ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS
CUSTOM REPORT

Generated on 02/21/2020 by Illya Sukhanov

How Trafigura Put Its Cybersecurity To The Test

02/14/2020 13:51 Jennifer L. SchenkerFollowFeb 14 · 7 min read

The global commodities trading firm replicated the NotPetya worm, strengthened it and then unleashed it on its production environment to assess its ability to fight back

Mark Swift was sitting in his third floor office at global commodities trading firm Trafigura in the Mayfair district of London's West End when he first starting hearing reports about NotPetya, a computer worm attack. The worm rapidly spread around the world in June, 2017, crippling multinational companies including global shipping company Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food

producer Mondelēz, and manufacturer Reckitt Benckiser, among others, causing an estimated $10 billion + in damages.

“It was clear there was a major problem; we got a very early understanding that something was going on that was much more significant than the usual ransomware but no one had a clear picture of what was happening,” says Swift, Trafigura’s Chief Information Security Officer. “There was a huge amount of confusion and quite a bit of angst. It was incredible that so many companies were being hit at the same time and extremely worrying because you can’t defend against what you don’t understand.”

Swift’s job it is to ensure the company can effectively play defense against cyberattacks. Trafigura manages more than $54 billion in assets and moves over $170 billion per annum of commodities around the world by ship, barge, truck, rail and pipeline.

While Swift believed the company was reasonably safe he could not quantify the risk. “The questions I kept asking myself is how does the worm get in, how does it move and would our defenses hold out?” he says. “The difficult thing is you don’t have a way to test. Working on assumptions is not a good way to be measuring your defenses.”

There was only one way to be sure: do the unthinkable.

With the help of NCC Group, a global firm specializing in cybersecurity and risk mitigation, Swift hatched a plan to replicate the Notpetya worm, strengthen it, and then unleash it on the company’s production environment, with the full support of the CEO and the board. The audacious move was deemed to be an acceptable risk because Trafigura had standardized the way it exercises cyber hygiene, something the World Economic Forum’s Centre For Cybersecurity has been encouraging companies to do.

Swift, a member of a World Economic Forum committee to improve resilience for the oil and gas industry, agreed to an interview with The Innovator in the hopes that Trafigura’s experience will help other large enterprises better prepare their cyber defense.

Deconstrucing NotPetya

It was one of Trafigura’s lead engineers that first suggested testing how well the company’s defenses would stand up to the NotPetya worm under controlled circumstances. Swift liked the idea and approached NCC Group. They struck an agreement: If the cybersecurity firm could help develop a replica of the worm Trafigura would test it and- if all went well — NCC could use the case as a reference to sell the service to other big corporate clients.

Oliver Whitehouse, NCC Group’s Global Chief Technology Officer, remembers the first discussion about replicating Notpetya with Swift, whom he has known for 20 years. “We were coming off a

busy summer in the U.K. We had two major worms, the last of which was NotPetya. Mark [Swift] was getting questions from his chief executive about whether it would have an impact on Trafigura. Mark could just say 'we think our controls would limit the impact' but it was very much a theory and he could offer no definitive assurance. When he outlined that he would like to run this test to quantify the risk I told him 'we can do that.' I had the confidence that we could replicate NotPetya by deconstructing it and then reconstructing it," says Whitehouse.

Swift's team and NCC Group started the work in November of 2017. "We decided to rewrite the worm so we knew exactly what every line of code did," says Swift. "We discovered a coding mistake in the way it moved and stole tokens and the way it scanned. It wasn't as efficient in moving as it might have been so we corrected those mistakes to make it even stronger." The team also installed kill switches to ensure the worm didn't proliferate outside of Trafigura's network and accidentally infect suppliers and partners.

The process was supposed to take three months but took a year.

"The complex bit was having the confidence that the controls would work and that it would not go awry and be disruptive," says Whitehouse. " We worked on the principle that if there was any doubt the first instruction was to shut itself down, ensuring that it would only spread to computer networks directly under Trafigura's control. There were key systems in the industrial operations technology in areas such as mining and fuel terminals that had to be excluded but all the corporate assets could be included. Then we built in various other safeguards, such as the rate at which it could propagate so it would not overload the system. We did three full environment tests before we even got near the production and were confident that the controls could do what they said they are going to do."

