

Eksploracja Sieci Teleinformatycznych

Rekonesans pasywny armorgames.com

Autor: Arkadiusz Ostrzyżek

Prowadzący: Dr. inż. Michał Jarosz

Styczeń 27, 2025

Spis treści

1 Uzasadnienie wyboru domeny	3
2 Dane ogólne dotyczące organizacji będącej właścicielem domeny	4
2.1 Podsumowanie	13
3 Serwery DNS obsługujące domenę	14
3.1 Rekordy Name Server	14
3.2 DnsSec	14
3.3 Podsumowanie	15
4 Ogólne dane dotyczące witryny domeny	16
4.1 Analiza kodu strony	22
4.1.1 Core.js	22
4.1.2 Informacje dla crawlerów	22
4.1.3 reCaptcha	23
4.1.4 Bootstrap	23
4.2 Podsumowanie	23
5 Struktura domeny	25
5.1 Blog	29
5.2 Developers	31
5.3 Files, Gamemedia, Services, Gameshare, Quests	31
5.4 Stage	31
5.5 Presskits	32
5.6 Podsumowanie	33
6 Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi	33
6.1 Otwarte porty	33
6.1.1 Porty 80, 443	35
6.1.2 Porty 8080, 8443, 8880	37
6.1.3 Porty 2082, 2083, 2086, 2087, 2095	39
6.2 Systemy operacyjne	40
6.3 Podsumowanie	42
7 Wykorzystywane technologie informatyczne	43
7.1 Podsumowanie	44
8 Pracownicy i osoby powiązane	49
8.1 John Cooney	49
8.2 Daniel McNeely	52
8.3 Obecni i byli Pracownicy	54
8.3.1 Louis-Simon Menard	56
8.3.2 tasselfoot	63

8.4	Emaile strony	65
8.5	Podsumowanie	65
9	Bezpieczeństwo	66
9.1	Zabezpieczenia	66
9.2	Skan podatności	66
9.3	Wyciek danych	70
9.4	Podsumowanie	71
10	Stosowane urządzenia sieciowe	72
10.1	Podsumowanie	73
11	Inne rodzaje uzyskanych danych	74
11.1	Rekordy A	74
11.2	Rekordy AAAA	79
11.3	Rekordy Mail Exchange	79
11.4	Rekordy Start of Authority	80
11.5	Siedziba	81
11.6	Reverse whois	82
11.7	Podsumowanie	82
12	Wnioski ogólne	85

1 Uzasadnienie wyboru domeny

Strona armorgames.com była jedną z najpopularniejszych stron z grami flash, w czasach ich największej popularności. Ze względu na to, że jest ona dostępna w internecie od roku 2004 i obsługuje ona dużą ilość użytkowników dziennie, a więc powinna być relatywnie dobrze udokumentowana i mieć dostępne dane historyczne. Dodatkowo za stronę jest odpowiedzialna za nią firma, a więc powinna mieć rozbudowaną infrastrukturę dostępną publicznie. W ciągu tak długiego okresu czasu, jest też większa szansa na przypadkowe ujawnienie danych przez firmę.



Rysunek 1. Logo armorgames.com

2 Dane ogólne dotyczące organizacji będącej właścicielem domeny

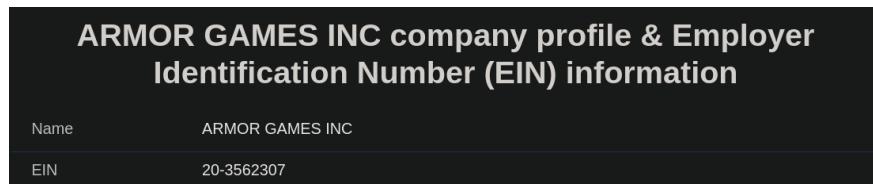
Armor Games to amerykańska firma zajmująca się tworzeniem, publikowaniem i dystrybucją gier wideo, zwłaszcza gier przeglądarkowych, komputerowych i mobilnych. Firma powstała w 2004 roku z inicjatywy Daniela McNeely'ego i szybko zdobyła popularność dzięki szerokiej ofercie darmowych gier flash, zyskując status jednego z liderów w branży gier przeglądarkowych. Już w 2012 roku była odwiedzana dziennie przez 2.5 miliona użytkowników (rys. 5) i posiadała ponad 3,6 tysiąca unikatowych gier i 10 milionów zarejestrowanych użytkowników już w 2014 roku (rys 6). Jest ona zarejestrowana w Irvine, California od roku 2005. (rys. 2). W Stanach Zjednoczonych mają także opatentowaną nazwę swojej firmy. (rys. 3) Ich EIN to 20-3562307. (rys. 4)

ARMOR GAMES INC. (2817382)		X
 Request Certificate		
<i>Initial Filing Date</i>		09/23/2005
<i>Status</i>		Active
<i>Standing - SOS</i>		Good
<i>Standing - FTB</i>		Good
<i>Standing - Agent</i>		Good
<i>Standing - VCFCF</i>		Good
<i>Formed In</i>		CALIFORNIA
<i>Entity Type</i>		Stock Corporation - CA - General
<i>Principal Address</i>		6230 BRENTWAY RD FRISCO, TX 75034
<i>Mailing Address</i>		6230 BRENTWAY RD FRISCO, TX 75034
! <i>Statement of Info Due Date</i>		09/30/2024
<i>Agent</i>		Individual Timothy J Folkers CPA 18818 TELLER AVE STE 275 IRVINE, CA 92612

Rysunek 2. Status firmy ze strony bizfileonline.sos.ca.gov

Trademark registrations						
MARK TEXT	IMAGE	REGISTER	NICE CLASSIFICATIONS	REGISTRATION DATE	EXPIRY DATE	
ARMOR GAMES		United States Patent and Trademark Office	41	2007-09-18		details
CRUSH THE CASTLE		United States Patent and Trademark Office	9, 41	2012-01-24	2018-08-31	historic details

Rysunek 3. Patenty należące do Armor Games ze strony opencorporates.com



Rysunek 4. EIN ze strony eindata.com

Gry przeglądarkowe zostały stworzone używając technologii Flash. Po zakończeniu wsparcia przez Adobe (rys. 7), firma zaczęła wykorzystywać Ruffle do emulacji. Za gry komputerowe oraz mobilne porty gier Flash odpowiedzialna jest sekcja Armor Games studio. Obecnie Armor Games koncentruje się również na rynku gier mobilnych oraz dystrybucji tytułów na platformy Steam i konsole, dostosowując swoje portfolio do zmieniających się trendów rynkowych. Aktualnym CEO jest John Cooney, od 2004 do 20021 roku był nim założyciel firmy, Daniel McNeely.

Firma specjalizuje się w gatunkach takich jak gry strategiczne, przygodowe, zręcznościowe i RPG, a jej bibliotekę zasiliły popularne tytuły, m.in. Kingdom Rush. Z raportu stworzonego z okazji 10 lat firmy (rys 8) można zobaczyć, że gra była odtworzona wtedy aż 63 miliony razy. Dzięki swojej platformie Armor Games stworzyła społeczność graczy, umożliwiając im nie tylko granie w gry online, ale też dzielenie się osiągnięciami i opiniami. Forum zgromadziło aż 68 tysięcy graczy i 2346655 komentarzy (rys. 9).



Rysunek 5. Analiza popularności ze strony semrush.com

With over **10 million users**, **3,680 games**, and **2.4 million forum posts** in over **77,000 threads**, see what else was accomplished thanks to you, wonderful users...

Rysunek 6. Podsumowanie 10 lat pracy armorgames.com

Adobe Flash Player EOL General Information

UPDATED: January 13, 2021

Since Adobe no longer supports Flash Player after December 31, 2020 and blocked Flash content from running in Flash Player beginning January 12, 2021, Adobe strongly recommends all users immediately uninstall Flash Player to help protect their systems.

Some users may continue to see reminders from Adobe to uninstall Flash Player from their system. See below for more details on how to uninstall Flash Player.

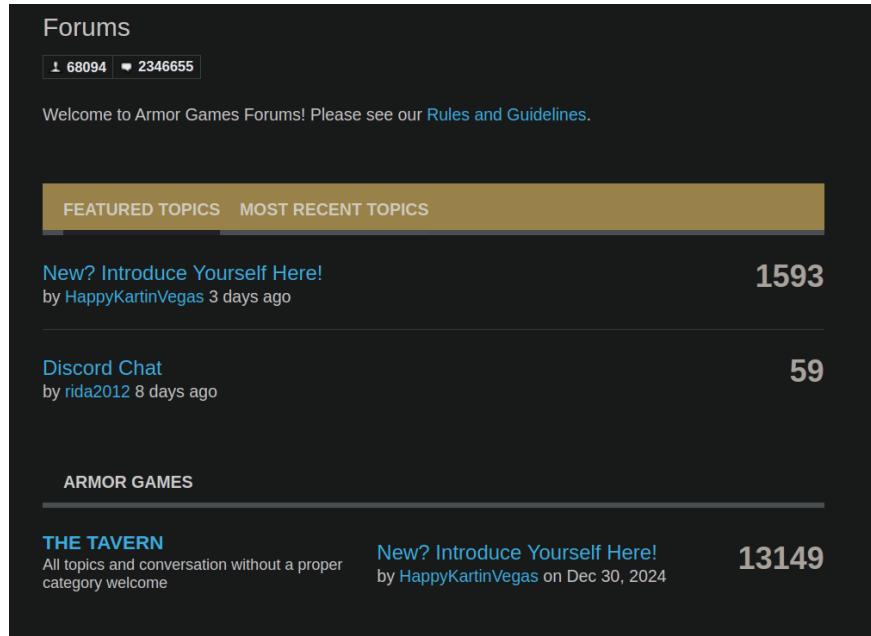
Rysunek 7. Informacja Adobe o zakończeniu wsparcia dla Flash Player

Top 10 Most Played Games

It's no surprise that **Kingdom Rush** tops the list of the most played game on Armor Games of all time, as it occupied the #1 highest rated game until its sequel.

- 1.) **62,959,136** – [Kingdom Rush](#)
- 2.) 55,582,389 – [The Last Stand – Dead Zone](#)
- 3.) 38,957,507 – [Warfare 1917](#)
- 4.) 38,027,075 – [Dawn of the Dragons](#)
- 5.) 32,796,311 – [Raze](#)
- 6.) 32,688,141 – [Warfare 1944](#)
- 7.) 32,530,051 – [Clicker Heroes](#)
- 8.) 32,357,376 – [Crush the Castle 2](#)
- 9.) 30,533,130 – [Kingdom Rush Frontiers](#)
- 10.) 26,698,285 – [Raze 2](#)

Rysunek 8. 10 najpopularniejszych gier, na pierwsze 10 lat



Rysunek 9. Witryna forum armorgames.com

Z analizy nie wynika jednoznacznie ile dokładnie zarabia firma Armor Games, ponieważ jest ona na giełdzie. Z dostępnych w internecie raportów wynika, że zarobki oscylują około 5 milionów dolarów rocznie. Najniższe zystki przedstawia firma Datanyze (rys. 10), 4.3 milionów dolarów, a najwyższe Rocketreach (rys. 11), 8 milionów dolarów. Aktualnie zdaniem linkedin.com (rys. 12) firma zatrudnia pomiędzy 11 a 50 osób. Strona linkedin.com posiada profile tylko 9 z tych osób, co jest bardziej zgodne z raportem Rocketreach (rys. 11). Tak mała ilość pracowników jest spowodowana zwolnieniami z roku 2024 (rys. 13). Były one prawdopodobnie spowodowane zmniejszoną popularnością strony oraz gier Flash. W ciągu ostatnich 6 miesięcy średnio 140 tysięcy osób wchodziło dziennie na stronę, co stanowi spadek o 93% względem 2016 roku. (rys. 14)

Domena została zarejestrowana używając Cloudflare (rys. 15). Jedynym oficjalnym sposobem kontaktu do właściciela strony jest email.

Company Name: Armor Games

Main Industry: Research & Development, Business Services

Website: www.armorgames.com

Contact Information:

- Headquarters:** 16808 Armstrong Ave Ste 205, Irvine, California, 92606, United States
- Phone:** (714) 253-7979

Armor Games Profile and History:

About Armor Games Studios: Armor Games Studios is a developers-first publisher with a focus on providing guidance and support. They release games for all platforms. This is an unedited press release made available courtesy of Tips 4 Gamers and its partnership with noteworthy game PR-related resource Games Press. This press release is from Armor Games.

Revenue: \$4.3 M **Employees:** 17 **Founded:** 2005

Rysunek 10. Raport dla firmy Armor Games ze strony Datanyze

ArmorGames Information

[View Top Employees from ArmorGames](#)

[Facebook](#) [Twitter](#) [LinkedIn](#) [CloudBees](#)

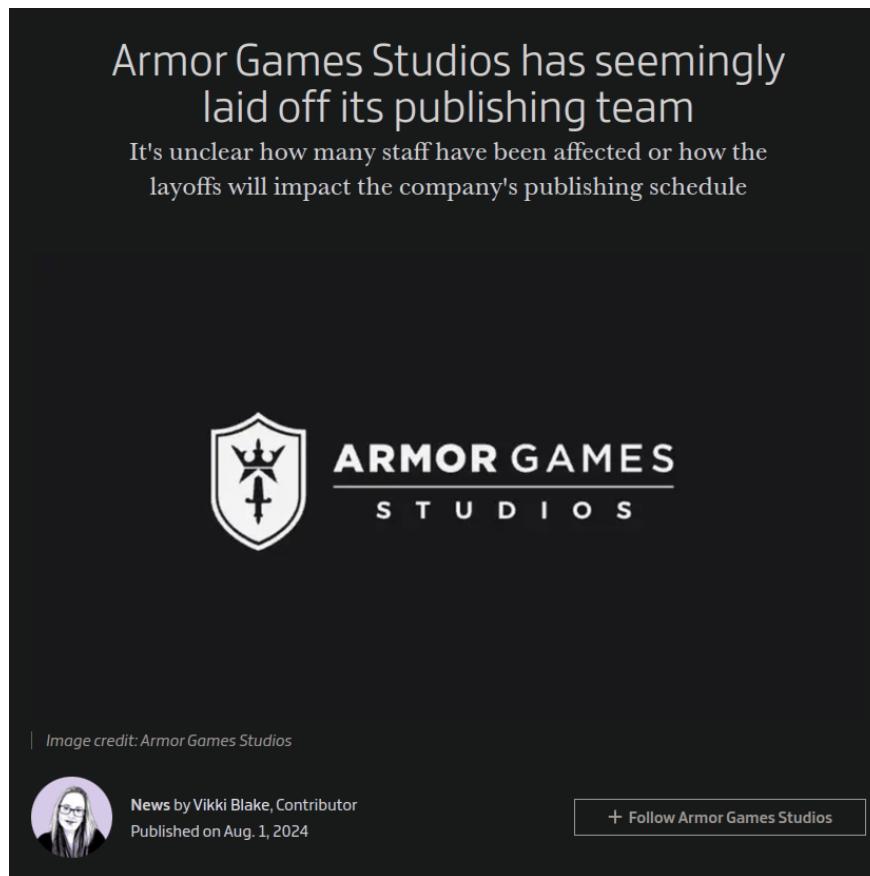
Armor Games is the leader in free flash games portals. It started the sponsorship trend and now counts many full time game developers in its team. The website is largely community oriented and is updated almost every day with new quality games.

	Website	http://www.armorgames.com
	Revenue	\$8 million
	Employees	13 (12 on RocketReach)
	Founded	2004
	Address	16808 Armstrong Ave Ste 205, Irvine, California 92606, US
	Phone	(714) 253-7979
	Industry	Business Services General, Digital Entertainment, Business Services, Media and Entertainment, Gaming, Social Media, Internet Services
	Web Rank	6853
	Web Visits	10 Million
	Keywords	Armor Games, Armorgames, Storm The House, Armour Games, Kingdom Rush, L Hoodie
	Competitors	Bored Panda , Kongregate , Miniclip , Newgrounds.com , Inc. , Shockwave KK
	SIC	SIC Code 729 Companies, SIC Code 72 Companies
	NAICS	NAICS Code 54 Companies, NAICS Code 54199 Companies, NAICS Code 5419 Companies, NAICS Code 541 Companies

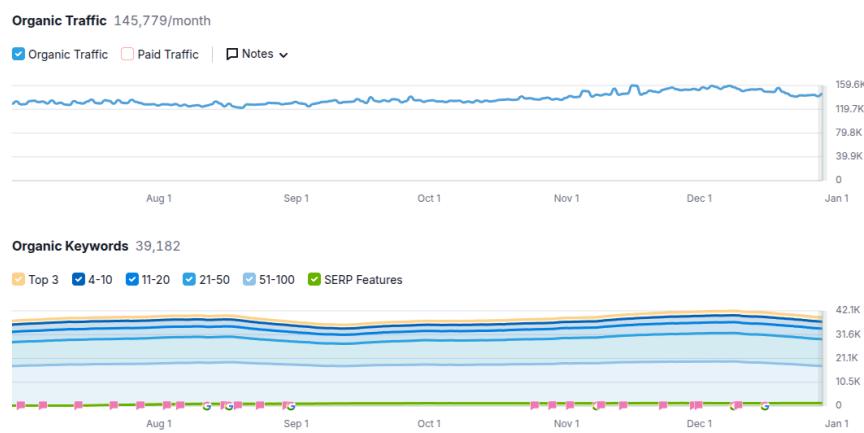
Rysunek 11. Raport dla firmy Armor Games ze strony rocketreach

The screenshot shows the LinkedIn profile of Armor Games Studios. At the top, there's a banner image of a character standing on a rocky cliff at sunset. Below the banner is the company logo, which is a shield with a crown and a sword. The company name, "Armor Games Studios", is displayed in bold black text. A brief description follows: "We are a loving group of talented and enthusiastic folks publishing wonderful games on PC, console, mobile, and beyond". It also mentions "Computer Games · 2K followers · 11-50 employees". Below this, there are three buttons: "+ Follow", "Message", and "...". A navigation bar below the bio includes links for "Home", "About", "Posts", "Jobs", and "People". The "Home" link is underlined, indicating it's the active page. The "Overview" section is expanded, showing a summary of the company's history and growth. It states: "Armor Games began as one of the most prominent Flash game portals ever, and has since become one of the leading indie game publishers. We remain wildly independent, excited about games and developers, and driven to be the best version of what we think the games industry shoul ... see more". There's a "Show all details →" link. The "Insights on Armor Games Studios" section is marked as "PREMIUM". It features a chart titled "Total employees" showing a decline from approximately 18 in Dec 2022 to about 10 in Dec 2024. To the right, it says "-25% Total headcount growth 6 months" and "9 years Median tenure". Below this, there's a call-to-action: "Unlock more organization insights Access employee, hiring, and job opening insights with Premium Try Premium for free".

Rysunek 12. Opis firmy ze strony linkedin.com



Rysunek 13. Potwierdzenie zwolnień z gamebiz.info



Rysunek 14. Analiza popularności z ostatnich 6 miesięcy ze strony semrush.com

armorgames.com

Updated 34 days ago 

Domain Information	
Domain:	armorgames.com
Registrar:	CloudFlare, Inc.
Registered On:	2005-09-29
Expires On:	2031-09-29
Updated On:	2022-08-22
Status:	clientTransferProhibited
Name Servers:	dale.ns.cloudflare.com lila.ns.cloudflare.com

Registrant Contact	
State:	CA
Country:	US
Email:	https://domaincontact.cloudflareregistrar.com/armorgames.com

Administrative Contact	
Email:	https://domaincontact.cloudflareregistrar.com/armorgames.com

Technical Contact	
Email:	https://domaincontact.cloudflareregistrar.com/armorgames.com

Billing Contact	
Email:	https://domaincontact.cloudflareregistrar.com/armorgames.com

Rysunek 15. Dane użyte do rejestracji domeny, pobrane z whois.com

2.1 Podsumowanie

Armor Games to amerykańska firma zajmująca się tworzeniem, publikowaniem i dystrybucją gier, która zdobyła popularność dzięki wysokiej jakości grom przeglądarkowym oraz wsparciu niezależnych twórców. Wraz z rozwojem rynku firma przeniosła się na platformy mobilne, Steam i konsole, dostosowując swoją ofertę do nowych technologii. Obecnie, mimo zmniejszenia liczby pracowników w 2024 roku, nadal działa jako wydawca znanych tytułów, takich jak Kingdom Rush i GemCraft. Zyski firmy oscylują między 4,3 a 8 milionów dolarów rocznie, a jej model biznesowy opiera się na reklamach, sprzedaży gier i mikrotransakcjach.

