



The Cybercriminal Roots of Selling Online Gaming Currency

Trend Micro Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

The Online Gaming Currency Marketplace

9

The Laundering of Online Gaming Currency

25

Fueling Traditional Cybercrime

27

The Impact of Online Gaming Currency Laundering

29

Conclusion

It is no secret that the gaming industry is a lucrative one. In 2015, gamers from all over the world generated a total of US\$91.8 billion of revenue for the whole gaming industry¹-with US\$23.5 billion of that revenue coming from the U.S. alone.² With that amount of money and influence, it is no surprise that cybercriminals have taken interest in adding gamers to their list of possible victims.

Games, especially those based online, have always been at the receiving end of cyber attacks. Most of the time these attacks involve the theft of personal information, gaming accounts, banking information, log-in credentials to other websites, and many more.

Even with numerous hacking incidents, cybercriminals are aware that stealing such information may not always provide immediate monetary rewards. And so, cybercriminals decided to search for other ways they can make a profit out of games. Thus, cybercriminals decided to widen their scope and began stealing online gaming currencies, which they will then sell to gamers who want to advance in the game. We discovered that this business model has proven to be an effective way for cybercriminals to earn money from their misdeeds and to establish an efficient source of funds for their illegal activities.

Although cybercriminal activities are illegal, the trade of online gaming currencies isn't. Therefore, law enforcement cannot be compelled to shut down every website selling these currencies. Despite that, it is important for online gamers to know that such tactic is being used by cybercriminals today. Gamers must be made aware of the crucial role they have in cybercrime whenever they take part in the exchange of online gaming currencies. Denial of service attacks, identity theft, and financial fraud are just a few of the attacks that have been funded by the sale of online gaming currencies and have devastated companies and organizations of all sizes.

Cybercriminals found easy profit in the sale of online gaming currencies and have successfully channeled that profit back to their schemes. As gamers are now more than willing to spend real money to enjoy a game, cybercriminals will continue to tap that market and inevitably use the profits gained from there to launch bigger and more damaging attacks in the real world.

Note:

For crimes involving the sale of online gaming currency, there is in no way that the video gaming industry should be blamed since they are also a victim. The video gaming industry pays a heavy price for such crimes-both from the loss of revenue to the negative impact to the brand due to the presence of dissatisfied players who find it difficult to "win" against players who pay real money to get ahead. In fact, gaming companies have been putting in several multiple safeguards in the game to prevent malicious actors from "gaming" their systems-the use of two-factor authentication seems to be the most successful method so far.

The Online Gaming Currency Marketplace

Over the years, video games have proven to be more than just a simple form of entertainment. The video game industry continues to grow and it has successfully positioned itself as one of the most lucrative means of entertainment around. In the United States alone, 63% of all households have at least one person playing video games for at least three hours a week. Also according to the Entertainment Software Association (ESA), there are a lot of individuals willing to invest in gaming devices, with 65% of U.S. households owning a device to play video games.³ Although the popularity of video games may benefit game developers and gamers alike, that fame had somehow also attracted cybercriminals.

With cybercriminals keeping a close eye on the gaming industry, common cybercriminal activities in video games, such as hacking and glitching, have continued to grow in number. The increase in cybercriminal activity related to online games can be attributed to the huge potential for revenue, the ease of hacking a game account, and the lack of severe penalties or criminal prosecution for such cybercrimes.

Though there are several forms of cybercriminal activities in video games, this report will specifically focus on cybercriminal activity related to the sale of online gaming currency for real money. We will also look into how the funds are funneled into other traditional cybercriminal attacks that have real-world implications. For this research, 'online games' will be used to define games that require the user to be connected to the internet to play and maintains a competitive aspect.

Online Gaming Currencies

Every online game has its own type of gaming currencies, which players can use to purchase items, weapons, skills, and services within the game. For example, the popular MMORPG (Massively-Multiplayer Online Role-Playing Game) *World of Warcraft* by Blizzard Activision has 'gold' as one of its main currencies⁴, while Riot Games' *League of Legends* has Influence Points and Riot Points as the main in-game currencies.⁵ There are several ways for players to "work" for those currencies. One of the most common methods is by completing goals or quests and by gaining experience through leveling up.

In contrast, there also exists an unconventional way of gaining these currencies. One of the most popular methods is called Real-Money Trading (RMT), which is the sale and/or trade of in-game currencies in exchange for real world money.⁶ The practice of using real money to avail of services or upgrades in the game is often viewed as an unethical way for players to get ahead in the game. Just like the use of 'boosting' services, wherein players can instantly achieve a desired level or state in the game for a certain fee⁷, most gamers believe that using real world money to advance in a game goes against the main idea of enjoying a game through the challenges and rewards the player receives by actual game experience.

In fact, a vast majority of online games prohibit RMT and threaten players with the immediate termination of accounts that are suspected of engaging in RMT. Then there are also some game developers who made premium items available without having to pay with real money. Another way game developers tried to combat the rise of RMT is by creating player markets or auction houses that allowed players to trade game items in exchange for in-game currency. Other than that, most of the efforts made to stop the proliferation of RMT have been met with negative reactions.⁸

But why is there a market for online gaming currency? The answer is rather simple: time.

Having large amounts of gaming currency is ideal in a game since it would provide gamers access to a wide variety of items, weapons, and skills that can make their character stronger. As stated earlier, completing quests and goals is one of the ways to get in-game currency. So in order to have a lot of in-game currency, players will have to put in hundreds of hours of gameplay in order to achieve that. Therefore, those people who just want to enjoy the benefits of having tons of in-game currency without spending so much time and effort in a game will naturally search for a shortcut. This desire for a get-rich-quick scheme in games is what gives life to the markets of online gaming currency.

Targeted Games and Platforms

What gaming currencies are usually sold online? By simply looking at the websites selling online gaming currencies, one can quickly identify the game titles that are usually targeted.

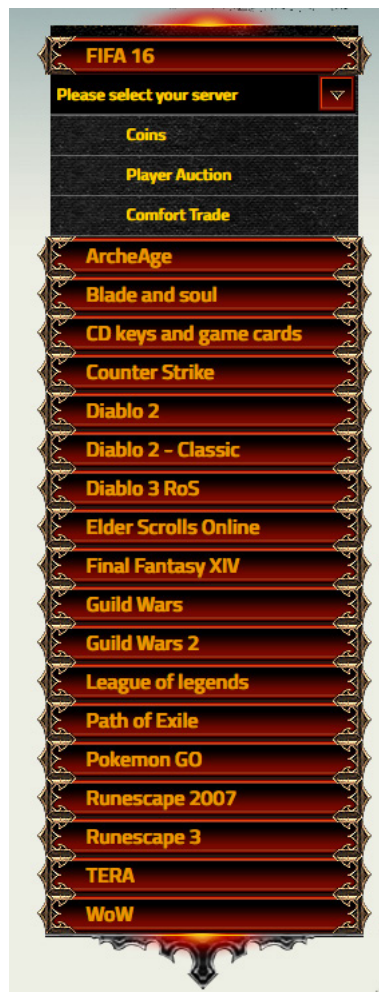


Figure 1. A website selling video gaming currency for various game titles

Some of the popular games listed on websites selling online gaming currencies are *World of Warcraft*, *Guild Wars/Guild Wars 2*, *League of Legends*, and *Final Fantasy XIV*—all of which are MMORPGs that have a stiff competition on resources and experience. With that, the sale of online gaming currency comes in handy as players would reach out to these websites and pay with real money in order to purchase a specific amount of in-game currency which they will use to buy rare or special items, weapons, skills, or even upgrades.

It may seem that the competitive aspect between gamers is what fuels cybercriminals to sell online gaming currency. Though competition is considered one of the many factors in the proliferation of online gaming currency markets, a game's popularity is also something cybercriminals consider when it comes to picking what gaming currencies to sell in their websites. For instance, the game *World of Warcraft* has around 5.5 million paying players in 2015, thus becoming a huge target of cybercriminals.⁹

A few more examples of online games that have their currencies sold online are the following:

- *Minecraft*
- *FIFA*
- *World of Warcraft*
- *Final Fantasy*
- *Star Wars Online*
- *Guild Wars 2*
- *Path of Exile*
- *Madden NFL 16*
- *NBA 2k16*
- *Grand Theft Auto V*

Aside from the title of games that have their currencies sold online, looking at these websites (Fig. 1) can also identify the gaming platform that is mostly targeted. In this case, the most targeted platform is the PC (with an exemption of *Pokemon Go*). While there are a number of games that are available on other platforms (Xbox and Playstation), there are still more websites selling online gaming currency for games available on the PC than for any other gaming console.

