Hiding in plain sight

Fighting online child sexual exploitation with VPN and proxy detection

GeoComply

Introduction

Internet users are increasingly assuming anonymous online personas as concerns about privacy have grown. Despite all of the internet's benefits, ever-increasing connectivity, camera-equipped technology, and online anonymity have made it easier for criminals to groom, recruit, and exploit with impunity.

Children are particularly vulnerable to the dark realities of the internet. Predators exploit children by using the same anonymizing tools many others use daily. Online Child Sexual Exploitation (OCSE) and the funding, production, and distribution of Child Sexual Abuse Material (CSAM) have been partly facilitated by the ability to share data on the internet anonymously.

With images and videos easily copied, transferred, and hosted on many online platforms, CSAM spreads faster than it can be taken down.

CSAM hosting around the world rose 64% last year.

With over a quarter million new URLs containing CSAM in the past 12 months,

4.3 million child sexual exploitation reports were processed by cybertip.ca from 2014-2020.

Where are they hiding?

Dark nets, encryption services, anonymization technologies, and peer-to-peer file-sharing services have created a safe harbor for offenders.

While the majority of CSAM is accessed through the surface web, a large portion is accessed and distributed on the dark web.

The most popular software used to access the dark web is the Tor Browser, an open-source privacy network with over 2.5 million daily users, which allows users to browse the web anonymously.

Consequently, law enforcement faces many obstacles in identifying and prosecuting criminals, and victims are trapped in a vicious cycle of continued abuse.

To combat OCSE, nonprofits, technology providers, law enforcement, and families must come together. Information sharing, collaboration, and technology are central in the fight against child exploitation.

Technical solutions can enhance the data available to law enforcement for investigations and create avenues for collaboration between organizations fighting CSAM.

The cost of anonymity

Nowadays, internet users place a high value on privacy. People have various motivations for operating anonymously online. They might want to access geofenced streaming content, evade censorship, or bypass firewalls. Or, less nefariously, they might just feel uneasy about having their online activity, location and movements being tracked.

Millions of people use anonymizing tools, such as virtual private networks (VPNs) and proxies.

Researchers have found

[1 in 3]

internet users has a VPN.

These numbers are higher in certain countries, such as the US where nearly half of internet users claim to use a VPN.

Anonymizing tools can conceal a user's actual internet protocol (IP) address, which is unique to each device and can reveal one's general location. Commonly used anonymizing tools include:

1. VPNs

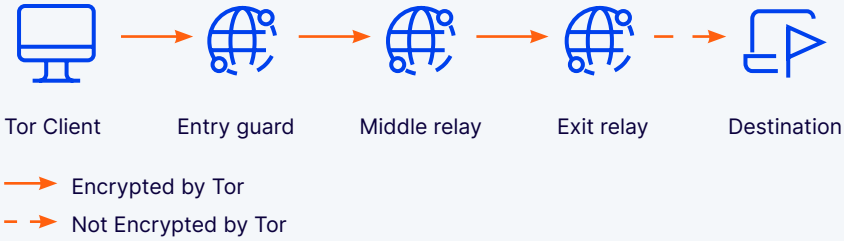
VPNs encrypt internet traffic and redirect it through a specially configured remote server run by a VPN host.

2. Proxies

Proxies do not encrypt internet traffic; instead, they send it to a proxy, then forward it to the internet, acting as the request's source.

3. Tor

The Tor network (Tor is short for The Onion Router) routes traffic through various nodes, wrapping it in encryption each time. A computer that uses a Tor browser never communicates directly with the website's server.



The ability to anonymously operate online can be used for darker purposes, including the distribution of child sexual abuse material (CSAM). Criminals can easily manipulate anonymizing tools to evade oversight and conduct illicit activity online.

Some VPN & proxy providers deliver "residential proxies" to their customers. Residential proxies are innocent users' home IP addresses hijacked through various techniques and re-sold as a premium anonymizing service. The residential IP hijacking tactic avoids using data centers, which VPNs and proxies have traditionally relied on, making detection even more challenging.

Lifting the veil of secrecy

VPNs and other internet anonymizers enable the funding, production, and circulation of CSAM. The Virtual Global Taskforce has found that some of the largest threats in online child sexual exploitation and transnational child sex offending are the increased use of personal privacy and anonymization technologies. The WeProtect Global Alliance affirms that even offenders with minimal technical knowledge can obstruct law enforcement investigations by using anonymizers.

These trends are exhibited in the regulators' Suspicious Activity Reports (SARs). The Financial Crimes Enforcement Network (FinCEN) recorded a 147 percent increase in OCSE-related SAR filings between 2017 and 2020. It observed that OCSE offenders are increasingly using convertible virtual currency, peer-to-peer mobile applications, the dark net, and anonymization and encryption services to avoid detection.

> "More offenders are using anonymizing technologies such as TOR as well as VPNs to commit sexual offenses against children online.
> **– The Virtual Global Taskforce, 2019.**

Case Studies

In 2020, international law enforcement agencies shut down a VPN service, Safe-Inet, that enabled hundreds of thousands of illegal online transactions involving images of child abuse and other illicit activity.

