Cybercrime on Telegram: How Hackers Are Using the Messaging App to Share Data Leaks and Hacks

vpnmentor.com/blog/cybercrime-on-telegram

Telegram, the semi-encrypted messaging and chat app seen as a rival to Whatsapp, has always received a lot of negative attention as a safe harbor and essential tool for extremist hate groups, conspiracy theorists, child pornographers, and so on.

Now, it appears **cybercriminals are also flocking to Telegram to share and discuss massive data leaks exposing millions of people** to unprecedented levels of online fraud, hacking, and attack.

vpnMentor's cybersecurity research team joined several cybercrime-focused Telegram groups and channels to learn more about how and why the app has become so popular amongst hackers and threat actors.

We discovered **a vast network disseminating data leaks and dumps amongst 1,000s of people** and openly discussing how to exploit them in various criminal enterprises.

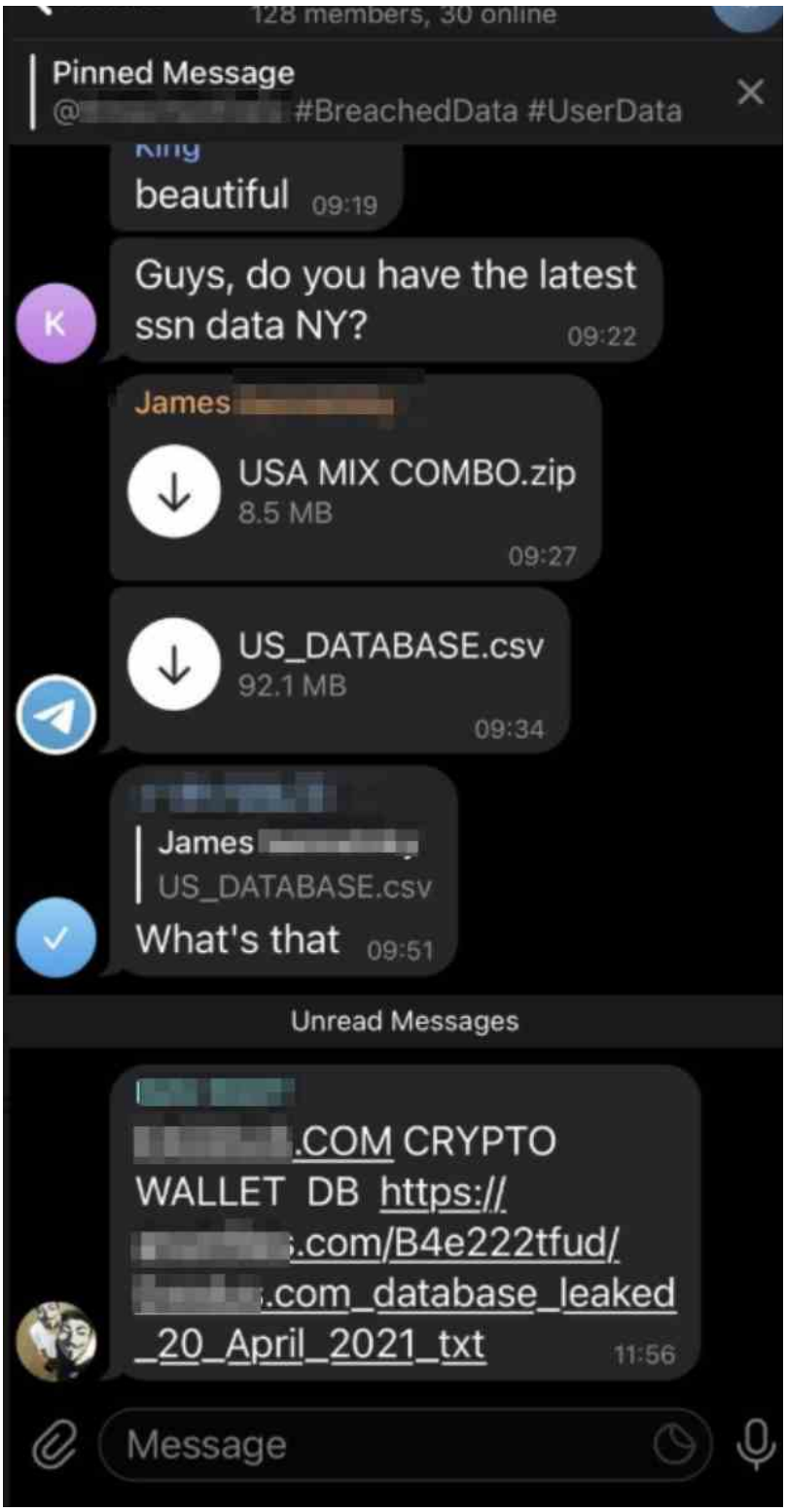
How are Hackers using Telegram?