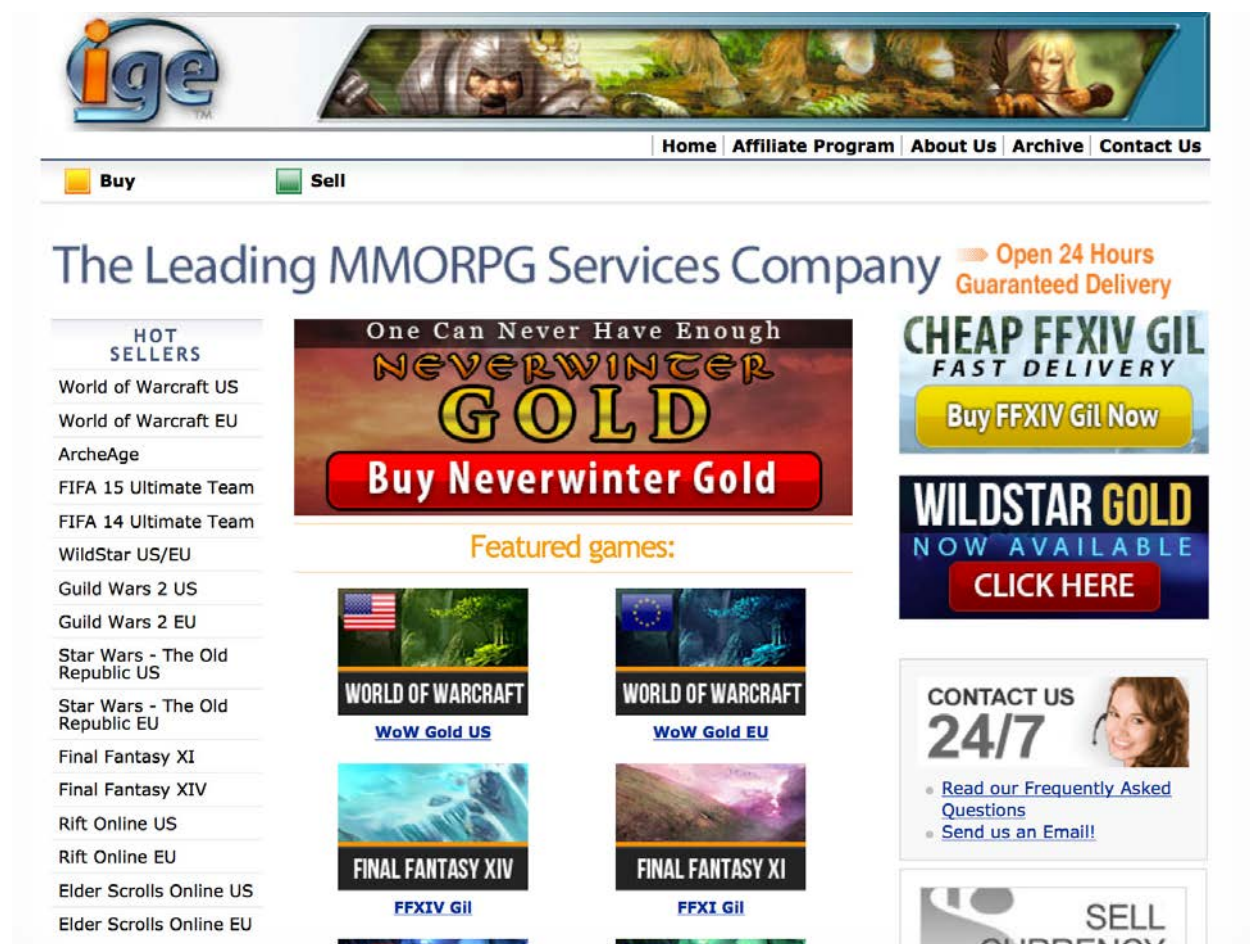


Figure 2. This is an example of a long-standing website that buys and sells MMO gaming currencies

Business Case for Selling Online Gaming Currency

While there are, in fact, so many other ways for cybercriminals to earn money, one may wonder why cybercriminals would even consider selling online gaming currency in the first place. What makes it so attractive to them?

One main reason behind this is that selling gaming currency is not inherently illegal. In relation to this, online gaming currencies are also not regulated. Meaning, there is no law today that exists to regulate digital currencies in games.

In fact in ESA's annual report, they made it clear how and why gaming currencies should not be regulated the same way as other virtual currencies:

ESA successfully advocated having video game-related points and prizes excluded from regulations covering virtual currencies that were issued by the New York Department of Financial Service in June. The department sought to regulate the use of digital currency, such as Bitcoin, that might pose consumer protection risk and be used for the online purchase of unlawful items, among other things. ESA sought and obtained clarification that these rules don not apply to digital units used solely within online game platforms or used as part of prepaid cards.¹⁰

There are also no laws set to indict a person involved in hacking, glitching, or even buying online gaming currencies—even if it were done through the use third-party programs or exploits.¹¹ The worst thing that can happen to someone caught doing such activities would be the suspension of their game account/s. However, while not necessarily illegal, the earnings gained from hacking may be supplying illegal and illicit activities which may lead the cybercriminal into a life, or even a career, of crime.

Other than that, the game platform also has something to do with rise of markets selling online gaming currencies. Most of the games that are listed in websites selling gaming currencies are games that are available on the PC. Experienced hackers and cybercriminals know that creating malware or third-party programs and bots that will exploit a system is much easier when done for the PC than for other gaming platforms. In a PC, games can be decompiled and modified easily for cheating purposes. Whereas the closed operating system of other gaming platforms or consoles makes it harder for hackers or cybercriminals to manipulate the system to carry out a cheat.

The Laundering of Online Gaming Currency

While the sale of ill-gotten online gaming currency and virtual items can disrupt the economy of an online game, earnings from such sales can also affect real-world economy in a negative way.

Based on our findings, the money earned from selling online gaming currency are used to fuel traditional cybercriminal campaigns such as denial of service attacks, identity theft, and financial fraud against different companies, organizations, and even other highly visible representatives in the media.

In this section, we will talk about how online gaming currency is laundered into real money and vice versa. We will also expose the link between selling online gaming currency and traditional cybercrime.

How is Gaming Currency Laundered?



Figure 3. The steps cybercriminals take in using online gaming currency to fund cybercriminal activities

Victimization Phase

The first phase in laundering money earned from selling online gaming currency requires the threat actor to obtain access to online gaming currency. While there may be some cases where cybercriminals do this legitimately, like patiently playing the game, it is more common for cybercriminals to resort to hacking players' accounts or exploiting the game servers. These are done through a variety of methods, which we will list below:

Stealing Gaming Credentials

Malware/Infostealers

Malware—specifically infostealers—play a vital role in the victimization phase of the laundering scheme. We spotted malware finding their way into popular game add-ons, malvertising schemes, gaming websites, fake gaming-themed websites hosting malware, as well as other major malware campaigns.

Recently, however, remote access Trojans (RATs) had become the preferred method of compromising credentials. The use of RATs gives the attacker far more ways to earn revenue from each infection as cybercriminals are provided with more things to do than simply selling stolen information pertinent to the game they've targeted. With RATs cybercriminals have access to other types of personal information, such as banking accounts, credit card information, and even account credentials to other websites, etc.

