

Fortnite's paid outfits, dances have made it a target for lucrative account theft



Fortnite / Aurich

reader comments

35 with 32 posters participating

Share this story

A Thursday *BBC* report takes a look at the state of Epic Games' mega-popular game *Fortnite* through the eyes of a particular audience: its black market of account thieves. After speaking with "about 20" perpetrators, reporter Joe Tidy put together a report that breaks down what's being stolen and resold, how it's happening, and what the game's players can do to shore up their own accounts.

The resulting story shouldn't surprise anyone in the infosec

world, and it doesn't expose any apparent data leaks on the part of Epic. But it's a reminder that a few modern trends have come together in convenient fashion, ready for any enterprising script kiddie to tap into, and that users should know how a mountain of years-old data leaks can come back to haunt them.

Off-the-shelf, off your old passwords

The report begins with a teenaged *Fortnite* fan speaking to the *BBC* via webcam with his identity hidden. He got into the *Fortnite*-theft game inadvertently, he claims, by starting as a victim. The bad news began when he received email alerts from Epic Games—one saying his account's email address had been changed, and another saying that two-factor authentication (2FA) had been turned on (and attached to a phone number that wasn't his). His original account was totally lost as a result, the teen alleged.

After taking to Twitter to publicly complain about his inability to reclaim the account and its paid content (including "battle pass" purchases and cosmetic items), the unidentified teen noticed something: other *Fortnite* accounts for sale. These offered all manner of in-game loot (particularly outfits and emotes) for much less than those items would cost via Epic's official store.

This teen then laid out the process that other unidentified thieves separately confirmed to *BBC*. Some of the steps include: hiding behind proxy servers; combing through major data breaches full of combinations of usernames, passwords, and email addresses; paying for "off-the-shelf" software that would automate the login process at Epic's site; and quickly accessing a swiped account for long enough to change its email and 2FA settings, presumably with anonymous or automated email addresses and phone numbers.

The first teen in the report told the *BBC* that he only spent one day trying to swipe other users' accounts in this manner—but still managed to scoop up more than 1,000 accounts in that span of time. The implication, then, is that many *Fortnite* account thefts come as a result of reused usernames, email addresses, and associated passwords.

Hackers confirmed that one issue consistently locked them out of successful quick-hit thefts: when victims already had 2FA enabled for their accounts. (In other words, for these script kiddies, they simply jiggled the car's door handle, noticed it was locked, and went on to the next one.)

1 vs. 99, meet 1 vs. £1,500

The *BBC* referred to PayPal and Bitcoin transaction records to confirm seriously high stolen-account sales, including this aforementioned teen racking up £1,500 in “his first few weeks” as a go-between for other thieves and sellers.

But for all the details this report scooped up about account sales, it lacks a serious response from Epic Games itself. (Epic did not immediately respond to requests for comment from Ars.) The primary point of contention is in understanding if or how Epic is recognizing automated attempts by single users to log in to a wave of accounts, then immediately change their credentials.

Additionally, Epic doesn't appear to have a system in place that allows aggrieved players to verify their payment credentials as part of a “my account was stolen” process. A visit to Epic's primary help site includes zero articles in either its main listing page or via a “stolen account” search that offer steps or help with the scenario of an account being stolen or locked out.

Epic does dangle a carrot for its *Fortnite* players to turn 2FA on in the form of free, exclusive in-game cosmetics, but the

company doesn't require 2FA to log in to any of its games. While most online services don't mandate the use of 2FA, one game maker, Valve Software, has leveraged 2FA to reinforce the idea of account identity in the online shooter game *Counter-Strike: Global Offensive*. Should you wish to join that game's "prime" series of servers, you can either pay the free-to-play game's retail price or submit a valid and verified phone number and then rack up a reasonable amount of gameplay time without any signs of cheating or other inappropriate activity in the online game.

<https://arstechnica.com/?p=1431405>