USE CASE

Modern Day Money Laundering: How Hackers and Fraudsters are Exploiting Online Video Games to Make Millions

PANOPTICON LABORATORIES

PROTECTING ONLINE GAMES FROM IN-GAME THREATS

THE SITUATION: Money Laundering in Video Games

In our first use case, we shined a light on the epidemic of account takeover in online video games: the virtual hijacking of player accounts by financially motivated hackers, fraudsters, and cheaters. While video game publishers once viewed account takeover as a nuisance and tolerated it as the cost of doing business, it has evolved into a global epidemic in which virtual and real-world currencies combine, and where sensitive player information is compromised and exploited daily. As a result, publishers of some of the world's most popular video game titles are now scrambling to remediate reputational and financial damages that adversely impact their bottom line.

Today, when assessing an online video game's overall risk profile, credit card fraud and associated chargebacks (the "demand by a credit-card provider for a retailer to make good the loss on a fraudulent or disputed transaction") rank highly among publishers as major causes of financial loss. As a consequence, significant attention and resources are devoted to stopping credit card fraud, chargebacks, and fees that, on average, cost the merchant an additional $2.40 for every $1 of losses.

Account hacking is just one vector for credit card fraud. When accounts are taken over, the hacker can use the connected credit cards to purchase virtual currency. With the rise of free-to-play games, however, fraudsters can also purchase lists of stolen credit card account numbers on the dark web, create hundreds or thousands of free-to-play game accounts, and purchase virtual items and currency using those stolen card numbers without ever having to "hack" into anything.

In both instances, after the virtual items are purchased using stolen cards, they are sold to other players for real money in an online gray market for a fraction of a publisher's official price, which negatively impacts the game's revenue. Kabam, publisher of The Hobbit: Kingdoms of Middle-earth, as well as other popular mobile games like Kingdoms of Camelot and Star Wars: Uprising, warned players about the risks of purchasing cheap Mithril (The Hobbit's virtual, in-game currency) from sites other than the in-game store:

> *"We have seen a surge of activity from fraudulent third-party sites that are not affiliated with Kabam, claiming to sell cheap Mithril for various Kabam games…the use of these sites may compromise your game and payment information. These web sites use stolen credit card information to make the Mithril purchases that you would receive. This opens you to potential fraudulent activity in the future."*

Today, when assessing an online video game's overall risk profile, credit card fraud and associated chargebacks rank highly among publishers as major causes of financial loss. As a consequence, significant attention and resources are devoted to stopping credit card fraud, chargebacks, and fees that, on average, cost the merchant an additional $2.40 for every $1 of losses.

Money Laundering in Video Games (cont'd)

As a means to mitigate chargeback risk, video game publishers are increasingly turning to tools that monitor every single transaction request, and then run a gauntlet of fraud checks before any transaction is approved. Jagex Game Studios, for example, described their multi-step processes for avoiding credit card fraud this way:

> *"At the point of sale we make a series of checks to reduce the risk of fraud from our previously identified fraudsters preventing known bad transactions going through our systems and increasing our processing costs. Our PSP does pre-auth checks for basic risks like CVV, blacklists and velocity limits, and then our main third party fraud solution does a post-auth check using a large dataset provided by Jagex as well as its own network linking tools. We manage all the rules and operations of these systems as we know our customers better than anyone, understand our appetite for risk and how it affects the overall business."*

Jagex also claims to analyze, "the performance of all our tools daily and make any changes to block new risks and assure our customers are not being blocked incorrectly."

Despite the ongoing efforts of in-house fraud teams and third-party fraud prevention solutions, the average digital merchant still incurs 2% in direct chargeback losses annually, which is well above the 1% threshold that is considered the high end of acceptable by credit card companies. Considering that publishers lose an additional $2.40 for each $1 in bad charges, the true financial impact of credit card fraud can add up quickly. In order to protect themselves from unexpected financial burden, some publishers opt to purchase chargeback insurance, which offers100% protection against chargebacks should a bad request manage to slip through the cracks. While this option allows publishers to plan financially and avoid unexpected financial outlays, costs for this type of insurance can be as high as 8% per transaction.

Because transaction-layer services do not benefit from any player behavior data generated in-game, discovery of fraudulent activity is limited to after a transaction is attempted, or worse, after it occurs. Under this reactive security posture, video game publishers frequently remain in the dark about fraudulent transactions for 60-90 days post-incident. This delay provides cyber criminals with ample time to use stolen credit cards to continue to purchase virtual assets before the compromised card is blacklisted.