Below is a list of the malware families targeting specific online games:

Malware Family	Targets
FRETHOG TATERF(worm version of FRETHOG)	<i>Rainbow Island, Cabal Online, A Chinese Odyssey, Hao Fang Battle Net, Lineage, Gamania, MapleStory, qqgame, Legend of Mir, World Of Warcraft</i>
STIMILIK/STEAMILIK (aka ESKIMO, SteamStealer) STIMILINI/STIMILINA	Targets the Steam application
WINNTI	Targets gaming companies
LEGMIR	Targets <i>Legend of Mir, World of Warcraft, QQ Game</i>
ONLINEG (generic family name) LOLYDA HELPUD DOZMOT	Steals passwords from various online games
ENTEROK	Targets Korean PC games and mobile online games e.g. <i>Elsword, MapleStory, WINBARAM, World of Warcraft</i> Games from Nexon and/or Hangame

Malware Family	Targets
TARCLOIN	Presents itself as game launcher of <i>The Sims 3</i> and <i>Assassin's Creed III</i> but installs a bitcoin mining application
ZUTEN	Targets online games: <i>MapleStory</i> , <i>ZhengTu</i> , <i>Perfect World</i> , <i>Legend of Mir</i> , <i>Ruler of the Land</i> , <i>Rainbow Island</i> , <i>Eudemons Online</i> , <i>Fantasy Westward Journey</i>
URELAS	Monitors applications related to card games
USTEAL	Targets online gaming-related applications, e.g. <i>World of Tanks</i> , <i>Dota2</i> , and Steam applications
KUOOG	<p>Targets <i>Aion</i> and <i>World of Warcraft</i></p> <p>Single User Games: <i>Call of Duty</i>, <i>Star Craft 2</i>, <i>Diablo</i>, <i>Fallout 3</i>, <i>Minecraft</i>, <i>Half-Life 2</i>, <i>Dragon Age: Origins</i></p> <p><i>The Elder Scrolls</i> and specifically <i>Skyrim</i> related files, <i>Star Wars: The Knights of the Old Republic</i>, <i>WarCraft 3</i>, <i>F.E.A.R.</i>, <i>Saints Rows 2</i>, <i>Metro 2033</i>, <i>Assassin's Creed</i>, <i>S.T.A.L.K.E.R.</i>, <i>Resident Evil 4</i>, <i>Bioshock 2</i></p>
CRYPTLOCK	<p>Online Games: <i>World of Warcraft</i>, <i>Day Z</i>, <i>League of Legends</i>, <i>World of Tanks</i>, <i>Metin2</i></p> <p>Application-specific files of the following gaming companies: Various EA Sports games, Various Valve games, Various Bethesda games</p> <p>Gaming application: Steam</p> <p>Game Development Software: RPG Maker, Unity3D, Unreal Engine</p>

Table 1. List of malware families used to hack games

Phishing

Email phishing, and in some instances spear phishing, had also been used to steal game login credentials.

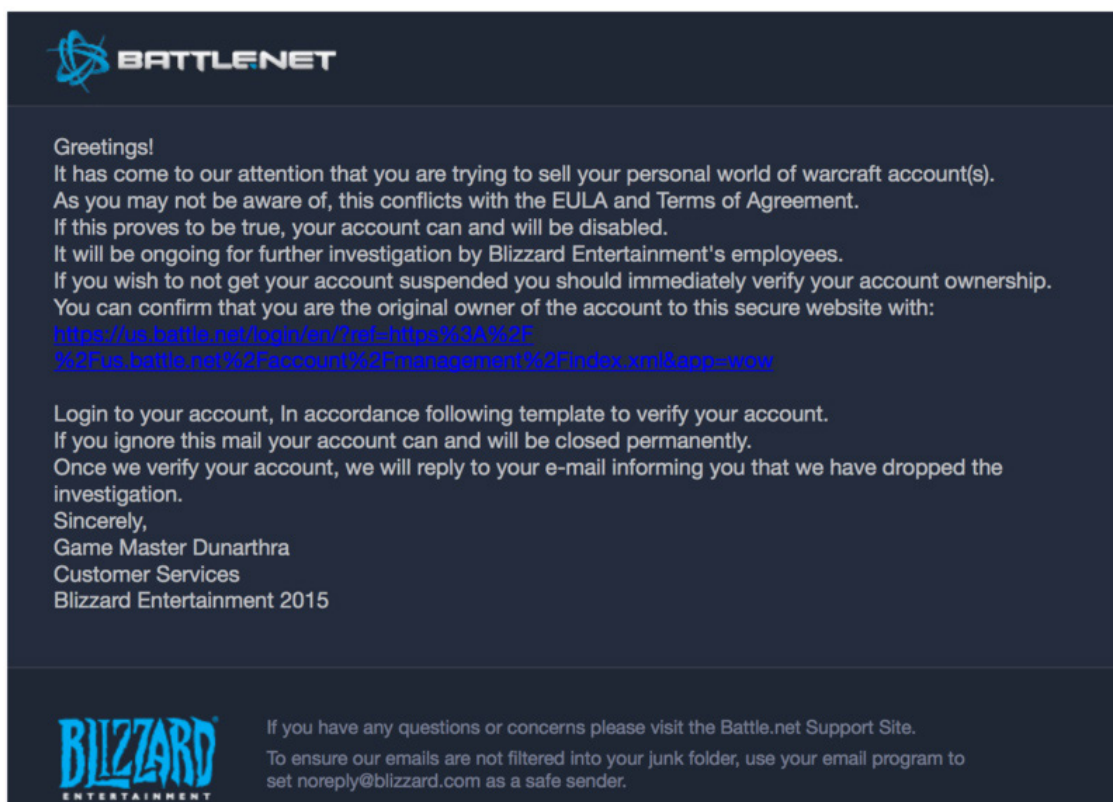


Figure 4. Phishing email targeting World of Warcraft users and scaring them into thinking that their game account has been banned or terminated

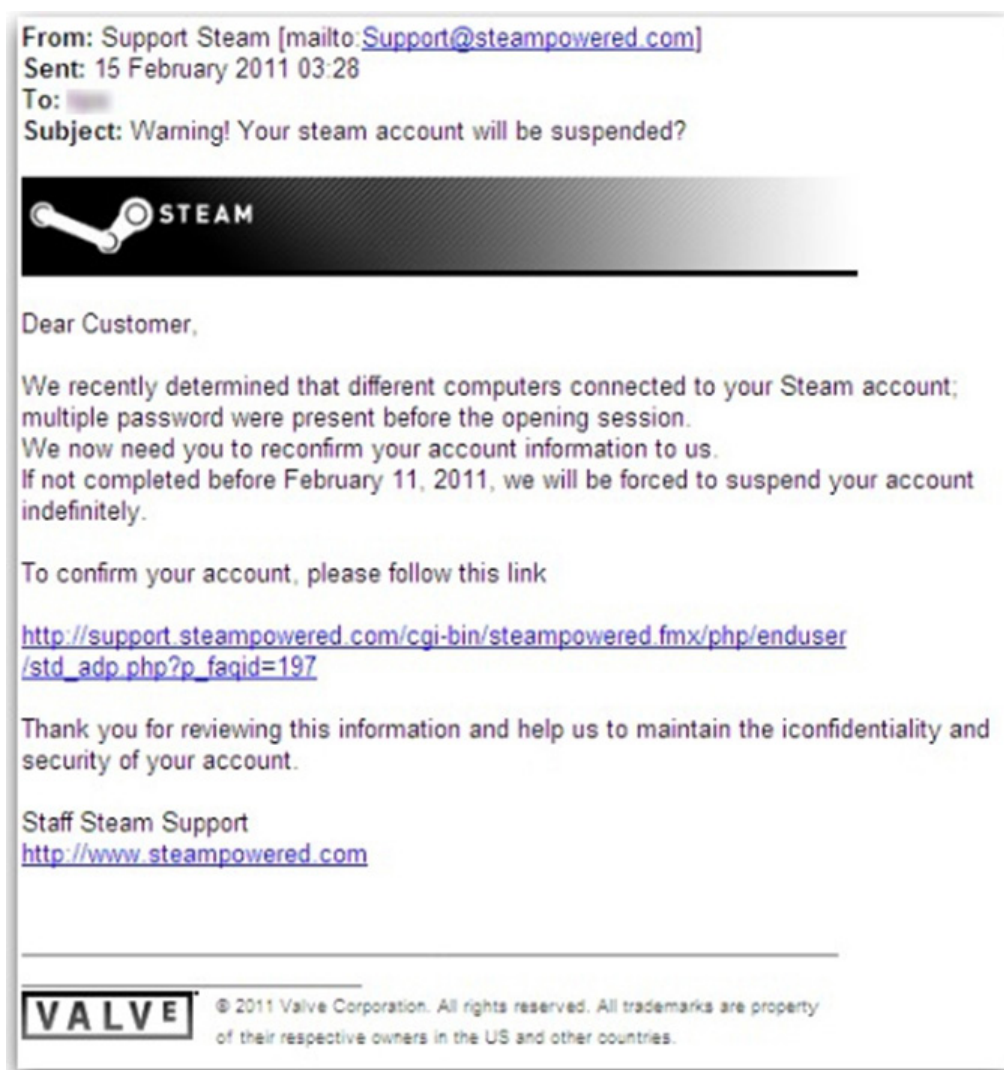


Figure 5. A sample phishing email targeting users of the Steam gaming network

Popular themes used in the social engineering of these scams come in the form of gaming account security warnings (i.e. unauthorized login detected, password change attempts), notifications of infractions committed by the gaming account (illegal purchases of gaming currency or goods), or actions taken against the gaming account (banned, illegal activity detected, etc.).

