The New York Times
https://nyti.ms/2Q893Pu

Across the internet, sexual predators flock to websites where they share images of child sexual abuse.

Seven years ago, three such sites went online. Groups dedicated to protecting children quickly started sending email notices to remove the illegal imagery.

As the imagery grew more extreme, the sites drew hundreds of thousands of visitors and found ways to hide behind tech companies.

Finally, one group in Canada overwhelmed the sites, forcing the images offline with a computer program that sent more than a million of the notices.

It was an epic battle, but can it be repeated?

Fighting the Good Fight Against Online Child Sexual Abuse

Several websites popular with sexual predators were thwarted last month after a determined campaign by groups dedicated to eliminating the content. It was a rare victory in an unending war.

By GABRIEL J.X. DANCE DEC. 23, 2019

In late November, the moderator of three highly trafficked websites posted a message titled “R.I.P.” It offered a convoluted explanation for why they were left with no choice but to close.

The unnamed moderator thanked over 100,000 “brothers” who had visited and contributed to the sites before their demise, blaming an “increasingly intolerant world” that did not allow children to “fully express themselves.”

In fact, forums on the sites had been bastions of illegal content almost since their inception in 2012, containing child sexual abuse photos and videos, including violent and explicit imagery of infants and toddlers.

The sites managed to survive so long because the internet provides enormous cover for sexual predators. Apps, social media platforms and video games are also riddled with illicit material, but they have corporate owners — like Facebook and Microsoft — that can monitor and remove it.

In a world exploding with the imagery — 45 million photos and videos of child sexual abuse were reported last year alone — the open web is a freewheeling expanse where the underdog task of confronting the predators falls mainly to a few dozen nonprofits with small budgets and outsize determination.

Several of those groups, including a child exploitation hotline in Canada, hunted the three sites across the internet for years but could never quite

defeat them. The websites, records show, were led by an experienced computer programmer who was adept at staying one step ahead of his pursuers — in particular, through the services of American and other tech companies with policies that can be used to shield criminal behavior.

But the Canadian hotline developed a tech weapon of its own, a sophisticated tool to find and report illegal imagery on the web. When the sites found the tool directed at them, they fought back with a smear campaign, sending emails to the Canadian government and others with unfounded claims of "grave operational and financial corruption" against the nonprofit.

It wasn't enough. The three sites were overwhelmed by the Canadian tool, which had sent more than 1 million notices of illegal content to the companies keeping them online. And last month, they were compelled to surrender.

"It's been a wonderful 7 years and we would've loved to go for another 7," the sites' moderator wrote in his final post, saying they had closed because "antis," short for "anti-pedophiles," were "hunting us to death with unprecedented zeal."

The victory was cheered by groups fighting online child sexual abuse, but there were no illusions about the enormous undertaking that remained. Thousands of other sites offer anybody with a web browser access to illegal and depraved imagery of children, and unlike with apps, no special software or downloads are required.

The three shuttered sites had hidden their tracks for years using the services of Cloudflare, an American firm that provides companies with cyberprotections. They also found a hosting company, Novogara, that gave them safe harbor in the Netherlands — a small country with a robust web business and laws that are routinely exploited by bad actors.

Cloudflare's general counsel said the company had cooperated with the nonprofits and law enforcement and cut ties with the sites seven times in all, as they slightly altered their web addresses to evade targeting. A spokesman for Novogara said the company had complied with Dutch law.

Last year, Europe eclipsed the United States as the top hosting location for child abuse material on the open web, according to a report by Inhope, a group that coordinates child abuse hotlines around the world. Within Europe, the Netherlands led the list.

In an interview in The Hague, the Dutch minister of justice, Ferdinand Grapperhaus, said he was embarrassed by the role Dutch companies played. “I had not realized the extent of cruelty, and how far it goes,” he said.

When hotlines like the one in Canada learn about illegal imagery, they issue a takedown notice to the owner of the website and its hosting company. In most cases, the content is removed within hours or days from law-abiding sites. But because the notices are not legally binding, some owners and web hosts ignore or delay.

Several Dutch hosting companies will not voluntarily remove such content, insisting that a judge decide whether it meets the legal definition of so-called child pornography. Even when they agree, abuse imagery reappears almost at once, setting the cycle back in motion.

