SIXGILL REPORT

Carding and The Digital Gaming Industry

January 23, 2019

Carding and The Digital Gaming Industry

Executive Summary

- The Digital gaming industry grossed over $100 billion in 2017[1]. With more than 125 million players[1] and revenues of over 300 million dollars every month, the online multiplayer game "Fortnite" has rocketed to the top of the online gaming industry, surpassing established giants like "World of Warcraft" and "Minecraft".
- Fortnite's format and popularity have drawn the attention of cyber criminals, and resulted in a thriving criminal eco-system around the game.
- Criminal activity focusing on Fortnite includes the laundering of money through primary and secondary markets of Fortnite-related goods, exploiting the game's currency "V-bucks" for illegal arbitrage, and the theft of personal credentials belonging to the game's users.
- As the game's popularity increases and the financial system around it becomes more diverse, fraud involving games such as Fortnite is likely to become more prevalent.

Background

From cheating in games of chance, through laundering money in cash-rich casinos, to grey market shark-lending, the gaming industry has historically been a hotbed of criminal activity. It is no surprise then that digital gaming, an industry that grossed over $100 billion in 2017[i], has also attracted the criminal underclass.

In the past few years we've seen some relatively well-known cases of gaming-related criminality on the deep and dark web (DDW). Such cases of scamming and fraud include World of Warcraft phishing scams, the theft of virtual items on Runescape, and perhaps most famously, the Mirai botnet, created for the purpose of knocking down other Minecraft servers (though eventually it was exploited for much broader and more sinister purposes).

With the recent surge in the popularity of Fortnite, an online game boasting more than 125 million players and monthly revenues in the hundreds of millions of dollars, cyber criminals have flocked to this massively successful game and began exploiting it to commit financial fraud.

How to Use Stolen Credit Cards with Fortnite?

Sixgill's investigation of the digital gaming industry and the DDW revealed that one of the most common fraud methods used involves an old criminal modus operandi, but with a new tool. Fraudsters use stolen credit cards, or otherwise illegally-acquired funds, to purchase Fortnite-related goods, and then unload those goods on a second actor/victim, to receive clean money in return.

Figure 1: How threat actors funnel and clean money through Fortnite

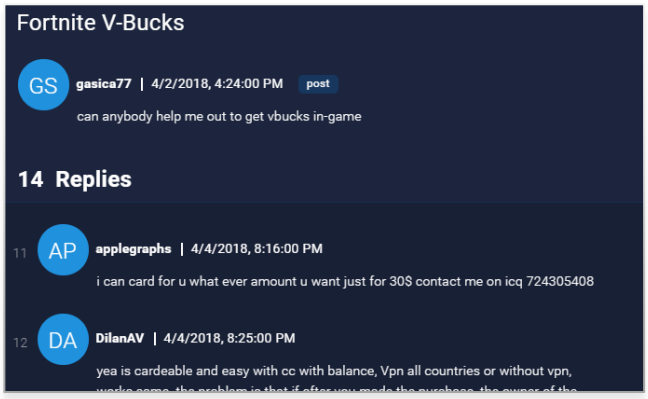


Figure 2: An underground conversation on how to whether and how to use stolen credit cards in Fortnite

In a post from April 2018, a threat actor by the name of *gasica77* asked: "can anybody help me out to get vbucks in-game".

In response, a second threat actor by the name of *DilanAV* replied with a lengthy description of how they were able to exploit the game for carding. The threat actor explains how they used multiple credit cards to buy V-bucks (the game's currency), by masking their location through the use of VPN services.

> *"yea is cardeable and easy with cc with balance, Vpn all countries or without vpn, works same. the problem is that if after you made the purchase, the owner of the card or somehow the card cancels the payment with fortnite, your account will be banned, but if this does not happen your account will not be banned, because to epic games [the developer of Fortnite] not care if you are from china, with vpn from mexico and you are buying with a cc from germany, they do not check any of that nor do they care, I personally made 3 accounts (assuming that by charging too much they would be banned) the first time I loaded 109,000 VBucks and bought the gold founder's 250usd package ... with Canada's VPN, the second account loaded with 68,000 VBucks and bought the same founder's package of 250 usd with vpn mexico, and the third charge 98,000 VBucks plus the same golden founder package from the other two accounts, not vpn, with my real ip."*

DilanAV notes that two of his accounts were banned, not for the use of VPN, but rather for the duplicate use of credit cards between the two of them.