3 Serwery DNS obsługujące domenę

3.1 Rekordy Name Server

Domena armorgames.com korzysta z serwerów DNS zarządzanych przez firmę Cloudflare: dale.ns.cloudflare.com (IP: 108.162.193.95) oraz lila.ns.cloudflare.com (IP: 172.64.32.186) (rys. 17, 16). Oba serwery znajdują się w bliskim sąsiedztwie i zapewnia redundancję. W razie potrzeby kontakt w sprawie konfiguracji domeny możliwy jest pod adresem domaincontact.cloudflare registrar.com/armorgames.com.

```
Billing Email: https://domaincontact.cloudflare registrar.com/armorgames.com
Name Server: dale.ns.cloudflare.com
Name Server: lila.ns.cloudflare.com
DNSSEC: unsigned
```

Rysunek 16. Fragment whois ze strony whois.com

Name Servers	
dale.ns.cloudflare.com	108.162.193.95
lila.ns.cloudflare.com	172.64.32.186

Rysunek 17. Fragment whois ze strony who.is

3.2 DnsSec

Dane dotyczące rekordów DS (Delegation Signer), DNSKEY oraz RRSIG (Resource Record Signature) wskazują, że armorgames.com korzysta z pełnej weryfikacji bezpieczeństwa DNS (rys. 18). Rekordy DS i DNSKEY są kluczowe dla zapewnienia autentyczności i integralności danych przekazywanych przez system DNS, a podpisy RRSIG zapewniają, że rekordy DNS nie zostały zmodyfikowane przez osoby trzecie. Użytkownicy odwiedzający stronę są chronieni przed atakami typu DNS spoofing oraz man-in-the-middle, gdzie atakujący mogliby próbować przejąć kontrolę nad zapytaniami DNS lub przekierować użytkowników na złośliwe strony.

	<ul style="list-style-type: none"> ✓ Found 2 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none"> ✓ Found 1 DS records for com in the . zone ✓ DS=19718/SHA-256 has algorithm ECDSAP256SHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=61050 and DNSKEY=61050 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=19718/SHA-256 verifies DNSKEY=19718/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19718 and DNSKEY=19718/SEP verifies the DNSKEY RRset ⚠ Zone com (192.52.178.30) returns NXDOMAIN for armorgames.com

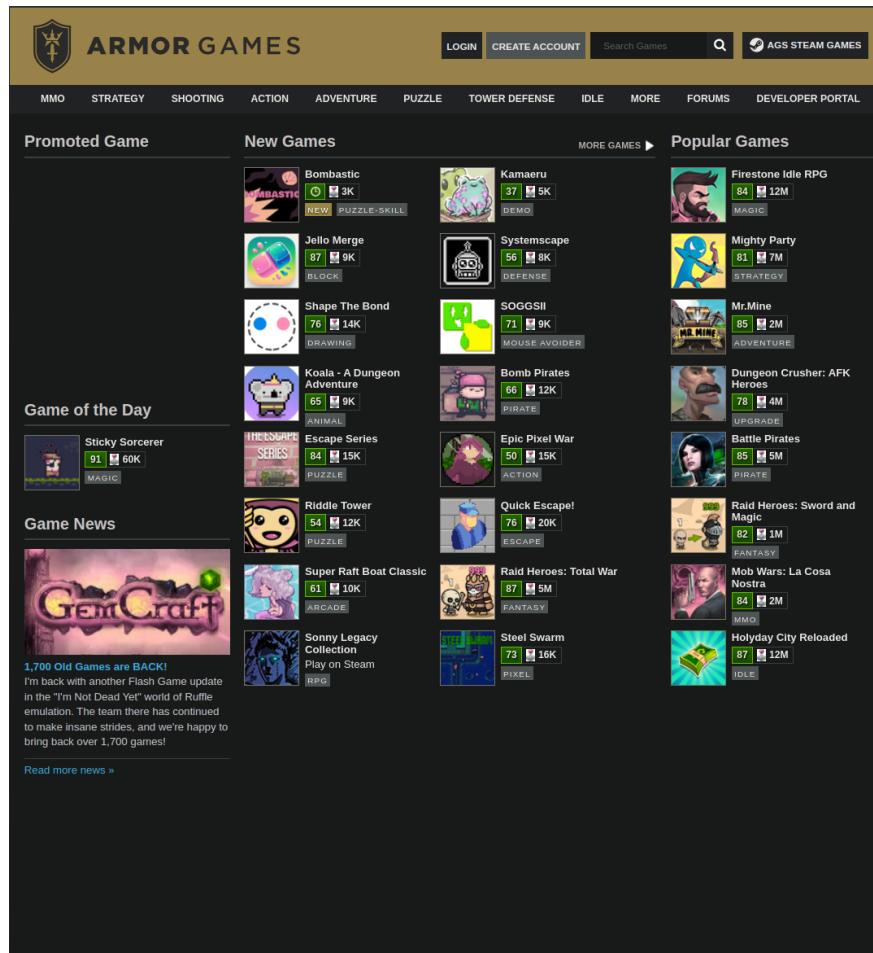
Rysunek 18. Wynik bezpieczeństwa DNS ze strony dnssec-analyzer.verisignlabs.com

3.3 Podsumowanie

Domena armorgames.com wykorzystuje serwery DNS zarządzane przez Cloudflare, co zapewnia rozproszone rozwiązywanie zapytań DNS oraz ochronę przed atakami DDoS. Konfiguracja DNSSEC zabezpiecza domenę przed atakami typu DNS spoofing i man-in-the-middle poprzez weryfikację integralności danych DNS za pomocą rekordów DS, DNSKEY oraz podpisów RRSIG.

4 Ogólne dane dotyczące witryny domeny

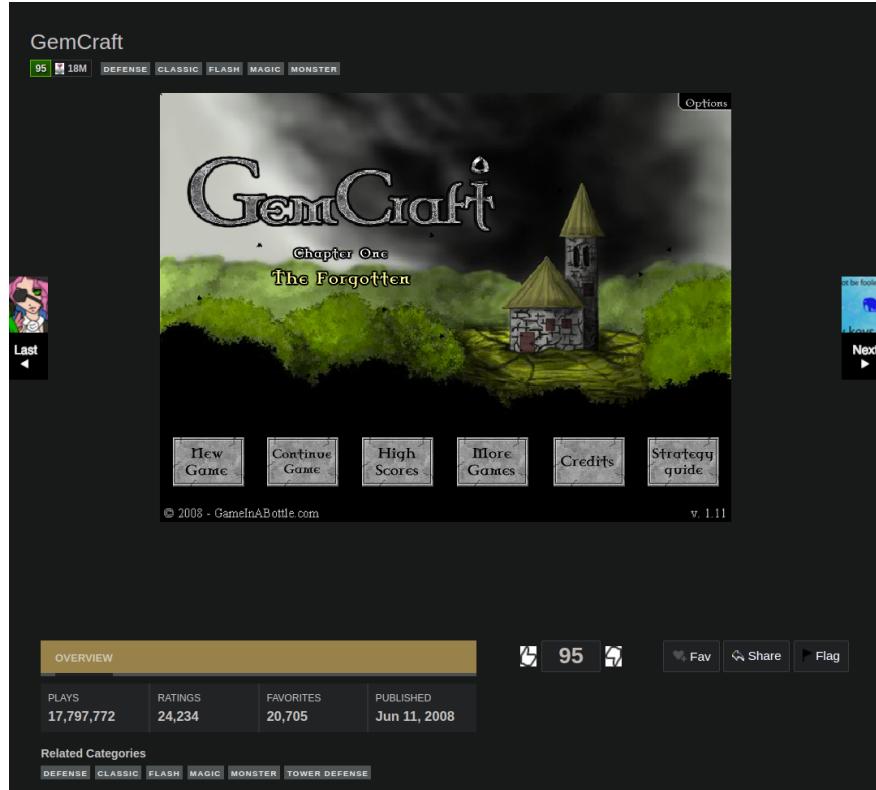
Witryna oferuje szeroką gamę gier flash, z których każda została odpowiednio opisana, posiadając przypisaną nazwę, ikonę oraz ranking, który jest ustalany przez użytkowników strony. Każda z tych gier jest również przypisana do jednej z wielu kategorii, które pomagają w organizacji i porządkowaniu dostępnych tytułów. Użytkownicy mogą łatwo przeglądać gry, wybierając interesującą ich kategorię z panelu znajdującego się na górze strony. Po dokonaniu wyboru, wyświetla się gry przypisane do danej kategorii, co ułatwia nawigację i umożliwia szybkie znalezienie odpowiednich tytułów. (rys. 19)



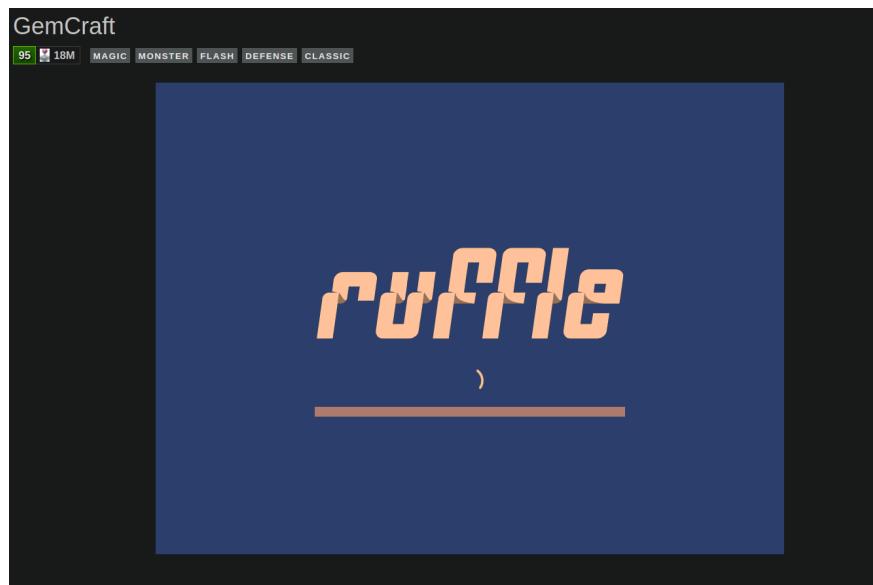
Rysunek 19. Stan witryny na dzień 27/11/24

Przykładowa gra GemCraft, którą można znaleźć na tej stronie, jest tylko jednym z wielu tytułów oferowanych użytkownikom. (rys. 20) Dla większości osób, głównym sposobem interakcji z tą stroną jest granie w gry flash, dookoła których skupiona jest strona. Wszystkie gry dostępne na stronie są emulowane przy pomocy narzędzia o nazwie Ruffle, co można zauważać podczas uruchamiania gier. (rys. 21) Zastosowanie tego emulatora jest absolutnie niezbędne, aby strona mogła dalej funkcjonować, ponieważ po 1 stycznia 2021 roku firma Adobe zaprzestała wspierania technologii Flash Player, co uniemożliwiło dalsze korzystanie z tego oprogramowania w tradycyjny sposób. (rys. 7) Dodatkowo, gry na tej stronie mają

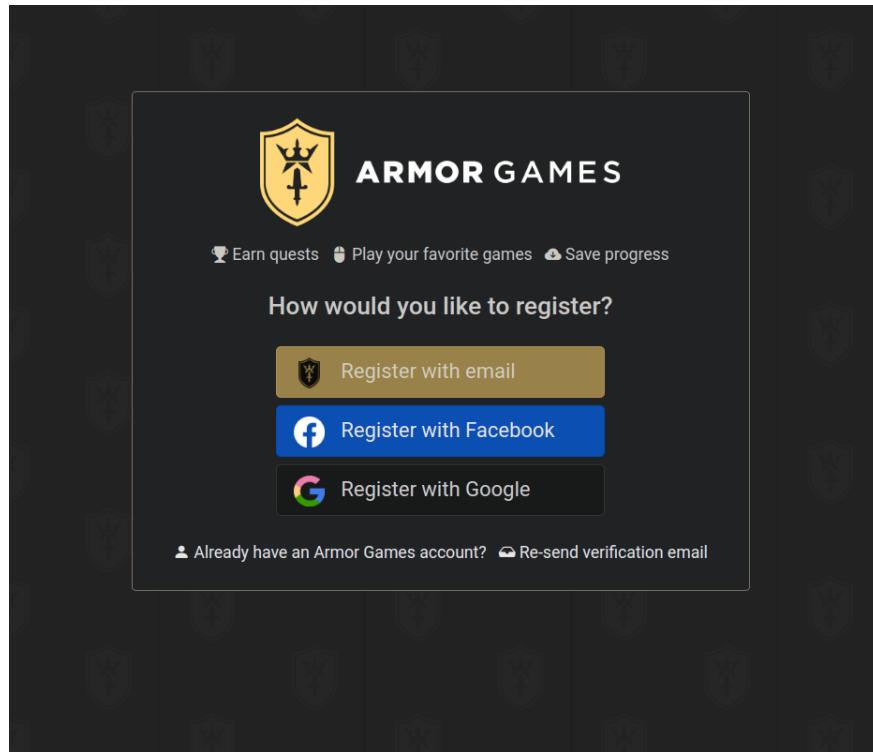
możliwość zapisywania postępów użytkowników, pod warunkiem, że są oni zalogowani na swoje konto. (rys. 22) Użytkownicy, którzy się logują, mają także możliwość zdobywania i zaliczania specjalnych osiągnięć, znanych jako „Quests”, co daje im szansę na pochwalenie się swoimi sukcesami przed innymi graczami na platformie. (rys. 23)



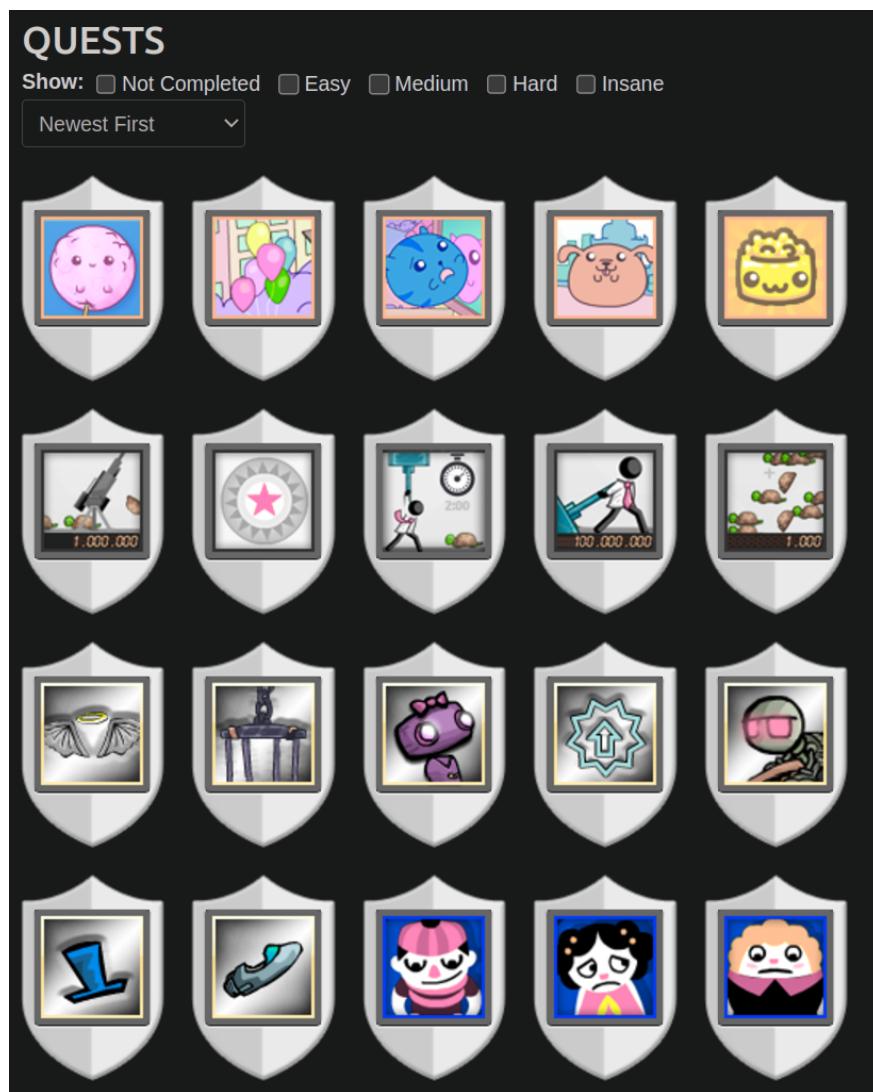
Rysunek 20. Emulkacja gry GemCraft na stronie armorgames.com



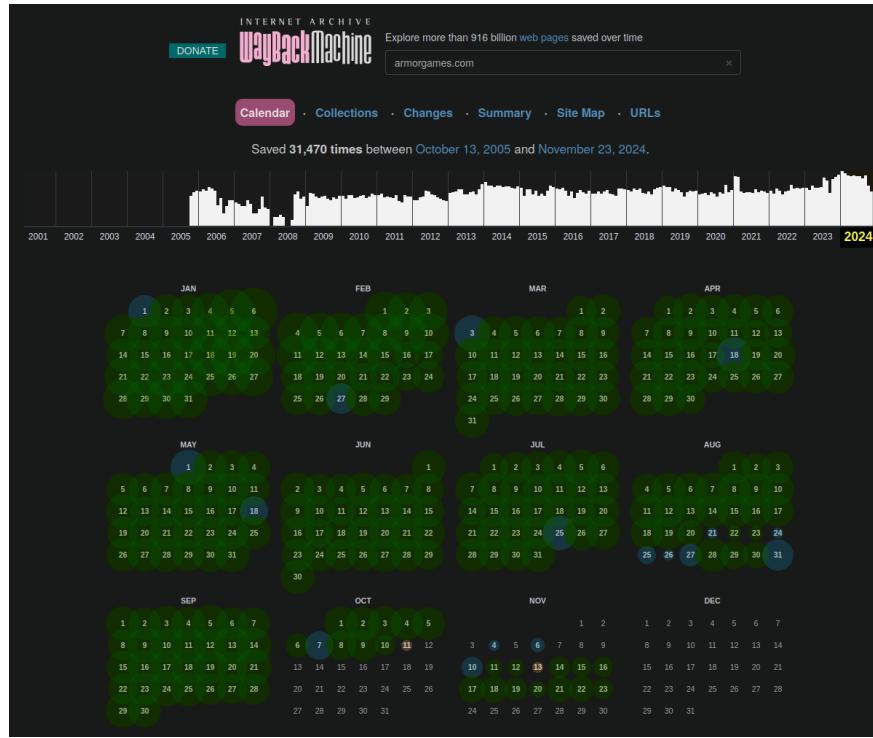
Rysunek 21. Przykład ładowania gry używając Ruffle



Rysunek 22. Użytkownicy są w stanie tworzyć własne konta na stronie, lub używać już istniejących kont Google i Facebook do logowania

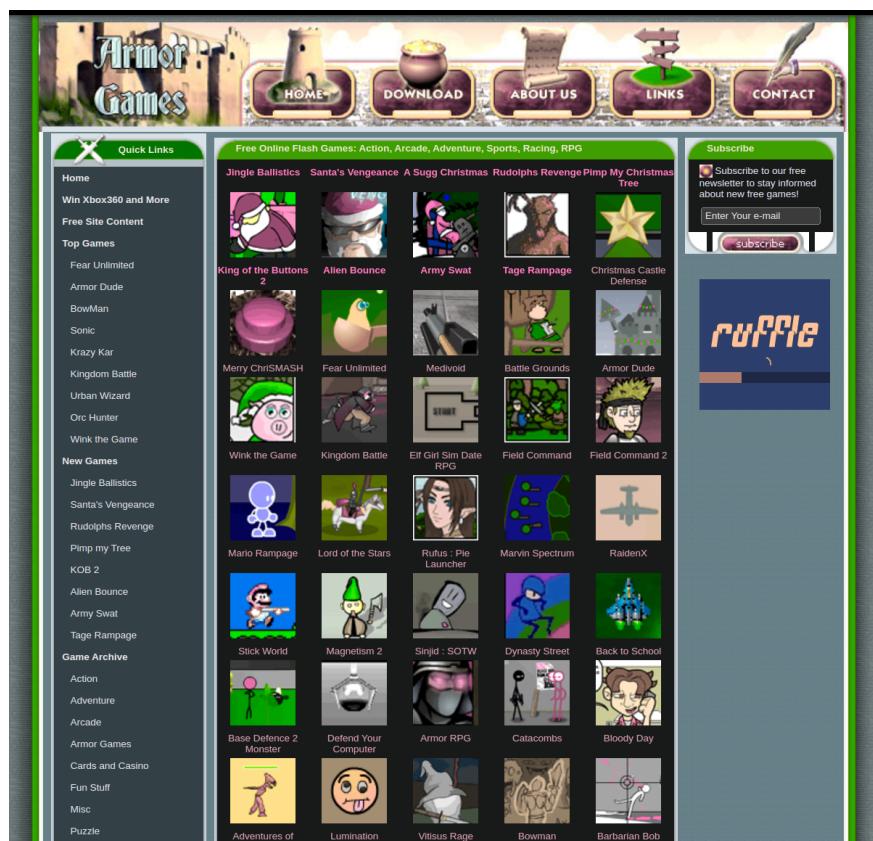


Rysunek 23. Wyzwania na armorgames.com



Rysunek 24. Dane o stanie witryny domeny uzyskane z Wayback Machine

Z danych dostępnych na stronie Wayback Machine wynika, że domena została po raz pierwszy zarejestrowana i używana już w 2005 roku. Od tego momentu, strona była regularnie monitorowana, co pozwala na śledzenie jej historii i stan aktualny niemal z dnia na dzień. Dzięki tej funkcji, można prześledzić, jak strona wyglądała w różnych momentach jej istnienia. Choć sama struktura witryny pozostała praktycznie niezmieniona pod względem układu, to główne zmiany dotyczą głównie gier dostępnych na stronie, które były dodawane lub modyfikowane w trakcie lat. (rys. 25)



Rysunek 25. Przykładowy stan strony z dnia 18/12/05

4.1 Analiza kodu strony

Analizując kod witryny armorgames.com, można zauważyc kilka istotnych elementów, które wskazują na używane technologie oraz podejście do optymalizacji, zabezpieczeń i zarządzania zawartością strony.