Hackers are sharing data leaks on Telegram in two different ways.

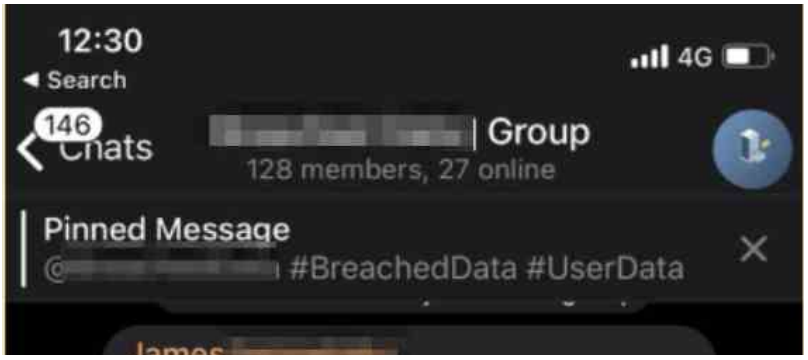
First, there are Telegram channels, where hackers post data dumps with brief explanations about what people can find inside. These channels are more passive, with minimal conversation happening in them. **Some channels have 10,000s of followers.**

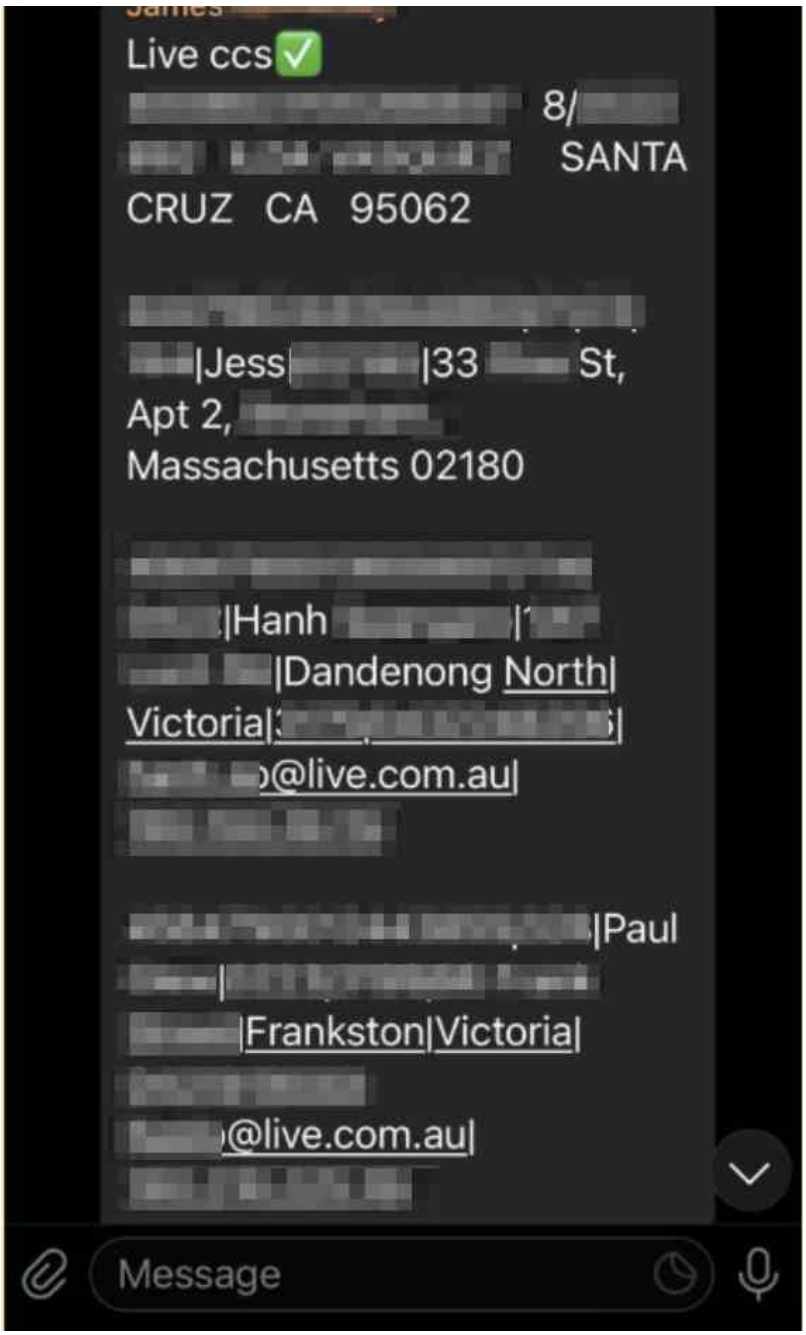
Data dumps shared on a hacking channel.

