Cheats, Hacks, and Cyberattacks

Threats to the Esports Industry in 2019 and Beyond

Mayra Rosario Fuentes and Fernando Mercês

TREND MICRO | research

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.

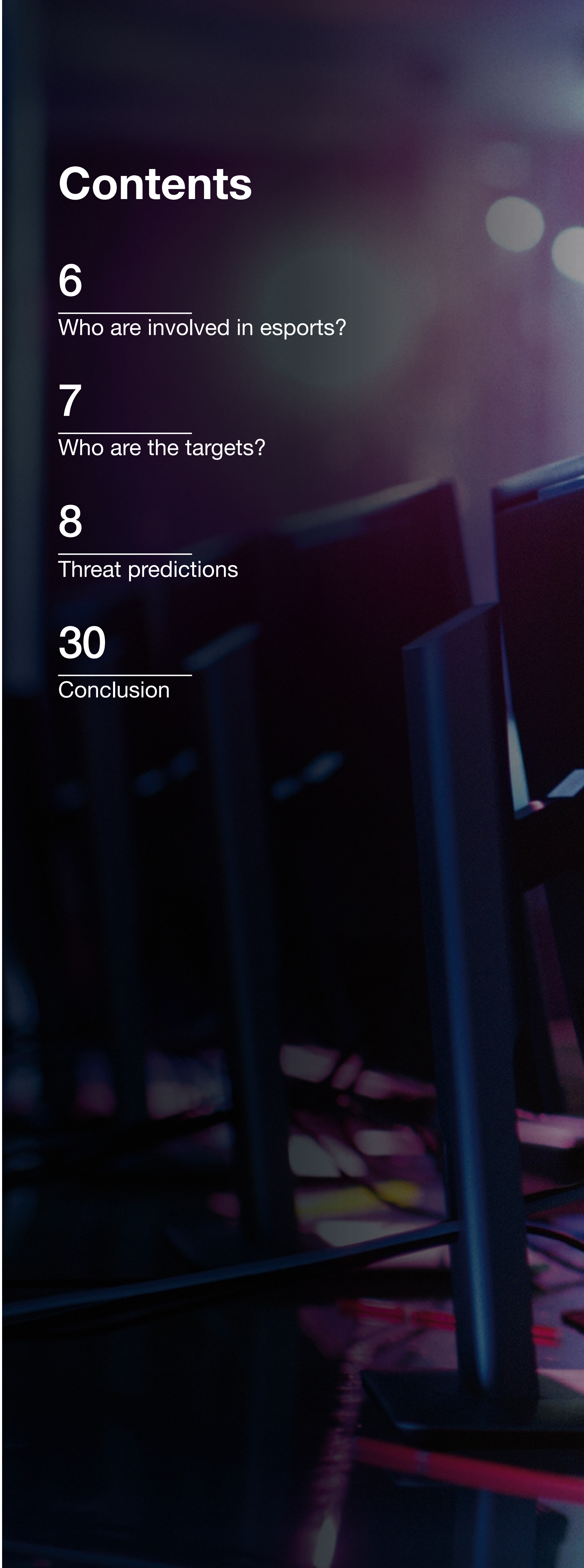
Published by
Trend Micro Research

Written by
Mayra Rosario Fuentes and Fernando Mercês

With contributions by
Ahmed Kamal Aly, Vladimir Kropotov, and Ariane Parra

Stock image used under license from Shutterstock.com

For Raimund Genes (1963-2017)



Contents

6
Who are involved in esports?

7
Who are the targets?

8
Threat predictions

30
Conclusion

Electronic sports, more commonly called esports, is positioned to be a billion-dollar industry in 2019, buoyed by growing ad revenues, sponsorships, media rights, and viewership.[1] Events that previously catered to a niche market are now considered mainstream entertainment, with major esports tournaments held in full-sized stadiums and fans coming in from all over the world. Cash prizes from these competitions are also increasing.[2] The total prize money for esports competitions reached $150.8 million in 2018 — a significant increase from the $112.1 million prize pool in 2017.[3] In 2019, The International 9, the largest Dota 2 tournament of the year, awarded more than US$30 million in prizes, taking the record for awarding the largest prize pool for a single esports event.[4]

Several universities in the United States and the United Kingdom have also started offering esports programs for those who want to enter the field, further legitimizing it as a viable career for young adults.[5] This progress shows how esports has evolved past being just entertainment; these hugely popular gaming competitions are now a thriving business. However, as an industry grows and becomes more lucrative, those who are involved in the business also become more attractive cybercrime targets.

Esports titles are individual or team-based games that are played worldwide in leagues or tournaments on PCs, gaming consoles, and mobile devices throughout the year. The competitions are typically watched by live audiences, and streamed on video platforms like Twitch and YouTube. In the United States, ESPN and TBS have broadcasted esports tournaments on cable networks. Viewership for these competitions has reached all-time highs — the 2018 League of Legends World Championship had 1.9 million peak viewers, logging a total of 78.8 million hours watched.[6]

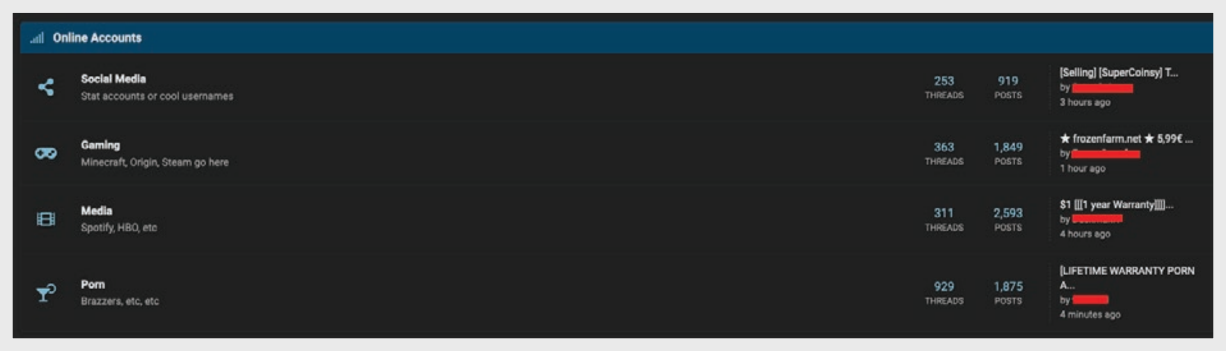
A study done by Syracuse University predicts that esports viewership will compete with — and even surpass — traditional sporting events by 2021. Their data projects that esports in the U.S. will have more viewers than every professional sports league but the NFL.[7]

The esports industry is a fast emerging target because the systems and infrastructure around it are still maturing. Its increasing popularity is also pulling in more investors and sponsors— and where there is money to be made, cybercriminals will predictably turn up.

Large cash prizes can motivate unscrupulous players to look for an unfair advantage over other players, which in turn creates a market for game cheats in the underground. These competitions also bring out underground entities looking to take advantage of esports for political, financial, or ideological reasons. Possible attacks can involve distributed denial of service (DDoS) and ransomware attacks, zero-day exploits, data breaches, supply chain attacks, and targeted malware. The lucrative esports market also attracts cybercriminals involved in illegal gambling and online bookmaker services.

These attacks can lead to identity theft, financial loss, and reputational damage to business advertisers and sponsors (major brands, like Coca-Cola, Intel, Nissan, ESPN, ABC, Disney, Red Bull and Mercedes-Benz, have all been involved with esports).

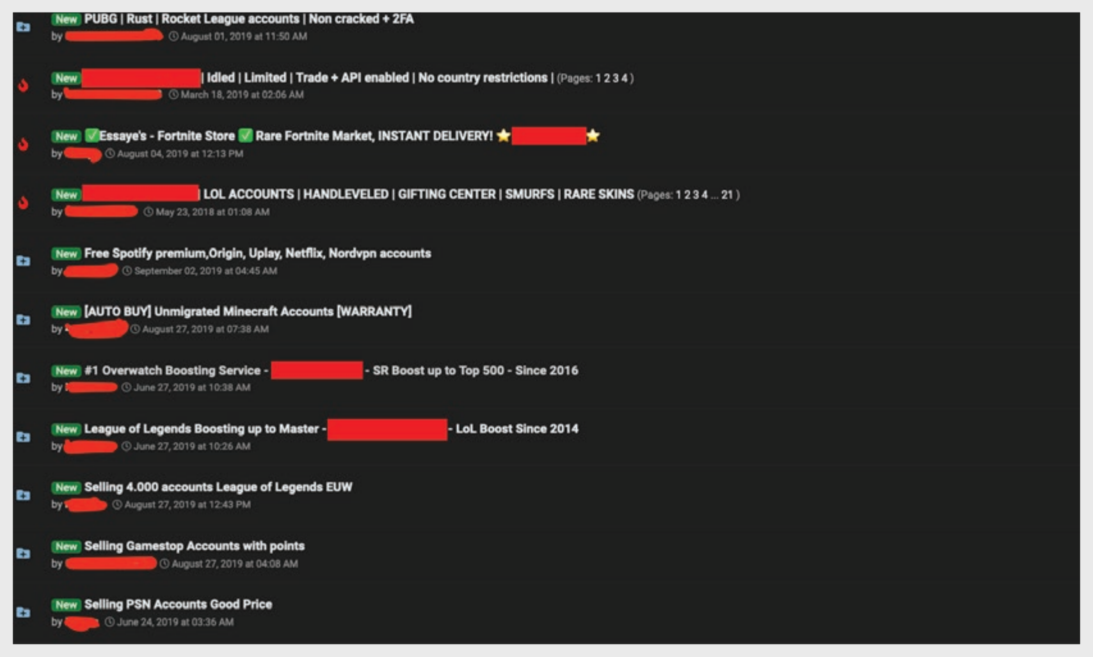
We predict that cybercriminals will increasingly target the esports industry over the next three years. Many cybercriminal underground forums already have sections dedicated to gaming or esports sales. The market for stolen gaming accounts and hacks are flooded, much like the market for stolen credit card accounts.



Online Accounts

Social Media Stat accounts or cool usernames	253 THREADS	919 POSTS	[Selling] [SuperCoinsy] T... by [redacted] 3 hours ago
Gaming Minecraft, Origin, Steam go here	363 THREADS	1,849 POSTS	★ frozenfarm.net ★ 5,99€ ... by [redacted] 1 hour ago
Media Spotify, HBO, etc	311 THREADS	2,593 POSTS	$1 [[[1 year Warranty]]]... by [redacted] 4 hours ago
Porn Brazzers, etc, etc	929 THREADS	1,875 POSTS	[LIFETIME WARRANTY PORN A... by [redacted] 4 minutes ago

Figure 1. Underground Forum with a dedicated section for the sale of gaming accounts



New PUBG | Rust | Rocket League accounts | Non cracked + 2FA
by [redacted] August 01, 2019 at 11:50 AM

New [redacted] | Idled | Limited | Trade + API enabled | No country restrictions | (Pages: 1 2 3 4)
by [redacted] March 18, 2019 at 02:06 AM

New ✓Essaye's - Fortnite Store ✓ Rare Fortnite Market, INSTANT DELIVERY! ⭐[redacted]⭐
by [redacted] August 04, 2019 at 12:13 PM

New [redacted] | LOL ACCOUNTS | HANDLEVELED | GIFTING CENTER | SMURFS | RARE SKINS (Pages: 1 2 3 4 ... 21)
by [redacted] May 23, 2018 at 01:08 AM

New Free Spotify premium,Origin, Uplay, Netflix, Nordvpn accounts
by [redacted] September 02, 2019 at 04:45 AM

New [AUTO BUY] Unmigrated Minecraft Accounts [WARRANTY]
by [redacted] August 27, 2019 at 07:38 AM

New #1 Overwatch Boosting Service - [redacted] - SR Boost up to Top 500 - Since 2016
by [redacted] June 27, 2019 at 10:38 AM

New League of Legends Boosting up to Master - [redacted] - LoL Boost Since 2014
by [redacted] June 27, 2019 at 10:26 AM

New Selling 4.000 accounts League of Legends EUW
by [redacted] August 27, 2019 at 12:43 PM

New Selling Gamestop Accounts with points
by [redacted] August 27, 2019 at 04:08 AM

New Selling PSN Accounts Good Price
by [redacted] June 24, 2019 at 03:36 AM

Figure 2. Underground offerings related to esports

The gaming community has long been a target for cybercriminals who have since made a slight shift to go after the growing esports industry. These threat actors have found different ways to monetize hacks for various esports activities, and these items are gaining popularity. For example, since 2018, gaming-related advertisements have increased by 40% in underground markets where gaming accounts and credit card accounts are sold. Cheats can be purchased for as little as US$20 from multiple online forums, while custom-made hacks can go for much higher, as these are designed to be more difficult to detect during professional tournaments. While anti-cheat and account-banning technologies exist for most competitive game titles, certain high-profile incidents have proven that players are willing to risk their accounts and reputations to win thousands in prize money.

Who are involved in esports?

The target base for esports includes game developers, sponsors, viewers, and players. We are particularly concerned about threats to esports players in the U.S., as it's the country with the most active competitors. According to a report by Statista, the U.S. has the most number of active esports players, which is almost triple the number of players in the country coming in second, South Korea.[8]

On the other hand, the number of esports viewers is higher in Asia. A 2019 report by Statista[9] shows that 57% of frequent viewers and enthusiasts resided in the Asia Pacific region. This leads us to believe these two regions will be the most targeted in the future.

- The U.S. had more active competition players, followed by China and Korea, each with over 1 thousand active esports players.[10]
- China has the largest esports revenue market.
- The Chinese city of Hangzhou, which will host the 2022 Asian Games, features an esports academy, a themed hotel, theme park, business center, and a hospital designed for esports players.[11]

In addition, esports appears to be growing rapidly in the Middle East, with the United Arab Emirates (UAE) constructing the region's first dedicated esports venue: the Dubai X-Stadium. The rise of esports in the MENA region is due to high internet and smartphone penetration rates. The video game industry in the Middle East is estimated to be worth more than $1 billion annually, and is expected to increase to $4.4 billion by 2022. The UAE, Jordan, and Syria are the first Arab countries to participate in The International 9 Dota 2 qualifiers in 2019.[12]

Other regions also have a significant presence in this market. In 2018, Brazil had 11.4 million viewers, accounting for almost half of the esports viewing audience in Latin America.[13] The Russian government officially recognized esports in 2016 as a sporting discipline; 38% of the online Russian population watch gaming video content. Russia's gaming market reportedly reached 1.8 billion in 2018, with 65.2 million players.[14] In 2018, Japan had 67.6 million gamers, with the majority playing on mobile platforms.[15]

Who are the targets?

This research paper discusses the predicted threat landscape of the esports industry based on current and emerging threats and rising market trends. We will cover threats against online game developers, businesses that sponsor and organize tournament events, individual gamers, stream viewers, and event attendees.

Before we start with our threat predictions, let's define the different parties or roles that make up the esports industry:

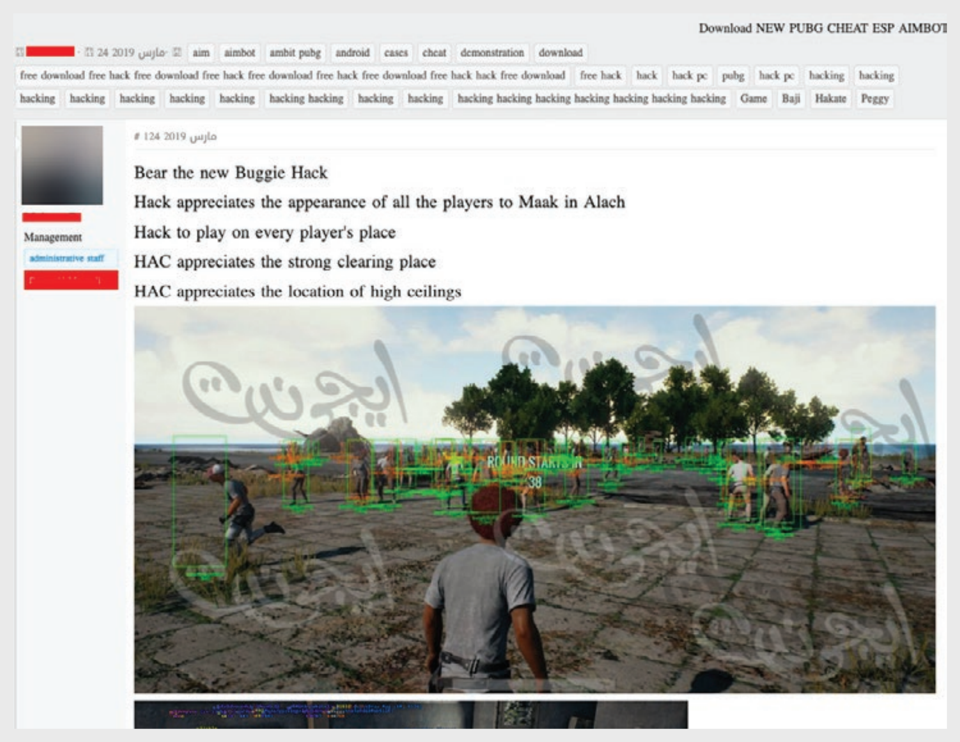
- **Game developers/publishers –** Companies, such as Valve Corporation (Dota 2) and Riot Games (League of Legends), that develop and release games
- **Gamers –** The people who play videos games casually or professionally
- **Professional players –** Competitive players paid by sponsors or teams to play a game.
- **Professional teams –** A team or franchise backed by an owner, comprised of players and coaches that usually receive a contract, health benefits, and a full-time salary
- **Leagues** – A franchise approach based on North American professional sports wherein teams compete in regular season matches to qualify for post-season "elite" competitions
- **Sponsors –** Companies that sponsor teams, events, prizes, etc.
- **Advertisers –** Companies that advertise products and services in the events
- **Attendees** – The audience for esports events, which can pertain to physical event attendees or viewers of online streaming platforms like Twitch or YouTube.

