



A G H

Analiza informacji umieszczanych w mediach o ataku na Colonial Pipeline

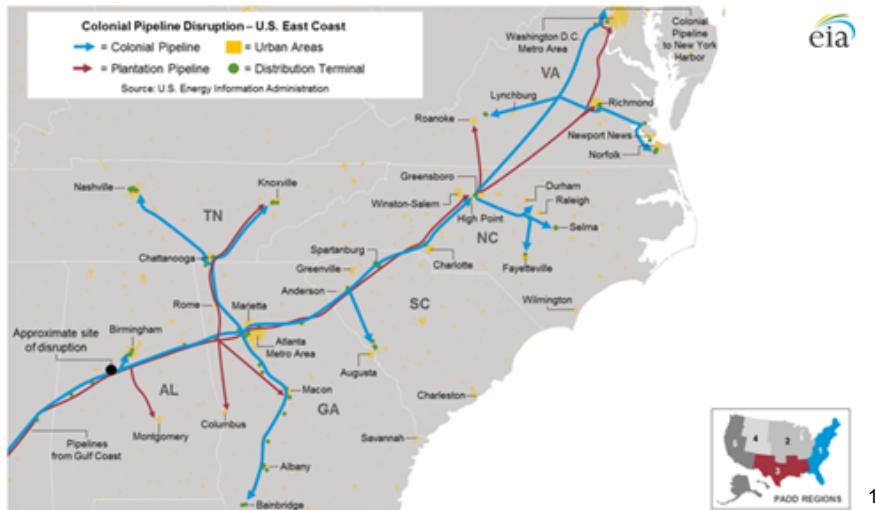
Klaudia Kiliańska
Aniela C.

Spis treści

Czym jest Colonial Pipeline?.....	2
Powstanie i rozwój.....	2
1. Pomysł:.....	2
2. Budowa:.....	2
3. Ukończenie i rozszerzenia:.....	3
4. Specyfikacja i działanie.....	3
Colonial Pipeline jako infrastruktura krytyczna.....	3
Atak na Colonial Pipeline.....	3
Oś czasu: Atak na Colonial Pipeline.....	4
Czym jest grupa przestępca DarkSide?.....	5
Dlaczego DarkSide zażądało kryptowalut?.....	5
Narracja medialna.....	6
Gazety prawicowe:.....	6
Gazety lewicowe:.....	6
Reakcje w social media:.....	7
1. X (Twitter).....	7
Przykład 1:.....	7
Przykład 2:.....	11
Przykład 3:.....	12
Przykład 4:.....	15
2. Facebook.....	16
Przykład 1:.....	16
Odpowiedź 1:.....	17
Odpowiedzi 2 i 3:.....	17
Analiza narzędzi użytych podczas projektu.....	19
Narzędzia sprawdzające wiarygodność stron.....	19
NetCraft.....	19
WhoIS.....	19
ip-tracker.org.....	20
Wayback Machine.....	21
Urlscan.io.....	22
Wyszukiwarki.....	22
Google.com.....	22
Google dorking.....	23
Wyszukiwarka na portalu X.com.....	24
Wtyczki i rozszerzenia.....	25
Gotanda.....	25
Wappalyzer.....	26
InVid.....	26
UBlock.....	27
NoScript.....	28
PrivacyBadger.....	28

Czym jest Colonial Pipeline?

Colonial Pipeline to największy rurociąg przesyłający paliwa, takie jak benzyna, olej napędowy i gaz lotniczy w Stanach Zjednoczonych. Rozciąga się on od Teksasu aż do Nowego Jorku i odgrywa kluczową rolę w dystrybucji paliw na Wschodnim Wybrzeżu USA.



Powstanie i rozwój

1. Pomysł:

Ideą budowy Colonial Pipeline było zmniejszenie zależności od transportu morskiego dla dostaw paliw, co miało znaczenie w kontekście rosnącego zapotrzebowania na paliwo oraz kwestii bezpieczeństwa narodowego. Rurociąg miał na celu zapewnienie niezawodnego i bezpiecznego sposobu dostarczania paliw z rafinerii w Zatoce Meksykańskiej do gęsto zaludnionych obszarów na Wschodnim Wybrzeżu.

2. Budowa:

Budowa Colonial Pipeline rozpoczęła się w połowie lat 60. XX wieku. Na wczesnych etapach budowy inżynierowie stanęli przed licznymi wyzwaniami, w tym zaprojektowaniem i wdrożeniem systemów zaworów zdolnych do obsługi dużych objętości bez mieszania produktu. Doprowadziło to do opracowania specjalnego systemu hydraulicznego w celu poradzenia sobie z tym problemem.

¹ https://en.wikipedia.org/wiki/Colonial_Pipeline

3. Ukończenie i rozszerzenia:

Pierwsza faza rurociągu została zakończona i oddana do użytku w 1964 roku. Od tego czasu rurociąg był wielokrotnie rozbudowywany i modernizowany, aby sprostać nowym wymaganiom technicznym.

4. Specyfikacja i działanie

- Długość: Colonial Pipeline rozciąga się na długość około 5500 kilometrów i jest jednym z najdłuższych rurociągów naftowych w USA.
- Przepustowość: System może przesyłać dziennie miliony baryłek paliwa, obsługując rynki konsumenckie na Wschodnim Wybrzeżu, które stanowią około 45% całkowitego zużycia paliw w tym regionie.

Colonial Pipeline jako infrastruktura krytyczna

Infrastruktura krytyczna to obiekty, systemy i sieci, które są niezbędne do funkcjonowania społeczeństwa i gospodarki. Obejmuje to elementy takie jak dostawy energii (elektrycznej i paliw), wodociągi, systemy komunikacji, transport, usługi finansowe i zdrowotne. Uszkodzenie lub zakłócenie działania infrastruktury krytycznej może mieć poważne konsekwencje dla bezpieczeństwa narodowego, gospodarki, zdrowia publicznego i bezpieczeństwa.

Colonial Pipeline jest kluczowym elementem infrastruktury krytycznej w USA, ponieważ dostarcza paliwa na dużą część Wschodniego Wybrzeża, co stanowi około 45% zapotrzebowania na paliwo w tym regionie. Jego działanie jest niezbędne dla funkcjonowania różnych sektorów gospodarki, w tym transportu, lotnictwa i codziennego życia obywateli.

Atak na Colonial Pipeline

Atak miał miejsce w maju 2021 roku i był to cyberatak typu ransomware przeprowadzony przez grupę przestępczą znaną jako DarkSide. W wyniku tego ataku, złośliwe oprogramowanie zainfekowało systemy komputerowe firmy, co doprowadziło do czasowego zamknięcia całego rurociągu. To spowodowało znaczne zakłócenia w dostawie paliw na Wschodnim Wybrzeżu oraz wzrost cen paliw. Atakujący zażądali okupu za odblokowanie dostępu do systemów. Firma Colonial Pipeline zdecydowała się zapłacić okup, który wynosił prawie 5 milionów dolarów w kryptowalutach, aby przywrócić funkcjonowanie rurociągu.

Oś czasu: Atak na Colonial Pipeline

6 maja 2021: DarkSide rozpoczyna atak, kradnąc dane, blokując komputery i żądając okupu.

7 maja 2021: Colonial Pipeline płaci okup.

