Cybercrime and Online Video Games

Emilio Lopez
Case Western Reserve University
Cleveland, USA
eil11@case.edu

Cameron Hochberg
Case Western Reserve University
Cleveland, USA
clh137@case.edu

Michael Silverman
Case Western Reserve University
Cleveland, USA
mhs126@case.edu

Anthony Smith
Case Western Reserve University
Cleveland, USA
aas182@case.edu

ABSTRACT

The growth of online video games has yielded a vast underground economy of criminals who sell exploits and credentials to give gamers unfair advantages in the games. This paper studies the sale of "crimeware" connected to the Epic Games' "Fortnite: Battle Royale" video game. The authors created a webscraping tool to collect large amounts of data from a hacker forum to analyze key distributers in the economy. After analyzing approximately 7000 comments and 113 threads posted on the forum, the authors found that crimeware called "Aimbots" and the CaaS (Crimeware-as-a-Service) "Account Sales" were the most common things for sale in the Hack Forums marketplaces. The authors propose several solutions that the developers can implement to combat the proliferation of underground economy dealing in Fortnite exploits.

CCS CONCEPTS

• **Information systems** → **Surfacing**; • **Applied computing** → **Evidence collection, storage and analysis**; • **Computing methodologies** → *Classification and regression trees.*

KEYWORDS

web scraping, sentiment analysis, cybercrime, video games

ACM Reference Format:
Emilio Lopez, Cameron Hochberg, Michael Silverman, and Anthony Smith. 2018. Cybercrime and Online Video Games. In *Proceedings of CWRU EECS349 '19: Final Project (EECS349 F19).* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Since their inception decades ago, video games have become hugely preavalent in society. Millions of people play video games as a hobby, and their demographics span all age groups, ethnicities, and socioeconomic class. In particular, online multiplayer video games have become hugely popular. Many of these games are highly competitive, and there any many players who look for unfair advantages in the form of video game cheats. Video game cheats give the player abilities to to outperform their opponents. This competitive milieu has led to the development of thriving marketplaces and economies devoted to creation and distribution of video game cheats. Online hacker forums are places where interested parties can sell, discuss, and review video game cheats. However, these vendors not only sell cheats but also online video game accounts. These are especially desirable to perons who have been forbidden from playing an online game by the developers - usually for cheating or other malicious behavior. Often, these accounts are stolen from innocent users and sold to malicious actors. Many of the players of online video games are children, and thus they are often the victims of account theft. This paper explores the crimware economy devoted to "Fortnite: Battle Royale."

2 BACKGROUND

2.1 Fortnite: Battle Royale

Developed by Epic Games, "Fortnite: Battle Royale" or "Fortnite" is a third-person shooter and battle royale online video game. The player must utilize a diverse arsenal of weapons to defeat 99 other human opponents and claim victory.

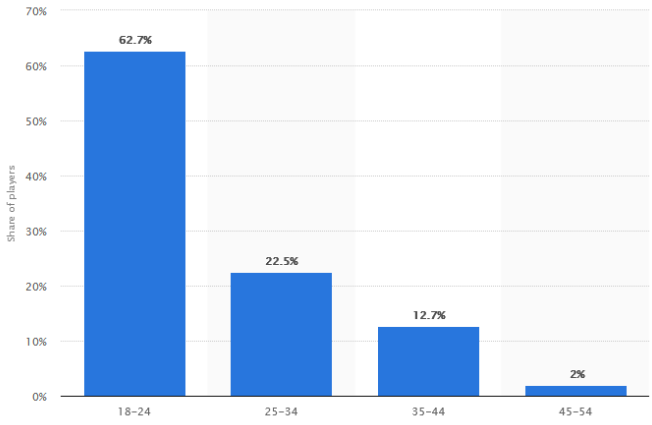


Figure 1: Fortnite Age Distribution

[3]

EECS349 F19, December 13, 2019, Cleveland, OH

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

2.2 Hack Forums

There exist many forums on the Internet for persons interested in computer hacking, but one the most visited is Hack Forums (hackforums.net). Ranked second in top sites for "hacking," [1] Hack Forums has several discussion boards on topics ranging from social engineering techniques to Internet-of-Things exploits. On Hack Forums, users make accounts to use the community forums: posting, searching, and even browsing requires an account to be registered. Users also can give feedback on each other. For example, a user with a high feedback score will be regarded as more trustworthy. Often, these users gain repute by participating in discussion or selling a legitimate product or service. Users can also privately message each other, without having to use another service like email. Due to Hack Forums' prominence and enablement of cybercrime, it merited our scrutiny to examine its contribution to cybercrime in the video game space.

