# CHOOSING YOUR VPN: A MATTER OF TRUST

Internet Users Rely on VPNs For Privacy –
But Well-Known Providers Have a Questionable Track Record


digitalcitizens alliance | whitebullet

November 2023

# Table of Contents

# Executive Summary

Virtual Private Networks, known as VPNs, are used by many people to shield their online identity, activities, and location. VPNs have laudable uses, from enabling the anonymity of whistleblowers and political dissidents to safeguarding business communications from cyber intrusions – especially for those working remotely.

Overall, VPNs represent a $50 billion global market, and an estimated 1.6 billion Internet users rely on VPNs. About a third of those users are required to use a VPN to access work email and files and therefore have no role in selecting the company that provides the service. But for the rest, deciding whether to use a VPN and, if so, which one to trust, can have profound implications for their privacy.

By subscribing to a VPN, an Internet user entrusts the VPN with a significant amount of personal data. Once a user signs up, the VPN can know:

- The user's name and credit card information, accessible when the user pays to subscribe;
- The user's exact IP address and geolocation, accessible because the user links their device to the VPN;
- And, most siginifcantly, the user's every action taken online, including every website visited and every activity undertaken on that website.

Users may believe that VPNs take great pains to keep all these highly sensitive data completely safe – after all, VPNs' marketing is all about how they protect and enhance privacy.  And most Internet users in the U.S. believe that VPNs are regulated by the government, a reasonable assumption given the confidential personal information they are privy to. In fact, however, VPNs are not directly regulated.

Many people may also assume that it doesn't much matter which VPN they choose. But not all VPNs equally deserve users' trust. In 2020, for example, seven VPNs left user data for roughly 20 million people – data which they had claimed they were not collecting – unprotected on a cloud server.

And Internet users who might expect a VPN to face swift and severe regulatory punishment for such breaches of trust, as an ISP might endure, might be surprised to learn that VPNs that advertise to the public face no direct regulatory oversight in the United States from the Federal Communications Commission or state entities.

This report, a joint investigation by Digital Citizens Alliance and White Bullet, found that many VPNs have a dubious track record that includes breaking promises to safeguard their customers' privacy, engaging in shady efforts to woo potential customers, and associating with entities in the dark underbelly of the Internet known to target users for harm.

People considering using a VPN may be disturbed to learn that:

- While relying on online reviews is the most common way people choose a VPN service, some review sites aren't the independent and neutral arbiters they pretend to be. For example, Kape Technologies, the owner of ExpressVPN, acquired VPN review sites in 2021, raising the question whether Internet users can now trust that those reviews are truly independent.

- While VPNs tout privacy, some associate themselves with illegal content theft websites – a nefarious $2.3 billion dollar industry that has been demonstrated to intentionally expose their users to malware designed to violate their privacy. The investigation found that VPN providers spend an estimated $45 million a year advertising on piracy sites.

- Users may not realize that their VPN provider logs their online activities. Free VPNs may make money by selling that data to third parties. VPNs claim to not retain user data. However, in 2020, seven VPNs left user data – which they claimed they were not collecting – for roughly 20 million people unprotected on a cloud server. The Center for Democracy and Technology – a well-respected tech think tank - has raised concerns that the claims made by VPNs that they protect user data have proven too often to be false.

These issues underscore why it's important for Internet users to choose wisely when considering whether to use a VPN. As the New York Times points out: "Many of the most popular VPN services are now also less trustworthy than in the past because they have been bought by larger companies with shady track records." The article warns: "That's a deal-breaker when it comes to using a VPN service, which intercepts our Internet traffic. If you can't trust a product that claims to protect your privacy, what good is it?"

Congress has also taken notice of these issues. Last year, Senator Ron Wyden and Representative Anna Eshoo urged the Federal Trade Commission to crack down on bad actors in the VPN industry: "It's extremely difficult for someone to decipher which VPN service to trust, especially for those in crisis situations. There are hundreds, if not thousands, of VPN services available to download, yet there is a lack of practical tools or independent research to audit VPN providers' security claims." These lawmakers point out a study that found that "75 percent of leading VPN providers misrepresented their products and technology or made hyperbolic claims about the protection they provide users on their websites…"

Concerns about how VPNs operate are compounded by a general lack of understanding about them. A Digital Citizens research survey conducted in October 2023 found that 54 percent of Americans weren't sure whether they used a VPN. Only 1 in 5 reported having a strong understanding of a VPN's purpose.

The survey of 1,318 Internet users also found that a majority believe that VPNs are regulated – when in fact these services are not subject to any regulation in the U.S. Indeed, only a small number of countries regulate or ban VPNs.

The importance of this point cannot be overstated. The Internet service providers that offer online access could also theoretically track user activity, but these are typically heavily regulated companies.

In comparison, VPN providers operate in the dark.

Given the important role that VPNs play, Internet users must have confidence in the service they use. And that starts by trusting that a VPN provider is a responsible actor. This report is designed to provide such users with knowledge about how VPN providers operate so they can make informed choices.

# VPNs – A Question of Need, A Matter of Trust

Even though an estimated 142 million Americans use a VPN, many have only a cursory understanding of how they work. VPN users who log on to the private network of their company may not even realize they are using a VPN to gain access to non-public information or connect remotely. Those who sign up individually may do so out of an abundance of caution or desire for privacy when accessing less secure public WiFi networks. Others may use VPNs out of fear that someone is snooping on their online activities.

Results from a new Digital Citizens survey supported the notion that VPNs are a popular way to protect users' privacy and prevent other from knowing what users are doing when they're online. When researchers asked 1,300 respondents what were their primary reasons for using a VPN – 30 percent said going to movie piracy sites, 27 percent included visiting adult content sites, 23 percent said gambling sites, while 13 percent acknowledged VPNs were used to visit sites that feature illegal content.

How does a VPN work? These services establish an encrypted point-to-point connection between a user's computer and the VPN. The only IP address that can be discerned upstream from the user's device is that of the VPN.  Thus, if the Internet Service Provider's logs for that device were examined, they would reveal no information about the user's location or activities. By cloaking the information, a VPN keeps a user's online activities and geo-location out of sight, in theory adding a level of privacy (if the provider doesn't expose the data).

There are important differences between a corporate VPN and a consumer or personal use VPN. A key distinction is a consumer VPN is typically used by one person for devices connected on a WiFi network. A corporate VPN is typically designed to be used by dozens to thousands of employees who need to create a secure and direct connection to a company's network.

The corporate and consumer markets also have distinct leaders. Cisco, Juniper, and Citrix are the go-to choices for business VPNs. In the consumer space, NordVPN, ExpressVPN, and Surfshark are among the most popular.

Whether typical Internet users need a consumer VPN is a matter of debate. Consumer Reports, a U.S. non-profit, advises: "For the average person accessing the web from their home WiFi, there's little reason to use a VPN service….if you are an activist, a journalist with sources to protect, or are at heightened risk because of who you are or what you do, a VPN might be part of the solution."

If Internet users choose to use a VPN, they should know what type of company they are choosing to trust. The track record of leading VPNs is decidedly mixed.

# VPN Reviews & Rankings: Conflict of Interest?

Imagine if a person interested in buying an automobile visited the Car and Driver Magazine website and found Toyota Corolla was the top- ranked car – and it turned out that the review site was owned by Toyota. That is what ExpressVPN does.

ExpressVPN is owned by London-based Kape Technologies. In the same year that Kape purchased VPN review sites such as VPNmentor it also acquired ExpressVPN.

Why is that problematic? Internet users rely heavily on online reviews to make a purchase, according to the Digital Citizens research survey.