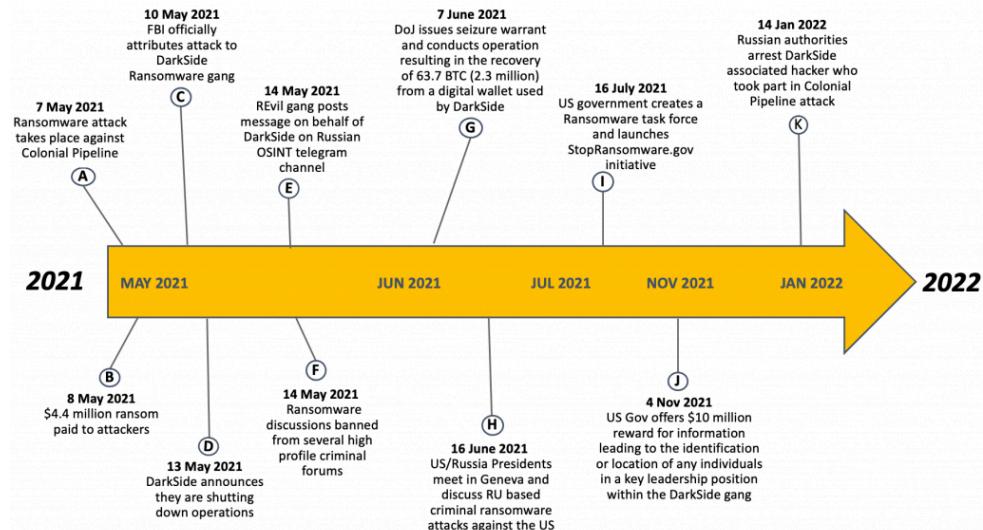
8 maja 2021: Colonial Pipeline publicznie ogłasza atak, a następnie wyłącza serwery i niektóre rurociągi.

9 maja 2021: Colonial Pipeline ogłasza drugi komunikat publiczny, omawiając plany restartu systemu.

10 maja 2021: FBI potwierdza, że atak ransomware DarkSide spowodował incydent, i ogłasza postępy w jego rozwiązaniu.

11 maja 2021: Federalne agencje wydają poradnik opisujący ransomware DarkSide oraz strategie przeciwdziałania i przywracania funkcji Colonial.

12 maja 2021: Colonial Pipeline przywraca funkcje i ogłasza dostawy paliwa po tym, jak ludzie zaczęli „panikować” i masowo kupować benzynę.²



3

² <https://maui.hawaii.edu/wp-content/uploads/2022/07/Scenario-Colonial-Pipeline-Ransomware-Attack.pdf>

³ <https://analyst1.com/wp-content/uploads/2022/11/Figure-A-min-1024x570.png>

Czym jest grupa przestępca DarkSide?

Grupa DarkSide to zespół cyberprzestępców, który zyskał rozgłos po ataku na Colonial Pipeline w maju 2021 roku. DarkSide, uważana za zlokalizowaną w Rosji, działa na modelu Ransomware-as-a-Service (RaaS), gdzie dostarcza oprogramowanie ransomware innym przestępcom do przeprowadzania własnych ataków.

Grupa stosuje szereg zaawansowanych technik do infiltracji i utrzymania dostępu do sieci ofiar, wykorzystując legalne narzędzia do zdalnego zarządzania, rekonesansu i pozyskiwania poświadczzeń, takie jak Mimikatz, oraz skrypty PowerShell do realizacji swoich celów. DarkSide zyskała też reputację za "profesjonalne" podejście do negocjacji z ofiarami, często zaczynając od wysokich żądań okupu, a następnie obniżając je w trakcie negocjacji.⁴ ⁵

Po ataku na Colonial Pipeline DarkSide ogłosiła zakończenie działalności w maju 2021 roku, co eksperci z branży cyberbezpieczeństwa uważają za możliwą taktykę mającą na celu odwrócenie uwagi i możliwość wznowienia działalności pod inną nazwą. Istnieją również doniesienia, że niektórzy członkowie i współpracownicy DarkSide mogli kontynuować działalność pod nową marką, taką jak BlackCat.⁶

Członkowie grupy są dobrze zaznajomieni z infrastrukturą, technologiami bezpieczeństwa i słabościami swoich ofiar, co sugeruje, że wśród nich mogą być byli profesjonalisci z dziedziny bezpieczeństwa IT. Charakterystyczne dla DarkSide jest unikanie ataków na organizacje zlokalizowane w Rosji, co jest częstą praktyką wśród rosyjskojęzycznych grup ransomware. Grupa ta podkreśla również, że jest apolityczna i jej głównym celem jest zarabianie pieniędzy, nie zaś generowanie większych problemów społecznych.

Dlaczego DarkSide zażądało kryptowalut?

Kryptowaluty zapewniają anonimowość, co utrudnia organom ścigania śledzenie transakcji, a brak centralnego regulatora oznacza, że transakcje nie podlegają kontroli rządowej, co sprawia, że są trudniejsze do przechwycenia. Ponadto szybkość transakcji kryptowalutowych pozwala hakerom sprawnie odebrać okup, a łatwość przekazania środków umożliwia im szybkie i anonimowe przyjęcie płatności. Dodatkowo brak możliwości odwrócenia transakcji utrudnia odzyskanie środków.

⁴ <https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/>

⁵ <https://unit42.paloaltonetworks.com/darkside-ransomware/>

⁶ <https://www.independent.co.uk/news/world/americas/darkside-hacker-group-pipeline-ransomware-b1844972.html>

Narracja medialna

Gazety prawicowe:

"The American Spectacle" w swojej relacji na temat ataku na Colonial Pipeline podkreśla potencjalne powiązania hakerskiej grupy DarkSide z rządem Rosji, pomimo braku konkretnych dowodów. Przykłady wcześniejszych cyberataków, takich jak te związane z chińską grupą MSUpdater czy rosyjską GRU, są przywoływane, by sugerować, że rządy przeciwnych krajów mogą ukrywać swoje motywy za działaniami cyberprzestępców. Jednocześnie artykuł przypisuje odpowiedzialność za kryzys energetyczny głównie polityce administracji Bidena, która "atakuje tradycyjne źródła energii i podnosi ceny." Wspomina się także o planowanym projekcie "The Green New Deal", który pojawi się w późniejszej analizie.

Tego typu narracje wykorzystują spekulacje, wybiórcze przedstawianie faktów oraz emocjonalne słownictwo, aby nakierować czytelników na jednoznaczne wnioski, bez pełnej analizy sytuacji.⁷

Gazety lewicowe:

Artykuł z "AlterNet" przedstawia atak na Colonial Pipeline jako kluczowy przykład na uwidocznienie słabości amerykańskiej infrastruktury energetycznej. W narracji podkreśla się, że sektory energetyczne dążą do efektywności kosztem redundancji, co czyni je podatnymi na zakłócenia, jak pokazuje przykład ostatnich ataków i klęsk żywiołowych. Autor wykorzystuje cytaty ekspertów, takich jak Martin Tallett, aby poprzeć swoją krytykę sektora energetycznego, wskazując na historyczne trendy wcięciu kosztów i obniżaniu bezpieczeństwa operacyjnego. W artykule podkreśla się również potrzebę poprawy odporności systemów energetycznych poprzez strategiczne inwestycje w celu zwiększenia pojemności magazynowej i zapewnienia lepszych zabezpieczeń na przyszłość.⁸

⁷ <https://spectator.org/g/colonial-pipeline-cyber-attack/>

⁸ <https://www.alternet.org/2021/05/national-grid-electric>

Reakcje w social media:

1. X (Twitter)

Do znalezienia teorii użyto wyszukiwarki słów kluczowych na X oraz google dorking

Przykład 1:



One of my fav conspiracy theories of the moments ... The Colonial Pipeline wasn't hacked. It was a 'psyop' by the US gov to push Biden infrastructure package, the Green New Deal AND secure funding for the FBI.