Getting Sign-Off

Getting the company's leadership to sign-off was an important part of the process. Trafigura, stores and delivers the commodities it trades, which includes approximately six million barrels of oil a day. In order to buy the assets that it later trades it has established access to credit from 155 banks. It has to manage credit risks, legal risks, IT risks and liquidity risks and all of these risks are integrally linked. "We are a high volume, low margin business," explains Christophe Salmon, Trafigura's Chief Financial Officer. "Our business is based on arbitrage, we fight for the last cent per barrel. Any basis point matters in terms of protection of our margins. If the integrity of our system was compromised it would have consequences in being able to conduct our business and in the daily reporting to our financial partners,", a factor that could impact Trafigura's access to both credit and its liquidity. "This was why, in discussing with Mark, testing the strength and integrity of our system — and identifying any potential vulnerabilities — was so important," says Salmon.

Unleashing The Worm

On November 8, 2018 the worm was unleashed. Swift, together with Trafigura's lead engineer, Whitehouse and an NCC Group developer huddled around a group of computer screens. "We looked at each other and said 'should we run it?', remembers Swift. "I paused for a moment and wondered 'What on earth am I doing?' before giving the green light. And then we waited for the havoc to begin."

Thirty minutes went by. Nothing happened. Then the worm found its way in through an unpatched computer in Switzerland and exploited that entry to gain privileges. At that point the team thought it would spread like wildfire. But to their surprise it didn't, due to a security configuration Trafigura had made that they had not fully appreciated. So the team launched different scenarios, purposely infecting different 'patient zeros' increasingly notching up the level of exposure. Eventually a misconfiguration in a software development network lit the fuse and the worm started to spread aggressively throughout the development environment, moving from from machine to machine and location to location. "We tracked the various ways the worm jumped between systems and were able to create a good map and a good understanding of its speed and its ferociousness," Whitehouse says.

The value of the test data can't be overstated, he says. Trafigura used it to make adjustments to its network. "This one configuration change by Trafigura significantly disrupts the speed at which worms can propagate even if they can access highly privileged systems," says Whitehouse.

To Swift's great relief unleashing the worm in this controlled manner had no operational impact on the business. None of the company's computer users noticed a thing.

Key Takeaways

NCC Group is eager to run similar tests for other big corporates but so far there have been no other takers. Although a number of big companies have expressed interest in doing so they have had trouble getting internal sign-off. Whitehouse says that often organizations think they have a picture of what their computer networks look like. However, 99% of the time this does not reflect reality. Knowing who is connected is one of the first things a company has to do to ensure its cyber security. The map needs to be accurate "at any point in any week," he says. "When I ask what is on their network, who is responsible for it, what each device does and what business operation it underpins they look at me quizzically and say they don't know. If you don't know then you don't know what your risk is. You have to understand the material risks before you can unleash tests like Trafigura's."

Swift agrees. "One of the reasons why we were more capable of running this was we know where the edge of our network boundary is," he says. "You have to fundamentally understand how many machines you have and where they are to be able to sign off on something like this. We spend a lot of time standardizing our environment because we believe you need to do things to standard and enforce things to standard."

One of thetakeaways from the test was that having hard data and being able to really measure risk is key, says Swift. Trafigura thought that being 99.9% compliant in some areas was good enough. It was not. “So now we understand that and if anybody says we are being overly cautious we can demonstrate why we need to do what we do. We believe it is worthwhile to get better at testing and measuring the effectiveness of security in our internal network, but is only worth doing if you also have an appetite to introduce major controls.”

Swift says he has no illusions. Controls or no controls the attacks will keep coming. The next worm, the next virus, is likely to be more virulent. And no matter how good its cyber defense is Trafigura — like any other company on the planet — will have to continue to be vigilant in the never-ending battle to keep its systems safe.