4.1.1 Core.js

Strona korzysta z pliku JavaScript core.js (kod 1), który został zminimalizowany (kod 2) , czyli skompresowany w celu zmniejszenia rozmiaru pliku. Jest to technika powszechnie stosowana w celu zwiększenia wydajności strony, ponieważ zmniejsza czas ładowania. Fragment skryptu pokazuje, że strona używa wersji jQuery 1.8.2:

```
1 <script src="/min/core.js?913c8840"></script>
```

Kod 1: Użycie biblioteki core.js w kodzie strony

```
1 /*! jQuery v1.8.2 jquery.com | jquery.org/license */
2 !function(a,b){function J(a,c,d){if(d==b&&1==a.nodeType){var
3   e="data-"+c.replace(I,"-$1").toLowerCase();
4   if("string"==typeof(d=a.getAttribute(e)))
5     {try{d="true"==d||"false"!=d&&("null"==d?null:+d+"")=="d"?+d:H.
6      test(d)?p.parseJSON(d):d}catch(f){}p.data(a,c,d)}else d=b}
7   return d}function K(a){for(var b in
8     a)if(("data"!==b||!p.isEmptyObject(a[b]))&&"toJSON"!==b)return;return
9   1}function ba(){return!1}function bb(){return!0}function bh(a)
10  <SNIP>
```

Kod 2: Początek zminiaturyzowanej biblioteki core.js

4.1.2 Informacje dla crawlerów

Kod strony zawiera także informacje dla crawlerów. (kod 3) Noodp informuje wyszukiwarki, aby nie używały danych z Open Directory Project (ODP) do generowania opisu strony w wynikach wyszukiwania. Używając noodp, wyszukiwarka powinna korzystać z opisu zamieszczonego na samej stronie, a nie z tego, który pochodzi z ODP. Noydir informuje wyszukiwarki, aby nie korzystały z danych Yahoo! Directory do generowania opisu strony. Zabieg ten jest prawdopodobnie w celu pokazywania lepszych opisów strony w wyszukiwarkach, aby bardziej zachęcić użytkowników do wejścia na stronę.

```
1 <meta name="robots" content="noodp,noydir">
```

Kod 3: Fragment strony przeznaczony dla crawlerów

4.1.3 reCaptcha

Strona korzysta z reCAPTCHA (kod 4), narzędzia ochrony przed automatycznymi atakami, botami i scrapingiem, stworzonego przez Google. reCAPTCHA działa poprzez analizę zachowania użytkownika oraz rozwiązywanie zadań, takich jak rozpoznawanie obrazów lub zaznaczanie pól wyboru, aby zweryfikować, że użytkownik jest człowiekiem. Rozwiążanie jest stosowane, aby powstrzymać tworzenie kopii strony.

```
1 <body id="page-home" >
2   <script defer data-domain="armorgames.com"
3     src="https://p.armorgames.net/js/script.js"></script>
4   <script src="https://www.google.com/recaptcha/api.js"></script>
5   <div id="content-canvas" class="container">
       <div id="ag3-header" class="ag-nav">
```

Kod 4: Fragment strony implementujący rozwiązanie reCAPTCHA

4.1.4 Bootstrap

Strona wykorzystuje także Bootstrap v2.1.1 (kod 5), framework stworzony przez firmę Twitter, który służy do budowania responsywnych i estetycznych interfejsów użytkownika. Bootstrap oferuje zestaw gotowych komponentów HTML, CSS i JavaScript, takich jak siatki (grid), przyciski, formularze oraz nawigacja, które ułatwiają szybkie projektowanie i wdrażanie spójnych elementów wizualnych.

```
1 @charset "UTF-8";/*
2 * Bootstrap v2.1.1
3 *
4 * Copyright 2012 Twitter, Inc
5 * Licensed under the Apache License v2.0
6 * http://www.apache.org/licenses/LICENSE-2.0
7 *
8 * Designed and built with all the love in the world @twitter by @mdo
9 * and @fat.
10 * /article,aside,details,figcaption,figure,footer,header,hgroup,nav,
11 * section{display:block}audio,canvas,
```

Kod 5: Fragment strony implementujący rozwiązanie reCAPTCHA

4.2 Podsumowanie

Witryna domeny Armor Games oferuje gry flash emulowane za pomocą Ruffle, co umożliwia ich działanie mimo zakończenia wsparcia dla Adobe Flash. Użytkownicy mogą zakładać konta, zapisywać postępy w grach i przeglądać zawartość według kategorii, przy czym układ

witryny pozostał niemal niezmieniony od 2005 roku. Wykorzystywany jest core.js z biblioteką jQuery 1.8.2, minimalizując kod dla poprawy wydajności. Dodatkowo wdrożono mechanizmy ochrony, takie jak meta tagi robots, reCAPTCHA oraz Bootstrap v2.1.1, co wspiera funkcjonalność i bezpieczeństwo witryny.

5 Struktura domeny

Strona zawiera plik robots.txt (kod 6), w którym można znaleźć odniesienie do mapy strony. Znajdują się w nim nazwy wszystkich gier. (rys. 26) Można się z niej dowiedzieć, że aktualnie na stronie jest potencjalnie dostępnych 19536 gier. Oznaczałoby to wzrost o 16 tysięcy względem roku 2014, co wskazywałoby na znaczne przyśpieszone tempo dodawania gier na stronę, względem pierwszych 10 lat istnienia firmy. Stopniowe dodawanie gier potwierdza wcześniej zaobserwowane na archive.org regularne modyfikowanie strony.

Używając narzędzia the Harvester jest się w stanie znaleźć 4 rekordy ASNS, 89 adresów IP oraz 149 różnych subdomen (kod 7). Strona merklemap.com potwierdza 23 z nich, (rys. 27), a c99.nl dalej potwierdza 20 z nich. (rys. 28). Znacznie pomniejszoną ilość subdomen, ale z wizualizacją, można uzyskać ze strony dnsdumpser.com. rys. 29)

Po nazwach subdomen można wywnioskować, że większość z nich to subdomeny przeznaczone do testów oraz z materiałami dla deweloperów. Nie jest to dziwne, ponieważ jest to strona, która na celu ma zaprezentowanie jak najprostrzegó interfejsu z grami dla osób młodszych. Ułatwienie dostępu do gier i zmniejszenie tarcia pomiędzy interfejsem a użytkownikiem, zwiększa także szansę na powrót użytkowników w krótkich przerwach oraz łatwiejsze przyciągnięcie uwagi przez nowe gry.

```
1 User-agent: *
2 Crawl-delay: 1
3 Allow: /
4 Allow: /service/disqus-widget
5 Disallow: /email/
6 Disallow: /favorites/
7 Disallow: /files/
8 Disallow: /friends/
9 Disallow: /login
10 Disallow: /quests-board
11 Disallow: /ranking
12 Disallow: /register
13 Disallow: /service/
14 Disallow: /user/
15 Sitemap: https://armorgames.com/sitemap
```

Kod 6: robots.txt

```

▼<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
  ▼<url>
    <loc>https://armorgames.com</loc>
    <changefreq>daily</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/</loc>
    <changefreq>daily</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/1700-old-games-are-back</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/warfare-legacy-collection</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/hundreds-of-old-games-are-back</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/the-last-stand-aftermath-is-coming-to-console</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/solas-128-now-available</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/solas-128-coming-soon</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/the-future-of-flash-on-armor-games</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/the-last-stand-kickstarter</loc>
    <changefreq>weekly</changefreq>
  </url>
  ▼<url>
    <loc>https://armorgames.com/news/soda-dungeon-2-available-now</loc>
    <changefreq>weekly</changefreq>
  </url>

```

Rysunek 26. Mapa strony z armorgames.com

```

1 [*] ASNs found: 4
2 -----
3 AS13335
4 AS14618
5 AS16509
6 AS27647
7
8 [*] IPs found: 89
9 -----
10 104.16.51.111
11 104.16.53.111
12 104.20.128.21
13 104.20.129.21
14 104.20.4.17
15 104.20.5.17
16 104.20.53.56
17 <SNIP>
18 99.84.74.127
19 99.84.74.15
20 99.84.74.38
21 99.84.74.43
22 99.84.79.113
23 99.84.79.129

```

```
24 | 99.84.79.16
25 | 99.84.79.27
26 |
27 | [*] Hosts found: 149
28 | -----
29 | *.armorgames.com
30 | *.cache.armorgames.com
31 | *.game-files.armorgames.com
32 | *.stage.armorgames.com
33 | 18730.cache.armorgames.com
34 | 18733.cache.armorgames.com
35 | 18739.cache.armorgames.com
36 | <SNIP>
37 | 19184.cache.armorgames.com
38 | 19191.cache.armorgames.com
39 | 19229.cache.armorgames.com
40 | agi.armorgames.com
41 | armatars.armorgames.com
42 | blog.armorgames.com
43 | <SNIP>
44 | services-stage.armorgames.com
45 | services.armorgames.com
46 | services.armorgames.com:104.20.129.21
47 | stage.armorgames.com
48 | stage.armorgames.com:104.20.128.21
49 | store.armorgames.com
50 | support.armorgames.com
51 | test.armorgames.com
52 | test2.armorgames.com
53 | test3.armorgames.com
54 | test3.test2.armorgames.com
55 | vpn.armorgames.com
56 | webdisk.test2.armorgames.com
57 | webdisk.test3.armorgames.com
58 | webmail.test2.armorgames.com
59 | webmail.test3.armorgames.com
```

Kod 7: Wynik programu the Harvester

Merklemap

Subdomain Search

Tip: You can use wildcards (*) in your search.

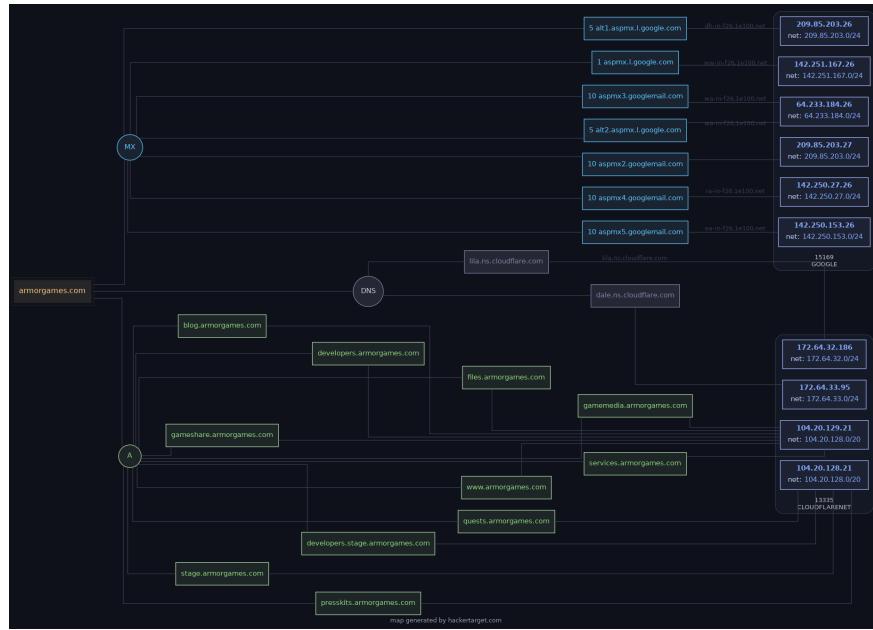
HOSTNAME	COMMON NAME	FIRST SEEN
+ calendar.armorgames.com	calendar.armorgames.com	12/08/2024
+ blog.armorgames.com	blog.armorgames.com	30/06/2022
+ vpn.armorgames.com	vpn.armorgames.com	19/11/2020
+ test.armorgames.com	test.armorgames.com	15/07/2020
+ www.test.armorgames.com	test.armorgames.com	15/07/2020
+ services.armorgames.com	services.armorgames.com	19/11/2019
+ developers.armorgames.com	developers.armorgames.com	19/11/2019
+ www.armorgames.com	armorgames.com	19/11/2019
+ api.armorgames.com	armorgames.com	19/11/2019
+ origin.armorgames.com	armorgames.com	19/11/2019
+ stage.armorgames.com	stage.armorgames.com	09/11/2019
+ mobile.armorgames.com	mobile.armorgames.com	08/11/2019
+ support.armorgames.com	support.armorgames.com	03/10/2019
+ *.cache.armorgames.com	cache.armorgames.com	05/07/2019
+ cache.armorgames.com	cache.armorgames.com	05/07/2019
+ services-stage.armorgames.com	services-stage.armorgames.com	13/03/2019
+ mobile.stage.armorgames.com	mobile.stage.armorgames.com	13/03/2019
+ developers.stage.armorgames.com	developers.stage.armorgames.com	13/03/2019
+ *.stage.armorgames.com	armorgames.com	13/03/2019
+ sendy.armorgames.com	sendy.armorgames.com	27/02/2019
+ presskits.stage.armorgames.com	presskits.stage.armorgames.com	12/10/2017
+ presskits.armorgames.com	presskits.armorgames.com	12/10/2017
+ *.armorgames.com	ssl1625.cloudflare.com	24/09/2014

Rysunek 27. Subdomeny uzyskane ze strony Merklemap.com

Scan date: 2024-11-30 12:02:54
 Domain Country: Worldwide (COM)
 Subdomains found: 46
 Most used IP: 172.67.2.10 (4x)

Whois Check	Check Status	Copy to clipboard	Download CSV	Download JSON
Subdomain	IP	Cloudflare		
agl.armorgames.com	13.32.145.39			
blog.armorgames.com	172.67.2.10			
cache.armorgames.com	99.86.91.55			
calendar.armorgames.com	85.121.14.139			
developers.armorgames.com	104.20.128.21			
developers.stage.armorgames.com	104.20.128.21			
files.armorgames.com	172.67.2.10			
presskits.armorgames.com	172.67.2.10			
services-stage.armorgames.com	104.20.129.21			
services.armorgames.com	104.20.128.21			
stage.armorgames.com	172.67.2.10			
support.armorgames.com	216.198.54.1			
vpn.armorgames.com	54.84.0.10			
www.armorgames.com	104.20.129.21			

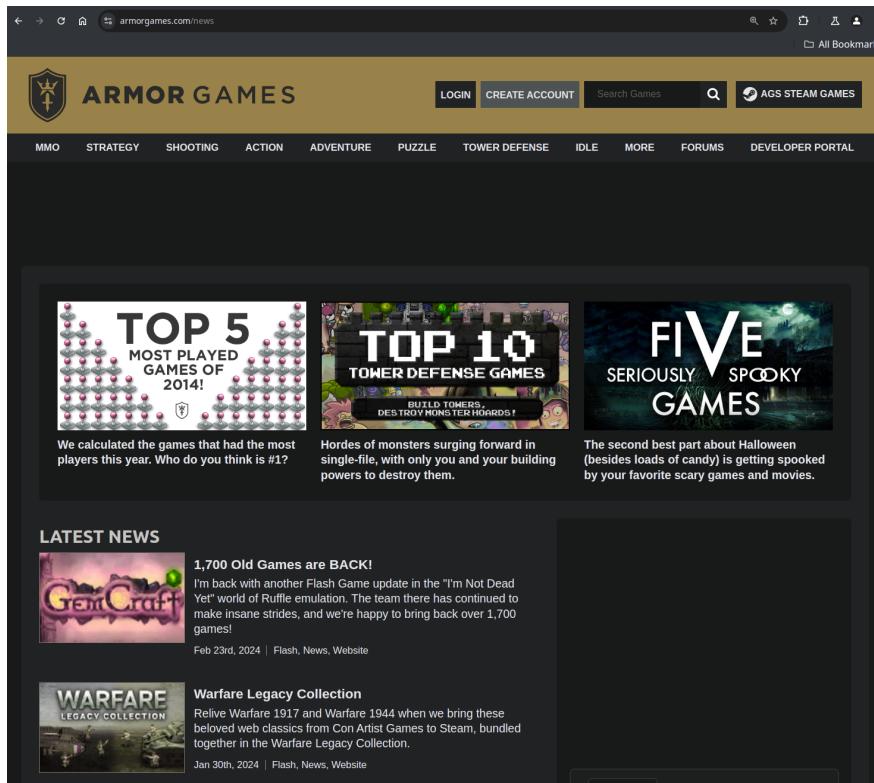
Rysunek 28. Subdomeny uzyskane ze strony c99.nl



Rysunek 29. Struktóra subdomen oraz serwerów do nich przypisanych uzyskana z dnsdumpster

5.1 Blog

Subdomena `blog.armorgames.com` przekierowywuje na stronę `armorgames.com`, w folder `/news` (rys. 30). Używając Wayback Machine, możliwe jest zweryfikowanie, że subdomena była odpowiedzialna za oddzielny blog ostatni raz w roku 2017. (rys. 31). Blog prawdopodobnie został usunięty ze względu na niską aktywność użytkowników na nim. Każdy z dostępnych postów posiadał zero komentarzy.



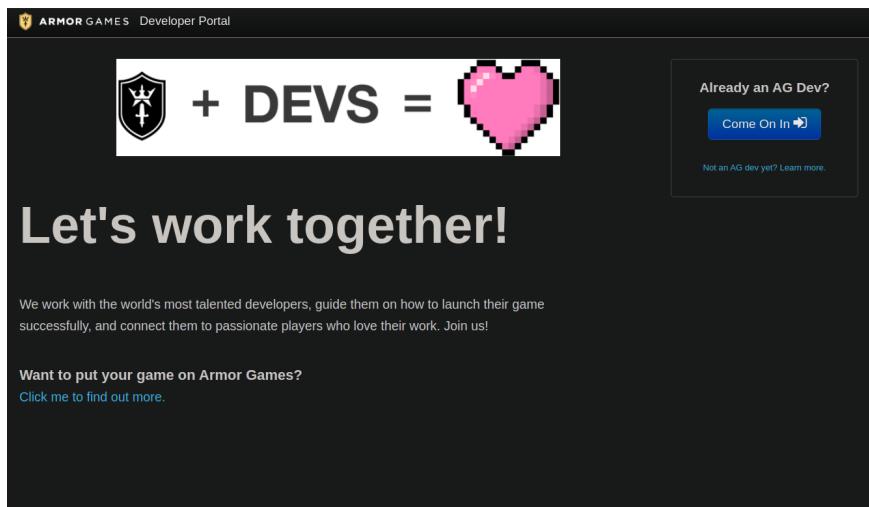
Rysunek 30. Witryna blog.armorgames.com



Rysunek 31. Armor Games Blog w 2017

5.2 Developers

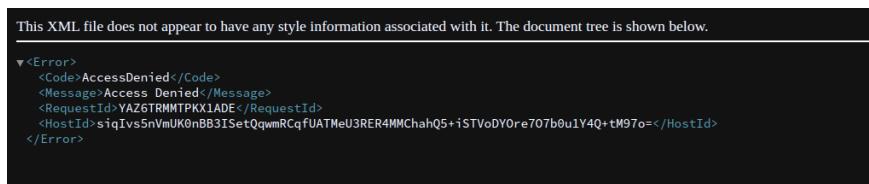
Subdomena developers.armorgames.com jest reklamą zachęcającą do współpracy z firmą Armor Games. (rys. 32) Są tylko dwa hiperłącza na stronie. Oba z nich przekierowywają na [/docs/introduction/overview](#), gdzie tłumaczone jest API Armor Games używane do gier online. Hiperłącze “Come on in” przekierowywuje ponownie na stronę logowania na armorgames.com. Subdomena jest jednym miejscem, w którym oficjalna dokumentacja API jest podlinkowana, a więc została ona zapewne stworzona, w celu zwiększenia jej widoczności dla przyszłych i obecnych deweloperów.