The other method hackers are using is **dedicated hacking groups, where hundreds of members actively discuss various aspects of cybercrime** and how to exploit data dumps shared.



Chat in a Telegram hacking group.





Examples of data shared directly in a group.

In general, it appears **that most data leaks and hacks are only shared on Telegram after being sold on the dark web** – or the hacker failed to find a buyer and decided to share the information publicly and move on.

Some of the data leaks were months old, but many were as recent as a few days.

Hackers have also used Telegram as part of cyber attacks and blackmail schemes. After hackers stole a database from Israeli company Shirbit, they created a Telegram group and started sharing sensitive information as a form of extortion against the company.

Why Post Leaks on Telegram?

Traditionally, hackers have relied on the dark web or other anonymous forums to share, discuss, and sell information about data leaks and successful hacks.

However, Telegram offers numerous advantages.

The app claims to be incredibly focused on guaranteeing privacy for its users. **The only thing you need to join is a mobile phone number, which is supposedly hidden from all other users, but visible to Telegram and SMS verification.** In theory, law enforcement could request the phone number of a Telegram user, or hackers could break in and steal it.

Creating Telegram channels and groups also saves criminals from registering with a web host or domain service, shielding them from attacks like DDoS, and reduces the need to protect their operations from online scanners and security tools.

Telegram also offers a much lower barrier to entry, both for people distributing data and those hoping to receive it. Telegram is considerably more accessible than the dark web, which requires specific technical know-how to access and navigate, and more robust safety and privacy measures. **Hackers can reach a much wider audience and share information a lot quicker** on an app installed on a device or computer.

Throughout our research, we witnessed members of these groups downloading zip files of data dumps and then asking how to open them, or what tools they needed to use them. This shows that even people with incredibly low computer literacy (and probably not on the dark web) are gaining access to incredibly sensitive data belonging to millions of people.

Most likely, they're also not storing this data in any secure fashion, creating another set of issues and concerns.

Telegram also offers malicious hackers and cybercriminals considerable scope for automating their activities. Telegram bots allow developers to run third-party apps on the platform. Usually, companies use the technology for advertising and marketing campaigns. **Hackers can use the bots to run their operations** while remaining in the shadows and spread their influence more easily across chats and groups.

Finally, **Telegram has proven incredibly slow at tackling how much illegal and dangerous activity takes place on the app.** Hackers know they can most likely remain anonymous and shielded from surveillance or basic accountability.

What Is Telegram doing to Combat These Groups?

Telegram has taken limited steps to shut these groups down, but some are operating for months before any action is taken. In that time, they can openly share private data from millions of people.

Some group admins also create a 'backup' group, ready to accept new members

and pinned to the top of the group. This way, members know to join the 'backup' group if the primary one is shut down. Thus, they can continue on the backup as if nothing happened.

In contrast, **Telegram has shown much greater enthusiasm in shutting down problematic groups in other areas, such as piracy.** The company consistently closes any groups or channels sharing copyrighted material amongst users.

Thus, it appears that **when they feel liable for legal action due to activity on the app, Telegram's owners are happy to step in** – and they keep a close eye on activity happening on the app.

Telegram is Not as Private as it Claims

Despite its growing popularity as a privacy-focused communications app, **most of Telegram's claims for high privacy standards are misleading**.

Telegram is **incredibly secretive and operates with zero transparency.** Two Russian brothers started the company, spent years moving around in different cities, before settling in Dubai. The company doesn't officially disclose where its team members or offices are based.

Their encryption is 'homemade' by the founders, and it's been widely criticized by experts. The company claims to be open-source, which is an exaggeration at best. The most crucial part of its system – the servers – remain a closed black-box.

And finally, **Telegram doesn't disclose what data it collects from users, how it's used, or who they share it with.** Their promised "transparency report" remains empty to this day despite numerous data requests from various governments.

These are just some of the many red flags surrounding the company.

