BreachDirectory

Whitepaper

Data Breach Deconstruction – Zynga Data Breach

TABLE OF CONTENTS

PREFACE

Zynga is an American social game developer which acknowledged a data breach in September 2019 – the result set contains 206,267,210 records including duplicates and 150,363,954 records without duplicates.

In this whitepaper, instead of analyzing the data breach, we are going to attempt to deconstruct it – instead of looking at why it happened, what data was stolen and how severe the actual damage of the data breach was, we are going to be looking at the things that allowed this data breach to take place.

UNDERSTANDING THE DATA BREACH

If we take a step back, we can see that Zynga is one of the most successful social game developers – its game portfolio includes the following games that are each available on separate platforms (the list below is not exhaustive):

Zynga Game	Year of Release	Available On
Zynga Poker	2008	Facebook, Mobile Platform
Mafia Wars	2008	Facebook
Chess with Friends	2008	Facebook
Farmville	2009	Facebook
Words with Friends	2009	Facebook, Mobile Platform
Cityville	2010	Facebook
Empires & Allies	2011	Mobile Platform
CSR Racing	2012	Mobile Platform
Draw Something	2012	Mobile Platform
Hit it Rich!	2013	Facebook, Mobile Platform

By looking at the data above, we can tell that there were various ways by which Zynga could have been attacked – Zynga broadened the scope available for attackers when it made its games available on multiple platforms.

The Zynga data breach first appeared on the news in September 2019. When the data breach appeared publicly, it was attributed to a hacker from Pakistan going by an alias „Gnosticplayers". From what we can tell so far by looking at multiple sources, the data was stolen via the data breach of a popular Zynga-developed word puzzle game Words with Friends.

According to the news, the data breach affected all Android and iOS game players who installed and signed up for the „Words with Friends" game on and before the 2nd September, 2019.

Zynga admitted the data breach on 12th September, 2019. In the news release, Zynga stated that they have recently discovered that certain player account information may have been accessed by hackers and that they have immediately commenced an investigation with the help of third-party forensics companies. Zynga has also contacted law enforcement.

Perhaps the most notable Zynga's discovery was the following: the news release said that Zynga has „identified account login information for certain players of Draw Something and Words with Friends that may have been accessed." In other words, Zynga, perhaps inadvertenly, admitted that the data breach happened when the games „Draw Something" and „Words with Friends" were compromised. Some news outlets also said that the breached data includes data belonging to some other Zynga-developed games including the discontinued „OMGPOP" game which allegedly exposed clear text passwords for more than 7 million users.

MAKING THE SCOPE SMALLER

When Zynga said that they think that the data breach occured by the games being compromised, the scope of the data breach instantly became smaller – we now know the following:

- The data that was at risk include data from games that were developed between 2009 and 2012, data from games that were developed prior to 2009 might also be at risk;
- The data that was at risk include such data classes that were used when playing the games in question;
- The data breach was not a result of a successful social engineering attack;
- The source code of all three of the games might need a security audit. If a code block that is used in the „Draw Something", „Words with Friends" or „OMGPOP" games is re-used somewhere else (i.e in another game or any infrastructure that is rolled out to production), it's safe to assume that the data from that game is at risk too.

