|VIΛVIS| střežíme podstatné

CYBERSEC FORUM 2024

Specifické incidenty za rok 2023/24

Vladimír Lazecký

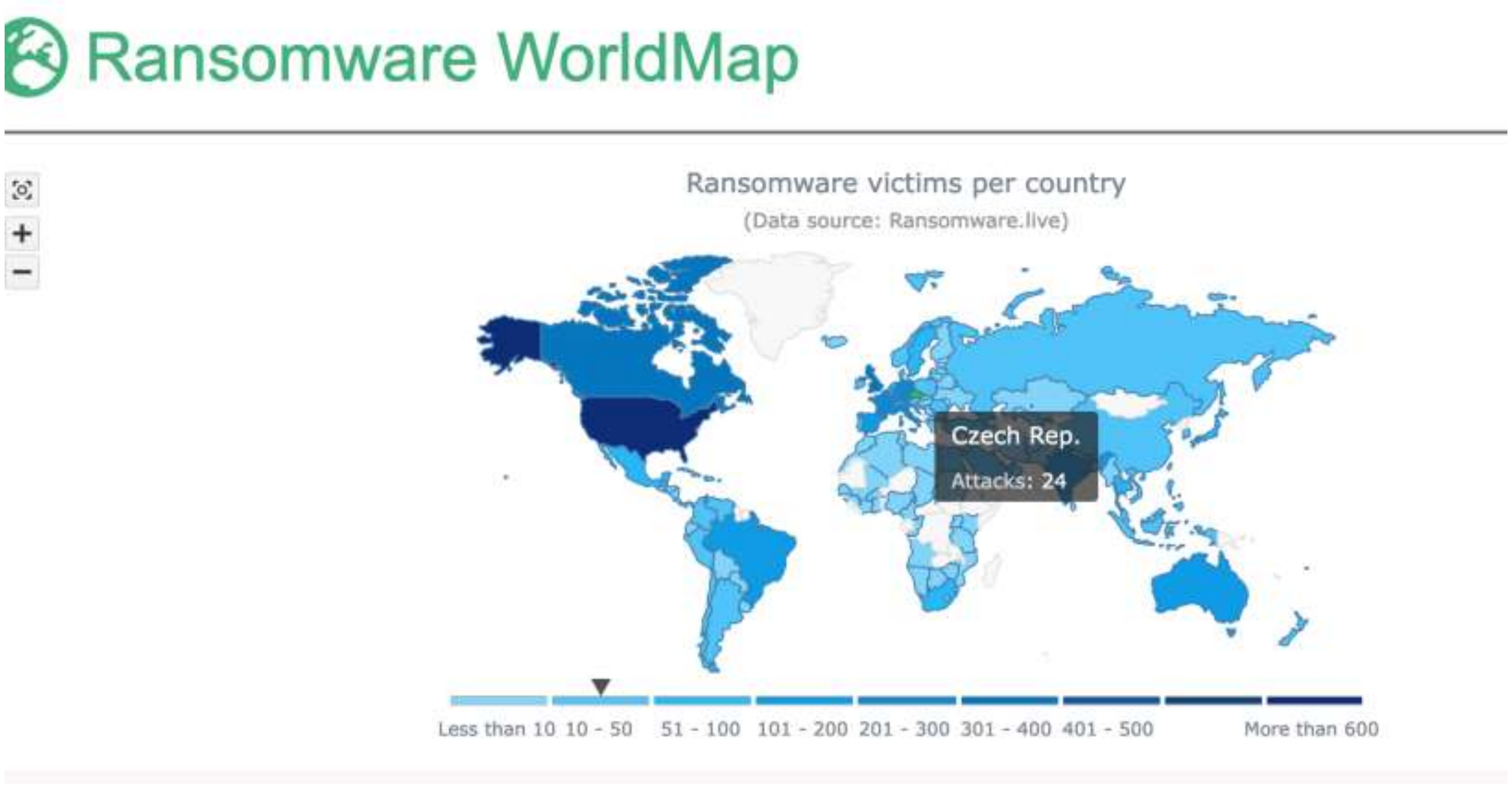
Martin Pavlíček

www.viavis.cz

Shrnutí roku 2023/24 – bez nároku na generalizaci

- ✓ Snížení počtu úspěšných ransomware útoků v roce 2023
- ✓ Nárůst útoků od Q3 v roce 2024
- ✓ Některé oběti minulých útoků se nepoučily
- ✓ Cílené útoky
- ✓ Útoky vedené laiky

Počet obětí ransomware v ČR za poslední rok



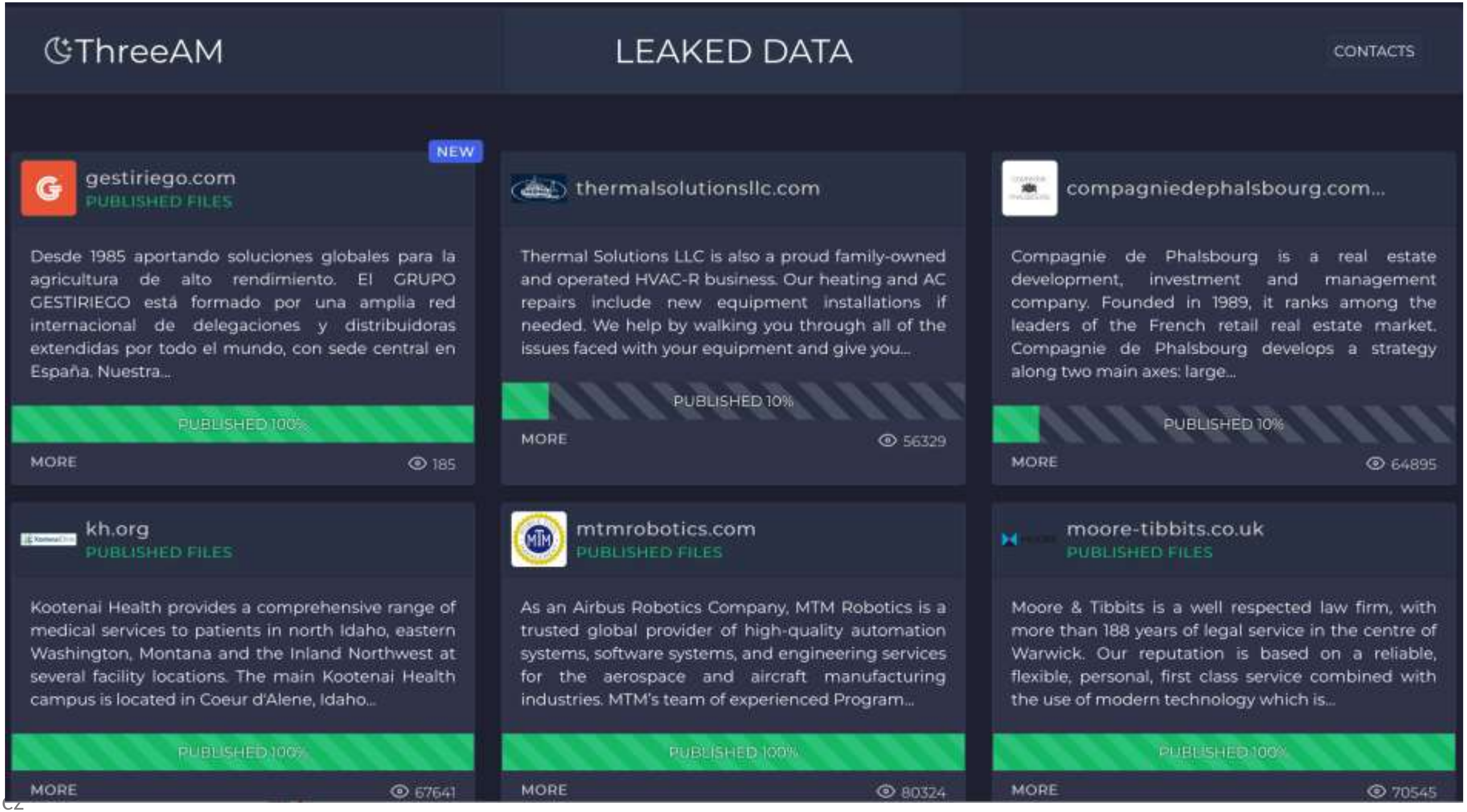
Ransomware WorldMap

Ransomware victims per country

(Data source: Ransomware.live)

https://www.ransomware.live/map/

Aktuální Wall of Shame



NEW

gestiriego.com
PUBLISHED FILES

Desde 1985 aportando soluciones globales para la agricultura de alto rendimiento. El GRUPO GESTIRIEGO está formado por una amplia red internacional de delegaciones y distribuidoras extendidas por todo el mundo, con sede central en España. Nuestra...