[Przetłumacz wpis](#)

Tłumaczenie:

Jedna z moich ulubionych teorii spiskowych w tej chwili... Colonial Pipeline nie zostało zhakowane. To był 'psyop' przeprowadzony przez rząd USA, aby przeforsować pakiet infrastrukturalny Bidena, Green New Deal ORAZ zapewnić finansowanie dla FBI.

Teoria spiskowa przedstawiona w tweecie sugeruje, że cyberatak na Colonial Pipeline był fikcją i stanowił część operacji psychologicznej, co autor tweeta określił jako "psyop" przeprowadzonej przez rząd Stanów Zjednoczonych. Zamiast ataku hakerskiego, całe wydarzenie miało być inscenizacją mającą na celu osiągnięcie trzech głównych celów politycznych:

1. Przeforsowanie pakietu infrastrukturalnego Bidena

Prezydent Joe Biden przedstawił plan dotyczący znaczących inwestycji w infrastrukturę kraju, który obejmował rozwój i modernizację sieci energetycznych, transportu oraz innych kluczowych aspektów gospodarki.

Dlaczego taka teoria powstała?

Dyskusje na temat pakietu infrastrukturalnego Bidena (Bipartisan Infrastructure Deal), o wartości 1.2 biliona dolarów nasiąły się na początku 2021 roku, czyli przed atakiem na Colonial Pipeline. Miesiąc po ataku Biden ogłosił poparcie i zaczął dążyć do formalizacji planów.

Oś czasu:

Czerwiec 2021 – Prezydent Biden ogłosił swoje wsparcie dla projektu Bipartisan Infrastructure Framework

10.08.2021 - Głosowanie w Senacie: Ustawa została zatwierdzona przez Senat. Wynik głosowania to 69 za i 30 przeciw.

Listopad 2021 – Ustawa o Inwestycjach i Zatrudnieniu w Infrastrukturę (Infrastructure Investment and Jobs Act) została przegłosowana przez Kongres i skierowana do prezydenta do podpisu.

5.11.2021 - Głosowanie w Izbie Reprezentantów: Następnie ustawa została przegłosowana przez Izbę Reprezentantów 5 listopada 2021 roku. Wynik głosowania to 228 za i 206 przeciw. Prezydent Joe Biden podpisał Bipartisan Infrastructure Law, formalnie uruchamiając inicjatywę infrastrukturalną.⁹

The screenshot shows the official White House website header with "THE WHITE HOUSE" and a small logo. Below the header, the date "NOVEMBER 06, 2021" is displayed. The main title "Fact Sheet: The Bipartisan Infrastructure Deal" is centered above a horizontal navigation bar with links for "BRIEFING ROOM" and "STATEMENTS AND RELEASES". The text of the fact sheet discusses the passed infrastructure deal, mentioning its purpose as a once-in-a-generation investment in infrastructure and competitiveness, and how it builds on previous promises made by the President.

Według tej teorii wywołanie strachu przed atakami na kluczową infrastrukturę mogło zwiększyć poparcie publiczne i polityczne dla tego pakietu.

Czy może być prawdziwa?

Prezydent Biden i jego administracja nie odpowiedzieli bezpośrednio na zarzuty, oskarżające ich o wykorzystanie ataku na Colonial Pipeline do przeforsowania pakietu infrastrukturalnego. W swoich uwagach po cyberataku prezydent opisał jedynie reakcję rządu na problemy z dostawą paliwa.¹⁰

⁹

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/06/fact-sheet-the-bipartisan-infrastructure-deal/>

¹⁰

<https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/>

2. Promocja Green New Deal

Green New Deal to propozycja pakietu reform mających na celu walkę ze zmianą klimatu. Termin "Green New Deal" nawiązuje do New Deal, czyli reform zapoczątkowanych przez prezydenta Franklina D. Roosevelt w latach 30. XX wieku, mających na celu odbudowę gospodarki USA po Wielkim Kryzysie. Przedstawiona została przez Alexandrię Ocasio-Cortez i Senatora Eda Markeya. Chociaż Kongres nie przyjął formalnej legislacji Green New Deal, niektóre cele znalazły się w innych inicjatywach.



Alexandria Ocasio-Cortez i Senator Ed Markey, źródło: Wikipedia

Dlaczego taka teoria powstała?

Teoria zakłada, że wywołanie kryzysu związanego z paliwami kopalnymi mogłoby przyspieszyć przejście na zieloną energię i technologie, które są kluczowym elementem Green New Deal. Teoria powstała tak samo jak poprzednia - przez zbieżność wydarzeń. Atak nastąpił w czasie, gdy administracja Bidena promowała swoje plany dotyczące infrastruktury i środowiska. Niektórzy założyli, że rząd mógł wykorzystać sytuację kryzysową do przyspieszenia swojego celu.

Czy może być prawdziwa?

Teoria spiskowa dotycząca Colonial Pipeline jako operacji psychologicznej rządu USA nie ma poparcia w rzetelnych źródłach ani dowodów, które by ją potwierdzały. Jest oparta na zbiegu okoliczności i podobnym czasie wydarzeń, a atak został potwierdzony przez ekspertów cyberbezpieczeństwa jako wykonany przez zewnętrzną grupę przestępco.

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Released: May 07, 2023

Since its establishment, the JCDC led the national response to one of the most extensive software vulnerabilities discovered; played a central role in CISA's [Shields Up](#) campaign to protect critical infrastructure from potential Russian cyber-attacks; and, along with our partners at the Transportation Security Administration (TSA), brought together more than 25 major pipeline operators and industrial control systems partners to strengthen security practices to safeguard the operational technology networks critical to pipeline operations, efforts that complement the Security Directives TSA issued in the aftermath of the attack on Colonial Pipeline. Separately, with the support of Congress, we expanded our capability known as "CyberSentry" which enables heightened visibility into and more rapid detection of cyber threats that could target our nation's most critical operational technology networks. Finally, we worked to help organizations of all sizes and skill levels prioritize the most impactful cybersecurity investments with the introduction of [cybersecurity performance goals, or CPGs.](#)

11

Artykuł podsumowujący atak na oficjalnej stronie CISA.

3. Zabezpieczenie finansowania dla FBI

Według teorii, stworzenie zagrożenia cyberbezpieczeństwa na dużą skalę mogłoby uzasadnić potrzebę większych środków dla FBI, które zajmują się bezpieczeństwem i zwalczaniem przestępcości, między innymi w sferze cyber.

Dlaczego ta teoria powstała?

Po ataku na Colonial Pipeline rząd USA stworzył wspólną grupę zadaniową do walki z ransomware, która obejmuje różne agencje federalne, w tym FBI. Również FBI odzyskało część okupu zapłaconego przez Colonial Pipeline, co było jednym z pierwszych sukcesów grupy zadaniowej.¹² "Proces odzyskania środków obejmował śledzenie płatności okupu poprzez różne transfery bitcoinów. FBI zidentyfikowało, że bitcoiny reprezentujące płatność okupu zostały przesłane na konkretny adres. Agencji udało się uzyskać dostęp do prywatnego klucza tego adresu, który jest niezbędny do dostępu i przesyłania bitcoinów z tego portfela. Mając ten klucz, FBI mogło przejąć kontrolę nad bitcoinami, kiedy potwierdziły ich lokalizację na blockchainie".¹³

Czy może być prawdziwa?