Exploiting Games and Gaming Servers

Exploitation of various games and gaming servers through a variety of methods is just another means to harvest gaming currency. These methods are described below:

Glitching

Glitching is the exploitation of a particular bug or irregularity in the game in order to gain unfair advantage. A glitch in the game, for example, can make a player purchase an item repeatedly even if the player does

not have the required amount of money. One other way also is when a character is able to slay a high-level enemy without a change in the players hit or health points (HP). A glitch can also allow a user to gain large sums of gaming currencies in a short period of time, just like what happened in the game The Division earlier this year.¹²

Duping (Duplicating)

Duping—a slang term for duplication—is the exploitation of an unpatched bug in the game that allows hackers to duplicate copies of a virtual item or currency in a game. Duping an expensive or highly sought after virtual item could allow a person to sell it repeatedly, thus providing the hacker with the chance to earn large sums of gaming currency.

No Man's Sky, which was one of the most anticipated games released this year, had a duping exploit that allowed players to have multiple copies of items in their inventory.



Figure 6. An example of duping at work, wherein the user makes several virtual items available with little to no cost to the gamer

Gold Farming

Gold farming is the term used to describe the methodical and repeated performance of an action over a long period of time in order to obtain large amounts of gaming currency. Gold farming had long been a valid business practice in Asia and had been a service wealthy gamers commonly purchase.

In 2005, an estimated 100,000 Chinese gamers were employed, by gamers from other countries, as full-time gold farmers for popular RPGs (role-playing games).¹³ In May 2011, the Guardian reported that Chinese prisoners were forced to farm for items and currency that were then sold to online gamers. Afterward, the proceeds went directly to the prison.¹⁴

Botting

Botting is the method of automating gameplay through the use of programs which do not require human interaction. To keep operating costs low, farming for gaming currencies is often conducted by these bot programs.

Advertising Phase

The advertising phase of the laundering of online gaming currency is conducted via a number of digital platforms, such as dedicated surface websites, advertisements in legitimate websites, and social media postings.

There are also forums and sites on the Deep Web that serve as proxy sites for the payment of goods or services through escrow.

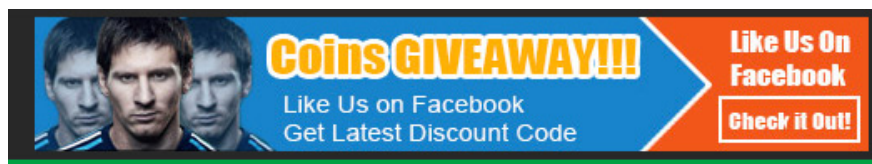


Figure 7. To gather more followers and gain popularity for increased sales, some gaming markets advertise giveaways

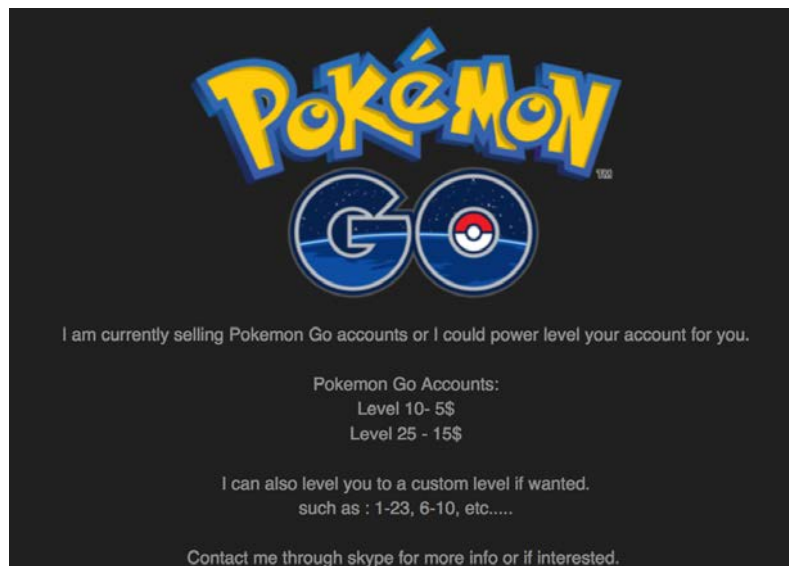


Figure 8. Game accounts of a wildly popular mobile game being sold on a forum on the surface web



Figure 9. Another example of a web advertisement used to sell gaming currency. It assures customers of fast delivery across multiple gaming platforms and the presence of customer support too.

Just like other competitive cybercriminal markets—such as bulletproof hosting service providers—gaming currency sellers strive to stand out by offering better terms, agreements, guarantees, or customer support.

Customer Support

To provide customers with a sense of security, some websites selling online gaming currencies offer live chat support—which is their way of assuring their customers that they are communicating with a friendly human being. Whether the question is about billing, delivery, or a simple process inquiry, these sites will gladly offer help just to convince clients, who want to buy gaming currencies, to finalize their transaction.

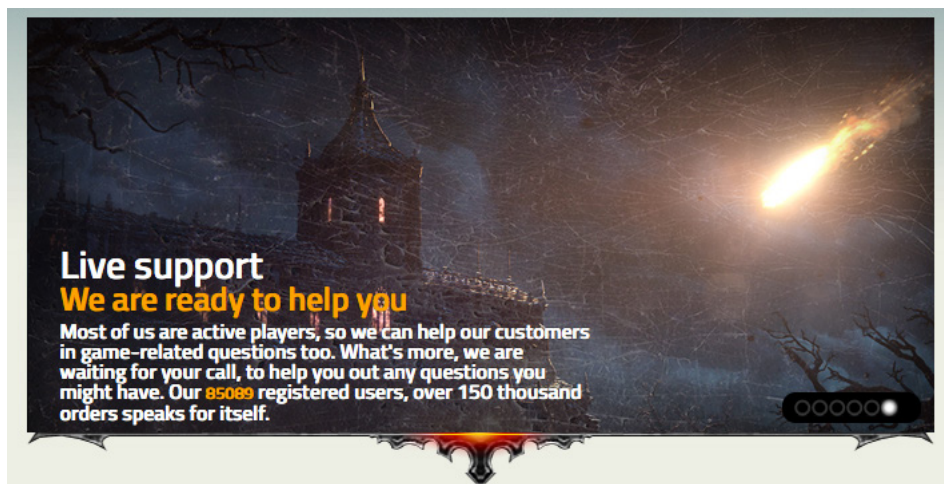


Figure 10. To stand out from the competition, some websites offer 24x7 live support while some boast of the number of clients and successful transactions made

Social Media

Social media sites, such as Facebook and Instagram, are used extensively to advertise and communicate with customers who are interested to purchase video gaming currency. Social media is also largely used as an advertising medium that can point visitors to the actual website selling the video gaming currency.