PUBLISHED 100%
MORE 185

thermalsolutionsllc.com

Thermal Solutions LLC is also a proud family-owned and operated HVAC-R business. Our heating and AC repairs include new equipment installations if needed. We help by walking you through all of the issues faced with your equipment and give you...

PUBLISHED 10%
MORE 56329

compagniedephalsbourg.com...

Compagnie de Phalsbourg is a real estate development, investment and management company. Founded in 1989, it ranks among the leaders of the French retail real estate market. Compagnie de Phalsbourg develops a strategy along two main axes: large...

PUBLISHED 10%
MORE 64895

kh.org
PUBLISHED FILES

Kootenai Health provides a comprehensive range of medical services to patients in north Idaho, eastern Washington, Montana and the Inland Northwest at several facility locations. The main Kootenai Health campus is located in Coeur d'Alene, Idaho...

PUBLISHED 100%
MORE 67641

mtmrobotics.com
PUBLISHED FILES

As an Airbus Robotics Company, MTM Robotics is a trusted global provider of high-quality automation systems, software systems, and engineering services for the aerospace and aircraft manufacturing industries. MTM's team of experienced Program...

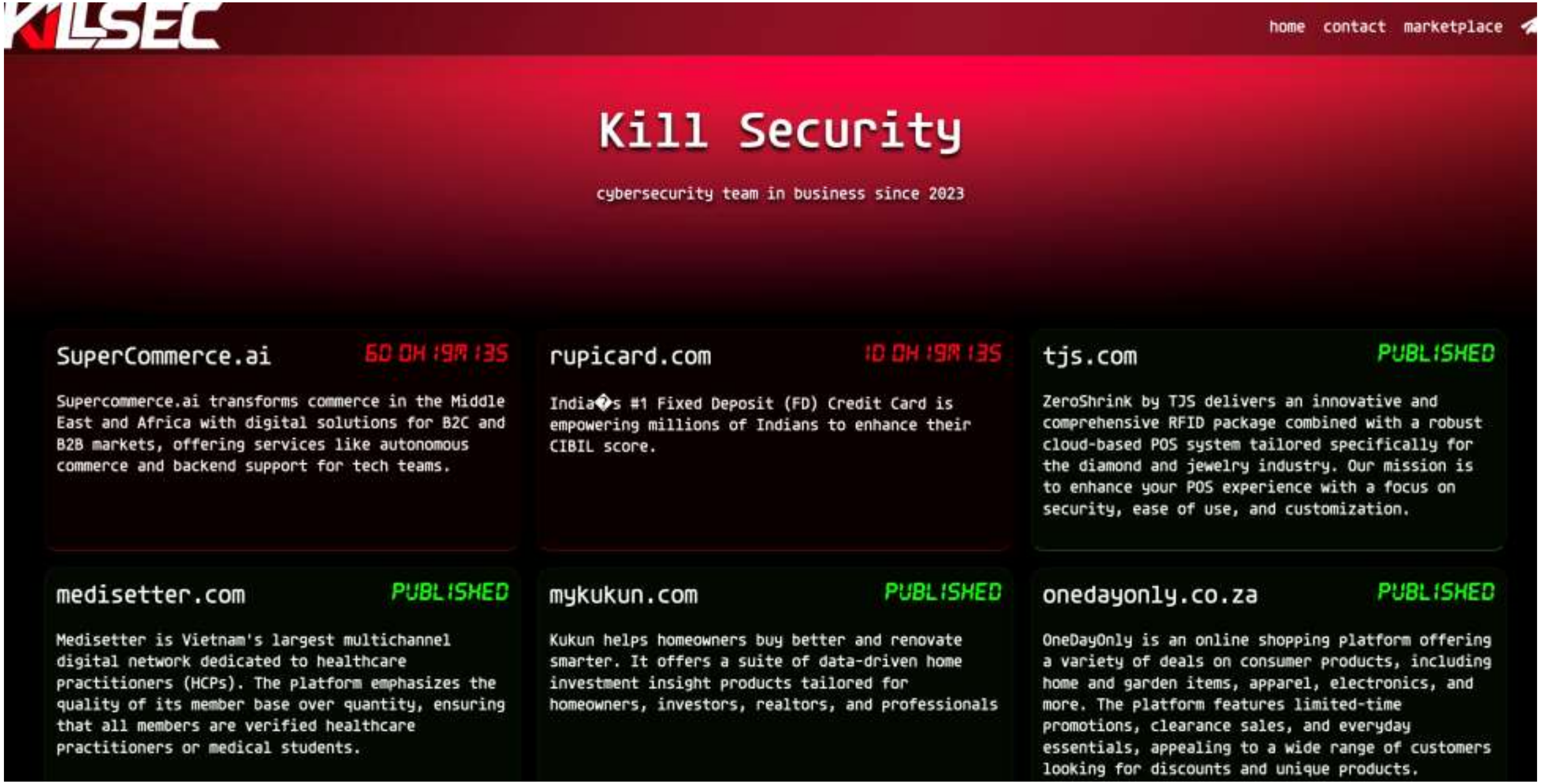
PUBLISHED 100%
MORE 80324

moore-tibbits.co.uk
PUBLISHED FILES

Moore & Tibbits is a well respected law firm, with more than 188 years of legal service in the centre of Warwick. Our reputation is based on a reliable, flexible, personal, first class service combined with the use of modern technology which is...

PUBLISHED 100%
MORE 70545

Aktuální Wall of Shame



KILSEC

Kill Security

cybersecurity team in business since 2023

SuperCommerce.ai 6D 0H :19M :35

Supercommerce.ai transforms commerce in the Middle East and Africa with digital solutions for B2C and B2B markets, offering services like autonomous commerce and backend support for tech teams.

rupicard.com 1D 0H :19M :35

India�s #1 Fixed Deposit (FD) Credit Card is empowering millions of Indians to enhance their CIBIL score.

tjs.com PUBLISHED

ZeroShrink by TJS delivers an innovative and comprehensive RFID package combined with a robust cloud-based POS system tailored specifically for the diamond and jewelry industry. Our mission is to enhance your POS experience with a focus on security, ease of use, and customization.

medisetter.com PUBLISHED

Medisetter is Vietnam's largest multichannel digital network dedicated to healthcare practitioners (HCPs). The platform emphasizes the quality of its member base over quantity, ensuring that all members are verified healthcare practitioners or medical students.