The Dutch police say they do not have the resources to play what is essentially an endless game of Whac-a-Mole with these companies, according to Arda Gerkens, a Dutch senator who leads Meldpunt Kinderporno, the Dutch child abuse hotline.

“It takes a lot of time,” Ms. Gerkens said, “and basically, they are swamped.”

That means results like last month’s, while relished by hotlines around the world, are likely to remain rare.

‘Our Little Community’

The trio of shuttered websites first emerged in early 2012, according to domain records and transcripts of online chats.

Their professed goal was to offer an easily accessible digital space for pedophiles and sexual predators to indulge their twisted obsessions, which had often been shunned even on notorious websites like 4chan and 8chan.

At least initially, the sites steered clear of imagery that was obviously illegal, the records show, focusing instead on photos and videos of young children posing in revealing clothing. Even so, the founder of the sites identified in the transcripts expressed surprise in 2014 that they had "lasted so long."

But the Canadians were already on to them. By then, the small hotline had been alerted to dozens of illegal images on the websites.

As the sites gained in popularity, child sexual abuse content became more and more common. The transcripts, which include over 10,000 time-stamped messages on a chat app, show how the founder, a man identifying himself as Avery Chicoine, reveled in the opportunity to interact with others who shared his interests.

"What we got here," he wrote in 2015, "is our little community."

By 2017, the sites' home pages featured images of young girls that did not legally qualify as child pornography in most countries but signaled that there was plenty available a click away. One of the girls, no older than 7, lay on her back in sparse clothing with her legs spread; she had been a victim of sexual abuse, according to the Canadians, and was easily recognizable to predators through widely circulated imagery of the crimes.

As illegal material flooded the sites, so did visitors. SimilarWeb, which measures internet traffic, estimated that the most popular of the sites received millions of visits a month earlier this year from an average of more than 500,000 unique visitors.

The moderator of the sites in recent months boasted about the traffic in a series of emails and encrypted messages to The New York Times, attributing the popularity to the extreme content.

The sites' many visitors were perhaps "the most hated people on earth," he said, describing them as belonging to an "oppressed sexual minority." He showed no remorse for their behavior, even casting the community of predators as visionaries whose crimes should be made legal.

He did not identify himself and would not say if he was Mr. Chicoine — the sites' founder, according to the chat transcripts — or if he knew him. Last year, a Canadian by the name of Avery Chicoine with a lengthy criminal record was arrested in British Columbia and charged with possessing and distributing child pornography. The Canadian authorities would not say whether the charges related to the websites. According to court documents, he pleaded not guilty, and a trial is set for next month. He and his lawyer did not respond to requests for comment.

The moderator would not address another pressing question: How had the sites managed to stay ahead of its pursuers so long?

He said he did not want to hand a blueprint to his enemies, writing: "99% of attempts to bring us down fail. So I want the antis to keep wasting 99% of their time, instead of figuring out what works."

In the chat transcripts, however, there were clues about the sites' evasion tactics. They pointed to a major cybersecurity firm, Cloudflare.

A High-Tech Hideaway

Based in San Francisco, Cloudflare built a billion-dollar business shielding websites from cyberattacks. One of its most popular services — used by 10 percent of the world's top sites, according to the company — can hide clients' internet addresses, making it difficult to identify the companies hosting them.

The protections are valuable to many legitimate companies but can also be a boon to bad actors, though Cloudflare says it is not responsible for the content on its clients' sites. The man accused of a mass shooting at a Walmart in Texas had posted his manifesto on 8chan, an online message board that had been using Cloudflare's services and was well known for

hosting hateful content. Cloudflare also came under criticism for providing services to the neo-Nazi site The Daily Stormer. (The company has since ended its relationship with both websites.)

In the chat transcripts, the man identifying as Mr. Chicoine showed he was fully aware of the company's advantages when he signed on. "What cloudflare does is it masks and replaces your IP with one of theirs," he wrote in 2015, using the abbreviation for internet address.

That year, he appeared to panic when a child abuse hotline identified one of his sites, telling a fellow moderator their operation was "finished." But when he later realized the hotline had sent the report to Cloudflare — and apparently not to the company that hosted the content — he seemed relieved. "Wait," he wrote, "may be ok."

He was right.

