Cybercrime and Online Video Games

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

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

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

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

ABSTRACT

[REWRITE THIS AT END] 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.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

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 *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, **??** 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."

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

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.

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" 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), Naive Bayes, Support Vector machines (SVC). Each algorithm gives each comment a probability to be either positive or negative. We sum each algorithm's score and determine based on that score whether the comment is positive, negative or neutral.

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 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.

3.2 Account Sales

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.

[DISCUSS OUR TECHNIQUE OF DATA ANALYSIS - i.e, sentiment analyze all, then manually confirm other details]

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.

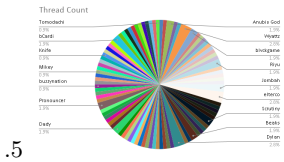

Figure 1: Thread Count

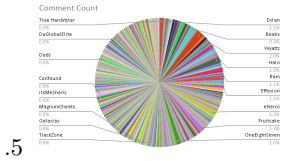

Figure 2: Comment Count

Figure 3: Thread and Comment Pie Charts

5 RESULTS

[RAW RESULTS DATA, THEN REFINED DATA] [TABLES WOULD BE HELPFUL HERE]

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 104 threads and 7932 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 "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 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

[MIN 1 PARA PER OUR SOLUTIONS, EXPLAINING WHY ADDRESSES]

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. 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

[CONCLUDE] [ALSO DISCUSS WHAT WE LEARNED (I think she wants that...)]

8 CITATIONS AND BIBLIOGRAPHIES

The use of BibTeX for the preparation and formatting of one's references is strongly recommended. Authors' names should be complete — use full first names ("Donald E. Knuth") not initials ("D. E. Knuth") — and the salient identifying features of a reference should be included: title, year, volume, number, pages, article DOI, etc.

The bibliography is included in your source document with these two commands, placed just before the `\end{document}` command:

```
\bibliographystyle{ACM-Reference-Format}
\bibliography{bibfile}
```

where "`bibfile`" is the name, without the "`.bib`" suffix, of the BibTeX file.

Citations and references are numbered by default. A small number of ACM publications have citations and references formatted in the "author year" style; for these exceptions, please include this command in the **preamble** (before "`\begin{document}`") of your LaTeX source:

```
\citestyle{acmauthoryear}
```

Some examples. A paginated journal article [**?**], an enumerated journal article [**?**], a reference to an entire issue [**?**], a monograph (whole book) [**?**], a monograph/whole book in a series (see 2a in spec. document) [**?**], a divisible-book such as an anthology or compilation [**?**] followed by the same example, however we only output the series if the volume number is given [**?**] (so Editor00a's series should NOT be present since it has no vol. no.), a chapter in a divisible book [**?**], a chapter in a divisible book in a series [**?**], a multi-volume work as book [**?**], an article in a proceedings (of a conference, symposium, workshop for example) (paginated proceedings article) [**?**], a proceedings article with all possible elements [**?**], an example of an enumerated proceedings article [**?**], an informally published work [**?**], a doctoral dissertation [**?**], a master's thesis: [**?**], an online document / world wide web resource [**?** **?** **?**], a video game (Case 1) [**?**] and (Case 2) [**?**] and [**?**] and (Case 3) a patent [**?**], work accepted for publication [**?**], 'YYYYb'-test for prolific author [**?**] and [**?**]. Other cites might contain 'duplicate' DOI and URLs (some SIAM articles) [**?**]. Boris / Barbara Beeton: multi-volume works as books [**?**] and [**?**]. A couple of citations with DOIs: [**?** **?**]. Online citations: [**?** **?** **?**]. Artifacts: [**?**] and [**?**].

9 ACKNOWLEDGMENTS

Identification of funding sources and other support, and thanks to individuals and groups that assisted in the research and the preparation of the work should be included in an acknowledgment section, which is placed just before the reference section in your document.

This section has a special environment:

```
\begin{acks}
...
\end{acks}
```

so that the information contained therein can be more easily collected during the article metadata extraction phase, and to ensure consistency in the spelling of the section heading.

Authors should not prepare this section as a numbered or unnumbered `\section`; please use the "`acks`" environment.

ACKNOWLEDGMENTS