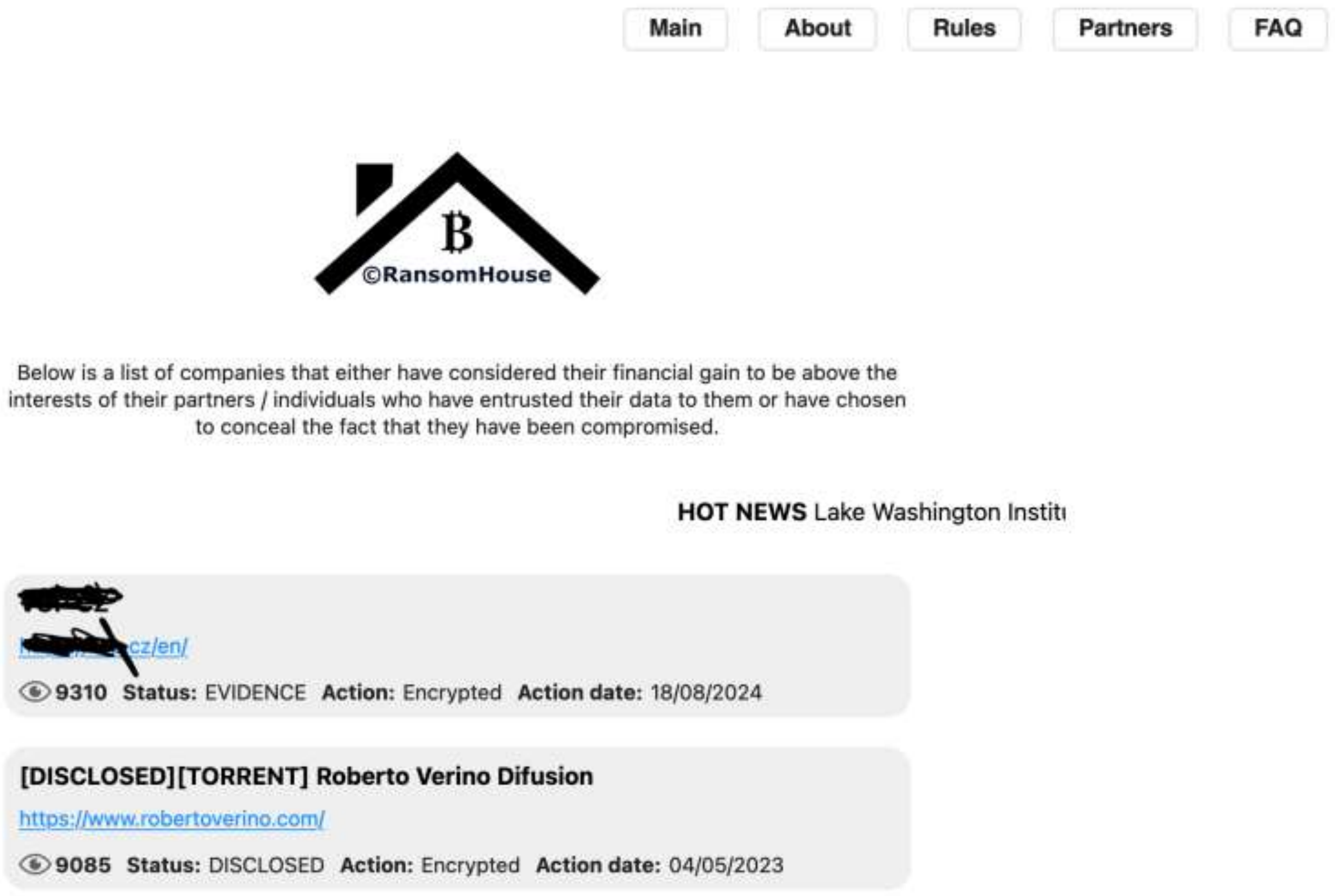
mykukun.com PUBLISHED

Kukun helps homeowners buy better and renovate smarter. It offers a suite of data-driven home investment insight products tailored for homeowners, investors, realtors, and professionals

onedayonly.co.za PUBLISHED

OneDayOnly is an online shopping platform offering a variety of deals on consumer products, including home and garden items, apparel, electronics, and more. The platform features limited-time promotions, clearance sales, and everyday essentials, appealing to a wide range of customers looking for discounts and unique products.

Aktuální Wall of Shame



Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

HOT NEWS Lake Washington Institu

[redacted]

[redacted]cz/en/

👁 **9310** **Status:** EVIDENCE **Action:** Encrypted **Action date:** 18/08/2024

[DISCLOSED][TORRENT] Roberto Verino Difusion

https://www.robertoverino.com/

👁 **9085** **Status:** DISCLOSED **Action:** Encrypted **Action date:** 04/05/2023

Co lze z darknetu vyčíst

- Obětí může být kdokoli:
  - Převažují útoky využívající zranitelnosti

- Rostou politicky motivované útoky
  - Souvislost s aktuálními konflikty

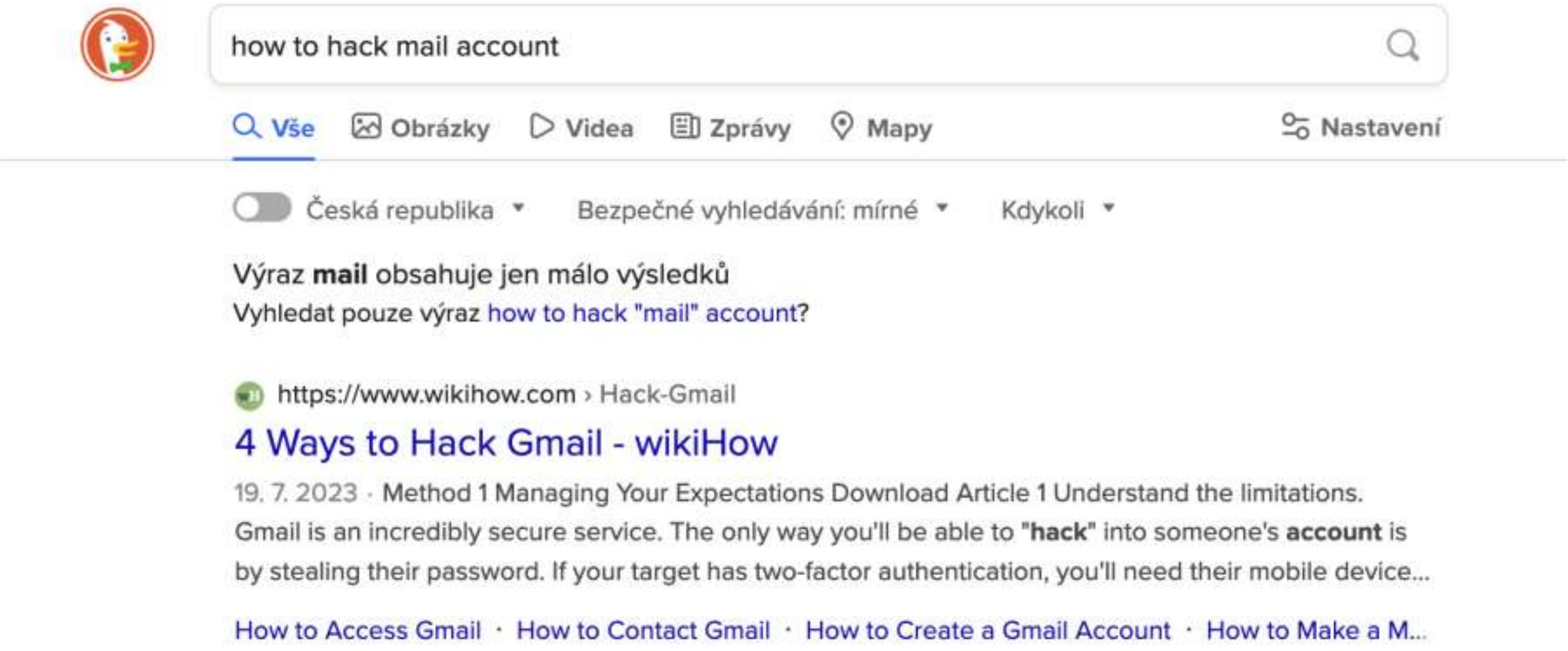
- Roste nabídka útoků jako služby

Co se také může stát - příběh ze života číslo 1

- Zaměstnanec ve výpovědi
  - Msta vedoucímu manažerovi
  - Útočník byl bez hlubokých IT znalostí
  - Útočník se naboural do mailové schránky a profilům na sociálních sítí
  - Informace využil k reputačnímu útoku

Jak byste to udělali?

Jak hacknout email? – Zeptám se google



Výraz **mail** obsahuje jen málo výsledků
Vyhledat pouze výraz how to hack "mail" account?