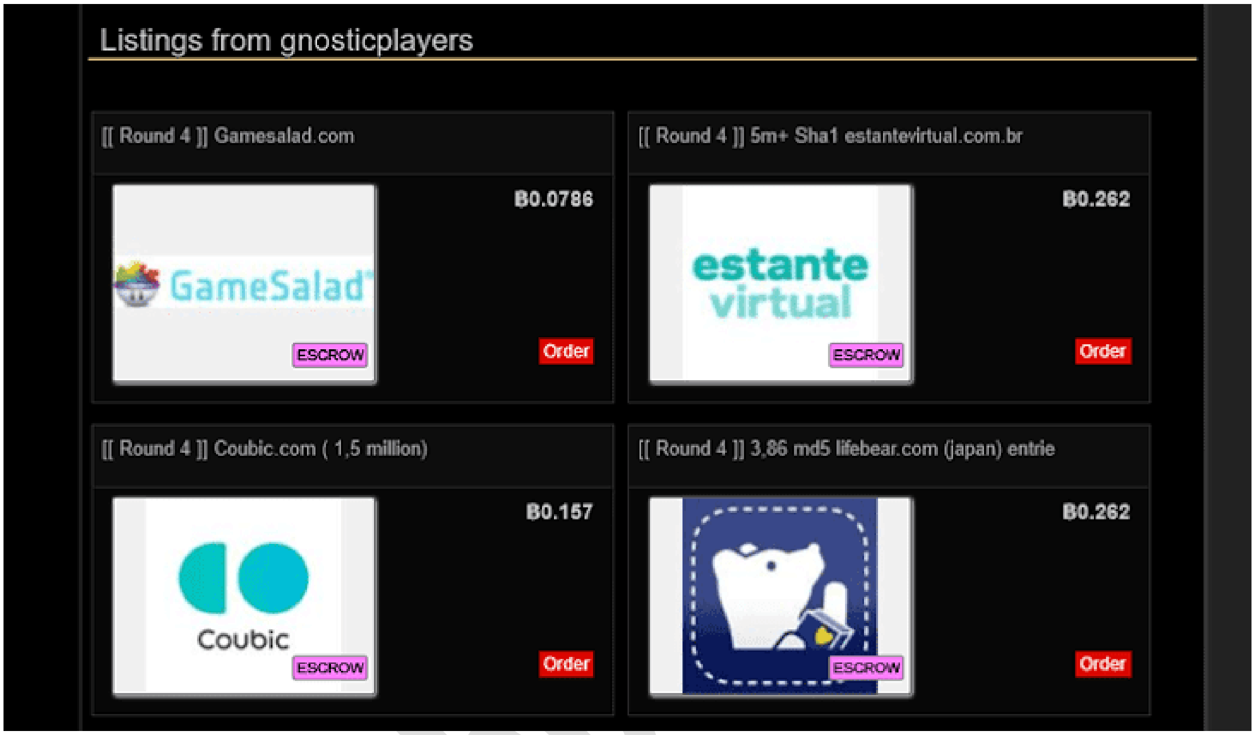
We also know what the stolen information consisted of. The stolen data included:

- Zynga account IDs;
- Login IDs;
- Usernames;
- Email addresses;
- Dates (presumably registration and last visit dates);
- Phone numbers;
- Passwords.

The stolen data also includes password reset tokens and Facebook IDs if they are connected to the account.

FORENSIC INVESTIGATION CLUES

We also know that the same hacker breached other websites (source: „Dream Market“):



Listings from gnosticplayers

[[Round 4]] Gamesalad.com — ฿0.0786

[[Round 4]] 5m+ Sha1 estantevirtual.com.br — ฿0.262

[[Round 4]] Coubic.com (1,5 million) — ฿0.157

[[Round 4]] 3,86 md5 lifebear.com (japan) entrie — ฿0.262

Figure 1 – „Dream Market“ Data Breach Marketplace

This clue might help forensic investigators determine if, for example, the same version of software was used across all of the platforms that were breached and listed for sale on „Dream Market“ (the image above) – by determining if the same version of software was used, the investigators could get clues what flaws could have been exploited.

We also see that all listings have the title „Round“ in them – that might help forensic investigators to get clues what rounds are in question – according to the news, „rounds“ refer to batches of stolen databases. Here‘s what we know about them:

- In February 2019, the same hacker who breached Zynga‘s systems made three rounds of stolen databases up for sale on the popular dark web market called „Dream Market“. The first round of databases included 620 million accounts stolen from 16 websites, the second round included 127 million accounts taken from 8 websites, the last round included 92 million accounts derived from 8 websites. News outlets also note that the hacker has not yet made available the fourth round of stolen databases which include 6 hacked websites – „Youthmanual“, „GameSalad“, „Bukalapak“, „Lifebear“, „EstanteVirtual“ and „Coubic“. Instead, the hacker is selling each database individually on Dream Market for 1.2431 Bitcoin which amounts to roughly $5,000.