For both criminal and ethical hackers, the illusion of pseudo-anonymity on Telegram could backfire incredibly if the company ever decided to exploit its access to their data, identity, and activity. Or if there was another data breach on the app itself. This already happened once, in 2020, when millions of Telegram users were exposed.

Examples of What Our Team Saw on Telegram

The following are a sample of the biggest and most concerning data dumps our team viewed as members of the Telegram groups in the last six months.

Disclaimer: we didn't discover these data breaches. They are currently being shared online across Telegram and, potentially, other platforms. Anyone who thinks they could be affected should be extra careful and vigilant for potential threats, such as account takeovers, phishing scams, identity theft, viral attack, and fraud.

If you're concerned about these data breaches, change your login credentials for any accounts online, learn how to spot phishing emails, and take some steps to improve your online privacy.

Playbook Sports

From: Appeared on Telegram on February 24th, 2021

Size: 800 MB

Website: http://playbooksports.com/

Data from 100,000s of US citizens, including information about online gambling activity and purchases made on the website's store.

The exposed data included:

- Usernames
- Passwords
- Full names
- Email addresses
- Home and business addresses

4Shared

From: Appeared on Telegram on April 10th, 2021

Website: 4shared.com

4Shared is a file-sharing website in which users can send one another a link to download media files.

A hacker was able to obtain a list of 3.5 million files uploaded to 4Shared.

These included pirated movies, music, books, along with personal items like photos and videos.

There were also links to 4Shared user profiles. The profiles only contained usernames, but these could still be used to find additional information. A few days after being shared on Telegram, the URLs were deactivated, and the content was no longer accessible.

Our team even discovered 'phishing kits' being shared between people targeting financial institutions for fraud among the files on the data dump. These illegal phishing kits exposed the person's name behind the scam and how they planned to target institutions in a criminal scheme.

Cayman National Bank and Trust (Isle of Man)

From: Originally leaked in 2019; appeared on Telegram again in 2021

In 2019, hacktivist Phineas Fisher released the ‘Sherword’ data dump containing a client list of an off-shore bank based in the Cayman Islands and Isle of Man (along with other destinations).

The data breach was shared again more recently on Telegram. This is an example of an old data breach that is shared on Telegram to reach a much wider audience than when it was initially revealed.

Click.org

From: Originally leaked in December 2020; appeared on Telegram in April 2021

Size: 35 GB

Website: click.org

Click is a marketing software provider that was breached in late December 2020. The breach has since surfaced on a Telegram group.

The data dump comprised 35GB of data, including an SQL dump with 2.7 million logs of transactions made by click.org users.

The exposed data included:

- Full names
- Home address
- Business email addresses for Click.org affiliates
- URLs allowing viewing and downloading of invoices

Meet Mindful

From: Appeared on Telegram in January 2021

Website: https://www.meetmindful.com/

A hacker released private data and account information from 2.28 million users on the Meet Mindful dating site on the dark web, and it appeared later on Telegram.

The exposed data included:

- Real names
- Email addresses
- City, state, and ZIP details
- Physical attributes
- Dating preferences
- Marital status

- Birth dates
- Latitude and longitude
- IP addresses
- Bcrypt-hashed account passwords
- Facebook user IDs
- Facebook authentication tokens

Facebook Data Dump

From: Originally leaked in 2019, appeared on Telegram in April 2021

Many people are now aware of a massive data breach in Facebook that occurred in 2019. At the time, the company was aware of the breach but chose not to report it to users or authorities.

The data for 533 million Facebook users were made available by hackers in April 2021 and made headlines worldwide.

However, before the story became viral, it was also possible to download the data from Telegram.

Unknown Source

From: Originally leaked circa. April 12th, 2021; appeared on Telegram on 23rd April 2021

Size: 26 GB

A database from an unknown source, with detailed files on up to 250 million US citizens. (depending on duplicate entries). The data was arranged into datasets based on households, suggesting it was harvested as part of a large-scale research or survey project.