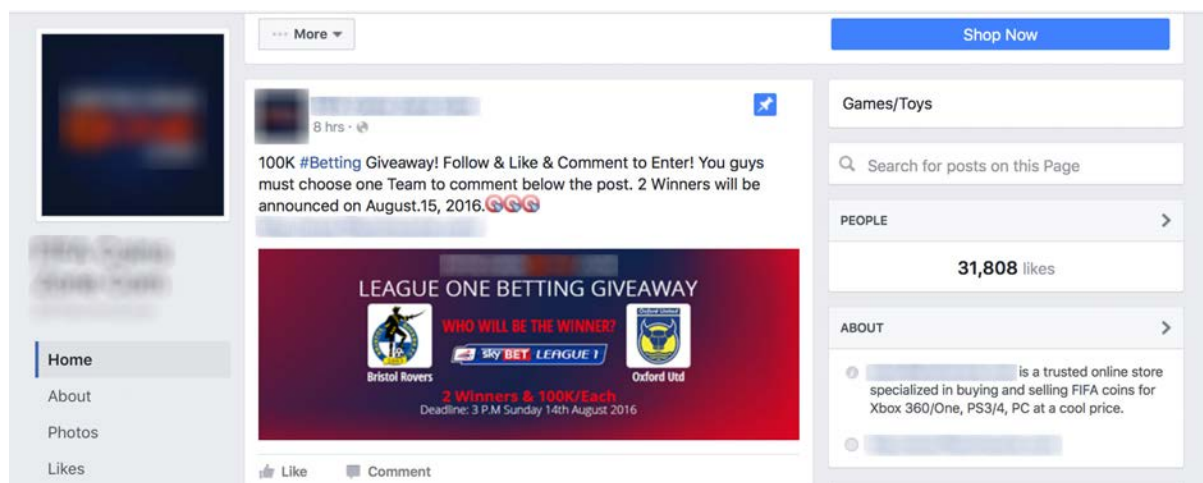


Figure 11. A Facebook page of a popular website selling video gaming currencies

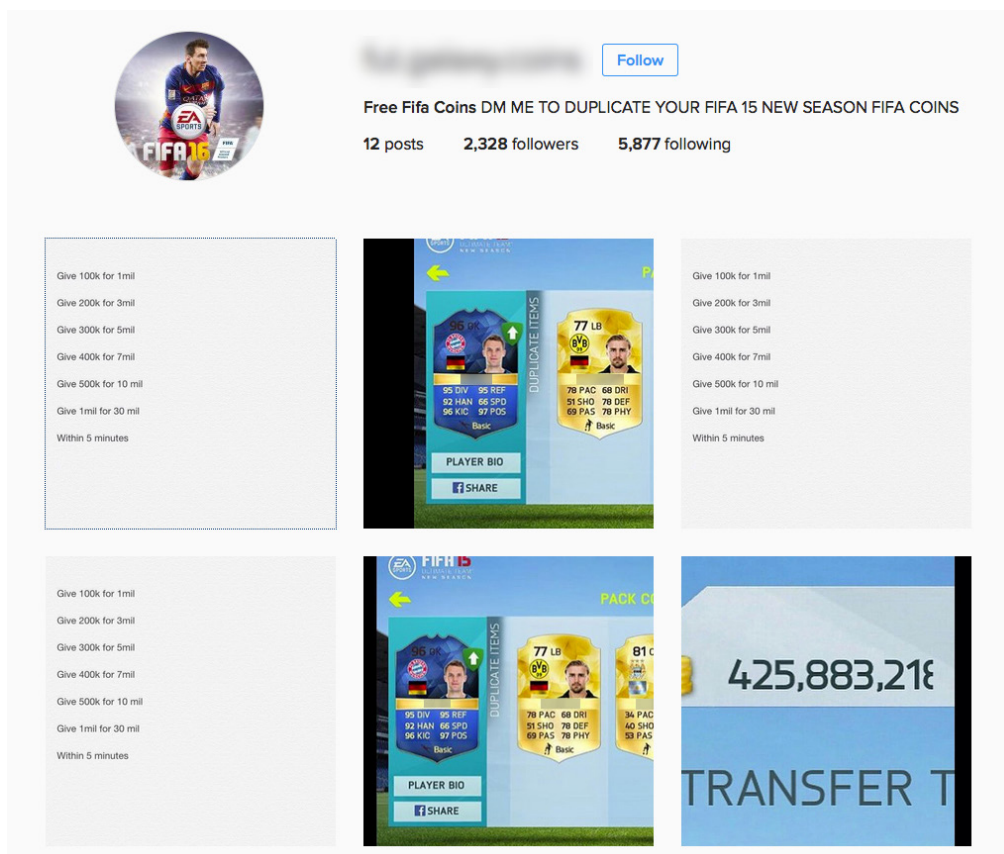


Figure 12. A sample of an advertisement on social media

Deep Web

For video games, the Deep Web is usually a place for cybercriminals to sell access to compromised game accounts or to sell other stolen information. Video game exploits and exploitation guides can also be purchased in markets found in the Deep Web.








	Game Hacking - Developing Autonomous Bots for Online Games	0.89 EUR	color (181 / -4)
	ALL NEW GAMES II PS4 ACCOUNT II INCREDIBLE PRICES!!	10.69 EUR	NEXTGAME (516)
	ALL OLD GAMES II PS4 ACCOUNT II INCREDIBLE PRICES!!	5.34 EUR	NEXTGAME (516)
	POKER Tracker 4 - Improve Your Online Poker Game	8.91 EUR	bank (2613)
	ALL NEW GAMES II PS3 ACCOUNT II INCREDIBLE PRICES!!	8.9 EUR	NEXTGAME (516)
	ALL OLD GAMES II PS3 ACCOUNT II INCREDIBLE PRICES!!	4.45 EUR	NEXTGAME (516)
	How to get steam games, Xbox live points, bitcoins, etc... for Fr	0.8 EUR	OnePiece (418)

Figure 13. Forums in the Deep Web selling access to game accounts

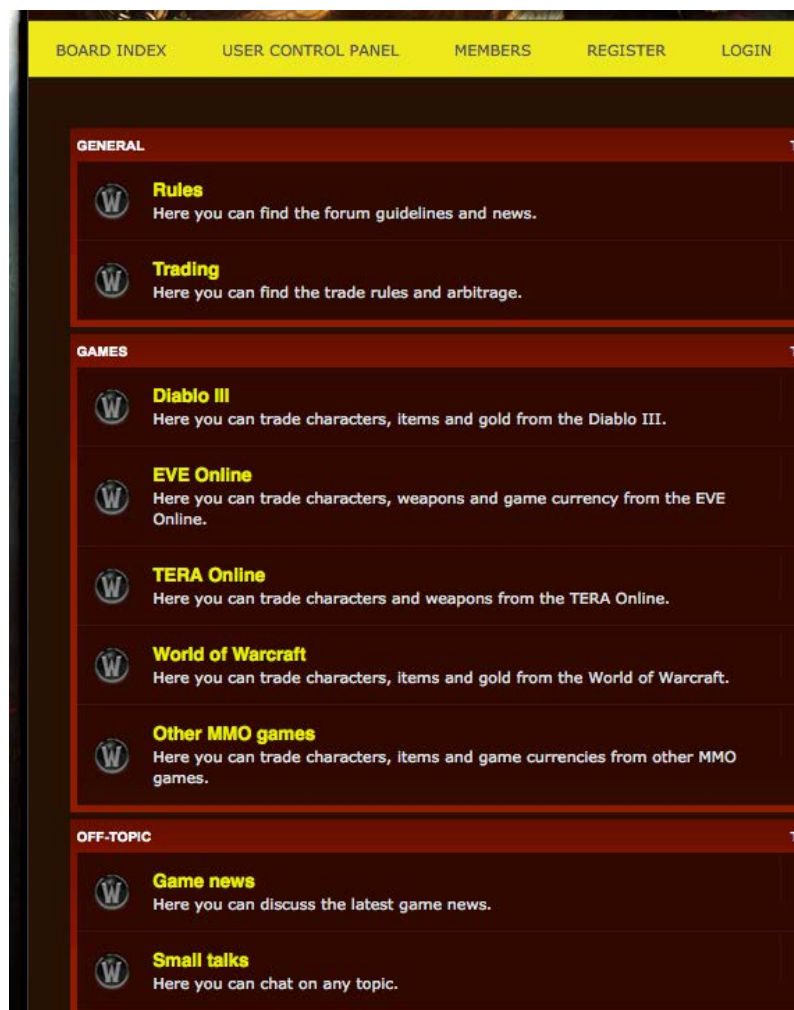


Figure 14. A forum in the Deep Web that is dedicated to selling and trading gaming currencies and virtual items

Selling Phase

To make a successful sale, the people behind the websites selling online gaming currencies must assure their customers that transactions with them are safe and secure. Therefore, websites go out of their way to make their customer, the online gamer, feel confident in completing their purchases. To do this website authors make sure that their site is professionally designed, offers live chat support, and declares the use of encryption software for all transactions.

Once a buyer has confirmed his/her purchase the process in obtaining the gaming currency is very similar to the usual process of purchasing items in any online shopping website. The process starts with the buyer logging in on the website, then selecting the amount and the type of currency he/she wishes to buy, and then confirming the sale by paying through various payment methods (credit card or online money transfers). After that, the buyer will simply have to wait for his/her purchase to be delivered.

Although majority of the process involving the sale of gaming currencies is similar to online shopping, there is a difference in the way purchased items are delivered to the buyers. Ordinarily, items purchased online are delivered directly to the buyer's doorstep. With gaming currencies, however, the buyer must log in on the game to receive the gaming currency that he/she just bought. Sometimes, the gaming currency is immediately credited to the buyer's account. Other ways to receive the purchased gaming currency would be through in-game communication systems or by receiving a rare or high-value item that is equivalent to the amount of gaming currency the buyer bought.

To better understand the process of purchasing gaming currency, refer to the image below (Fig.16) that shows the process of buying gaming currencies from the website, PlayerAuctions. In the same image, we can see that the website is using PlayerGuardian, an escrow-type of service that secures transactions between buyers and sellers.