In fact, online reviews were the most cited as the reason Internet users gave to why they chose a specific VPN:

| Reason for Choice of VPN Purchased | |
|---|---|
| Online Reviews | 34% |
| Advertising | 16% |
| Someone recommended | 14% |
| Recommendation from blog or non-review site | 13% |

VPNmentor includes a disclosure on its website about its ownership:

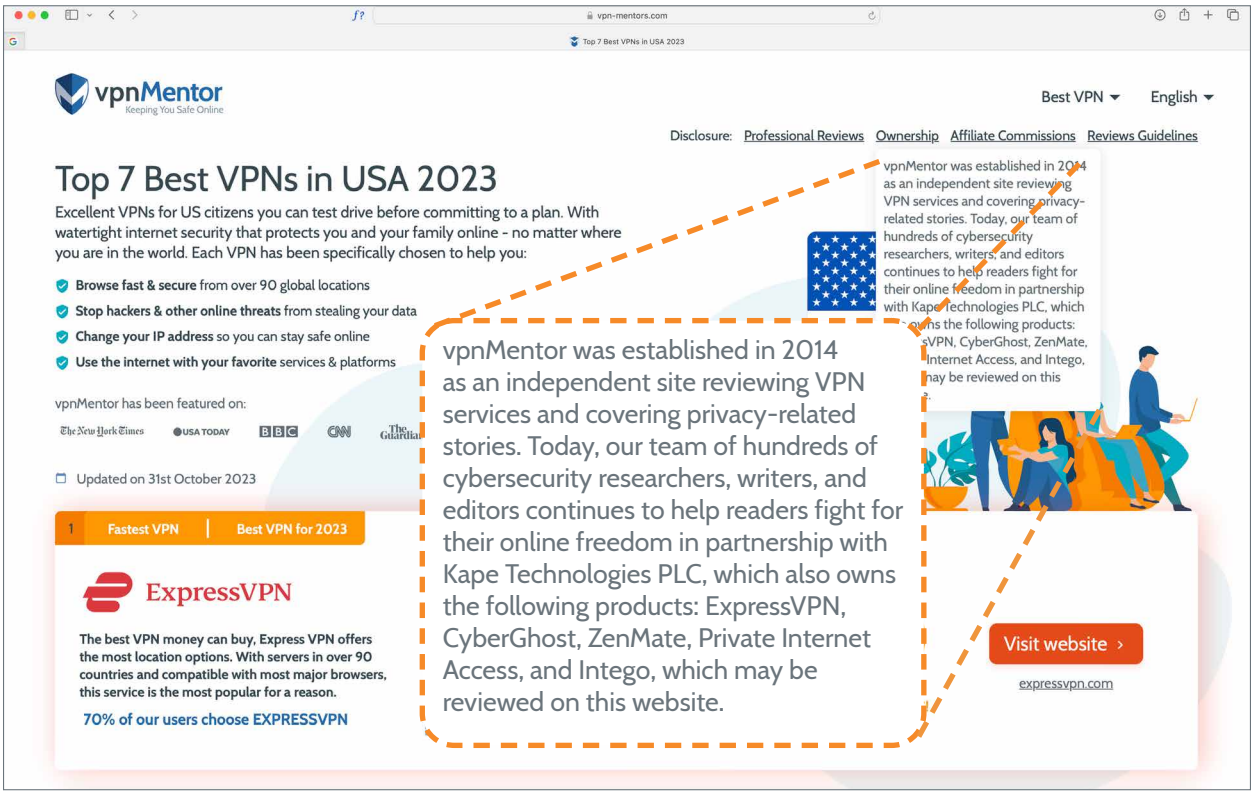


Image 1

When asked for comment, an ExpressVPN spokesperson stated that its review sites "continue to maintain their impartial editorial standards, and have been committed to doing so. Their editorial teams operate completely separately from ExpressVPN, and continues to review all products and services by the same strict and transparent evaluation standards. These sites also clearly and transparently share their links to Kape and other Kape-owned products."

Even taking ExpressVPN at their word, it is disconcerting that review sites that Internet users rely upon are owned by the parent company of one of the VPNs recommended.

And it's fair to question whether an average consumer would even think to investigate potential conflicts of interest between a review site and a product, or search for the fine print that spells out the ownership connection between VPNmentor and its number-ranked VPN.

Given these blurred lines, it can be challenging for Internet users to determine whether they need a service, and if so, which is the best one for them. Internet users should double-check whether the review site they are relying upon is independent of the VPNs it recommends.

# The Company VPNs Keep: Advertising on Piracy Sites

VPNs generally market themselves as necessary to provide an extra layer of privacy. One could expect that ads for such companies would not show up on sites that can jeopardize users' privacy. But they do. The investigation found that VPN providers spend an estimated $45 million annually advertising on piracy platforms. The most prominent advertisers included ExpressVPN and NordVPN.

Why is this disturbing? The links between piracy, malware, and credit card fraud have been well documented. Prior Digital Citizens investigations found that illegal online piracy is a $2.3 billion industry with deep and illicit relationships with shady operators that make tens of millions of dollars by installing malware into misleading ads.

As a follow up to earlier research, investigators decided to explore what advertising is among the most likely to appear on piracy sites. White Bullet investigators examined advertising on 1,278 piracy domains from April to May 2023. White Bullet found VPN ads on numerous piracy websites. ExpressVPN ads ran on piracy websites that have been put on "Watch Lists" that either governmental or industry bodies flagged as especially pernicious.

Here's an example of an ExpressVPN ad on a piracy site in image 2:


Image 2

When a user clicks on an ExpressVPN ad on a piracy site, they are redirected to the company's website with messages such as image 3 below.

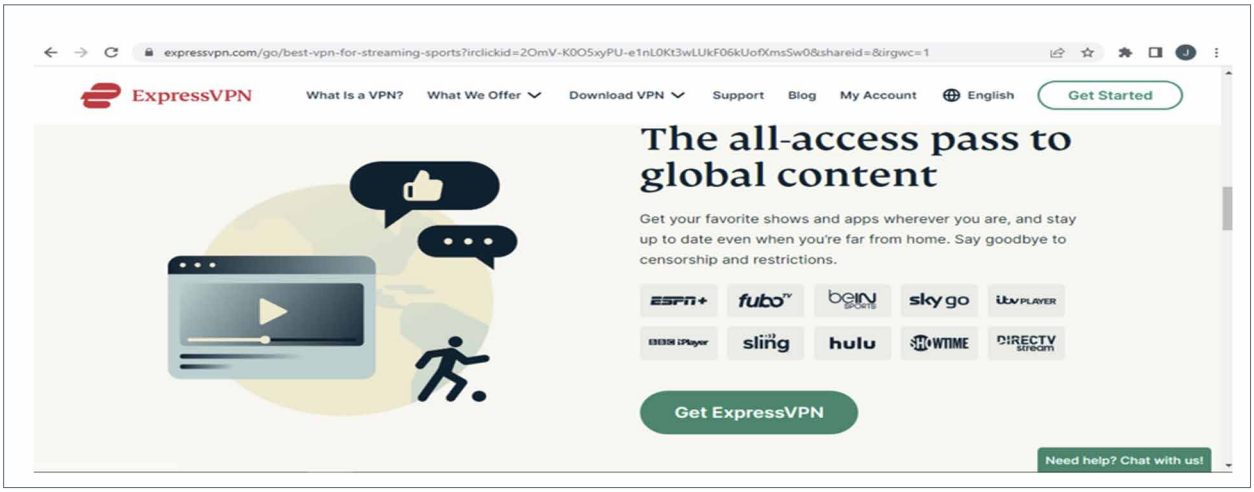


Image 3

This ExpressVPN United States-originated ad was found on the piracy site, tvseries.in. TVseries.in allows users to stream pirate films and television series for free, with numerous IP infringements reported from multiple rights holders.