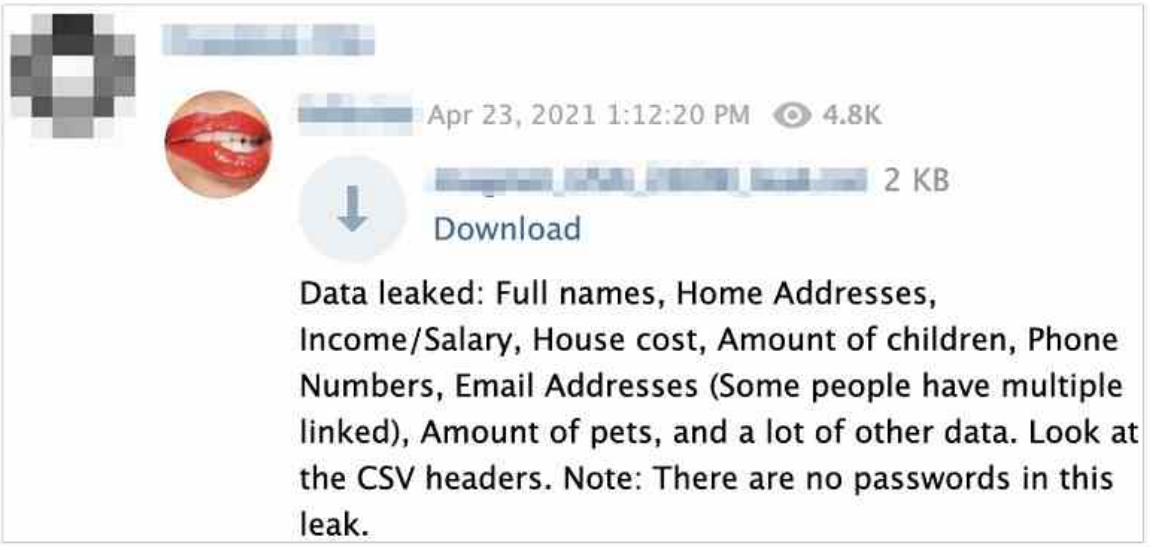
Each dataset contained a massive amount of incredibly detailed information about the individuals within a household.

The exposed data included:

- Full contact details (name, address, email, phone, dob);
- Hobbies
- Political affiliations and donations;
- Ailments and illnesses
- Marriage status
- Number of children
- Income(s)
- House price
- Ethnicity
- Location coordinates

- Pets

The following is a screenshot from a Telegram group in which the data dump was shared as a CSV file for anyone to read.



A hacker shares private data from up to 250 million US citizens

Mega-Dump: “open data.7z”

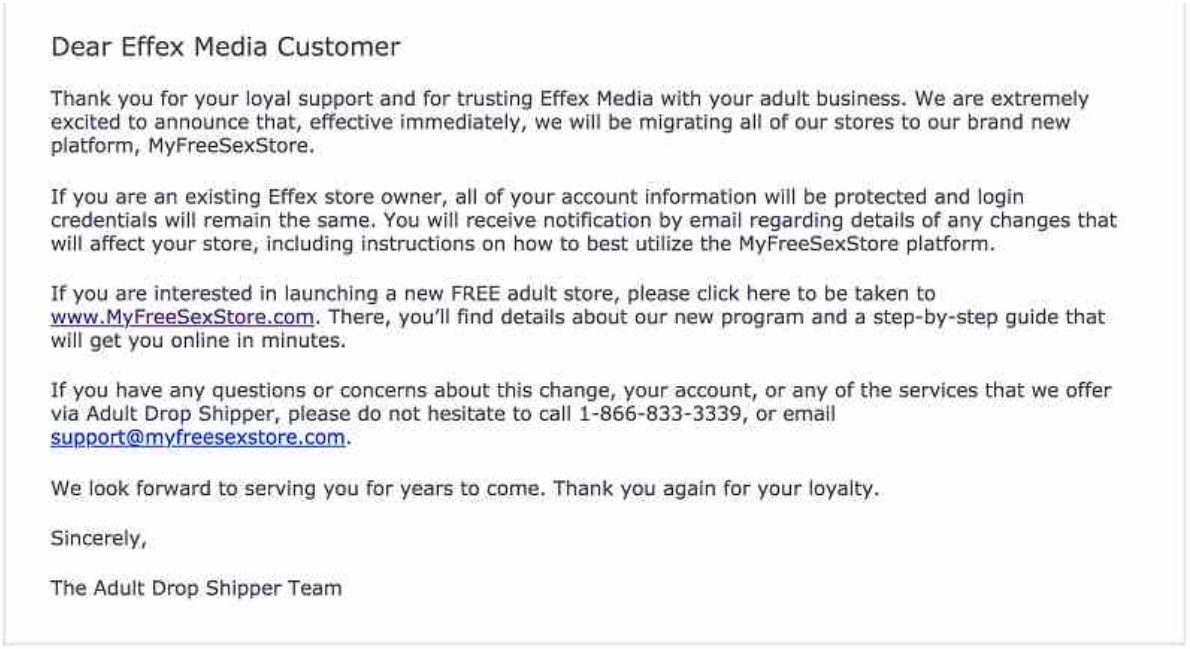
One of the biggest data breaches we saw in our research was a truly massive dump of data from 670 websites, including **a network of porn websites and their affiliates.**

The hacker responsible shared over 515MB of data from the company Effex Media. **The giant data dump contained hundreds of smaller dumps from various websites managed and owned by Effex Media, and affiliate websites selling the companies’ products.**

Each of these dumps exposed the private data for dozens of individuals who had signed up to the websites or bought products from one of their online stores.