The section below covers the threats that target the abovementioned parties.

Threat predictions

Cheats and hacking services will flourish underground

As esports revenues and tournament prizes continue to increase, unscrupulous players will look for opportunities to exploit the game to gain an advantage over competitors. A quick search for hacks on cybercriminal underground forums reveals hundreds of *aimbots* and *wallhacks* — essentially cheat tools prohibited in official competitions for sale. Aimbots are a type of software used in multiplayer first-person shooter games to provide varying levels of automated targeting that gives the user an advantage over other players. Wallhacks allow the player to change the properties of in-game walls by making them transparent or nonsolid, making it easier to locate or attack enemies. Prices for such tools start at US$5, but we found an aimbot being sold for $1,500.



Download NEW PUBG CHEAT ESP AIMBOT

[redacted] · 24 2019 مارس · aim aimbot ambit pubg android cases cheat demonstration download free download free hack free download free hack free download free hack free download free hack hack free download free hack hack hack pc pubg hack pc hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking hacking Game Baji Hakate Peggy

124 2019 مارس

[redacted]

Management

administrative staff

[redacted]

Bear the new Buggie Hack

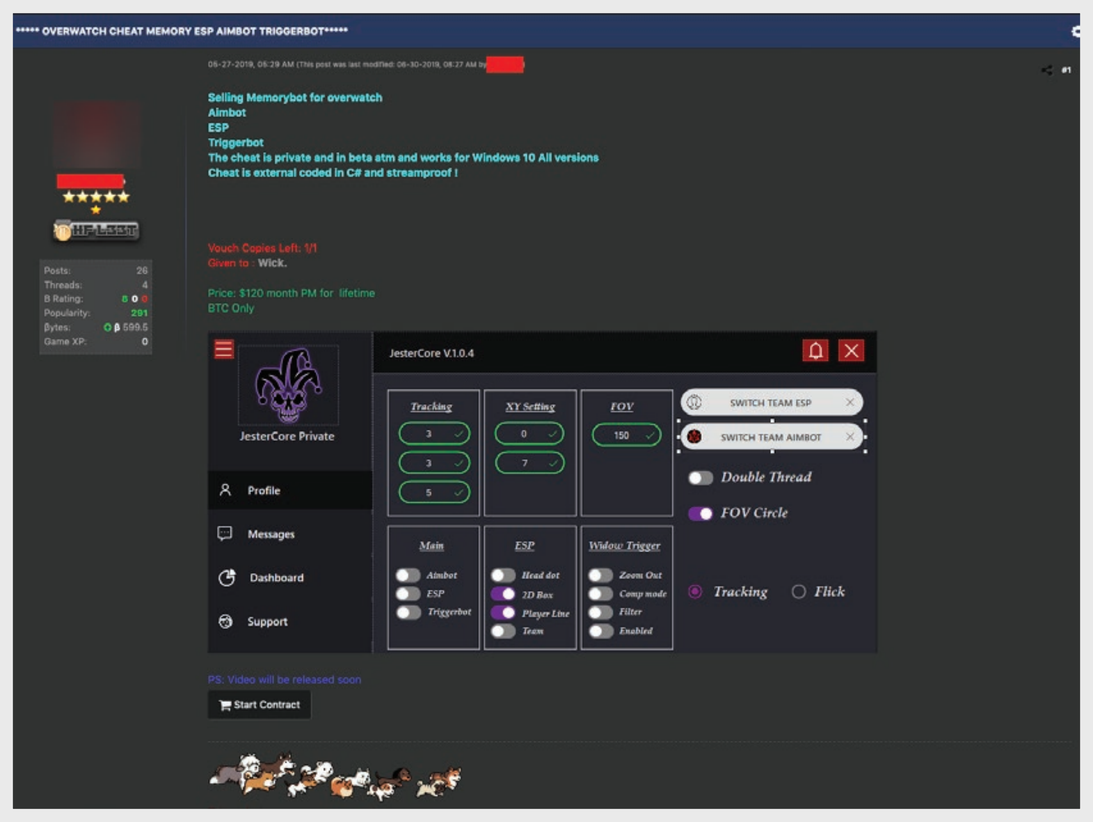
Hack appreciates the appearance of all the players to Maak in Alach

Hack to play on every player's place

HAC appreciates the strong clearing place

HAC appreciates the location of high ceilings

Figure 3. A post on an Arabic forum offering a free aimbot for PUBG, with a download link to a Russian website



***** OVERWATCH CHEAT MEMORY ESP AIMBOT TRIGGERBOT*****

[redacted]

Posts: 26
Threads: 4
B Rating: 8 0 0
Popularity: 291
βytes: β 599.5
Game XP: 0

06-27-2019, 05:29 AM (This post was last modified: 06-30-2019, 08:27 AM by [redacted])

Selling Memorybot for overwatch
Aimbot
ESP
Triggerbot
The cheat is private and in beta atm and works for Windows 10 All versions
Cheat is external coded in C# and streamproof !

Vouch Copies Left: 1/1
Given to : Wick.

Price: $120 month PM for lifetime
BTC Only

JesterCore V.1.0.4

JesterCore Private

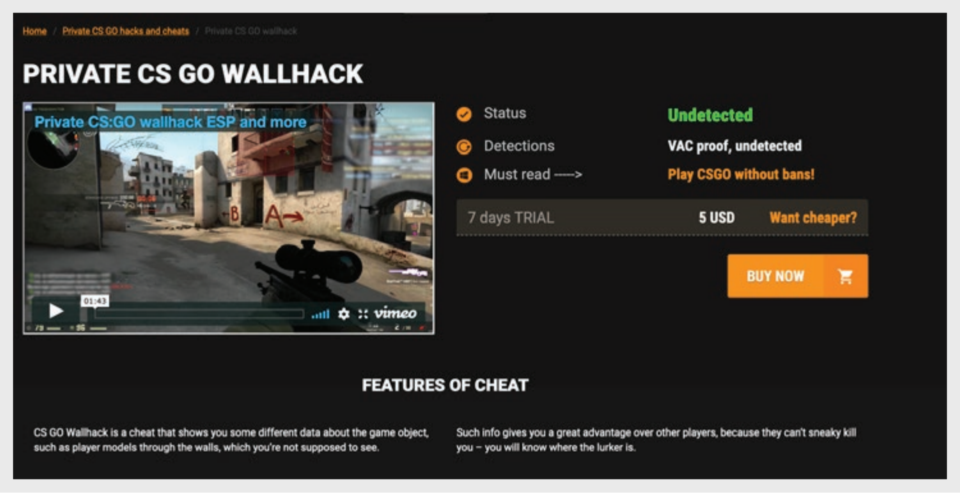
Tracking: 3, 3, 5
XY Setting: 0, 7
FOV: 150

Main: ○ Aimbot, ○ ESP, ○ Triggerbot
ESP: ○ Head dot, ● 2D Box, ● Player Line, ○ Team
Widow Trigger: ○ Zoom Out, ○ Comp mode, ○ Filter, ○ Enabled

○ Double Thread
● FOV Circle
● Tracking ○ Flick

PS: Video will be released soon

Figure 4. An advertisement for a private cheat for Overwatch



Home / Private CS GO hacks and cheats / Private CS GO wallhack

PRIVATE CS GO WALLHACK

Status: Undetected
Detections: VAC proof, undetected
Must read ----> Play CSGO without bans!

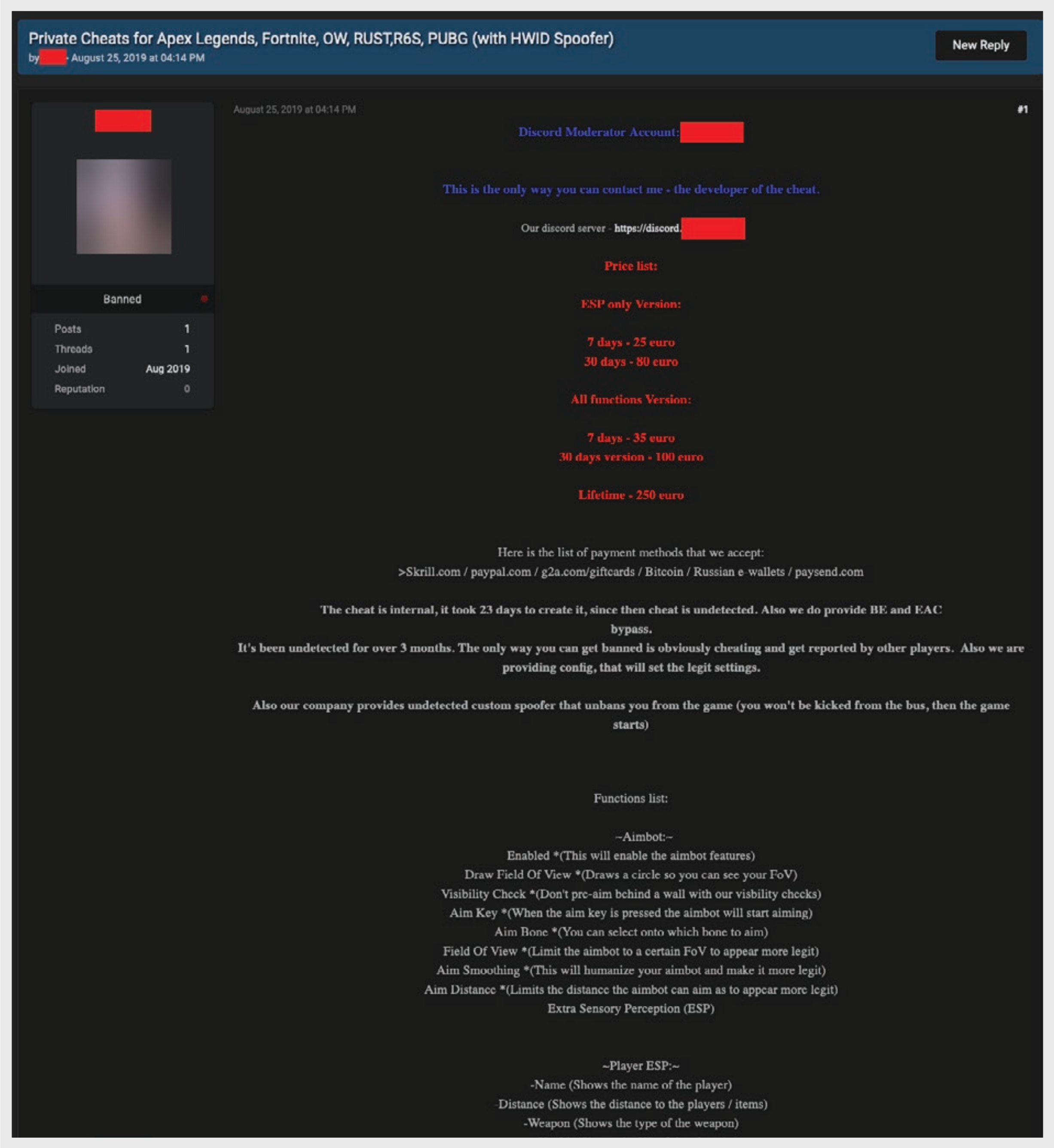
7 days TRIAL 5 USD Want cheaper?

FEATURES OF CHEAT

CS GO Wallhack is a cheat that shows you some different data about the game object, such as player models through the walls, which you're not supposed to see.

Such info gives you a great advantage over other players, because they can't sneaky kill you – you will know where the lurker is.

Figure 5. A page selling a private wallhack



Private Cheats for Apex Legends, Fortnite, OW, RUST,R6S, PUBG (with HWID Spoofer)

by [redacted] - August 25, 2019 at 04:14 PM

[redacted]

Banned

Posts	1
Threads	1
Joined	Aug 2019
Reputation	0

August 25, 2019 at 04:14 PM

#1

Discord Moderator Account: [redacted]

This is the only way you can contact me - the developer of the cheat.

Our discord server - https://discord.[redacted]

Price list:

ESP only Version:

7 days - 25 euro
30 days - 80 euro

All functions Version:

7 days - 35 euro
30 days version - 100 euro

Lifetime - 250 euro

Here is the list of payment methods that we accept:
>Skrill.com / paypal.com / g2a.com/giftcards / Bitcoin / Russian e-wallets / paysend.com

The cheat is internal, it took 23 days to create it, since then cheat is undetected. Also we do provide BE and EAC bypass.
It's been undetected for over 3 months. The only way you can get banned is obviously cheating and get reported by other players. Also we are providing config, that will set the legit settings.

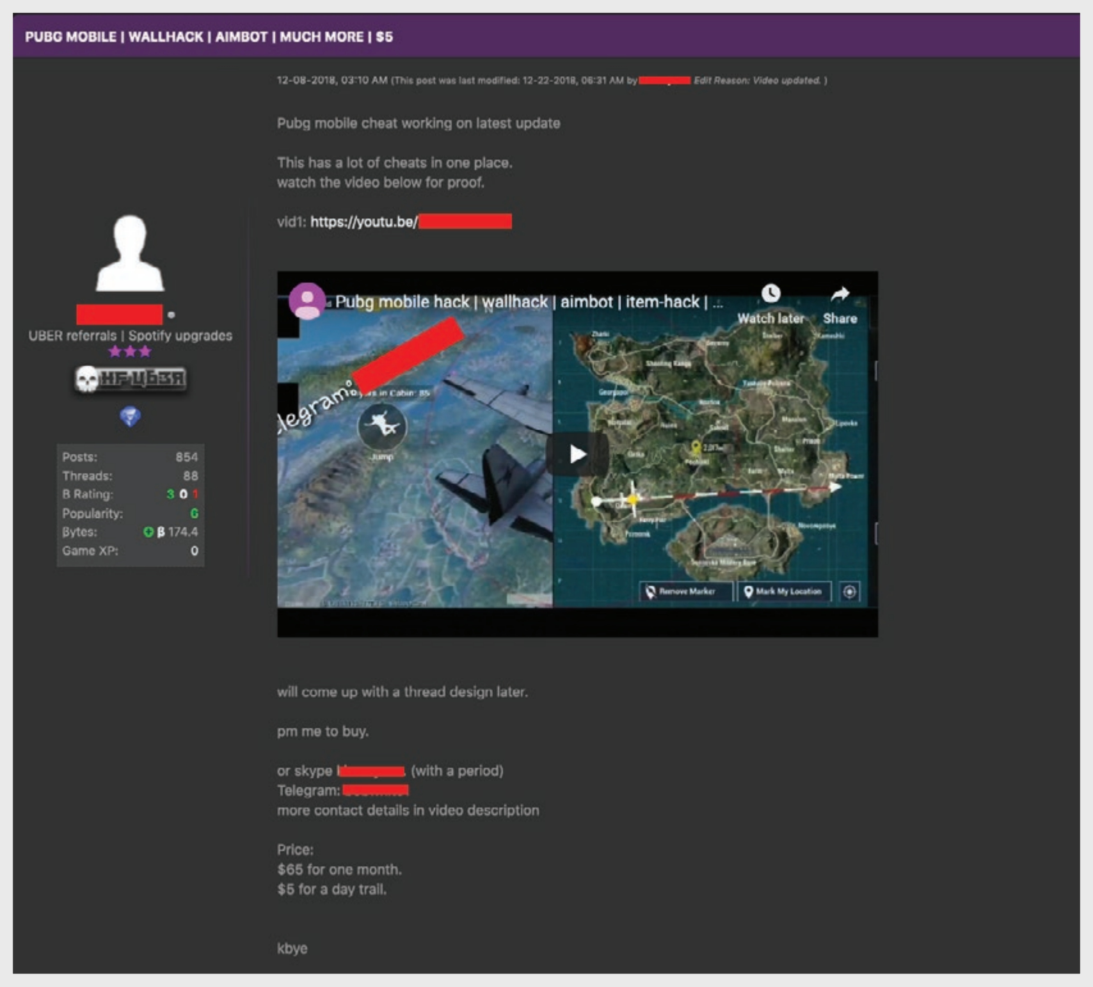
Also our company provides undetected custom spoofer that unbans you from the game (you won't be kicked from the bus, then the game starts)

Functions list:

~Aimbot:~
Enabled *(This will enable the aimbot features)
Draw Field Of View *(Draws a circle so you can see your FoV)
Visibility Check *(Don't pre-aim behind a wall with our visbility checks)
Aim Key *(When the aim key is pressed the aimbot will start aiming)
Aim Bone *(You can select onto which bone to aim)
Field Of View *(Limit the aimbot to a certain FoV to appear more legit)
Aim Smoothing *(This will humanize your aimbot and make it more legit)
Aim Distance *(Limits the distance the aimbot can aim as to appear more legit)
Extra Sensory Perception (ESP)

~Player ESP:~
-Name (Shows the name of the player)
-Distance (Shows the distance to the players / items)
-Weapon (Shows the type of the weapon)

Figure 6. A forum post selling subscription-based access to gaming cheats



PUBG MOBILE | WALLHACK | AIMBOT | MUCH MORE | $5

[redacted]