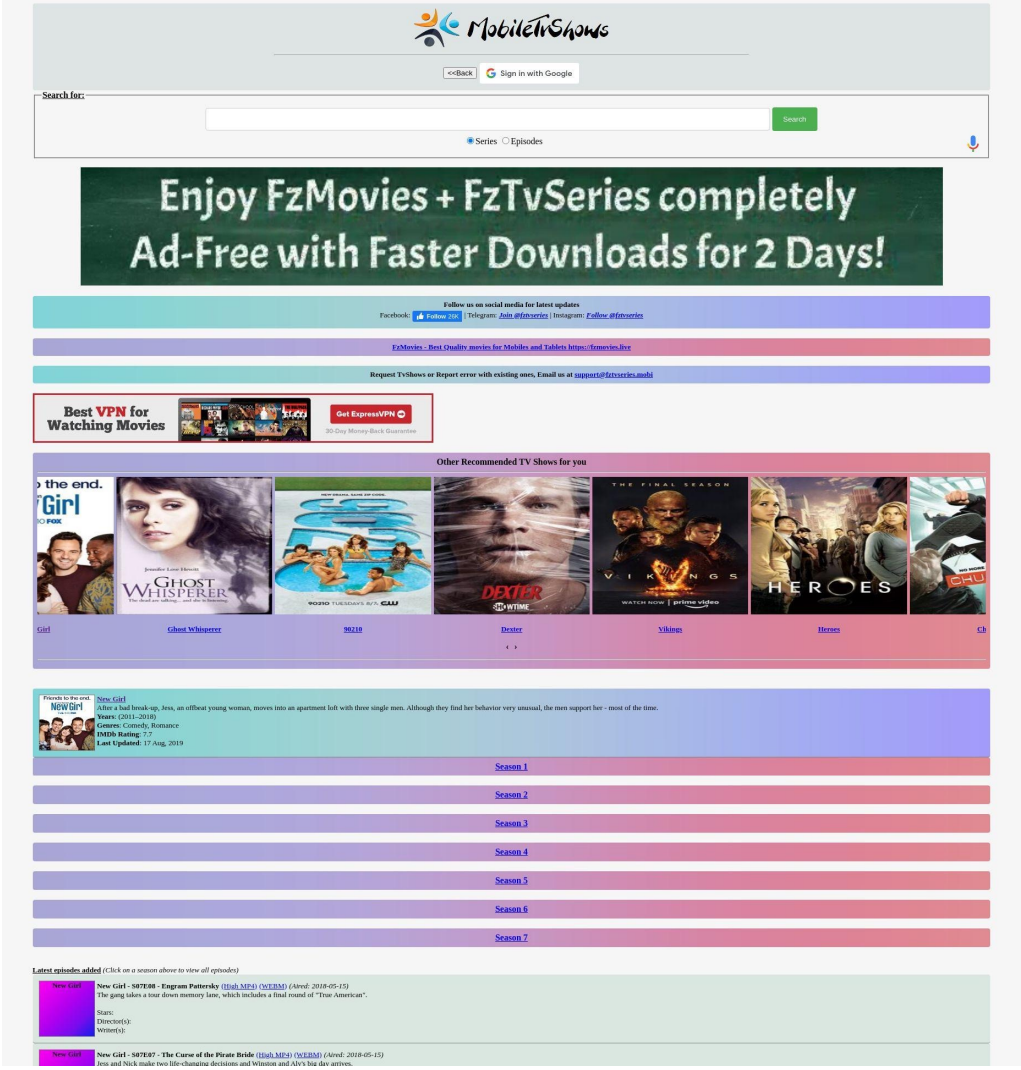


Image 4

The next example, naijaloaded.com.ng, includes both an ExpressVPN and gambling advertisements. Like others, naijaloaded.com.ng is on a Watch List.


Image 5

ExpressVPN sent the following response about the report's findings:

"Regarding advertising, ExpressVPN does not spend any advertising dollars on piracy sites, including during the period you cite of April to May 2023. We also have a very strict approval policy on our affiliate partnerships program, and we reject any torrenting/pirate sites. There have been rare instances where a torrent site slipped through the cracks by hiding under a sub-affiliate network (i.e., external affiliate program). To monitor this, we do regular checks on the sub-networks traffic sources and clearly state in our policy that we don't work with torrenting/pirate sites. We double checked both tvseries.in and naijaloaded.com.ng, and can confirm that they are not part of our affiliate program of any sort. We will investigate whether how this brand infringement is occurring, but we are confident we are not spending advertising or affiliate dollars with these sites. We do work with a brand protection agency to check for assets that are on sites like these and ask them to remove such unauthorised ads and use of our brand. We have flagged this to our agency for takedown."

NordVPN is perhaps the most prominent VPN provider in the world. It has an estimated valuation of $1.6 billion, sponsors the Spanish soccer club Atletico de Madrid, runs ads on prominent national television programs, and seems to aspire to become a publicly traded company. Its website states, "If you use a VPN illegally, you can lose your internet connection, be fined anywhere from a few hundred to hundreds of thousands of dollars, or face imprisonment."

Given this, you would think NordVPN would steer clear of being associated with piracy operators. Yet NordVPN advertised on 88 piracy sites across 26 countries during the period of the investigation. (It should be noted that NordVPN's advertising on piracy sites ebbed and flowed during the course of the investigation.)

The NordVPN ad in image 6 below, which originated in Bulgaria, appeared on the piracy site, flvto.com.mx. That piracy site is on a Watch List.

