Use Case:

How Video Game Account Takeover Cost One Publisher a Loyal Player

PANOPTICON LABORATORIES

PROTECTING ONLINE GAMES FROM IN-GAME THREATS

WHAT IS VIDEO GAME ACCOUNT TAKEOVER?

Online video game accounts hold valuable personal and financial (i.e. credit card) information, but also hold virtual items and virtual currency that have been bought or earned in-game by the player who owns the account. Like bank and eCommerce accounts that also hold value, game accounts are locked behind a username, password, and other login controls. With the video game industry's rapidly changing business model – which has evolved from static, single player, offline games to dynamic, multiplayer, online experiences with virtual economies that interface with the global 'real money' economy – online video game accounts are increasingly a target for account hacking and takeover.

Today, the same kinds of malware that have traditionally been used to exploit bank account IDs and passwords are being used to hack into online game accounts. Once criminals gain access to a player's account, they can steal their accumulated virtual items and wealth, commit traditional credit card fraud, or introduce destructive bots into the game that farm resources and currency. Subsequently, a thriving online gray market for virtual items and currency that are normally won or purchased inside of games has erupted; providing a safe haven for cyber criminals to sell their illegally obtained items for a fraction of the publisher's price.

Today, the same kinds of malware that have traditionally been used to exploit bank account IDs and passwords are being used to hack into online game accounts. Once criminals gain access to a player's account, they can steal their accumulated virtual items and wealth, commit traditional credit card fraud, or introduce destructive bots into the game that farm resources and currency.

Some video game publishers are attempting to prevent account takeover by using common login controls, such as multifactor authentication, secret questions, device reputation, and IP/geolocation technology. Unfortunately, hackers have had more than a decade to learn to defeat these front-end controls. To monitor in-game activities, publishers typically create manual reports and database queries based on forensic investigation of confirmed takeover events to try and identify suspicious behavior with limited success. Game companies are learning what banks learned ten years ago: these reactive reports are expensive to set up, hard to keep updated, and require extensive manual review. Neither login controls nor forensic reports effectively prevent hackers and fraudsters from initiating attacks.

A TRUE STORY: The Case of "Crafty"

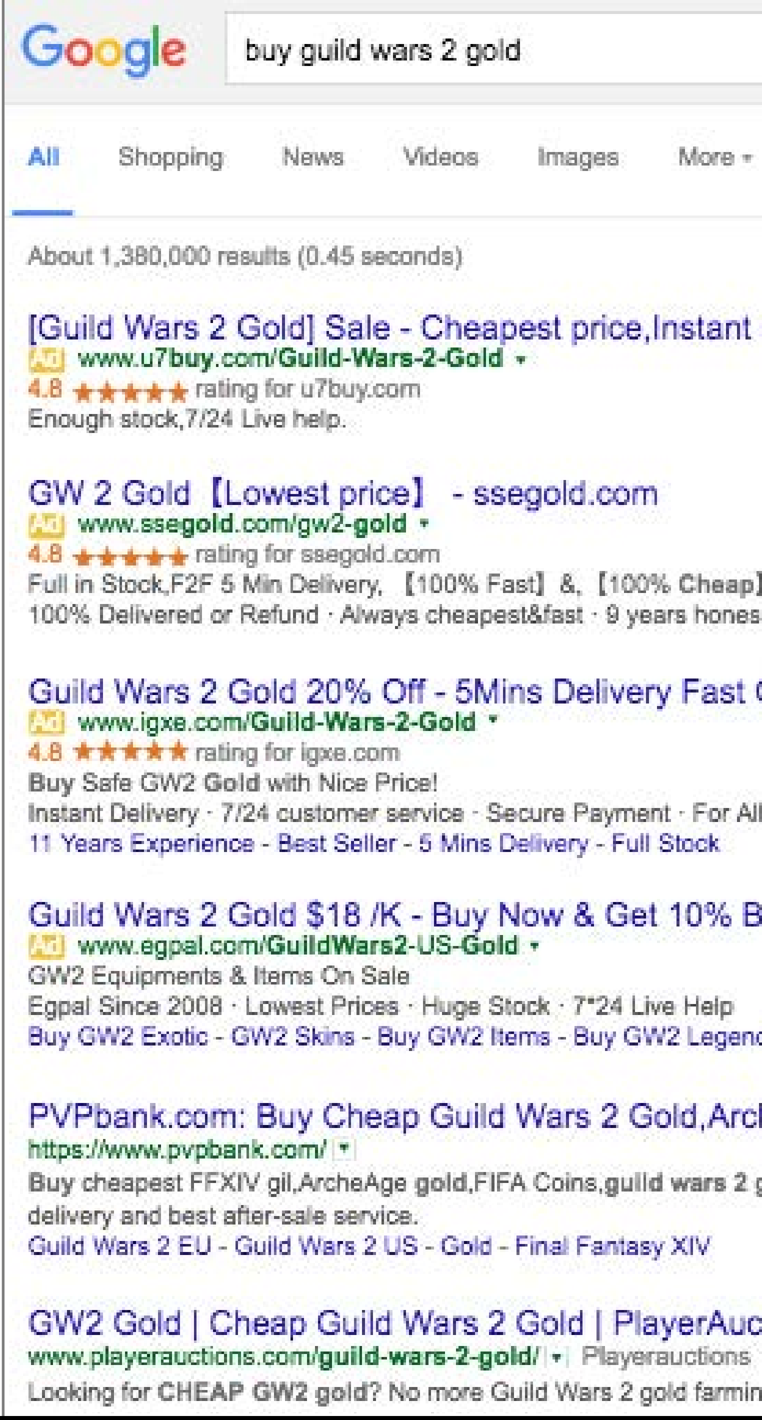
Guild Wars 2 (GW2) is one of the world's most popular online video games with more than 7 million players worldwide. It is a Massively Multiplayer Online game (MMO), set in a fantasy world. As the name suggests, GW2 encourages cooperative play and allows players to self-organize into "guilds." GW2 players can earn gold, armor, weapons, and a variety of other materials used for crafting, and can also buy gems, the game's virtual currency that is purchased with real money.