By 90 days out, however, it's all but impossible to track down the fraudster or hacker, leaving the video game publisher on the hook for the chargeback and lofty fees. The criminal, on the other hand, wastes no time in unloading the stolen virtual goods and currency on the gray market in exchange for cash. In doing so, the criminal has effectively perpetrated a 21st century money-laundering scheme at the expense of the video game industry.

With billions of dollars now being spent in online video games, the motivation for cyber criminals to perpetrate credit card fraud increases every day. Knowing this to be true, many transaction service providers readily admit that without access to in-game player behavior, there is only so much that their technology can do to differentiate between authorized, but unusual transactions and truly fraudulent payments. As a result, the tools developed by the card processing industry often suffer from a large number of false positives (legitimate payments which are incorrectly flagged as fraudulent by the anti-fraud system), which also negatively impacts monetization and player satisfaction.

Credit card fraud might be one of the most common forms of financial fraud, but the proliferation of account hijacking via cyber attack alongside the growth of free-to-play games is making the problem more frequent and damaging for the video game industry.

HYPOTHETICAL USE CASE: Attack on Major Video Game Publisher Cost it Millions of Dollars and Thousands of Players

A large and successful online video game publisher (we'll call the company FridgeArt Interactive, Limited) maintains a diverse library of over 20 Multiplayer Online Battle Arena (MOBA) and Massively Multiplayer Online (MMO) games. Currently, more than 30 million people around the world play one or more of the company's games each month.

FridgeArt's games generate revenue either through a "pay-to-play" model, where the player purchases and downloads the game client and plays online (typically on a PC or game console) or through a "freemium" model, where the player is able to play a basic version of the game for free (typically on mobile devices and smartphones). In both models, substantial revenue is generated via in-game sales of virtual currency or items such as upgraded armor or weapons, experience boosters, or extra character slots. A significant portion of FridgeArt's $400 million annual revenue is driven by these in-game purchases of virtual items and currency by loyal fans and new players alike.

On average, FridgeArt enjoys a solid Average Revenue per User (ARPU) of $0.63 for its mobile games and $3.25 for its console games, spent over the course of multiple microtransactions. To ensure the integrity of all of these transactions, on top of using multifactor authentication to secure the login component of players' to game accounts, FridgeArt also employs a layered approach to identify fraudulent in-game purchases, utilizing white/blacklisting, IP/Geolocation and device reputation, alongside a comparison to previous transaction activity.

During the course of a three-month span, FridgeArt unexpectedly became inundated with customer service calls from players all over the world being locked out of their game accounts. Before the customer service team could finish resolving the thousands of reported account issues, players also suddenly began to report unauthorized credit card activity ranging from a few dollars to a few hundred dollars. One highly monetized player in particular reported a charge of more than $1,000, which was 50% more than the total he had spent during the past 2 years.

In order to prevent chargebacks and fees, the company offered refunds to players who reported fraudulent charges, but the small customer service team was not able to keep up with massive influx of complaints that were continuing to flood in on a daily basis.

During the course of a three-month span, FridgeArt unexpectedly became inundated with customer service calls from players all over the world being locked out of their game accounts. Before the customer service team could finish resolving the thousands of reported account issues, players also suddenly began to report unauthorized credit card activity ranging from a few dollars to a few hundred dollars. One highly monetized player in particular reported a charge of more than $1,000, which was 50% more than the total he had spent during the past 2 years.

USE CASE (cont’d)

Following an internal investigation, FridgeArt discovered that thousands of player accounts had been compromised, resulting in millions of dollars of fraudulent charges. Upon learning of the fraud, FridgeArt’s board of directors immediately hired a security consultant to determine what happened and to learn how to prevent such a situation in the future. After 4 weeks, an incident response was issued, and the fraud was determined to be the result of hackers who targeted FridgeArt’s players with a phishing email, offering a one-time discount designed to look like an official email from the company.

Even more shocking to the board was just how easily the attack was executed. The hackers simply embedded a readily-available malware toolkit onto the machines of every player who clicked the link, which, in turn, enabled a man-in-the-middle attack that silently hijacked their accounts the next time they logged in using their valid ID, password, and multifactor key. Once inside the player’s account, the hackers were able to transfer all the player’s accumulated virtual items and virtual currency into fence accounts and use their stored credit card information to purchase even more virtual goods. The hackers then used the credit cards in small increments to mimic regular player behavior, and infiltrated accounts across all 20+ titles, so as to not draw attention by having too much purchasing activity within one game. Plus, the attack occurred during summer vacation, which was the company’s busiest season. So while the purchasing activity was higher than normal, FridgeArt thought that it was nothing more than an unusually busy summer.