Effex Media owns several lesser-known porn websites, such as seymourbutts.com, airerose.com, and bustynetwork.com. Each of these, and many more, were included in the data breach.

Effex Media also works with a network of ‘dropshipping’ stores to sell its products online. Dropshipping stores are online retailers who never stock any products but simply act as a middleman connecting a consumer trying to buy a product with a supplier selling it (in this case, Effex Media).



Dear Effex Media Customer

Thank you for your loyal support and for trusting Effex Media with your adult business. We are extremely excited to announce that, effective immediately, we will be migrating all of our stores to our brand new platform, MyFreeSexStore.

If you are an existing Effex store owner, all of your account information will be protected and login credentials will remain the same. You will receive notification by email regarding details of any changes that will affect your store, including instructions on how to best utilize the MyFreeSexStore platform.

If you are interested in launching a new FREE adult store, please click here to be taken to www.MyFreeSexStore.com. There, you'll find details about our new program and a step-by-step guide that will get you online in minutes.

If you have any questions or concerns about this change, your account, or any of the services that we offer via Adult Drop Shipper, please do not hesitate to call 1-866-833-3339, or email support@myfreesexstore.com.

We look forward to serving you for years to come. Thank you again for your loyalty.

Sincerely,

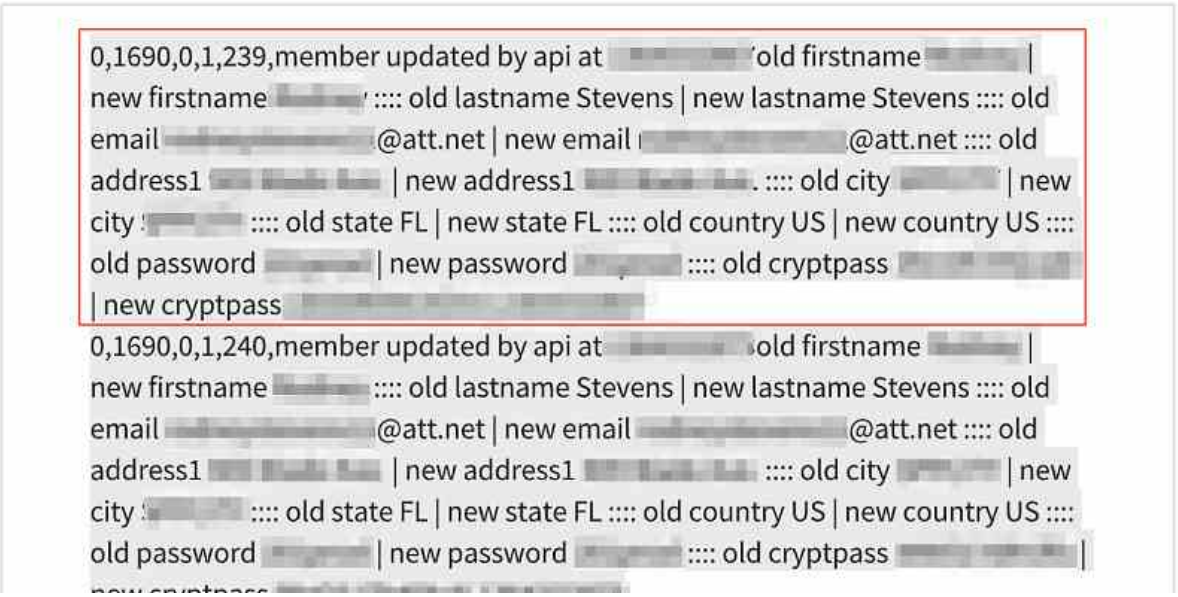
The Adult Drop Shipper Team

Homepage message on the Effex Media website.