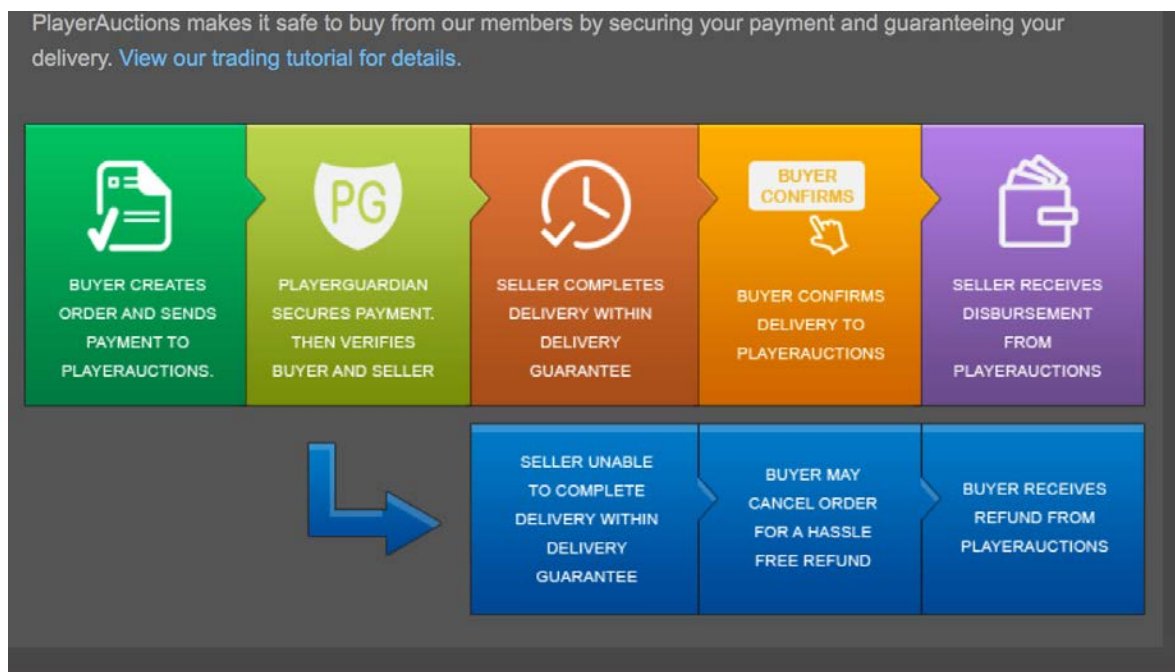


Figure 16. One website selling gaming currency that acts as the escrow during the transaction process. While this is common in Deep Web markets, it is uncommon to find such websites on the surface web.

TODAY'S SPECIALS







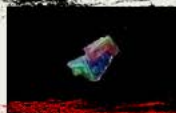

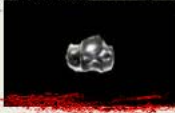



 <p>Betting Bundle with skins worth 100 USD Counter Strike CSGO Betting Bundle is used for betting on professional CSGO games for better profit.</p>	 <p>High-End Account - Ancient Quality Custom - Class of your choice Diablo 3 RoS Check our new Seasonal and Non-Seasonal High-End accounts with Normal or Ancient quality built characters. With these accounts you can easily play on higher greater rifts!</p>	 <p>60 000 Coins FIFA 16 Create your dream team with cheapest FIFA 16 coins. Available on PS4 and XBOX One too!</p>	 <p>Comfort Trade - 1 000 000 Coins FIFA 16 With this FIFA Comfort Trade we will trade the coins to your account while you don't have to put a single card for the Transfer Market.</p>
 <p>1000 Gold Guild Wars 2 You can always find the cheapest gw2 gold at us! Stock up and spend your gold on whatever you need!</p>	 <p>10 Exalted Orb Path of Exile Now in the one week league selection! Enchant your rare with a new random property with the most popular POE currency. Available on Tempest and Warbands too!</p>	 <p>100 Chromatic Orb Path of Exile Reforge the right color you need with these orbs for the success. Now on the Tempest and Warbands leagues!</p>	 <p>20 Orb of Fusing Path of Exile Don't like the sockets of your item? Reforge them with these Orbs! Available in Tempest and Warbands!</p>
 <p>40 Orb of Regret Path of Exile Buy Orb of Regret and reset your misplaced skill points with this Path of Exile orb.</p>	 <p>Catching 100 Pokemons Pokemon GO With this service we will catch 100 Pokemons in Pokemon GO for you. The Pokemons caught are random.</p>	 <p>Leveling 1-10 Pokemon GO Pokemon GO leveling within a few hours. Have you missed the start? No problem, we can help you catch up with your friends with this safe and quick Pokemon GO service.</p>	 <p>30 000 Gold WoW Stock up with the most popular WoW currency now on a discount price! Safe and face to face wow gold delivery!</p>

Figure 17. Special offers available on gaming marketplaces that entice would-be buyers with limited time sales

Despite the promise of untraceable transactions made with these websites, there is still significant risk to the online gamer whenever he/she purchases gaming currencies. This risk involves the suspension and/or termination of accounts that are caught participating in the trade of gaming currencies. However, despite this known risk, websites selling gaming currencies continue to flourish and rise in number.

If the idea of having accounts terminated don't seem to do much to curtail RMT, then perhaps knowing that purchasing gaming currencies from these websites could in turn fund cybercriminal activity would be more effective in shrinking the number of RMT.

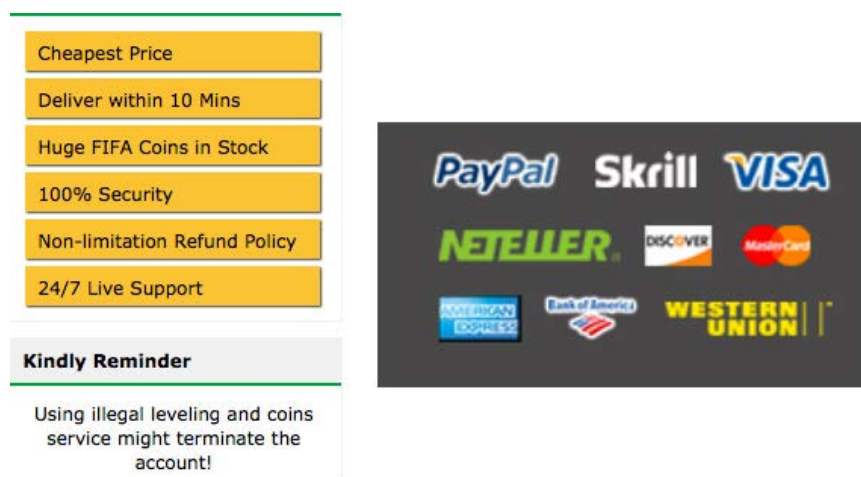


Figure 18. Accepted payment methods

Laundering Phase

Once the transaction is completed and the online gaming currency is transferred to the buyer, the cybercriminal now has real world money in his/her possession. At this point, the cybercriminal has a few available options to take to keep the newly obtained money away from the prying eyes of law enforcement.

Cryptocurrency Conversion

Cybercriminals often “clean” the currency, or remove traces of past transactions, by converting it to cryptocurrency. By doing this, the cybercriminal significantly reduces the chances of the original transaction being tracked or traced back to him/her.

After that, cybercriminals usually take the cleaning process one step further by letting the money go through cryptocurrency-cleaning services, which also “cleans” the cryptocurrency by mixing it with other cryptocurrencies from other sources, and thus effectively “erasing” the record of the original transaction.

they can find every transaction related to that wallet - where every amount of Bitcoin came from, and where it went to.

WHAT DOES CleanCoin DO

CleanCoin has an established reserve of Bitcoin from thousands of sources. When you use CleanCoin to mix your Bitcoins, you will receive Bitcoins that originate from lots and lots of different transactions and wallet addresses, making it almost impossible for someone to track your wallet activity.

GO CleanCoin

Enter the destination address for your transaction below:

Bitcoin address (e.g. 1DEyrG9XYNqpxdDgzc4kyCuMFFugFpM5Nv)

You may use this calculator to determine the fee that will be charged for your transaction. Note that any value entered is not submitted or locked in - the actual fee will be calculated from the exact amount that you send to CleanCoin.

Bitcoin amount

Fee: 0.000000 BTC.

0.000000 BTC will be sent to the destination address.

Go CleanCoin

Please note

Use of the CleanCoin service has the following fees:

0.5% of the total Bitcoin amount, and

0.001 BTC flat fee per transaction

How long does it take?