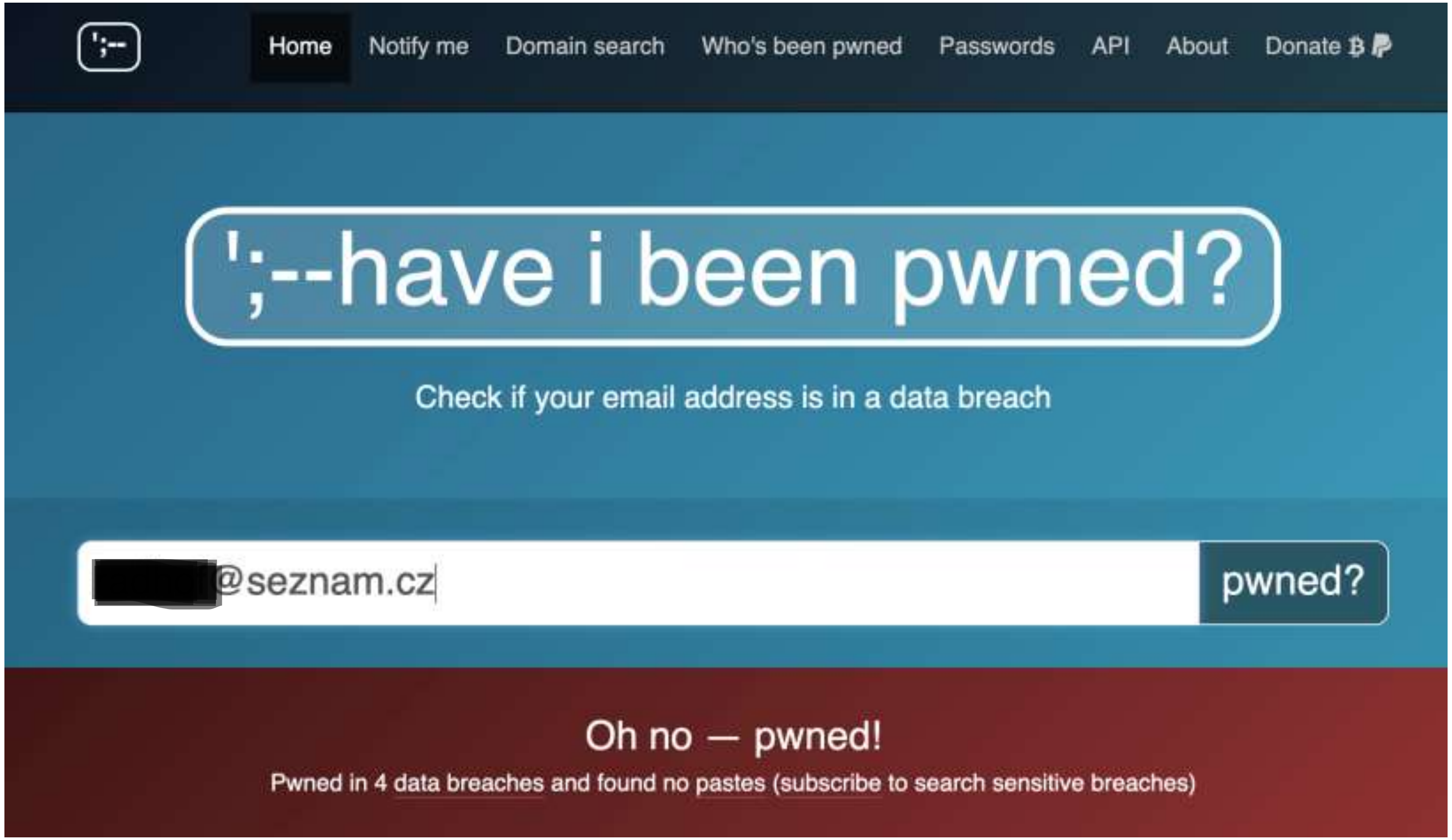
https://www.wikihow.com › Hack-Gmail

4 Ways to Hack Gmail - wikiHow

19. 7. 2023 · Method 1 Managing Your Expectations Download Article 1 Understand the limitations. Gmail is an incredibly secure service. The only way you'll be able to "**hack**" into someone's **account** is by stealing their password. If your target has two-factor authentication, you'll need their mobile device...

How to Access Gmail · How to Contact Gmail · How to Create a Gmail Account · How to Make a M...

Jak získat autentizační data pomocí mailové identity



';--have i been pwned?

Check if your email address is in a data breach

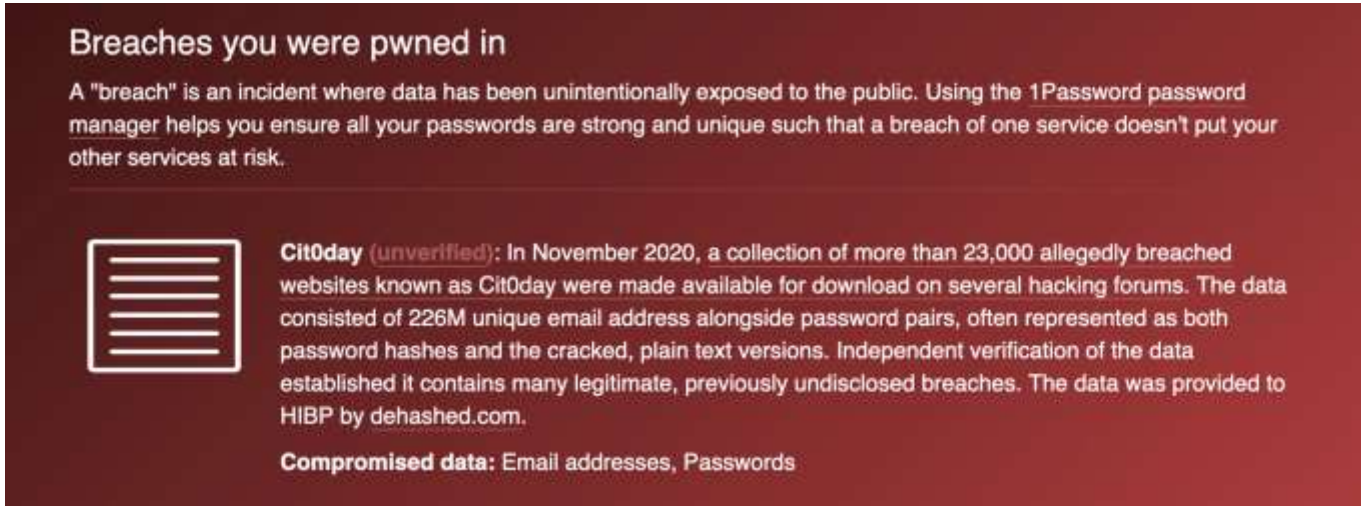
[redacted]@seznam.cz

Oh no — pwned!

Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)