Rysunek 32. Witryna developers.armorgames.com

5.3 Files, Gamemedia, Services, Gameshare, Quests

Wszystkie z tych subdomen zwracają XML z kodem AccessDenied (rys. 33). Są to prawdopodobnie subdomeny dostępne tylko dla zarejestrowanych deweloperów Armor Games, współpracujących przy tworzeniu kolejnych gier flash.



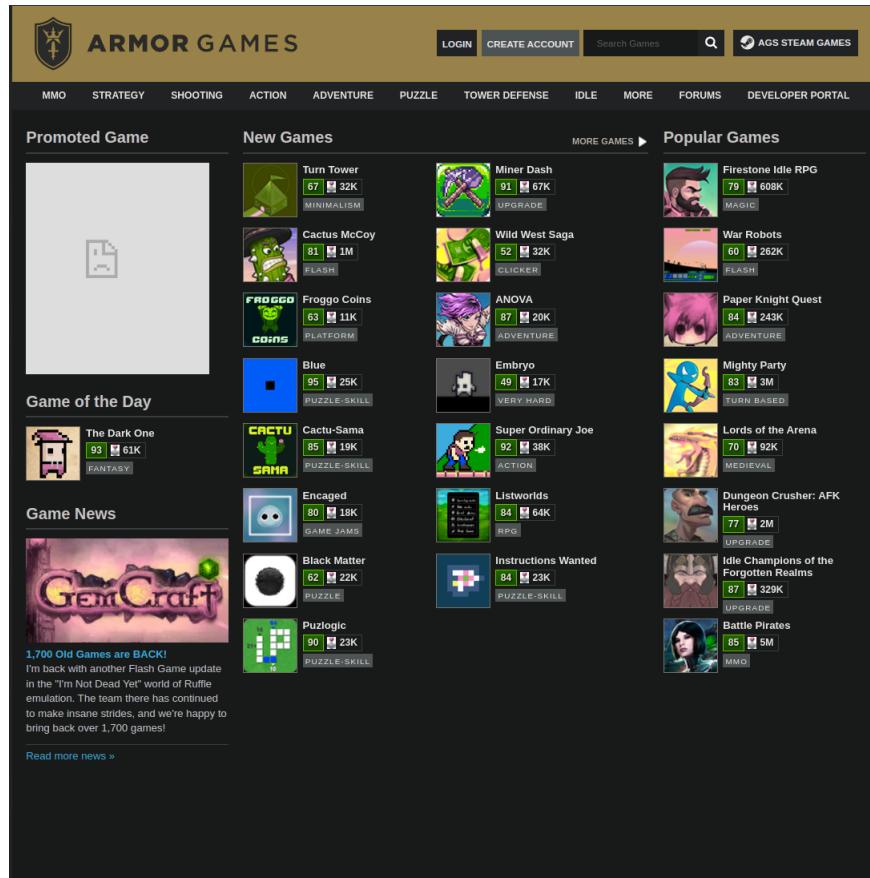
Rysunek 33. Witryna gamemedia.armorgames.com

5.4 Stage

Witryna stage.armorgames.com wygląda zasadniczo podobnie do witryny głównej armorgames.com (rys. 34), jednak prezentuje inne gry. Wygląda jakby była to strona do testów

publicznych. Niektóre z gier nie istnieją, niektóre nie posiadają dokładnych opisów. Zastosowanie tej domeny było omawiane dwukrotnie na oficjalnym blogu, a więc deweloperzy wiedzą o jej publicznym dostępie, jednak nigdzie jej nie rozpowszechniali.

Można wyciągnąć pare informacji po przeanalizowaniu stanu strony: - Gry mają inne rankingi użytkowników, niż na oficjalnej stronie - Dodawane są puste tytuły, bez gier - Dodawane są tam gry testowe, z przyszłą datą wydania - Pozostawione są tam gry, które zostały usunięte z głównej strony



Rysunek 34. Witryna stage.armorgames.com

5.5 Presskits

Witryna presskits.armorgames.com prezentuje stare informacje dla prasy (rys. 35). Strona nie jest aktualizowana od dłuższego czasu, ponieważ została zastąpiona nową na domenie armorgamesstudios.com. Pokazuje to coraz większe nastawienie firmy na tworzenie gier na inne platformy i odseparowanie marki Armor Games od Armor Games Studios.

◆ Please see our new web site with updated press kits here. ◆

Armor Games Studios

armorgamesstudios.com

Factsheet

Developer:
Armor Games Studios
Based in Irvine, California

Founding date:
October 2005

Website:
armorgamesstudios.com

Press / Business contact:
Presskits@ArmorGames.com

Social:
Facebook
Twitter

Releases:

- Swords & Souls: Neverseen
- Bear and Breakfast
- Bilkins' Folly
- Chock & Sosig: Walk the Plank
- Crush the Castle: Legacy Collection
- Crush the Castle: Siege Master
- Deep Sleep Labyrinth of the Forsaken
- Deep Sleep Trilogy
- Don't Escape: 4 Days to Survive
- Don't Escape Trilogy
- In Stars and Time
- Infectorator 3: Apocalypse
- Islets
- ITTA
- Jet Lancer
- The Last Stand: Aftermath
- The Last Stand: Legacy Collection
- Lumberjack
- Nauticrawl
- Never Give Up
- Pinstripe
- A Rogue Escape
- Snacko
- Soda Dungeon
- Soda Dungeon 2
- SOLAS 128

Description

Armor Games Studios is both a publisher of unique and creative indie games from all over the world, and one of the internet's longest running curated free Flash gaming portals. Play thousands of free games online at <http://www.armorgames.com>, or visit our publishing website at <http://www.armorgamesstudios.com>.

History

Early history

Since 2004, from its original inception as Games of Gondor to its 2005 rebranding, Armor Games has been a place that unites passionate players and talented gamers. It is best known for the sponsorship of iconic Flash titles such as Kingdom Rush, Sushi Cat, and the original Sonny games, though its current catalogue spans thousands of games in every genre.

After that

While Armor Games has launched successful mobile titles for iOS and Android for years, in 2015 it created the Armor Games Studios to serve as a publishing arm for indies looking to bring their games to Steam and other platforms, with the company's first console releases on Xbox One, Nintendo Switch, and PlayStation 4 in 2018. Focusing an emphasis on working with its developers rather than dictating, Armor Games Studios enjoys a relationship with many talented creators, bringing their games to Steam, GOG, the Humble Store, and many platforms to come.

Games

- Swords & Souls: Neverseen
- Bear and Breakfast
- Bilkins' Folly
- Chock & Sosig: Walk the Plank
- Crush the Castle: Legacy Collection
- Crush the Castle: Siege Master
- Deep Sleep Labyrinth of the Forsaken
- Deep Sleep Trilogy
- Don't Escape: 4 Days to Survive
- Don't Escape Trilogy
- In Stars and Time
- Infectorator 3: Apocalypse
- Islets
- ITTA
- Jet Lancer
- The Last Stand: Aftermath
- The Last Stand: Legacy Collection
- Lumberjack

Rysunek 35. Witryna presskits.armorgames.com

5.6 Podsumowanie

Domena posiada wiele subdomen, jednak większość z nich jest dostępna dla zwykłych użytkowników. Strony dostępne dla nas są już przestarzałe i nieaktualizowane albo stronami do testów publicznych. Jedyną stroną, która może być ciągle wykorzystywana jest developers.armorgames.com, która pozwala na przekierowanie do mniej oczywistej strony z dokumentacją API dla deweloperów.

6 Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi

6.1 Otwarte porty

Skan otwartych portów z dnsportchecker.org (rys. 36, 37) oraz shodan.io (rys. 38) pokazuje, że serwer pod adresem IP 104.20.128.21 ma otwarte porty 80, 443, 8080, 8880, 8443, 2082, 2083, 2086, 2087, 2095.

Ping Result for IP: 104.20.128.21			
Connected To	Response Time	TTL	No of Bytes
104.20.128.21	2.26 ms	57	64
104.20.128.21	1.58 ms	57	64
104.20.128.21	1.23 ms	57	64
104.20.128.21	1.36 ms	57	64
104.20.128.21	1.17 ms	57	64
Packet Summary			
Sent	Received	Loss	Time
5	5	0%	4004 ms
Latency Summary			
Min	Max	Avg	StdDev
1.176	2.262	1.524	0.395

Rysunek 36. Adres IP serwera z dnschecker.org

Custom Port # 1	80	Open
Custom Port # 2	443	Open
Custom Port # 3	2080	Timed-Out
Custom Port # 4	2083	Open
Custom Port # 5	2086	Open
Custom Port # 6	2087	Open
Custom Port # 7	2095	Open
Custom Port # 8	8080	Open
Custom Port # 9	8443	Open
Custom Port # 10	8880	Open

Rysunek 37. Wynik skanu portów z dnschecker.org

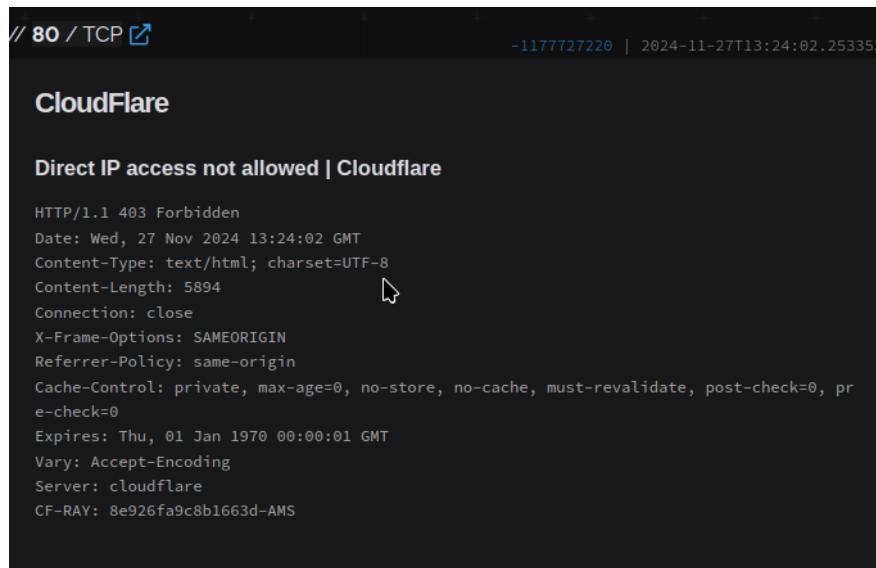


Rysunek 38. Wynik skanu portów z shodan.io

6.1.1 Porty 80, 443

Wynik łączenia z portem 80 przez shodan.io (rys. 39), pokazuje jakbyśmy nie mieli dostępu do niego. Wynik jest jednak taki, ponieważ shodan stara się ominąć przekierowanie. Przy normalnym użytkowaniu, przy próbie połączenia z portem 80, użytkownik jest przekierowywany na port 443, w celu używania zaszyfrowanego połączenia.

Port 443 jest domyślnie używanym portem do serwowania gier użytkownikom. (rys. 40) Jest tak, ponieważ aktualnie większość użytkowników strony loguje się przed graniem w gry, a więc w celu ochrony ich danych wykorzystywany jest HTTPS. Można sprawdzić poprawność konfiguracji, poprzez weryfikację certyfikatu dostarczonego nam przez serwer (rys. 41) oraz poprzez stronę shodan.io (rys. 42). Można zauważyć, że serwer wykorzystuje TLS 1.3, a więc aktualnego standardu, oraz wykorzystuje do szyfrowania danych TLS_AES_128_GCM_SHA256. Certyfikat został podpisany przez Let's Encrypt.



The screenshot shows a Shodan search result for port 80/TCP. At the top, it says "Cloudflare" and "Direct IP access not allowed | Cloudflare". Below that is a detailed HTTP response header:

```
HTTP/1.1 403 Forbidden
Date: Wed, 27 Nov 2024 13:24:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5894
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 8e926fa9c8b1663d-AMS
```

Rysunek 39. Wynik łączenia z portem 80 przez shodan.io



Play Free Games Online at Armor Games

```

HTTP/1.1 200 OK
Date: Wed, 27 Nov 2024 12:45:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
p3p: policyref="/w3c/p3p.xml", CP="CA0 DSP COR CURa ADMa DEVa TAia OUR BUS IND UNI COM NAV INT"
origin-agent-cluster: ?
content-security-policy: frame-ancestors 'self', upgrade-insecure-requests
x-frame-options: SAMEORIGIN
Cache-Control: max-age=300, public
vary: Cookie,Accept-Encoding
x-cache: Miss from cloudfront
via: 1.1 dbbla0d298f6a202c2f5a2e11bef88fe.cloudflare.net (CloudFront)
x-amz-cf-pop: SF053-P6
x-amz-cf-id: HYnfK9ixdZ6dp65j9joYXPy2F-sP_1p0Cx0PmFbaQP-wqPvCLVRcw==
CF-Cache-Status: HIT
Age: 188
Last-Modified: Wed, 27 Nov 2024 12:42:47 GMT
Server: cloudflare
CF-RAY: 8e9237d67f16cf7a-SJC
alt-svc: h3=":443"; ma=86400

```

Rysunek 40. Wynik łączenia z portem 443 przez shodan.io

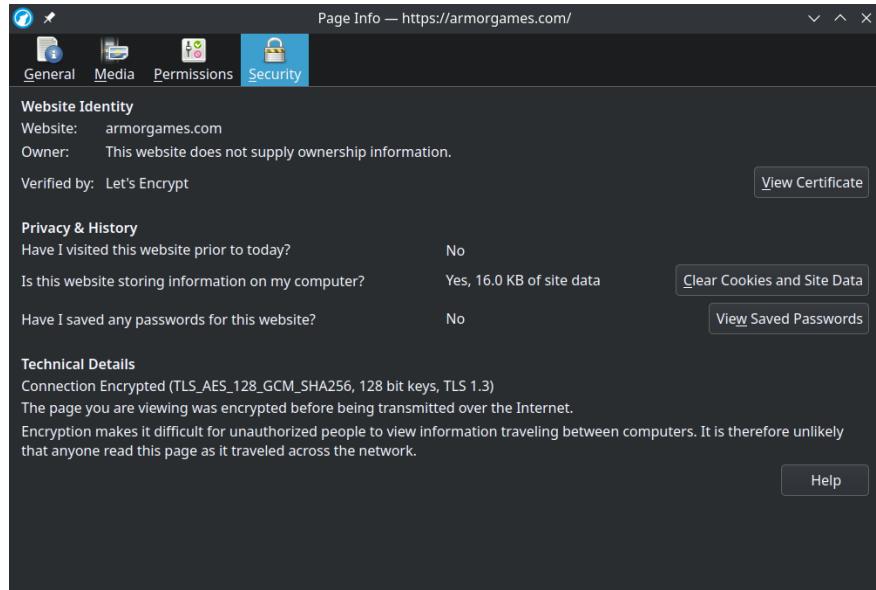
SSL Certificate

```

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
03:4a:bd:3e:11:a8:7e:09:5a:5c:6b:bc:7d:ed:19:0f:b6:74
Signature Algorithm: ecdsa-with-SHA384
Issuer: C=US, O=Let's Encrypt, CN=E6
Validity
Not Before: Nov 1 01:10:47 2024 GMT
Not After : Jan 30 01:10:46 2025 GMT
Subject: CN=armorgames.com
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:a6:2c:02:dc:a3:59:65:bd:a0:4b:df:d4:59:4f:
f5:18:fb:5d:f1:7a:db:79:67:3a:f3:d8:a4:43:64:
43:dc:52:8a:25:ce:53:63:0c:19:46:05:5e:dc:11:
08:eb:e4:cc:e2:46:a9:ce:3e:a0:96:9f:e0:5e:69:
e0:78:b0:ca:1d
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Subject Key Identifier:
03:EE:E3:C2:D7:0D:BE:5C:17:08:25:7D:C6:6F:80:F4:6D:CE:EB:B5
X509v3 Authority Key Identifier:
93:27:46:98:03:A9:51:68:8E:98:D6:C4:42:48:DB:23:BF:58:94:D2
Authority Information Access:
OCSP - URI:http://e6.o.lencr.org
CA Issuers - URI:http://e6.i.lencr.org/
X509v3 Subject Alternative Name:
DNS:*.armorgames.com, DNS:*.stage.armorgames.com, DNS:armorgames.com

```

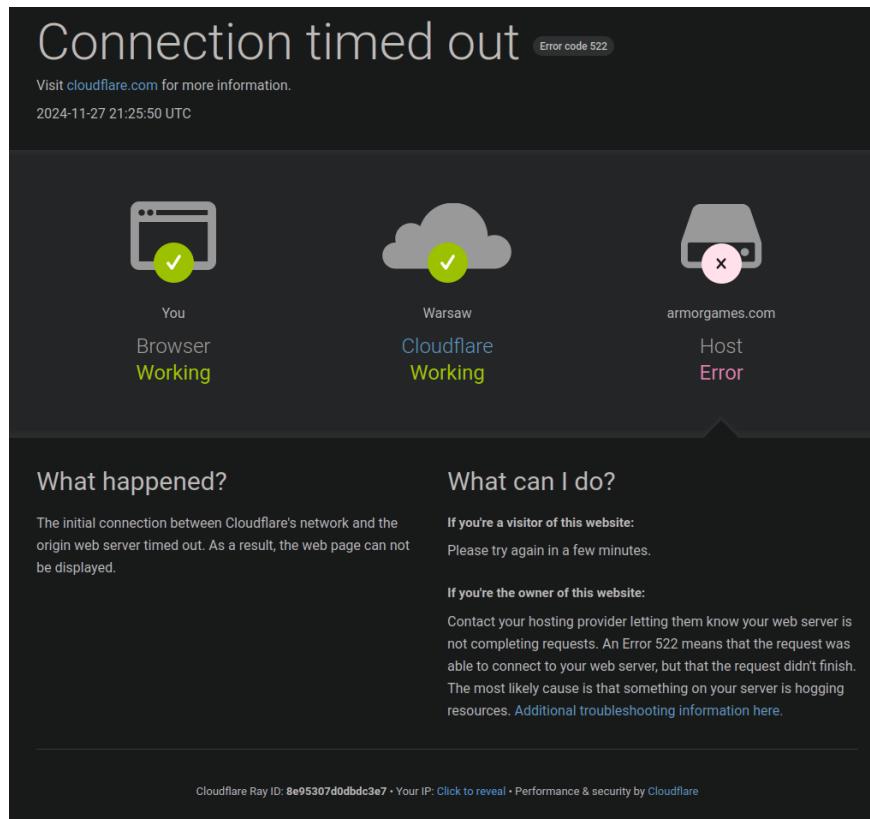
Rysunek 41. Certyfikat SSL używany na porcie 443 wykryty przez shodan.io



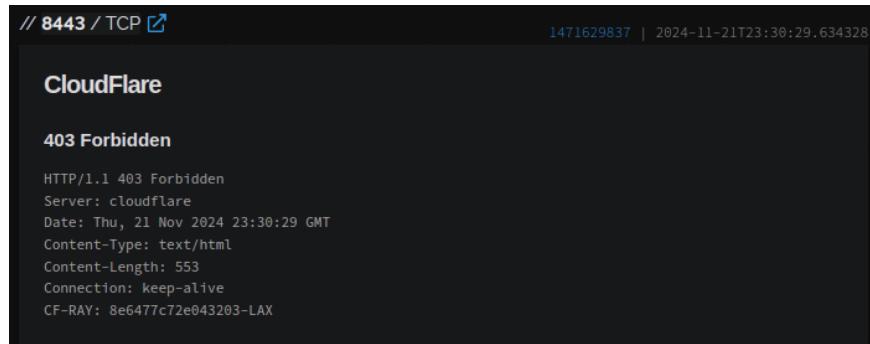
Rysunek 42. Certyfikat SSL na stronie armorgames.com

6.1.2 Porty 8080, 8443, 8880

Wszelkie manualne próby połączenia się z portami 8080, 8443 oraz 8880 skutkują niepowodzeniem. (rys. 43) Shodan.io zwraca ten sam wynik dla tych portów. (rys. 44). Można spekulować, że są to porty używane przez Apache Tomcat, do których mają dostęp tylko określone adresy IP.