2.3 Web Scraping

Web scraping refers to the process of extracting data from web pages, and the term typically implies the automation of this process. Data extracted from web pages will then be parsed to be usable. Often, websites will not provide easily accessible data sets of the website content, which means that a web scraping program must be written to extract the relevant information from the HTML present on the page. Given the sheer volume of information that must be collected, the best action is to implement our own program to scrape data from Hack Forums.

2.4 Sentiment Analysis

One of our tasks was to analyze the intentions behind each comment, whether they were criticizing the product or, on the contrary, if they were lauding the product. For that, we decided to use a Python package provided by scikit-learn.org We used 3 different machine learning techniques to classify each comment as either positive or negative:

- Stochastic Gradient Descent (SGD)

$$E(w,b) = \frac{1}{n}\sum_{i=1}^{n} L(y_i, f(x_i)) + \alpha R(w)$$

[6]

- Naive Bayes

$$\theta_y i = \frac{N_{yi} + \alpha}{N_y + \alpha n} where\ N_y i = \sum_{x \in T} x_i\ and\ N_y = \sum_{i=1}^{n} N_y i$$

[5]

- Support Vector machines (SVC)

$$sgn(\sum_{i=1}^{n} y_i \alpha_i K(x_i, x) + \rho)$$

[7]

Each algorithm gives each comment a probability to be either positive, negative or neutral. It also classifies whether a comment involves a trade or a Q&A with the thread poster. We sum each algorithm's score and determine based on that score whether the comment is positive, negative or neutral. Below are charts showing the percentage of comments that were deemed positive, negative and neutral, percentage of comments involving a trade and percentage of comments with a Q&A. For the trade and Q&A charts, a one represents a trade or Q&A and a zero represents no trade of Q&A.

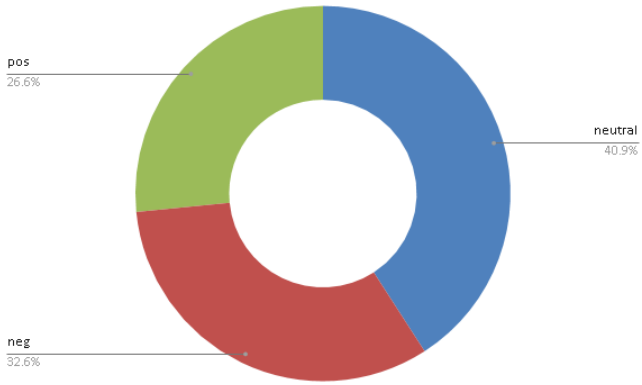


Figure 2: Sentiment Analysis Chart

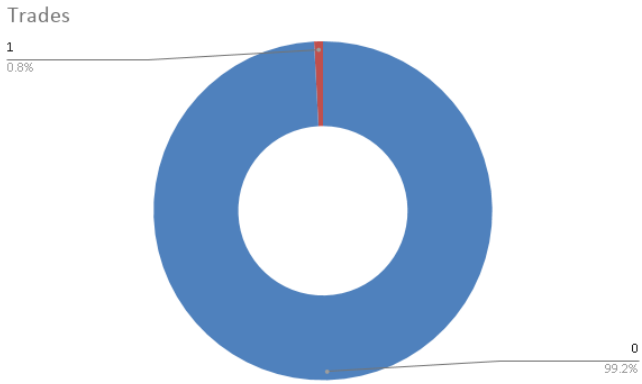


Figure 3: Trade Chart

Along with the webscraper was some manual analysis. Because we could not find out all information about a thread or comment from the webscraping, we had to manually enter in some data. One of the categories we had to manually analyze was the payment type for the product or service the poster was selling. The payments methods ranged from standard credit cards all the way to gift cards. Below is a chart depicting the distribution of payment methods. Please keep in mind that not all posters stated the payment methods and some posts allow for more than one type.

