



Don't Fall Asleep On Online Games

🔗 technology risk management BSA-AML

Summary: Money launderers have found another channel - online games. Although this is an unusual way to launder money, staying in the know is important for all banks.

Researchers have found that people who nod off during the day are more likely to develop dementia. It seems falling asleep when you are supposed to be awake is a sign of having too many beta amyloid proteins in the brain (3x as many as those who stayed awake). These proteins have been found to trigger dementia.

As you jolt yourself awake this morning, we shift our focus to online gaming. If you've ever played a free online game, you know that in most of them, players need resources to advance through the game. Those who play lots of online games know that gathering gems, gold, objects of power, or other talismans can take a long time. That's why game makers also make money by selling those resources inside the game app.

However, for banks, you should also know that it is another avenue to launder money. Recently, security researchers at Kromtech Security in Dubai found this out and warned the US Department of Justice, Apple, and a game manufacturer that a group of money launderers created automated tools to launder money by buying and selling online game premiums.

It was pretty easy to do as well. Apple makes it simple to create lots of online gaming accounts, requiring just a valid email address, password, date of birth, and three security questions after all.

Researchers found the scam in June, when they happened to find a database left exposed online without authentication. This database happened to belong to credit card thieves. It contained the card numbers, expiration dates, and security codes for over 150k credit cards issued by 19 different banks. It also included an automated tool set up to create gaming and email accounts for users in Mauritania, Indonesia, Kuwait, Saudi Arabia and India.

Once the money launderers had lots of Apple accounts and valid email addresses, they acquired stolen credit card numbers, automatically charging goods on the cards to find those that were still valid. They then used the valid cards to buy game resources and then put up virtual talismans for sale. Gamers flowed in and digital wallets handled the order processing. Multiple Apple accounts and devices distributed the demand and the result was automated money laundering for credit card thieves.

The criminals targeted Clash of Clans and Clash Royale, both manufactured by Supercell. They also targeted another game, called Marvel Contest of Champions, by Kabam. While these aren't among the top 5 games in the US, they do boast more than 250mm users and generate around \$330mm in annual revenue.

Researchers say Apple, email providers and game makers should all do more to prevent similar attacks. They suggest providing multiple account verification requirements, better card verification, and a commitment from game companies to pursue abusers. Doing so could help reduce the chance of a repeat issue and help keep gamers and others safe.

Although this is an unusual way to launder money, it is a good reminder to keep your eyes open because BSA/AML sophistication continues to expand.

LOAN GROWTH AND FLOATING RATE ASSETS

Your bank can purchase [fully-funded, senior secured floating rate loans](#) to diversify your portfolio and increase your loan assets. Contact us today for more information.

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.