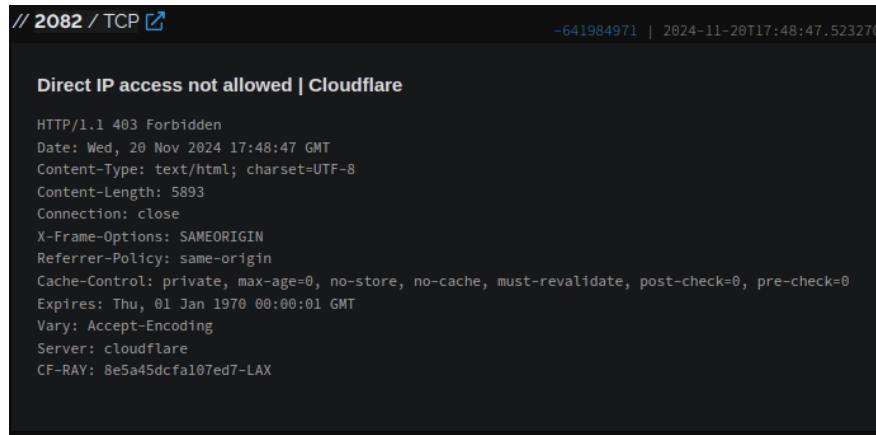
Rysunek 43. Próba połączenia z portem 8443



Rysunek 44. Wynik łączenia z portem 8443 przez shodan.io

6.1.3 Porty 2082, 2083, 2086, 2087, 2095

Analiza wyników z shodan.io (rys. 45, 46, 47) pokazuje nam, że nie jest możliwym uzyskanie dostępu do tych portów poprzez bezpośrednią próbę uzyskania informacji z tych portów. Uzyskanie do nich dostępu jest możliwe, tylko z odpowiednimi headerami. Można spekuluwać, że za portami 2082 i 2083 schowany jest cpanel, 2086 i 2087 Web Host Manager, a za portem 2096 webmail. Są to najczęstrze zastosowania dla tych subdomen.

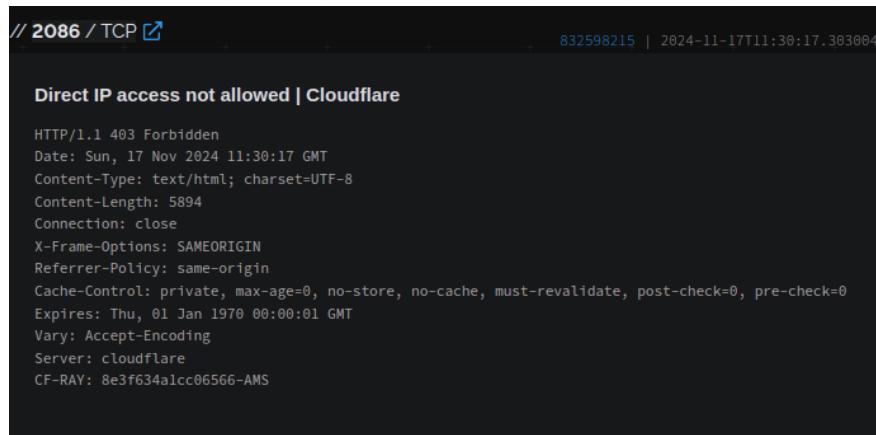


// 2082 / TCP [🔗](#) -641984971 | 2024-11-20T17:48:47.523270

Direct IP access not allowed | Cloudflare

```
HTTP/1.1 403 Forbidden
Date: Wed, 20 Nov 2024 17:48:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5893
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 8e5a45dcfa107ed7-LAX
```

Rysunek 45. Wynik łączenia z portem 2082 przez shodan.io



// 2086 / TCP [🔗](#) 832598215 | 2024-11-17T11:30:17.303064

Direct IP access not allowed | Cloudflare

```
HTTP/1.1 403 Forbidden
Date: Sun, 17 Nov 2024 11:30:17 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5894
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 8e3f634a1cc06566-AMS
```

Rysunek 46. Wynik łączenia z portem 2086 przez shodan.io

// 2095 / TCP ↗
-2096746543 | 2024-10-31T19:14:32.391965

Direct IP access not allowed | Cloudflare

```
HTTP/1.1 403 Forbidden
Date: Thu, 31 Oct 2024 19:14:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 8db5f7f86c171c94-AMS
```

Rysunek 47. Wynik łączenia z portem 2095 przez shodan.io

6.2 Systemy operacyjne

Skany wykonane używając censys.io (rys. 48), shodan.io (rys. 49) oraz securityheaders.com (rys. 50) nie pozwalają na zweryfikowanie systemu operacyjnego używanego przez dany serwer.

104.20.128.21
As of: Jan 03, 2025 2:52pm UTC | Latest

[Summary](#) [History](#) [WHOIS](#) [Explore](#)

Basic Information

- Forward DNS presskits.armorgames.com, 059879e5-b2e8-4f58-aa46-95f69d92aa34.random.13noon.com, developers.armorgames.com, stage.armorgames.com, armorgames.com, ...
- Routing 104.20.128.0/20 via CLOUDFLARENET, US (AS13335)
- Services (13) 80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

HTTP 80/TCP 01/03/2025 12:05 UTC

Rysunek 48. Skan censys.io

104.20.128.21

Regular View Raw Data

// TAGS: cdn

General Information

Hostnames	armorgames.com
Domains	ARMORGAMES.COM
Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

Web Technologies

Miscellaneous

HTTP/3

Rysunek 49. Skan shodan.io

Security Report Summary

Site:	https://armorgames.com/
IP Address:	104.20.129.21
Report Time:	03 Jan 2025 15:06:52 UTC
Headers:	Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

Advanced: Your site could be at risk, let's perform a deeper security analysis of your site and APIs. Start Now

Rysunek 50. Skan securityheaders.com

6.3 Podsumowanie

Użytkownicy są w stanie uzyskać dostęp tylko do jednego z wielu portów serwera odpowiadającego za armorgames.com. Reszta z nich wymaga innych uprawnień lub sposobu dostępu. Nie możliwym jest zweryfikowanie systemu operacyjnego wykorzystywanego przez serwer.

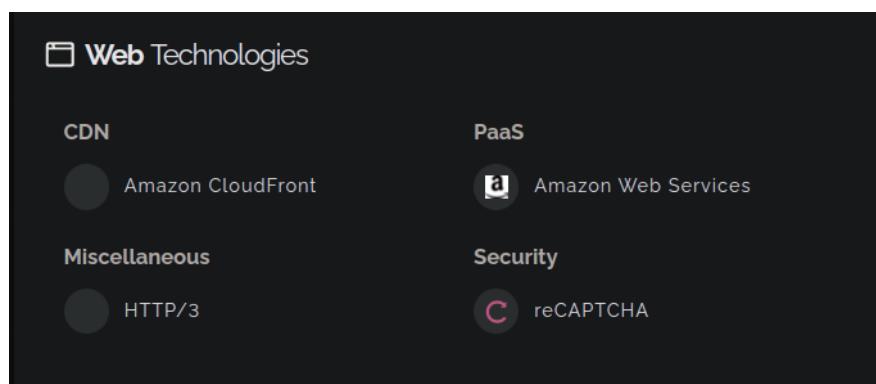
7 Wykorzystywane technologie informatyczne

Strona opiera się na infrastrukturze chmurowej Amazon Web Services (rys. 51, 52, 53, 56), integrując usługi takie jak Amazon CloudFront do globalnego dostarczania treści oraz Amazon S3 do przechowywania zasobów statycznych. W analizie technologicznej wykazano również obecność Cloudflare, zarówno jako dostawcy DNS, jak i warstwy ochronnej WAF, co umożliwia skuteczne filtrowanie ruchu oraz ochronę przed atakami typu DDoS.

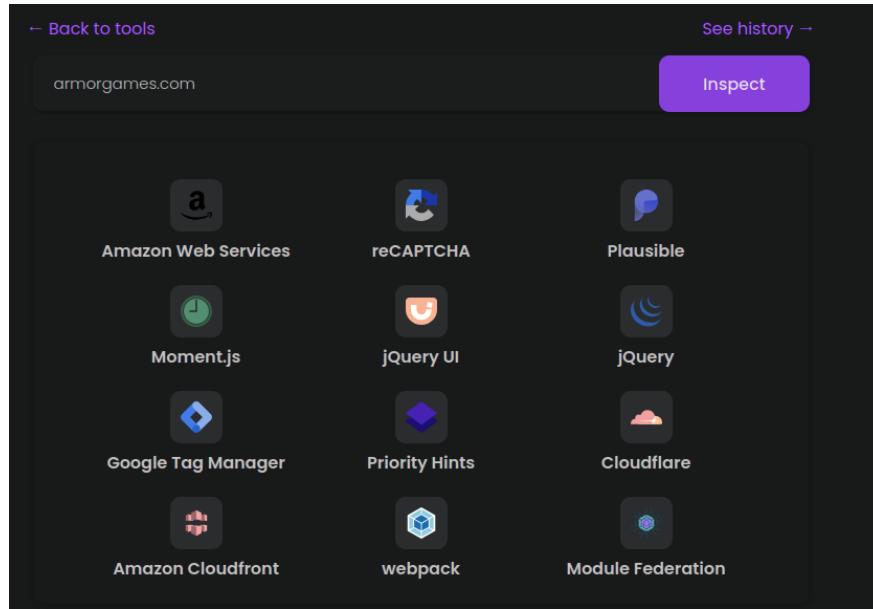
Skany strony wykonane używając shodan.io (rys. 51), hexomatic.io, (rys. 52), wappalyzer.com (rys. 53) oraz buildwith.com (rys. 55) wskazują na to, że strona wykorzystuje system reCAPTCHA, w celu powstrzymania botów oraz prób scrapingu. Jest to popularne rozwiązanie stworzone przez firmę Google, zmuszające podjerzane próby połączenia do rozwiązania prostych zadań. W teorii tylko ludzie są w stanie je rozwiązać. Polegają one na zaznaczaniu odpowiednich obrazków.

Do analizy zachowań użytkowników strona wykorzystuje Google Analytics, Google Universal Analytics oraz Facebook Domain Insights (rys. 57). Zastosowanie tych technologii pozwala na dokładne śledzenie sposobu spędzania czasu przez użytkowników na tych stronach oraz monetyzacji tego. Lepsze badanie użytkowników pozwala zwiększenie dochodów z reklam dla Armor Games. Monetyzację tego ruchu widać poprzez używanie kilkunastu różnych mechanizmów obsługi reklam takich jak DoubleClick, Ads.txt czy AppNexus. Używanie tych mechanizmów pozwala efektywne dopasowywanie reklam dla każdego użytkownika. (rys. 58) Strona stara się dostosować sposób zbierania informacji o użytkownikach do regionu z którego się łączą, dlatego wykorzystuje US privacy user signal. (rys. 55) Zastosowanie takich technologii jest konieczne, ponieważ Armor Games jest legalnie zarejestrowana firma w Kalifornii, a więc mogliby się narazić na kary finansowe, jeśli naruszyliby RODO i jego odpowiedniki w innych krajach.

W celu zapewnienia interaktywnego interfejsu używane są biblioteki jQuery oraz Bootstrap.js. (rys. 52, 53, 54)



Rysunek 51. Technologie sieciowe wykryte przez shodan.io



Rysunek 52. Dane na temat narzędzi używanych przez stronę zdaniem Hexomatic

7.1 Podsumowanie

Strona ArmorGames.com wykorzystuje infrastrukturę Amazon Web Services i zabezpieczenia Cloudflare do ochrony i globalnego dostarczania treści. reCAPTCHA wykorzystywana jest w celu ograniczenia działania botów i scrapingu. Google Analytics i mechanizmy reklamowe, takie jak DoubleClick, wspierają monetyzację ruchu. Interfejs jest generowany używając jQuery.

The screenshot shows the Wappalyzer interface with a purple header containing the logo and navigation icons. Below the header, there are tabs for 'TECHNOLOGIES' (selected), 'MORE INFO', and a download icon labeled 'Export'. The main content area is divided into several sections: 'Analytics' (Plausible), 'CDN' (Amazon CloudFront, Cloudflare), 'Security' (reCAPTCHA), 'JavaScript libraries' (jQuery 1.8.2, jQuery UI 1.8.23, Moment.js 2.9.0), 'Miscellaneous' (HTTP/3, Open Graph, RSS), and 'PaaS' (Amazon Web Services). A link 'Something wrong or missing?' is at the bottom.

Rysunek 53. Dane na temat narzędzi używanych przez stronę z analizy programu Wappalyzer

Open Graph	Miscellaneous
Plausible	Analytics
Webpack	Miscellaneous
Module Federation	Miscellaneous
Priority Hints	Performance
Cloudflare	CDN
reCAPTCHA	Security
Google Tag Manager	Tag managers
RSS	Miscellaneous

Rysunek 54. Analiza Pentest Tools

Widgets View Global Trends

 **Apple Whitelist**
[Apple Whitelist Usage Statistics](#) · [Download List of All Websites using Apple Whitelist](#)
 This website domain is on the Apple TLD whitelist which may potentially mean these domains will appear in autocomplete when looking up URLs on Apple products.

 **Slack**
[Slack Usage Statistics](#) · [Download List of All Websites using Slack](#)
 Messaging app for teams that makes working together simple and efficient.

 **reCAPTCHA**
[reCAPTCHA Usage Statistics](#) · [Download List of All Websites using reCAPTCHA](#)
 Anti-bot CAPTCHA widget from Google.
 CAPTCHA

 **Google Tag Manager**
[Google Tag Manager Usage Statistics](#) · [Download List of All Websites using Google Tag Manager](#)
 Tag management that lets you add and update website tags without changes to underlying website code.
 Tag Management

 **US Privacy User Signal Mechanism**
[US Privacy User Signal Mechanism Usage Statistics](#) · [Download List of All Websites using US Privacy User Signal Mechanism](#)
 The US Privacy API (USP API) is a lightweight API used to communicate signals represented in the US Privacy String.
 Privacy Compliance

 **CrUX Dataset**
[CrUX Dataset Usage Statistics](#) · [Download List of All Websites using CrUX Dataset](#)
 CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the internet.

 **CrUX Top 50m**
[CrUX Top 50m Usage Statistics](#) · [Download List of All Websites using CrUX Top 50m](#)
 Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 50 million.

 **CrUX Top 50k**
[CrUX Top 50k Usage Statistics](#) · [Download List of All Websites using CrUX Top 50k](#)
 Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 50k.

 **Azure Active Directory**
[Azure Active Directory Usage Statistics](#) · [Download List of All Websites using Azure Active Directory](#)
 Enterprise identity service that provides single sign-on, multifactor authentication and more.
 Login

Rysunek 55. Dodatkowe mechanizmy wykryte przez buildwith.com

Content Delivery Network View Global Trends

 **GStatic Google Static Content**
[GStatic Google Static Content Usage Statistics](#) · [Download List of All Websites using GStatic Google Static Content](#)
 Google has off-loaded static content (Javascript/Images/css) to a different domain name in an effort to reduce bandwidth usage and increase network performance for the end user.

 **CDN JS**
[CDN JS Usage Statistics](#) · [Download List of All Websites using CDN JS](#)
 CloudFlare's CDN with popular javascript frameworks available.

 **Amazon S3**
[Amazon S3 Usage Statistics](#) · [Download List of All Websites using Amazon S3](#)
 Amazon Simple Storage provides unlimited storage to developers and online businesses - saving costs and increase storage reliability.

 **Cloudflare**
[Cloudflare Usage Statistics](#) · [Download List of All Websites using Cloudflare](#)
 Automatically optimizes the delivery of your web pages so your visitors get the fastest page load times and best performance.

 **AJAX Libraries API**
[AJAX Libraries API Usage Statistics](#) · [Download List of All Websites using AJAX Libraries API](#)
 The AJAX Libraries API is a content distribution network and loading architecture for the most popular, open source JavaScript libraries.

 **Cloudflare JS**
[Cloudflare JS Usage Statistics](#) · [Download List of All Websites using Cloudflare JS](#)
 Loads content from Cloudflare CDN.

Rysunek 56. Znalezienie CDN używając buildwith.com

Analytics and Tracking View Global Trends

 **Facebook Domain Insights**
[Facebook Domain Insights Usage Statistics](#) · [Download List of All Websites using Facebook Domain Insights](#)
 This website contains tracking information that allows admins to see Facebook Insights out of Facebook to this domain.
 Social Management

 **Google Analytics**
[Google Analytics Usage Statistics](#) · [Download List of All Websites using Google Analytics](#)
 Google Analytics offers a host of compelling features and benefits for everyone from senior executives and advertising and marketing professionals to site owners and content developers.
 Application Performance · Audience Measurement · Visitor Count Tracking

 **Google Universal Analytics**
[Google Universal Analytics Usage Statistics](#) · [Download List of All Websites using Google Universal Analytics](#)
 The analytics.js JavaScript snippet is a new way to measure how users interact with your website. It is similar to the previous Google tracking code, ga.js, but offers more flexibility for developers to customize their implementations.

Rysunek 57. Tracking wykryty przez buildwith.com

Advertising View Global Trends

 **DoubleClick.Net**
[DoubleClick.Net Usage Statistics](#) · [Download List of All Websites using DoubleClick.Net](#)
DoubleClick enables agencies, marketers and publishers to work together successfully and profit from their digital marketing investments. Owned by Google and now referred to as DoubleClick Digital Marketing or Google Enterprise Advertising.

 **Google Direct**
[Google Direct Usage Statistics](#) · [Download List of All Websites using Google Direct](#)
Website is a direct publisher for Google ad content.
[ads.txt](#)

 **Ads.txt**
[Ads.txt Usage Statistics](#) · [Download List of All Websites using Ads.txt](#)
A public record of Authorized Digital Sellers for a website.
[ads.txt](#)

 **SpotXChange Direct**
[SpotXChange Direct Usage Statistics](#) · [Download List of All Websites using SpotXChange Direct](#)
Website is a direct publisher for SpotXChange ad content.
[ads.txt](#)

 **33 Across Reseller**
[33 Across Reseller Usage Statistics](#) · [Download List of All Websites using 33 Across Reseller](#)
The website owner has authorized another entity to control 33 Across ads on this site.
[ads.txt](#)

 **Amazon Reseller**
[Amazon Reseller Usage Statistics](#) · [Download List of All Websites using Amazon Reseller](#)
The website owner has authorized another entity to control Amazon ads on this site.
[ads.txt](#)

 **OpenX Reseller**
[OpenX Reseller Usage Statistics](#) · [Download List of All Websites using OpenX Reseller](#)
The website owner has authorized another entity to control OpenX ads on this site.
[ads.txt](#)

 **ContextWeb Reseller**
[ContextWeb Reseller Usage Statistics](#) · [Download List of All Websites using ContextWeb Reseller](#)
The website owner has authorized another entity to control ContextWeb ads on this site.
[ads.txt](#)

 **AppNexus Reseller**
[AppNexus Reseller Usage Statistics](#) · [Download List of All Websites using AppNexus Reseller](#)
The website owner has authorized another entity to control AppNexus ads on this site.
[ads.txt](#)

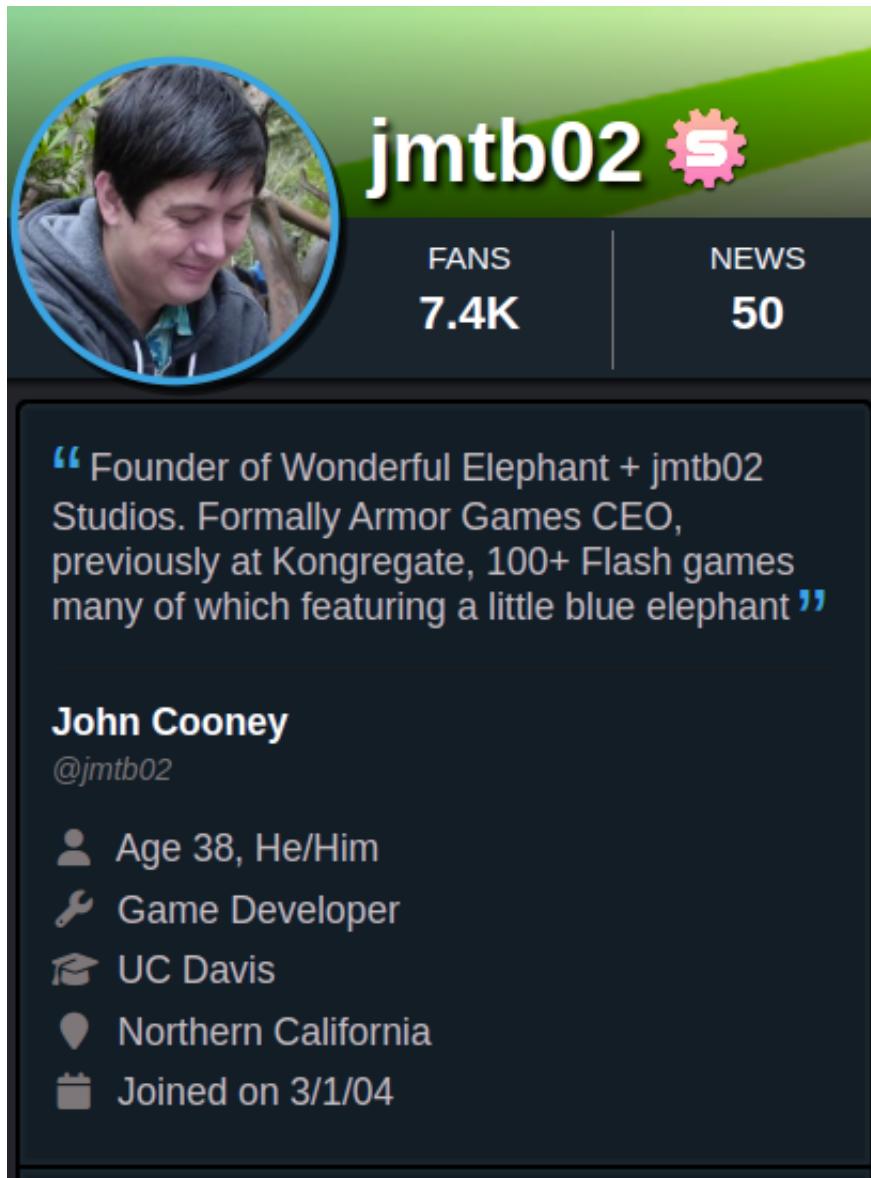
 **SpotXChange Reseller**
[SpotXChange Reseller Usage Statistics](#) · [Download List of All Websites using SpotXChange Reseller](#)
The website owner has authorized another entity to control SpotXChange ads on this site.
[ads.txt](#)

Rysunek 58. Reklamodawcy ze strony buildwith.com

8 Pracownicy i osoby powiązane

8.1 John Cooney

John Cooney jest aktualnym CEO firmy Armor Games. Jest on znany w internecie jako jmtb02. (rys. 59) Jest znany w internecie z tworzenia gier flash, głównego źródła dochodu firmy Armor Games. Jest także właścicielem firmy Wonderus Elephant (rys. 60), która także zajmuje się tworzeniem gier flash. Jest też on aktywny na mediach społecznościowych, na przykład na platformie X. Na bierząco informuje on tam o swoich planach. (rys. 61)



Rysunek 59. Profil John Cooney ze strony newgrounds.com

About

W O N D E R F U L E L E P H A N T I S C R E A T I N G V I D E O
G A M E S W I T H H A P P I N E S S A N D W O N D E R



My name is John Cooney (he/him) and Wonderful Elephant is my label for games.