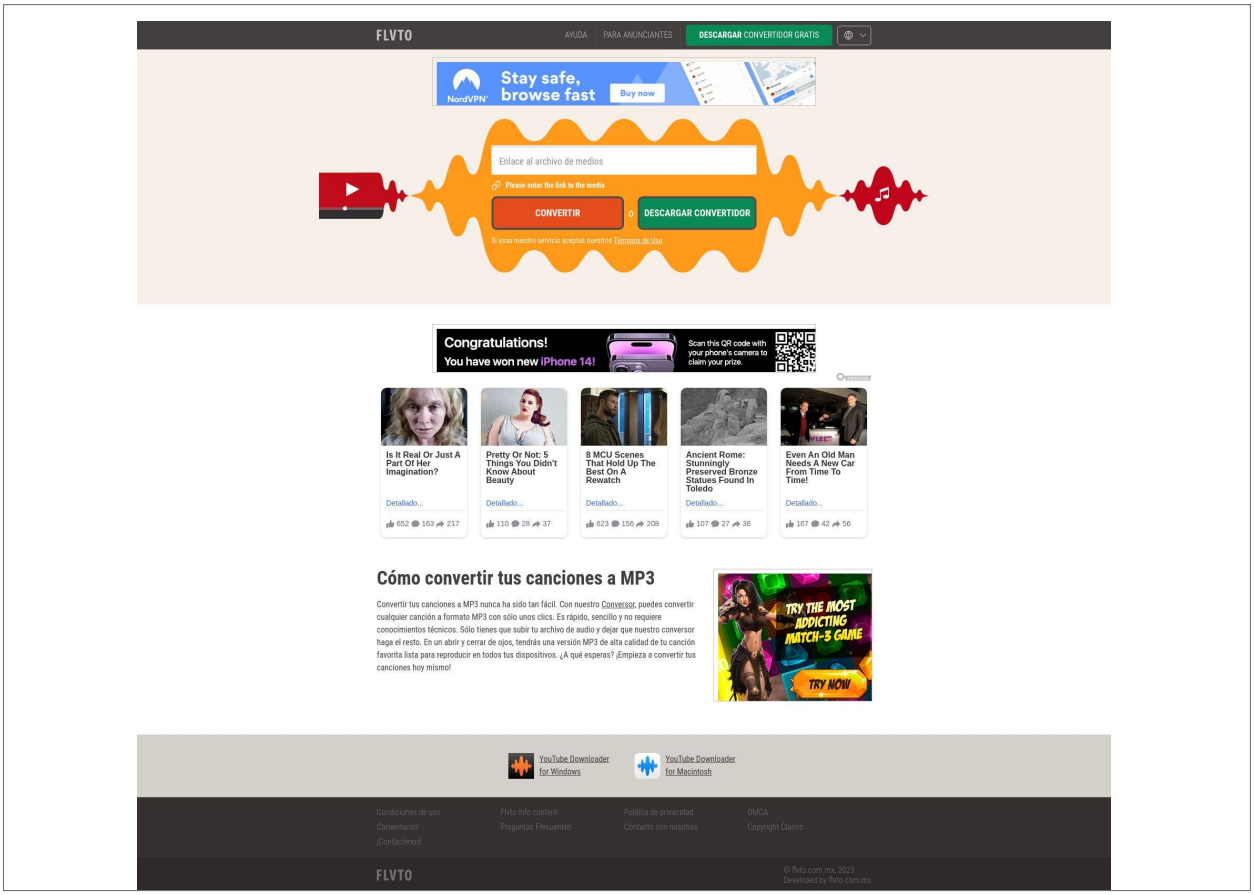


Image 6

This next ad, which originated in Italy, was found on the piracy site hdonline.cc. It is also on an industry Watch List.

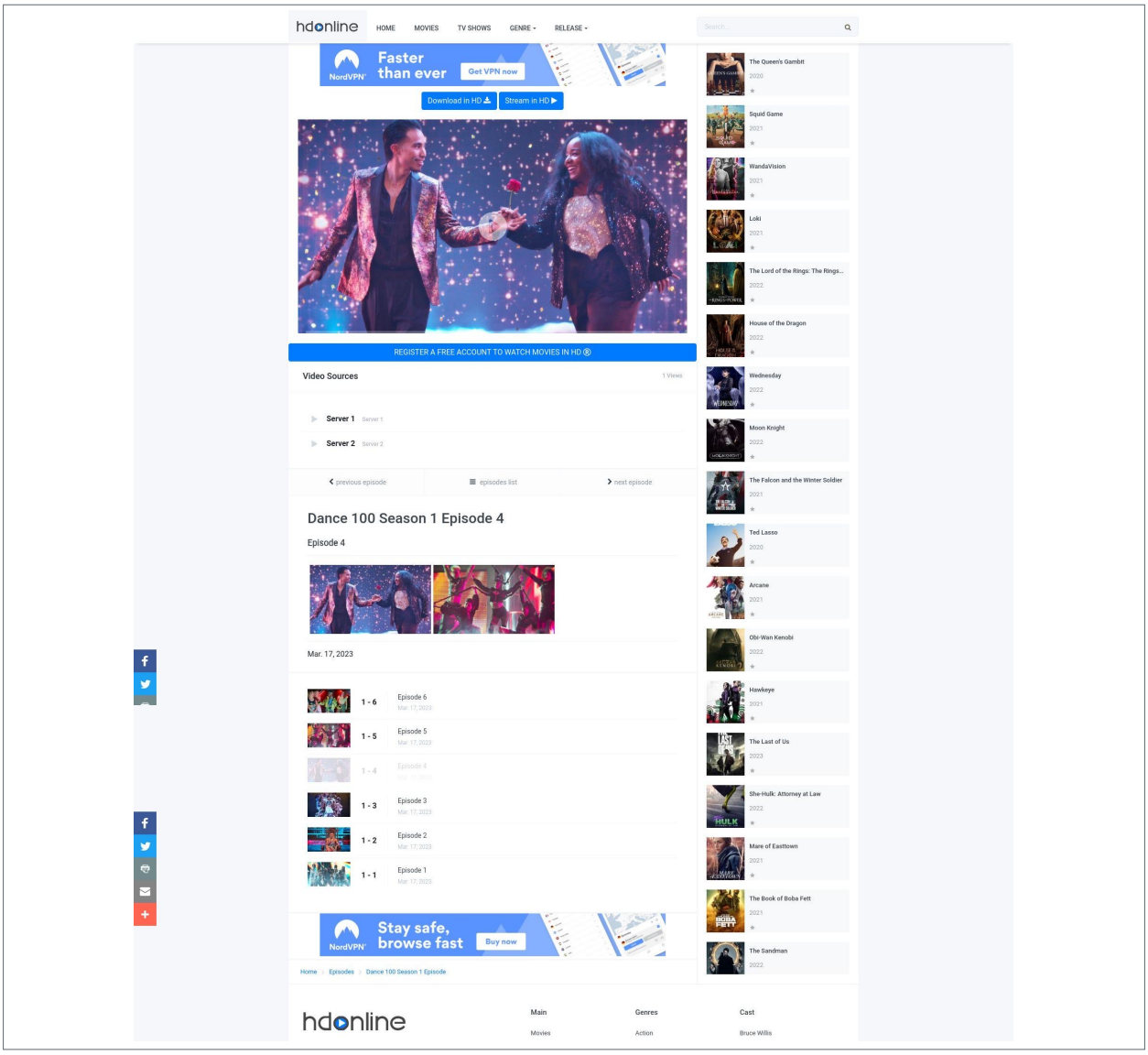


Image 7

Sometimes, the marketing is less direct. image 8 below is an example of how a VPN markets on Thehiddenbay.com, an illicit piracy site that harkens back to the infamous Pirate Bay website:

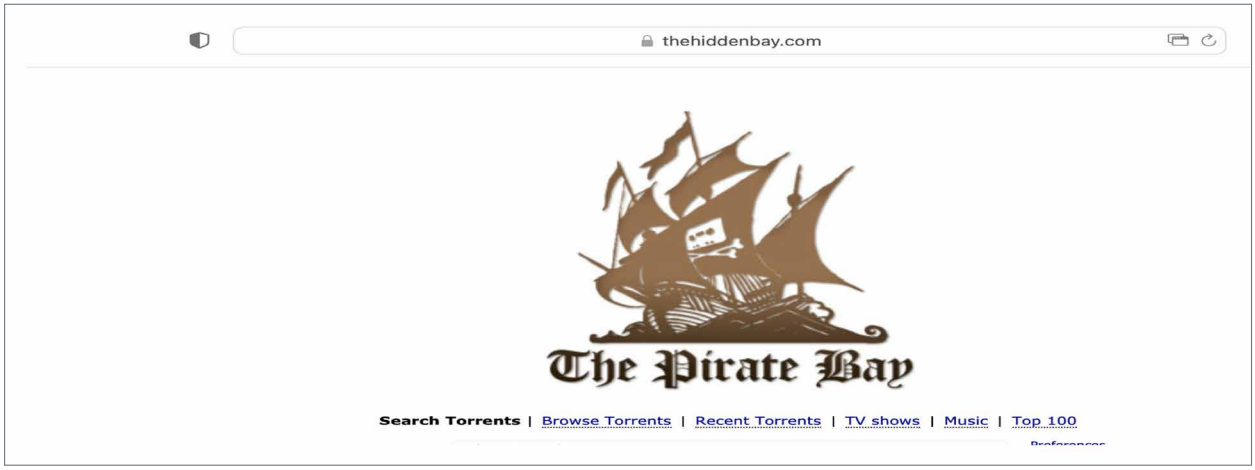


Image 8

If a user clicks on a link, a warning pops up about the risks of accessing illegal pirated content:

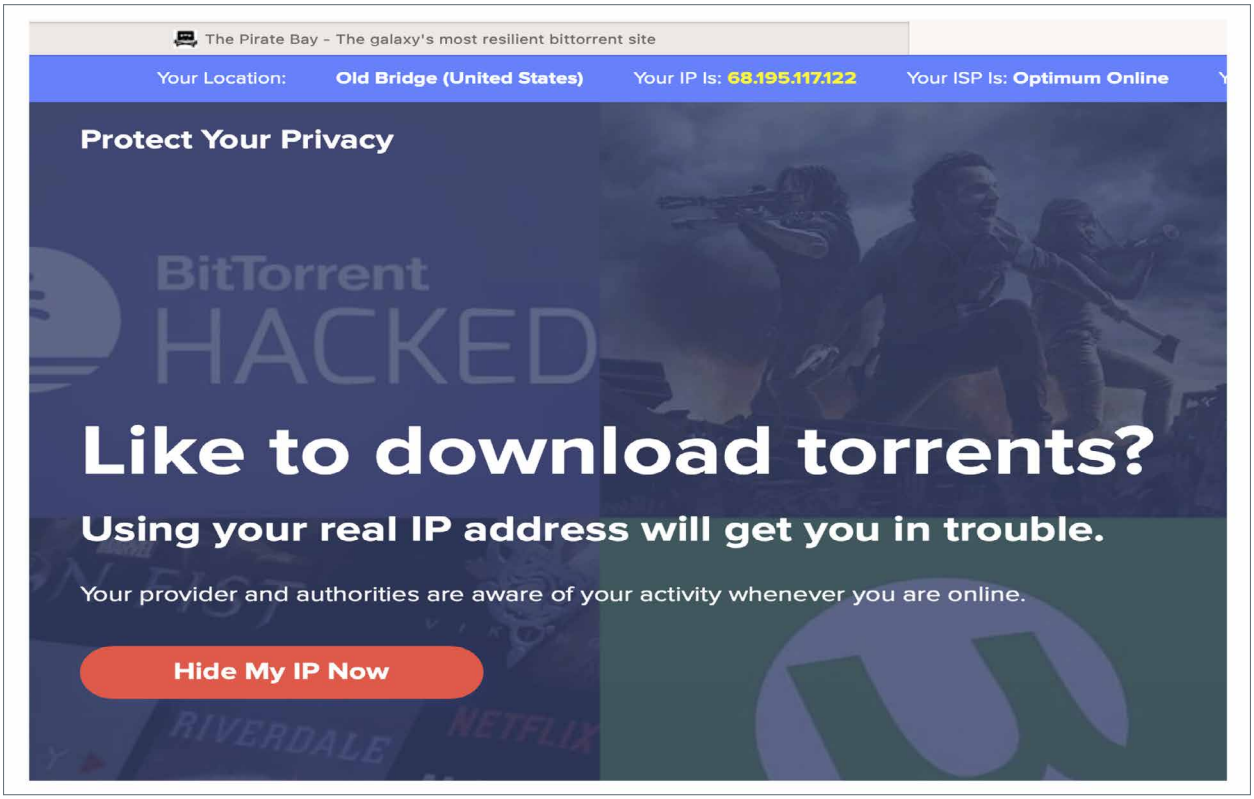


Image 9

A click on "Hide My IP Now" sends the user to an ad for VPN provider TotalVPN:

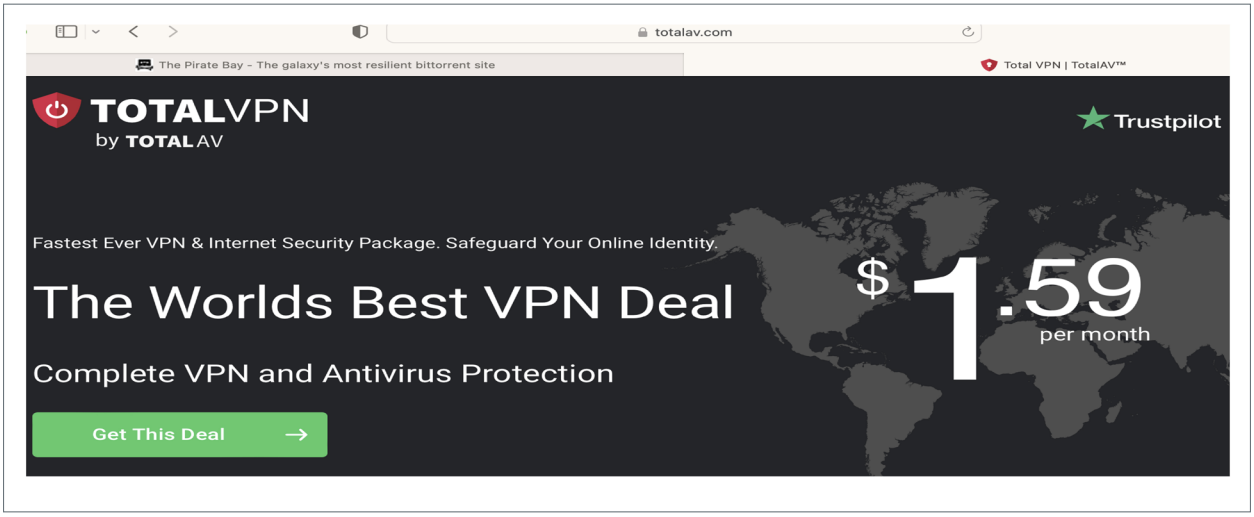


Image 10

VPNs also advertise on websites dedicated to piracy themes. image 11 below is an example of how VPNs advertised on the piracy-themed websitekodifiresticktricks.com:

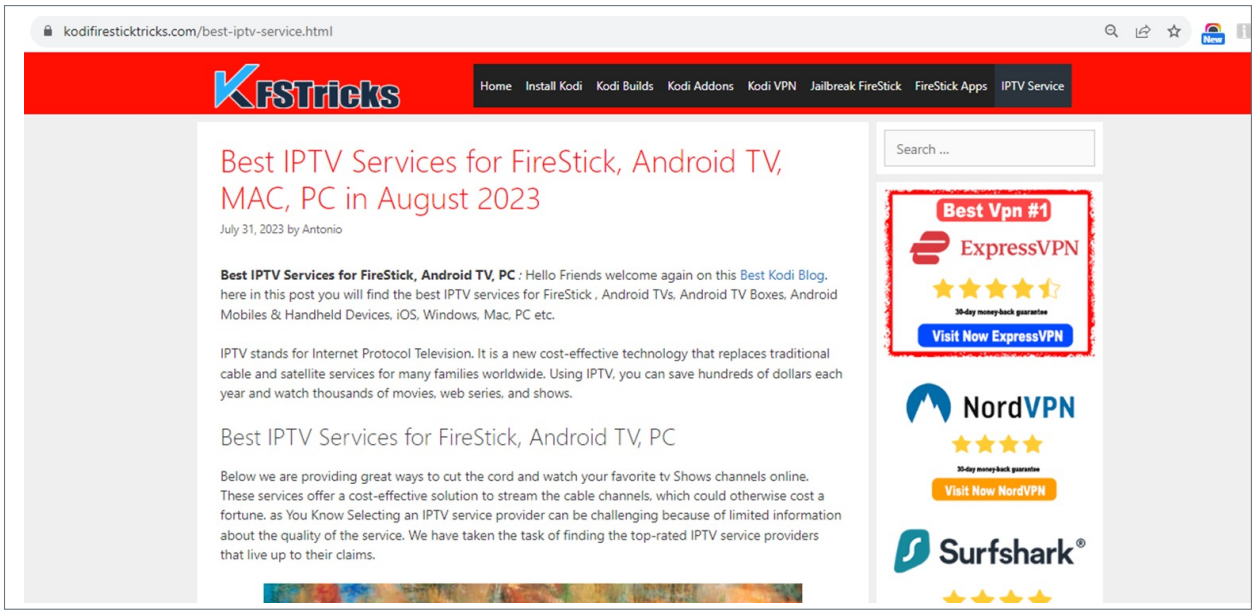


Image 11

NordVPN offered the following response about the report's findings: "A $45 million spending for advertising on piracy sites is false statement. Otherwise, it requires a solid evidence to support it. It is also important to mention that in theory, there might be a small window between the appearance of infringing ad and us spotting and blocking the infringer, but these are rare and minor cases."