> *"The issue is as follows, the first and the third account I made all the payments of Vbucks + the golden package with approximately 8-9 different CC's on different days and from different countries, that is, between 7 or 8 cards per account, from different countries and different days of publication, buy those 109,000 VBucks and the 98,000 VBucks plus the golden packages. And even in the address of payment (name, surname, address, zip code, etc etc) I put: sdasdsad, sadsadasd, asdasdasd, ... and even then the payment became effective.*

The issue is the following, after 12 days ... the first and third account were banned and I can assure you that it was the last card I used that canceled the payment, and only that's why they blocked both accounts, since I bought them both with the same card, however to the second account I bought the 68,000 VBucks with only 2 Cards, one card for the 250usd package and another one for the 68,000 VBucks on the same day. this account was not banned (and it has been alive for 4 months and I play the save the world every day) and I still have the 68,000 vbucks and the golden package of 250."

The threat actor concludes by emphasizing that this fraud method is based on proven experience:

"I know all this because I am selling fortnite accounts with the founder doraro package and a good load of VBucks (always more than 60,000), and from that test that I made of those 3 accounts I have never been banned an account that I created ... I currently have approximately 12 accounts at rest with the gold package and 100,000 Vbucks with more than 1 month of life, and I have sold more than 20 accounts. I hope all this information can serve something."

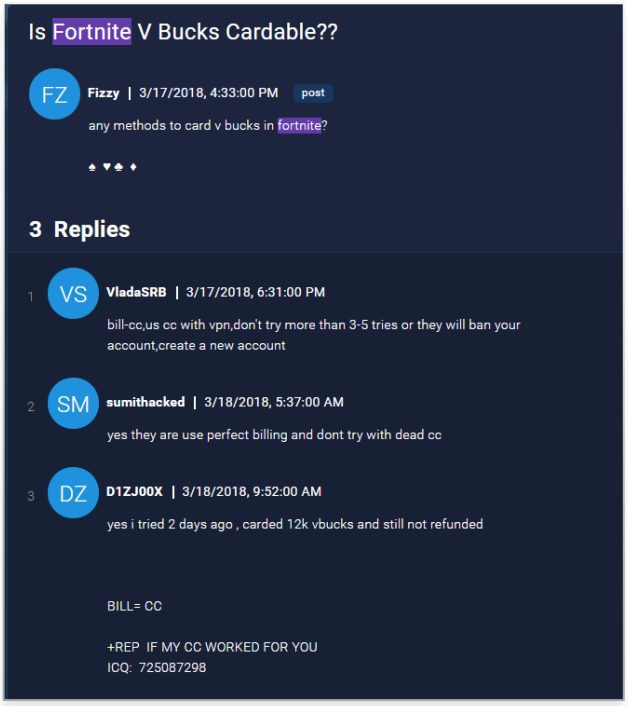


Figure 3: Is fortnite cardable? A dark web conversation

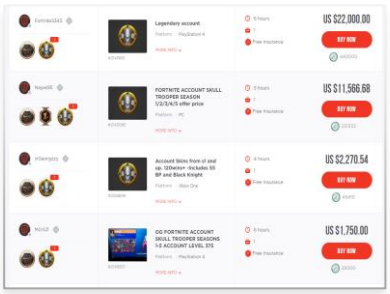
Additional posts show a similar pattern. In the following thread (left), a threat actor asked whether they can use Fortnite to commit carding fraud.

In response, several other threat actors replied that they were able to make in-game purchases using stolen credit cards, with very little difficulty.

Cashing Out

Sold Fortnite accounts and other related goods enable threat actors to complete the criminal sequence, turning ill-gotten funds (usually in the form of stolen credit cards) to clean money. Once the threat actor acquired V-bucks, or any other in-game good, they are able to cash them out by one of two main ways: Selling the goods on either clearnet secondary markets, or on DDW forums and markets.