Beginning in 2004 I've created and published over a 100 games across a billion+ gameplays on the web in the height of the Flash Game renaissance, additionally publishing dozens of indies titles with teams across PC and console at Armor Games (where I was formally CEO) and Kongregate (where I lead their premium games initiative).

I graduated with a Bachelor of Arts in Technocultural Studies from the University of California, Davis in 2007. During this period I started my first company, JMTB02 Studios, which self-developed and published games and animations. Many of my games went under the label "jmtb02." In 2017 I rebranded to Wonderful Elephant.

John have cats named Poppy and Bulldozer.

Rysunek 60. Profil John Cooney ze strony wonderfulelephant.com



Rysunek 61. Profil na x.com

8.2 Daniel McNeely

Daniel McNeely jest byłym CEO Armor Games oraz jej założycielem. Aktualnie nie jest już CEO, jest tylko właścicielem firmy. W 2002 roku skończył marketing na Uniwersytecie Biola. (rys. 62)

McNeely nie jest aktywny na mediach społecznościowych. Strona rocketreach.com pozwala na pozyskanie 6 numerów telefonów oraz 4 adresów email. (rys. 63)

Daniel McNeely
Owner/Founder of Armor Games Studios Inc.
Frisco, Texas, United States · [Contact info](#)
234 connections

[+ Connect](#) [Message](#) [More](#)

About
CEO with business development and management skills. Grew ArmorGames.com from 100,000 unique visitors per day, to over 750,000 and its still growing.
Also experienced in market research, meeting customer needs, and planning and executing 12-month business plans.
Specialties: Online Marketing, Game Publishing, Management, Project Lead, Website branding and Identity, Web 2.0, Casual Gaming

Activity
308 followers
Daniel McNeely commented on a post • 3w
Congrats Krin! 🎉

[Show all comments →](#)

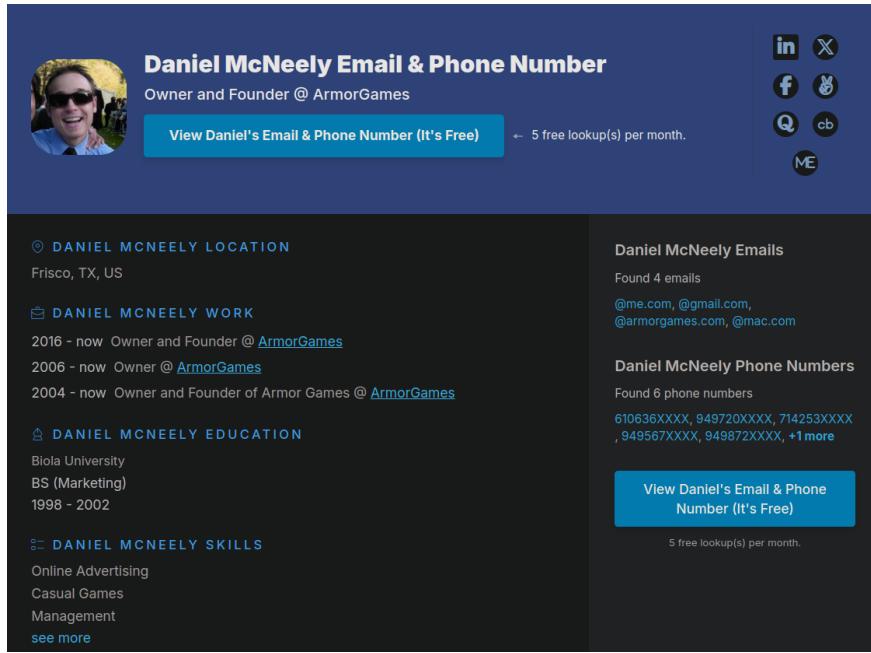
Enhance your own profile by adding a work experience. [Add experience](#)

Experience

Armor Games Studios
18 yrs 2 mos

- Owner/Founder**
Full-time
May 2016 - Present • 8 yrs 8 mos
Frisco, Texas, United States • Remote
- Owner**
Nov 2006 - Present • 18 yrs 2 mos
I oversee the business aspects and growth strategies of Armor Games.

Rysunek 62. Strona McNeely na LinkedIn.png

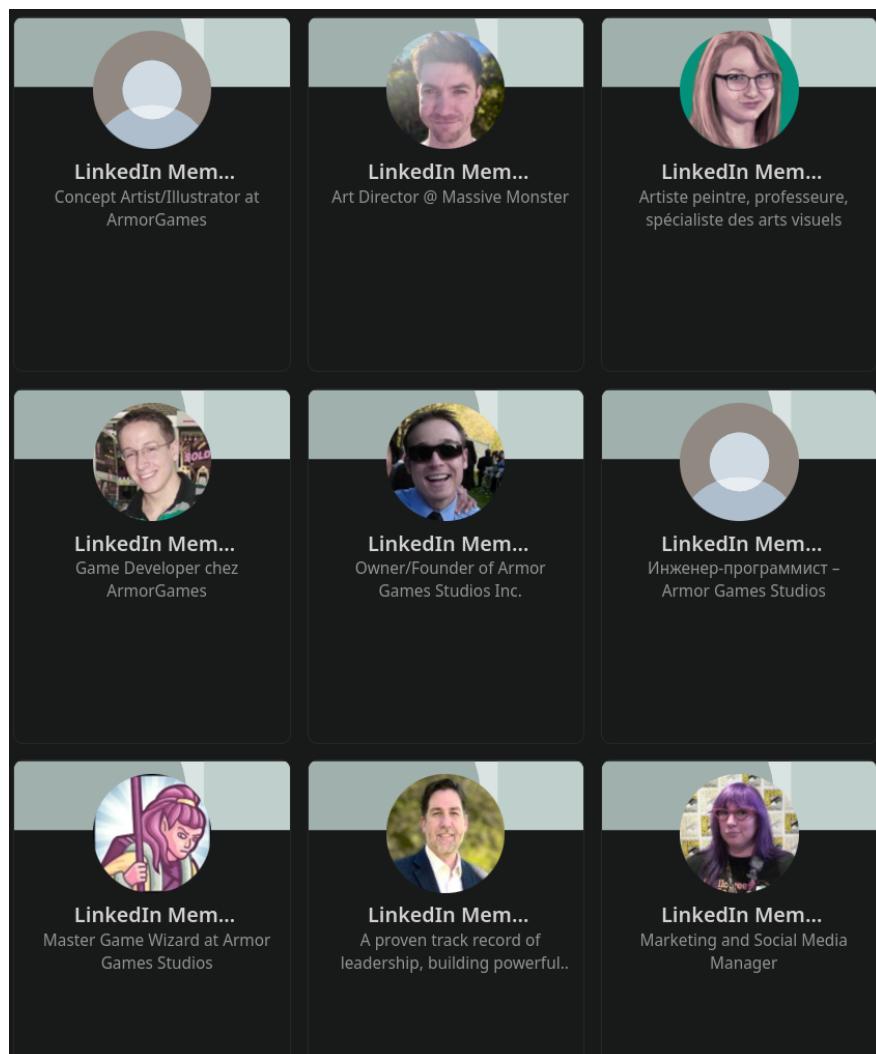


Rysunek 63. Strona McNeely na RocketReach.com

8.3 Obecni i byli Pracownicy

Pracowników można wyszukać za pomocą strony linkedin.com. Osoby te nie udostępniają swoich danych obcym osobom na stronie, jednak możliwym jest zobaczenie ich zdjęcia. (rys. 64)

Używając stron do wyszukiwania po obrazach takich jak tineye.com, można znaleźć imiona tych osób.



Rysunek 64. Widok pracowników na stronie linkedin.com

8.3.1 Louis-Simon Menard



Rysunek 65. Zdjęcie profilowe z linkedin.com

W celu znalezienia imienia danego pracownika, wyszukać można jego zdjęcie ze strony linkedin.com (rys. 65) na stronie tineye.com. Znajduje ona to samo zdjęcie, na forum jednej z płatnych bibliotek Javascript. (rys. 66)

Można się tam dowiedzieć, że nick tej osoby to Louissi. Wyszukanie na newgrounds.com (rys. 67) oraz armorgames.com (rys. 68) znajduje nam tego użytkownika i potwierdza fakt, że jest lub był on pracownikiem armorgames.com. Użytkownik jest też dostępny na x.com. (rys. 69) Strona osobista nie jest już aktywna.

Jego prawdziwe imię jest widoczne po włączeniu jednej z jego gier flash. Nazywa się on Louis-Simon Menard. (rys. 70) Po imieniu można znaleźć jego nowy profil na linkedin.com, z którego dowiadujemy się, że aktualnie pracuje nad unity, a firmę Armor Games opuścił dawno temu. (rys. 71)

The screenshot shows a user profile page for 'Louissi' on a forum. The profile picture is a blue circle with a white letter 'L'. The name 'Louissi' is displayed above 'Members'. Below the profile picture, there are three status indicators: 'Posts' (2), 'Joined' (September 22, 2010), and 'Last visited' (September 22, 2010). A green horizontal bar highlights 'Louissi's Profile'. To the right, a link says 'See their activity'. Below this, a section for 'Louissi's Achievements' shows a box containing the number '0' and the word 'Reputation'. Two posts by 'Louissi' are listed. The first post, dated September 22, 2010, has 8 replies. It asks for help with a selection box not showing up in TransformManager (Flash) and includes an email link. The second post, also from September 22, 2010, has 8 replies. It discusses buying TransformManager and its usage in a map editor, mentioning a component for creating and managing objects.

Louissi
Members

Posts Joined Last visited

2 September 22, 2010 September 22, 2010

Louissi's Profile See their activity

Louissi's Achievements

0 Reputation

handles and selection box not showing
Louissi replied to Louissi's topic in TransformManager (Flash)
I sent you a PM, I need your email.
September 22, 2010 8 replies

handles and selection box not showing
Louissi posted a topic in TransformManager (Flash)
Hi. I just bought TransformManager. I am working on a flex project. The project is a map editor. In my map editor, there is a component to create and manage objects. These objects are visual objects. I have an object viewer, that is a simple.as class. This class is loading an external swf, creating a movie clip and...
September 22, 2010 8 replies

Rysunek 66. Forum gasp.com

The screenshot shows a user profile for "Louissi". At the top left is a circular icon containing a stylized white figure wearing a mask. To the right of the icon, the name "Louissi" is displayed in large, bold, white letters. Below the name are two status indicators: "FANS 2K" and "NEWS 80".

Use this email for business inquiries:
louissi@armorgames.com

User Information:

- Age 35, Male
- Programmer
- Cégep du Vieux Montréal
- Montreal, Quebec, Canada
- Joined on 9/27/03

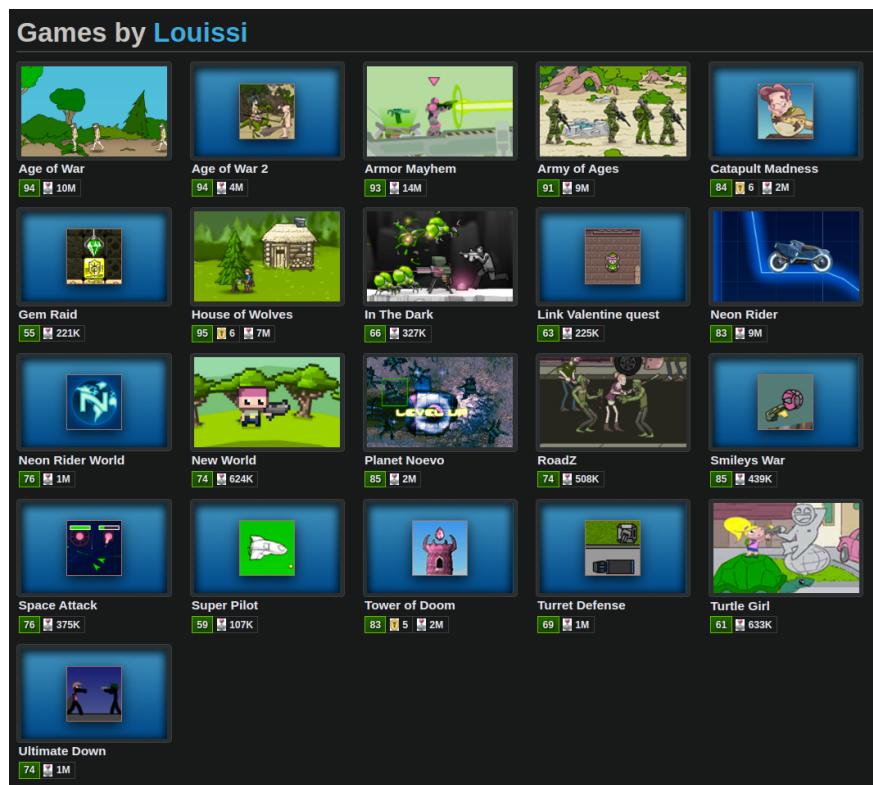
My Blog

Level: 14
Exp Points: 2,030 / 2,180
Exp Rank: 31,123
Vote Power: 5.61 votes

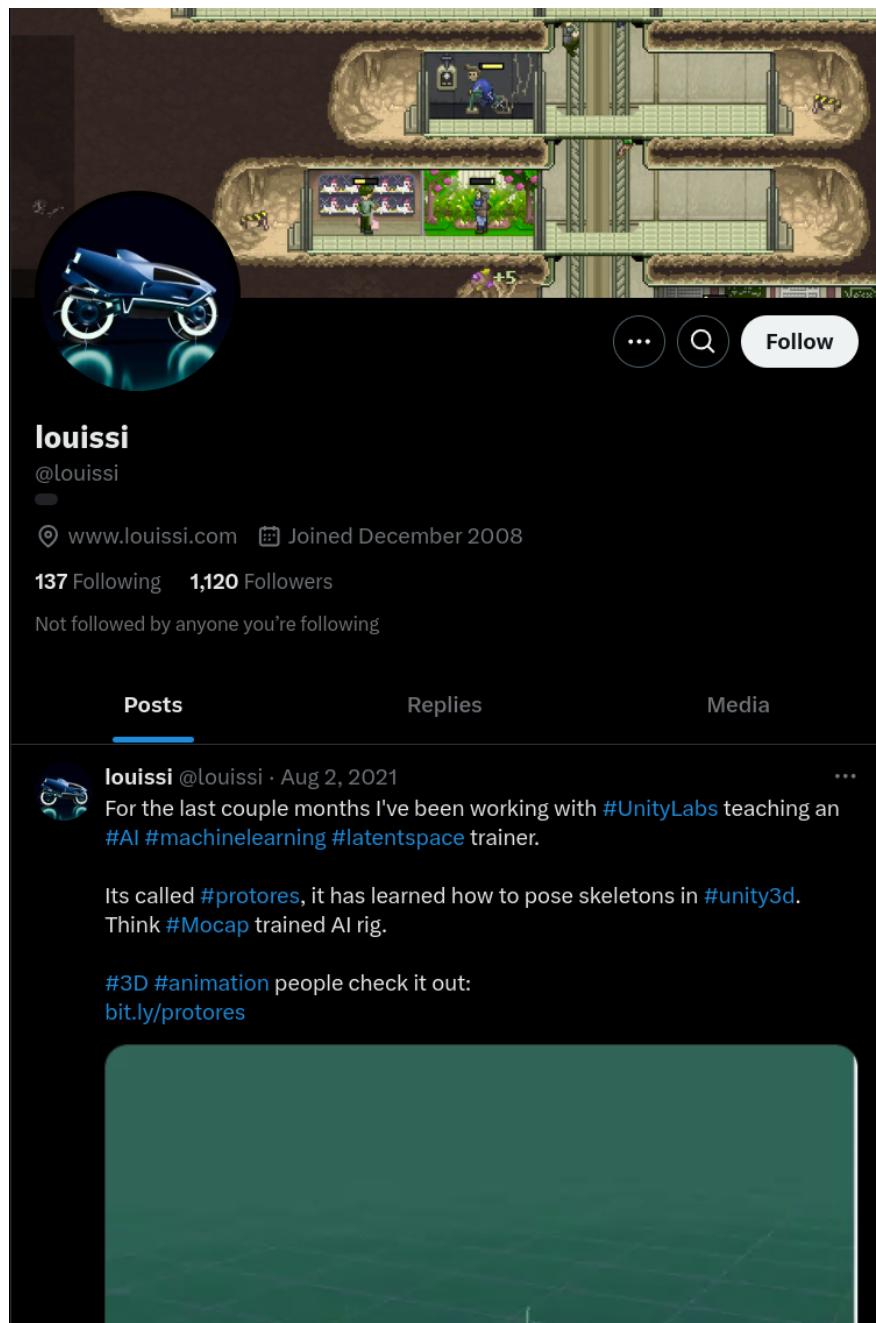
Rank: Safety Patrol
Global Rank: 30,268
Blams: 198
Saves: 123
B/P Bonus: 6%

Whistle: Normal

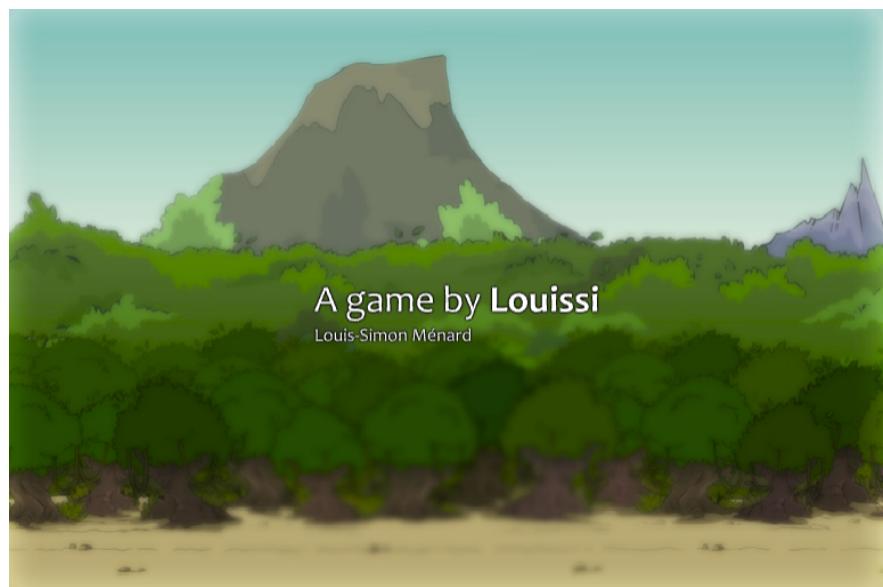
Trophies: 25
Medals: 372
Supporter: 11m 30d
Gear: 6