It is important to note that the $45 million estimate is for all VPN providers, not just NordVPN.

The advertising raises questions about the efforts VPN providers are making to keep their ads off illicit platforms such as piracy sites. For example, ExpressVPN states on its website that its service "is not intended to be used as a means of copyright circumvention." In a statement, ExpressVPN said it does not purchase ads on piracy sites while acknowledging that some advertising and marketing can "slip through the cracks." However, the investigation found ExpressVPN ads on at least 19 piracy sites generating an estimated 61.9 million ad impressions.

There are multiple reasons that could explain VPN advertising showing up on piracy sites. The VPNs could directly and intentionally advertise on these sites. Or these VPN operators could rely on intermediaries to place the advertising but fail to instruct those intermediaries not to allow the ads to appear on piracy sites. In many cases, VPNs work through affiliates or affiliate networks for digital advertising, and either fail to properly vet the affiliate publishers where ads will appear or neglect to manage an affiliate compliance program to ensure that their ads do not appear on piracy sites.

Whatever the explanation, what's most telling is that the investigation determined that VPNs were one of the few well-known industries advertising consistently on piracy sites — along with Gambling companies. Rather, the most prominent advertisers during the study included crypto casinos and crypto exchanges – in both instances promoting services that may be illegal in some countries.

By having ads appear on piracy sites, that is the company VPN providers keep.

In coming months, Digital Citizens will track whether VPN advertising remains on piracy sites. If VPNs didn't know, they now have an opportunity to stop.

VPN promotions on piracy sites go beyond ad placement. Recall that vpnMentor acknowledged its ranking system for best VPNs may be affected by "affiliate commissions we earn for purchases through links on our website."

In plain speak, what that means is VPNs incent others to promote their services. For example, if a website operator promotes ExpressVPN, the operator gets a commission for a referral that leads to a sale. Affiliate programs are common in the digital world; what is uncommon is for companies to rely upon, and pay, illicit players such as piracy operators to promote their services.

Affiliate marketing is commission-based promotion that brands like VPNs may use and takes many forms. Affiliates drive traffic to a VPN's website and commissions can be paid for traffic or for actions taken on the VPN's website such as purchase of products. These promotions may take a variety of forms, including any combination of the following:

- Display or video advertising,
- Clicks anywhere on the affiliate website that take the user to the VPN's website opening either in a new tab or a new window, and
- Links on text or images on the affiliate website that induce the user to click, leading to the VPN's website.

VPN providers presumably do this on the belief visitors to piracy sites are concerned that their visits might come to the attention of service providers or governmental authorities – and therefore may be in the market for a VPN to shield their activities.

The investigation found evidence that VPN operators make extensive use of link-based affiliate marketing on piracy sites in addition to digital advertising. White Bullet found that ExpressVPN alone had at least 2,764 examples of unique webpages linked back to sites offering pirated content in a six-month period between February 2023 and August 2023.

These include blogs on piracy platforms and sites that discuss piracy. Typically, they recommend ExpressVPN as the best VPN. When users click on these links, they are directed to an offer on the ExpressVPN website and if the user signs up, the site that made the recommendation receives a referral fee.

Image 12 below is an example of how VPNs are recommended on kodifiresticktricks.com (the same site that included direct advertising by ExpressVPN and others). Note how the website warns users that "Government agencies can watch your online activity and accessing copyrighted content on your Fire TV Stick could be serious trouble." The website then recommends ExpressVPN with a special offer:

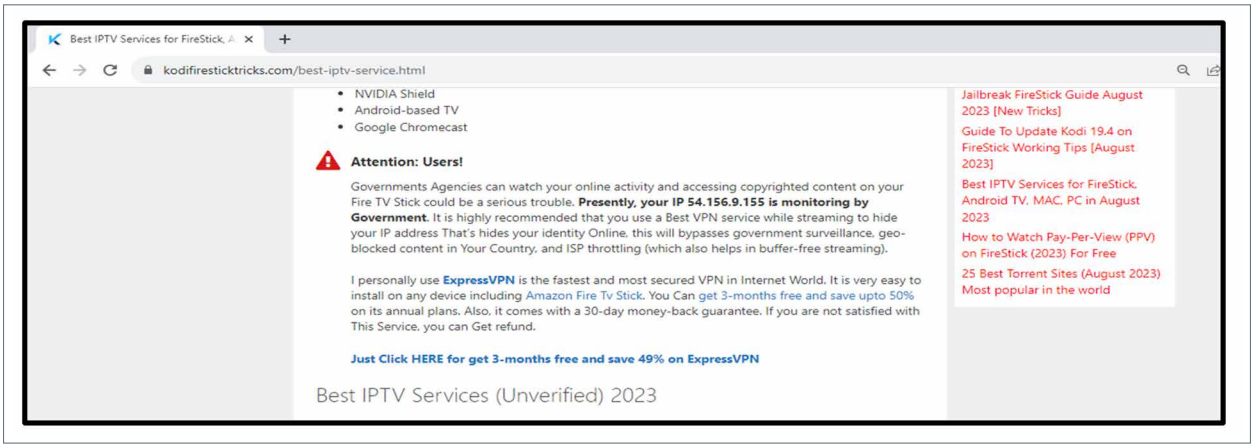


Image 12

While oftentimes the pitch to sign up for a VPN is done with a nod-and-a- wink – for example offering an "all access pass to global content" – in cases like image 13 below the message is explicit: viewing pirated content is illegal and the best way to avoid detection is with a VPN.

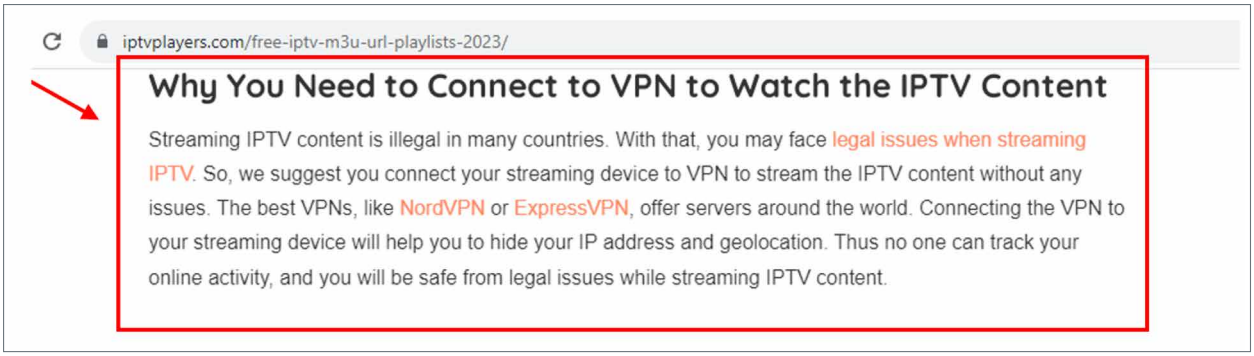


Image 13

Like display or pop-under digital advertising, link affiliate relationships may or may not be handled directly by the VPN. But just like digital advertising, there are countless examples that suggest that if VPN providers don't know they are being promoted on illicit piracy sites, they should. Or at least they do now. Digital Citizens will track these piracy sites, just as it intends to do with advertising, to see if the promotional links remain.