Nie ma dowodów na to, że dodatkowe finansowanie dla FBI lub innych agencji było motywem przeprowadzenia ataku. Na bazie "Audit of the Federal Bureau of Investigation Annual Financial Statements Fiscal Year 2021"¹⁴ widać, że w 2021 roku FBI otrzymało o 6% więcej wsparcia finansowego względem poprzedniego roku. Nie ma żadnych dowodów, z których można wywnioskować, aby zostało to spowodowane opisywanym atakiem.

¹¹ <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

¹² <https://www.cpomagazine.com/cyber-security/fbi-recovers-2-3-million-of-colonial-pipeline-ransomware-payment-some-questions-about-the-attack-answered/>

¹³ <https://www.cpomagazine.com/cyber-security/fbi-recovers-2-3-million-of-colonial-pipeline-ransomware-payment-some-questions-about-the-attack-answered/>

¹⁴ <https://oig.justice.gov/sites/default/files/22-021.pdf>

Przykład 2:

Dasein.
@CavedIsolation

just to get everything straight:

>colonial pipeline "hacked"
>wow oil price go up
>wow we need renewables
>ransom paid
>pipeline opened
>entire bitcoin ransom recovered
>bitcoin was on a "bitcoin server" (lmfao) in South Carolina
>FBI saves the day

Przetłumacz wpis

Tłumaczenie:

Aby wszystko było jasne:

- >Colonial Pipeline "został zhakowany"
- >ceny ropy naftowej idą w górę
- >teraz potrzebujemy odnawialnych źródeł energii
- >okup został zapłacony
- >rurociąg został otwarty
- >cały bitcoinowy okup został odzyskany
- >bitcoin był na "serwerze bitcoinowym" (śmiech) w Karolinie Południowej
- >FBI ratuje dzień

¹⁵

Autor tweeta wyraża sceptyczny stosunek do narracji medialnej i oficjalnych oświadczeń dotyczących ataku na Colonial Pipeline. Stosuje humorystyczne podejście, aby zwrócić uwagę na „absurdy” podawane do informacji publicznej. Autor nie wierzy w atak na Colonial Pipeline - stosuje cudzysłów przy słowie “hacked”. W tweecie tym umieszczone są teorie omówione w poprzednim przykładzie - preparacja ataku, po to, aby zwrócić uwagę społeczeństwu na problem braku zielonej energii (co później mogło pomóc przegłosować i zatwierdzić pakiet Bidena). Autor nie wierzy również tłumaczeniom FBI, w jaki sposób zostały odzyskane pieniądze.

¹⁵ <https://twitter.com/CavedIsolation/status/1402283153725833221>

Przykład 3:



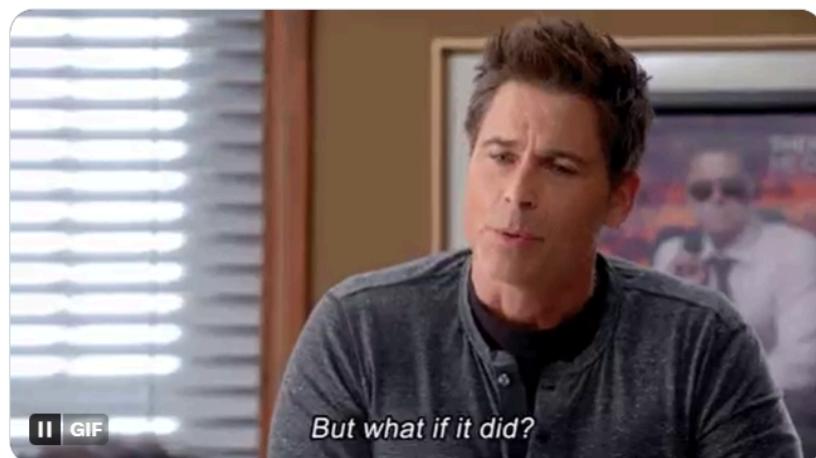
Carl Cooke @TheycallmeMrC · 11 maj 2021

Let's get in on the conspiracy **theory** bandwagon.

...

The **Colonial Pipeline** wasn't hacked in a cyberattack. It's a plot by the GOP and Big Oil to raise gas prices and try to make President Biden look bad.

OK NOT REALLY...BUT MAYBE?



16

Tłumaczenie:

Załóżmy na chwilę kapelusz foliowy. Colonial Pipeline nie został zhakowany w cyberataku. To spisek Partii Republikańskiej i dużych koncernów naftowych, aby podnieść ceny paliw i sprawić, że prezydent Biden wyjdzie na złego.

OK, NIE NAPRAWDĘ... ALE MOŻE?

Autor nie jest raczej osobą wierzącą w teorie spiskowe, zastanawia się nad teorią, która uważa, że może być prawdziwa. Teoria mówi, że atak na Colonial Pipeline jest rzekomo inscenizacją zorganizowaną przez Partię Republikańską i duże koncerny paliwowe.

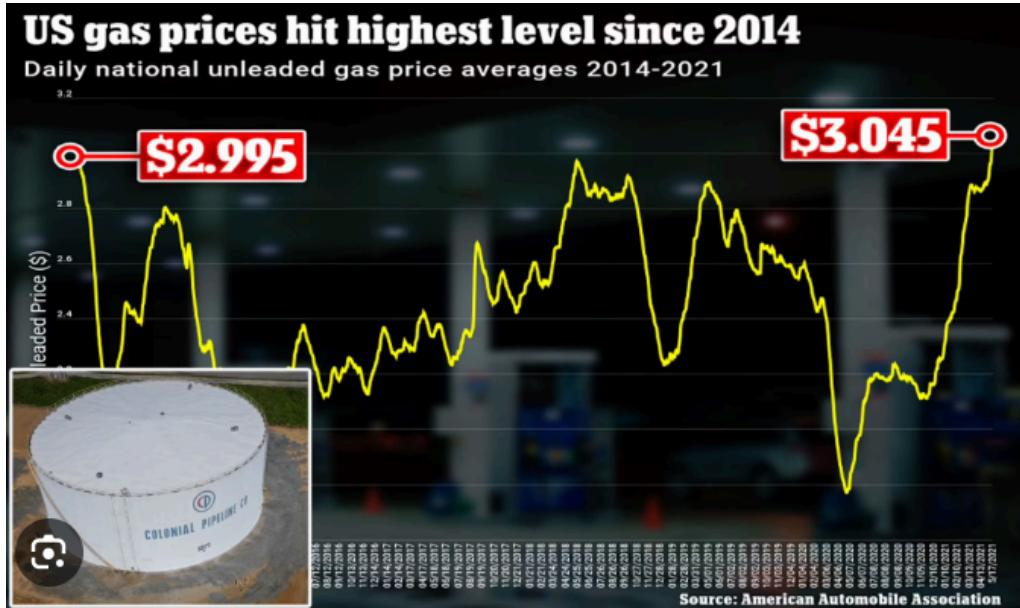
Dlaczego ta teoria powstała?

Cel takiego spisku miałby być podwójny: po pierwsze, spowodowanie wzrostu cen paliwa, a po drugie, zaszkodzenie reputacji prezydenta Bidena poprzez skojarzenie go z kryzysem paliwowym i ekonomicznym.