Rysunek 68. Profil na armorgames.com



Rysunek 69. Profil na stronie x.com



Rysunek 70. Grafika ze stratu gry Age of War 2

Louis-Simon Ménard
Senior Software Developer at Unity Technologies
Montreal, Quebec, Canada · [Contact info](#)
58 connections

[Connect](#) [Message](#) [More](#)

About
Passionate about video games, art and programming. Creative, curious by nature, I have been developing video games for over ten years.
I have experience in management, programming, art, game design and marketing. I have worked with ...[see more](#)

Activity
68 followers
Louis-Simon hasn't posted yet
Recent posts Louis-Simon shares will be displayed here.
[Show all activity →](#)

Enhance your own profile by adding a work experience. [Add experience](#) [×](#)

Experience
Senior Software Developer
Unity Technologies · Permanent Full-time
May 2021 - Present · 3 yrs 8 mos
Montreal, Quebec, Canada
 helped me get this job

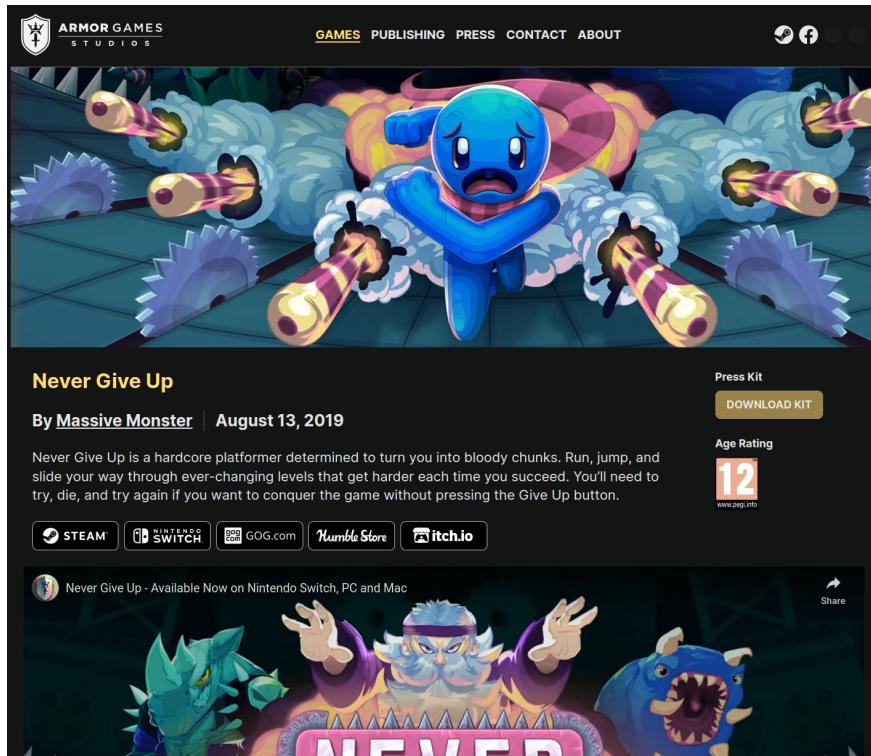
Rysunek 71. Profil Louisa-Simona Menarda na stronie linkedin.com

8.3.2 tasselfoot

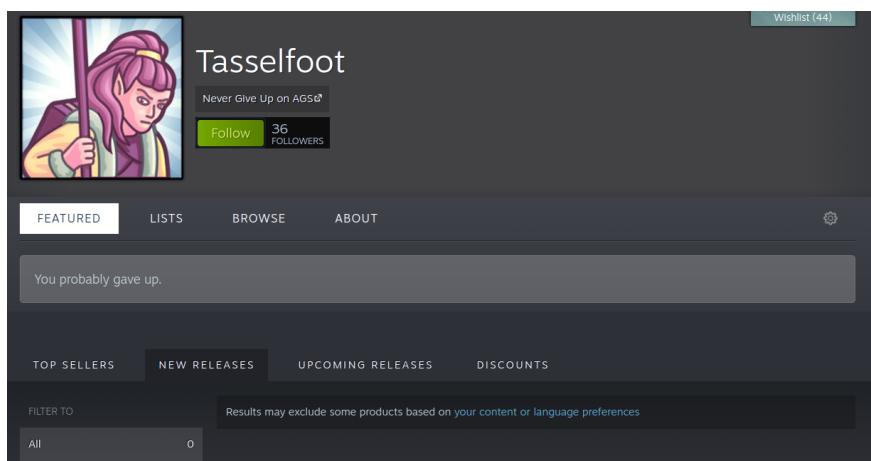


Rysunek 72. Zdjęcie profilowe tasselfoot

Tasselfoot jest aktywnym pracownikiem Armor Games. (rys. 73) Zajmuje się przedewszystkim zarządzaniem prawami autorskimi oraz kupowaniem nowych gier dla firmy. Jest odpowiedzialny za jedną z gier Armor Games Studio zwaną "Never Give Up". (rys. 74) Posiada on też swoją stronę osobistą <https://tasselfoot.com/>, jednak nie jest aktywna. Był on kiedyś bardzo znaną osobą w środowisku gier flash, tworzył filmy z poradnikami dostępne dalej na jego kanale youtube. Jest też współwłaścicielem strony flashflashrevolution.com. (rys. 75) Jest aktywny na x.com.



Rysunek 73. Never give up na stronie Armor Games Studio



Rysunek 74. Strona dewelopera na steam



Rysunek 75. witryna flashflash revolution

8.4 Emaile strony

Używając programu the Harvester możliwe jest znalezienie 3 emaili z głównej witryny strony, ads@armorgames.com, help@armorgames.com oraz support@armorgames.com. Wszystkie z nich to są oficjalne emaile do kontaktu z pracownikami Armor Games.

```

1 [*] Emails found: 3
2 -----
3 ads@armorgames.com
4 help@armorgames.com
5 support@armorgames.com
6
7 [*] LinkedIn Links found: 0
8 -----
```

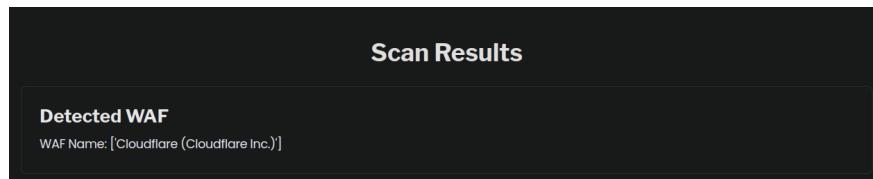
8.5 Podsumowanie

Armor Games posiada od 11 do 50 pracowników. tylko część z nich jest widoczna dla wszystkich, lecz bez imion. Można zidentyfikować aktualnego CEO, założyciela, osobę zajmującą się prawami autorskimi oraz jednego z byłych deweloperów. Osoby te są aktywne na mediach społecznościowych. Główna witryna zawiera 3 emaile. Strona posiada trzy oficjalne maile.

9 Bezpieczeństwo

9.1 Zabezpieczenia

Strona wykorzystuje Web Application Firewall (WAF) stworzony przez Cloudflare.



Rysunek 76. Wynik skanu WAF ze strony safesecureaudit.com

9.2 Skan podatności

Skan podatności wykonany przez stronę pentest-tools.com, sugeruje iż, strona armorgames.com posiada przestarzałą wersje jquery, 1.8.23 oraz Moment 2.9.0. (rys. 77, rys. 78, rys. 79)



Rysunek 77. Graf z pentest-tools.com

Możliwe jest potwierdzenie tego w konsoli naszej przeglądarki, po wejściu na armorgames.com, iż strona używa JQuery w wersji 1.8.23. (rys. 80) Jest to ważne, ponieważ wersja ta jest podatna na ataki typu XSS. Podatności dla tej wersji potwierdza firma Snyk. (rys. 81)

Z raportów wynika, że armorgames.com jest podatne na ataki typu Cross-site scripting, w których złośliwy kod jest wstrzykiwany do aplikacji internetowej w celu wykonania go w przeglądarce ofiary. Celem takiego ataku jest wykonanie nieautoryzowanego działania na stronie internetowej, co może prowadzić do kradzieży danych użytkownika, przejęcia sesji, modyfikowania treści strony lub infekowania komputerów złośliwym oprogramowaniem. Oznacza to, że aktualnie korzystanie ze strony armorgames.com może nie być bezpieczne dla użytkowników.

Kolejnym możliwym problemem strony wykrytym przez pentest-tools.com jest moment.2.9.0. Podatności tej wersji są potwierdzane przez firmę Snyk. (rys. 82)

Wersja ta jest podatna na ataki typu DDOS oraz path traversal, co może prowadzić do nieautoryzowanego dostępu do systemów, potencjalnie pozwalając na dostęp do poufnych danych lub przejęcie kontroli nad zasobami serwera.


```
>> console.log('jQuery version:', jQuery.fn.jquery);
jQuery version: 1.8.2
← undefined
```

Rysunek 80. Sprawdzenie wersji w konsoli

The screenshot shows a report from the Snyk Vulnerability Database for the jquery package at version 1.8.2. The page title is "jquery@1.8.2 vulnerabilities". It is described as a "JavaScript library for DOM operations". A section titled "Direct Vulnerabilities" lists known vulnerabilities. A "How to fix?" section provides instructions and a "Fix for free" button. A detailed table entry for a Cross-site Scripting (XSS) vulnerability is shown, including the vulnerability description, affected versions, and mitigation steps.

Vulnerability	Vulnerable Version
M Cross-site Scripting (XSS)	<1.9.1
<p>jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.</p> <p>Affected versions of this package are vulnerable to Cross-site Scripting (XSS). <code>load()</code> fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e; "</script >" which results in the enclosed script logic to be executed. This can lead to Cross-site Scripting attacks when an attacker has control of the enclosed script.</p> <p>How to fix Cross-site Scripting (XSS)?</p> <p>Upgrade jquery to version 1.9.1 or higher.</p>	

Rysunek 81. Raport firmy Snyk dla jQuery 1.8.2

Snyk Vulnerability Database / npm / moment / moment@2.9.0

moment@2.9.0 vulnerabilities

Parse, validate, manipulate, and display dates

Direct Vulnerabilities

Known vulnerabilities in the moment package. This does not include vulnerabilities belonging to this package's dependencies.

How to fix?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

Vulnerability	Vulnerable Version
H Directory Traversal moment is a lightweight JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of this package are vulnerable to Directory Traversal when a user provides a locale string which is directly used to switch moment locale. How to fix Directory Traversal? Upgrade moment to version 2.29.2 or higher.	<2.29.2

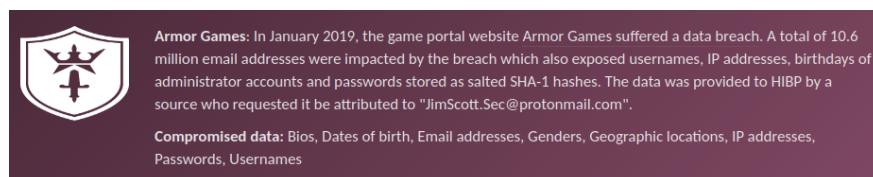
Rysunek 82. Raport firmy Snyk dla Moment 2.9.0

9.3 Wyciek danych

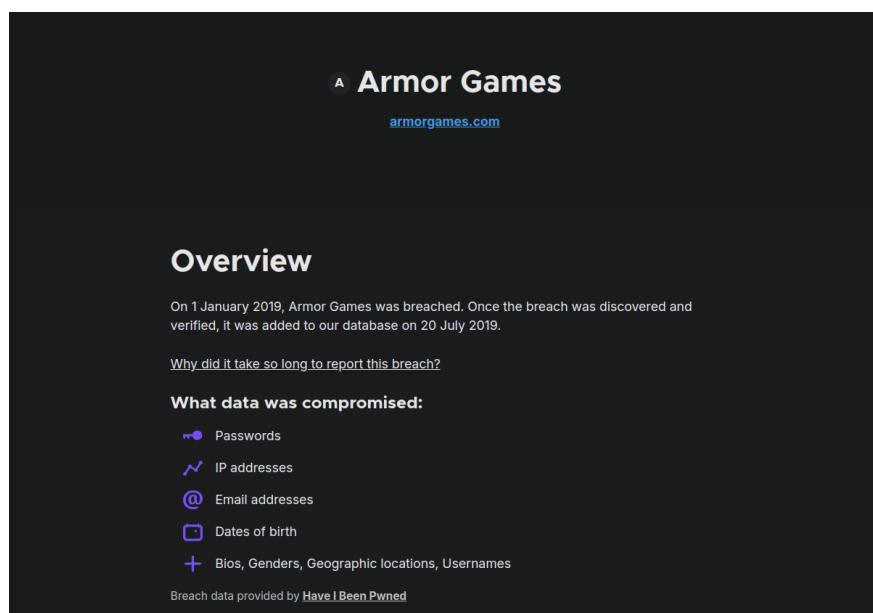
Strona armorgames.com miała wyciek danych użytkowników 3 Marca 2019 roku. Dane były sprzedawane w sklepie darkweb nazywanym Dream Market. Potwierdza to wiele źródeł, takich jak haveibeenpwned.com (rys. 83), Mozilla Monitor (rys. 84) oraz Techraptor (rys. 85). W ramach ataku zostały ujawnione:

- Profile publiczne
- Dane logowania
- Nazwy użytkowników
- Adresy ip
- Zhashowane hasła
- Daty urodzenia administratorów
- Informacje o sposobie ochrony haseł, razem z solą

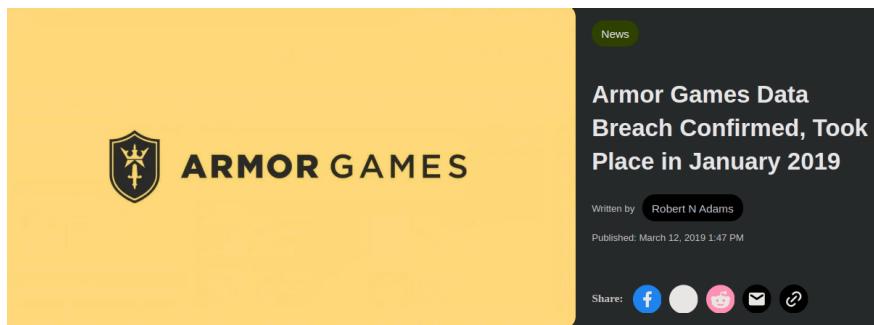
Można sprawdzić, czy dany adres email wyciekł poprzez podawanie go na stronie haveibee npwned.com.



Rysunek 83. Potwierdzenie wycieku ze strony haveibeenpwned.com



Rysunek 84. Potwierdzenie wycieku danych z Mozilla Monitor



Rysunek 85. Potwierdzenie wycieku ze strony Techraptor

9.4 Podsumowanie

Strona armorgames.com wykorzystuje przestarzałą wersję jQuery 1.8.23 oraz Moment.js 2.9.0, które narażają stronę na ataki typu XSS, DDOS i path traversal, co zostało potwierdzone przez skan wykonany przez Pentest-tools.com oraz raporty firmy Snyk. W wyniku tych podatności, złośliwy kod może zostać wstrzyknięty do aplikacji, co prowadzi do zagrożenia kradzieżą danych użytkowników i przejęciem kontroli nad serwerem. Dodatkowo, w marcu 2019 roku miało miejsce naruszenie danych użytkowników armorgames.com, w wyniku którego wyciekły informacje takie jak dane logowania, adresy IP i hasła. Potwierdzenie tego wycieku można znaleźć na stronach HaveIBeenPwned, Mozilla Monitor i Techraptor.

10 Stosowane urządzenia sieciowe

Analiza wyników z censys.io (rys. 86), shodan.io (rys. 87) oraz intelx.io (rys. 88) nie pozwala na znalezienie danych o urządzeniach sieciowych.

The screenshot shows the Censys.io interface for the IP address 104.20.129.21. The page header indicates the data is from Jan 03, 2025, at 2:37pm UTC. Below the header, there are four navigation links: Summary (underlined), History, WHOIS, and Explore. The main content area is titled "Basic Information" and contains the following details:

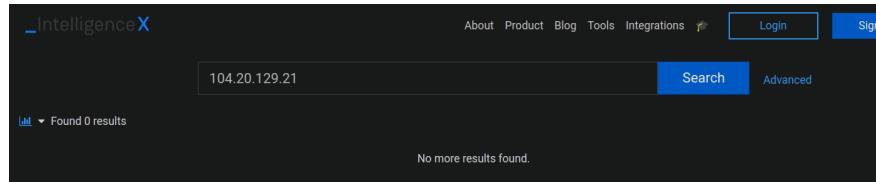
- Forward DNS:** presskits.armorgames.com, 059879e5-b2e8-4f58-aa46-95f69d92aa34.random.13noon.com, developers.armorgames.com, stage.armorgames.com, armorgames.com, ...
- Routing:** 104.20.128.0/20 via CLOUDFLARENET, US (AS13335)
- Services (13):** 80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

Rysunek 86. Wynik scanu censys.io

The screenshot shows the Shodan.io interface for the IP address 104.20.129.21. The page header indicates the data is from Jan 03, 2025, at 2:37pm UTC. Below the header, there are four navigation links: Summary (underlined), History, WHOIS, and Explore. The main content area is titled "Basic Information" and contains the following details:

- Forward DNS:** presskits.armorgames.com, 059879e5-b2e8-4f58-aa46-95f69d92aa34.random.13noon.com, developers.armorgames.com, stage.armorgames.com, armorgames.com, ...
- Routing:** 104.20.128.0/20 via CLOUDFLARENET, US (AS13335)
- Services (13):** 80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

Rysunek 87. Wynik skanu shodan.io



Rysunek 88. Wynik Intelx.io

10.1 Podsumowanie

Nie jest możliwym znalezienie informacji o urządzeniach sieciowych używanych przez Armor Games.