https://haveibeenpwned.com/

Jak získat autentizační data pomocí mailové identity

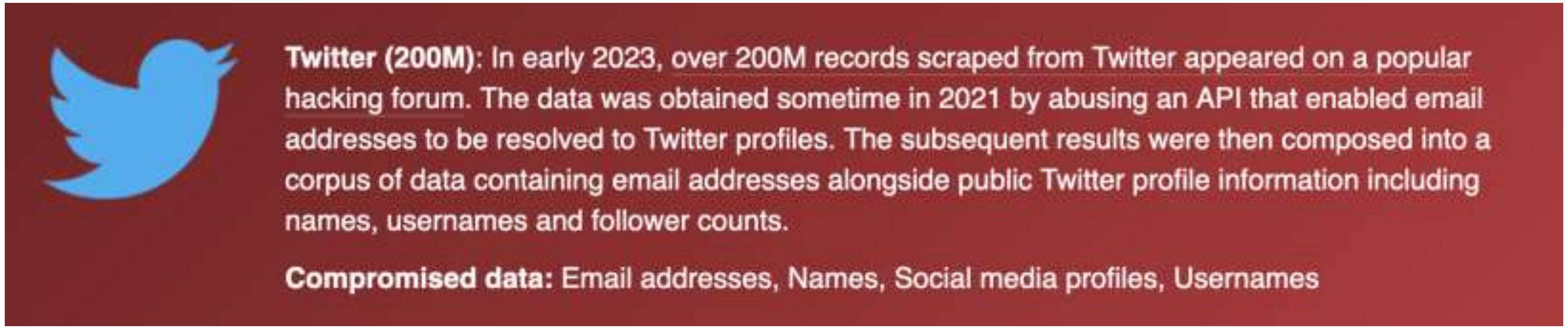


Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

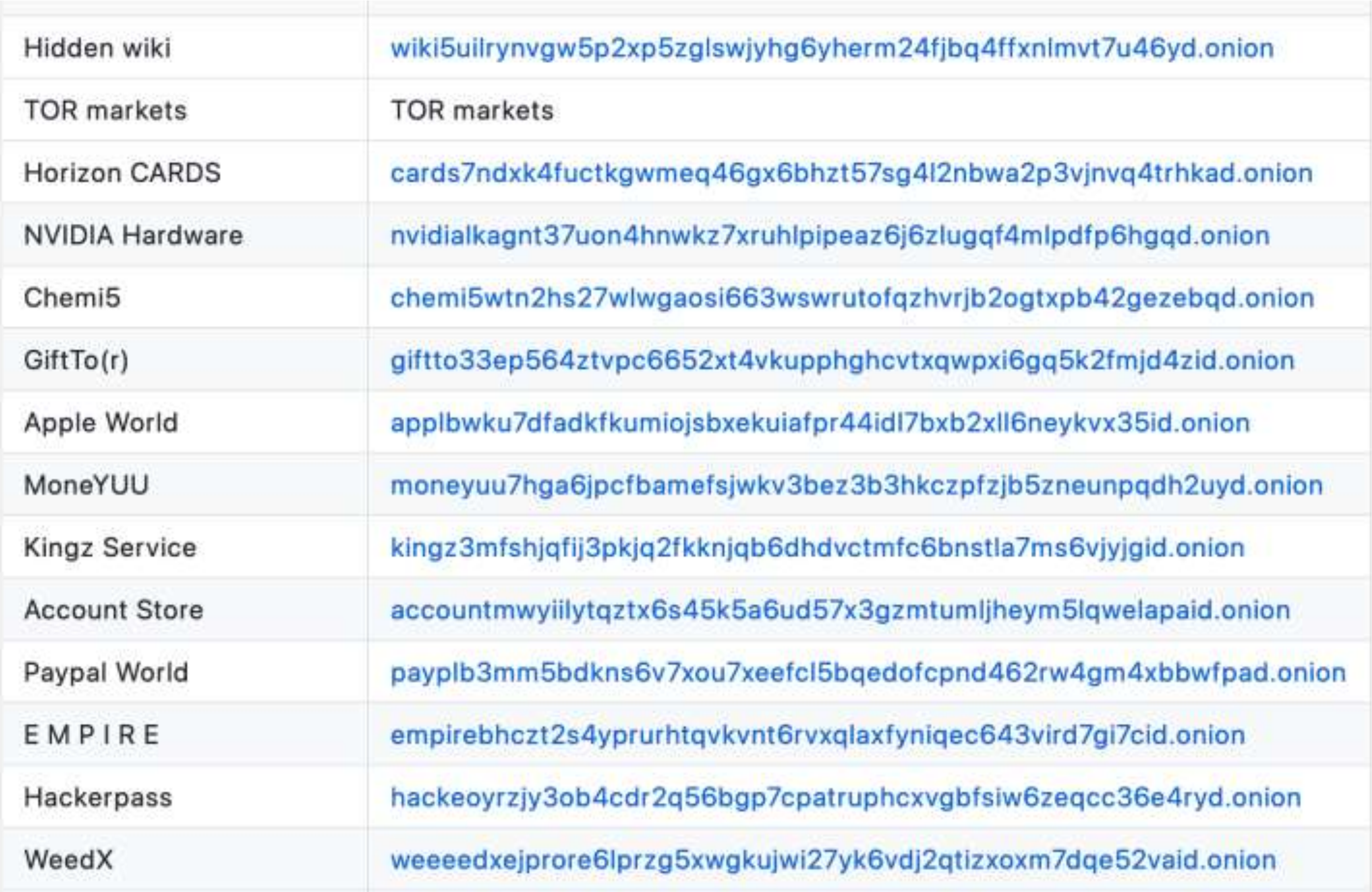


Twitter (200M): In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.

Compromised data: Email addresses, Names, Social media profiles, Usernames

https://haveibeenpwned.com/

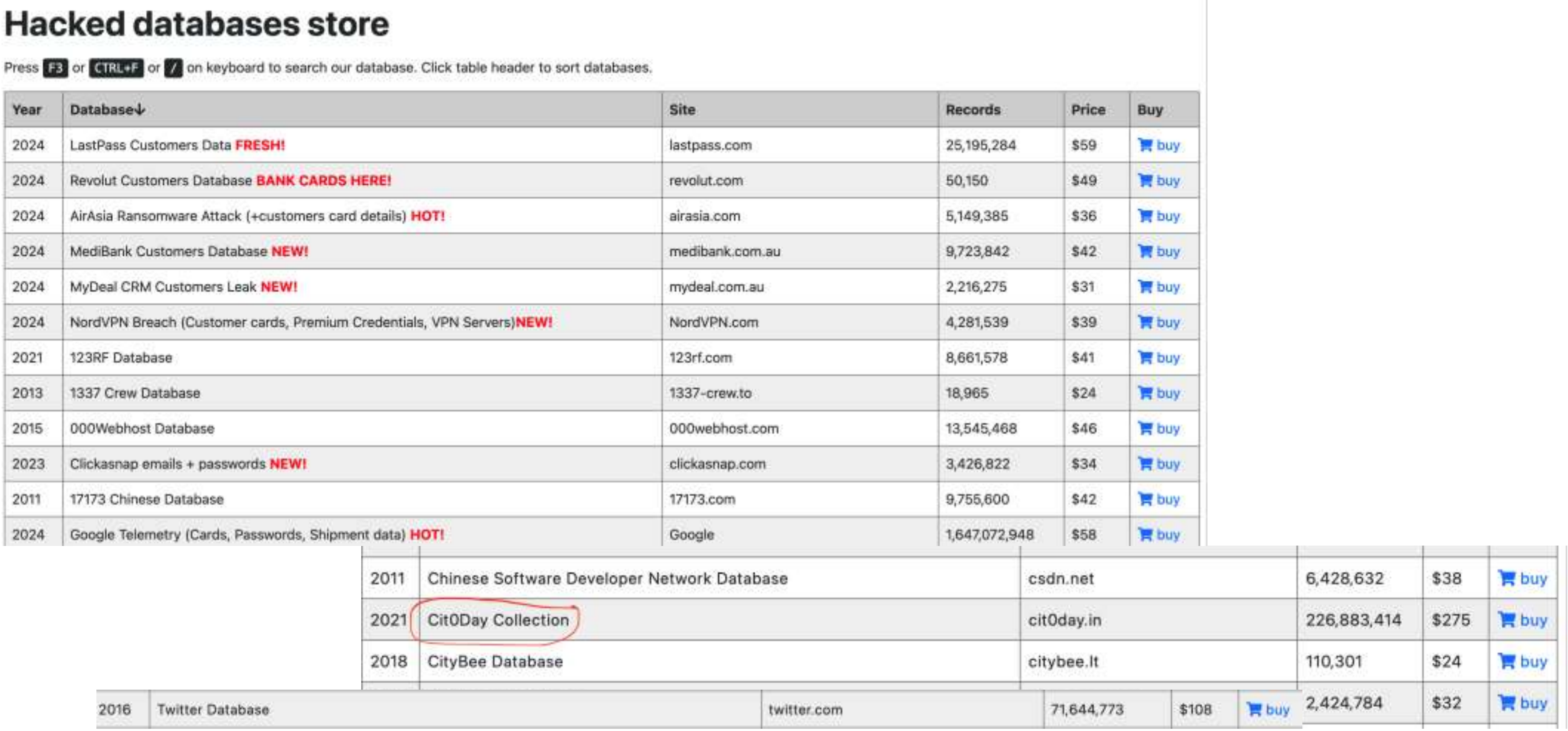
Jak najít databázi zcizených identit



Hidden wiki	wiki5uilrynvgw5p2xp5zglswjyhg6yherm24fjbq4ffxnlmvt7u46yd.onion
TOR markets	TOR markets
Horizon CARDS	cards7ndxk4fuctkgwmeq46gx6bhzt57sg4l2nbwa2p3vjnvq4trhkad.onion
NVIDIA Hardware	nvidialkagnt37uon4hnwkz7xruhlpipeaz6j6zlugqf4mlpdfp6hgqd.onion
Chemi5	chemi5wtn2hs27wlwgaosi663wswrutofqzhvrjb2ogtxpb42gezebqd.onion
GiftTo(r)	giftto33ep564ztvpc6652xt4vkupphghcvtxqwpxi6gq5k2fmjd4zid.onion
Apple World	applbwku7dfadkfkumiojsbxekuiafpr44idl7bxb2xll6neykvx35id.onion
MoneYUU	moneyuu7hga6jpcfbamefsjwkv3bez3b3hkczpfzjb5zneunpqdh2uyd.onion
Kingz Service	kingz3mfshjqfij3pkjq2fkknjqb6dhdvctmfc6bnstla7ms6vjyjgid.onion
Account Store	accountmwyiilytqztx6s45k5a6ud57x3gzmtumljheym5lqwelapaid.onion
Paypal World	payplb3mm5bdkns6v7xou7xeefcl5bqedofcpnd462rw4gm4xbbwfpad.onion
EMPIRE	empirebhczt2s4yprurhtqvkvnt6rvxqlaxfyniqec643vird7gi7cid.onion
Hackerpass	hackeoyrzjy3ob4cdr2q56bgp7cpatruphcxvgbfsiw6zeqcc36e4ryd.onion
WeedX	weeeedxejprore6lprzg5xwgkujwi27yk6vdj2qtizxoxm7dqe52vaid.onion

https://thehidden-wiki.github.io/Links/

Ceny nejsou závratné (dají se najít i zdarma)



Hacked databases store

Press F3 or CTRL+F or / on keyboard to search our database. Click table header to sort databases.