UBER referrals | Spotify upgrades

Posts:	854
Threads:	88
B Rating:	3 0 1
Popularity:	6
Bytes:	β 174.4
Game XP:	0

12-08-2018, 03:10 AM (This post was last modified: 12-22-2018, 06:31 AM by [redacted] *Edit Reason: Video updated.*)

Pubg mobile cheat working on latest update

This has a lot of cheats in one place.
watch the video below for proof.

vid1: https://youtu.be/[redacted]

will come up with a thread design later.

pm me to buy.

or skype [redacted] (with a period)
Telegram: [redacted]
more contact details in video description

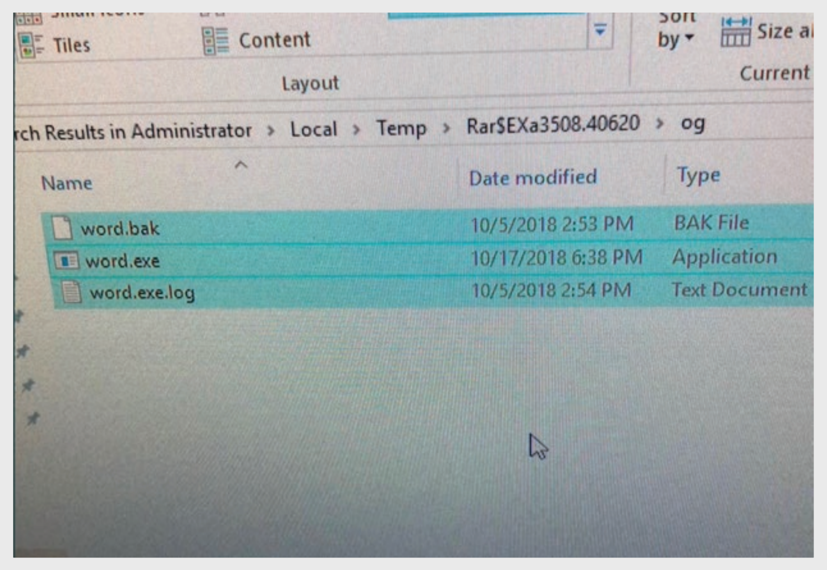
Price:
$65 for one month.
$5 for a day trall.

kbye

Figure 7. A forum post selling wallhacks and aimbots; prices start at US$5 for a one-day trial

Players found using such tools do get banned when caught, and some have been caught running cheats during major esports events. The Counter-Strike: Global Offensive (CS:GO) player known as “Forsaken” was banned for five years after he was caught using an aimbot during the eXTREMESLAND ZOWIE Asia tournament in 2018. The player tried to disguise the program by using “word.exe” as a filename.[16]

This happened because the players were allowed to use their own computers in this particular tournament. Each tournament sets their own rules regarding the devices the players are allowed to bring, such as computers, headphones, mice, and keyboards.



rch Results in Administrator > Local > Temp > Rar$EXa3508.40620 > og

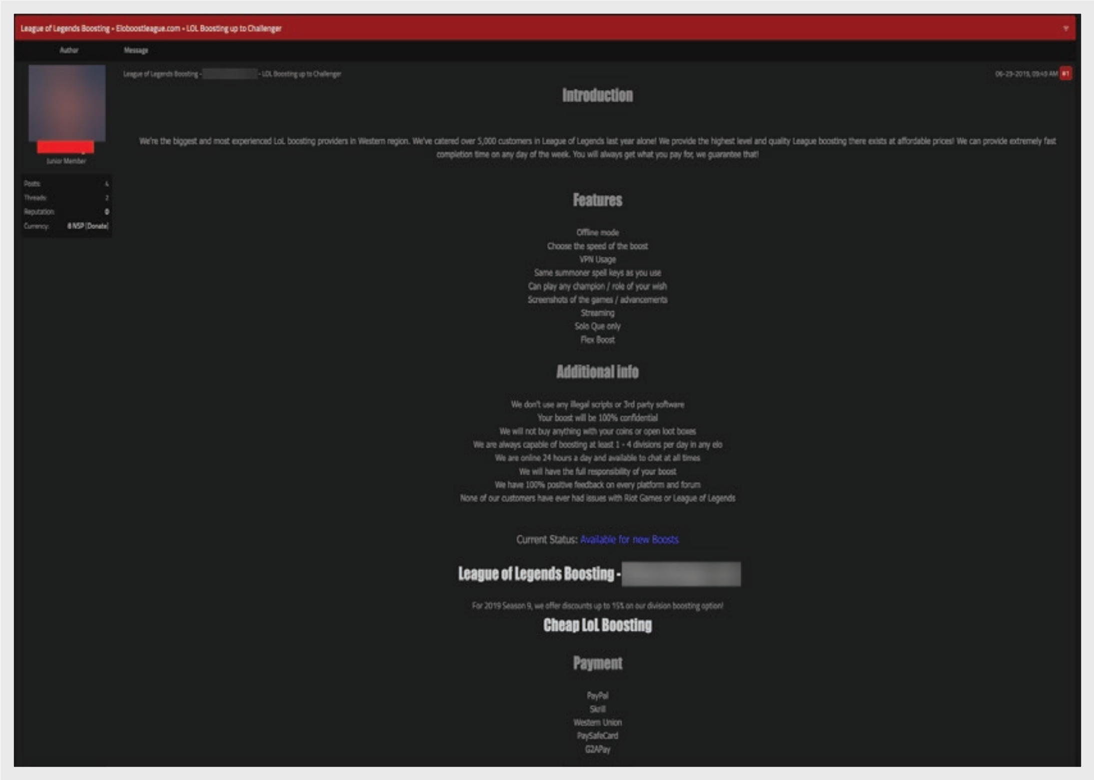
Name	Date modified	Type
word.bak	10/5/2018 2:53 PM	BAK File
word.exe	10/17/2018 6:38 PM	Application
word.exe.log	10/5/2018 2:54 PM	Text Document

Figure 8. The files that tournament judges found on Forsaken's computer

Players cannot sign up for a professional tournament if they have been banned for cheating on other gaming titles. However, one way to overcome bans is to purchase stolen accounts that have a clean gaming history. We predict an increase in attacks that aim to steal gaming accounts, which would parallel the trend of messaging and social network account theft through phishing and malware. Caches of these accounts typically wind up being sold fairly cheap in the cybercriminal underground market.

Pay-for-play: Score-boosting services

We also expect "boosting" to become more popular in cybercriminal underground forums. Boosting involves a player allowing another player to log into his or her account and play to increase their levels or leaderboard standings. We have found several boosting-for-hire services in the underground market, shown below:



League of Legends Boosting • Eloboostleague.com • LOL Boosting up to Challenger

[redacted]
Junior Member

Posts: 4
Threads: 2
Reputation: 0
Currency: 8 NSP [Donate]

League of Legends Boosting - [redacted] - LOL Boosting up to Challenger

06-23-2019, 09:49 AM #1

Introduction

We're the biggest and most experienced LoL boosting providers in Western region. We've catered over 5,000 customers in League of Legends last year alone! We provide the highest level and quality League boosting there exists at affordable prices! We can provide extremely fast completion time on any day of the week. You will always get what you pay for, we guarantee that!

Features

Offline mode
Choose the speed of the boost
VPN Usage
Same summoner spell keys as you use
Can play any champion / role of your wish
Screenshots of the games / advancements
Streaming
Solo Que only
Flex Boost

Additional info

We don't use any illegal scripts or 3rd party software
Your boost will be 100% confidential
We will not buy anything with your coins or open loot boxes
We are always capable of boosting at least 1 - 4 divisions per day in any elo
We are online 24 hours a day and available to chat at all times
We will have the full responsibility of your boost
We have 100% positive feedback on every platform and forum
None of our customers have ever had issues with Riot Games or League of Legends

Current Status: Available for new Boosts

League of Legends Boosting - [redacted]

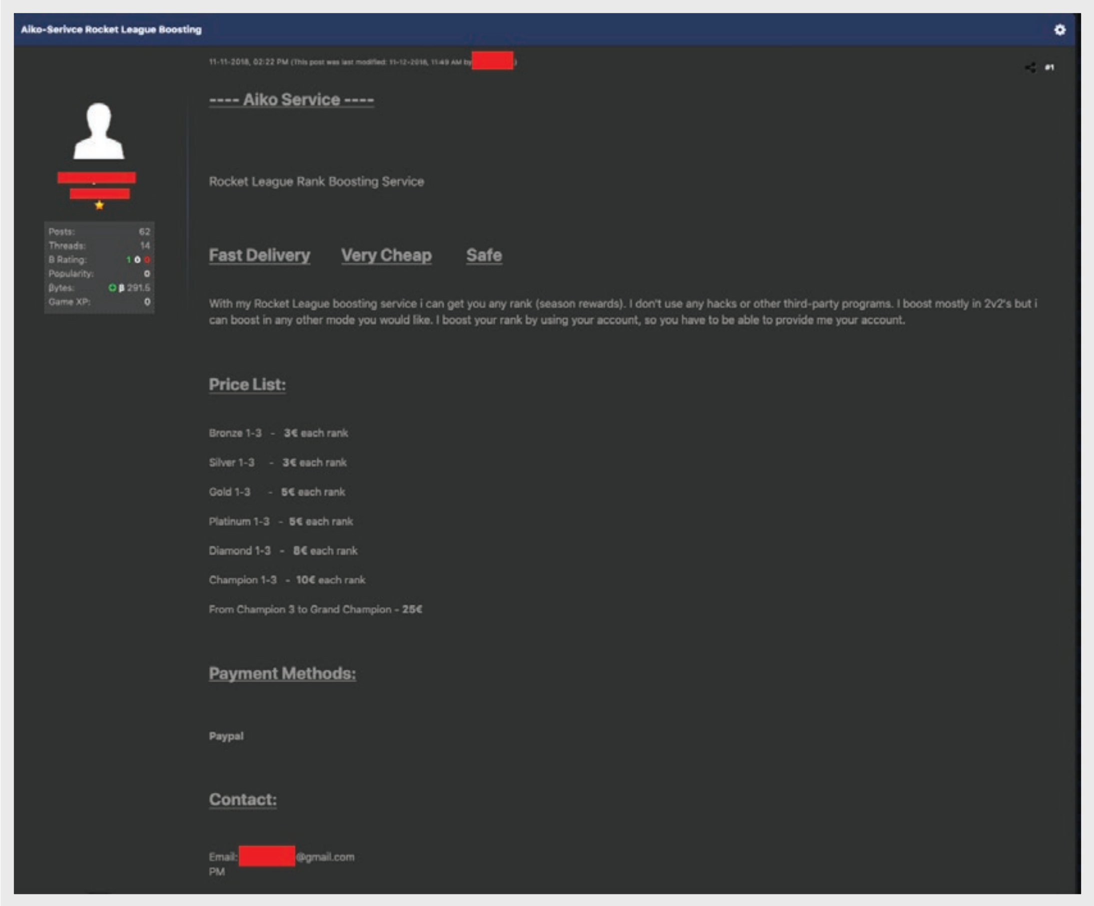
For 2019 Season 9, we offer discounts up to 15% on our division boosting option!

Cheap LoL Boosting

Payment

PayPal
Skrill
Western Union
PaySafeCard
G2APay

Figure 9. Forum post offering a boosting-for-hire service for League of Legends



Aiko-Serivce Rocket League Boosting

11-11-2018, 02:22 PM (This post was last modified: 11-12-2018, 11:49 AM by [redacted])

#1

[redacted]

Posts: 62
Threads: 14
B Rating: 1 0 0
Popularity: 0
βytes: β 291.5
Game XP: 0

---- Aiko Service ----

Rocket League Rank Boosting Service

Fast Delivery Very Cheap Safe

With my Rocket League boosting service i can get you any rank (season rewards). I don't use any hacks or other third-party programs. I boost mostly in 2v2's but i can boost in any other mode you would like. I boost your rank by using your account, so you have to be able to provide me your account.

Price List:

Bronze 1-3 - 3€ each rank

Silver 1-3 - 3€ each rank

Gold 1-3 - 5€ each rank

Platinum 1-3 - 5€ each rank

Diamond 1-3 - 8€ each rank

Champion 1-3 - 10€ each rank

From Champion 3 to Grand Champion - 25€

Payment Methods:

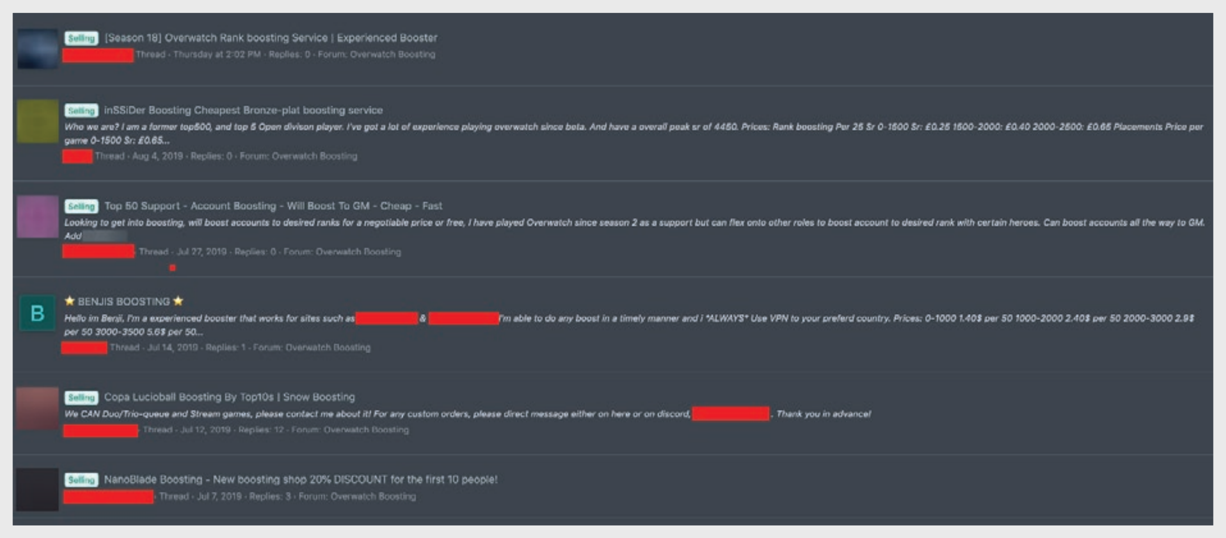
Paypal

Contact:

Email: [redacted]@gmail.com
PM

Figure 10. Another post offering a boosting service for League of Legends

There have been players caught boosting, and esports entities have made it clear that the practice will result in severe penalties. In February this year, twelve Overwatch players in China were banned for boosting. The twelve players have also been banned from all future Blizzard-endorsed tournaments — the first ever such ban given.[18] In early 2018, South Korea passed a law that made boosting illegal in the country. Offenders face a stiff fine if caught.[19]



Selling [Season 18] Overwatch Rank boosting Service | Experienced Booster
[redacted] Thread · Thursday at 2:02 PM · Replies: 0 · Forum: Overwatch Boosting

Selling inSSiDer Boosting Cheapest Bronze-plat boosting service
Who we are? I am a former top500, and top 5 Open divison player. I've got a lot of experience playing overwatch since beta. And have a overall peak sr of 4450. Prices: Rank boosting Per 25 Sr 0-1500 Sr: £0.25 1500-2000: £0.40 2000-2500: £0.65 Placements Price per game 0-1500 Sr: £0.65...
[redacted] Thread · Aug 4, 2019 · Replies: 0 · Forum: Overwatch Boosting

Selling Top 50 Support - Account Boosting - Will Boost To GM - Cheap - Fast
Looking to get into boosting, will boost accounts to desired ranks for a negotiable price or free, I have played Overwatch since season 2 as a support but can flex onto other roles to boost account to desired rank with certain heroes. Can boost accounts all the way to GM. Add [redacted]
[redacted] Thread · Jul 27, 2019 · Replies: 0 · Forum: Overwatch Boosting

★ BENJIS BOOSTING ★
Hello im Benji, I'm a experienced booster that works for sites such as [redacted] *&* [redacted] *I'm able to do any boost in a timely manner and I *ALWAYS* Use VPN to your preferd country. Prices: 0-1000 1.40$ per 50 1000-2000 2.40$ per 50 2000-3000 2.9$ per 50 3000-3500 5.6$ per 50...*
[redacted] Thread · Jul 14, 2019 · Replies: 1 · Forum: Overwatch Boosting

Selling Copa Lucioball Boosting By Top10s | Snow Boosting
We CAN Duo/Trio-queue and Stream games, please contact me about it! For any custom orders, please direct message either on here or on discord, [redacted]*. Thank you in advance!*
[redacted] Thread · Jul 12, 2019 · Replies: 12 · Forum: Overwatch Boosting

Selling NanoBlade Boosting - New boosting shop 20% DISCOUNT for the first 10 people!
[redacted] Thread · Jul 7, 2019 · Replies: 3 · Forum: Overwatch Boosting

Figure 11. Boosting service offered by elite players

Players can also use other techniques to gain an advantage: one example is stream snipping. This is when a player sees the screen of another player using someone else's Twitch stream, which allows one to see other players' locations and current moves. Players caught doing this can also get a lifetime ban from certain competitions.[20]

Hidden hardware hacks

Cheating in esports competitions is not limited to software hacks — hardware used in competitions can be manipulated as well. For each tournament, a gaming board sets the rules on what equipment they allow tournament participants to use. A lot of professional tournaments allow players to bring their own mouse and keyboard, which have been known to house hacks.