# Privacy Gained, Privacy Lost?

A mountain of evidence exists that many piracy websites are riddled with malware designed to target businesses and consumers; in addition Internet users who subscribe to piracy sites are four times more likely to get targeted for credit card fraud.

These are the entities that VPN providers are associated with and helping to fund.

Targeting Internet users that visit piracy sites is big business: malvertisers spend an estimated $121 million placing ads on piracy platforms with the express goal of infecting devices. Image 14 below is an example of a malicious ad on the piracy website zt-za.live, which is subject to a blocking order in France.

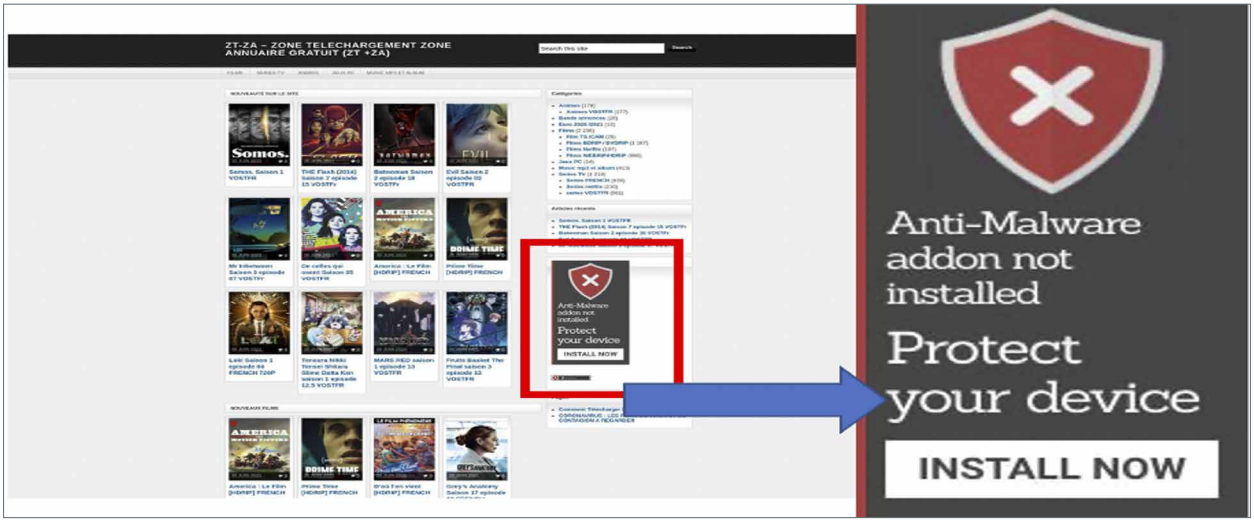


Image 14

Ads are created specifically to scare an Internet user into taking action that ultimately exposes devices. Here is an example of an ad that falsely claims an Internet user's computer is infected with a virus. If the user takes the bait and clicks on the ad, that is when real malware is installed.


Image 15

When investigators conducted an audit of piracy websites in 2022, they were hit with a ransomware attack that encrypted the researchers' files. To release the files, the illicit actors demanded a ransom of $980, as the image below shows:

Research studies have shown that piracy and risk of malware are closely linked. A Digital Citizens survey found those who said they visited piracy sites are three times more likely to report an issue with malware than those who did not.

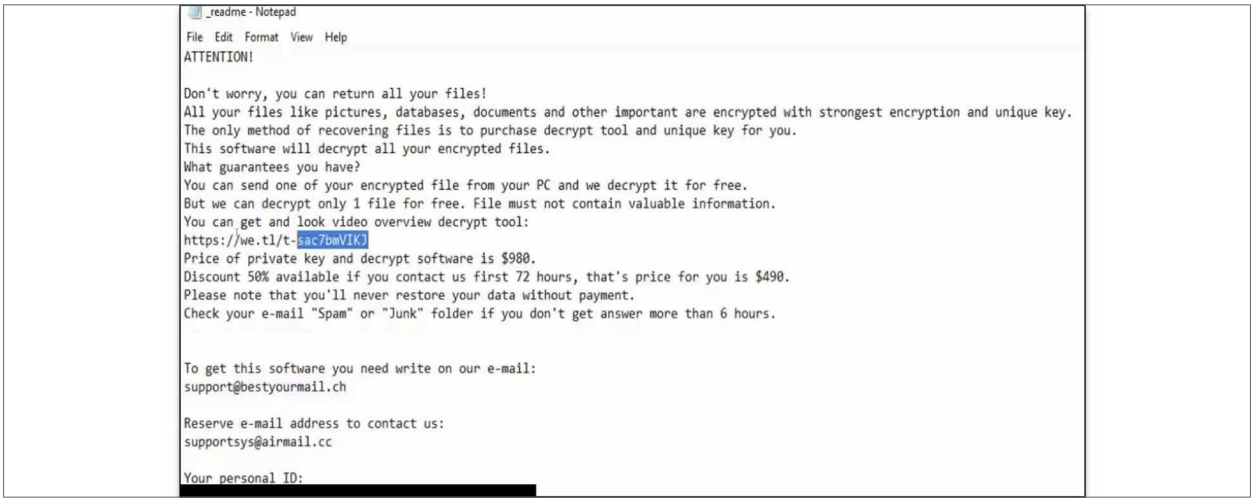


Image 16

In addition, there are risks of credit card fraud from signing up for piracy subscription services. In a study earlier this year, a pristine credit card was used to sign up for 20 piracy services. Within weeks of signing up for piracy subscription services, the investigators' credit card was targeted for $1,495 in illicit purchases –for grocery delivery, women's apparel, computer software, a cash advance, and a large mystery charge of $850 that, ultimately, wasn't processed. These purchases appear to originate from China, Singapore, Hong Kong, and Lithuania.

These reports underscore that piracy operators, in addition to peddling all kinds of intellectual property that they don't own, are willing to undermine users' privacy and safety if the price is right. Given these threats, it's disturbing that leading VPN providers would not take the same steps as other legitimate industries to disassociate themselves from such enterprises.

# A Trustworthy Internet Needs Trustworthy VPNs

When VPN leaders blur the lines of privacy and trust, they do a disservice to promoting faith in VPNs specifically and the Internet overall.

If VPN leaders such as ExpressVPN and NordVPN are serious about protecting privacy and security, they should be even more transparent about their ownership of review and use of affiliated sites. In addition, VPNs should know where their advertising is and who their affiliate partners are. Providers should commit to stop advertising on dangerous websites known to spread malware, including piracy sites.

Internet users expect VPN providers to be trustworthy. Seventy-four percent of Americans said if VPNs advertised on websites that have a reputation for spreading malware, they would consider it a breach of trust.

One of the challenges is that VPNs are unregulated. If an ISP takes steps that undermine user privacy, they may be subject to enforcement by government regulatory agencies, including the Federal Communications Commission. That is not the case with VPNs. By a 2-1 margin, Internet users believe that because VPNs have access to sensitive user information, they should be regulated or at least more closely scrutinized by government consumer protection bodies.

For Internet users, strengthening faith in VPNs comes down to two things.

First, it is up to VPN providers to decide the company they keep. If they allow their ads to appear on nefarious sites or engage in questionable marketing tactics, then they are signaling that revenues are more important than privacy. That is their prerogative, but their straddling of the legitimate and illicit advertising worlds should be called out.