- During the first round of stolen databases being published, a couple of companies have confirmed that they have indeed suffered data breaches which allows us to see that the data breaches aren‘t fake – data breaches have been confirmed by „500px“, „Artsy“, „DataCamp“, „CoffeeMeetsBagel“, „MyFitnessPal“, „MyHeritage“, „Animoto“ and „Dubsmash“.
- „500px“ seems to have been aware of a data breach since February 8, 2019, „Artsy“, „DataCamp“ and „CoffeeMeetsBagel“ have been aware of the data breach since February 14, 2019, „MyFitnessPal“ has been aware of a data breach since March 29, 2018, „MyHeritage“ has been aware of a data breach since June 4, 2018, „Animoto“ has been aware of a data breach since July 10, 2018.
- According to „The Hacker News“, the hacker removed the collection of the first round of databases while putting the second round of databases up for sale on the „Dream Market“ – by doing so he could avoid them getting leaked.
- Much like the first round, the second round of collection of 127 million stolen accounts has also been removed from sale on the dark web.
- The last (fourth) round of databases is also likely to be „legit“ (i.e the data should also be derived from the services in question) because the majority of compromised services that have been listed in previous rounds have acknowledged the data breaches.
- The entire story seems to have hit the press on March 17, 2019 – the hacker apparently interviewed with „The Hacker News“ through email shortly before the date saying that „many targeted companies have probably no idea that they have been compromised and that their customers‘ data have already been sold to multiple cyber criminal groups and individuals.“

The first round of data breaches contained 16 compromised websites:

1. „Dubsmash“ – 162 million records;
2. „MyFitnessPal“ – 151 million records;
3. „MyHeritage“ – 92 million records;
4. „ShareThis“ – 41 million records;
5. „HauteLook“ – 28 million records;
6. „Animoto“ – 25 million records;
7. „EyeEm“ – 22 million records;
8. „8fit“ – 20 million records;
9. „Whitepages“ – 18 million records;
10. „Fotolog“ – 16 million records;
11. „500px“ – 15 million records;
12. „Armor Games“ – 11 million records;
13. „BookMate“ – 8 million records;
14. „CoffeeMeetsBagel“ – 6 million records;
15. „Artsy“ – 1 million records;
16. „DataCamp“ – 700 thousand records.

In total, the first batch of data breaches consisted of around 616,700,000 records.

By looking at all of those data breaches at once, we can also see the data classes that were stolen. In total, the data classes could be categorized into 17 categories:

1. First and last names – „500px“, „DataCamp“ and „CoffeeMeetsBagel“ data breaches;
2. Usernames – „500px“ and „Dubsmash“ data breaches;
3. Email addresses – „500px“, „DataCamp“, „CoffeeMeetsBagel“, „MyFitnessPal“, „MyHeritage“ data breaches;
4. Passwords, which were hashed using one-way cryptographic algorithms (BCrypt etc.) – „500px“, „DataCamp“, „MyFitnessPal“ and „Dubsmash“ data breaches;
5. Account creaction dates – „DataCamp“ data breach;
6. Last sign in dates – „DataCamp“ data breach;
7. IP addresses – „DataCamp“ data breach;
8. Birth dates, if they were provided – „500px“ data breach;
9. Genders, if they were provided – „500px“ data breach;
10. Cities, if they were provided – „500px“ data breach, possibly the „DataCamp“ data breach;
11. States / Provinces, if they were provided – „500px“ data breach, possibly the „DataCamp“ data breach;
12. Genders, if they were provided – „500px“ data breach;
13. Location – „DataCamp“ data breach;
14. Company – „DataCamp“ data breach;
15. Biography – „DataCamp“ data breach;
16. Education – „DataCamp“ data breach;
17. Profile pictures – „DataCamp“ data breach.