Nearly a year ago, a Dota 2 team was disqualified from a $15 million tournament after judges caught one of its members using a programmable mouse. The mouse allowed the player to perform movements that would be impossible without macros (a shortcut of preset key sequences not possible with standard non-programmable hardware).[21]

In 2018, the player “Ra1f” was caught using an advanced hardware cheat for Counter-Strike: Global Offensive that bypassed ESEA anti-cheat technology. Ralf later confessed, and admitted to paying 400 Euros for the exploit. This is how it worked:

- The main computer has both CS:GO and the needed ESEA client (anti-cheat software) installed, like any other ordinary CS:GO installation
- The second computer (let’s call it the “attack PC”) has a special software installed ready to receive data
- The main computer has a physical DMA (Direct Memory Access) device plugged into a PCI Express (PCIe) slot
- A USB cable connects the DMA device to the attack PC
- The DMA device sends data via the USB cable to the attacker PC, and the main computer captures and parses it
- After parsing the data, the attack PC sends it to a Raspberry Pi
- A mobile phone connected to the Raspberry Pi via Wi-Fi downloads the data, which includes all player locations and puts it on the screen, providing the cheater with the positions of his enemies[22]

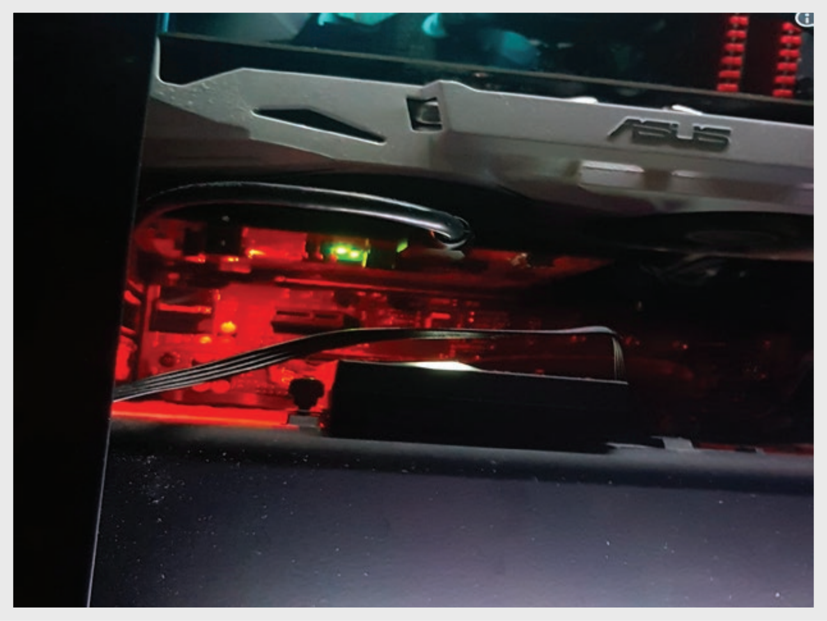
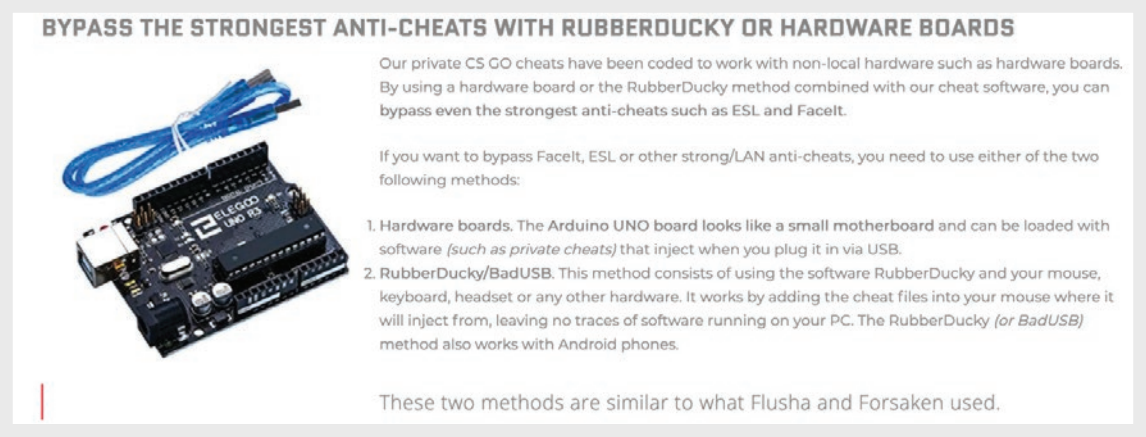


Figure 12. PCI Express equipment used for cheating

We have also seen hardware hacks that require a hardware board such as an Arduino or a Rubber Ducky USB. Rubber Duckys, which cost around US$45, are typically used for penetration testing, but their capabilities allow them to be misused. Hardware boards are readily available on places like Amazon, but underground sellers offer the hardware with other cheats for an additional fee. These legitimate tools are used to carry cheating software, and some members of the underground have become proficient at creating and selling these for profit — one website offered custom hardware starting at $500.



BYPASS THE STRONGEST ANTI-CHEATS WITH RUBBERDUCKY OR HARDWARE BOARDS

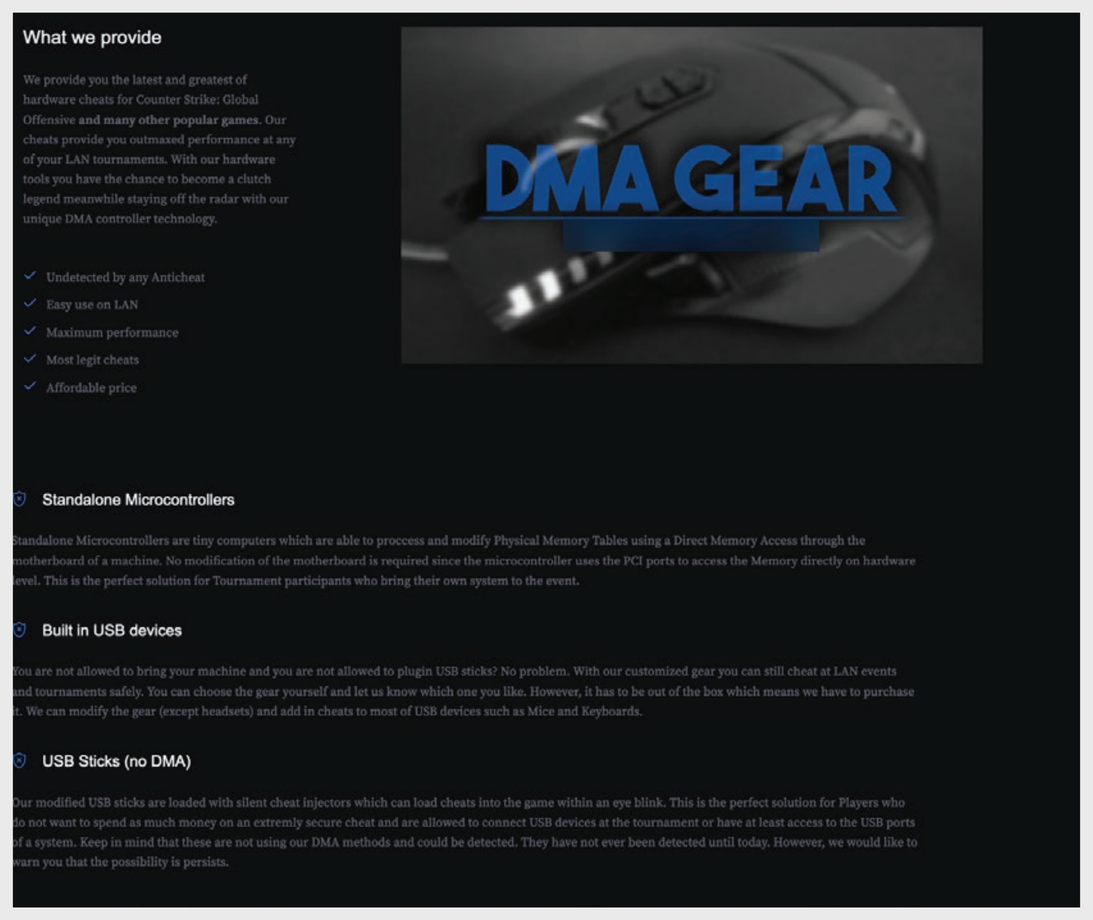
Our private CS GO cheats have been coded to work with non-local hardware such as hardware boards. By using a hardware board or the RubberDucky method combined with our cheat software, you can bypass even the strongest anti-cheats such as ESL and Facelt.

If you want to bypass Facelt, ESL or other strong/LAN anti-cheats, you need to use either of the two following methods:

1. Hardware boards. The Arduino UNO board looks like a small motherboard and can be loaded with software *(such as private cheats)* that inject when you plug it in via USB.
2. RubberDucky/BadUSB. This method consists of using the software RubberDucky and your mouse, keyboard, headset or any other hardware. It works by adding the cheat files into your mouse where it will inject from, leaving no traces of software running on your PC. The RubberDucky *(or BadUSB)* method also works with Android phones.

These two methods are similar to what Flusha and Forsaken used.

Figure 13. Gaming private cheat website suggesting users purchase a Rubber Ducky or hardware board to use with their hacks.



What we provide

We provide you the latest and greatest of hardware cheats for Counter Strike: Global Offensive **and many other popular games**. Our cheats provide you outmaxed performance at any of your LAN tournaments. With our hardware tools you have the chance to become a clutch legend meanwhile staying off the radar with our unique DMA controller technology.

- ✓ Undetected by any Anticheat
- ✓ Easy use on LAN
- ✓ Maximum performance
- ✓ Most legit cheats
- ✓ Affordable price

Standalone Microcontrollers

Standalone Microcontrollers are tiny computers which are able to proccess and modify Physical Memory Tables using a Direct Memory Access through the motherboard of a machine. No modification of the motherboard is required since the microcontroller uses the PCI ports to access the Memory directly on hardware level. This is the perfect solution for Tournament participants who bring their own system to the event.

Built in USB devices

You are not allowed to bring your machine and you are not allowed to plugin USB sticks? No problem. With our customized gear you can still cheat at LAN events and tournaments safely. You can choose the gear yourself and let us know which one you like. However, it has to be out of the box which means we have to purchase it. We can modify the gear (except headsets) and add in cheats to most of USB devices such as Mice and Keyboards.

USB Sticks (no DMA)

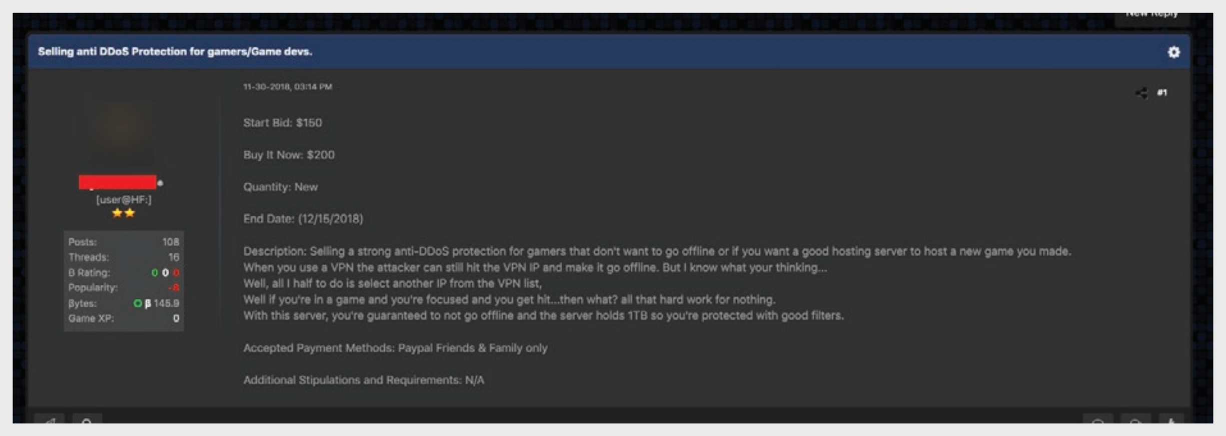
Our modified USB sticks are loaded with silent cheat injectors which can load cheats into the game within an eye blink. This is the perfect solution for Players who do not want to spend as much money on an extremly secure cheat and are allowed to connect USB devices at the tournament or have at least access to the USB ports of a system. Keep in mind that these are not using our DMA methods and could be detected. They have not ever been detected until today. However, we would like to warn you that the possibility is persists.

Figure 14. Page offering custom hardware hacks, with prices starting at US$500

DDoS services will be used to disrupt games

There is a clear risk of disruption when we consider DDoS and esports events. DDoS attacks cause serious lag issues in a competition where every second matters — they can be used to influence and even fix matches. This can affect revenue, tournament schedules, sponsors' reputations, legal online betting, and even get a team disqualified. DDoS incidents have already caused disruptions at esports tournaments.

In several English-speaking cybercriminal underground forums, users often ask how to attack game servers such as Fortnite and PUBG. Members sell DDoS tools or offer DDoS-for-hire services, and some even offer DDoS protection applications for gamers. There are offers of multiple free or paid tools and services starting from $10 a month.



Selling anti DDoS Protection for gamers/Game devs.

[redacted]
[user@HF:]

Posts: 108
Threads: 16
B Rating: 0 0 0
Popularity: -8
Bytes: β 145.9
Game XP: 0

11-30-2018, 03:14 PM

#1

Start Bid: $150

Buy It Now: $200

Quantity: New

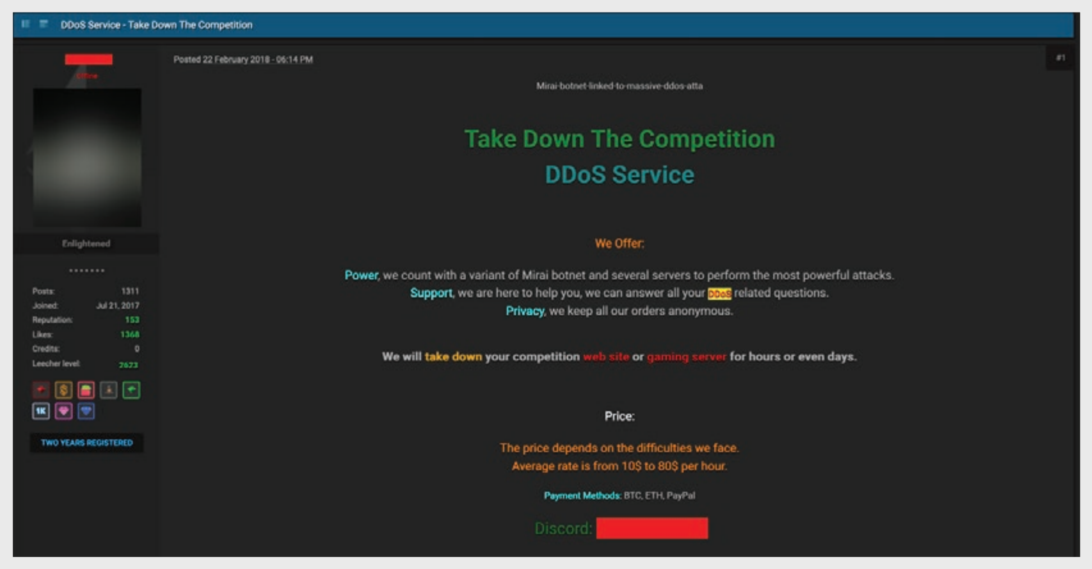
End Date: (12/15/2018)

Description: Selling a strong anti-DDoS protection for gamers that don't want to go offline or if you want a good hosting server to host a new game you made.
When you use a VPN the attacker can still hit the VPN IP and make it go offline. But I know what your thinking...
Well, all I half to do is select another IP from the VPN list,
Well if you're in a game and you're focused and you get hit...then what? all that hard work for nothing.
With this server, you're guaranteed to not go offline and the server holds 1TB so you're protected with good filters.

Accepted Payment Methods: Paypal Friends & Family only

Additional Stipulations and Requirements: N/A

Figure 15. Underground forum post offering an anti-DDoS application for players



DDoS Service - Take Down The Competition

[redacted]

Enlightened

Posts: 1311
Joined: Jul 21, 2017
Reputation: 153
Likes: 1368
Credits: 0
Leecher level: 2623

TWO YEARS REGISTERED

Posted 22 February 2018 - 06:14 PM

#1

Mirai-botnet-linked-to-massive-ddos-atta

Take Down The Competition
DDoS Service

We Offer:

Power, we count with a variant of Mirai botnet and several servers to perform the most powerful attacks.
Support, we are here to help you, we can answer all your DDoS related questions.
Privacy, we keep all our orders anonymous.

We will take down your competition web site or gaming server for hours or even days.