Once the virtual items were purchased, the hackers immediately dumped everything on the gray market in exchange for real-world currency. The security team, despite its best efforts, could not track down where the phishing email originated from, nor could they find out who was responsible for it. Despite weeks of effort, hundreds of hours of overtime, and thousands of research cases, the hackers got away clean.

In less than 120 days, FridgeArt was forced to refund several hundred thousand dollars and pay close to $1 million in chargebacks and fees. It also had to shell out $200,000 for the security audit and $250,000 to upgrade its cybersecurity defenses. The company’s reputation also took a profound hit through unfavorable media coverage in some of the industry’s most prominent news sites and magazines. Even worse, FridgeArt’s players flooded the games’ online forums to publically vocalize their frustrations and fears concerning their compromised accounts. In the following quarter, in-game revenue was down 40% and monthly active users had dropped by more than15%.

A BETTER SOLUTION: In-Game Anomaly Detection & Behavioral Analytics

FridgeArt thought it was being risk averse by using multi-layered defenses, covering front-end login and back-end transactions. As illustrated in FridgeArt's story, however, the problem with credit card fraud prevention technology is that it is always reactive, essentially creating a false sense of security. In fact, it is common for online game operators to learn that a player's account has been hacked only when that player contacts customer support, or when an unauthorized credit card transaction is charged back by the cardholder, sometimes 30-60 days after the takeover.

By this time, significant damage would have already been done: the player's accumulated items and wealth would have been stolen and sold on the gray market, his or her credit card would be compromised, and/or destructive bots would be introduced into the game to farm resources and in-game currency. It can be difficult, if not impossible, for the operator to restore stolen items and currency, and even if it can be done, the player is still likely to leave the game for good after his or her account has been taken over due to a sense of unease or violation.

Panopticon Laboratories has better solution to detect credit card fraud, account takeover, and other destructive in-game behaviors before it causes irreparable damage to the game, the publisher's bottom line and its reputation.

WatchtowerTM, the first and only in-game security product, provides video game publishers with a 360-degree overview of player behavior over time. Watchtower identifies and alerts on suspicious behavior by modeling normal, historic player behavior and looking for activity that varies from the established norm. The SaaS-based, product's real-time, actionable alerts and research tools, allow company analysts to make quick and informed decisions that stop malicious in-game behavior before damages can occur.

In FridgeArt's case, Watchtower would have proactively alerted the publisher to suspicious in-game activity at the moment a player's account was taken over, well before any credit cards were actually compromised. Players establish a baseline of normal, in-game behavior over time. They play with the same people (friends, clans, guilds, etc.), at similar times (on weeknights from 9 p.m. to 11 p.m., for example), in similar ways (PVE vs. PVP, group raids vs. solo farming, etc.), and establish unique patterns of monetization. Combined, these behaviors add up to a snapshot of how the player plays for fun. When an account is taken over, however, the hacker is playing for profit, not fun. Even when fraudsters successfully hijack players' accounts utilizing man-in-the-middle malware (which makes it appear as if the session is originating from a previously-observed, valid IP address) their actual in-game behavior will look vastly different from the player's. The fraudster will be communicating with and transferring items to previously unknown associates, playing at different times and in different ways, and purchasing patterns will differ from what is normal for that player.

Fraudsters are expert liars. They can lie about who they are, where they're connecting from, and even what machine they're using to play. But history never lies. Historic player behavior can be a powerful tool in a game operator's arsenal, but only when it can be easily accessed and interpreted.

Contact us today for a Watchtower demo or to get started. Don't let cyber criminals cost you your revenue and your players.

PANOPTICON

LABORATORIES

Panopticon Laboratories is the first and only in-video game cybersecurity company, built to protect online video game publishers from the financial and reputational damages that can result from cyber attack.

Through proprietary technology that is uniquely focused on gameplay itself, Panopticon sets a baseline of activity for every player who participates in online play. Upon discovering anomalous behavior, Panopticon alerts publishers with more than 98 percent accuracy, along with providing recommendations for incident investigation and immediate remediation. Panopticon was founded in 2013 and is based in Columbus, Ohio.

TRUST US.

Hackers, cheaters and scammers won’t stop their cyber attacks unless you make them. Contact us for a Watchtower demo today.

sales@panopticonlabs.com

For more information about Panopticon, visit www.panopticonlabs.com and follow @PanopticonLabs on Twitter.

PROTECTING ONLINE GAMES FROM IN-GAME THREATS