The entire CleanCoin service is automated. This means that once your transaction has been sent and confirmed, the system selects a block of Bitcoin to forward to your destination address. The process should take no longer than 1 hour, however if your transaction takes longer than usual to confirm, it may be processed manually - this can take up to 24 hours.

Any tips?

You don't have to send your Bitcoins to CleanCoin from the same address as your destination address - in fact, they **should be different**. By using different addresses, your Bitcoin transactions will be virtually *impossible* to trace. Other than that, sit back and relax while your Bitcoins are safely mixed. If you have any questions or concerns, feel free to [contact us](#).

Advertising, Investors and General Queries: [Contact Us](#)

Current Reserve: **More than >2370 BTC**

Figure 19. A sample of a website offering cryptocurrency laundering services, also known as the tumbling or mixing of coins



Figure 20. Another website offering cryptocurrency laundering services that's available on the Deep Web

Aside from converting the profit to cryptocurrency, the cybercriminal may also invest the money back into their operations, cash it out through bank accounts, shop for gift cards, and even procure gaming currencies in large quantities that they will resell later on in smaller batches at higher rates.

Incidental Profits

The profits a cybercriminal gains from selling a particular gaming currency does not end after the buyer claims his/her purchase. Depending on how the cybercriminal obtained the gaming currency, there is a chance that incidental profits can be made.

For example, if the cybercriminal used an infostealer or RAT to hack into a player’s account, then the cybercriminal can loot that account for other credentials or personal information, which can be sold to other cybercriminals.

Cybercriminals can also retain control of the hacked system and use it for malicious purposes, such as DDoS attacks, identity theft or fraud, and even for social engineering (like pretending to be the user/player and scamming the player’s contacts in the game).

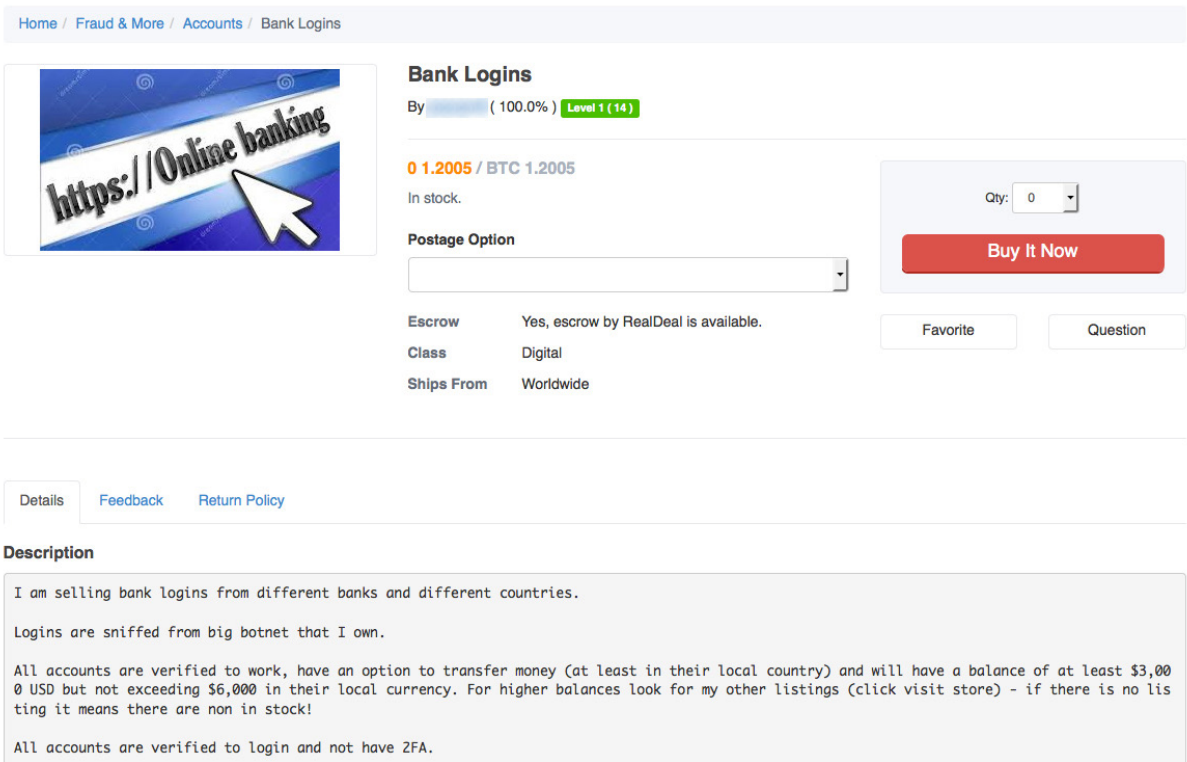


Figure 21. A forum in the Deep Web selling bank account credentials from a large botnet. Keep in mind that the botnet administrator can sell bank account credentials, video game account credentials, personally identifiable information, email credentials, website subscription credentials, private/confidential documents/pictures, etc. to maximize profitability from the botnet.

Fueling Traditional Cybercrime

Just like any business, expansion is a sign of growth. So once a cybercriminal has gained enough expertise and skills in harvesting gaming currencies, it won't be a surprise for that cybercriminal to begin exploring other areas of cybercrime soon.

After all, the skills used in harvesting gaming currencies—glitching/hacking larger servers, running phishing campaigns, spreading infostealing malware—are all applicable to other traditional forms of cybercrime. Based on our observation, some of the cybercriminal pursuits that are fueled from the profit of the sale of online gaming currencies are as follows, but not limited to: DDoS services, infrastructure rental (for cybercrime purposes), spam campaigns (which can result in ransomware infection), identity theft/fraud, and many others.

It is also important to note that selling various online gaming currencies is an effective method to launder real world money that is stolen or gained from other forms of cybercrime.

The Culprits Observed

To fully understand the serious implications of purchasing online gaming currencies from cybercriminals, it is essential to take a look at the cybercriminal activities that these groups are involved in. There is evidence that these threat actors used their ill-gotten gains to commit damaging forms of cybercrime. Some of these perpetrators are well-known gangs like Lizard Squad, Team Poison, Armada Collective, among others. These groups, funded by the profits gained from hacking online games, are capable of carrying out large-scale cyber attacks against corporations and other organizations.¹⁵

In 2015, Akamai reported a DDoS attack that targeted several companies in the financial sector. The perpetrator behind the attacks is the hacking group from Saudi Arabia known as OurMine, which started out as a group that claimed to be efficient in hacking the games *Minecraft* and *FIFA*. Soon after, the group quickly became infamous when they began giving away stolen *FIFA* coins and *Minecraft* hacks to a large number of followers on various social media platforms like Instagram, Twitter, and Facebook.

As the group's fame grew, OurMine began to broadcast its hacking skills to other gamers by inviting the public to their websites and chatrooms to learn how to hack games. As the team's activities garnered the attention of wider audiences, OurMine began making their attacks more sophisticated. They also went ahead in widening the scope of their attacks by targeting companies in the financial industry.

The team also carried out a large DDOS attack campaign against a number of companies from other industries. Some of these attacks involved compromising *Minecraft* game servers, *Pokemon Go* servers, video game console online services, Wikileaks, and even other groups involved in hacking games.

OurMine's fame, however, came with a price as the group was soon attacked by several hacking groups such as LizardSquad, Anonymous, and TTD. The attacks that were carried out against OurMine involved DDoS attacks as well as "doxxing", which is the public release of a server's personally-identifiable information (PII). As a result, OurMine took down all their related social media accounts, websites, and accounts that may carry the PII that was dumped.

Later on, the groups that attacked OurMine claimed that the attacks they launched were a form of retaliation against OurMine's initial attacks on other gaming services. For those groups, this was a simple form of hacktivism against OurMine.

Despite such attacks, OurMine was resilient. Recently the group came back and rebranded themselves as security professionals offering penetration testing and social account security testing. Aside from a new image, OurMine continued to refine its DDoS capabilities—as shown by the recent hacks they made to the social media accounts of a few notable personalities, like the CEOs of Facebook, Google, and Twitter.¹⁶

The Impact of Online Gaming Currency Laundering

As recent attacks showed, cybercriminal activities have serious and far-reaching implications. Not only can such attacks disrupt normal operations in any organization, but these attacks can also put people's lives at risk. There are a vast number of ways victims of cyber attacks are affected—corporate hacking and DDoS attacks are just one of those ways. In fact, one of the more serious effects of the illegal harvesting of online gaming currencies is the presence of forced labor that is funded and supported by the profits gained from such an activity.