Each of those data classes may perceive a different value to an attacker:

1. First and last names can be used for doxing and gaining information on the person‘s family, friends, colleagues, etc.
2. Usernames can be used to map the user‘s most frequently visited sites, sometimes birth dates, important things to the user etc. – we can make such an assumption because millions of people are affected and usernames like „Name – sitename.com“, „Username_birthdate“, pet names etc. could be common choices between millions of people.
3. Email addresses could be used to map which email domains were used, then they may be used for corporate spying, sending bulk mails, spam, fraud or other activities;
4. Passwords may not perceive as big of a value to the perpetrators because they were hashed using one-way cryptographic algorithms (BCrypt etc.) – these algorithms are extremely resilient which may be because of the fact that the affected websites had a thought that they could be breached and thus, chose strong cryptographic algorithms to secure their users‘ data in advance.
5. Account creation dates may point the attackers to different accounts that are used by the same people;
6. Last sign in dates could give the attackers a clue when do people log in to the services the most, the least etc. which may give the attackers additional clues in regards to what do people do when logged in – i.e do people log in to the service during mornings? Evenings? Nights? What actions do they perform? How often do they perform those actions? Why do they do what they

do? How much money do they spend? How often? What are the demographics that spend money the most? The least? etc.;

7. IP addresses could be used to map the locations of people that logged in to the services and to obtain other information by, for example, comparing it to information derived from different data sets;
8. Birth dates could be used to get the age demographics of people who used the services, which could further be used for blackmail or other activities;
9. Genders could be of use to an attacker when he wants to decide how to execute a, for example, identity theft. They could be combined with birth dates in order to provide the perpetrator a demographic of what genders with what age use the service the most etc.;
10. Cities could be used to create a demographic that shows from what cities people use certain services, then make assumptions on what services could be used next and attack them next time;
11. States or provinces could be used to figure out what states or provinces are used to create certain accounts, they could be used by a nefarious party to look what states or provinces are the most or the least active on certain services, etc.;
12. Genders could be used to create gender demographics on certain services;
13. Locations could be used for doxing or in order to create location demographics;
14. Companies could be used for corporate espionage or to pick targets for the next data breach;
15. Biographies could be utilized by an attacker for doxing purposes;
16. Education information could be used by an attacker to pick education-industry targets to steal data from;
17. Profile pictures could be useful for an attacker because the attacker could see how people look like and thus make predictions on their age, nationality, health issues, living environment etc. – such an information could be invaluable if the attacker is, for example, doxing targets and wants to guess the target age or living area.

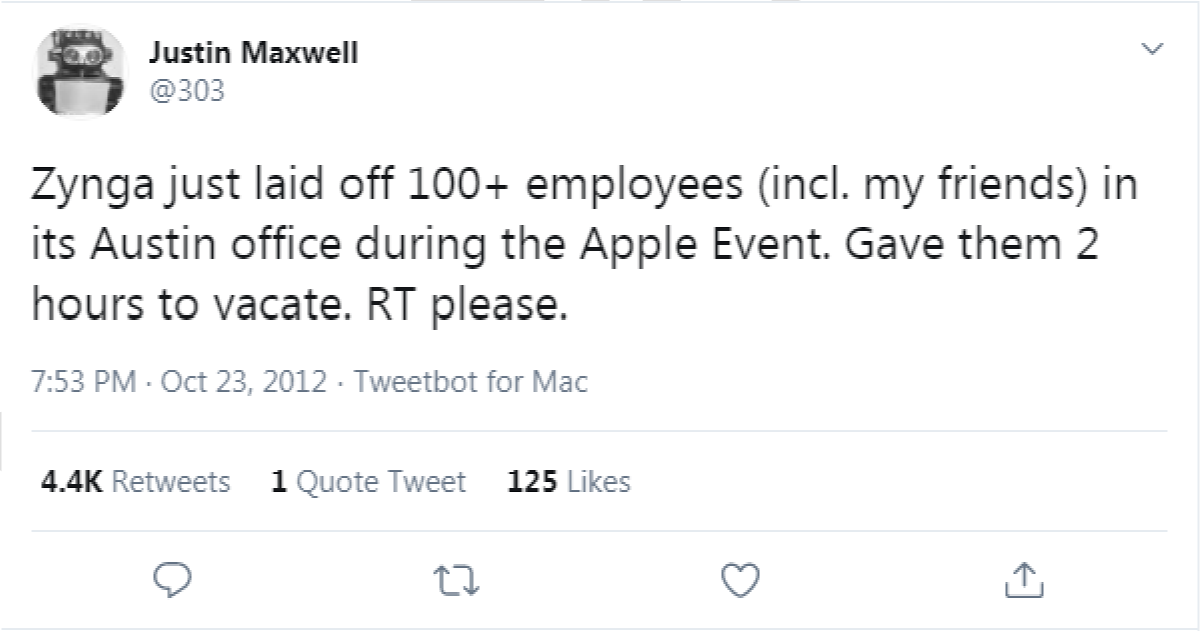
HOW DID THE DATA BREACH HAPPEN?