Second, Internet users looking for a VPN provider should know the trustworthiness of the companies they rely upon. For whatever reason an individual signs up for a VPN, they should research and carefully consider their choice.

When VPN provider IVPN closed their affiliate program down several years ago, it did so because it found "increasingly unethical behavior." The provider noted that unscrupulous advertising practices undermine the integrity of VPNs – and underscored that "people are using VPNs in circumstances where compromising their anonymity could be life threatening. For this reason alone, it's imperative that companies advertising VPN services are honest about their relationship with the brands they are advocating."

While VPNs are likely to remain unregulated, that shouldn't discourage the Federal Trade Commission from calling out VPNs that don't protect their customers or Congress from asking hard questions of whether VPN leaders are living up to their principles.

VPN operators can't have it both ways. They cannot trumpet their role as champions of privacy while having their advertising show up on illicit websites that spread privacy-undermining malware.

Internet users need to have faith in their online providers, including VPNs. Too often, VPNs have let down their users, either by misleading about the data they collect, leaks of sensitive information, and now, playing both sides of the privacy street.

Internet users deserve better.

# Methodology

### 1. Selection of piracy sites

A total of 1,500 piracy sites were initially selected for ad monitoring and analysis by White Bullet. Due to piracy site churn (including redirection), and the dynamism of ad placement and campaigns, 1,278 domains delivered ads during the project. The sites were chosen from the thousands of piracy sites in White Bullet's Intellectual Property Infringement Platform (IPIP™) to include the most popular piracy sites as well as sites with significant ad impressions in sectors for technology and computing, security services, personal finance, or health and fitness. Specifically, sites were included if they were known to have advertising and met one or more of the following criteria:

- The site was among the most popular piracy sites (those with highest ad impressions overall) in the three months prior to the selection process, or
- The site was one of those delivering high levels of ad impressions in the three months prior to the ad tracking project in one or more of the following sectors: technology and computing, security services, personal finance, and/or health and fitness.

### 2. Collection/training ads

White Bullet's proprietary technology collected data on the ad profiles for this study from 26 countries during April and May 2023:

- Australia
- Belgium
- Brazil
- Bulgaria
- Canada
- Czech Republic
- Denmark
- Estonia
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Lithuania
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Russia
- Slovakia
- Spain
- Sweden
- United Kingdom
- United States

White Bullet has developed its proprietary advertising monitoring system, which captures high volume data about advertising placed on IP infringing sites (defined as infringing copyright or disseminating counterfeit goods) through which parties may monitor ad profile changes (the Ad Monitoring System).

*The Ad Monitoring System*:

- visits IP infringing sites from local internet protocol addresses (IP addresses) to track locally served ads,
- captures images of ads in the context of the infringing web page,
- uses White Bullet's proprietary technology to identify brands and advertising sectors (e.g. malware, adult, financial, fashion, travel, technology), and
- identifies adtech intermediaries engaged in the placement of advertising (Ad Intermediaries), by analysing data on all intermediaries involved in the process of targeting, placement and delivery of ads.

Each URL was visited daily from all countries tracked using one of the three user profiles below. Each profile was rotated on a scheduled cycle to ensure all sites were visited equally.

- *Neutral (cookieless) profile*: for collection of non-targeted ads. This gave the monitoring exercise a neutral benchmark. It was also an important stand-alone category as many consumers of digital IP-infringing content use anonymization technology – such as VPNs and proxies – to protect their privacy and, therefore, do not visit IP infringing sites with any attributable cookie profiles.
- *Female user profile*: profile included multiple interest-based user profiles within this category.
- *Male user profile*: profile which included multiple interest-based user profiles within this category.

Over 100 specific interest sectors were used to develop profiles (including travel, weather, fashion, personal finance, technology, etc.). Cookies also related to previous visits to IP infringing content.

### 3. Revenue Calculation

Potential annual worldwide revenue is the potential estimated annual ad revenue that sites could generate worldwide based on actual advertising data collected by White Bullet's automated Ad Monitoring System and incorporating available pageview data and extrapolating to include full annual coverage for all countries.

White Bullet calculates estimates of the advertising revenue of piracy sites by combining multiple independent and proprietary data sources within a revenue calculation algorithm. This includes (i) data about actual ads captured by White Bullet during ad harvesting visits, (ii) pageview data for those sites indicating traffic volume drawn from independent third-party sources, and (iii) advertising valuation data based on a proprietary matrix calculated from industry advertising payment values combined with advertising bid values identified by White Bullet in the code behind captured ads.

To create the advertising valuation matrix, White Bullet applies multipliers to core base values for the three dominant payment models in digital advertising: Cost Per Mille (CPM), Cost Per Click (CPC), and Cost Per Action (CPA). White Bullet's methodology uses a different core base value for CPM, CPC or CPA advertising drawn from industry estimates from third-party sources, which depend on various data components, including market sector (e.g., health, finance, travel), ad format (e.g. display, pop up/under) and media type (e.g. image, video, rich media). Multipliers applied are dependent on the advertiser type (e.g., premium household brand, clickbait), ad dominance (e.g. density of ads on the webpage) and country where the ad is displayed (a multiplier is applied to each ad for that country based on average advertising spend by internet user for that country as a percentage of average advertising spend by internet user benchmarked against the US). For CPC and CPA advertising, core base values and related click-through rates depend on market sector, and multipliers are applied to both core base values and click-through rates depending on the ad format, media type, as well as advertiser type, ad dominance and country, again drawn from industry estimates from third-party sources. Data points collected from ad harvesting visits by the Ad Monitoring System are cross referenced with the advertising valuation matrix, after which extrapolation calculations are created using estimated third-party pageviews to those sites and ratio of ads to visits by brand by country. Third-party data included in the above calculations are drawn from numerous sources, including Statista, eMarketer, Google AdSense, industry experts and ad exchange bid data.

Advertising values are heavily dependent on a range of factors and are therefore estimates based on extrapolating data using statistical correlations. White Bullet uses conservative base values and multipliers within the advertising revenue matrix and conservative pageview extrapolations, understanding that sites might command varying advertising rates with different demand side and advertiser buyers. The values in the advertising revenue calculation algorithm are periodically reviewed and updated as needed to reflect the digital marketplace.

**4. Link Affiliate Research**

To investigate VPNs' use of link affiliate relationships on websites, including piracy sites, Ahrefs' SEO service (Ahrefs.com) was used to collect data on websites linking to ExpressVPN between February and August 2023. White Bullet analysed this backlink data and compared the results against its IPIP™ database to identify piracy sites linking to ExpressVPN webpages. In addition, a White Bullet researcher reviewed and evaluated the unique ExpressVPN landing pages that users would see if they clicked on the link from the piracy sites as indicated in the backlink data.

## About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org.

## About White Bullet Solutions

Founded in 2013 by a leadership team of experienced Intellectual Property lawyers from the media and advertising industries, White Bullet offers companies piracy risk data and protection, brand safety solutions and full transparency on their advertising placement and digital supply chains.

White Bullet works collaboratively with brands, policy makers and the advertising industry to safeguard advertising spend and prevent ad placements from appearing on IP Infringing domains and apps. White Bullet is a certified brand safety anti-piracy solutions provider under the advertising industry regulator TAG and is a stakeholder to the EU Commission Memorandum of Understanding on Advertising and IPR.

White Bullet comprises IP experts and dedicated technical engineers who specialize in AI, big data models and predictive machine learning. The team includes highly skilled investigators and data analysts experienced in tackling the funding and distribution of pirated content. With offices in London, New York and Chicago, White Bullet advises policy makers and government bodies on regulatory and compliance programs globally. Learn more about White Bullet at www.white-bullet.com.

digitalcitizens alliance | whitebullet