is a bit less temporary depending on how the player is booted. It could be a simple one-time attack (like a DOS attack that locks up the player's system and forces them out) that will boot the player out of a party or off the game for inactivity, or it might be more permanent in the way of reporting a player for bad behavior or cheating and getting them permanently banned from the game. There are also a number of websites where all you need is an IP address and the site will boot the player off the system for you. Easy as pie. It is a very effective way to get a player out of the game for a short time while you ransack their in-game home, take their stuff, or kill their character.

General cheaters are typically players who don't want to play the game as it was designed. They'll download add-ons and/or additional software to make them better players. Things like aimbots, ESP, attack immunity, and other perks that otherwise don't exist in the game. Depending on the game you play, it might be obvious if someone's using downloaded software, but others, like massive multiplayer online role-playing games (MMORPGs) it's trickier to find the cheaters. They may be using inventory stockers that give them infinite resources to build or craft items like in Minecraft or Skyrim and Elder Scrolls Online (ESO) or they might be buying older accounts and

using the XP, coins, or points from that to boost their own stats on their otherwise "young" player sheets (FIFA).

Bottom line is, most people purchase a game to have fun with it and want to get the best experience out of it. It sucks when you feel like you're having a great day only to get demolished by someone who's purchased or weasled their way into a game ability most players don't/couldn't have.

Not official sources, but here are some booting sites:

- PS4 Booter
- Play Station Network Booter/Instructions
- Xbox Booter (with recent activity ticker)
- LANC Remastered (PS4 and Xbox booter)

6. The Half Life 2 hacker.

Valve's Half Life 2, a first-person shooter (FPS) game with a focus on manipulating physics in-game (now you're thinking in portals!) was set to be released in September of 2004, but was released online on October 2nd, 2003, nearly a full year before it's official release date. Half Life when it originally launched was a game changer for the Valve Corporation, so Half Life 2 was highly anticipated, and they'd been working on this game for five years. Its premature release was a huge blow to the company. They informed the FBI that they were looking at a loss of revenue of nearly $250 million.

There are a lot of good ways to get in trouble as a hacker, but the most common seems to be stealing source code and posting it online. But what if you sat in a network for months, watching a developers every move, stole their source code, then asked them for a job? Alex Gembe had the audacity to do just that.

Alex seemingly stumbled into the hacking scene, falling for a World of Warcraft 3 scam that turned out to be a malicious worm. Instead of removing it from his system, he reverse engineered it to find out how it worked. He ended up using this knowledge to steal CD keys for the games he couldn't afford. So, he had a history of hacking and stealing games, but unlike other hackers like Manfred or Team Xecutor, he wasn't bored and seemingly didn't want money from these games, he just wanted to play games. But, sometimes when you play games, you win prizes. Alex thought he'd use his current plushy space in Valve's webserver to his advantage.

After finding a way into Valve's systems that lead to him stealing the Half Life 2 source code, he emailed the Valve CEO, Gabe Newell, and admitted he was the hacker in the system. Gabe, after working with the FBI to find Alex, responded and they began their correspondence. Eventually, Alex admitted to his hacking abilities and working for a red team, ultimately asking Gabe for a job while reminding Gabe that Alex was still sitting comfortably inside Valve's networks.

Alex Gembe was taken into custody by the German police on an unrelated investigation, but ultimately was taken to court for the Valve hack. While the courts couldn't prove that Alex was the one who released the Half Life 2 source code online, they did sentence him to 2 years of probation for hacking into Valve's networks. Valve officially released Half Life 2 in November of 2004 and seemingly saw no drop in sales despite the early online hack release.

- Deleon, Nicholas, TechCrunch, Clever: Valve tried to offer job to guy who stole Half-Life2 source code, November 13, 2008
- Levi, Ran, Malicious Life, The Half Life 2 Hack
- Parkin, Simon, Eurogamer, The boy who stole Half-Life 2, May 14, 2019
- Parkin, Simon, ars technica, Catching up with the guy who stole Half-Life 2's source code, 20 years later, June 19, 2016

5. Hacking FIFA Coins

So, the way FIFA Ultimate Team works is players can use game-earned coins to purchase player packs. These player packs make your team better and can be used to get you more coins as you go. These coins, according to FIFA, can not be purchased by a third-party vendor. So you can't just log into Ebay and purchase a player pack or coins from FIFA, you need to earn them in the game.

Well, Anthony Clark wanted in. He wanted to be able to sell these coins and player packs to make money outside the game. He worked with his friends Nick Castellucci, Ricky Miller, and Eaton Zveare and they got their hands on FIFA source code. Yeah, are you hearing this, developers? You've got to protect that source code. With this, they created a program called a FIFA Server Tool Application that would effectively play thousands of games at once. These games would collect various amounts of coins per game and send them all back to one master account. At their peak, Anthony, Nick, Ricky, and Eaton estimated they'd earned around 67 million coins in a single hour. They ran this gambit for two years, starting in 2013 and finally getting caught in 2015. I'm going to take this opportunity to tell my viewers, if you're online buying coins, outfits, weapons, or whatever you need for a game and you aren't buying it *from the game*, you might want to check to make sure the person you're buying from is selling things legally.