3 CRIMEWARE

3.1 Video Game Cheats

3.1.1 Aimbots. Aimbots are a sub set of game hacks. These reffer to scripts that run on the client side of the game and track things such as hit boxes of other players in the game and aim for you once

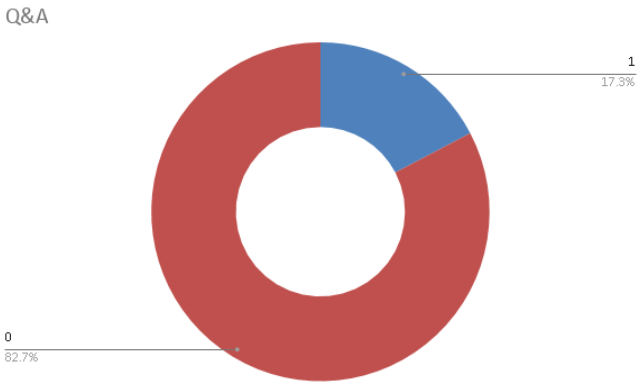


Figure 4: Q&A Chart

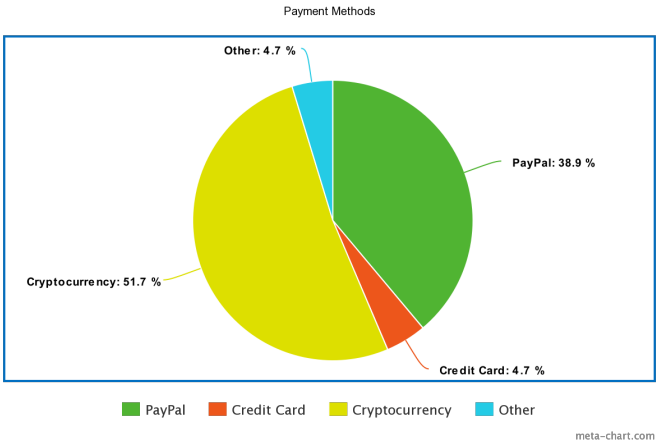


Figure 5: Payment Method Chart

activated. It is an easy kind of cheat to spot as it will usually result in unhuman reflexes or movement or such things as wall tracking where a player is aiming at you through a wall. Since they also track only specific areas, a statistical analysis of the areas where the player regularly hit his targets can reveal whether or not he was hacking. Normal humans can't aim at the same target over a long period of time and will usually stay within one or two standard deviations of the mean for any given area. Someone who aimbots on the other hand will usually have one area that is way above the mean.

3.1.2 Hacks. There are several versions of this cheat but there is usually two types: a script that uses a bug from the developer to allow the user to view more than he should be making walls transparent or "see-through"; another would be to make walls non solid objects allowing the player to shoot through walls or even hide in them. These hacks usually relly on the fact the FPS games in particular send only the raw positional information of players and let the player or client's 3D renderer to hide other players behind walls or through "fog of war". These can be turned off from the client side and thus make it look like the players are moving around what seams like an empty space. Obviously a completely empty map serves no purpose for the hacker as he couldn't navigate the map properly either. This third party software allows the user to only hide certain surfaces from its client 3D renderer so that the hacker may have an edge compared to other players.

3.1.3 Nuking or artificial lag. The sub genre of hacks, as its name suggests, consists of artificially generating lag between the client and the server in order to gain an advantage. In some games, hits aren't registered until the server registeres a hit. In this case, overloading the server with packets just enough to create lag for every player on the server but not enough to cause the server to crash allows you to stall the game enough for you to be able to win effortlessly in the next round.

3.1.4 Code Injection. "Code Injection is the general term for attack types which consist of injecting code that is then interpreted/executed by the application."[4] Usually these attacks are the result of poor data validation from input/output. Code Injection deffiers from Command Injection in the sense that the attacker, in the case of Command Injection, is limited by what the API has to offer; while Code Injection is only limited by the language used. The risk from Code Injection if that, if the attack is successful, this can lead to loss of data, confidentiality and loss of availability.