The Cost of Avast’s Free Antivirus: Companies Can Spy on Your Clicks

01/27/2020 15:30 PCMagJan 27 · 10 min read

Avast is harvesting users’ browser histories on the pretext that the data has been ‘de-identified,’ thus protecting your privacy. But the data, which is being sold to third parties, can be linked back to people’s real identities, exposing every click and search they’ve made.

By Michael Kan

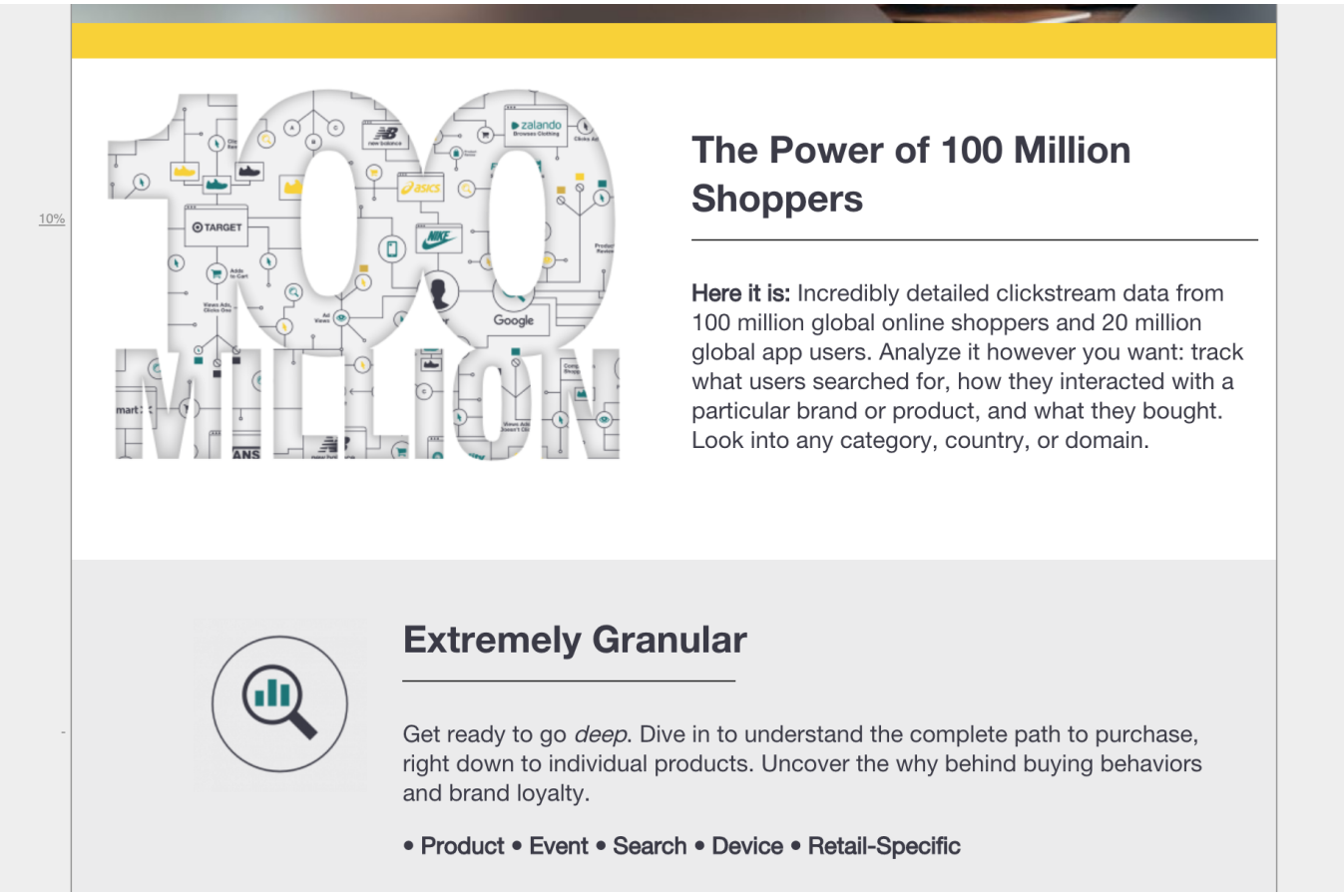
Your antivirus should protect you, but what if it's handing over your browser history to a major marketing company?