Year	Database↓	Site	Records	Price	Buy
2024	LastPass Customers Data **FRESH!**	lastpass.com	25,195,284	$59	buy
2024	Revolut Customers Database **BANK CARDS HERE!**	revolut.com	50,150	$49	buy
2024	AirAsia Ransomware Attack (+customers card details) **HOT!**	airasia.com	5,149,385	$36	buy
2024	MediBank Customers Database **NEW!**	medibank.com.au	9,723,842	$42	buy
2024	MyDeal CRM Customers Leak **NEW!**	mydeal.com.au	2,216,275	$31	buy
2024	NordVPN Breach (Customer cards, Premium Credentials, VPN Servers)**NEW!**	NordVPN.com	4,281,539	$39	buy
2021	123RF Database	123rf.com	8,661,578	$41	buy
2013	1337 Crew Database	1337-crew.to	18,965	$24	buy
2015	000Webhost Database	000webhost.com	13,545,468	$46	buy
2023	Clickasnap emails + passwords **NEW!**	clickasnap.com	3,426,822	$34	buy
2011	17173 Chinese Database	17173.com	9,755,600	$42	buy
2024	Google Telemetry (Cards, Passwords, Shipment data) **HOT!**	Google	1,647,072,948	$58	buy

2011	Chinese Software Developer Network Database	csdn.net	6,428,632	$38	buy
2021	Cit0Day Collection	cit0day.in	226,883,414	$275	buy
2018	CityBee Database	citybee.lt	110,301	$24	buy
			2,424,784	$32	buy

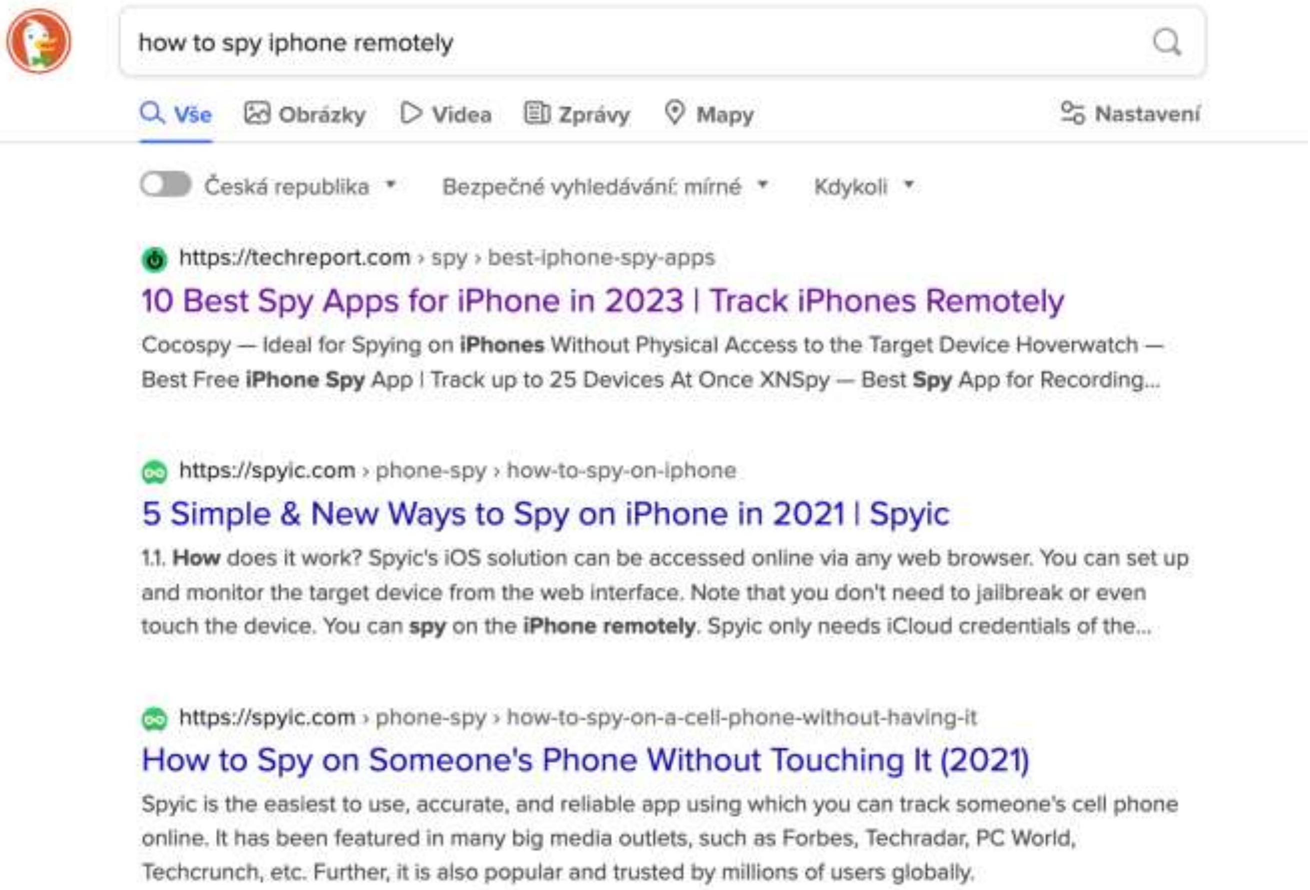
2016	Twitter Database	twitter.com	71,644,773	$108	buy

Příběh ze života číslo 2

- Žárlivý partner/partnerka
  - Nedůvěra k partnerovi
  - Bez jakýchkoli IT znalostí, pouze silná motivace
  - Útočník ovládl mobilní telefon oběti
  - Oběť pod plnou kontrolou -> psychické problémy, rozpad rodiny, reputační dopady

Jak to uděláte?

Jak lze ovládnout iPhone?



https://techreport.com › spy › best-iphone-spy-apps

10 Best Spy Apps for iPhone in 2023 | Track iPhones Remotely

Cocospy — Ideal for Spying on **iPhones** Without Physical Access to the Target Device Hoverwatch — Best Free **iPhone Spy** App | Track up to 25 Devices At Once XNSpy — Best **Spy** App for Recording...

https://spyic.com › phone-spy › how-to-spy-on-iphone

5 Simple & New Ways to Spy on iPhone in 2021 | Spyic

1.1. **How** does it work? Spyic's iOS solution can be accessed online via any web browser. You can set up and monitor the target device from the web interface. Note that you don't need to jailbreak or even touch the device. You can **spy** on the **iPhone remotely**. Spyic only needs iCloud credentials of the...

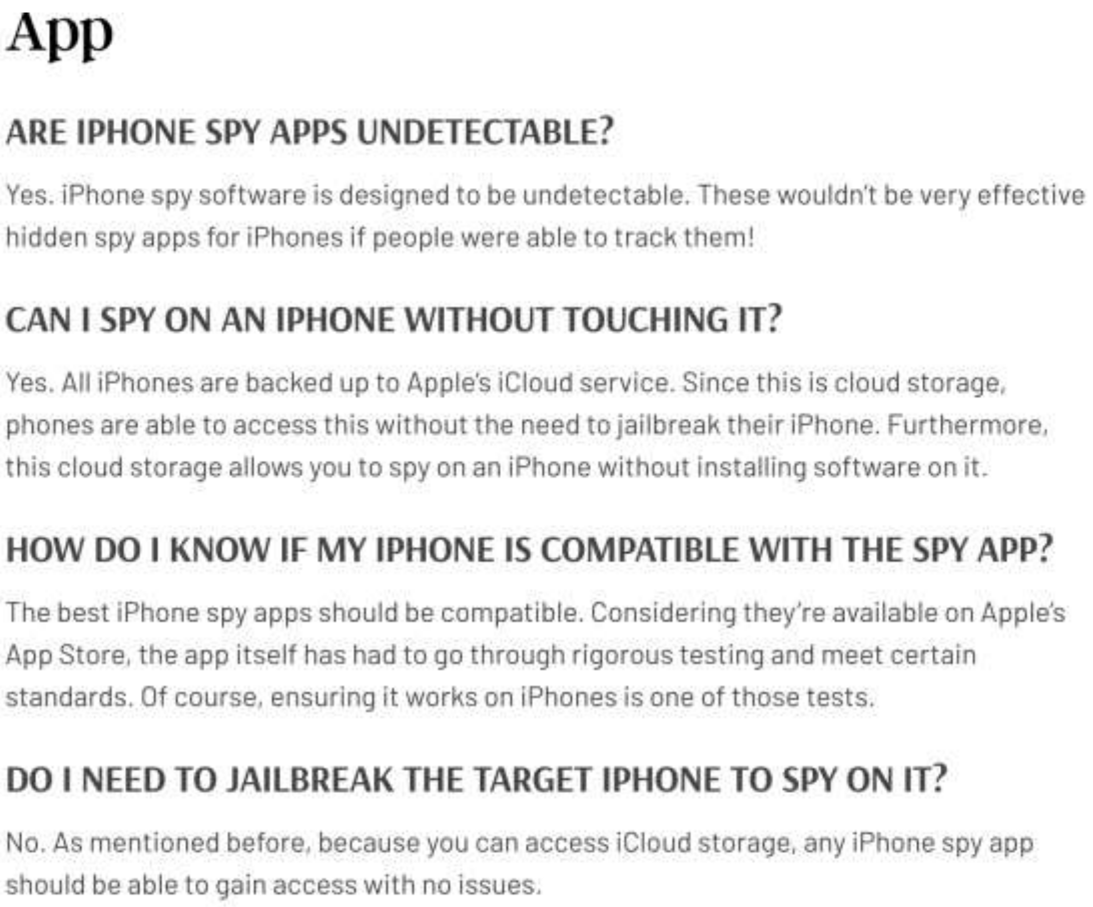
https://spyic.com › phone-spy › how-to-spy-on-a-cell-phone-without-having-it