Now we‘ve reached the interesting question – how did the data breach happen in the first place?

In order to answer this question, we will travel back in time and see what happened to Zynga in the past and how Zynga‘s past actions could have influenced the hackers.

Zynga has gone public in 2011 with headquarters in San Francisco, California (its San Francisco headquarters had reportedly been sold for $600 million according to „VentureBeat“). However according to multiple sources, 2012 was a disastrous year for Zynga. In March of 2012 Zynga was worth 11 million (source „Business Insider“), it also pumped out new games every month very, very quickly. At the end of the year however, the landscape changed. Zynga‘s stock plumetted, in October it has shut down its Boston office and laid off more than two thirds (a hundred) of its employees in its office in Austin, Texas.

The layoff news were first leaked by a former „Apply“, „Sony“, „Mint“ and „Smule“ employee Justin Maxwell who said that Zynga‘s employees were apparently given just two hours to clean their desks having learned this from his friends who worked at the company:



Justin Maxwell
@303

Zynga just laid off 100+ employees (incl. my friends) in its Austin office during the Apple Event. Gave them 2 hours to vacate. RT please.

7:53 PM · Oct 23, 2012 · Tweetbot for Mac

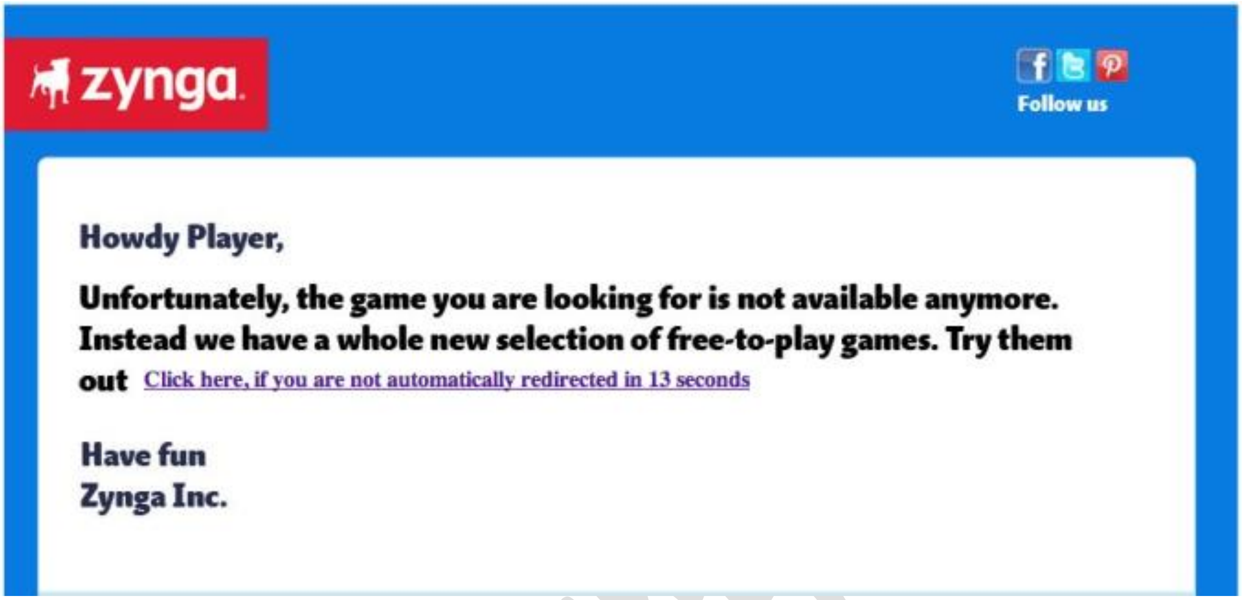
4.4K Retweets 1 Quote Tweet 125 Likes

Figure 2 - News about Zynga's layoff on Twitter

In November, Zynga has shut down, pulled from the app stores, or stopped accepting players to new games, with some turning off their functions on Monday, December 31, 2012.