Relax. That's what Avast told the public after its browser extensions were found harvesting users' data to supply to marketers. Last month, the antivirus company tried to justify the practice by claiming the collected web histories were stripped of users' personal details before being handed off.

"The data is fully de-identified and aggregated and cannot be used to personally identify or target you," Avast told users, who opt in to the data sharing. In return, your privacy is preserved, Avast gets paid, and online marketers get a trove of "aggregate" consumer data to help them sell more products.

There's just one problem: What should be a giant chunk of anonymized web history data can actually be picked apart and linked back to individual Avast users, according to a joint investigation by PCMag and Motherboard.

The Avast division charged with selling the data is Jumpshot, a company subsidiary that's been offering access to user traffic from 100 million devices, including PCs and phones. In return, clients-from big brands to e-commerce providers-can learn what consumers are buying and where, whether it be from a Google or Amazon search, an ad from a news article, or a post on Instagram.



The data collected is so granular that clients can view the individual clicks users are making on their browsing sessions, including the time down to the millisecond. And while the collected data is never linked to a person's name, email or IP address, each user history is nevertheless assigned to an identifier called the device ID, which will persist unless the user uninstalls the Avast antivirus product.

For instance, a single click can theoretically look like this:

At first glance, the click looks harmless. You can't pin it to an exact user. That is, unless you're Amazon.com, which could easily figure out which Amazon user bought an iPad Pro at 12:03:05 on Dec. 1, 2019. Suddenly, device ID: 123abcx is a known user. And whatever else Jumpshot has on 123abcx's activity-from other e-commerce purchases to Google searches-is no longer anonymous.

PCMag and Motherboard learned about the details surrounding the data collection from a source familiar with Jumpshot's products. And privacy experts we spoke to agreed the timestamp information, persistent device IDs, along with the collected URLs could be be analyzed to expose someone's identity.

“Most of the threats posed by de-anonymization-where you are identifying people-comes from the ability to merge the information with other data,” said Gunes Acar, a privacy researcher who studies online tracking.

He points out that major companies such as Amazon, Google, and branded retailers and marketing firms can amass entire activity logs on their users. With Jumpshot’s data, the companies have another way to trace users’ digital footprints across the internet.

“Maybe the (Jumpshot) data itself is not identifying people,” Acar said. “Maybe it’s just a list of hashed user IDs and some URLs. But it can always be combined with other data from other marketers, other advertisers, who can basically arrive at the real identity.”

According to internal documents, Jumpshot offers a variety of products that serve up collected browser data in different ways. For example, one product focuses on searches that people are making, including keywords used and results that were clicked.