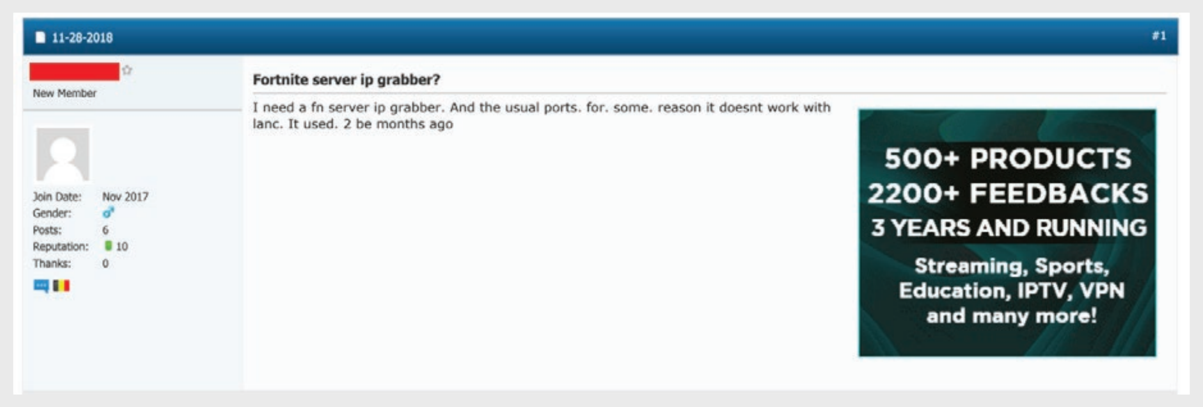
Price:

The price depends on the difficulties we face.
Average rate is from 10$ to 80$ per hour.

Payment Methods: BTC, ETH, PayPal

Discord: [redacted]

Figure 16. Forum post advertising a DDoS service



11-28-2018 #1

[redacted]

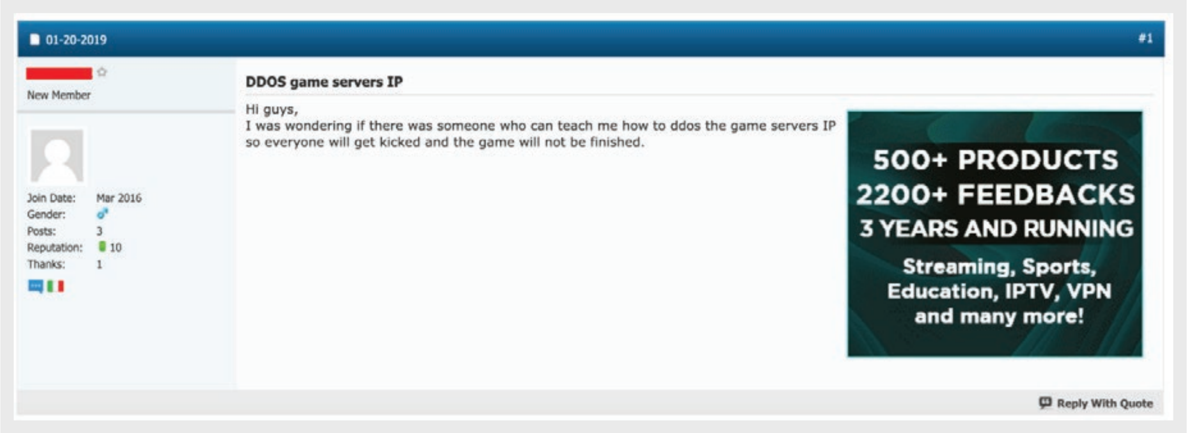
New Member

Join Date: Nov 2017
Gender: ♂
Posts: 6
Reputation: 10
Thanks: 0

Fortnite server ip grabber?

I need a fn server ip grabber. And the usual ports. for. some. reason it doesnt work with lanc. It used. 2 be months ago

Figure 17. Forum user inquiring how to find the IP of a Fortnite server



01-20-2019 #1

[redacted]

New Member

Join Date: Mar 2016
Gender: ♂
Posts: 3
Reputation: 10
Thanks: 1

DDOS game servers IP

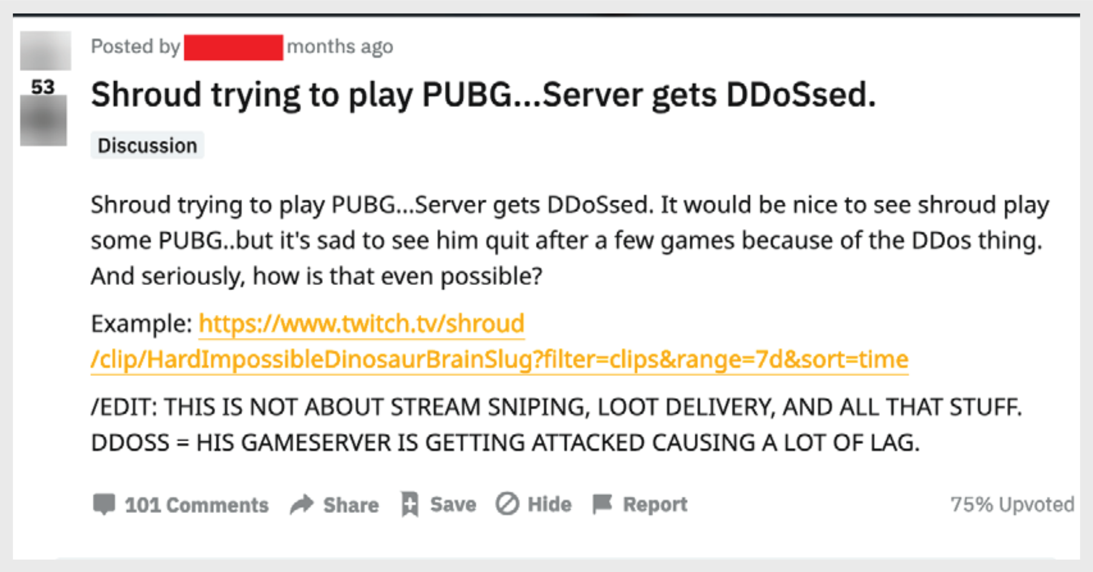
Hi guys,
I was wondering if there was someone who can teach me how to ddos the game servers IP so everyone will get kicked and the game will not be finished.

Figure 18. Forum post of a player asking how to DDoS a gaming server

There have already been several instance of successful DDoS attacks on major esports competitions. In 2015, The International Dota 2 Championships, which had a prize pool of US$18 million, suffered a DDoS attack during the event's second day. In June 2019, the cybercriminal Austin Thompson was sentenced to 27 months in jail and charged a US$95,000 fine for launching DDoS attacks against Dota 2 and League of Legends competitions in 2013.[23] Cybercriminals also launch DDoS attacks for extortion.[24] In 2017, attackers launched sustained DDoS attacks on the online game Albion, then demanded a ransom to make it stop.[25]

We predict DDoS attacks will continue to disrupt major tournaments in the near future, as DDoS-for-hire services have become more available and the underground market has an abundance of sellers. We can also assume that cybercriminals will continue to demand a ransom in similar extortion activities.

In general, DDoS attacks can result in serious downtime; according to a DDoS attack report from IDG, 36% of companies that experience more than five DDoS attacks suffer seven to 12 hours of downtime.[26] For a gaming platform, even a few minutes of downtime is a serious issue. Esports entities might be compelled to pay the ransom since performance lag will hurt the brand's reputation, ultimately resulting in financial losses if players become too frustrated and move on to other games.



Posted by [redacted] months ago

53

Shroud trying to play PUBG...Server gets DDoSsed.

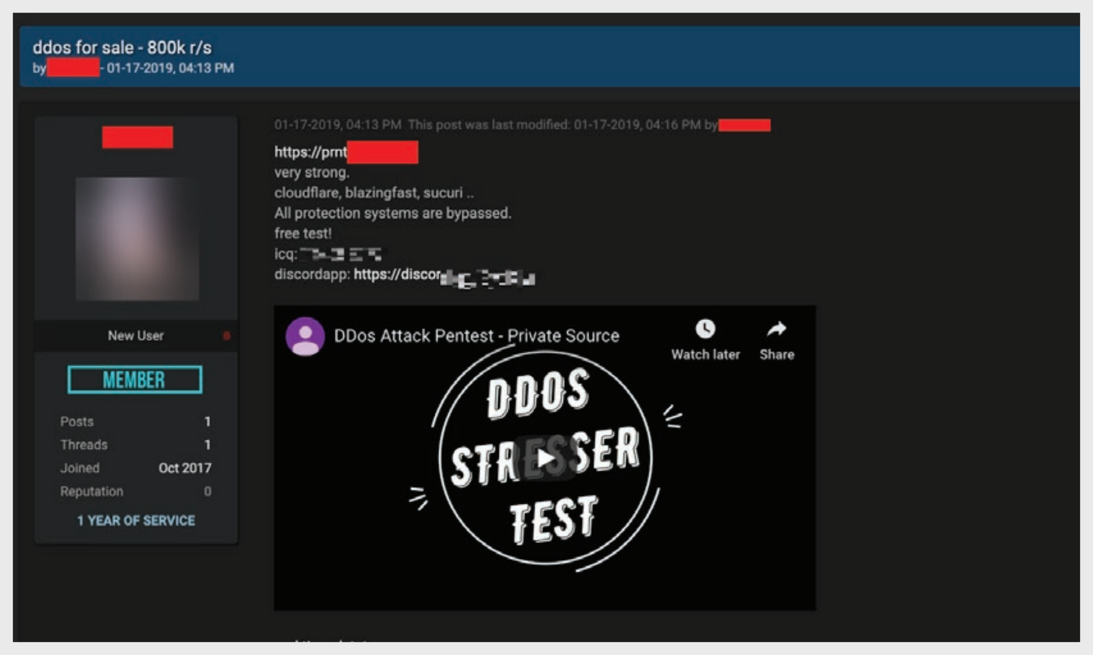
Discussion

Shroud trying to play PUBG...Server gets DDoSsed. It would be nice to see shroud play some PUBG..but it's sad to see him quit after a few games because of the DDos thing. And seriously, how is that even possible?

Example: https://www.twitch.tv/shroud/clip/HardImpossibleDinosaurBrainSlug?filter=clips&range=7d&sort=time

/EDIT: THIS IS NOT ABOUT STREAM SNIPING, LOOT DELIVERY, AND ALL THAT STUFF. DDOSS = HIS GAMESERVER IS GETTING ATTACKED CAUSING A LOT OF LAG.

Figure 19. Player complaining about DDoS attacks on Reddit



ddos for sale - 800k r/s
by [redacted] - 01-17-2019, 04:13 PM

[redacted]

New User

MEMBER

Posts	1
Threads	1
Joined	Oct 2017
Reputation	0

1 YEAR OF SERVICE

01-17-2019, 04:13 PM This post was last modified: 01-17-2019, 04:16 PM by [redacted]

https://prnt [redacted]
very strong.
cloudflare, blazingfast, sucuri ..
All protection systems are bypassed.
free test!
icq: [redacted]
discordapp: https://discor [redacted]

Figure 20. Forum post offering DDoS services

Sponsors should expect to be attacked or have their services go down when sponsoring an esports event. The risk here comes from multiple origins: hacktivists, adversaries, competitors and so on. If they lose money, they'll probably reconsider sponsoring again. It's a general risk for both sponsors and the event organizers, as large scale DDoS attacks continue to be difficult to deal with.

Cybercriminals will start to target game servers

Cybercriminals will look for ways to disrupt daily operations such as live game competitions. These include using exploits and tools to attack any vulnerabilities the game servers may have.

We tried to determine if, and how many, esports gaming assets were accessible through the internet using Shodan, a search engine for internet-connected devices. As of July 25, 2019, we found 219,981 gaming assets that were accessible online. Germany had the highest with 61,272, while the U.S. had 56,500. Steam dedicated servers had 21,930 online assets, while the popular game title Counter-Strike had 12,164.

Searching with Shodan provides an easy one-stop solution to conduct Open-Source Intelligence (OSINT) gathering for different geographic locations, organizations, devices, services, etc. It is not unusual for a server to be accessible in this manner. However, software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in accessible cyber assets. Servers are online by nature, and this exposes them to some level of risk. An adversary can use Shodan to perform detailed surveillance and gather intelligence about a target server, and more thorough probing can reveal certain vulnerabilities in the servers.

Here are some of the vulnerabilities found on a few of the game-related servers we scanned:

Vulnerability	Type
CVE-2012-4558[27]	Could allow remote attackers to inject arbitrary web script or HTML via a crafted string
CVE-2013-1896[28]	Could allow remote attackers to cause a denial of service (segmentation fault) via a MERGE request
CVE-2012-3499[29]	Could allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs
CVE-2014-0231[30]	Could allow remote attackers to cause a denial of service (process hang) via a request to a CGI script
CVE-2017-7679[31]	Could let actor read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2018-1312[32]	In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2010-5107[33]	Makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability	Type
CVE-2016-0778[34]	Could allow remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
CVE-2012-2531[35]	"Password Disclosure Vulnerability" could allow local users to discover credentials by reading Operational log
CVE-2018-10549[36]	Servers with this vulnerability have an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-10548[37]	Could allow remote LDAP servers to cause a denial of service
CVE-2018-10545[38]	Could allow one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications.
CVE-2014-1692[39]	Could allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
CVE-2017-15906[40]	Could allow attackers to create zero-length files.
CVE-2019-11039[41]	Could lead to information disclosure or crash.
CVE-2019-11040[42]	Could lead to information disclosure or crash.

The servers scanned include those operated by private gamers and groups, not just those run by the gaming companies.

Targeted malware will be launched to compromise high-profile gamers and brands

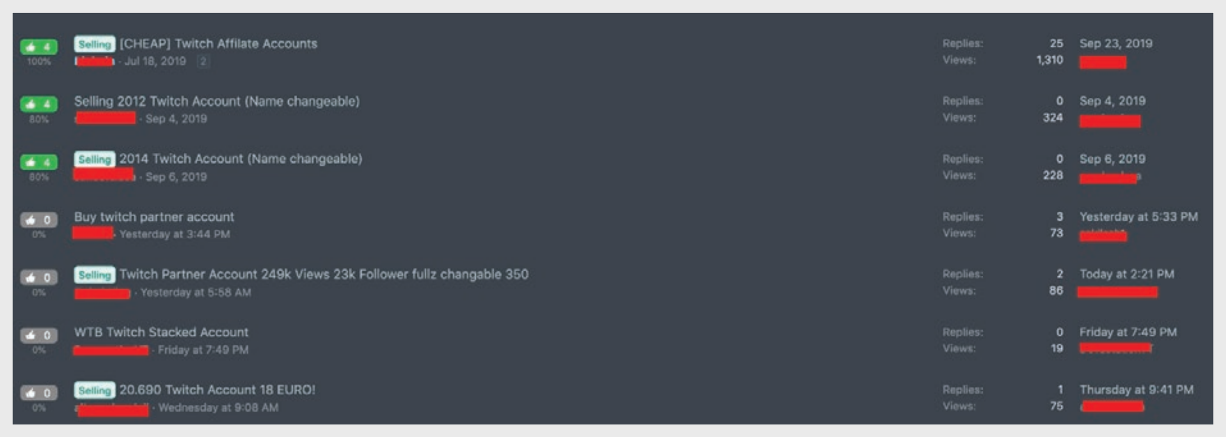
Cybercriminals are increasingly deploying targeted ransomware, aiming for a higher success rate of payments from victims. We believe sponsors of esports events should be very careful here as it could expose their brands to certain risks. If a hacktivist or financially-motivated group started looking for targets, sponsors will likely be first in their sights — attackers might assume a known brand's pockets are deeper than the players' or the game organizers'.

Undoubtedly, ransomware has plagued gamers and businesses for years. A curious case appeared in 2018 when criminals targeted gamers with ransomware that demanded people play PlayerUnknown's Battlegrounds in order to unlock their files.[43] While the case turned out to be a joke, it was still dangerous.

We are also aware of TeslaCrypt ransomware variants that infected gamers' computers and searched for file extensions related to various popular game titles (such as Call of Duty, Diablo, League of Legends, Minecraft and Resident Evil) and locked the games' saved data, player profiles, DLCs, and game mods stored in the victim's computer. Victims of the ransomware were instructed to pay US$500 in bitcoin within one week; the ransom doubles to $1,000 after the deadline.[44] As saved games and gaming profiles represent hundreds of hours of gameplay, victims could feel inclined to pay the ransom.

We also expect cybercriminals to compromise famous Twitch and YouTubers gamers' social media accounts. Cybercriminals will look for accounts that have several million followers and will use targeted phishing attacks and malware to take over these accounts. The cybercriminal underground is already flooded with sales of Twitch and YouTube accounts with a large number of followers. These famous and popular social media accounts not only have a wide reach (imagine if they share a link containing malware for instance) and capillarity, but also represent their brands and sponsors.