One month later, he expressed exasperation that a hotline had fired off another notice, this time to Cloudflare as well as the hosting company. The hotline confirmed the report with The Times. Still, the sites remained online.

Interviews and records show that Cloudflare's services helped hold off the day of reckoning for Mr. Chicoine's sites by providing protections that forced hotlines to go to the company first.

The National Center for Missing and Exploited Children, the clearinghouse for abuse imagery in the United States, had sent Cloudflare notices about the sites starting in 2014, said John Shehan, a vice president at the center. Last year, it sent thousands.

Even apart from the three sites, Mr. Shehan said, Cloudflare was well known to be used by those who post such content. So far this year, he said, the company had been named in 10 percent of reports about hosted child sexual abuse material. The center is in touch with Cloudflare "every day," Mr. Shehan said.

Separately, records kept by the Canadian hotline, known as the Canadian Center for Child Protection, showed that since February 2017 there had been over 130,000 reports about 1,800 sites protected by Cloudflare.

In December, the company was offering its services to 450 reported sites, according to records reviewed by The Times.

Through its general counsel, Doug Kramer, Cloudflare said it worked closely with hotlines and law enforcement officials and responded promptly to their requests. It denied being responsible for the images, saying customer data was stored on its servers only briefly. Efforts to eliminate the content, the company said, should instead focus on the web-hosting companies.

Records from the Canadian hotline revealed several cases in which abuse material stayed on Cloudflare's servers even after the host company removed it. In one instance, the imagery remained on Cloudflare for over a week afterward, allowing predators to continue viewing it.

"The reality is that it is totally within Cloudflare's power to remove child sexual abuse material that they have on their servers," said Lloyd Richardson, the technology director at the Canadian hotline.

When asked why it did not cut ties with a number of companies known to host child sexual abuse imagery, Mr. Kramer said Cloudflare was not in the business of vetting customers' content. Doing so, he said, would have "a lot of implications" and is "something that we really have not entertained."

Still, he said, the company had stopped providing services over the past eight years to more than 5,000 clients that had shared abuse material. And on Wednesday, the company announced a new product — currently in development — that would allow clients to scan their own sites.

The tension over Cloudflare's protections reflects a larger debate about the balance between privacy on the internet and the need of law enforcement to protect exploited children. For example, Facebook's recent decision to encrypt its Messenger app, the largest source of reports

last year about abuse imagery, was hailed by privacy advocates but would make it much more difficult for the authorities to catch sexual predators.

Addressing that broad tension, Matt Wright, a special agent with the Department of Homeland Security, said law enforcement and the tech industry needed to find "a mutual balance" — "one where companies intended to secure data, and protect privacy, don't get in the way of our need to have access to critical information intended to safeguard the public, investigate crimes and prevent future criminal activity."

Going Rogue in the Netherlands

There were other clues about the sites' ability to stay online, in a trail of activity across the web that led to the Netherlands. Internet criminals come from far and wide to leverage Dutch technology, some of the best in the world, for the purposes of spam, malware and viruses. They do this by using rogue hosting companies, which are infamously uncooperative except in response to legal requests.

"I realize that because we have such excellent internet logistics, we now have it on our plate," said Mr. Grapperhaus, the country's minister of justice.

For child abuse sites like the ones identified as Mr. Chicoine's, a top draw has been the company Novogara, formerly known as Ecatel, one of the country's most criticized hosting businesses.

The Chicoine sites were hosted on Novogara's servers for all of 2018 and through the early part of this year, records show. While working with the company, and without Cloudflare's protections at the time, the sites came under increasing pressure from the Canadians. Their hotline, along with at least four others around the world, stepped up their offensive, issuing hundreds of thousands of more reports about abuse imagery.

The number was so great, according to the Dutch and Canadian hotlines, that Novogara blocked the groups' email addresses to avoid receiving

additional notices. Ultimately, though, the targeting was effective: Novogara pulled the plug on the sites in May.

[Read more about the hotlines' role in the global fight against abuse.]

Aside from sites like Mr. Chicoine's, the Dutch have an even larger problem with sexual predators taking advantage of platforms used to upload and share images. Since June, a company that hosts those platforms, NFOrce, has appeared in more than half of reports the Dutch hotline has received about illegal imagery. Over the past three years, sites using NFOrce servers have received more than 100,000 notices of illegal content, records show, but the company has not removed the material, according to Ms. Gerkens, who leads the hotline.