In 2013, about a year after the game was released to the general public, a GW2 player – we'll call her "Crafty" – had her account hacked. One day, Crafty didn't show up for her guild's weekly meeting, which was unusual, especially since she was seen in-game earlier that day, although at an unusual time and without "repping" (not displaying the guild's tag). The group eventually learned that Crafty's account had been hacked and she had been working with GW2's support team to reset her password for more than a week.

GW2's developer and publisher, ArenaNet, is known for being proactive in working to safeguard its player's accounts. However, its email-based authentication system (which automatically sends out a link via email that the user must click any time the system notices a new IP address being used) was easily defeated by basic key-logging and screen-scraping tools, which exposed both Crafty's game and email login credentials. Since the hacker had obtained her email login information, the multifactor authentication was easily defeated and new Chinese IP address was authorized.

Once inside her account, the hacker changed Crafty's password, locking her out of the game, as well as the account management system, player forums, and support ticketing system. Next, the hacker liquidated all transferrable in-game items from her account, including valuable Tier-6 crafting materials, unbound top-tier weapons and armor pieces, and gems. Once the account was cleaned out, the hacker then used her max-leveled characters as gold farming bots, remote controlling them via scripts so that they would gather virtual currency and items around the clock.

Crafty contacted support immediately upon becoming locked out, but it still took ArenaNet more than a week to complete its investigation and restore her access. By then, of course, everything of value was gone, sold on the game's auction house for liquid virtual currency or transferred to consolidation or "fence" accounts for later re-sale on any number of gray market websites for real money.



buy guild wars 2 gold

About 1,380,000 results (0.45 seconds)

[Guild Wars 2 Gold] Sale - Cheapest price,Instant
Ad www.u7buy.com/Guild-Wars-2-Gold ▾
4.8 ★★★★★ rating for u7buy.com
Enough stock,7/24 Live help.