Clearnet secondary markets are relatively well-known and public, from gamer-specific markets like G2G and G2A, to generic markets like eBay. As evident by the sales numbers, the open market for Fortnite goods is booming.



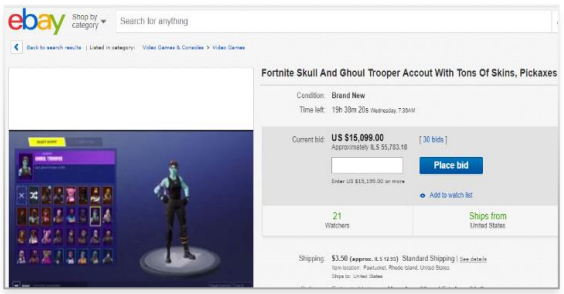


Figure 4 (left): Fortnite goods sold on the G2G market for tens of thousands of dollars each. Figure 5 (right): 30 bids on a Fortnite account, eventually sold for over $15,000 on eBay.

In the past 60 days, the top 50 Fortnite items on eBay grossed over $250,000.

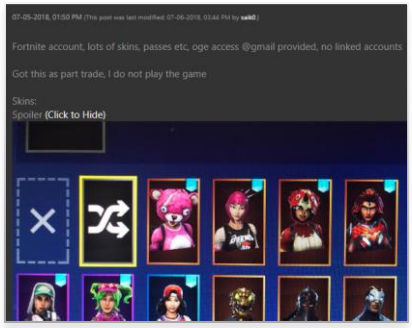
Similarly, deep and dark web forums and markets offer countless possibilities for threat actors to monetize Fornite goods. Less structured than clearnet markets, DDW trades of Fortnite goods usually take place in an ad hoc fashion, whereby threat actors post their offerings, and the deals are finalized through direct contact via email, or other means of online communication.

For example, in a post published on a well-known deep web hacking forum, a threat actor is offering to sell their Fortnite account, complete with 55,000 V-bucks and over 50 skins (in-game customization to the avatar's appearance), all for $150. As a form of payment, the threat actor accepts PayPal, Bitcoin, and WebMoney (WMZ).

The vendor notes that the package comes complete with email and password login information, access to the original email associated with the account, and even payments receipts. Additionally, the threat actor attached

screenshots of the account itself, adding further proof that the offer is authentic.

Figure 6 (left): The post in which a threat actor sells their Fortnite account for $150. Figure 7 (Right): Another offering of a Fortnite account on a different dark web forum. The vendor received a reply with an offer of



Once the threat actor is able to sell the account, they have effectively laundered the money, receiving the clean funds in one of the payment forms listed above.

Assessment

Sixgill estimates that fraud involving digital games, and specifically Fortnite, is likely to grow more common in the coming years.

Recent news[ii] suggest that the game's developer is set to update Fortnite with a new "gifting" mode, which will allow some form of direct transfer of goods inside the game. While details of this development are still unclear, it will likely not stem the tide of criminal activity surrounding the game.

Even though Fortnite's revenue growth has slowed down in the past few months, the game's popularity continues to increase, with August being the game's strongest month yet. This trend is reflected by DDW chatter about the game, which has been consistently active for the past six months (see chart below).

Consequently, we expect Fortnite-related criminal activity on the DDW to continue in the near future as well.

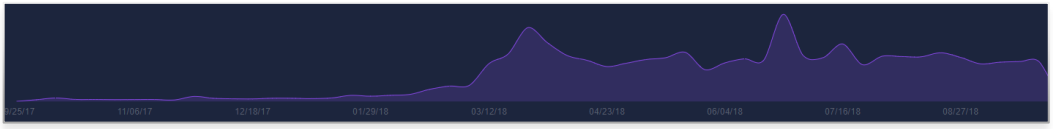


Figure 8: Deep and dark web conversation of Fortnite has increased exponentially in the past six months.

[i] https://www.superdataresearch.com/
[ii] https://www.vgr.com/gifting-system-is-finally-coming-to-fortnite/