Gaming Companies

Game developers and publishers are the primary victims of the illegal acquisition of gaming currencies. In any game, players invest a certain amount of trust in the game—which revolves around the belief that advancement in the game is done in a fair method. Therefore, this trust is shattered when players learn about the prevalence of RMT for gaming currency. Upon learning that, players may opt to abandon the game completely. This reaction shall immediately translate into a huge loss of revenue for the game publishers and developers.

To inhibit the proliferation of RMT, gaming companies work very hard to implement different tactics to prevent such abuses. Some of these methods involve having their staff patrol the game and launch a system wherein other gamers can report similar abuses. Despite that, however, cybercriminals hacking game accounts to harvest gaming currencies continue to rise in number.

Corporations and Enterprises

While corporations and enterprises may not be directly affected by cyber attacks on games, the funds received from the sale of ill-gotten gaming currencies are often used to support other cybercriminal activities that will or may target said corporations and enterprises. Such an effect is evident in the attacks made by the hacking group OurMine against several private corporations.

Children / Teens

For the majority of children and teens, the goal of gaming is to simply enjoy the game. To do that, they search for a way to become stronger and more powerful in the fastest way possible. This particular desire of getting ahead fast is what makes children and/or teens targets of cybercriminals. Cybercriminals also make it easy to lure children and teens to cheat by promoting ads and videos that show them how to get free credit online.

Once these children or teens take the bait, it is more likely that they will be reaching out to these cybercriminals again after discovering how easy it is to get what they want by simply paying up. The concept of supporting such trade of ill-gotten gaming currencies promotes cybercrime is foreign to them. For these children or teens, availing of such a service is just a simple extension of their gaming experience.

Involuntary Human Workers

With the high demand for gaming currency, there is now an emergence of sweatshops that are capable of generating gaming currency that will be resold online.¹⁷

Just like the typical sweatshops in other industries, these gaming currency farmers are forced to work for long hours with very little pay—or none at all—and are exposed to poor working conditions. One evidence of such a sweatshop is when labor camp prisoners in China were forced to play online games for hours on end in order to farm online ‘gold’.¹⁸

Conclusion

Today, as more people choose to do business online, the preference for virtual currency systems will continue to grow. With virtual currencies, users are allowed to move their money in a quick and efficient manner without having to worry about distance and exorbitant fees. The utilization of virtual currency also provides its patrons increased privacy in their transactions and the absence of an intercessor.

Although virtual currency is not inherently illegal, the fact that virtual currency systems functions with privacy and anonymity in mind makes it an ideal medium for cybercriminals to conduct illicit activities. Due to the likelihood of virtual currency systems being exploited by malicious actors, law enforcement has been keeping a close eye on businesses or individuals who use virtual currency to launder money gained from any illegal venture.¹⁹ There are numerous ways for cybercriminals to launder their ill-gotten wealth. One of the more popular ways cybercriminals hide or bury their money today is through the sale of online gaming currencies.

As the gaming industry is growing, the trade of online gaming currencies will remain relevant to players and cybercriminals as well. For the cybercriminals, the profits derived from the sale of online gaming currencies are simply used to fund their operations. In the basic sense, buying and selling online gaming currencies is not illegal. Players should, however, practice caution in participating in such an exchange since they may, after all, be financing cybercriminal acts that will have devastating real-world implications.

References

1. Newzoo. (21 April 2016). *Newzoo*. "The Global Games Market Reaches \$99.6 Billion in 2016, Mobile Generating 37%." Last accessed on 29 September 2016, <https://newzoo.com/insights/articles/global-games-market-reaches-99-6-billion-2016-mobile-generating-37>.
2. Chris Morris. (16 February 2016). *Fortune*. "Level up! Video Game Industry Revenues Soar in 2015." Last accessed on 29 September 2016, <http://fortune.com/2016/02/16/video-game-industry-revenues-2015>.
3. Entertainment Software Association. (n.d.). *Essential Software Association*. "Essential Facts About the Computer and Video Game Industry." Last accessed on 29 September 2016, <http://essentialfacts.theesa.com/Essential-Facts-2016.pdf>.
4. Blizzard Entertainment. (n.d.) *Blizzard Entertainment*. "WoW Token." Last accessed on 05 October 2016, <https://us.battle.net/shop/en/product/world-of-warcraft-token>
5. Riot Games. (13 July 2009). *Riot Games*. "League of Legends' Currency Explained." Last accessed on 05 October 2016, <http://www.riotgames.com/articles/20090713/254/league-legends-currency-explained>
6. Dan Crawley. (19 March 2014). *VentureBeat*. "Meet the Gamers Who Earned Big in the Now-Closed Diablo III Real-Money Auction House." Last accessed on 29 September 2016, <http://venturebeat.com/2014/03/19/meet-the-gamers-who-earned-big-in-the-now-closed-diablo-iii-real-money-auction-house/>.
7. Paul Tassi. (18 March 2014). *Forbes*. "'Diablo 3' Finally Exorcises Its Demon, The Auction House." Last accessed on 13 September 2016, <http://www.forbes.com/sites/insertcoin/2014/03/18/diablo-3-finally-exorcises-its-demon-the-auction-house/>.
8. Mike Schramm. (28 March 2013). *Engadget*. "Diablo 3 Director Jay Wilson: Auction Houses 'really hurt' Game." Last accessed on 29 September 2016, <https://www.engadget.com/2013/03/28/diablo-3-director-jay-wilson-auction-houses-really-hurt-game/>.
9. Jessica Conditt. (19 April 2016). *EndGadget*. "'World of Warcraft' Keeps Growing with 'Legion' in August." Last accessed on 26 September 2016, <https://www.engadget.com/2016/04/19/world-of-warcraft-legion-release-date/>.
10. Entertainment Software Association. (n.d.). *Essential Software Association*. "2015 Annual Report: A Year of Innovation and Achievement." Last accessed on 30 September 2016, <http://www.theesa.com/wp-content/uploads/2016/04/ESA-Annual-Report-2015-1.pdf>
11. Samuel Steiner (n.d.) *Hackerbot*. "Is Cheating/ Cheating/Hacking/Botting in Online Games and Shooters Legal/ Against any Laws?" Last accessed on 13 September 2016, <https://hackerbot.net/blog/27-game-cheating/228-cheat-hack-bot-illegal-legal-law-question>.
12. Billy D. (20 April 2016). *One Angry Gamer*. "New Division Glitch Allows for Massive DPS Damage and Money Rewards". Last accessed on 4 October 2016, <http://www.oneangrygamer.net/2016/04/new-division-glitch-allows-for-massive-dps-damageand-money-rewards/1533/>

13. David Barboza. (9 December 2005). *The New York Times*. "Ogre to Slay? Outsource It to Chinese." Last accessed on 06 October 2016, <http://www.nytimes.com/2005/12/09/technology/ogre-to-slay-outsource-it-to-chinese.html>.
14. Danny Vincent. (25 May 2011). *Guardian*. "China Used Prisoners in Lucrative Internet Gaming Work." Last accessed on 13 September 2016, <https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam>.
15. Bill Brenner. (29 July 2015). *Akamai*. "OurMine Team Attack Exceeded 117 Gbps." Last accessed on 14 September 2016, 31 | The Cybercriminal Roots of Selling Online Gaming Currency <https://blogs.akamai.com/2015/07/ourmine-team-attack-exceeded-117-gbps.html>.
16. Mary Pascaline. (18 July 2016). *IBTimes*. "'Pokemon Go' Servers Brought Down by OurMine DDoS Attack." Last accessed on 12 September 2016, <http://www.ibtimes.com/pokemon-go-servers-brought-down-ourmine-ddos-attack-2392273>.
17. John R. (17 March 2016). *The Online Economy*. Outsourcing Fun: Gold Farming & the Rise of Digital Sweatshops." Last accessed on 29 September 2016, <https://onlineeconomy.hbs.org/submission/outsourcing-fun-gold-farming-the-rise-of-digital-sweatshops/>.
18. Malcolm Moore. (26 May 2011). *Telegraph*. "Chinese Labour Camp Prisoners Forced to Play Online Games." Last accessed on 29 September 2016, <http://www.telegraph.co.uk/technology/news/8537467/Chinese-labour-camp-prisoners-forced-to-play-online-games.html>.
19. Brett Nigh, J.D. and C. Alden Pelker. (08 September 2015). *The Federal Bureau of Investigation*. "Virtual Currency: Investigative Challenges and Opportunities." Last accessed on 14 September 2016, <https://leb.fbi.gov/2015/september/virtual-currency-investigative-challenges-and-opportunities>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com