Between the data hackers obtained from Effex Media's websites and those of its affiliates, **we were able to view a massive amount of private and compromising data from the people using these sites, including:**

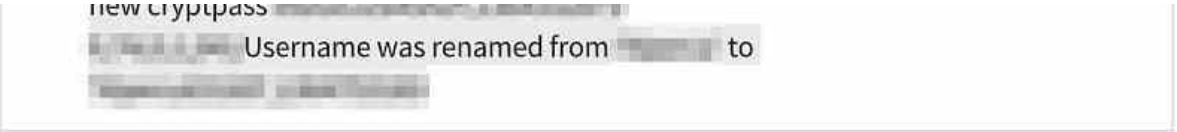
- Names
- Email
- Home addresses,
- Payment records
- cleartext Account passwords for memberships and online stores
- IP addresses
- Timestamps for activity on sites

The following are samples of user and customer data from Effex Media websites and their affiliates.

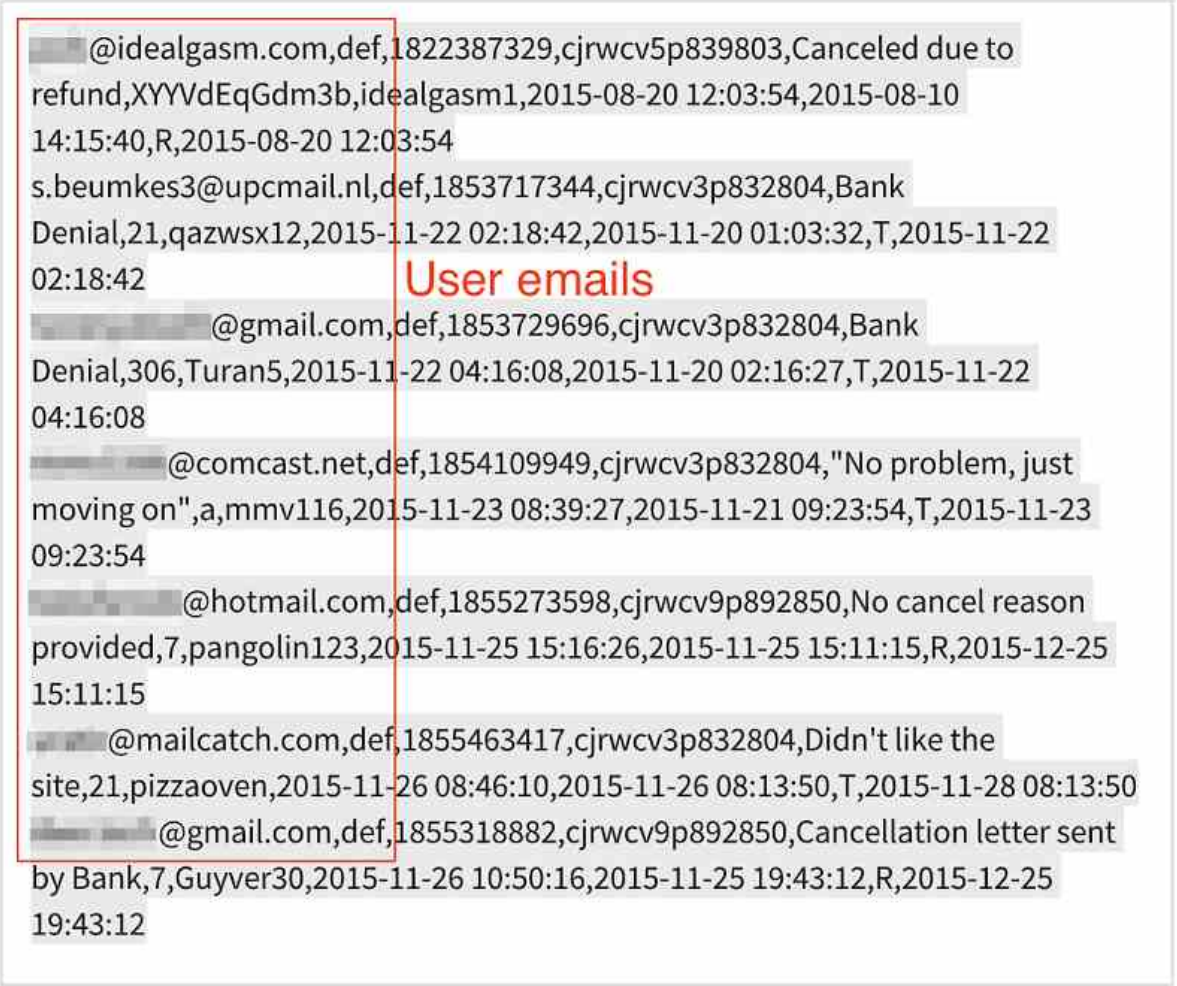


0,1690,0,1,239,member updated by api at [redacted] old firstname [redacted] | new firstname [redacted] :::: old lastname Stevens | new lastname Stevens :::: old email [redacted]@att.net | new email [redacted]@att.net :::: old address1 [redacted] | new address1 [redacted] :::: old city [redacted] | new city [redacted] :::: old state FL | new state FL :::: old country US | new country US :::: old password [redacted] | new password [redacted] :::: old cryptpass [redacted] | new cryptpass [redacted]