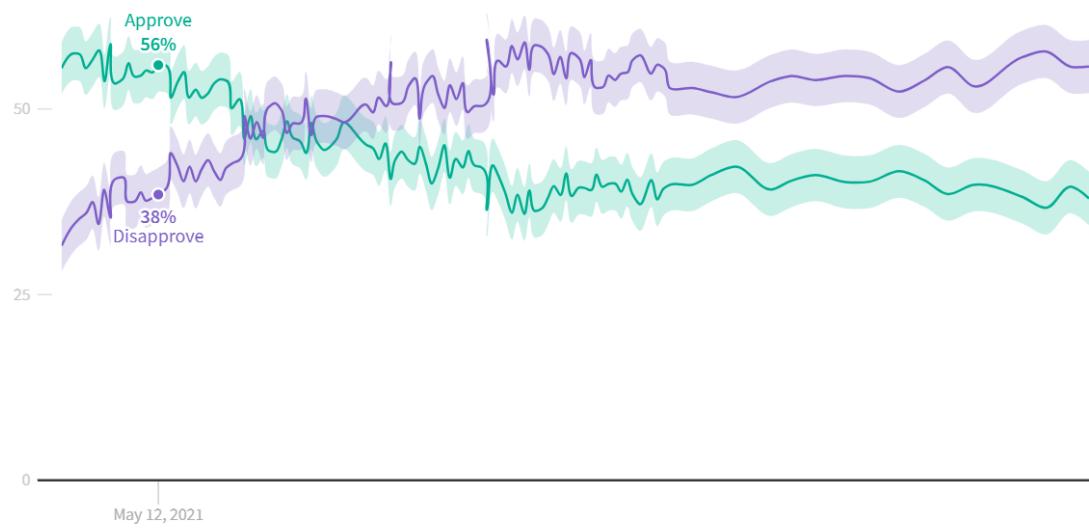
Czy może być prawdziwa?

Wzrost cen paliwa jest zauważalny, co może potwierdzać tą teorię. Poparcie prezydenta Bidena w tygodniu po ataku spada, co również może potwierdzić tę teorię. Niestety, na moment pisania pracy strona internetowa Partii Republikańskiej nie odpowiada.

¹⁶ <https://x.com/TheycallmeMrC/status/1392206832433733633>



Wzrost cen w maju 2021 (podczas ataku), źródło: American Automobile Association



17

Poparcie Bidena na przełomie lat - po 12.05.2021 widoczny jest spadek 4%

Po głębszej analizie wypowiedzi osób należących do partii wywnioskowałam, że oskarżają oni Bidena o złą reakcję na atak¹⁸. Nie podoba im się również wzrost ceny paliw oraz rozmowy o zmianie na „zieloną energię”.¹⁹

¹⁷ <https://www.reuters.com/graphics/USA-BIDEN/POLL/nmopagnqapa/>

¹⁸ <https://pfluger.house.gov/news/documentsingle.aspx?DocumentID=254>

¹⁹ <https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>

Przykład 4:

Oilfield Rando @Oilfield_Rando · 10 maj 2021
Ok gimme the best Colonial Pipeline conspiracy theories

43 5 66 ... ↗ ⌂

Great Scott!!!! @SierraAlpha24
My conspiracy is that it was some powerful people. Keep crippling things to keep everyone at home. Price of gas to high hurricane season right around the corner? No travel. Country is at tipping point. Just keep piling more on until we tip to government/world leader dependency.

[Przetłumacz wpis](#)

6:04 AM · 10 maj 2021

20

Tłumaczenie: "Moja teoria spiskowa mówi, że to byli jacyś potężni ludzie. Ciągłe sparaliżowanie wszystkiego, żeby ludzie siedzieli w domach. Cena paliwa za wysoka, a tuż za rogiem sezon huraganów? Brak podróży. Kraj jest na granicy wytrzymałości. Po prostu dokładajmy coraz więcej, aż osiągniemy zależność od rządów/liderów światowych."

Dlaczego ta teoria powstała?

Atak na Colonial Pipeline spowodował znaczne zakłócenia w dostawach paliwa, prowadząc do podwyżek cen i niedoborów na wschodnim wybrzeżu USA. Niektórzy mogą wierzyć, że za tymi zdarzeniami stoją potężne, ukryte siły mające na celu manipulację społeczną i ograniczenie mobilności ludzi, co zwiększa zależność od decyzji rządowych i międzynarodowych liderów.

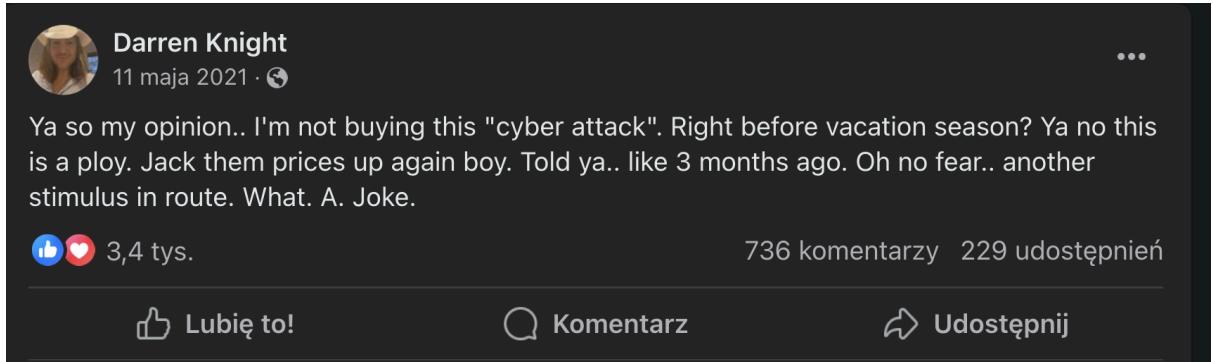
Czy może być prawdziwa?

Spekulacje dotyczące "potężnych ludzi" za atakiem na Colonial Pipeline są chętnie poruszane, choć nie ma dla nich wielu dowodów. Atak został po dochodzeniu przypisany grupie cyberprzestępca DarkSide, która działa z motywów finansowych, a nie politycznych. Idea społecznej manipulacji nie jest częścią ich planu działania. Choć grupa ta jest "potężna" w sensie zdolności do przeprowadzania skutecznych cyberataków, przypisywanie jej intencji ograniczenia mobilności ludzi w ramach jakiegoś większego planu jest niepoparte dowodami.

²⁰ <https://x.com/SierraAlpha24/status/1391605108576817152>

2. Facebook

Przykład 1:

A screenshot of a Facebook post from user Darren Knight. The post was made on May 11, 2021. The text reads: "Ya so my opinion.. I'm not buying this "cyber attack". Right before vacation season? Ya no this is a ploy. Jack them prices up again boy. Told ya.. like 3 months ago. Oh no fear.. another stimulus in route. What. A. Joke." Below the post are engagement metrics: 3,4 tys. likes, 736 comments, and 229 shares. There are also buttons for "Lubię to!", "Komentarz", and "Udostępnij".

21

Tłumaczenie:

Tak więc moja opinia... Nie kupuję tego "cyberataku". Tuż przed sezonem wakacyjnym? Nie, to podstęp. Znowu podnoszą ceny. Mówiłem ci... jakieś 3 miesiące temu. Bez obaw... kolejny bodziec w drodze. Co. Za. Żart.

Autor sugeruje, że opisywany atak może być oszustwem mającym na celu sztuczne podniesienie cen paliw, zauważając, że incydent miał miejsce tuż przed sezonem wakacyjnym, co podnosi ceny. Wydaje się więc, że autor ma podobne podejrzzenia co do tej teorii, jak przedstawiono w pierwszym fragmencie, chociaż wyraża je bardziej nieformalnie.

Co ciekawe autorem nie jest przypadkowa osoba, a komik z Alabamy mający 148 401 obserwujących²² na Facebooku. Tłumaczy to liczne odpowiedzi pod postem, które są również omawiane.

Dlaczego ta teoria powstała?