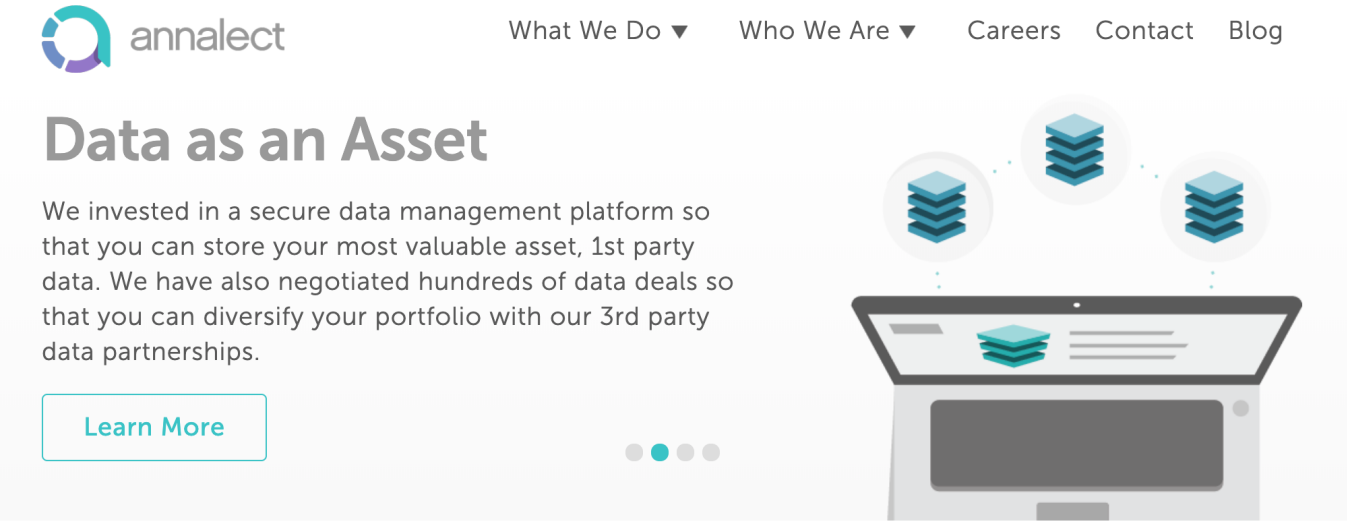
We viewed a snapshot of the collected data, and saw logs featuring queries on mundane, everyday topics. But there were also sensitive searches for porn-including underage sex-information no one would want tied to them.

Other Jumpshot products are designed to track which videos users are watching on YouTube, Facebook, and Instagram. Another revolves around analyzing a select e-commerce domain to help marketers understand how users are reaching it.

But in regards to one particular client, Jumpshot appears to have offered access to everything. In December 2018, Omnicom Media Group, a major marketing provider, signed a contract to receive what's called the "All Clicks Feed," or every click Jumpshot is collecting from Avast users. Normally, the All Clicks Feed is sold without device IDs "to protect against triangulation of PII (Personally Identifiable Information)," says Jumpshot's product handbook. But when it comes to Omnicom, Jumpshot is delivering the product with device IDs attached to each click, according to the contract.

In addition, the contract calls for Jumpshot to supply the URL string to each site visited, the referring URL, the timestamps down to the millisecond, along with the suspected age and gender of the user, which can inferred based on what sites the person is visiting.

It's unclear why Omnicom wants the data. The company did not respond to our questions. But the contract raises the disturbing prospect Omnicom can unravel Jumpshot's data to identify individual users.



Although Omnicom itself doesn't own a major internet platform, the Jumpshot data is being sent to a subsidiary called Annalect, which is offering technology solutions to help companies merge their own customer information with third-party data. The three-year contract went into effect in January 2019, and gives Omnicom access to the daily click-stream data on 14 markets, including the US, India, and the UK. In return, Jumpshot gets paid $6.5 million.

Who else might have access to Jumpshot's data remains unclear. The company's website says it's worked with other brands, including IBM, Microsoft, and Google. However, Microsoft said it has no current relationship with Jumpshot. IBM, on the other hand, has "no record" of being a client of either Avast or Jumpshot. Google did not respond to a request for comment.

Other clients mentioned in Jumpshot's marketing cover consumer product companies Unilever, Nestle Purina, and Kimberly-Clark, in addition to TurboTax provider Intuit. Also named are market research and consulting firms McKinsey & Company and GfK, which declined to comment on its partnership with Jumpshot. Attempts to confirm other customer relationships were largely met with no responses. But documents we obtained show the Jumpshot data possibly going to venture capital firms.

Wladimir Palant is the security researcher who initially sparked last month's public scrutiny of Avast's data-collection policies. In October, he noticed something odd with the antivirus company's browser extensions: They were logging every website visited alongside a user ID and sending the information to Avast.