We see signs that the cybercriminal underground market for stolen gaming accounts will grow over the next three years. Cybercriminals usually target popular games like Fortnite and Counter-Strike: Global Offensive looking for valid accounts. Stolen accounts are found in abundance in underground forums, with prices starting at just US$1 per account. Counter-Strike: Global Offensive accounts with The Global Elite rank were found being sold for US$99. The Global Elite is the game's highest rank, only reached by less than 1% of the player base as of March 2019.[45]



4 100%	Selling [CHEAP] Twitch Affilate Accounts [redacted] · Jul 18, 2019 2	Replies: Views:	25 1,310	Sep 23, 2019 [redacted]
4 80%	Selling 2012 Twitch Account (Name changeable) [redacted] · Sep 4, 2019	Replies: Views:	0 324	Sep 4, 2019 [redacted]
4 80%	Selling 2014 Twitch Account (Name changeable) [redacted] · Sep 6, 2019	Replies: Views:	0 228	Sep 6, 2019 [redacted]
0 0%	Buy twitch partner account [redacted] · Yesterday at 3:44 PM	Replies: Views:	3 73	Yesterday at 5:33 PM [redacted]
0 0%	Selling Twitch Partner Account 249k Views 23k Follower fullz changable 350 [redacted] · Yesterday at 5:58 AM	Replies: Views:	2 86	Today at 2:21 PM [redacted]
0 0%	WTB Twitch Stacked Account [redacted] · Friday at 7:49 PM	Replies: Views:	0 19	Friday at 7:49 PM [redacted]
0 0%	Selling 20.690 Twitch Account 18 EURO! [redacted] · Wednesday at 9:08 AM	Replies: Views:	1 75	Thursday at 9:41 PM [redacted]

Figure 21. Forum sellers pushing various Twitch accounts

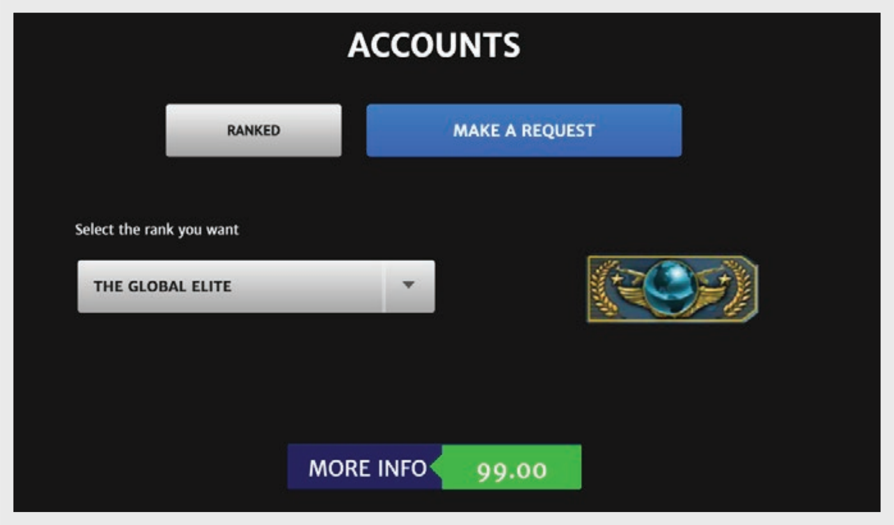
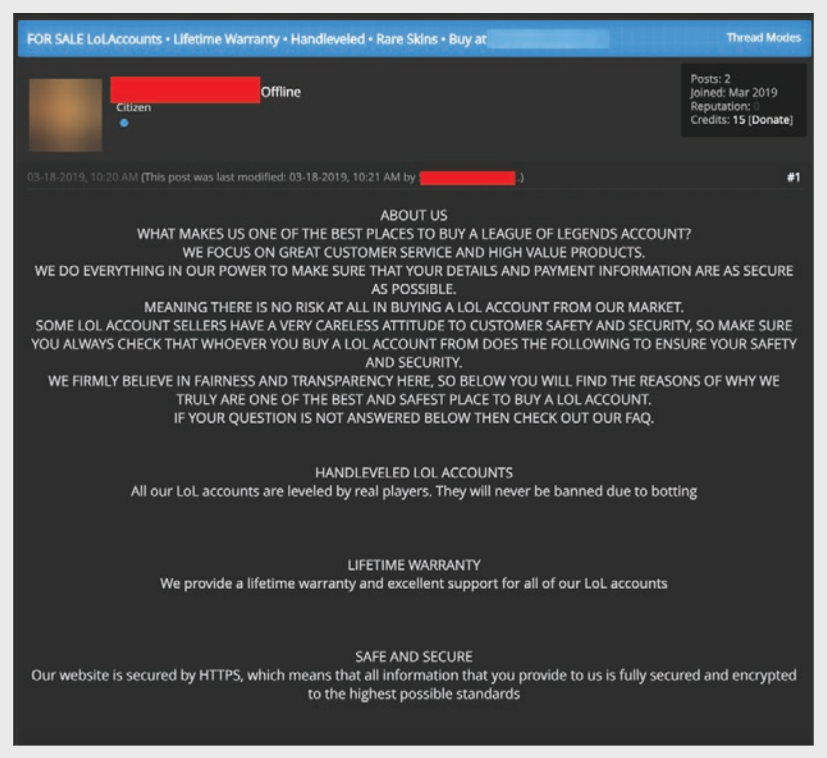


Figure 22. CS:GO accounts with The Global Elite rank sells for $99

The stolen account market is supported by players using weak passwords; and also weak authentication methods have made it easier to steal these accounts. This is particularly dangerous since they are usually tied to items and digital currencies. Gamers and viewers can lose money when cybercriminals purchase items on these accounts using the original owners' credit card and then make a profit selling these items.



FOR SALE LolAccounts • Lifetime Warranty • Handleveled • Rare Skins • Buy at [redacted]

Thread Modes

[redacted] Offline
Citizen

Posts: 2
Joined: Mar 2019
Reputation: 0
Credits: 15 [Donate]

03-18-2019, 10:20 AM (This post was last modified: 03-18-2019, 10:21 AM by [redacted].)

#1

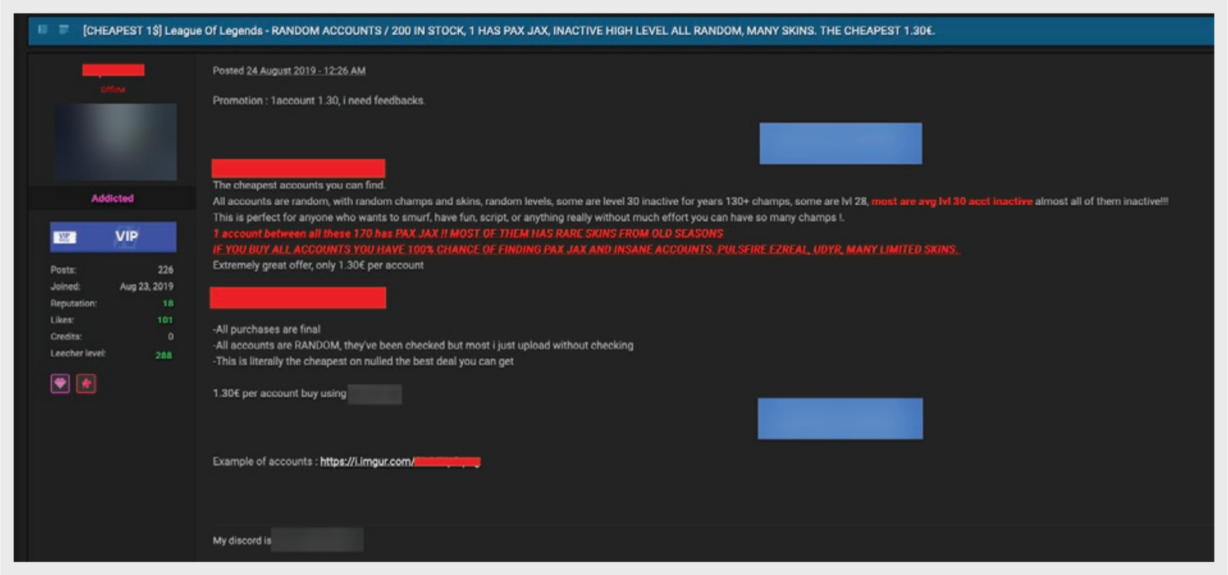
ABOUT US
WHAT MAKES US ONE OF THE BEST PLACES TO BUY A LEAGUE OF LEGENDS ACCOUNT?
WE FOCUS ON GREAT CUSTOMER SERVICE AND HIGH VALUE PRODUCTS.
WE DO EVERYTHING IN OUR POWER TO MAKE SURE THAT YOUR DETAILS AND PAYMENT INFORMATION ARE AS SECURE AS POSSIBLE.
MEANING THERE IS NO RISK AT ALL IN BUYING A LOL ACCOUNT FROM OUR MARKET.
SOME LOL ACCOUNT SELLERS HAVE A VERY CARELESS ATTITUDE TO CUSTOMER SAFETY AND SECURITY, SO MAKE SURE YOU ALWAYS CHECK THAT WHOEVER YOU BUY A LOL ACCOUNT FROM DOES THE FOLLOWING TO ENSURE YOUR SAFETY AND SECURITY.
WE FIRMLY BELIEVE IN FAIRNESS AND TRANSPARENCY HERE, SO BELOW YOU WILL FIND THE REASONS OF WHY WE TRULY ARE ONE OF THE BEST AND SAFEST PLACE TO BUY A LOL ACCOUNT.
IF YOUR QUESTION IS NOT ANSWERED BELOW THEN CHECK OUT OUR FAQ.

HANDLEVELED LOL ACCOUNTS
All our LoL accounts are leveled by real players. They will never be banned due to botting

LIFETIME WARRANTY
We provide a lifetime warranty and excellent support for all of our LoL accounts

SAFE AND SECURE
Our website is secured by HTTPS, which means that all information that you provide to us is fully secured and encrypted to the highest possible standards

Figure 23. Advertisement selling League of Legends accounts



[CHEAPEST 1$] League Of Legends - RANDOM ACCOUNTS / 200 IN STOCK, 1 HAS PAX JAX, INACTIVE HIGH LEVEL ALL RANDOM, MANY SKINS. THE CHEAPEST 1.30€.

[redacted]
Offline

Addicted

VIP

Posts:	226
Joined:	Aug 23, 2019
Reputation:	18
Likes:	101
Credits:	0
Leecher level:	288

Posted 24 August 2019 - 12:26 AM

Promotion : 1account 1.30, i need feedbacks.

[redacted]

[redacted]

The cheapest accounts you can find.
All accounts are random, with random champs and skins, random levels, some are level 30 inactive for years 130+ champs, some are lvl 28, **most are avg lvl 30 acct inactive** almost all of them inactive!!!
This is perfect for anyone who wants to smurf, have fun, script, or anything really without much effort you can have so many champs !.
1 account between all these 170 has PAX JAX !! MOST OF THEM HAS RARE SKINS FROM OLD SEASONS
IF YOU BUY ALL ACCOUNTS YOU HAVE 100% CHANCE OF FINDING PAX JAX AND INSANE ACCOUNTS. PULSFIRE EZREAL, UDYR, MANY LIMITED SKINS.
Extremely great offer, only 1.30€ per account

[redacted]

-All purchases are final
-All accounts are RANDOM, they've been checked but most i just upload without checking
-This is literally the cheapest on nulled the best deal you can get

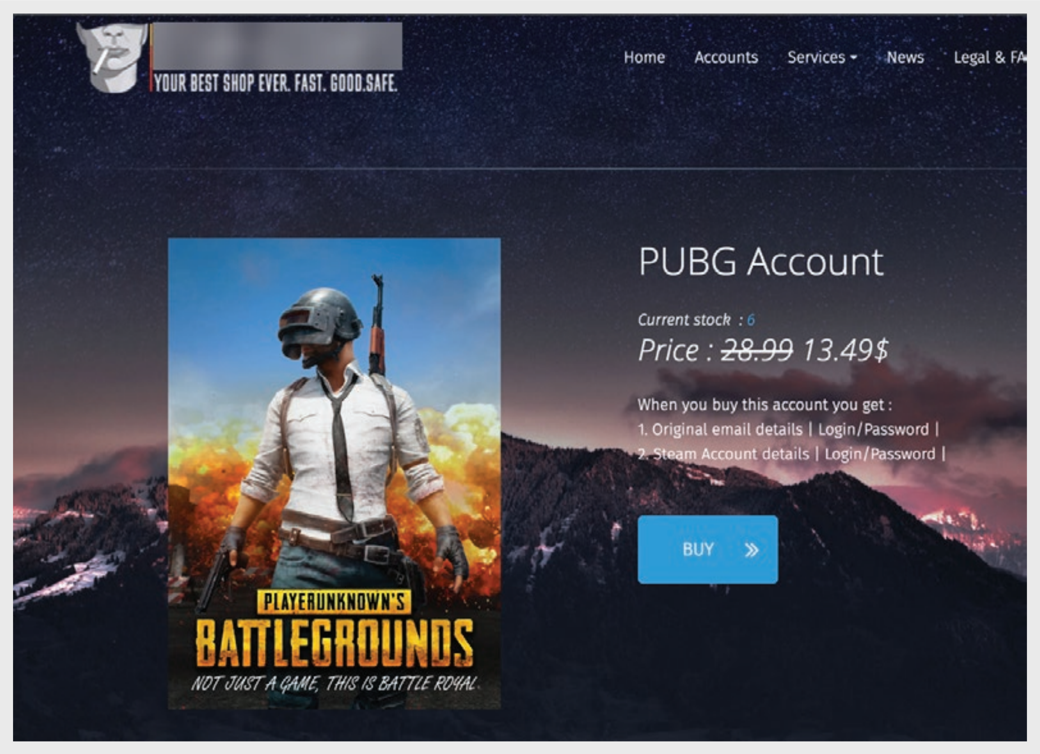
1.30€ per account buy using [redacted]

[redacted]

Example of accounts : https://i.imgur.com/[redacted]

My discord is [redacted]

Figure 24. Advertisement selling League of Legends accounts



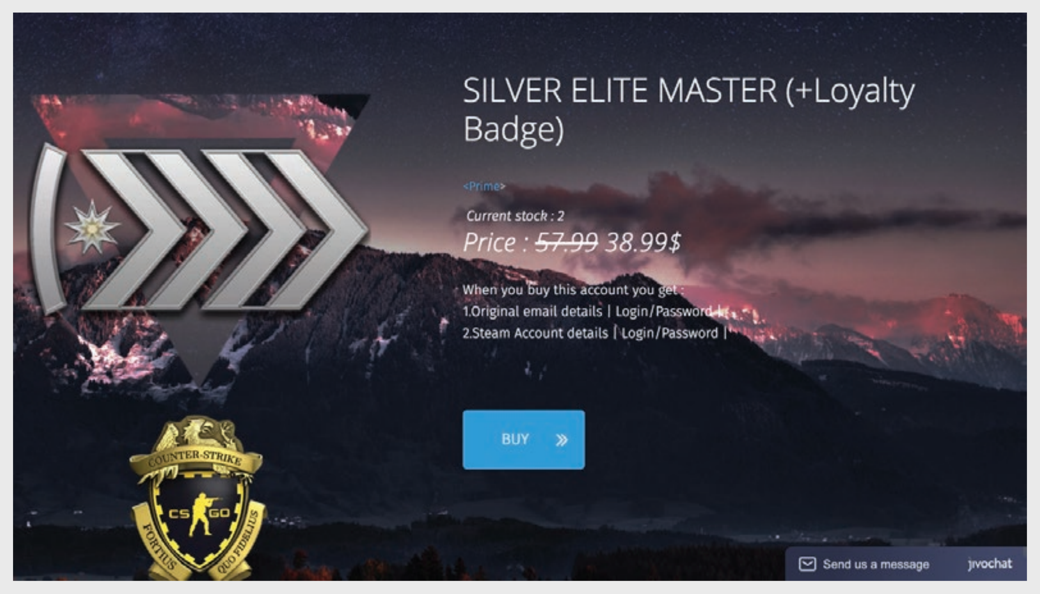
PUBG Account

Current stock : 6

Price : ~~28.99~~ 13.49$

When you buy this account you get :
1. Original email details | Login/Password |
2. Steam Account details | Login/Password |

Figure 25. Steam account shop offering PlayerUnknown's Battlegrounds (PUBG) accounts for US$13.49



SILVER ELITE MASTER (+Loyalty Badge)

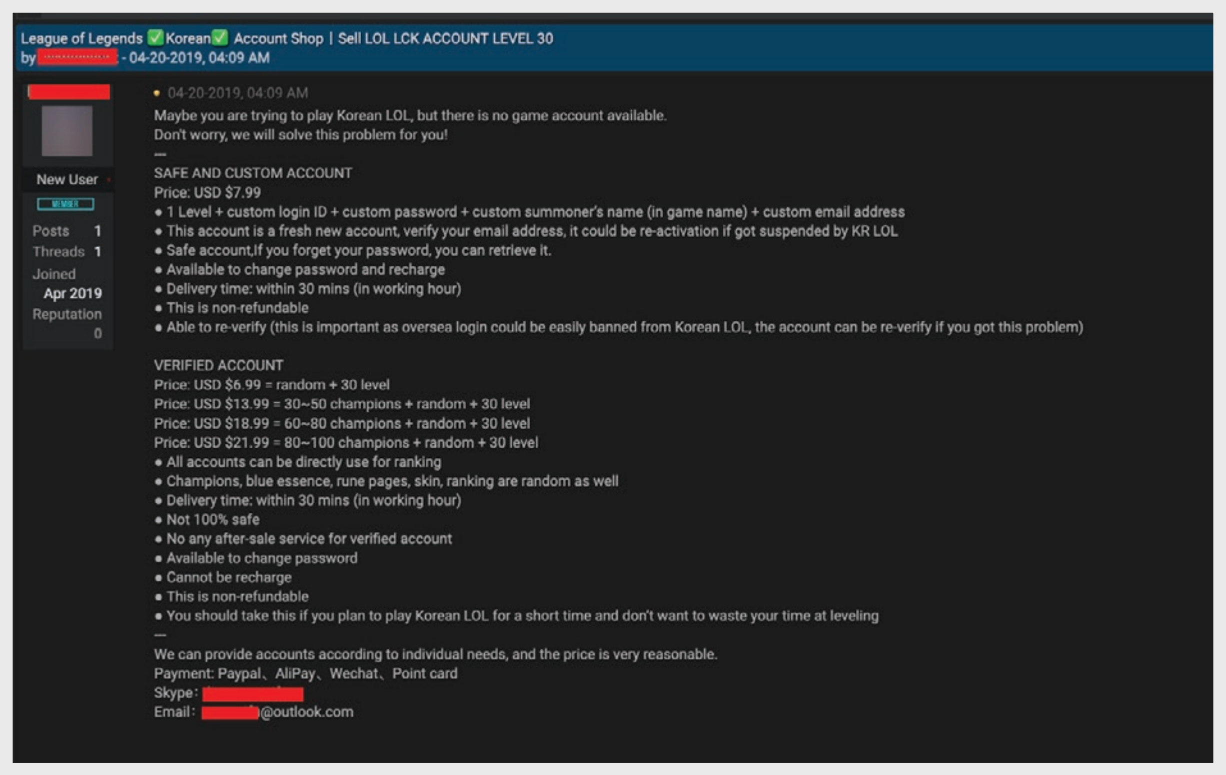
<Prime>

Current stock : 2

Price : ~~57.99~~ 38.99$

When you buy this account you get :
1.Original email details | Login/Password |
2.Steam Account details | Login/Password |

