MATT BURGESS SECURITY APR 23, 2020 1:00 AM

Researchers have finally cracked the secret paedophile code

A major breakthrough will make it easier to remove child abuse images and videos from the web

WIRED

WHEN CHRIS HUGHES started removing child abuse images and videos from the internet, almost a decade ago, paedophiles were not discreet. Predators would share content through newsgroups, forums and on dedicated websites, often with clear descriptions of what could be seen in the pictures.

For people seeking out depraved content, it used to be alarmingly easy to track it down. “It was possible to go to a search engine, type it in and get exactly what you wanted,” he says. Hughes now leads a team of 13 analysts at the Internet Watch Foundation (IWF), a UK-based charity which is responsible for removing tens of thousands of webpages, images and videos of child sexual abuse content from the web each year.

As technology giants, law enforcement and organisations such as the IWF have become better at detecting abuse content and dismantling the networks behind it, the offenders have evolved their behaviour to avoid being caught. It’s a horrendous game of cat and mouse. To stay one step ahead, paedophiles have long-used

secretive code words and phrases to disguise the conversations and sharing of abusive content. Without knowledge of this language, it was impossible to decipher much of its meaning from everyday chatter. Until now.

Through a combination of years of human investigation and technological advancements, the IWF has now dismantled large swathes of this paedophile code. The charity now has a vast database of keywords associated with content depicting child sexual abuse, a secret language that took paedophiles years to develop and that has been crucial in their ability to evade detection. The IWF started identifying the language offenders use more than ten years ago and developed a database of around 450 words and phrases. Over the last few weeks it has increased the number of entries in its database by 3,681, with several hundred more still to be added.

“By having a greater understanding of these slang terms that are associated with these images, we can find websites and locate images that we haven’t seen before,” says Sarah Smith, the IWF’s technical projects officer who has overseen the work and leads a tech team of seven people. “The significant amount of keywords we have now identified will make it very much harder for them to be able to use those to identify and locate this type of content.”

The terminology included on its keyword list is shared with the IWF’s 140-plus members, who range from the web’s biggest companies – Apple, Amazon, Google, Microsoft and Facebook are all involved – to firms such as gaming platform Roblox, Zoom, law enforcement groups and mobile phone operators. Companies can use the keywords identified to limit searches on their services and identify where illegal content is being shared. This is in addition to a database of hashed images that companies use to stop existing abuse content being uploaded.
The cracking of this lexicon, both Smith and Hughes say, means it will be easier to proactively hunt down illegal content and remove it. More power has also been handed to investigators who spend their time verifying illegal images and trying to find newly created abuse content.

To understand how IWF’s researchers unlocked the code you first need to understand how offenders operate. “It’s very hard to determine the scale of abuse content,” says Elena Martellozzo, a criminologist and expert in online abuse from

Middlesex University London. She says criminals often share content between one another using community networks that are built up over time.

Once a network of those sharing abuse content online has been discovered, it quickly expands out. “From one individual you realise that immediately this person is linked to 30, 40, or 100 others,” says Martellozzo, who was not involved in the IWF’s work. “We’re not talking about the individual operating in the darkness, but a virtual community of sex offenders.”

These groups can reform very quickly after they have been discovered, Martellozzo adds. Often this leads to the dark web – although lots of abuse content is shared on the open web, social networks, or private messaging apps. Smith says the IWF gets a lot of its intelligence from the dark web as it is where a lot of new abuse content emerges. “The analysts will identify particular phrases that are clearly being associated with this type of imagery, we can then use that as a starting point to look at what other search terms may be used elsewhere on the internet, which are associated with those,” Smith says.

The words used by paedophiles to classify, share and find abuse images are varied. Hughes says that some are obvious, explicit terms describing sexual acts or what is happening in images. Some networks of offenders act in plain sight. Last year, a WIRED investigation exposed how paedophiles were commenting on YouTube videos involving children and sharing contact details where they could swap other videos.

But the more sophisticated criminals co-opt words used in every day language to indicate types of abuse. For obvious reasons, the new keywords the IWF has identified will not be published. “Some of them are almost alien,” Hughes explains. “They don’t necessarily make a nice tidy word or phrase. They could be a collection of characters that don’t make an actual word.” He gives a hypothetical example of how common the phrases used by offenders may be: it could be something as simple a ‘purple cushions’, he says. The words and phrases used can often refer to the name of a victim, where content can be found, or a particular set of images. “If you were to read something like that on a forum, where every other conversation is perhaps less covert, then we would take that phrase, do some additional searching on different sites and see if it produces results that give us an indication that ‘purple

cushions' is a phrase that people are using openly," he explains. (He uses 'purple cushions' because they are an everyday object he could see in front of him. The phrase is just used as an example, he says).

The keywords that are actually used can operate in combination with other words to make them mean something. Multiple keywords can be used at one time to reference certain images or behaviours. "Sometimes it's using them in the right combination," he says.