GW 2 Gold 【Lowest price】 - ssegold.com
Ad www.ssegold.com/gw2-gold ▾
4.8 ★★★★★ rating for ssegold.com
Full in Stock,F2F 5 Min Delivery, 【100% Fast】 &, 【100% Cheap】
100% Delivered or Refund · Always cheapest&fast · 9 years hones

Guild Wars 2 Gold 20% Off - 5Mins Delivery Fast
Ad www.igxe.com/Guild-Wars-2-Gold ▾
4.8 ★★★★★ rating for igxe.com
Buy Safe GW2 Gold with Nice Price!
Instant Delivery · 7/24 customer service · Secure Payment · For All
11 Years Experience - Best Seller - 5 Mins Delivery - Full Stock

Guild Wars 2 Gold $18 /K - Buy Now & Get 10% B
Ad www.egpal.com/GuildWars2-US-Gold ▾
GW2 Equipments & Items On Sale
Egpal Since 2008 · Lowest Prices · Huge Stock · 7*24 Live Help
Buy GW2 Exotic - GW2 Skins - Buy GW2 Items - Buy GW2 Legend

PVPbank.com: Buy Cheap Guild Wars 2 Gold,Arch
https://www.pvpbank.com/ ▾
Buy cheapest FFXIV gil,ArcheAge gold,FIFA Coins,guild wars 2 g
delivery and best after-sale service.
Guild Wars 2 EU - Guild Wars 2 US - Gold - Final Fantasy XIV

GW2 Gold | Cheap Guild Wars 2 Gold | PlayerAuc
www.playerauctions.com/guild-wars-2-gold/ ▾ Playerauctions
Looking for CHEAP GW2 gold? No more Guild Wars 2 gold farmin

The Case of “Crafty” continued...

After Crafty was able to take stock of the theft, she asked the GW2 support team if they could restore the stolen items. Support opened a second research case to investigate. In the meantime, Crafty began playing again, starting the arduous process of rebuilding her inventory.

More than four months later, ArenaNet finally decided that, based on its research, an item restore was warranted. The best they could offer, however, was to set the account back to the point in time at which it had been first compromised, effectively wiping out all the work she’d done since the attack. Crafty wasn’t thrilled about losing months’ worth of experience points and the new item drops she’d managed to find in the meantime, but since the items that had been stolen were even *more* valuable, she accepted their offer.

When the restore was finally completed, the hacker (who unbeknownst to Crafty still had access to her machine via deeply-embedded malware that several antivirus scans failed to detect) broke in all over again. This time, the bad guy not only stole all of her gold and materials (for a second time!), he also deleted every one of Crafty’s max Level-80 characters, wiping out every account-bound weapon, item, and armor set that each of those characters had in their inventories. Several months’ of gameplay needed to level each of those characters, along with hundreds of hours of farming and crafting, were wiped out in seconds.

While the integrity of Crafty’s online gaming experience was completely diminished, the successful attacks against her account had big consequences for ArenaNet. Not only did it cost them multiple hours of expensive support and research to decide whether or not Crafty’s case was legit, but everything that ArenaNet did to help her only benefitted the hacker in the end. As a result, despite the publisher’s best efforts, Crafty, a committed, monetized player, was driven away from the game, taking her dollars with her. She hasn’t been back since.

Unfortunately, Crafty’s experience is not isolated. One former video game executive contends that “account takeover is the single most important security issue facing the industry today.” Cost associated with it encompass lost revenue due to hacked players leaving the game and other players buying the stolen items on the gray market rather than from the publisher; credit card chargebacks and fees; support and investigation time; and reputational damages.

When the restore was finally completed, the hacker broke in all over again. This time, the bad guy not only stole all of Crafty’s gold and materials (for a second time!), he also deleted every one of her max Level-80 characters...Several months’ of gameplay needed to level each of those characters, along with hundreds of hours of farming and crafting, were wiped out in seconds.

A BETTER SOLUTION: In-Game Anomaly Detection vs. Login Controls and Forensic Reports

ArenaNet, to its credit, did everything in its power to remediate the attack on Crafty's account (she even said she was "satisfied" with their assistance); but at the end of the day, it was all for nothing.