Figure 26. Counter-Strike accounts for sale based on rank



League of Legends ✅Korean✅ Account Shop | Sell LOL LCK ACCOUNT LEVEL 30
by [redacted] - 04-20-2019, 04:09 AM

[redacted]

New User

MEMBER

Posts 1
Threads 1
Joined Apr 2019
Reputation 0

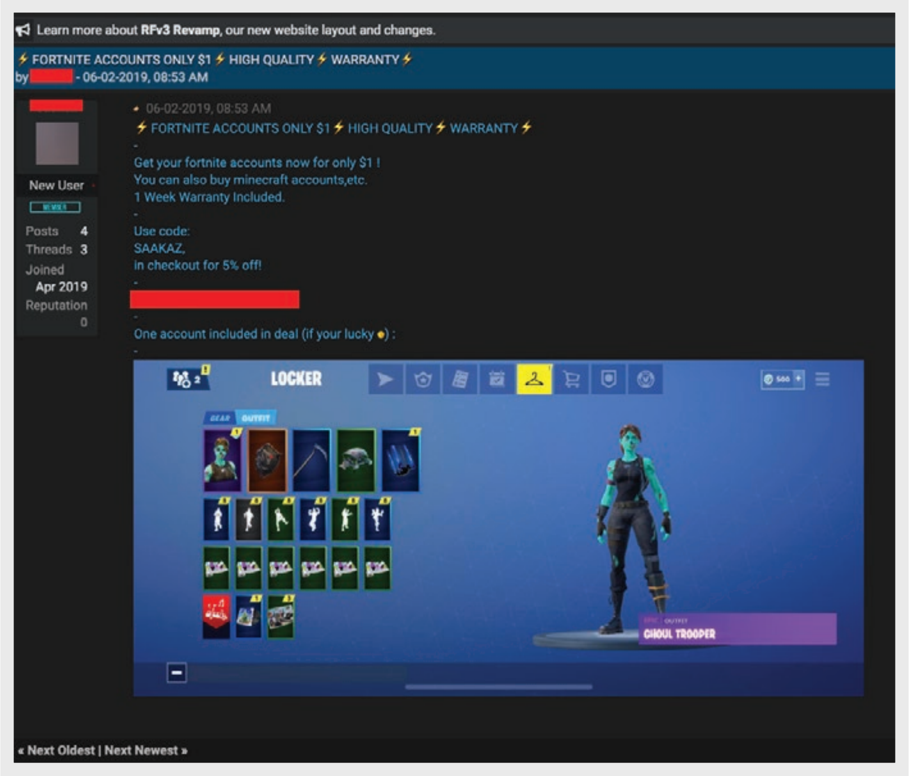
● 04-20-2019, 04:09 AM

Maybe you are trying to play Korean LOL, but there is no game account available.
Don't worry, we will solve this problem for you!
—
SAFE AND CUSTOM ACCOUNT
Price: USD $7.99
- 1 Level + custom login ID + custom password + custom summoner's name (in game name) + custom email address
- This account is a fresh new account, verify your email address, it could be re-activation if got suspended by KR LOL
- Safe account,If you forget your password, you can retrieve it.
- Available to change password and recharge
- Delivery time: within 30 mins (in working hour)
- This is non-refundable
- Able to re-verify (this is important as oversea login could be easily banned from Korean LOL, the account can be re-verify if you got this problem)

VERIFIED ACCOUNT
Price: USD $6.99 = random + 30 level
Price: USD $13.99 = 30~50 champions + random + 30 level
Price: USD $18.99 = 60~80 champions + random + 30 level
Price: USD $21.99 = 80~100 champions + random + 30 level
- All accounts can be directly use for ranking
- Champions, blue essence, rune pages, skin, ranking are random as well
- Delivery time: within 30 mins (in working hour)
- Not 100% safe
- No any after-sale service for verified account
- Available to change password
- Cannot be recharge
- This is non-refundable
- You should take this if you plan to play Korean LOL for a short time and don't want to waste your time at leveling

—
We can provide accounts according to individual needs, and the price is very reasonable.
Payment: Paypal、AliPay、Wechat、Point card
Skype: [redacted]
Email: [redacted]@outlook.com

Figure 27. Advertisement selling accounts for the Korean server of League of Legends



Learn more about **RFv3 Revamp**, our new website layout and changes.

⚡ FORTNITE ACCOUNTS ONLY $1 ⚡ HIGH QUALITY ⚡ WARRANTY ⚡
by [redacted] - 06-02-2019, 08:53 AM

[redacted]

New User

Posts 4
Threads 3
Joined Apr 2019
Reputation 0

06-02-2019, 08:53 AM

⚡ FORTNITE ACCOUNTS ONLY $1 ⚡ HIGH QUALITY ⚡ WARRANTY ⚡

-

Get your fortnite accounts now for only $1 !
You can also buy minecraft accounts,etc.
1 Week Warranty Included.

-

Use code:
SAAKAZ,
in checkout for 5% off!

-

[redacted]

-

One account included in deal (if your lucky ●) :

-

« Next Oldest | Next Newest »

Figure 28. Advertisement selling Fortnite accounts for US$1

Some gaming platforms have introduced multiple-factor authentication (MFA) to their systems to help protect users from account theft. For example, Valve's Steam Guard system implements two-factor authentication via both e-mail and mobile app. However, we still see hacked accounts for sale in underground forums. This probably means that not all the users have enabled MFA or not all the systems have MFA in place.

Hackers will target players' PII and banking credentials

Data breaches are a threat to esports as cybercriminals look for other targets to harvest personally identifiable information (PII). According to recent findings by Akamai, the tech industry has experienced nearly 55 billion credential stuffing attacks globally, and out of these, 12 billion attacks were directed towards the gaming industry.[46]

In 2016, a malware called Steam Stealer targeted players on Valve's Steam platform via phishing attacks. The malware targeted online gaming items and user account credentials, and we found that the malware was stealing 77,000 accounts per month.[47] Also in 2016, the eSports Entertainment Association was hacked. The hacker leaked the data of 1.5 million players after the attacker's demand of US$100,000 was denied.[48] The stolen information included the username, first and last name, email address, date of birth, zip code and phone numbers of each player. Hackers can also steal players' in-game tokens and weapons, which can be worth a lot of money in the underground market. And there have been a few records on Reddit forums[49, 50] of players complaining that their accounts have been stolen and sold, or their information was used to purchase in-game items. In August 2019, a scam used a fake "free game" giveaway site to steal the account information of Steam users. It used a fake login page, and even a fake popup that helped it bypass two-factor authentication. The hackers then accessed the account's friend list and sent them phishing messages to gain more victims.[51]

Our previous research[52] revealed a big surplus of PII currently available in the cybercriminal underground. We believe this will increase based on the increasing demand for gaming credentials and similar types of esports data.

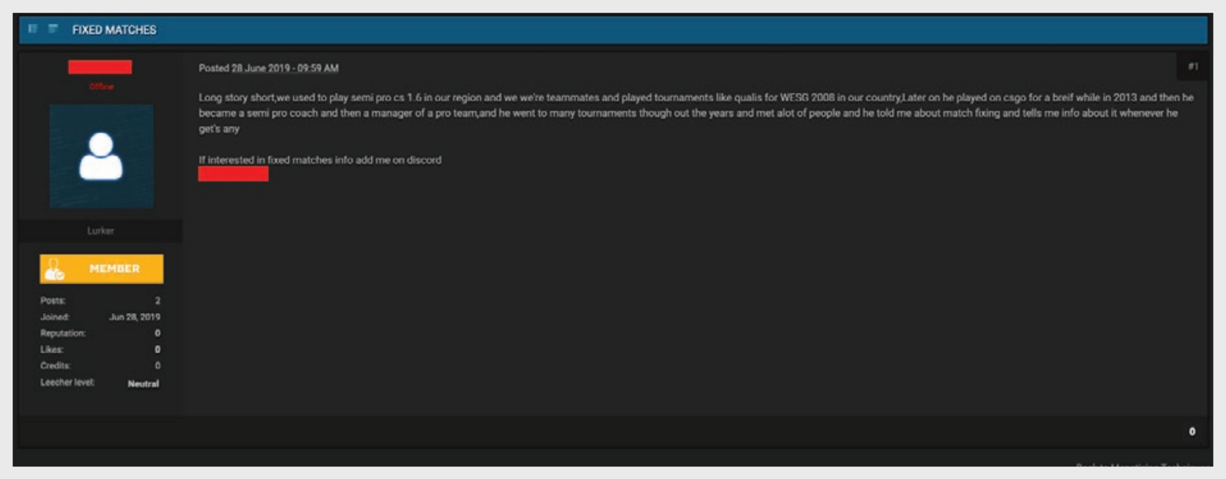
Illegal gambling and match-fixing will continue to rise

We expect illegal bookmaking companies to try to tap into the lucrative and still-growing esports market. Traditional organized crime rings and low-level criminals will have an opportunity to influence match outcomes and profit from them in betting markets, and the cybercriminal underground market is flooded with betting and bookmaker services. According to the American Gaming Association, Americans illegally wager more than $150 billion on traditional sports every year, whether through offshore betting sites or illegal bookmakers.[53] Meanwhile, a study from the UK Gaming commission in 2018 reported that 8.5% of British respondents have placed bets on eSport games.[54]

Esports gambling started with Skin gambling — using virtual goods such as in-game items as gambling currency — but it has since moved towards more traditional methods of gambling. In 2018, 81% of gamers in Russian bought virtual goods.[55] These virtual goods, which mostly consist of cosmetic items that modify the player's in-game appearance (or "skins"), have an intrinsic value to the players, but in popular gaming titles they are actually sold and traded for cash too.

A string of match-fixing scandals have already occurred in major esports events, affecting Counter-Strike, League of Legends, Dota 2, and Overwatch tournaments. A Dota 2 professional player known as Bryan Freddy "SmAsH" Machaca Siña from Peru was banned from Valve-endorsed competitions after it was concluded that his team intentionally lost in 2016.[56]

If a team is playing poorly, a surge of bets might be placed on the opposing team. Suspicions arise when those mistakes are preceded by high stakes wagers.



[redacted]

Offline

Lurker

Posts:	2
Joined:	Jun 28, 2019
Reputation:	0
Likes:	0
Credits:	0
Leecher level:	Neutral

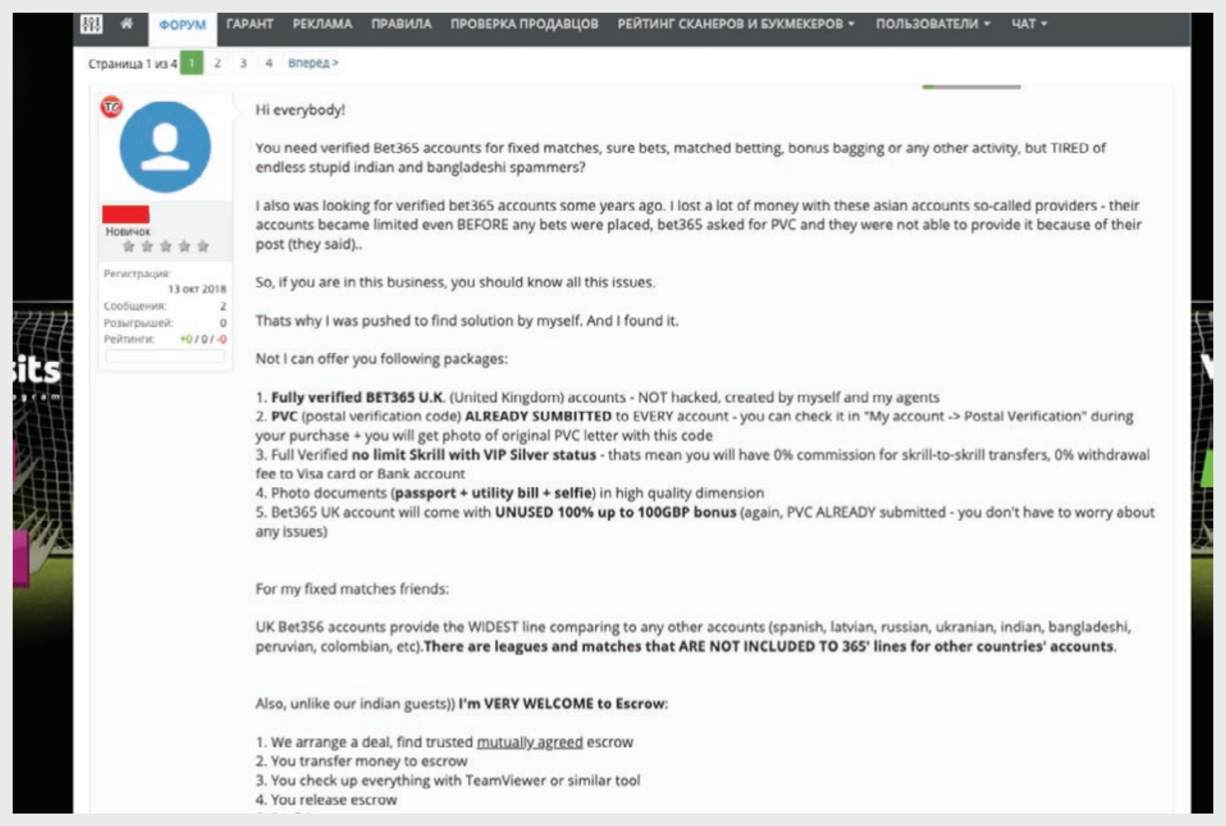
Posted 28 June 2019 - 09:59 AM

#1

Long story short,we used to play semi pro cs 1.6 in our region and we we're teammates and played tournaments like qualis for WESG 2008 in our country,Later on he played on csgo for a breif while in 2013 and then he became a semi pro coach and then a manager of a pro team,and he went to many tournaments though out the years and met alot of people and he told me about match fixing and tells me info about it whenever he get's any

If interested in fixed matches info add me on discord
[redacted]

0



ФОРУМ ГАРАНТ РЕКЛАМА ПРАВИЛА ПРОВЕРКА ПРОДАВЦОВ РЕЙТИНГ СКАНЕРОВ И БУКМЕКЕРОВ ▾ ПОЛЬЗОВАТЕЛИ ▾ ЧАТ ▾

Страница 1 из 4 1 2 3 4 Вперед >

[redacted]

Новичок

Регистрация:	13 окт 2018
Сообщения:	2
Розыгрышей:	0
Рейтинги:	+0 / 0 / -0

Hi everybody!

You need verified Bet365 accounts for fixed matches, sure bets, matched betting, bonus bagging or any other activity, but TIRED of endless stupid indian and bangladeshi spammers?

I also was looking for verified bet365 accounts some years ago. I lost a lot of money with these asian accounts so-called providers - their accounts became limited even BEFORE any bets were placed, bet365 asked for PVC and they were not able to provide it because of their post (they said)..

So, if you are in this business, you should know all this issues.

Thats why I was pushed to find solution by myself. And I found it.

Not I can offer you following packages:

1. **Fully verified BET365 U.K.** (United Kingdom) accounts - NOT hacked, created by myself and my agents
2. **PVC** (postal verification code) **ALREADY SUMBITTED** to EVERY account - you can check it in "My account -> Postal Verification" during your purchase + you will get photo of original PVC letter with this code
3. Full Verified **no limit Skrill with VIP Silver status** - thats mean you will have 0% commission for skrill-to-skrill transfers, 0% withdrawal fee to Visa card or Bank account
4. Photo documents (**passport + utility bill + selfie**) in high quality dimension
5. Bet365 UK account will come with **UNUSED 100% up to 100GBP bonus** (again, PVC ALREADY submitted - you don't have to worry about any issues)

For my fixed matches friends:

UK Bet356 accounts provide the WIDEST line comparing to any other accounts (spanish, latvian, russian, ukranian, indian, bangladeshi, peruvian, colombian, etc).**There are leagues and matches that ARE NOT INCLUDED TO 365' lines for other countries' accounts.**

Also, unlike our indian guests)) **I'm VERY WELCOME to Escrow**:

1. We arrange a deal, find trusted mutually agreed escrow
2. You transfer money to escrow
3. You check up everything with TeamViewer or similar tool
4. You release escrow

Figure 29. Forum posts offering a match-fixing service

Match-fixing is a common issue for traditional sports, and we believe that it will become a challenge for esports too. Match-fixing is actually illegal in South Korea and the U.S., and players can be banned or disqualified for match fixing. The term “322,” shorthand for match-fixing, is now common in the esports vocabulary. The term was coined after a player bet US$322 against his own team during a Dota 2 competition in 2013. In 2019, League of Legends player Condi was banned from competitive League of Legends games after violating match-fixing and gambling rules.[57]

Politically motivated and targeted attacks will increase

We expect to see nation state actors attempting to influence politics in esports and cause identity theft, financial loss, and reputation damage to businesses and players.