3.2 Account Sales

One of the more common video game hacks is account selling. This isn't giving a player an unfair advantage but selling hacked accounts to people. It is not too uncommon to see somone's account information for sale on hackforums without their knowledge. Selling accounts can be a lucrative business and gaining access to accounts through techniques such as phishing is not the most difficult form of hacking out there. Given Fortnite's popularity with people under 18, we feel the game's players are more at risk for these kinds of attacks than for other online games.

4 METHOD

4.1 Web Scraper Implementation

We opted to implement our web scraping program in the Python 3 programming language. Given the time constraints of the project, we found that Python matched our needs well given its rapid development time. In addition, the external library support of Python was deemed essential in traversing Hack Forums and extracting the data. We also used Selenium web automation tool and its relevant Python bindings. For Python, we also used the "Requests" and "BeautifulSoup" libraries. "Requests" simplifies the creation of HTTP requests to obtain web content, and "BeautifulSoup" is an HTML parser which assists in unraveling the web page content to extract. Finally, to actually create the requisite Excel file, we used the OpenPyXL library to generate and populate the file.

Since the program's scraping is based on the website's specific content and design (e.g., names of tag classes and id attributes in the page HTML), the web scraper can only be used for Hack Forums. Hack Forums provided some unique challenges for our scraping. For example, the website seems to heavily rely on the PHP programming language. For searching the forum threads, this is troublesome, because the search itself is not a simple web endpoint

where the search term can be replaced. This design decision requires the use of Selenium to "click" buttons and enter search terms into the website's forms. For each page of search results, the URL for the thread is acquired along with the original poster, number of replies, and other relevant information. With the URL for a thread, the comment pages are requested and the relevant information per comment is scraped from each page for the thread.

After all the is collected from a search, the data is written to an Excel file which contains all the results. With all the data aggregated, manual data analysis can begin.

However, the data analysis for sentiment does not always apply to the comment. For example, if the comment is actually a question or a request to receive a private message, then AI sentiment analysis of the comment is likely irrelevant. Therefore, the comments must be analyzed for different criteria. For example, if the comment is actually a user "bumping" the thread, then it should be discarded. It was not feasible for us to develop an AI solution to accurately categorize comments in each possible scenario, so we have chosen to automate the collection of data but manually classify it.

5 RESULTS

After executing our web scraping suite of programs, we successfully collected a large amount of data within the following parameters. Each thread we scraped had to have a minimum of 30 replies to the topic, ensuring that only intensely discussed crimeware and CaaS would be analyzed.

The program successfully searched Hack Forums and found 126 threads with a total of 7994 comments. About half of these were video game cheats crimewarea, and the other half was Account Sales and in-game currency sales. However, a few threads were ultimated not related to our research. For example, a user had posted threads advertising their livestreamed playing of Fortnite. It did not have any relation to crimeware. Additionally, our scraper extracted a few general discussion threads of people arguing about the game. When we filtered from our data these threads and their respective comments, about 900 comments were deemed irrelevant from a total of 13 threads.

5.1 Key Players

In the context of our project, the key players in the Fortnite hacker forums are those who have the most threads and/or comments under their names. We defined a user as a key player if they posted more than one thread or more than fifty comments from our 126 threads and 7994 comments. We determined these metrics by manually analyzing the comments and threads and determining who were the minority of more active users. These active user threads will usually take the form of either crimeware or CaaS with the poster selling to whoever can pay with some supposedly "legal" methods scattered throughout. Some of the more popular services are account selling, radar hacks, aimbot hacks and cheaper V-Bucks. Below are two pie charts depicting the thread and comment counts with the labels identifying the greater contributors.