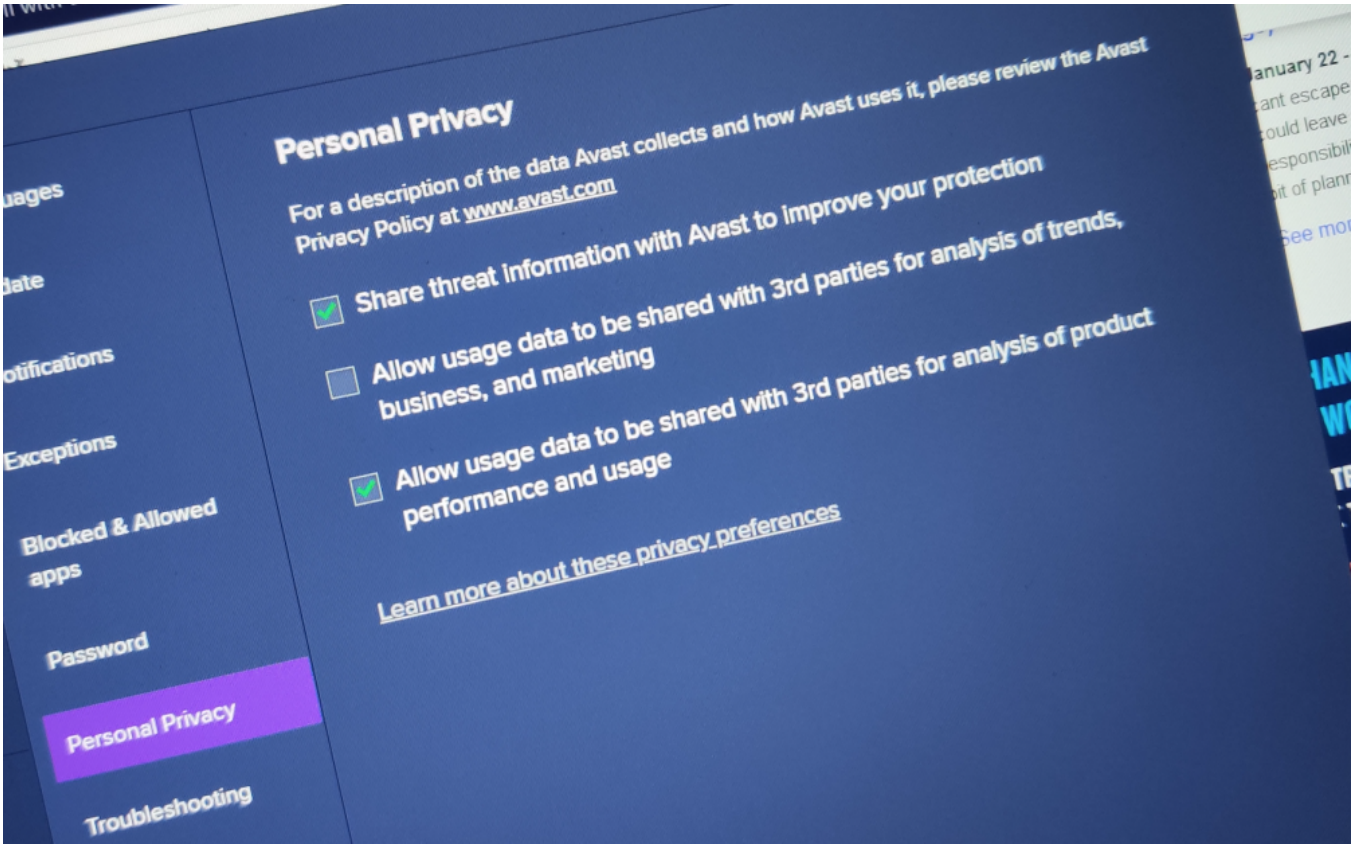
The findings prompted him to call out the extensions as spyware. In response, Google and Mozilla temporarily removed them until Avast implemented new privacy protections. Still, Palant has been trying to understand what Avast means when it says it "de-identifies" and "aggregates" users' browser histories when the antivirus company has refrained from publicly revealing the exact technical process.

"Aggregation would normally mean that data of multiple users is combined. If Jumpshot clients can still see data of individual users, that's really bad," Palant said in an email interview.