0,1690,0,1,240,member updated by api at [redacted] old firstname [redacted] | new firstname [redacted] :::: old lastname Stevens | new lastname Stevens :::: old email [redacted]@att.net | new email [redacted]@att.net :::: old address1 [redacted] | new address1 [redacted] :::: old city [redacted] | new city [redacted] :::: old state FL | new state FL :::: old country US | new country US :::: old password [redacted] | new password [redacted] :::: old cryptpass [redacted] |



PII data from a member of an Effex Media website.



Users canceling membership on Effex Media website.

PII from Effex Media affiliate website

Implications and Impact

The fact that so many hackers and cybercriminals (not to mention would-be 'fans' of cybercrime) have adopted Telegram is **a serious escalation in the ongoing surge of cybercrime.**

Those involved in illegal hacking, online fraud, and other criminal activities have clearly gotten used to almost zero accountability. They've grown increasingly bold, and seemingly have no qualms about openly discussing their activities on a semi-public messaging app.

In doing so, they could significantly increase the scope of their own malicious activities and inspire many people to give cybercrime a go, making it look easy and risk-free. This could create a devastating ripple effect across the globe.

Governments and cybersecurity organizations are already struggling to keep up with the growing scale and frequency of cyber attacks, hacking, and online fraud. There are an estimated 3.5 million unfilled cybersecurity jobs in 2021, as employers struggle to meet the demand with adequately trained staff.

If a whole generation of amateur hackers hanging out on Telegram was inspired to pursue cybercrime, the impact could be devastating. Whether or not they were successful, **chasing down and prosecuting these amateurs would be a huge drain on already strained efforts, taking valuable resources away from monitoring and combating bigger criminals and cyber attacks.**

And while we're not exactly sympathetic to the people using Telegram to celebrate and distribute their hacks, they may eventually regret doing so.

Telegram operates in secrecy, with zero transparency or accountability. The company never shares any details about how it monitors users or their data – or who it shares this information with.

Using Telegram for illegal pursuits could backfire spectacularly – for both the hackers sharing their work, and the people following them.

So, hopefully, Telegram will finally start addressing this issue.

The Bottom Line

The discovery of thriving criminal hacking communities on Telegram represents a troubling new chapter in the worsening epidemic of cybercrime spreading across the globe.

If the company doesn't step in and address the issue, or regulators and government don't force it to, **Telegram's cybercrime communities threaten the safety and security of millions of people.** Furthermore, they could turn cybercrime into an amateur pursuit, in which even someone with limited computer literacy can pursue potentially devastating criminal schemes.

While these communities represent a major escalation, **they could simply be a small step towards cybercrime becoming a mainstream pastime.**

About Us and Previous Reports

vpnMentor is the world's largest VPN review website. Our research lab is a pro bono service that strives to help the online community defend itself against cyber threats while educating organizations on protecting their users' data.

Our ethical security research team has discovered and disclosed some of the most impactful data breaches in recent years.

This has included a group of free VPNs secretly tracking their users' activity and data and leaking it online. We've also uncovered potential criminal activities and scams targeting users on Spotify, Instagram, and Facebook.

You may also want to read our VPN Leak Report and Data Privacy Stats Report.

Help Us Protect The Internet!

Introducing The Leak Box

The Leak Box is hosted on the Dark Web and allows ethical hackers to anonymously report any data breach they find online. Alternatively, anyone can submit a breach here on vpnMentor, any time, from anywhere, without compromising your privacy.

About the Author

vpnMentor Research Team Cybersecurity and Research Lab

vpnMentor Research Lab is a pro bono service that strives to help the online community defend itself against cyber threats while educating organizations on protecting their users' data. Our ethical security research team has discovered and disclosed some of the most impactful data breaches in recent years.

Honesty and Transparency are two core values of vpnMentor. VPN Companies can't pay to change or delete reviews. When readers choose to buy a vpn service, we sometimes

earn affiliate commissions that support our work. Here is an explanation of exactly what we do, and how to support our work.