The IWF's list of expanded keywords are mostly in the English language, but there are also terms in Dutch and German. In 2018, the charity removed 105,000 web addresses that were hosting abuse image – 47 per cent of these were hosted in the Netherlands. "There were some terms that had been translated from Spanish," Hughes adds. "These were some of the keywords that were acronyms. The acronym from one language, such as Spanish, was then used with the English language."

Smith says the IWF has developed intelligent crawlers that identify new potential keywords. These crawlers work in a similar way to the technology of Google and other search engines by scanning parts of the web for potential abuse content. This information may be comments alongside content, or metadata attached to files.

"The crawler is targeted based on the existing data we have and will then return information from those websites that we've already identified may have child sexual abuse material in there," Smith says. During the charity's two decades of operation it has built up a huge database of URLs it has removed from the web. The IWF is also incorporating elements of machine learning into its systems to help identify the phrases that are commonly being used.

Once the crawler has produced potential keywords, it is then up to human analysts to confirm they are being used for signposting abuse content. The IWF says words or phrases do not get included on the list of phrases it provides to members without them being verified in multiple different places.
Humans are crucial to the project's success. While it would be technically possible to create a system that automates detection and produces potential keywords and phrases, this also risks censorship. For instance, if an innocuous phrase, such as the

example of ‘purple cushions’, was blocked automatically, it could stop people finding pillows.

The context keywords are used in is crucial. “We have to try and follow the offender mindset and look at how they might be going about finding this content and try to disrupt that and cut those routes off,” Smith says.

The IWF says the expanded keywords list will take some time to be implemented by its members, but it anticipates the end result will be more child sexual abuse images and videos being discovered and removed from the web.

“We’re hoping that we’ll be able to get out there and identify previously unseen imagery, which will have a massive impact on potential victim identification,” Smith says. “We’re doing everything we can to eliminate this.”

Matt Burgess is WIRED's deputy digital editor. He tweets from @mattburgess1

Coronavirus coverage from WIRED

😓 How did coronavirus start and what happens next?

❓ The UK's job retention furlough scheme, explained

💲 Can Universal Basic Income help fight coronavirus?

🎲 Best video and board games for self-isolating couples

👉 Follow WIRED on Twitter, Instagram, Facebook and LinkedIn

This article was originally published by WIRED UK

Matt Burgess is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and

now lives in London. Send tips to Matt_Burgess@wired.com.

SENIOR WRITER

TOPICS CRIME SECURITY

READ MORE

The Hottest Startups in Madrid in 2024

The Spanish capital is drawing talent from Latin America, and its eye-catching startups are working on smarter payments, eldercare, and an AI-powered virtual nurse.

STEPHEN ARMSTRONG

The Hottest Startups in Zurich in 2024

The Swiss financial capital might be most associated with fintech, but its startups are also focusing on medical robotics, AI-powered language learning, and the batteries of the future.

ALEX CHRISTIAN

The Hottest Startups in Berlin in 2024

The German capital attracts talent from all over the world, and its startups are building endless AI-generated audio apps, virtual pet apps, and sensors for early wildfire detection.

MORGAN MEAKER

The Hottest Startups in Dublin in 2024

The Irish capital's embrace of Big Tech is filtering through to its startups, who are building better tools for IT teams, AI content moderation tools, and RNA screening for herds of cattle.

STEPHEN ARMSTRONG

Inside the Massive Crime Industry That's Hacking Billion-Dollar Companies

When you download a piece of pirated software, you might also be getting a piece of infostealer malware, and entering a highly complex hacking ecosystem that's fueling some of the biggest breaches on the planet.

JOSEPH COX

The Hottest Startups in London in 2024

The UK capital's most exciting startups showcase its strengths in biotechnology and artificial intelligence.

JOÃO MEDEIROS

The Hottest Startups in Paris in 2024

The French capital has become the home of Europe's growing AI industry—but alongside giants like Mistral are startups building EV charging infrastructure and trying to revolutionize social media.

MORGAN MEAKER

The Hottest Startups in Helsinki in 2024

The Finnish capital's most exciting startups are building nuclear-powered heating networks, better weather forecasting tools, and an esports streaming platform that lets viewers bet on the outcome.

STEPHEN ARMSTRONG

Thousands of People Are Cloning Their Dead Pets. This Is the Woman They Call First

“I try to prepare customers not to expect the same pet all over again. The new pet is not going to know who you are right off the bat.”

CAMILLE BROMLEY

The Hottest Startups in Lisbon in 2024

The Portuguese capital's most exciting startups include a platform to help entrepreneurs get going, a smart punchbag, and the Uber of hair salons.

JOÃO MEDEIROS

The Hottest Startups in Stockholm in 2024

The Swedish capital produced Skype, Spotify, Klarna, and Minecraft—its stars of the future are building fintech for businesses, gen AI for lawyers, and full-body health care scans.

JOÃO MEDEIROS

A Mysterious Hacking Group Has 2 New Tools to Steal Data From Air-Gapped Machines

It's hard enough creating one air-gap-jumping tool. Researchers say the group GoldenJackal did it twice in five years.

DAN GOODIN, ARS TECHNICA