One safeguard Jumpshot uses to prevent clients from pinpointing the real identities of Avast users is a patented process designed to strip away PII information, such as names and email addresses, from appearing in the collected URLs. But even with the PII stripping, Palant says the data collection is still needlessly exposing Avast users to privacy risks.

"It is hard to imagine that any anonymization algorithm will be able to remove all the relevant data. There are simply too many websites out there, and each of them does something different," he said. For example, Palant points out how visiting the collected URL links for one user could consistently reveal which tweets or videos the person commented on, and thus expose the user's real identity.

"It's almost impossible to de-identify data," said Eric Goldman, co-director of the High Tech Law Institute at Santa Clara University, who also took issue with an antivirus company monetizing users' data. "That just sounds like a terrible business practice. They're supposed to be protecting consumers from threats, rather than exposing them to threats."



We asked Avast more than a dozen questions concerning the extent of the data collected, who it's being shared with, along with information about the Omnicom contract. It declined to answer most of our questions or provide a contact for Jumpshot, which didn't respond to our calls or emails. However, Avast did say it stopped collecting user data for marketing purposes via the Avast and AVG browser extensions.

"We completely discontinued the practice of using any data from the browser extensions for any other purpose than the core security engine, including sharing with Jumpshot," the company said in a statement.

Nevertheless, Avast's Jumpshot division can still collect your browser histories through Avast's main antivirus applications on desktop and mobile. This include AVG antivirus, which Avast also owns. The data harvesting occurs through the software's Web Shield component, which will also scan URLs on your browser to detect malicious or fraudulent websites.

For this reason, PCMag can no longer recommend Avast Free Antivirus as an Editors' Choice in the category of free antivirus protection.

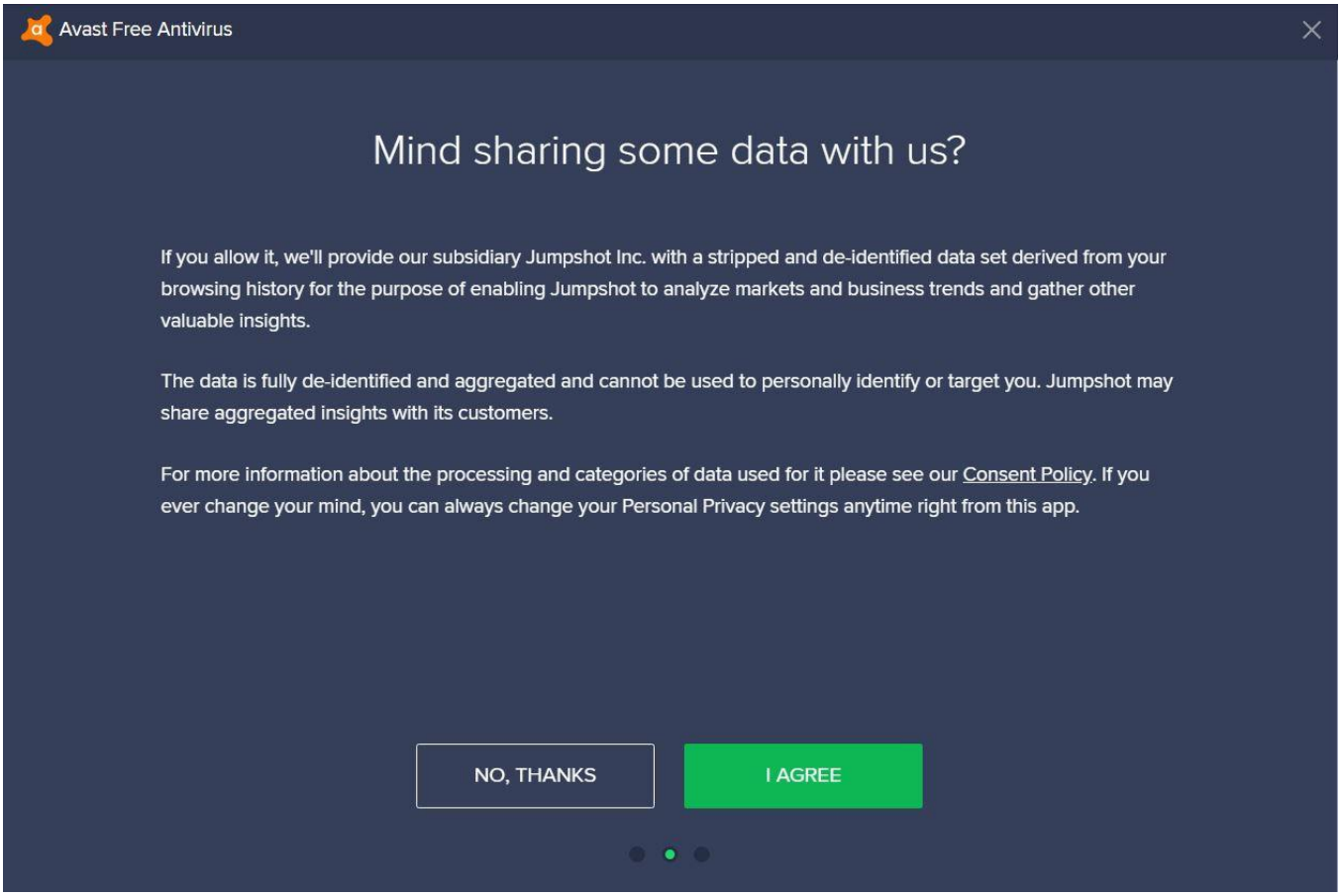
Whether the company really needs your URLs to protect you is up for debate. Avast says taking the