NFOrce's sales operations manager, Dave Bakvis, said the company's hands were tied by Dutch laws, which prevent it from monitoring customer servers without a court order. He said NFOrce acted immediately when it received requests from the authorities. Separately, the websites themselves can and do remove the content.

"I hate child pornography," Mr. Bakvis said.

The Dutch national prosecutor for cybercrimes, Martijn Egberts, said in an email that issues involving "sovereignty" and "jurisdiction" complicated the removal of illegal material — leading the authorities to cooperate "as much as possible" with web hosts to get results.

Legislation is now being drafted that would require Dutch web hosts to keep the material out of their systems, essentially forcing to them to scan for it. If a company falls short, it could face ever-increasing fines.

Ben van Mierlo, the national police coordinator for online child sexual exploitation, said in an email that companies like Novogara "see themselves as a provider of a service." The challenge for the Dutch authorities and lawmakers, he said, was to convert them into partners in preventing the spread of illegal imagery.

“There is no space in the Netherlands for those individuals or companies that threaten these basic rights for children,” Mr. van Mierlo said.

The Final Assault

By May of this year, the moderator of the three sites was apoplectic, complaining in an email to The Times that “tolerance” for his views was coming to a halt.

Over the next several months, the sites hopscotched around the world, finding more than a half-dozen new hosts — to pick up where Novogara left off — in Denmark, Russia, the Seychelles and elsewhere. For years, they had deployed a similar tactic of changing the last part of their web address — moving from .com to .org, for example — to avoid being targeted and blocked. Companies and governments that provide these domains often do not coordinate with one another, allowing offenders to move around the globe while largely preserving their site’s identity.

But there was no hiding this time.

The Canadian hotline, working from offices in Winnipeg, Manitoba, were using a computer program named Arachnid to crawl the internet in search of Mr. Chicoine’s sites, and to send takedown notices whenever it identified illegal material.

And as soon as the three sites reappeared somewhere, the Canadians reached out to the new hosts. In all, they found more than 18,000 confirmed images of abuse on the pages, reporting most of them hundreds of times each. It is also possible that law enforcement officials and other groups directed their firepower at the sites.

Signy Arnason, the associate executive director of the Canadian center, described Arachnid as a “survivor-centric” endeavor, inspired by a survey that found victims of child sexual abuse feared being recognized in person by those who had viewed their abuse online.

Since its launch two years ago, Arachnid has found more than 1.6 million confirmed images of child sexual abuse, and has sent more than 4.8 million takedown notices to websites and hosting providers. The British child sexual abuse hotline, the Internet Watch Foundation, has also developed a "spider" to crawl the internet.

"Arachnid is one oar — a big oar — in a ship of many oars rowing against this issue," said Denton Howard, executive director of Inhope, the organization supporting child abuse hotlines.

Throughout the battle, the moderator of the sites would email the Canadians, accusing them of corruption and filling their inboxes with spam. He also contacted Canadian government agencies with false claims about the center, and even built software that altered the child sexual abuse imagery, hoping to trick Arachnid into skipping it over.

It was not enough. All imagery of abuse has been removed from the sites, and the forums for the predators are closed, at least while their opponents have the upper hand.

But as a parting shot, the home pages were filled with links to other sites that offered similar content, giving criminals a road map to continue their pursuits — and the groups dedicated to stopping them a list of new targets.

Michael H. Keller contributed reporting from New York.

Produced by Rich Harris, Virginia Lozano and Rumsey Taylor.

Related Coverage

- No 'Magic Bullets' in the Fight Against Online Abuse, but 'Spiders' Help DEC. 22, 2019
-

Video Games and Online Chats Are ‘Hunting Grounds’ for Sexual Predators DEC. 7, 2019

- How to Protect Your Children From Online Sexual Predators DEC. 7, 2019
- Child Abusers Run Rampant as Tech Companies Look the Other Way NOV. 9, 2019
- ‘If Those Were Pictures of You, You Would Understand’ NOV. 9, 2019
- The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? SEPT. 28, 2019
- Preying on Children: The Emerging Psychology of Pedophiles SEPT. 29, 2019
- An Explosion in Online Child Sex Abuse: What You Need to Know SEPT. 29, 2019