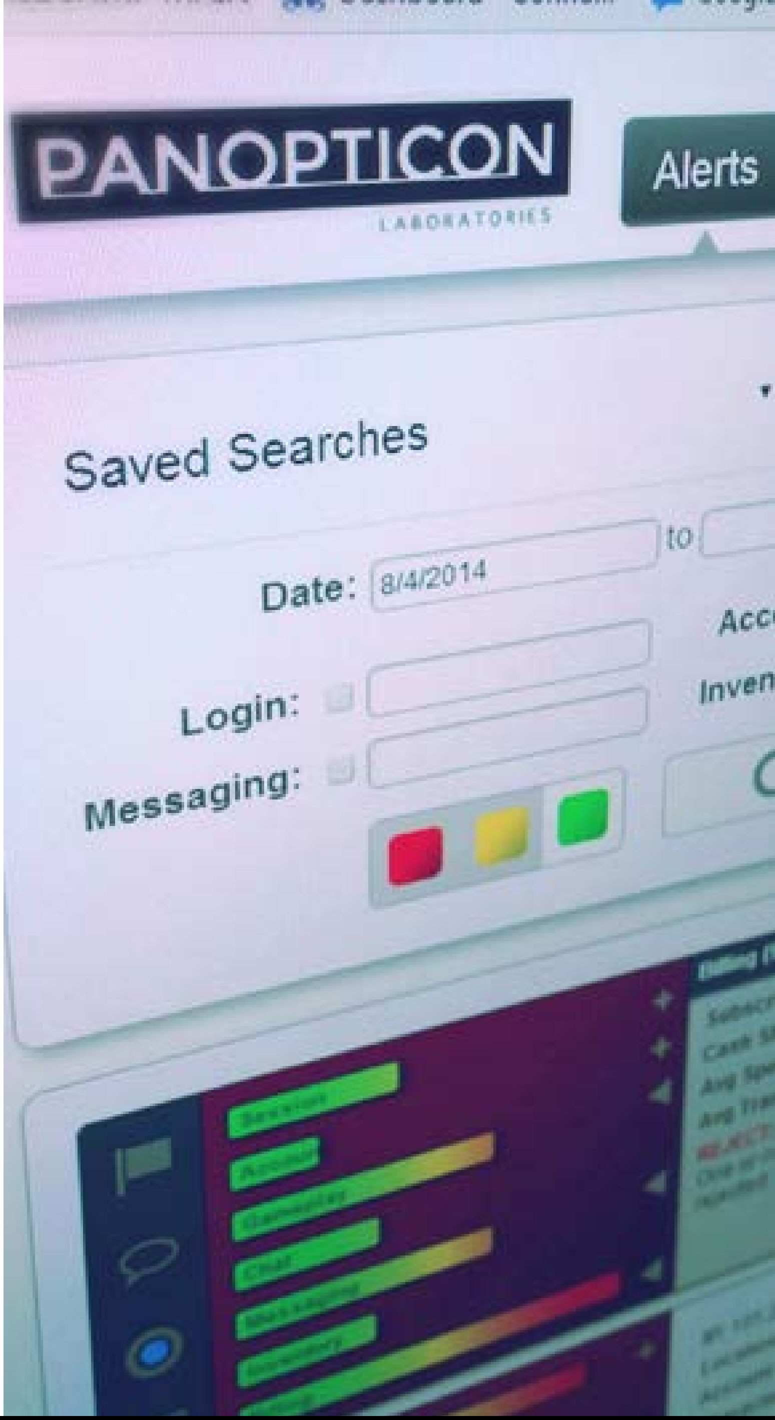
As illustrated in the true story of Crafty, it is common for online game operators to learn that a player's account has been hacked only when that player contacts customer support or when an unauthorized credit card transaction is charged back by the cardholder, sometimes 30 to 60 days after the takeover. By this time, significant damage has already been done: the player's accumulated items and wealth have been stolen and sold on the gray market, their credit card has been compromised, and/or destructive bots have been 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 they can, the player is likely to leave the game for good after he or she's been taken over due to a sense of unease or violation.

Introducing a better solution, **Watchtower** from Panopticon Laboratories, the first and only in-game security product, provides video game publishers with a 360-degree overview of player behavior over time. Using proprietary anomaly detection and behavioral analytics, Watchtower enables video game publishers to identify and alert on suspicious behavior by modeling normal, historic player behavior and looking for activity that varies from what is normal. The SaaS-based product's real-time, actionable alerts and research tools allow analysts to make quick and informed decisions that stop malicious in-game behavior before damages can occur.

Hackers and fraudsters are expert liars, 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 ruin the gaming experience for your players.

Contact us for a Watchtower demo today.

sales@panopticonlabs.com



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