5.1.1 Wyattz. Wyattz can be considered the most active user on the Fortnite hacker forums being tied for the most threads at three and having the most comments at 162. Wyattz is also a veteran member of hackforums.net and appears to be a trusted source of

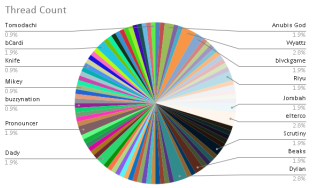


Figure 6: Thread Count

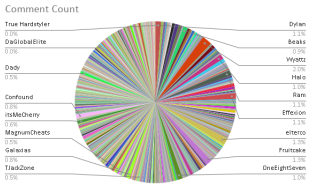
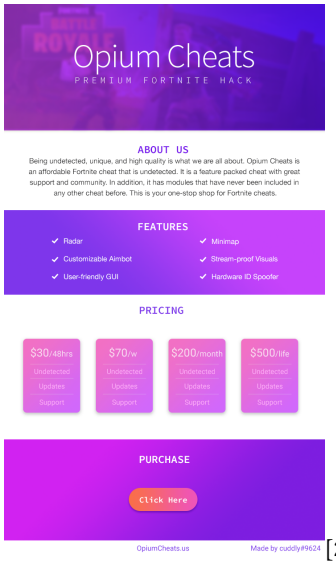


Figure 7: Comment Count

"legal" software and methods. His Fortnite posts revolve around making money playing Fortnite using what he claims to be a legal method. Since we were unable to access his method we could not determine its legality but his customers have commented back with general satisfaction. The other factor that makes Wyattz interesting is his number of comments. These comments were not made on other threads but on his own. His comments are either responses to other user's comments or simply declarations that he is online and ready to talk. Wyattz places a lot of effort into his work on hackerforum so even though his comments rarely range outside his own threads and his product is not explicitly illegal, he is still a major player worth looking at.

5.1.2 Jombah. Jombah is also considered a key player on the Fortnite hacker forums even though he is on the lower end of the thread and comment counts with only two threads and 43 comments. He still passes the threshold for being a key player but the reason he is being focused on is due to his product. Jombah sells Fortnite accounts which is one of the crimewares we are focusing on. Jombah's products are "premium" accounts which he appears to sell for a relatively cheap price as compared to other sellers though unlike some other sellers he does not offer custom accounts that a buyer can specify. Jombah is also a decently active user on hackerforum.net though not as active as Wyattz or as well liked by his customers. Jombah's relevance lies not with his stellar service but with the product he provides.

5.1.3 Dylan. The last key player we will feature is probably the most important figure in the overall Fortnite hackforum community, though that is not saying much. Dylan provides the cheats for users such as radar and silencers. His presentation and communication with clients is professionally done and there are very few complaints regarding his product. While this is important for Dylan's hierarchy as a key player, what is most important about him is that he interacts with other Fortnite posters. While analyzing threads and comments, we noticed that very few posters comment beyond their threads. There is little to no communication among the Fortnite hackforum



[2]

Figure 8: Dylan's Product Advertisement

community. Dylan is the exception to the rule. He comments on other threads whether he is providing explanations of services, vouching for others or shooting down fraudulent products. Dylan is not the most active user in his community, but nobody is as far reaching making him the most important key player in this community.

5.2 Key Players Conclusion

After analyzing the comments and threads we formed a decent understanding of the hackforum Fortnite community. The community doesn't appear to revolve around any given person or group with many independent people providing products and/or services to Fortnite players. Even the most active figures in the community don't communicate with each other in general. The Fortnite threads almost cannot be considered a community, more like a loose collection of people with similar ideas. This makes the key players less important as nobody has control over any aspect of the community.

6 SOLUTIONS

6.1 Video Game Cheats

6.1.1 Mirrored server design. The general idea for this is that all client functionality runs either solely on the server or alternatively, it runs synchronously between the client and a miror of the game server. This way, the state of the game is continously validated where the miror server uses the exact same inputs received to validate the results from the client game. If there is ever a discrepency, the client's game session resets and thus prevents cheating by reseting the game state to the last valid state of the game. One problem that isn't so common is that this method requires a lot of bandwidth, storage and memory but nowadays, most of those concerns are minimal.

6.1.2 Pattern Detection/Analyze performance. This is a common way of detecting cheats for most online games since it rarely affects players direcly due to its none invasive nature. Like normal anti virus software, some program in the game will scan the hard drive to find any know cheat software or cheat codes. Another is that it will analyze the statistical data from the player. For example, you might want to see how often a player is able to hit a certain part of the hitboxes of other players. If there is a statistical different greater than the expected standard deviation, there is a high chance that the player is cheating. However, thsi method also leads to false positive/negative. Very highly skilled players may get flagged as cheaters because of how good they are, while others may use cheats but in areas that aren't verified by the statistical data and thus be flagged as regular player.