In February of 2016, Anthony was officially convicted of wire fraud by the Texas department of Justice. He was awaiting sentencing, and according to his family, was researching which federal prisons had the best school options, when he was found dead from an overdose of painkillers on February 26th, 2016. A mere two days before his sentencing. Because of his untimely death, his charges were dropped and his sentence was never delivered.

- The Lines, Will Green, Man Convicted Of Wire Fraud, Bilking EA Of $16 Million Worth Of FIFA Coins, November 16, 2016.

- Whittier Daily News, Brian Day, October 30, 2017, This Whittier man built a video game currency empire and became a millionaire — then an FBI raid brought it down
- Department of Justice, U.S. Attorney's Office, Northern District of Texas, Fourth Defendant Convicted in Scheme that Defrauded Software Company of More Than $16 Million Worth of Virtual Currency, November 16, 2016

4. Team Xecuter

Sometimes, hackers will gain access to game makers systems and release various items for games or release games early, before their official release date. Typically, when information or code like this is discovered and released online, others verify and/or use as they see fit often doing so with encryption/decryption. Another, much harder way, is to get access to a game maker's source code. Once you have access to source code, you can effectively create the game or a reasonable facsimile of it. From there, it's just a matter of making the game playable.

Team Xecuter is a group of hackers known for their ability to hack consoles to play pirated versions of videogames. They gained access to the Nintendo Switch, the Nintendo 3DS, the Nintendo Entertainment System Classic Edition, the Sony PlayStation Classic, and the Microsoft Xbox. Once they gained access to these systems, they then sold the pirated versions of the games to players, making millions of dollars in the process. Team Xecuter didn't just upload the source code online for all to see/use, they went so far as to create their own section of the market. They created an online database where players could download their pirated versions of popular games. They even created their own hardware that came preloaded with these pirated versions of games.
Team Xecuter spent a lot of time and effort making their pirated versions look and feel like the real thing. Coming up with creative but official-sounding names for their devices like Gateway 3DS, the Stargate, the TrueBlue Mini. Even attachments for existing Nintendo devices like the SX line that included the SX OS, the SX Pro, the SX Lite, and the SX Core. These names and the "about us" section on the website were intended to make the public believe they were a legitimate company and team working hand in hand with large gaming companies.

With the Nintendo Switch, they created hardware that would automatically connect the gamer to Team Xecuter's suite of games, bypassing Nintendo entirely and by making the user pay a licensing fee to play the games.

Ultimately, the members of Team Xecuter were arrested and charged with fraud on August 20, 2020. Sentencing is still being determined.

- Cox, Joseph, Motherboard, Vice, How Pirated Versions of 'Super Smash Bros. Ultimate' Leaked Weeks Before Release, November 26, 2018
- Department of Justice, US Attorney's office Two members of notorious videogame piracy group "Team Xecuter" in custody, October 2, 2020

- United States Department of Justice, Indictments for Team Xecuter

3. Manfred

Manfred was an active player of MMORPGs, but, like many programmers, he'd get bored with the game after a while and start wondering what *else* he could do with the game. This led him to searching through code to find ways to get him advantages in the games. Maybe more coins, extra experience points, or access to in-game homes of other players. He played and found vulnerabilities in a multitude of games like Ultima Online, Dark Age of Camelot, Anarchy Online, Lineage II, Final Fantasy Online (the first one), World of Warcraft, and…you get the picture.

Now, there are a lot of ways you can get into or break a system, but he mostly used buffer overflow and integer overflow exploits.

He hacked the server to be able to send it information directly. He used the hacks mentioned above to give his character higher stats, more boosts, and eventually progressed to doing this in multiple games and then farming and selling these items. Shadowbane was his biggest/best hack. He played for a while, then as he got bored, he wanted to find a way to exploit it. Using a lot of the hacks mentioned, he found a way to delete the houses of other players in the game. Once he learned this, he'd go to old houses getting ready to be destroyed just by game mechanics and delete them before other players got there so he could take the stuff.

After one ill-timed house delete, the home's original owner showed up to use his house only to find it gone. They talked for a while, brought in a GM and the GM ended up reporting the issue to the game maker. Ultimately, the GM was fired and Manfred got fed up. In retaliation, he waited for the dark of night, then logged back into the game. He went from house to house, systematically deleting every home he could find in the game. When he finished, he'd deleted every home existing in the game and logged off. The servers were eventually reset, but he showed that the exploit wasn't the GM exploiting higher user creds, it was a player exploiting a vulnerability within the system.