How to Spy on Someone's Phone Without Touching It (2021)

Spyic is the easiest to use, accurate, and reliable app using which you can track someone's cell phone online. It has been featured in many big media outlets, such as Forbes, Techradar, PC World, Techcrunch, etc. Further, it is also popular and trusted by millions of users globally.

https://duckduckgo.com/?q=how+to+spy+iphone+remotely&t=newext&atb=v377-1&ia=web

Existuje cesta - iCloud



App

ARE IPHONE SPY APPS UNDETECTABLE?

Yes. iPhone spy software is designed to be undetectable. These wouldn't be very effective hidden spy apps for iPhones if people were able to track them!

CAN I SPY ON AN IPHONE WITHOUT TOUCHING IT?

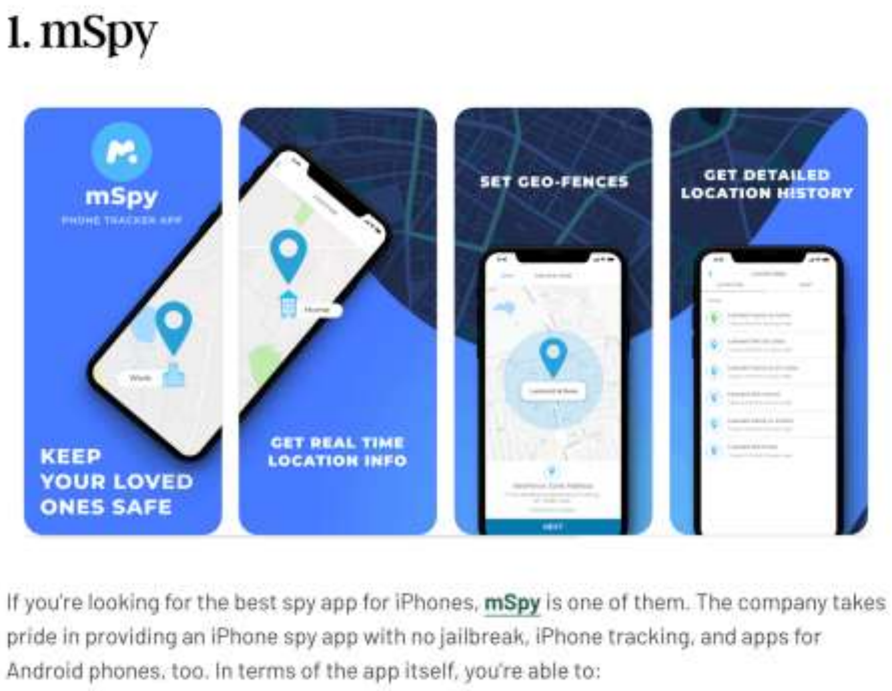
Yes. All iPhones are backed up to Apple's iCloud service. Since this is cloud storage, phones are able to access this without the need to jailbreak their iPhone. Furthermore, this cloud storage allows you to spy on an iPhone without installing software on it.

HOW DO I KNOW IF MY IPHONE IS COMPATIBLE WITH THE SPY APP?

The best iPhone spy apps should be compatible. Considering they're available on Apple's App Store, the app itself has had to go through rigorous testing and meet certain standards. Of course, ensuring it works on iPhones is one of those tests.

DO I NEED TO JAILBREAK THE TARGET IPHONE TO SPY ON IT?

No. As mentioned before, because you can access iCloud storage, any iPhone spy app should be able to gain access with no issues.



1. mSpy

mSpy
PHONE TRACKER APP
KEEP YOUR LOVED ONES SAFE
GET REAL TIME LOCATION INFO
SET GEO-FENCES
GET DETAILED LOCATION HISTORY

If you're looking for the best spy app for iPhones, mSpy is one of them. The company takes pride in providing an iPhone spy app with no jailbreak, iPhone tracking, and apps for Android phones, too. In terms of the app itself, you're able to:

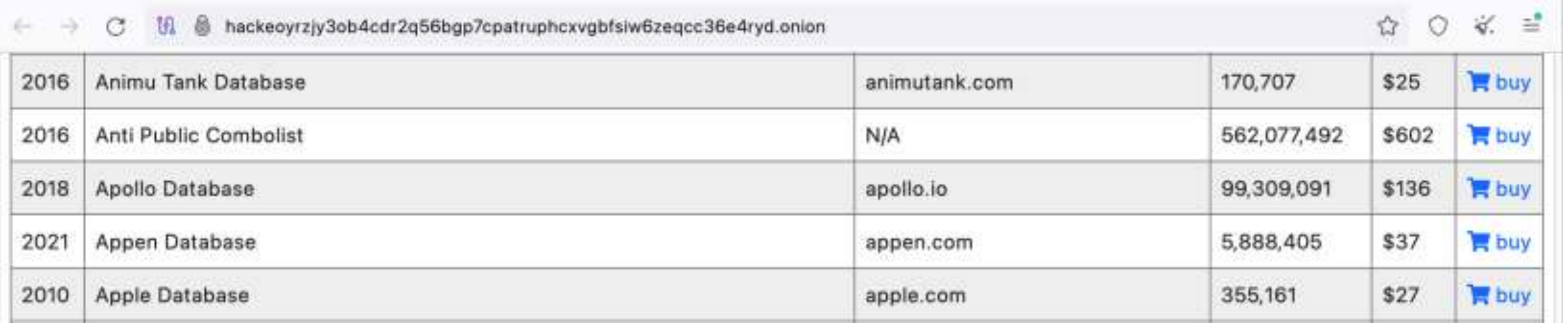
https://www.lifehack.org/881462/best-spy-apps-for-iphone