Taka opinia powstała z powodu powtarzających się sytuacji, w których zakłócenia w dostawach spowodowanych awariami lub atakami wpływały na wzrost cen, a także z powodu braku zaufania do dużych korporacji i rządu.

Czy może być prawdziwa?

Oficjalne dochodzenie FBI uznało za wykonawców ataku rosyjską grupę przestępczą. Nie ma żadnych dowodów, aby nie było to prawdą.

²¹ <https://www.facebook.com/darren.knight.9/posts/3874661152570739>

²² <https://www.facebook.com/darren.knight.9>

Analiza odpowiedzi pod podanym wyżej postem:

Odpowiedź 1:



Wesley C. Allen

The gotta make sure all the American citizens would rather stay at home and collect a check than work so there will be plenty of jobs for all the "refugees" rushing the southern border.

2 lat Lubię to! Odpowiedz

2

Tłumaczenie:

Muszą upewnić się, że wszyscy amerykańscy obywatele będą woleli zostać w domu i odebrać czek niż pracować, aby było mnóstwo miejsc pracy dla wszystkich „uchodźców” pędzących przez południową granicę.

Autor sugeruje, że oferowanie czeków dla obywateli amerykańskich jest narzędziem mającym na celu zachęcenie ich do pozostania w domu zamiast pracy, co w efekcie miałyby stworzyć wolne miejsca pracy dla imigrantów.

Dlaczego ta teoria powstała?

Niektórzy wierzą, że rząd chciałby zyskać poparcie polityczne, zmieniając rynek pracy na korzyść pewnych grup demograficznych, lub kształtuwać gospodarkę poprzez kontrolę podaży pracy i konsumpcji. Tego rodzaju opinie często wynikają z lęku przed zmianami demograficznymi, obawami związanymi z imigracją lub sceptycyzmem wobec działań rządu. Podniesione ceny paliwa miałyby wpływać na pozostanie Amerykanów w domu przez większe koszty podróży.

Czy może być prawdziwa?

Nie ma żadnych dowodów, aby rządowi zależało na pozostaniu jego obywateli w domach, ani na żadnych pozytywnych skutkach, jakie miałyby to nieść dla gospodarki.

Odpowiedzi 2 i 3:



Tonya W Griffin

They want you to buy electric cars too.

Its another scare tactic thats all caused & Set up by THEM.

Also makes you wonder what theyre trying to distract us from too.

2 lat Lubię to! Odpowiedz

3

Tłumaczenie:

Chcą, abyś kupował też samochody elektryczne. To kolejna taktyka straszenia, która została spowodowana i ustawniona przez NICH. Sprawia również, że zastanawiasz się, od czego próbują odwrócić naszą uwagę.



Debbie Lumpkin

Perfect set up to push these electric cars!!

2 lat

Lubię to!

Odpowiedz

5



Tłumaczenie:

Perfekcyjna ustawka, aby promować te elektryczne samochody

Dlaczego ta teoria powstała?

Niektórzy wierzą, że nieokreślona grupa "ONI" może manipulować rynkiem i prawem. Ta opinia często wynika z poczucia nieufności wobec dużych korporacji i rządów, które mogą być postrzegane jako współpracujące w celach nie zawsze jasnych dla ogółu społeczeństwa. Używanie frazy "NICH" podkreśla anonimowość i potencjalną wszechmoc tych, którzy stoją za rzekomymi działaniami.

Teorie te mogą sugerować, że promocja samochodów elektrycznych to sposób na ograniczenie indywidualnej wolności przez wymuszanie zmiany sposobu podróżowania.

Czy może być prawdziwa?

Na bazie statystyk rządowych²³ liczba samochodów elektrycznych zwiększyła się w 2021 roku o 435500 względem poprzedniego roku. Jednak trend jest rosnący już od paru lat i nic nie świadczy o tym, aby ten atak miał duży wpływ na liczbę zakupów. Sama branża ma się bardzo dobrze, co widać po wciąż rosnących liczbach pojazdów i nie wygląda, jakby potrzebowała pomocy od rządu w formie sfałszowanych ataków.

Podsumowanie

Atak na Colonial Pipeline ujawnił, jak głęboko różnice polityczne wpływają na sposób, w jaki media relacjonują wydarzenia. W mediach społecznościowych szybko rozprzestrzeniły się teorie spiskowe, oskarżające rząd o zainscenizowanie ataku w celu przeforsowania nowych inicjatyw politycznych, co odzwierciedla istotny poziom nieufności społecznej. Te wydarzenia podkreślają kluczową rolę przejrzystej i otwartej komunikacji ze strony instytucji publicznych i mediów, szczególnie w czasach kryzysu, co może pomóc w ograniczeniu dezinformacji i odbudowie zaufania społecznego.

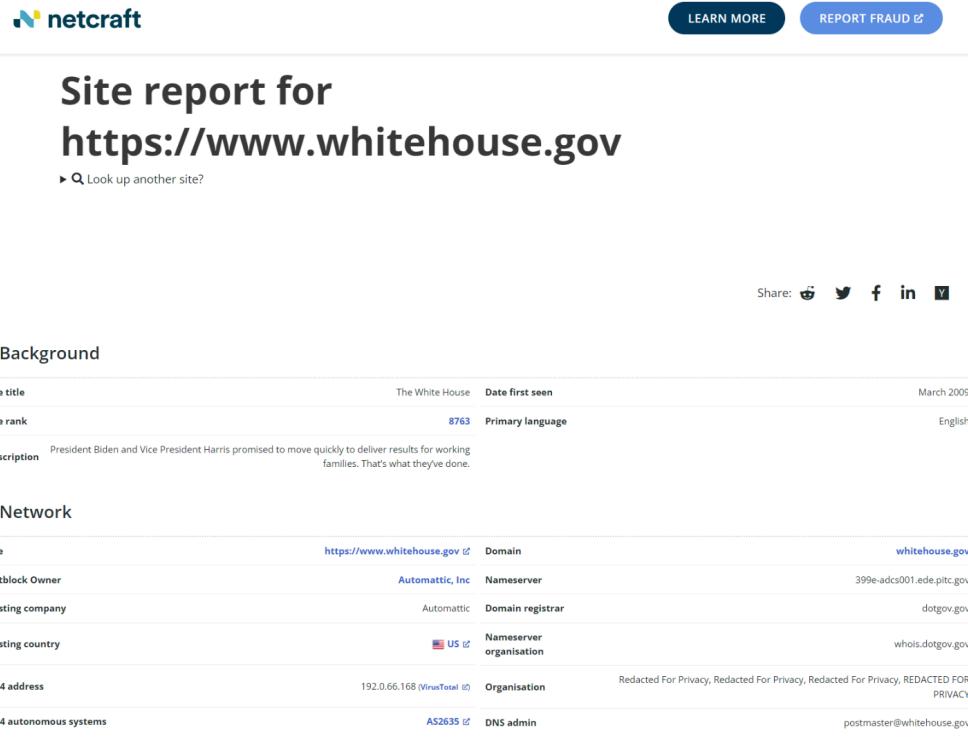
²³ <https://afdc.energy.gov/vehicle-registration?year=2021>