6.1.3 Player Supervision. This is a more intrusive method of detection as it requires someone monitoring the player. Obviously, it is impossible to monitor every single player in the game but this method can be used in conjonction with Pattern detection. If a player is flagged, he doesn't have to be banned just yet, that could mean that someone can start reviewing that player's gameplay and decide for himself whether or not that player is cheating or not. Some games have implemented player supervision by allowing the community to send reports of disruptive behavior or suspected cheating. Reports can include data such as screenshots, videos, and chatlogs that are then sent to the administrators of the gamef for review. If the player reported happens to be cheating any form of punishment can be dispensed.

6.1.4 Sandboxing. Sandboxing reffers, in security, to a mechanism that allows you to separate running programs. This prevents most vulnerabilities from spreading throught the system. Since it is often used on unested or untrusted code, code injection can't propagate and thus can't work, preventing the cheat from ever working in the first place. This also allows the commpany to avoid banning players since the cheats don't work.

6.2 Account Theft

Given the prominence of account theft and sales, we propose that Fortnite - and other online video games like it - mandate the use of multi-factor authentication (MFA) in combination with username and password credentials to secure accounts. Epic Games has already implemented an MFA tool for players to use to protect their accounts, and the game incentivizes players to use it; however, we argue that optional usage of MFA is insufficient, and that online video game developers should require the usage of MFA as part of accessing one's account. According to a study from Google, adding a recovery phone number reduced the prevented "100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks" in their study" [8]. Although this study is specific to Google's implementations and security policies, it is a valuable heuristic to show how multi-factor authentication can greatly bolster security for a user.

Additionally, we suggest that video game developers create their own solution instead of relying on a simple SMS numerical code. SMS messages can be intercepted, and an attacker can actually acquire the code for login. However, a robust, novel implementation can likely thwart the majority of hackers and provide for the safety of a user's account.

7 CONCLUSION

The solutions that we proposed can most effectively curtail the growth of crimeware and CaaS in the online video game community of Fortnite. For the game to maintain a strong population of players, the proliferation of crimware must be addressed. No player will feel compelled to continue investing time into Fortnite if cheating is unpunished and undetected. Our solutions to video game cheats ensure that games are fair for all players, and our solution to account sales inhibits the ability of cybercriminals to infiltrate and sell a legitimate player's account. The implementation of even a few of our solutions can greatly improve the player experience. And the relative ease with which our scraper was implemented could be emulated by video game developers to surveil Hack Forums to prepare countermeasures to new cheats.

ACKNOWLEDGMENTS

We would like to thank Professor Yanfang "Fanny" Ye of Case Western Reserve University for assisting us with the completion of our project. The guidance helped to refine the direction of our research and focus. With her assistance, we found a novel concept to explore.

REFERENCES

[1] Amazon. [n.d.]. *The top 500 sites on the web by category (Hacking).* https://www.alexa.com/topsites/category/Top/Computers/Hacking
[2] Dylan. [n.d.]. *Opium Cheats premium fortnite hack.* https://hackforums.net/showthread.php?tid=5866690
[3] Christina Gough. [n.d.]. Distribution of players of Fortnite in the United States as of April 2018, by age group. ([n. d.]). https://www.statista.com/statistics/865616/fortnite-players-age/
[4] OWASP. [n.d.]. *Code Injection.* https://www.owasp.org/index.php/Code_Injection
[5] scikit learn. 2019. *Naive Bayes.* https://scikit-learn.org/stable/modules/naive_bayes.html
[6] scikit learn. 2019. *Stochastic Gradient Descent.* https://scikit-learn.org/stable/modules/sgd.html#classification
[7] scikit learn. 2019. *Support Vector Machines.* https://scikit-learn.org/stable/modules/svm.html#classification
[8] Kurt Thomas and Angelika Moscicki. [n.d.]. *New research: How effective is basic account hygiene at preventing hijacking.* https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html