Advanced persistent threat (APT) groups have already taken advantage of the gaming industry. A good example is the financially motived APT41, which has been targeting gaming platforms with ransomware since 2012.[58] The group is still active and has evolved to espionage campaigns.[59] Another organization called the Winnti group targeted three Asian gaming companies with a backdoor trojan.[60] This could happen to esports companies as well.

Also consider the 2018 Winter Olympics opening ceremony, where cybercriminals actually brought the Wi-Fi service down.[61] Attendees were unable to print their tickets; internet services were down; and TV media was offline. Months before the Olympics started, APT28 (Pawn Storm) actors deployed coordinated attacks: they released fake news reports and compromised email accounts of the International Olympic Committee, allegedly in retaliation for Russia's doping suspension.[62] Two years before, the same group published stolen medical data belonging to mostly British and American athletes from the Summer Olympics Games in Rio de Janeiro.[63] If esports became an Olympic event or was included in other international games, we could see cybercriminals attacking the event in a similar way.

We predict that companies involved with esports will be open to certain risks if the games ever become an Olympic sport — and we believe they are already on the way. In 2018, esports was incorporated as a demonstration sport in the Jakarta Palembang 2018 Asia Games, which included titles such as League of Legends, Hearthstone, StarCraft II, Clash Royale and Arena of Valor. Esports was initially announced as a medal event in the 2022 Hangzhou Asia Games, but it has not been officially added to the program as of September 2019.[64] The Asian Games, which is governed by the Olympic Council of Asia, is the world's second-largest multi-sport event after the Olympics. The International Olympic Committee (IOC) has also been in talks with international committees on the future of esports in an Olympic event. As of now, IOC is still exploring this topic and has not made any official statements but the interest shown is noteworthy in itself.

Conclusion

We have no doubts that cybercriminals will heavily target the esports industry starting this year. Most importantly, through analysis of the esports market and the technology behind it, we strongly believe that it will face the same types of cyberattacks that the gaming community is already facing — but on a larger scale. Also, with esports predicted to join the Olympics in the future, new challenges lie ahead — matches among nations might inspire nation-sponsored hackers to rig games for pride and bragging rights.

These threats should also concern the parties and organizations (such as game developers, event organizers, and sponsors) with ties to the esports industry. They have to be careful as such exposure may lead to financially or politically motivated attacks. Both brand reputation and company earnings are at risk here.

Finally, the players have to pay more attention to their online security and demand more security from the platforms (such as game servers and social media) that store or access their profiles, since any compromise could put money and credibility at risk.

It should be said that our message is not that the esports industry is unsafe. The gaming companies and organizers are well aware of their status as targets, and they are always on the lookout for new cheating techniques and tools. They are constantly adding new security features to their processes and infrastructure. There are also different anti-cheat services that are specifically geared towards protecting esports and gaming competitions.[65, 66] This research effort was done to raise awareness about the risks we predict evolving in the near future.

References

1. Hilary Russ. (13 February 2019). *Reuters*. "Global esports revenues to top $1 billion in 2019: report."Last accessed on 21 October 2019 at https://www.reuters.com/article/us-videogames-outlook/global-esports-revenues-to-top-1-billion-in-2019-report- idUSKCN1Q11XY.

2. Mary Hanbury. (29 July 2019). *Business Insider*. "This 16-year-old gamer is $3 million richer after winning the Fortnite World Cup." Last accessed on 21 October 2019 at https://www.businessinsider.com/16-year-old-kyle-giersdorf-wins-3-million-in-fortnite-world-cup-2019-7.

3. Newzoo. (April 2019). *Strive*. "Global esports market report 2019". Last accessed on 21 October 2019 at https://strivesponsorship.com/2019/06/18/newzoo-global-esports-market-report-2019/.

4. Mike Stubbs. (27 July 2019). *Forbes*. "The International 9 'Dota 2' Tournament Prize Pool Breaks $30 Million". Last accessed on 21 October 2019 at https://www.forbes.com/sites/mikestubbs/2019/07/27/the-international-9-dota-2-tournament-prize-pool-breaks-30- million/#4429cdd22c07.

5. Kelvin Chan. (1 October 2019). *Phys Org*. "Ready student one? Universities launch degrees in esports". Last accessed on 21 October 2019 at https://phys.org/news/2019-10-ready-student-universities-degrees-esports.html.

6. ESC. Escharts. "Esports Viewership Stats for 2018". Last accessed on 21 October 2019 at https://escharts.com/2018.

7. Syracuse Staff. (18 January 2019). *Whitman Syracuse University*. "With Viewership and Revenue Booming, Esports Set to Compete with Traditional Sports". Last accessed on 21 October 2019 at https://onlinebusiness.syr.edu/blog/esports-to-compete-with-traditional-sports/.

8. Cristina Gough. (8 February 2019). *Statista*. "Leading eSports countries ranked by number of active players 2018". Last accessed on 21 October 2019 at https://www.statista.com/statistics/780631/esports-competition-country-number-of-players-world/.

9. Cristina Gough. (11 June 2019). *Statista*. "Share of eSports fans worldwide 2019, by region". Last accessed on 21 October 2019 at https://www.statista.com/statistics/673740/share-of-esports-viewers-by-region-worldwide/.

10. Cristina Gough. (8 February 2019). *Statista*. "Leading eSports countries ranked by number of active players 2018". Last accessed on 21 October 2019 at https://www.statista.com/statistics/780631/esports-competition-country-number-of-players-world/.

11. Robert Adams. (22 November 2018). *Tech Raptor*. "$280m Hangzhou Esports Town Opens In Advance of 2022 Asian Games". Last accessed on 21 October 2019 at https://techraptor.net/content/hangzhou-esports-town.

12. Sam Edge. (2 July 2019). *Esports Middle East*. "This is how you can participate in The International 9 open qualifiers from the Middle East". Last accessed on 21 October 2019 at https://es.me/en/this-is-how-you-can-participate-in-the-international-9-open-qualifiers-from-the-middle-east/.

13. Mariana Rosignoli. (20 July 2019). *Law in Sport*. "The rise of e-Sports in Brazil - and how football clubs are getting on board". Last accessed on 21Octover 2019 at https://www.lawinsport.com/topics/sports/item/the-rise-of-e-sports-in-brazil-and-how-football-clubs-are-getting-on-board.

14. Newzoo. (11 July 2019). *Newzoo*. "Russia GamesMarket 2018". Last accessed on 21 October 2019 at https://newzoo.com/insights/infographics/russia-games-market-2018/.

15. Newzoo. (1 August 2018). *Newzoo*. “Japan Games Market”. Last accessed on 21 October 2019 at https://newzoo.com/insights/infographics/japan-games-market-2018/.

16. Owen Good. (25 October 2019). *Polygon*. “CS:GO pro caught cheating gets five-year ban.” Last accessed on 21 October 2019 at https://www.polygon.com/2018/10/25/18023236/forsaken-cs-go-cheating-optic-india-ban.

17. Danny Palmer. (22 August 2019). *ZDNet*. “Phishing: These are the companies that hackers impersonate when they try to steal your data.” Last accessedon 21 Otober 2019 at https://www.zdnet.com/article/phishing-these-are-the-companies-that-hackers-impersonate-when-they-try-to-steal-your-data/.

18. Andrew Amos. (23 February 2019). *DOT Esports*. “First permanent competitive ban for boosting in Overwatch handed down in China”. Last accessed on 21 October 2019 at https://doteSports.com/overwatch/news/first-permanent-competitive-ban-for-boosting-in-overwatch-handed- down%ef%bb%bf-in-china.

19. Colin Stevens. (11 December 2018). *IGN*. “South Korea Makes Boosting Other Players’ Game Levels Illegal”. Last accessed on 21 October 2019 at https://sea.ign.com/esports/144233/news/south-korea-makes-boosting-other-players-game-levels-illegal.

20. Christopher Livingston. (9 August 2017). *PCGamer*. “Streamers vs. stream-snipers: why cheaters will always prosper on Twitch”. Last accessed on 21 October 2019 at https://www.pcgamer.com/stream-sniping/.

21. Matthew Gault. (26 June 2019). *Vice*. “‘Dota 2’ Player Who Used Programmable Mouse Disqualified His Team From $15 Million Tournament”. Last accessed on 21 October 2019 at https://www.vice.com/en_us/article/3k49z9/dota-2-player-who-used-programmable-mouse-disqualified-his-team-from- dollar15-million-tournament.

22. Andrew Norton. (28 November 2018). *Elecspo*. “CS:GO Cheater ra1f Exposes Cheating in CS:GO”. Last accessed on 21 October 2019 at https://www.elecspo.com/games/csgo-cheater-ra1f-exposes-cheating-in-csgo/.

23. Luke Plunkett. (3 July 2019). *Kotaku*. “DDoS Attacker Will Spend Two Years In Prison”. Last accessed on 21 October 2019 at https://kotaku.com/ddos-attacker-will-spend-two-years-in-prison-1836091110.

24. Matt Weinberger. (5 August 2015). *Business Insider*. “An $18 Million Video Game Tournament Taken Down by a Hack Attack”. Last accessed on 21 October 2019 at was https://www.businessinsider.com/dota-2-the-international-match-downed-by-hack-attack-2015-8.

25. Bree Royce. (7 August 2017). *Massively Overpowered*. “Albion Online hit with ransom demand during weekend DDOS outages”. Last accessed on 21 October 2019 at https://massivelyop.com/2017/08/07/albion-online-hit-with-ransom-demand-during-weekend-ddos-outages/.

26. Ahmad Nassiri. (24 June 2019). *A10*. “This Is How Much Time and Money a DDoS Attack Will Cost You”. Last accessed on21 October 2019 at https://www.a10networks.com/blog/this-is-how-much-time-and-money-ddos-attack-will-cost-you/.

27. The MITRE Corporation. *CVE*. “CVE-2012-4558.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4558.

28. The MITRE Corporation. *CVE*. “CVE-2013-1896.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1896.

29. The MITRE Corporation. *CVE*. “CVE-2012-3499.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3499.

30. The MITRE Corporation. *CVE*. “CVE-2014-0231.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0231.

31. The MITRE Corporation. *CVE*. “CVE-2017-7679.” Last accessed on 25 October 2019 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7679.

32. The MITRE Corporation. *CVE*. “CVE-2018-1312.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1312.

33. The MITRE Corporation. *CVE*. “CVE-2010-5107.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5107.

34. The MITRE Corporation. *CVE*. “CVE-2016-0778.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0778.

35. The MITRE Corporation. *CVE*. “CVE-2012-2531.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2531.

36. The MITRE Corporation. *CVE*. “CVE-2018-10549.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10549.

37. The MITRE Corporation. *CVE*. “CVE-2018-10548.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10548.

38. The MITRE Corporation. *CVE*. “CVE-2018-10545.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10545.

39. The MITRE Corporation. *CVE*. “CVE-2014-1692.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1692.

40. The MITRE Corporation. *CVE*. “CVE-2017-15906.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15906.

41. The MITRE Corporation. *CVE*. “CVE-2019-11039.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11039.

42. The MITRE Corporation. *CVE*. “CVE-2019-11040.” Last accessed on 25 October 2019 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11040.

43. Lawrence Abrams. (9 April 2018). *Bleeping Computer*. “PUBG Ransomware Decrypts Your Files If You Play PlayerUnknown’s Battlegrounds”. Last accessed on 22 October 2019 at https://www.bleepingcomputer.com/news/security/pubg-ransomware-decrypts-your-files-if-you-play-playerunknowns- battlegrounds/.

44. Jose Vilches. (23 March 2015). *Techspot*. “New crypto-ransomware attack holds your PC games hostage unless you cough up $500”. Last accessed on 22 October 2019 at https://www.techspot.com/news/60130-ransomware-attack-holds-pc-games-hostage.html.

45. Vincenzo Milella. (March 2019). *Esports Tales*. “CS:GO Rank Distribution and Percentage of Players March 2019”. Last accessed on 22 October 2019 at https://www.esportstales.com/csgo/rank-distribution-and-percentage-of-players.

46. Monique Bonner et. Al. (June 2019). *Akamai*. “Web Attacks and Gaming Abuse”. Last accessed 22 October 2019 at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf.

47. Trend Micro. (11 November 2016). *Trend Micro Simply Security*. “The money-making world of gaming cybercrime”. Last accessed on 22 October 2019 at https://blog.trendmicro.com/money-making-world-gaming-cybercrime/.

48. Chris Brook. (9 January 2017). *Threat Post*. "Following Extortion Attempt, Gaming Network ESEA Breached, 1.5M Profiles Leaked". Last accessed on 22 October 2019 at https://threatpost.com/gaming-network-esea-breached-1-5m-profiles-leaked/122933/.

49. Bdoqq. (April 2019). *Reddit*. "Account stolen and now support wants me to pay them money". Last accessed on 22 October 2019 at https://www.reddit.com/r/blackdesertonline/comments/b9iauf/account_stolen_and_now_support_wants_me_to_pay/.

50. M1ghty boy. (August 2019). *Reddit*. "My epic games account was compromised and all my vbucks were spent (tragic I know) and I added as much detail as I know but for some reason their customer support system cut off the message about 1/4 of the way through and now I don't know what I can do to prove it's me". Last accessed on 22 October 2019 at https://www.reddit.com/r/fuckepic/comments/chg3e4/my_epic_games_account_was_compromised_and_all_my/.

51. Lawrence Abrams. (18 August 2019). *Bleeping Computer*. "Steam Accounts Being Stolen Through Elaborate Free Game Scam". Last accessed on 22 October 2019 at https://www.bleepingcomputer.com/news/security/steam-accounts-being-stolen-through-elaborate-free-game-scam/.

52. Trend Micro Research. (n.d.). *Trend Micro Security News*. "The Cybercriminal Underground". Last accessed on 22 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground.

53. Rey Mashayekhi. (10 April 2019). *Fortune*. "Inside the Battle for the Future of Sports Betting". Last accessed on 22 October 2019 at https://fortune.com/longform/sports-betting-battle/.

54. Gambling Commission. (2017 March). *Gamble*. "Virtual currencies, eSports and social casino gaming – position paper". Last accessed on 22 October 2019 at https://live-gamblecom.cloud.contensis.com/PDF/Virtual-currencies-eSports-and-social-casino-gaming.pdf.

55. Newzoo. (11 July 2018). *Newzoo*. "Russia Games Market 2018". Last accessed on 22 October 2019 at https://newzoo.com/insights/infographics/russia-games-market-2018/.

56. The Score Staff. (24 March 2016). *The Score Sports*. "SMASH, Mstco, ztok marked "Ineligible" before roster lock". Last accessed on 22 October 2019 at https://www.thescoreesports.com/dota2/news/6896.

57. Alex Leckie-Zaharic. (18 June 2019). *DOT Esports*. "Condi suspended for 18 months as major LPL match-fixing scandal exposed". Last accessed on 22 October 2019 at https://dotesports.com/league-of-legends/news/condi-suspended-for-18-months-as-major-lpl-match-fixing-scandal- exposed.

58. Trend Micro Cyber Safety Solutions Team. (19 April 2019). *Trend Micro Security Intelligence Blog*. "Of Pigs and Malware: Examining a Possible Member of the Winnti Group". Last accessed on 22 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/.

59. Nalani Fraser et. Al. (7 August 2019). *Fire Eye*. "APT41: A Dual Espionage and Cyber Crime Operation". Last accessed on 22 October 2019 at https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html.

60. Ryan Stewart. (12 March 2019). *Cyware*. "Winnti cyberespionage group breaches three Asian gaming companies to install a backdoor Trojan."Last accessed on 22 October 2019 at https://cyware.com/news/winnti-cyberespionage-group-breaches-three-asian-gaming-companies-to-install-a-backdoor- trojan-723a04a6.

61. Andrew Liptak. (25 February 2018). *The Verge*. "Russia was behind the cyberattack during the opening ceremonies for the 2018 Winter Olympics". Last accessed on 22 October 2019 at https://www.theverge.com/2018/2/25/17050868/winter-olympics-2018-russia-north-korea-cyberattack-opening-ceremonies.

62. Louise Matsakis. (18 January 2018). *Wired*. “Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban”. Last accessed on 22 October 2019 at https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/.

63. Louise Matsakis. (18 January 2018). *Wired*. “Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban”. Last accessed on 22 October 2019 at https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/.

64. Hongyu Chen. (10 April 2019). *Esports Observer*. “No Esports Yet for Hangzhou Asia Games, NEXT Adds China UnionPay and Li-Ning Sponsorships”. Last accessed on 22 Ocober 2019 at https://esportsobserver.com/china-recap-april10-2019/.

65. Easy Anti Cheat. (n.d.). “Don’t Bear with the Cheaters”. Last accessed on 22 October 2019 at https://easy.ac/en-us/.

66. Battleeye. (n.d.). “The Anti CheatGold Standard”. Last accessed on 22 October 2019 at https://www.battleye.com/.

TREND MICRO™ RESEARCH
Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com