The reason for this happening is apparent Zynga‘s overextension of itself – during its heyday on Facebook the company had built dozens of games, then aggressively launched mobile games. The activities of the company became a problem when the company was preparing for a big initial public offering (IPO).

Investors feared that the company would never recover. After that, Zynga announced a deep set of cost-cutting measures including reducing investments, layoffs, office closures, refusing to renew deals with contractors and shutting down certain games:



Howdy Player,

Unfortunately, the game you are looking for is not available anymore. Instead we have a whole new selection of free-to-play games. Try them out Click here, if you are not automatically redirected in 13 seconds

Have fun
Zynga Inc.

Figure 3 - Zynga shutting down certain games

The list of games that have been shut down includes:

1. „Mafia Wars Shakedown“ – pulled from app stores;
2. „Forestville“ – pulled from app stores;
3. „Mojitomo“ – pulled from app stores;
4. „Word Scramble Challenge“ – pulled from app stores;
5. „Indiana Jones Adventure World“ – closed to new players since 2012 December. Shut down at January 14, 2013;
6. „FishVille“ – shut down on December 5th, 2012;
7. „Vampire Wars“ – shut down on December 5th, 2012;
8. „Treasure Isle“ – shut down on December 5th, 2012;
9. „Montopia“ – shut down on December 21st, 2012;
10. „PetVille“ – shut down on December 30th, 2012;
11. „Mafia Wars 2“ – shut down on December 30th, 2012.

These changes might not be very impactful to some players, but to others it might seem very significant: some of the players have put time and money into these games. According to „Tech Crunch“, some of the gamers were heartbroken that their favorite games might be gone forever. Some of the comments from people who played these games included accusing Zynga of making them depressed, disappointed and angry. Zynga did react to these comments and offered people who played „Fishville“, „Adventure World“ and some other games a free bonus package of virtual items in its other games such as „CastleVille“, „ChefVille“, „YoVille“, „FarmVille 2“ or „Mafia Wars“ (source: „Tech Crunch“).

It would appear that Zynga shut down these titles because it wanted to save other games that may do well in the future and avoid further layoffs – as „Tech Crunch“ puts it, sometimes you have to put old dogs to sleep.

Knowing that Zynga has shut down certain games, hackers could have done some research on the company, chosen the most „vulnerable“ game in their opinion and started searching for weak spots in the game‘s infrastructure – those games turned out to be „Words with Friends“ and „Draw Something“.

Here‘s what we know about the games through which Zynga has been breached:

Zynga Game	Genre(s)	Year of Release	Latest Stable Release	Available On	Notes
„Words with Friends“	Puzzle	2009	Unknown, originally released in 2009	Facebook, Windows, Windows Phone, Android, iOS, Kindle Fire, Nook Tablet	Game is available on both Facebook and mobile platforms, but the game can be played on both Android and iOS without using Facebook – in 2012, Zynga, in collaboration with „Hasbro“, also released a physical board version of the game.
„Draw Something“	Drawing	2012	2.4.7 – released July 31, 2015	Windows Phone, Android 2.3 or later, iOS 5.1.1 or later	The game can only be played by two players.

Zynga did confirm there was a data breach of account information for „Draw Something“ and „Words with Friends“ players on September 12, 2019. If we dig further into the news sources, we can see that „CBSNews“ reported that the hacker accessed a database that included data from Android and iOS players who installed the game before September 2, 2019. „The Hacker News“ first reported the story.

Since the hacker accessed a database that included data from both Android and iOS players, it is probable that the data breach was accomplished through one or multiple of the following scenarios:

- A physical data compromise – the hacker could have simply infiltrated Zynga and stole the devices that held sensitive information in regards to players using Android and iOS platforms. Such an event is very unlikely to have occured though, since nor Zynga nor the press reported any physical damage and the attacker would have a hard time knowing which servers hold which information;
- Social engineering – the hacker could have acquired data by simply psychologically manipulating staff into performing certain actions or disclosing confidential information. Such a method is, however, unlikely, since Zynga themselves didn‘t mention that they were suspicious of such a method being exploted and there are no probable public clues (email, text messages, phone calls etc.) pointing to such a method being used;
- A data breach through a vulnerability in Zynga‘s website – such an event is possible, but not very likely, since the hackers accessed a database consisting of account information of players that have installed certain games („Words with Friends“) before September 2, 2019. If the Zynga‘s website would have been breached, it would be very possible that the stolen data set would include more data classes (Zynga‘s forum information etc.), besides, the hackers themselves claimed responsibility for breaching the data of more than 200 million „Words with Friends“ accounts: the entire data set contains just over 200 million entries;

A data breach through a vulnerability in Zynga‘s mobile applications – taking everything else into consideration (the hacker accessed a database that included data from Android and iOS players who had installed the game before September 2, 2019), such a scenario is one of the most probable ones that could have been exploited – we will now dive deeper into this scenario.

A POSSIBLE VULNERABILITY IN ZYNGA’S MOBILE APPLICATIONS

There are numerous ways how Zynga‘s mobile applications could have been attacked:

1. One or more of Zynga‘s games could have failed to use proper platform security controls and therefore made themselves susceptible to an Improper Platform Usage vulnerability. In order for such a vulnerability to be exploited, one of Zynga‘s games must have exposed a web service or an API call that would have been consumed by the app. In general, such a vulnerability covers misuse of a platform feature or failure to use proper platform security controls.
2. Zynga‘s games could have been breached if one or more of Zynga‘s employees that worked on the game development would have lost a mobile device that would have then been attained by an adversary or ran an app that contained malware which executed on the mobile device.
3. If the communication between Zynga‘s employees that worked on the game was not confidential, it could have been intercepted and the attacker could have gained some valueable insights that could have allowed him to steal the data.
4. Zynga could have had a security vulnerability in its authentication scheme that could have been exploited by an attacker allowing him to bypass authentication requests and once the requests would be bypassed, the attacker could have gained more insight into Zynga‘s infrastructure that could have potentially allowed the adversary to steal data.
5. The data could have been stolen if the attacker would have gained access to data that was improperly encrypted or not encrypted at all.
6. Zynga‘s games could have been susceptible to an insecure authentication vulnerability – if the attacker would have understood how the authentication scheme is vulnerable, they could have logged in to the application as a regular user.
7. Zynga‘s games could have been breached if the code that the games contained had poor quality – if the attacker could have supplied carefully crafted payloads that executed on another device, that might have led them to something else.
8. An attacker could have exploited security flaws in Zynga‘s games by utilizing code tampering. If the attacker could have built an unauthorized version of one or more games that Zynga developed and managed to attract a lot of Zynga‘s user base, the data of the users could have been stolen.
9. An attacker may have exploited the possibility of reverse engineering to reveal information about Zynga‘s infrastructure (back-end servers etc.) and perform attacks against them, gain some valueable insights needed to perform a data breach or steal data outright.
10. An attacker could have downloaded Zynga‘s games on their own environment in order to examine configuration or log files and perhaps find some code that was forgotten to be removed by developers that could have allowed the attacker to steal Zynga‘s data.
11. Social engineering could also have been a factor, but such a method isn‘t very likely to have been exploited, because if it would have occured, there‘s a pretty big possibility of Zynga confirming this themselves – Zynga did not mention that they are investigating such a thing.

Which method was exploited is hard to tell exactly, but from what we can tell so far, the most probable methods that could have been used by the attacker are as follows (the list is comprised of the most probable scenario at the top coming down to the least probable scenario at the bottom):

1. Poor Zynga‘s game code quality;
2. Zynga‘s usage of improper security controls;
3. A security vulnerability in Zynga‘s authentication scheme;
4. One or more of Zynga‘s applications containing an insecure authentication vulnerability;
5. One or more of Zynga‘s applications holding improperly encrypted or unencrypted data;
6. Reverse engineering;
7. Code tampering;
8. The exploiting of extraneous functionality.

SUMMARY

Zynga became victims of a data breach in September 2019 – the data breach most likely occurred when one or more applications developed by Zynga contained poor quality and possibly security vulnerabilities or by the attacker exploiting improper security controls that might have been present in the code of the applications developed by Zynga.