Jak získat AppleID

Fyzický přístup k zařízení

Sdílené přístupy

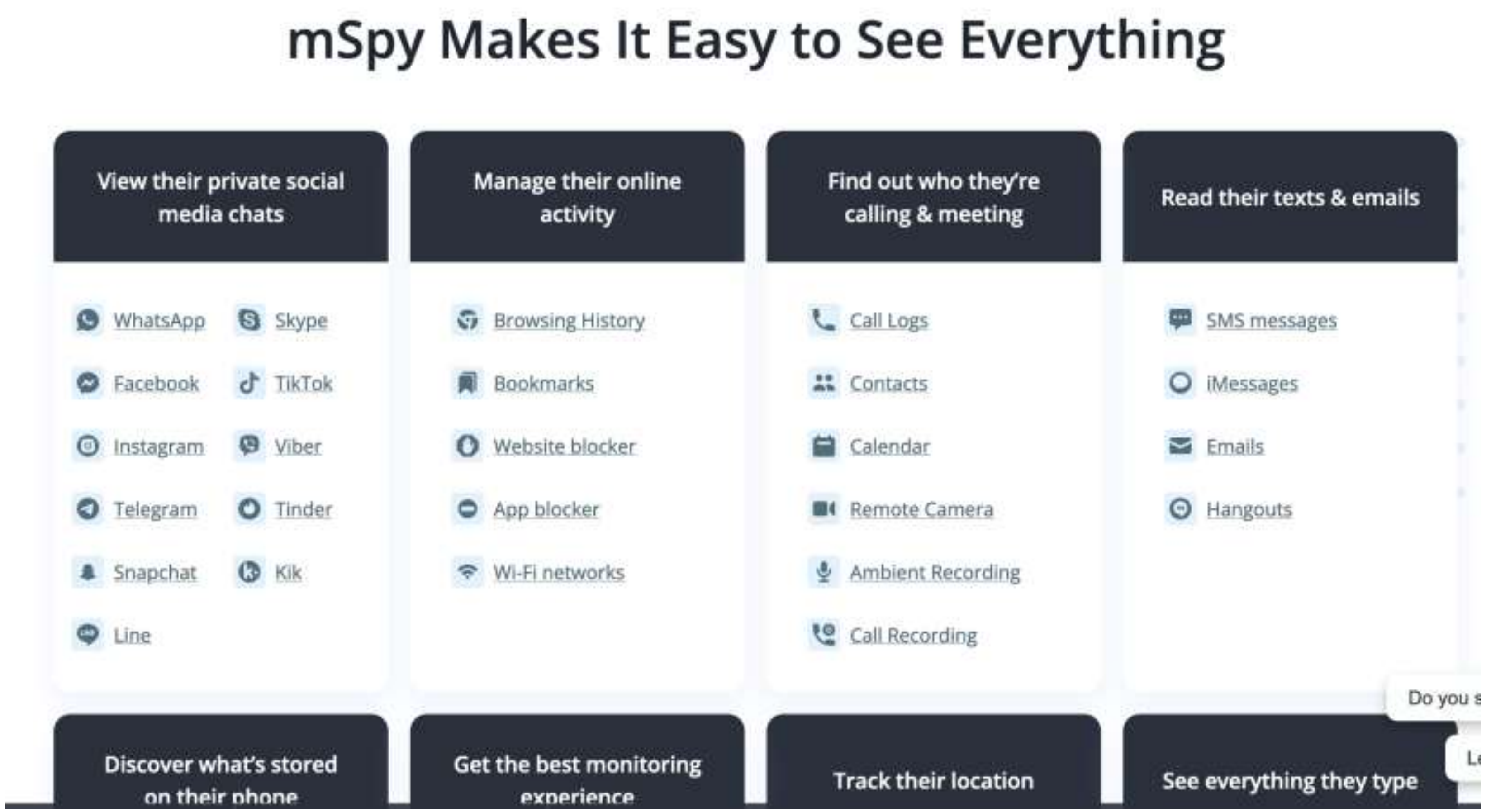
Databáze uniklých autentizačních údajů



hackeoyrzjy3ob4cdr2q56bgp7cpatruphcxvgbfsiw6zeqcc36e4ryd.onion

2016	Animu Tank Database	animutank.com	170,707	$25	buy
2016	Anti Public Combolist	N/A	562,077,492	$602	buy
2018	Apollo Database	apollo.io	99,309,091	$136	buy
2021	Appen Database	appen.com	5,888,405	$37	buy
2010	Apple Database	apple.com	355,161	$27	buy

Co umí mSpy



mSpy Makes It Easy to See Everything

View their private social media chats

- WhatsApp
- Skype
- Facebook
- TikTok
- Instagram
- Viber
- Telegram
- Tinder
- Snapchat
- Kik
- Line

Manage their online activity

- Browsing History
- Bookmarks
- Website blocker
- App blocker
- Wi-Fi networks

Find out who they're calling & meeting

- Call Logs
- Contacts
- Calendar
- Remote Camera
- Ambient Recording
- Call Recording

Read their texts & emails

- SMS messages
- iMessages
- Emails
- Hangouts

Do you s

L

Discover what's stored on their phone

Get the best monitoring experience

Track their location

See everything they type

https://www.mspy.com/features.html

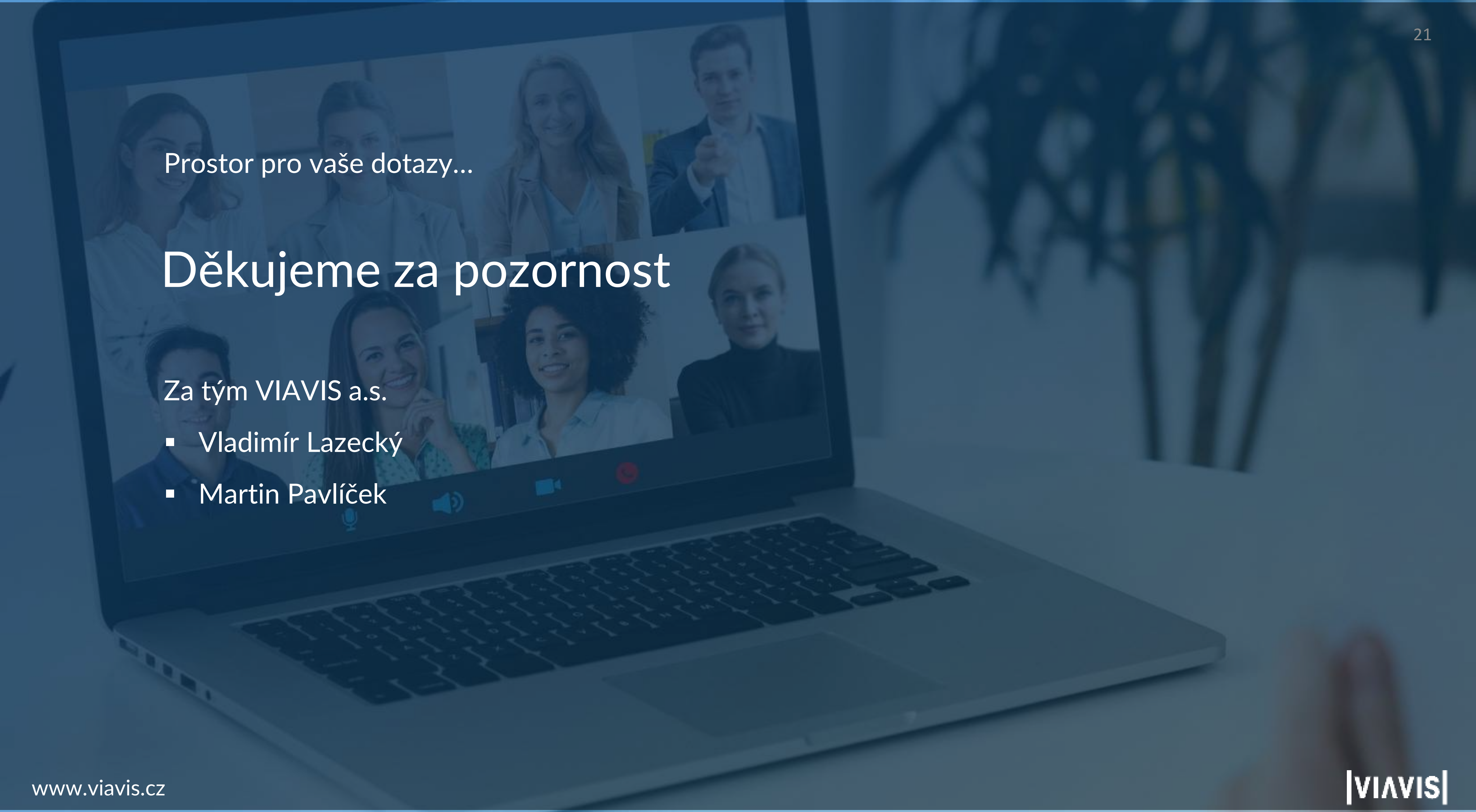
Poučení z příběhů?

- ✓ Některým incidentům se lze vyhnout obtížně
- ✓ **Některým naopak velmi snadno**

Jak se dalo incidentům předejít?

Poučení z příběhů?

- Vše zlé je pro něco dobré…
  - Klíčoví manažeři reagují na témata osobní bezpečnosti
  - Bezpečnost organizace následuje v závěsu
- Vysvětlování principů KB
  - Pochopení
  - Návyky
  - Technologie
- **Není to recept, ale funguje to o něco lépe**



Prostor pro vaše dotazy…

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký
- Martin Pavlíček