Analiza narzędzi użytych podczas projektu

Narzędzia sprawdzające wiarygodność stron

NetCraft

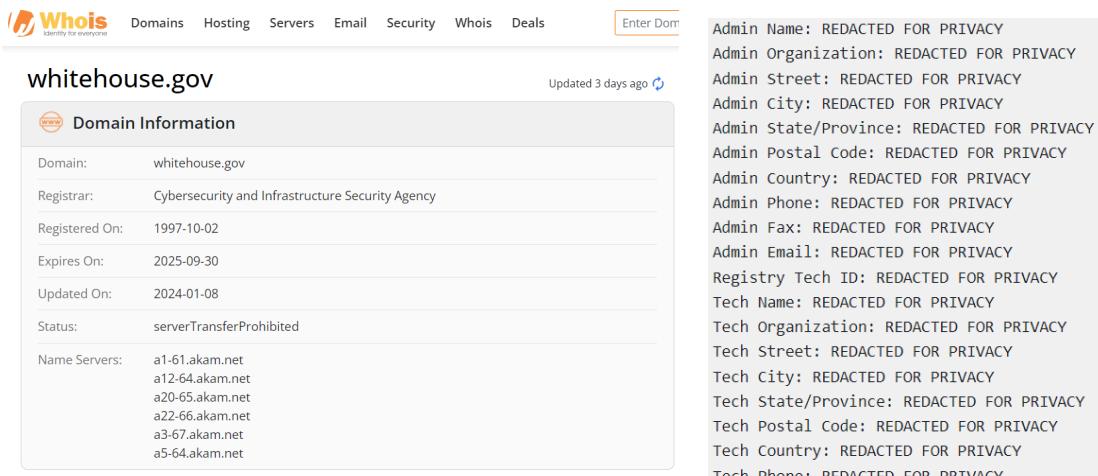
NetCraft służy do zbierania danych o stronach internetowych, takich jak ich bezpieczeństwo, hosting, używane technologie i ruch sieciowy. Netcraft oferuje również usługi związane z bezpieczeństwem, takie jak wykrywanie phishingu i fałszywych stron.



The screenshot shows the NetCraft site report for <https://www.whitehouse.gov>. The page includes the NetCraft logo, a search bar, and buttons for 'LEARN MORE' and 'REPORT FRAUD'. The main content area displays the site report with sections for 'Background' and 'Network'. The 'Background' section provides details like site title ('The White House'), date first seen ('March 2009'), site rank ('8763'), primary language ('English'), and a description about Biden's promise to deliver results for working families. The 'Network' section lists various network components and their details, such as Netblock Owner ('Automatic, Inc'), Hosting company ('Automatic'), Hosting country ('US'), IPv4 address ('192.0.66.168'), and Autonomous Systems ('AS2635').

WhoIS

Użytkownicy mogą używać WHOIS do sprawdzania kto jest właścicielem domeny lub adresu IP, kiedy dana domena została zarejestrowana, kiedy wygasła oraz jakie są dane kontaktowe do rejestatora.



The screenshot shows the Whois.com domain information for `whitehouse.gov`. It includes a 'Domain Information' table with fields like Domain, Registrar, Registered On, Expires On, Updated On, Status, and Name Servers. The 'Name Servers' listed are `a1-61.akam.net`, `a12-64.akam.net`, `a20-65.akam.net`, `a22-66.akam.net`, `a3-67.akam.net`, and `a5-64.akam.net`. To the right of the table, a large block of contact information is completely redacted with placeholder text: 'REDACTED FOR PRIVACY'.

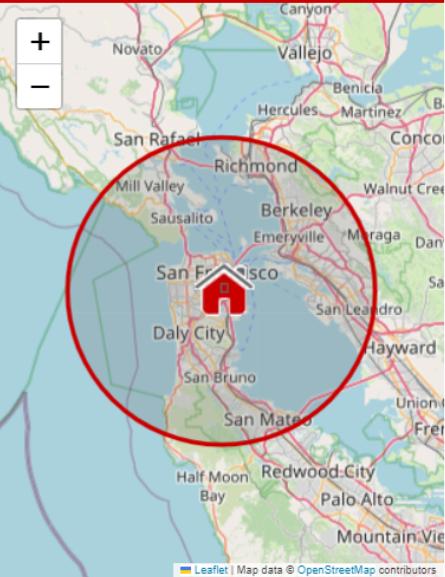
ip-tracker.org

IP-Tracker.org to internetowe narzędzie służące do śledzenia i analizy adresów IP. Umożliwia użytkownikom lokalizowanie geograficzne adresów IP, sprawdzanie szczegółów dotyczących właścicieli tych adresów, a także dostarcza informacji o dostawcach internetu (ISP) i nazwach hostów

Www.whitehouse.gov Server IP 192.0.66.168

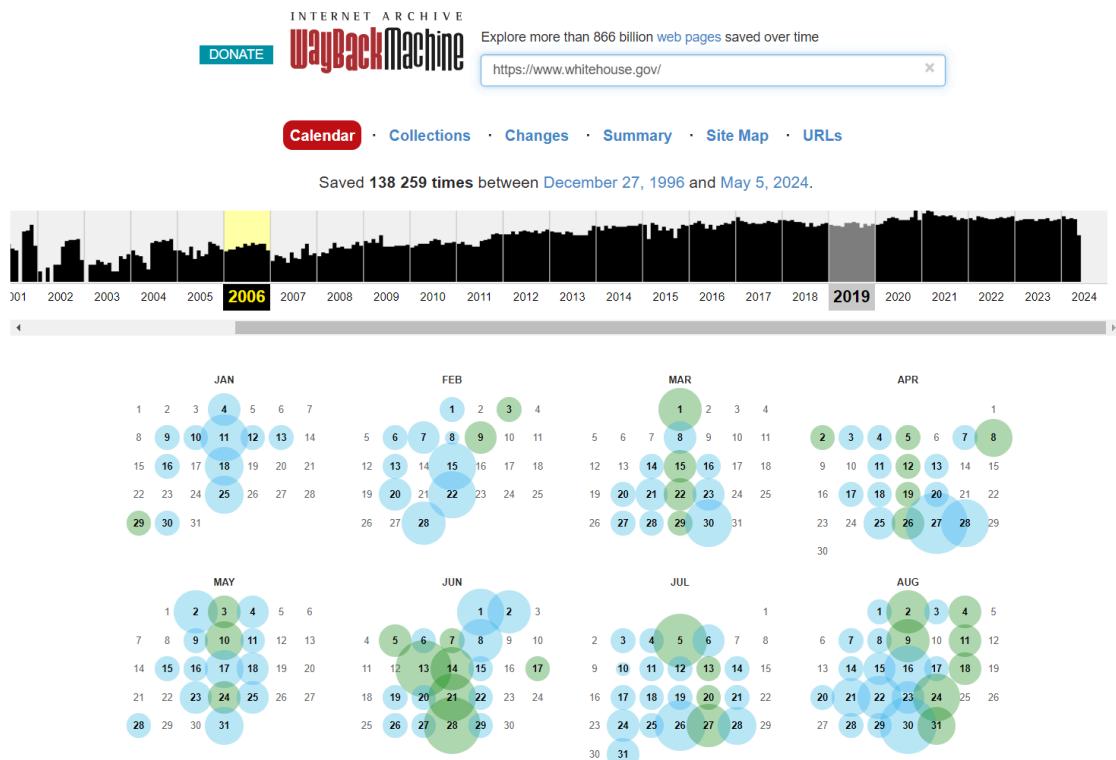
Our tracking system found the following website location information for the domain [Www.whitehouse.gov](#), at latitude 37.7506 and longitude -122.4121, in the city [San Francisco](#), state California in [United States](#) (US). [Www.whitehouse.gov](#) is assigned a US server IP 192.0.66.168 (ASN: AS2635 AUTOMATIC) and identifies itself as "The White House".

Currently, the website has a ranking value of 7/10 (more precisely 7.36 on a scale from 0 to 10) and is ranked on the website top list of popularity, in position 295, in competition with millions of other websites.