11 Inne rodzaje uzyskanych danych

11.1 Rekordy A

Domena wykorzystuje także trzy A rekordy, także należące do Cloudflare (rys. 89, 90)

- 104.67.2.10
- 104.20.128.21
- 104.20.129.21

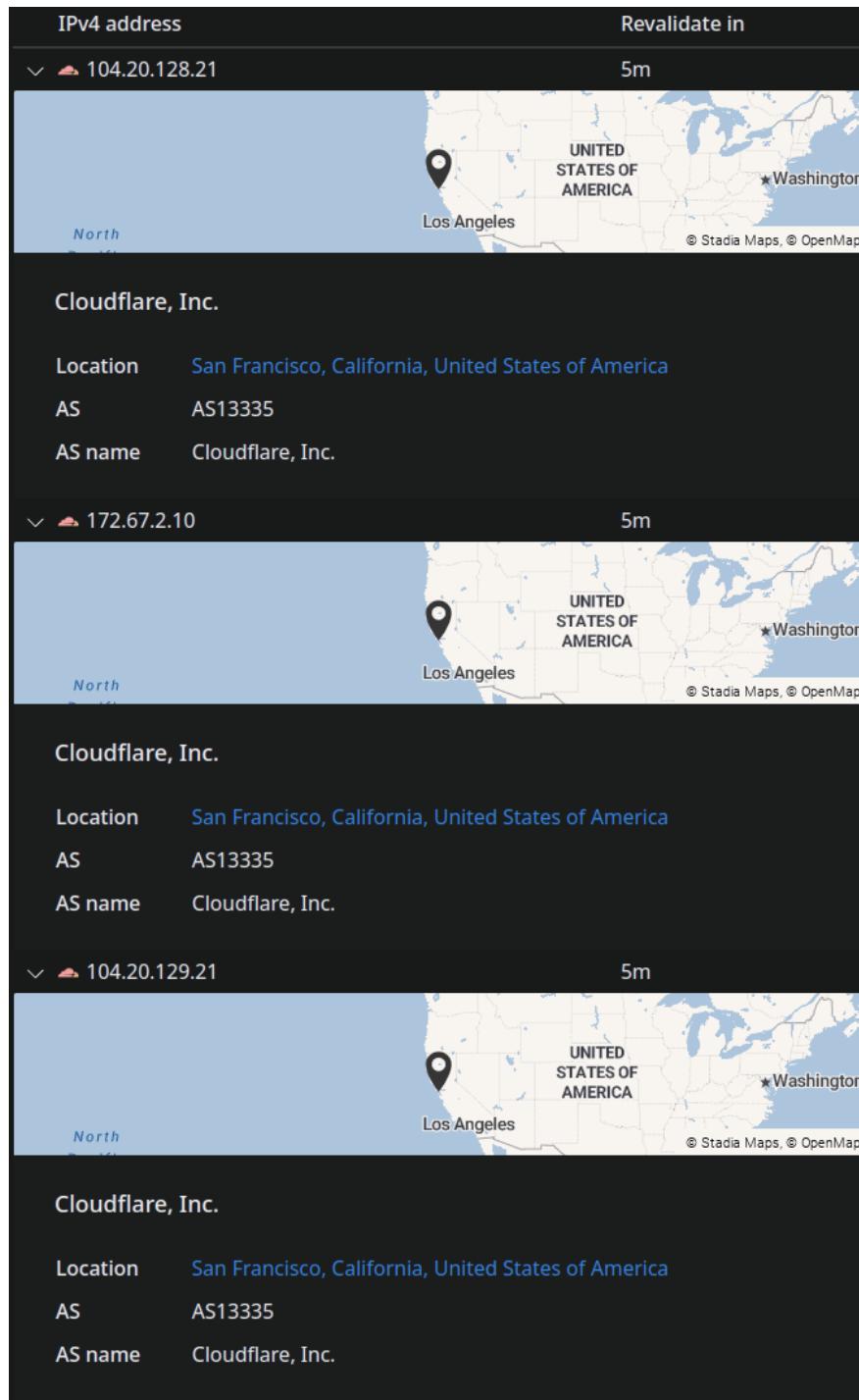
Wszystkie te serwery znajdują się w Los Angeles, USA i mają Time To Live równy 5 minut. (rys. 91, 92, 93, 94). Oznacza to, że osoby które będą chciały mieć dostęp do gier dostępnych na witrynie armorgames.com, będą musiały mieć dostęp do serwerów w Cloudflare w USA, co w niektórych krajach może być nie możliwe.

Type	Domain Name	IP Address	TTL
A	armorgames.com	172.67.2.10 Cloudflare, Inc. (AS13335)	5 min
A	armorgames.com	104.20.128.21 Cloudflare, Inc. (AS13335)	5 min
A	armorgames.com	104.20.129.21 Cloudflare, Inc. (AS13335)	5 min

Rysunek 89. Lista serwerów DNS ze strony mxtoolbox.com

A records	
IPv4 address	Revalidate in
> 104.20.128.21	5m
> 172.67.2.10	5m
> 104.20.129.21	5m

Rysunek 90. Lista serwerów DNS ze strony nslookup.io



Rysunek 91. Lokalizacja serwerów DNS ze strony nslookup.io

104.20.128.21

Hide this IP Address

Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from	IP2Location	Product: DB6, 2024-11-1
 IP ADDRESS: 104.20.128.21	 ISP: CloudFlare Inc.	
 COUNTRY: United States 	 ORGANIZATION: Not available	
 REGION: California	 LATITUDE: 37.7757	
 CITY: San Francisco	 LONGITUDE: -122.3952	

Incorrect location? Contact IP2Location [view map](#)

Geolocation data from	ipinfo.io	Product: API, real-time
 IP ADDRESS: 104.20.128.21	 ISP: Not available	
 COUNTRY: United States 	 ORGANIZATION: AS13335 Cloudflare, Inc.	
 REGION: California	 LATITUDE: 37.7621	
 CITY: San Francisco	 LONGITUDE: -122.3971	

Incorrect location? Contact ipinfo.io [view map](#)

Rysunek 92. Lokalizacja serwera 104.20.128.21 ze strony iplocation.net

172.67.2.10

 Hide this IP Address

Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from	IP2Location	Product: DB6, 2024-11-1
 IP ADDRESS: 172.67.2.10	 ISP: CloudFlare Inc.	
 COUNTRY: United States 	 ORGANIZATION: Not available	
 REGION: California	 LATITUDE: 37.7757	
 CITY: San Francisco	 LONGITUDE: -122.3952	
Incorrect location? Contact IP2Location		 view map
Geolocation data from	ipinfo.io	Product: API, real-time
 IP ADDRESS: 172.67.2.10	 ISP: Not available	
 COUNTRY: United States 	 ORGANIZATION: AS13335 Cloudflare, Inc.	
 REGION: California	 LATITUDE: 37.7621	
 CITY: San Francisco	 LONGITUDE: -122.3971	
Incorrect location? Contact ipinfo.io		 view map

Rysunek 93. Lokalizacja serwera 172.67.2.10 ze strony iplocation.net

104.20.129.21

 Hide this IP Address

Here are the results from a few Geolocation providers. Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from IP2Location Product: DB6, 2024-11-1

 IP ADDRESS: 104.20.129.21	 ISP: CloudFlare Inc.
 COUNTRY: United States 	 ORGANIZATION: Not available
 REGION: California	 LATITUDE: 37.7757
 CITY: San Francisco	 LONGITUDE: -122.3952

Incorrect location? Contact IP2Location  view map

Geolocation data from ipinfo.io Product: API, real-time

 IP ADDRESS: 104.20.129.21	 ISP: Not available
 COUNTRY: United States 	 ORGANIZATION: AS13335 Cloudflare, Inc.
 REGION: California	 LATITUDE: 37.7621
 CITY: San Francisco	 LONGITUDE: -122.3971

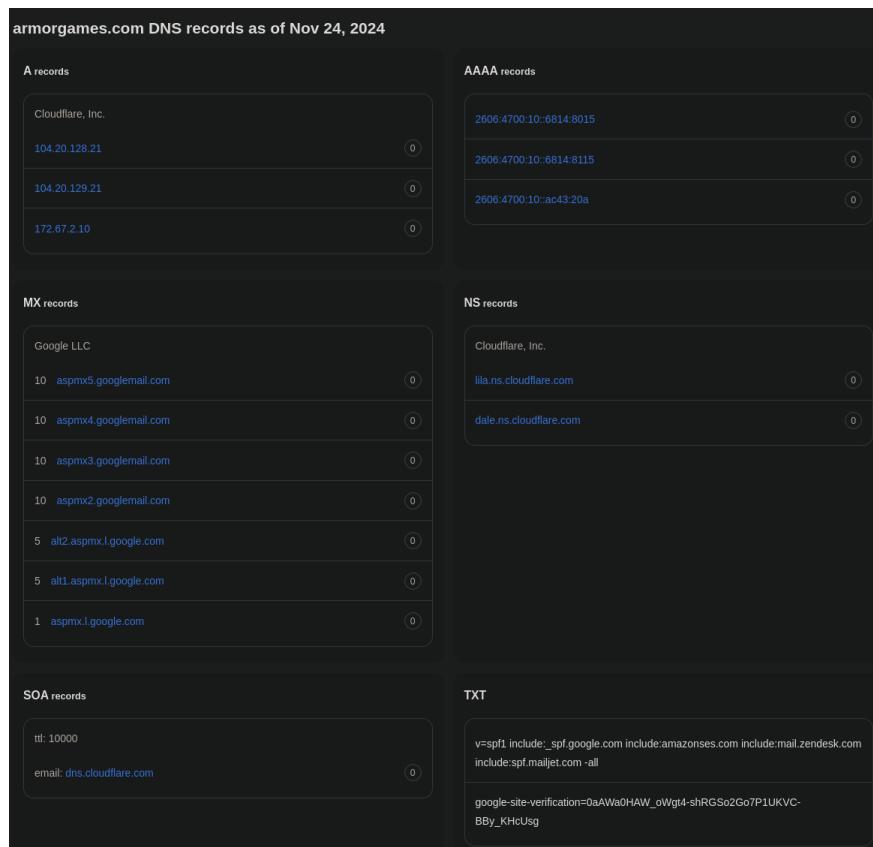
Incorrect location? Contact ipinfo.io  view map

Rysunek 94. Lokalizacja serwera 104.20.129.21 ze strony iplocation.net

11.2 Rekordy AAAA

Rekordy AAAA wskazują na adresy IPv6 przypisane do domeny (rys. 95):

- 1 2606:4700:10:6814:8015
- 2 2606:4700:10:6814:8115
- 3 2606:4700:10:ac43:20a



Rysunek 95. Lista rekordów DNS uzyskane z security trails

11.3 Rekordy Mail Exchange

Rekordy MX dla domeny armorgames.com wskazują serwery odpowiedzialne za obsługę poczty elektronicznej (kod 8). W tym przypadku poczta jest obsługiwana przez serwery Google. Wyniki potwierdza strona (dnsdumpster.com. (Kod 8)

- 1 aspmx1.google.com (priorytet 1)
- 2 aspmx2.google.com (priorytet 10)
- 3 aspmx3.google.com (priorytet 10)
- 4 aspmx4.google.com (priorytet 10)
- 5 aspmx5.google.com (priorytet 5)
- 6 alt1.aspmx.l.google.com (priorytet 5)

7 | alt2.aspmx.l.google.com (priorytet 5)

Kod 8: Rekordy MX

```
MX Records ** This is where email for the domain goes...
10 aspmx5.googlemail.com.          142.250.153.27      GOOGLE
# 10 aspmx5.googlemail.com.          142.250.153.27      GOOGLE
# 1 aspmx.l.google.com.             142.251.179.26     GOOGLE
# 1 aspmx.l.google.com.             142.251.179.26     GOOGLE
# 5 alt1.aspmx.l.google.com.        209.85.202.26      GOOGLE
# 5 alt1.aspmx.l.google.com.        209.85.202.26      GOOGLE
# 5 alt2.aspmx.l.google.com.        64.233.184.26      GOOGLE
# 5 alt2.aspmx.l.google.com.        64.233.184.26      GOOGLE
# 10 aspmx2.googlemail.com.         209.85.202.27      GOOGLE
# 10 aspmx2.googlemail.com.         209.85.202.27      GOOGLE
# 10 aspmx3.googlemail.com.         64.233.184.27      GOOGLE
# 10 aspmx3.googlemail.com.         64.233.184.27      GOOGLE
# 10 aspmx4.googlemail.com.         142.250.27.27       GOOGLE
# 10 aspmx4.googlemail.com.         142.250.27.27       GOOGLE

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations
# 10 aspmx4.googlemail.com.         142.250.27.27       GOOGLE
```

}[#fig:dnsDumpMX]

11.4 Rekordy Start of Authority

Rekord SOA dla armorgames.com zawiera informacje o strefie DNS (rys. 95) w tym: TTL: 10000 sekund (czas przechowywania rekordu w pamięci podręcznej), Email: dns.cloudflare.com (adres e-mail administratora strefy DNS).



Rysunek 96. Struktura subdomen oraz serwerów do nich przypisanych uzyskana z dnsdumpster

11.5 Siedziba

Siedziba firmy znajduje się na 16808 Armstrong Avenue Suite #205. w Irvine, California, co wiemy z ich rejestracji firmyt w stanie Kalifornia. (rys. 2) Budynek tam się znajdujący to centrum biznesowe, które współdzielą z wieloma innymi firmami. (rys. 97) Na stronie Premier Work Spaces można zobaczyć wygląd całej siedziby. (rys. 99) Możliwe jest także wynajęcie pomieszczenia oraz zamówić oprowadzenie po placówce. (rys. 98)



Rysunek 97. Budynek w którym znajduje się Armor Games

The screenshot shows a dark-themed website section titled "Our workspaces". It features three cards:

- Virtual Offices**: Shows a small image of a modern office interior, "Virtual Offices" text, "from \$125/month" price, and a "Buy Now" button.
- Memberships**: Shows a small image of an office with large windows, "Memberships" text, "Monthly Memberships" subtext, "from \$29/month" price, and a "Buy Now" button.
- Meeting Rooms**: Shows a small image of a conference room with a long table, "Meeting Rooms" text, "Meeting Rooms" subtext, "from \$85/hour" price, and a "Reserve Now" button.

Rysunek 98. Oferta Premier Work Spaces



Rysunek 99. Fragment budynku Premier Work Spaces w Irvine

11.6 Reverse whois

Z reverse whois uzyskanego ze stron reversewhois.io (rys. 100) oraz viewedns.info (rys. 101) wynika, że firma Armor Games wykupiła wiele innych domen powiązanych z ich grami, bądź zbliżonych do ich nazwie.

Atkualnie wszystkie strony, które w nazwie odwołują się do gier tej firmy są nieaktywne, a domeny o nazwach zbliżonych do armorgames.com oraz armorgamesstudio.com przekierowywają na nie. (rys. 102)

Dla armorgames.com jest to: 1. armor.ag 2. armorgame.com 3. armorgames.net

Dla armorgamesstudios.com jest to: 1. armorgamestudio.com 2. armorgamestudios.com

Jednym wyjątkiem jest guidesandcheats.com, który został wykupiony przez nieznaną osobę, przekierowywającą na sponsorowane strony.

11.7 Podsumowanie

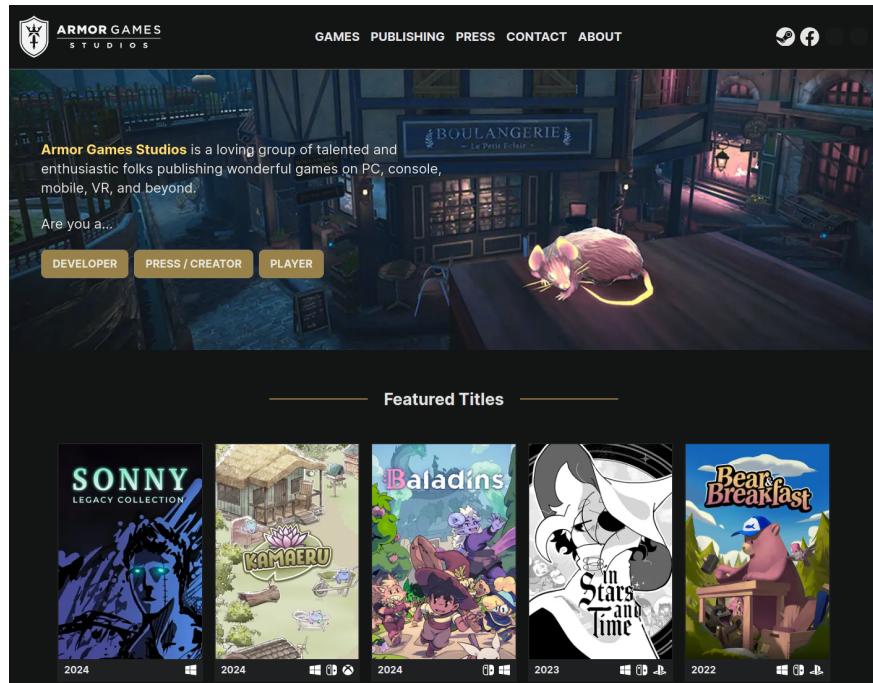
Firma Armor Games wynajmuje lokal w Irvine, California. Posiada ona wszystkie domeny o zbliżonych nazwach, w celu ochrony użytkowników przed literówkami. Jedyna domena, którą prawdopodobnie kiedyś posiadali i została przejęta to guidesandcheats.com, która aktualnie serwuje reklamy.

#	Domain Name	Created Date	Registrar
1	armor.ag	2010-02-25	GODADDY.COM, LLC
2	armorblog.com	2007-10-25	EVERYONES INTERNET, LTD. DBA SOFTLAYER
3	armorgame.com	2005-09-29	ENOM, INC.
4	armorgames.com	2005-09-29	EVERYONES INTERNET, LTD. DBA SOFTLAYER
5	armorgames.net	2005-09-29	ENOM, INC.
6	armorgames.xxx	2011-12-07	ENOM, INC.
7	armorgamesstudio.com	2016-05-23	ENOM, INC.
8	armorgamesstudios.com	2016-05-23	ENOM, INC.
9	armorgamestudio.com	2016-05-23	ENOM, INC.
10	armorgamestudios.com	2016-05-23	ENOM, INC.
11	armourgames.xxx	2011-12-07	ENOM, INC.
12	cheatsandguides.com	2011-10-27	ENOM, INC.
13	chuckthesheep.com	2011-09-28	ENOM, INC.
14	gemhuntersgame.com	2016-10-20	ENOM, INC.
15	guidesandcheats.com	2011-10-25	ENOM, INC.
16	just2play.com	2006-04-25	ENOM, INC.
17	kingskollege.com	2015-08-27	ENOM, INC.
18	lastcastlegame.com	2011-10-19	ENOM, INC.
19	monsterbark.com	2011-10-26	ENOM, INC.
20	onlylevel.com	2011-12-20	ENOM, INC.
21	phagewarslive.com	2011-09-28	ENOM, INC.
22	play-flight.com	2012-07-11	ENOM, INC.
23	play-house-of-shadows.com	2012-10-24	ENOM, INC.
24	scarletstranger.com	2011-12-20	ENOM, INC.
25	shoresiege.com	2011-10-19	ENOM, INC.
26	starlostgame.com	2011-12-20	ENOM, INC.
27	tapthetower.com	2016-10-20	ENOM, INC.
28	vote4slingbaby.com	2011-12-20	ENOM, INC.
29	voteforslingbaby.com	2011-12-20	ENOM, INC.

Rysunek 100. Reverse whois uzyskany z reversewhois.io

Domain Name	Creation Date	Registrar
armor.ag	2010-02-25	GODADDY.COM, LLC
armorblob.com	2007-10-25	EVERYONES INTERNET, LTD. DBA SOFTLAYER
armorgame.com	2005-09-29	ENOM, INC.
armorgames.com	2005-09-29	EVERYONES INTERNET, LTD. DBA SOFTLAYER
armorgames.net	2005-09-29	ENOM, INC.
armorgames.xxx	2011-12-07	ENOM, INC.
armorgamesstudio.com	2016-05-23	ENOM, INC.
armorgamesstudios.com	2016-05-23	ENOM, INC.
armorgamestudio.com	2016-05-23	ENOM, INC.
armorgamestudios.com	2016-05-23	ENOM, INC.
armourgames.xxx	2011-12-07	ENOM, INC.
cheatsandguides.com	2011-10-27	ENOM, INC.
chuckthesheep.com	2011-09-28	ENOM, INC.
gemhuntersgame.com	2016-10-20	ENOM, INC.
guidesandcheats.com	2011-10-25	ENOM, INC.
just2play.com	2006-04-25	ENOM, INC.
kingskollege.com	2015-08-27	ENOM, INC.
lastcastlegame.com	2011-10-19	ENOM, INC.
monsterbark.com	2011-10-26	ENOM, INC.
onlylevel.com	2011-12-20	ENOM, INC.
phagewarslive.com	2011-09-28	ENOM, INC.
play-flight.com	2012-07-11	ENOM, INC.
play-house-of-shadows.com	2012-10-24	ENOM, INC.
scarletstranger.com	2011-12-20	ENOM, INC.
shoresiege.com	2011-10-19	ENOM, INC.
starlostgame.com	2011-12-20	ENOM, INC.
tapthetower.com	2016-10-20	ENOM, INC.
vote4slingbaby.com	2011-12-20	ENOM, INC.
voteforslingbaby.com	2011-12-20	ENOM, INC.

Rysunek 101. Reverse whois uzyskany z viewedns.info



Rysunek 102. Witryna armorgamesstudios.com

12 Wnioski ogólne

Armorgames.com jest platformą z grami flash wykorzystującą infrastrukturę Amazon Web Services oraz Cloudflare do serwowania treści swoim użytkownikom. Wszyskie gry są emulowane używając Ruffle, emulatora stworzonego przez Armor Games.

Strona była kiedyś jedną z najpopularniejszych w swojej kategorii i przynosiło jej to ogromną oglądalność. W szczytowym momencie było to około 2.5 miliona użytkowników. Teraz jednak dziennie jest odwiedzana tylko przez 150 tysięcy osób. Cała monetyzacja tego ruchu opiera się na reklamach, serwowanych poprzez Double Click oraz Ads.txt.

Firma Armor Games stara się w związku z tym dywersyfikować swoją ofertę poprzez stworzenie Armor Games Studios, tworzenie gier mobilnych oraz dystrybucji swoich produktów na platformie Steam. Dodatkowo była zmuszona zwolnić kolejne osoby ze swojej firmy w roku 2023. W związku z tym, nie jest to najlepszy okres dla tej firmy, która raczej chyli się ku upadkowi.