An OSCE offender based in China exploited children via peer-to-peer file-sharing sites, often using a VPN to hide his IP address.

A U.S. Federal Bureau of Intelligence (FBI) investigation found that a cyberstalker used various anonymizing services, including Tor, VPN services, anonymized international texting services, and offshore private email providers to conduct their predatory activity.

As of 2014, an estimated 17 percent of Tor services provided "adult content," about half of which is classified as CSAM. One of the most prolific examples is the Welcome to Video Tor service, a forum that traded CSAM between 2015 and 2018 and offered over 250,000 CSAM files to over 4,000 customers.

The ability to share data online anonymously obfuscates the data available to identify offenders, challenging law enforcement's ability to conduct investigations and places extreme pressures on organizations dealing with cyber tips. It can trap a child in a cycle of direct and indirect victimization.

The scale of the problem

Nonprofits and law enforcement are fighting OCSE daily

Child exploitation reports to the National Center for Missing & Exploited Children (NCMEC) increased 35 percent to 29.3 million from 2020 to 2021. Over 99 percent of the reports in 2021 included incidents of suspected CSAM.

With more youth spending time online, there are more opportunities for exploitation

The Canadian Centre for Child Protection (CCCP) saw an 88 percent increase in reports during the COVID-19 pandemic. Girls appear in the overwhelming majority of CSAM, making up 80.42 percent of children depicted in the material assessed by the CCCP.

The task of removing CSAM and identifying offenders is hugely complex

CSAM appears on various online platforms and services, including websites, email, instant messaging, peer-to-peer networks, internet gaming sites, social networking sites, and anonymized networks.

1 in 3

luring attempts reported to cybertip.ca happened on Instagram, Snapchat, or KIK messenger.

In recent months, youth sextortion has seen a 150 percent increase. Sextortion is blackmail – the act of threatening to send a sexual image or video to other people if the victim doesn't pay or provide more sexual content. Cybertip is currently receiving an average of 57 sextortion reports per month.

GeoComply's solution: Industry-leading VPN and proxy detection, GeoGuard

VPN and proxy detection tools serve a critical role in the fight against online criminals. While many products are available in the market, nonprofits and law enforcement agencies have turned to GeoComply's industry-leading products for help.

GeoComply's GeoGuard™ solution provides multi-layered protection against malicious spoofing tools and techniques. It dynamically tracks and flags compromised VPNs, proxies, Tor exit nodes, residential proxies, and other types of IP address manipulation.

GeoGuard™ is a database of IP addresses that have been flagged as compromised by anonymization services. GeoGuard™ has been independently tested to detect IP fraud with 99.6 percent accuracy. Using advanced and proprietary technology combined with GeoComply's expertise, GeoGuard is continuously updated with new IPs multiple times per day and retires old IPs to ensure fewer "false positives."

Available as a locally hosted database or via API, GeoGuard is a simple solution to combat even the most advanced IP spoofing methods. Advanced VPN and proxy detection streamlines investigations, provides insights into IP addresses commonly used by offenders, and empowers investigators with enhanced analysis.

How GeoComply Helps

GeoComply works closely with the Child Rescue Coalition (CRC), a U.S.-based nonprofit organization, leveraging technology to protect children and stop online predators.

> "The utility of GeoComply's GeoGuard VPN detection to our mission is already proving itself. It is crucial that we're able to provide the most accurate information possible to our law enforcement users. It is not an exaggeration to say that **GeoGuard will literally help stop and, in some cases, even prevent the sexual abuse of a child.**
>
> – **Glen Pounder**, Chief Operating Officer, Child Rescue Coalition

CRC technology harnesses GeoComply's VPN and proxy detection capability to help:

prevent	arrest	rescue
690,000+	13,967	3,212
cases of abuse	predators	children

More than 10,000 law enforcement officials in 97 countries use CRC technology.

Working Together

Technology is a core component of the path toward a safer internet. Tackling anonymization is a meaningful step in the right direction. Cryptocurrency exchanges, video-sharing platforms, social media sites, and other online platforms only need to take small steps, such as implementing VPN and proxy detection, to have an enormous impact on the investigation and prevention of OSCE.

With enhanced data intelligence from technology such as VPN and proxy detection, online platforms can help regulators and law enforcement better identify suspicious activity. As a result, online environments are made safer, and more offenders are removed from the streets. Working together, we can take productive steps to protect current and future generations of children from online predators. Legislators, regulators, industry, nonprofits, and law enforcement must use the available technology and collaborate to make the internet safer for everyone.

Through collaboration with nonprofit, public, and privatesector partner, we fight online child exploitation. Join us in taking a stance for a safer internet

Since our start in 2011, GeoComply's goal has always been to make the internet a safer place. Our highly advanced compliance and anti-fraud solutions bring clarity to your digital ecosystem and all suspicious activity, giving you the assurance you're always one step ahead of fraud. And while fighting internet fraud is an intricate business, using GeoComply isn't. **Fraud moves quick. But GeoComply will always move quicker.**

GeoComply

geocomply.com

To **learn more about** how GeoComply can help protect children and support investigations, contact our IMPACT team: impact@geocomply.com