After 20 years, Manfred has now moved away from the selling of in-game items online. He's now totally white-hat and works for a security assessment company. Manfred is an incredible and charismatic hacker. If you want to learn more about him, check out my Manfred two-part episode on my podcast, Darknet Diaries.

- https://darknetdiaries.com/episode/7/
- https://darknetdiaries.com/episode/8/.

2. h1z1 30,000 players banned.

In January of 2015, Daybreak games released h1z1. Riding the wave of popular FPS (first-person shooter) games featuring zombies like Call of Duty Black Ops, h1z1 became popular pretty fast. So popular that there became an entire second market dedicated just to cheats and hacks for this game. Aimbots or autoaim add-ons that

would aim for the player, meaning an almost sure-thing kill every time. Or ESP add ons that would allow the player to see through walls and around or through buildings to show the exact locations of other players.

These cheats and others like them became so rampant in the game that then-president John Smedley decided to crack down on cheaters in the game. “@H1Z1Insider you don't think we know these cockroaches? We do. We are going to be relentless and public. Screw not provoking them.” John Smedley Tweet, 11:54AM, May 19 2015

Rather than ban one player at a time, he and Daybreak decided to do a system-wide ban of all cheaters using this software. Literally overnight, just under 25,000 players were banned for cheating or using cheat-based software in the game. There was a caveat, though. Any one of the more than 30,000 players banned in the initial wave and subsequent smaller waves could be unbanned. But only if they uploaded a public (emphasis on *public*) apology video.

After this tweet, you’d expect him to get bombarded with people trying to get back in to play the game, right? Well, apparently not. Despite the game only being out a few months, nobody was really jumping at the chance to get unbanned from the game. As we’ve seen with people like Manfred, players, especially with programming knowledge, eventually run the course of the game and get bored. However, as of today, only a handful of apology videos were ever uploaded, and only one seems to be left open to the public.

The first apology video uploaded proved that Daybreak would keep their word. The player uploaded their apology and got unbanned from h1z1, allowing them to play the game again. However, based on another tweet from John Smedley, this person didn’t learn their lesson and were “well on their way” to getting banned again. I guess some lessons don’t stick as well as they should.

On Screen Content:

- Jonathan Ore · CBC News · Posted: May 21, 2015 2:54 PM ET | Last Updated: May 22, 2015
- ESP Hack example 1 (2015) explicit (Timestamp 4:40, 9:06) no autoaim
- ESP Hack example 2 (2018) explicit
- Aimbot Hack example 1 (2015) Explicit
- Seemingly legit apology video

Sources:

- Savage, Phil, PC Gamer, Banned H1Z1 cheaters may be allowed back, if they publicly apologise, May 20, 2015
- John Smedley Tweet
- Marks, Tom, PC Gamer, Daybreak president John Smedley talks H1Z1 and leaving Sony, May 8, 2015

- Ore, Jonathan, CBC, Cheaters banned from H1Z1 video game unbanned if they publicly apologize, May 21, 2015

1. XBox Underground

Ok, this one's a long one and the story gets a little crazy, so if you want more information, I actually did a two-part series on my podcast about just this group. Let me tell you, it's a wild ride, so strap in before you listen.

This group is maybe the most prolific video game hacking group to date. They started their endeavor in 2011 and ran through around 2014/15. The team went from maybe four or five people and became almost a dozen or more. They started by buying old Xbox developer kits that had extra features and early access to in-development games, meaning they could play games well before release.

One guy got into the unreal engine, which contains source code used by virtually all video game companies. Once they had access to the Unreal Engine, they quickly gained access to other video game manufacturers networks. In their three-year reign, they gained access to Microsoft, Activision, Valve, Epic Games, EA, Bungee, Blizzard, Zombie Studios, Disney, Intel, and a bunch of other game makers networks. Once they got into one system, they'd find similar personnel and use the same login info to pivot to other game developers. While in the network, sometimes they'd just watch inboxes, but other times they'd move through the system. In one case, they actually found the source code for Gears of War 3 and downloaded it to their personal servers.

Their main goal from the start was just to get access to games nobody could play or early access to unreleased games. It was just a cool trick they'd show their friends, they'd play their games and no harm done. That was until they started letting in more people. Curious people. Curious people don't often like to play by the rules or they get careless. As you can imagine, the more careless they got, the closer they got to the prying eyes of the government. In the end, a lot of them served time for various sentences, which on its own is worth listening to the podcast for. Seriously, they could make a movie about these guys (Wargames 2?).

- Anti Cheat software, Epic Games
- https://darknetdiaries.com/episode/45/
- https://darknetdiaries.com/episode/46/
- Koerner, Brendan I, Wired, The Young and the Reckless, April 17, 2018