Geolocation of Website on the Map		Www.whitehouse.gov Tracking Information	
		Domain / Website: Www.whitehouse.gov [Check DNS Record - Whois - Blacklist Check]	
		Domain Server IP: 192.0.66.168	
		Domain CIDR IP: 192.0.66.168/8	
		Hostname of Website: 192.0.66.168 (Not set. Same as IP address above)	
		Internet Protocol: IPv4 - IP Version 4	
		Types: Public	
		IP Classes: Class C Range (192.0.0 to 223.255.255.255)	
		Reverse DNS: ** server can't find 168.66.0.192.in-addr.arpa: SERVFAIL	
		IPv6 Address: 2a04:fa87:ffff::c000:42a8	
		Reverse DNS IPv6: 8.a.2.4.0.0.c.0.0.0.0.0.0.0.0.0.0.d.f.f.7. 8.a.f.4.0.a.2.ip6.arpa	
		Blacklist Check: Not Blacklisted (Clean) [Blacklist Check]	
Advertisements		TOR (The Onion Router) Network: Not detected in TOR exit nodes list	

Wayback Machine

Wayback Machine pozwala użytkownikom przeglądać zapisane wersje stron internetowych z przeszłości, co jest przydatne w przypadku stron, które zostały zmienione lub usunięte



The screenshot shows the official website of the White House under President George W. Bush. The top navigation bar includes links for 'President', 'News', 'Vice President', 'History & Tours', 'First Lady', and 'Mrs. Cheney'. Below the navigation is a banner featuring the White House building and the text 'YOUR GOVERNMENT KIDS ESPAÑOL CONTACT PRIVACY POLICY SITE MAP SEARCH'. The main headline reads 'The White House' with 'PRESIDENT GEORGE W. BUSH' underneath. To the left is a sidebar with 'Issues' and 'News' sections, and an 'RSS Feeds' link. The central content area features a story about President Bush thanking military personnel at Fort Bragg on July 4, 2006. To the right is a photograph of President Bush and Japanese Prime Minister Junichiro Koizumi in a room decorated with a lamp and a piano.

- Issues**
- Budget Management
 - Education
 - Energy
 - Health Care
 - Homeland Security
 - Hurricane Recovery
 - Immigration
 - Jobs & Economy
 - Medicare
 - National Security
 - Pandemic Flu
 - Patriot Act
 - Renewal in Iraq
 - Social Security
 - More Issues »

- News**
- Current News
 - Press Briefings
 - Proclamations
 - Executive Orders
 - Radio

RSS Feeds

July 4, 2006 | Last Updated 12:12 p.m. (EDT)

President Bush Thanks Military on Independence Day at Fort Bragg, North Carolina

President Bush On Tuesday said, "Since that first 4th of July, some 43 million Americans have defended our freedom in times of war. These brave men and women crossed oceans and continents to defeat murderous ideologies and to secure the peace for generations that followed. We live in liberty because of the courage they displayed -- from Bunker Hill to Baghdad, from Concord to Kabul -- on this Independence Day we honor their achievements and we thank them for their service in freedom's cause." [full story](#)



More Photos **White House photo by Shealah Craighead**
President George W. Bush and Japanese Prime Minister Junichiro Koizumi share a laugh in the Jungle Room while Laura Bush, Priscilla Presley and daughter Lisa-Marie Presley look on, Friday, June 30, 2006, in Memphis, Tennessee, during a tour of Graceland, the home of Elvis Presley. White House photo by Shealah Craighead

President's Radio Address

Wyszukiwarki

Google.com

Google jest liderem na rynku wyszukiwarek i jego algorytmy dostarczają wyniki dla miliardów zapytań każdego dnia.

Google dorking

Google Dorking, znane także jako Google hacking, to technika wykorzystująca zaawansowane zapytania w wyszukiwarce Google do znajdowania informacji, które są trudne do odnalezienia przy użyciu standardowych wyszukiwań.

Przykład:

Wszystkie wyszukiwania na temat Colonial Pipeline i ze strony whitehouse.gov

The screenshot shows a Google search results page. The search query is 'site:whitehouse.gov "Colonial Pipeline"'. The results are filtered under the 'Wszystko' tab. There are approximately 169 results. The top result is from whitehouse.gov, dated May 11, 2021, titled 'FACT SHEET: The Biden-Harris Administration Has ...'. The snippet describes a cyberattack targeting the Colonial Pipeline.

Wyszukiwarka na portalu X.com

Na Twitterze wyszukiwanie jest rozbudowane i posiada wiele filtrów, które pozwalają użytkownikom dopasować wyniki.

- Słowa kluczowe: można wyszukiwać tweety zawierające określone słowa, wyrażenia lub hasztagi.
- Od i do określonych użytkowników: pozwala na wyszukiwanie tweetów, które zostały wysłane przez konkretnego użytkownika lub skierowane do konkretnego użytkownika.
- Wzmianki: pozwala na wyszukiwanie tweetów, w których wspomniany jest użytkownik.
- Daty: można wyszukiwać tweety z określonego zakresu dat.
- Lokalizacja: filtrowanie tweetów na podstawie ich geolokalizacji.
- Język: można filtrować tweety według języka, w którym zostały napisane.

← Q colonial pipeline theory ...

Najlepsze

Najnowsze

Użytkownicy

Multimedia

Listy



Bill Taylor ✅ @ProTradersOpin · 8 cze 2021

Conspiracy **theory**? US intelligence agency hacked **Colonial Pipeline** to discredit Bitcoin. FBI to the rescue and funds retrieved. Only \$5M for a pipeline shutdown? Really? #Bitcoin 💰 @HalftimeReport #crypto @BTC #bitcoin 💰



David @athomeinbklyn · 8 cze 2021

My **theory** on how the FBI swiftly recovered the ransom money paid by **Colonial Pipeline**:

They paid them with marked bits.



@nikhileshde@journa.host @nikhileshde · 8 cze 2021

Quick thread on **theories** as to how the FBI gained control of the private keys in the **Colonial Pipeline** ransomware recovery:



Główna

Przeglądaj

Powiadomienia

Wiadomości

Listy

Zakładki

Grupy dyskusyjne

Premium

Profil

Więcej

Opublikuj wpis



from:WhiteHouse Biden

...

Najlepsze

Najnowsze

Użytkownicy

Multimedia

Listy



The White House ✅ @WhiteHouse · 29 kw

...

Small businesses are the engine of our economy.

Since the start of the **Biden**-Harris Administration, Americans have filed a record 17 million new business applications.

This Small Business Week, our Administration continues to fight to grow the small business boom.



625

510

1 tys.

124 tys.



Filtr wyszukiwania

Użytkownicy

Od wszystkich
Osoby, które obserwujesz



Lokalizacja

Wszędzie
W pobliżu Ciebie



Wyszukiwanie zaawansowane

Warcí obserwowania

 THEPOLANDNEWS ✅ @thepolandnews_

Obserwuj

 haze 🇵🇱 @rockandberries

Obserwuj

 FAST INFO ✅ @Fastinfoo

Obserwuj

Pokaż więcej

Najpopularniejsze w Polska

1 • Piłka nożna - Trendy

#LEGRAD

1 666 posts



Wtyczki i rozszerzenia

Gotanda

Gotanda to rozszerzenie OSINT, które wyszukuje informacje z niektórych IOC na stronach internetowych (IP, domena, URL, SNS itp.)



Wappalyzer

Wappalyzer to narzędzie do wykrywania technologii używanych na stronach internetowych. Pozwala identyfikować, jakie systemy zarządzania treścią, języki, bazy danych, platformy e-commerce, serwery sieciowe są używane przez różne strony.