information directly and letting Avast's cloud servers immediately scan them provides users with "additional layers of security." But the same approach has its own risks, according to privacy researcher Gunes Acar, who said the safest way to process visited URLs is to never collect them. Google's Safe Browsing API, for example, sends an updated blacklist of bad websites to your machine's browser, so the URLs can be checked on your machine rather than over the cloud.

"It can be done in a more private way," Acar said. "Avast should definitely adopt that. But it seems they're in the business of making money from the URLs."

On the flip side, Avast is offering a free antivirus product. The company also points out the browser history collection is optional. You can shut it off on install or within the settings panel.

"Users have always had the ability to opt out of sharing data with Jumpshot. As of July 2019, we had already begun implementing an explicit opt-in choice for all new downloads of our AV (antivirus), and we are now also prompting our existing free users to make an explicit choice, a process which will be completed in February 2020," the company said.



Indeed, when you install the Avast or AVG antivirus on a Windows PC, the product will show you a pop-up that asks: “Mind sharing some data with us?” The pop-up will then proceed to tell you the collected data will be de-identified and aggregated as a way to protect your privacy.

However, no mention is made about how the same data can be combined with other information to connect your identity to the collected browser history. Nor does the pop-up mention how Jumpshot can retain access to the data for three years. For that detail, you’ll have to look at the fine print in Avast’s privacy policy.

As a result, users who see the pop-up may assume their data will be protected, and opt in when in reality, the privacy policies around tech products are often deliberately vague and simplified. “You want the consumer to buy or use your product. But you don’t want to scare them either,” said Kim Phan, a partner at legal firm Ballard Spahr, who works in privacy and data security group.

The trade-off is that the policies can become opaque. “It’s harder to figure out what you’re doing,” she added. “People won’t be able to understand the details, or they will think you are trying to hide something.”

In Avast’s case, the controversy around the largely unknown data-collection practices prompted enough scrutiny that US Sen. Ron Wyden decided to investigate. “Americans expect cybersecurity and privacy software to protect their data, not sell it to marketers,” he tweeted at the time.

In a statement, Wyden said he was encouraged that Avast is ending the data collection through the company’s browser extensions. “However I’m concerned that Avast has not yet committed to deleting user data that was collected and shared without the opt-in consent of its users, or to end the sale of sensitive internet browsing data,” he added. “The only responsible course of action is to be fully transparent with customers going forward, and to purge data that was collected under suspect conditions in the past.”

Originally published at https://www.pcmag.com.