This pixel tracking demo shows how easy it is to make a creepy surveillance tool

theverge.com/2019/7/19/20700843/supertracker-email-tracking-pixel-location-superhuman-delian-asparouhov

Nick Statt

July 19, 2019

Illustration by Alex Castro / The Verge

The Superhuman controversy from earlier this month, in which a former Silicon Valley exec blew the lid off a series of controversial email surveillance tools offered by the up-and-coming startup, has prompted a bit of soul searching among those in the tech industry. But in twisted fashion, the public blasting of a company like Superhuman has been the tech equivalent of opening Pandora's Box, unearthing all sorts of free and easily available tools that have done this for years and can be employed by anyone with just the tiniest shred of tech savvy.

For instance, an open source, Python-based web tool called Supertracker has popped up on Github, courtesy of Delian Asparouhov, an investor with the venture capital firm Founder's Fund. It lets anyone create their own tracking pixel, coyly disguised as either a transparent image, an image of the pokémon pikachu, or a not-so-subtle magnifying glass.

Creating it is as easy as inputting a user name, picking a tracking pixel image, and hitting the enter key. From there, you can save the image, paste it in the body of any email, and send it off. Whoever opens it will have the when and even the where transmitted back to you. Of course, you can do similar styles of tracking with any number of available Superhuman competitors and browser extensions. But Asparouhov's tool has the added benefit of walking you through the process step by step and laying out just how simple it is to siphon away this kind of sensitive info with a few simple lines of code. (He also outlines some good defenses against this type of surveillance.)

> I'll get some heat for this but... this weekend I put together a quick site called Supertrackerhttps://t.co/sjpmqjVEo9
>
> It lets anyone make their own pixel just like Superhuman had, and lets you track in-depth where it is opened.
>
> Came away from the conversation last week...
>
> — Delian Asparouhov (@zebulgar) July 7, 2019

There are a number of considerations worth mentioning here. Asparouhov has created this tool as a demonstration, but it appears to have some serious limitations and privacy issues you have to take into account. For one, there's no proper login system, so choosing a username just keeps track of your individual tracking pixel.

That means anyone can guess your username and have access to the pixel's location and open history. And anytime someone else loads that location history page, they're also recording their own data. None of this data appears deletable, either. So take caution: anything you type in the username field could reveal your approximate location to someone who guesses what you typed, even if you have no intention of ever using the pixel in an actual email. Asparouhov's demonstration site also potentially has logs of all that information.

In short, it's a demonstration of how easy it is to gather this kind of tracking information, not something anybody should actually use. When reached for comment, Asparouhov told *The Verge* that because Supertrakcer was a "weekend project," he didn't "build a login system so anyone can see any username."

The tool can also be a bit finicky because there's no way to prevent it from recording time and location whenever you reload the tracking history page, which can make it appear like you've been opening your own pixel repeatedly. Asparouhov says a lot of existing browser plugins get around this by pasting the tracking pixel as an image into your email message automatically, so fully baked tracking software you can already access for free is even more powerful it seems.

""We should ask for more defensive options, not expect that there won't be any offense." " Asparouhov did say on Twitter he created Supertracker as a way to both educate the public as to how easy it is to create this type of tool, and therefore how widespread it likely is. The goal is to apply pressure on the only entities that can stop it — the large email providers like Google and Microsoft that could create more proactive defensive measures to protect users.

"Marketers and salespeople regularly violate our privacy by inserting tracking pixels and we should demand our email client fight against that," he wrote on Twitter shortly after releasing the tool on July 7th. "We should ask for more defensive options, not expect that there won't be any offense."

Asparouhov's approach may not all that appreciated by the pro-privacy crowd who decried Superhuman and the seemingly widespread practice of tracking pixel use in the marketing and ad tech industries. On that side of the debate are staunch privacy advocates who see email tracking tools like Superhuman's, which previously let you track when someone opened an email and where in the world they were located, as gross and unethical violations of privacy.

This type of tracking was typically being performed without the consent of the recipient, and without their knowledge, either. It may be commonplace in industries where this data is aggregated across hundreds or thousands of users — email newsletter creators or e-commerce companies, for instance. But Superhuman sold it as part of a souped up email package to individual users for the price of $30 a month. There was no way of telling if you received an email from a Superhuman user, and if that user then knew sensitive information about you, like what city you were located in and what time of day you were at your computer.

Related

How to stop your emails from being tracked

Mike Davidson, the former vice president of design at Twitter who publicized Superhuman's practices to the world in a viral blog post, is in that camp, writing, "Superhuman teaches its user to surveil by default," and pushing the company publicity until it disabled read receipts by default and removed its location tracking feature entirely. (Davidson thinks the company isn't doing enough, because it's still allowing its users to surveil anyone they like via email through non-consensual read receipts.)

On the other side are people like Asparouhov, who essentially believes only defensive measures can combat aggressive, even unethical product design. If it's not illegal, someone will use it. So Asparouhov's approach of handing the tech to anyone to use is designed to be alarming, hopefully so much so that it results in productive changes from email providers.

Companies like Google already allow you to disable image loading by default, so you can avoid those tracking pixels from ever gleaning information in the first place. The company also does some behind-the-scenes server tricks to prevent exposing your IP address to third parties, so location tracking doesn't work in some, but not all, cases.

Notably, Supertracker appears capable of loading images and recording location even when using Gmail and when having image loading turned off by default, and Asparouhov says this is likely because Google doesn't have this technology built into its mobile apps. (On desktop, Gmail's web client does appear to block the tracker from functioning properly.)

It's not clear how widely used Supertracker is right now, or if it will ever rise to the level of notoriety as Davidson's blog post exposing Superhuman's unsavory offerings. But it does make a strong case that this type of technology has not only been around for a long time, but it's also relatively easy to throw together with some standard coding chops and the right amount of reckless abandon with regard to user privacy and product development ethics.

"Plenty of companies seem more than willing to offer tracking technology"
If anything, Asparouhov is exposing with a free, open source product the type of mindset that is likely bubbling under the surface of all too many startups in the marketing,

advertising, and sales industries. There are countless companies that appear eager to offer these type of tracking and data-collection features to stay competitive and because they're implemented in clandestine enough fashion as to go under the radar of most everyday internet users.

With Superhuman, the company's CEO Rahul Vohra admitted that he didn't properly consider how a product he designed to please email superusers and give them features they *asked* for could possibly have ripple effects on the greater public. You can find that argument repeated ad nauseam, from high-level executives and CEOs at Facebook and YouTube and any number of other companies now reckoning with how technology can be misused and contorted to ends these entrepreneurs never considered or were too blinded by growth and profits to acknowledge.

But just as Asparouhov's approach highlights the ease with which technology can overstep ethical boundaries, it's Davidson's willingness to call out even the hot and shiny new startup on the block that helps the public wake up to the privacy-violating practices occurring all around us. Both approaches could ultimately end up being necessary in pushing companies to better protect us, and pushing users to finally realize the way tech's adverse side effects may be harming them in subtle but insidious ways.